

Vulnerability Assessment and Penetration Testing Report

Client	ABC Pvt. Ltd.
Assessment Date	04-06-2024
A	





About Invia

Invia is a cybersecurity, SAAS and Enterprise consulting company headquartered in Sydney, with a presence across South-East Asia and India. We provide solutions to leading companies around the globe in various sectors like telecom, banking, logistics, aviation, healthcare, energy, government, education.

We provide 360-degree cyber security solutions. We help you identify vulnerabilities and protect your data. Our services include Vulnerability Assessment & Penetration Testing (VAPT) and Attack Surface Management. VAPT is designed to test the overall security of web applications, mobile applications, network and cloud by performing an in-depth security analysis. We provide you with detailed reports and actionable insights to help secure your network and data.

Private and Confidential

This report ("Report") is confidential and proprietary to Invia Pty. Ltd. ("Invia") and is intended solely for the private and confidential use of the client, ABC Pvt. Ltd. ("Client"). The contents of this Report, including any information, data, or analysis contained herein, shall not be copied, used, distributed, or disclosed to any third party without the prior express written permission of Invia or the Client. Unauthorized use, copying, distribution, or disclosure of this Report is strictly prohibited and may violate applicable laws. Legal action may be taken accordingly.



Table of Contents

Web Application Penetration Testing1
1.1 Executive Summary1
1.2 Background1
1.3 Objectives1
1.4 Scope of Assessment2
1.5 Out of Scope2
1.6 Tools Used3
1.7 Summary of Findings4
Vulnerability Details
2.1 CSRF leads to account takeover5
2.2 CSRF on the Claim Create/Update page9
2.3 Weak Password Policy (password in plain text)14
2.4 No Rate Limit15
2.5 Token doesn't implement properly (Token Misconfigured)18
2.6 Outdated jQuery and Bootstrap20
2.7 Clickjacking21
2.8 Server Information Disclosed23
2.9 HTTP Strict Transport Security (HSTS) Header is Missing24
2.10 CSP Not Implemented25
Testing Methodology
Common Vulnerabilities
Risk Assessment
Terms and Conditions



Web Application Penetration Testing

1.1 Executive Summary

ABC Pvt. Ltd. engaged Invia to conduct a white-box penetration test for their web application. Our work was limited to the specific procedures and analysis described herein and was based only on the information made available through 4th June 2024 to 9th June 2024. Accordingly, changes in circumstances after this date could affect the findings outlined in this report.

The purpose of these Web Security Assessments was to identify exploitable vulnerabilities and insufficiently configured security controls to determine the likelihood that users with considerable, little, or no prior knowledge of the applications (e.g., informed, and uninformed insiders and outsiders) could exploit weaknesses in their applications as those cataloged in the OWASP Top 10, OWASP ASVS, SANS, NIST, OWASP testing guide and Penetration Testing Execution Standard.

The assessment also included a review of security controls and requirements listed in the OWASP Application Security Verification Standard (ASVS). This review does not, nor is it intended to, identify all the potential vulnerabilities in all applications.

The team leveraged tools to facilitate their work, however, the majority of the assessment involved manual analysis. The details of the tools used in the assessment are given in this report.

The results summarized in this document are based upon a collection of methodologies and tests interacting at a single point in time with technology that is continually changing and becoming ever more complex. Any projection to the future of the findings contained in this document is subject to the risk that they may no longer portray the system or environment in existence at that time because of change.

1.2 Background

This exercise aimed to perform Penetration Testing of the Applications in scope to determine if they were vulnerable to attacks and exploitation. The test consisted of manual testing to detect and exploit vulnerabilities.

The assessment was conducted to identify the security vulnerabilities in the Application in scope and propose solutions for the project team to remediate the identified vulnerabilities to make the Application more secure.

The Security Assessment was performed by Invia Pty. Ltd. between 4th June 2024 to 9th June 2024.

1.3 Objectives

The objective of the tests performed was to:

- Identify the possible vulnerabilities and gaps in the web applications.
- Assess the gaps and vulnerabilities to determine the Risk associated.
- Suggest recommendations to overcome existing vulnerabilities and gaps.



This assessment report contains:

- Technical details of the vulnerabilities discovered with substantiation of the exploits.
- **Risk mitigation recommendations** that need to be implemented to ensure that the systems are secure from the risks arising due to the discovered vulnerabilities.

1.4 Scope of Assessment

The scope for this Security assessment includes, but is not limited to, the following tests:

- Information Gathering
- Configuration Management
- Business Logic
- Authentication
- Authorization
- Session Management
- Data Validation, Governance, and Transfer.

URLs

DEMO URL

Accounts

User	Role
J1@invia.co.in	Self-Register

Environment Details

Application Name	Demo
Environment	Production
Accessibility	INTERNET
Authentication Method	Login
Backend	AWS

1.5 Out of Scope

The following activities and applications were considered out of scope for this Engagement:

- Social Engineering
- Denial of Service
- Vulnerability Fixes
- Intrusive Tests and Exploitation



As this is a production system, we did not perform the following tests as it could potentially impact customers.

- Denial of Service (DoS) Attacks
- Brute Force Attacks
- Directory Fuzzing
- Exploits with Known Consequences
- Data Manipulation or Deletion
- Excessive Traffic Generation
- Unverified Third-Party Tools or Scripts
- Social Engineering Attacks
- Exhaustive Vulnerability Scanning
- Security Tests without Proper Authorization

1.6 Tools Used

Invia penetration testing team uses a combination of manual testing and commercial/open-source tools as part of its penetration testing methodology. This is accompanied by custom scripts to ensure optimum results.

The following tools are used for the testing.

- Burp Suite
- Nmap
- Mozilla Firefox Plugins
- Kali Linux



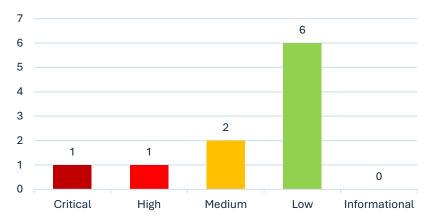
1.7 Summary of Findings

The Web Vulnerability Assessment and Penetration Testing (VAPT) conducted for the target organization yielded important findings and insights. This summary provides an overview of the key results obtained during the assessment.

It was observed that the application was exposed to a total of **10 security vulnerabilities** during the given assessment tenure with 1 as Critical, 1 as High 2 as Medium, & 6 as Low Severity vulnerabilities.

S. No.	Name	Severity	Risk Score	Status
1.	CSRF Leads to account takeover	Critical	9.1	Unresolved
2.	CSRF on the claim Create/ Update page	High	8.8	Unresolved
3.	Weak Password Policy (Password in plaintext)	Medium	6.5	Unresolved
4.	No Rate Limit	Medium	5.0	Unresolved
5.	Token doesn't implement properly (Token Misconfigured)	Low	3.1	Unresolved
6.	Outdated jQuery and Bootstrap	Low	3.1	Unresolved
7.	Clickjacking	Low	4.0	Unresolved
8.	Server Information Disclosed	Low	3.1	Unresolved
9.	HTTP Strict Transport Security (HSTS) Header is missing	Low	3.0	Unresolved
10.	CSP not implemented	Low	3.1	Unresolved

Critical High Medium Low Informational





Vulnerability Details

In this section we will give details of the observed vulnerabilities in the website.

2.1 CSRF leads to account takeover

Parameter	Description
Severity	Critical
Impact	Critical
Risk Score	9.1
Affected URL	https://demoURL
Threat	 The impact of a successful CSRF attack can be severe, leading to unauthorized actions and potential account takeover: 1. Account Takeover 2. Data Manipulation 3. Privacy Violations

Cross-Site Request Forgery (CSRF) is a security vulnerability that arises when an attacker tricks a user's web browser into making unintended and potentially harmful requests on a targeted website where the user is authenticated. This occurs by exploiting the trust that a website places in the user's browser, allowing the attacker to perform actions on behalf of the user without their consent.

It has been observed that an attacker can craft a forged page to take over the account of a legitimate user by sending the forged page/ link.

Steps to Reproduce

- 1. Access given URL <u>https://demoURL</u>
- 2. Enter your registered email address to get the forgotten password link

c													×	9	- 0	5	×
e → o	¢							2									-
🕀 Import bookmarks 🔞	Getting Started 👋 Invia e	Contracts 🔛 What is a M	agic Byte 🧖 Android	Filda + A wo	- P&G Money	Back Galar											
										L	og In						
			Change/Rese	t My Pa	ssword												
			Please enter your en	nail address	and further instr	ructions will be e											
			Email Address *	ji@invi	a.co.in		* Decisites as	exclutory Refer									
			fm not a rob	ot	ROAPTDIA Pring-Term												
			\square		CONTIN	VUE		\supset									
			1	Contact Us	Terms & Con	nditions Priv	vacy Policy										

3. Open the link given in the mail that you have received and click on the **'click here.'** to open the change password page



P&G Money Back Guarantee - Password Reminder		
🗊 Delete 🗧 Archive 🕧 Report 🗸 🗠 Reply 🗞 Reply a	all 🔿 Forward 🗸 🔍 Zoom 🛛 🖄 Read / Unread 🖉 Categorize 🗸 📮 Flag / Unflag 🗸 🕞 Print 🛛 🚥	
CAUTION: This email originated from outside of the organization. Do not click	inks or open attachments unless you recognize the sender and know the content is safe.	
	Dear Javed,	
	We recently received a request to resend your password associated with this e-mail address.	
	You can log in by <u>clicking here</u> and entering your password:	
	(If the link above doesn't work, please copy the following into your browser <ahtps: mbg.campaign.net.au="" oraib="" trackclaim="">)</ahtps:>	
	OR	
	If you wish to create your own password, please click here	
	(If the link doesn't work, please copy the following into your browser	
	<htps: forgotpassword\$\$?token="setsature</td" mbg.campaign.net.au="" orab=""><td></td></htps:>	
	Kind Regards,	
	P&G Promotions Team	

4. Enter new password and confirm password

	+	✓ - ∅ ×
$\leftarrow \rightarrow \circ$ (\$	ල 🕑 🚰 🚰 🚰 🛍 🖬 ම ණ දු =
- Import bookmarks 🔲 Getting Started 🐜 Invia eContracts 🚥 What is	a Magic Byte 🗧 Android Frida • A wo 🔷 P&G Money Back Guar	
		Log In
	Change/Reset My Password Please enter a new password	
	*Denotes mandatory fields Password *	
	Confirm Password • ••••	
	CONTINUE	
	Contact Us Terms & Conditions Privacy Policy	

5. Click continue and intercept the request in Burp Suite, Right click on the request, and click on Generate CSRF PoC.



Burp Project Intruder Repeater View Help Param Miner Server Side Dashboard Target Provy Repeater Intruder Collaborator S	Prototype Pollution Logger++ E	Burp Suite Professional v2023.12.1.5 - Temporary Project - licensed to Invia Pty Ltd [3 user license] - Ø X
Dashboard Target Proy Repeater Intruder Collaborator S Intercept HTTP history WebSockets history @ Proy settings	Scan Do passive scan Do active scan	Logger Organizer Extensions Learn CSP Upload Scanner Logger++ (④ Settings
Forward Drop Intercept is on Action Or	Send to Intruder Ctrl+I	Add notes 👋 HTTP/2
Pretty Raw Hex	Send to Repeater Ctrl+R Send to Sequencer	🖬 \n ≡ Inspector ■ 🔳 Ξ ÷ ③ × 🔒
2 Rock may campaign net an 3 Cookie: JSESSIONID=TEB64C841ADD61F1096ED0F64FEF9105; _ga=GA1.3.543300801 GA1.3.146175305 1700794655	Send to Comparer	8074238.7.1.1708075424.0.0.0; _g14+ Request attributes 2 v 3
Wallsline (1996) (1997) (19	Send to Decoder Send to Organizer Ctrl+O	Request query parameters 0 🗸
<pre>% Accept imaging: on expine the state, br % Content-Type: application/x-www-form-urlencoded 9 Content</pre>	Insert Collaborator payload Request in browser >	Request body parameters 3 V
10 Origin 11 Referet. https://mwg.camparyn.net.an/orans/iorgotrasseoru 12 Upgrade-Insecure-Requests: 1	Extensions >	Request cookies 4 V Z
18 Sec-Fetch-Dest: document 14 Sec-Fetch-Mode: navigate 15 Sec-Fetch-Site: same-origin	Engagement tools > Change request method	Find references Discover content
10 (Berfach-User 7) 7s: traiter 19 19 passerfdreet.confirmPasserfdreer.combait=Continue	Charge body encoding Copy URL Copy as curl command (bash) Copy to file Paste from file Save item	Schedule task Generate CSRF PoC
	Don't intercept requests > Do intercept >	
	Convert selection > URL-encode as you type	
	Cut Ctrl+X	
	Copy Ctrl+C	
	Paste Ctrl+V	
⑦ ⑦ ← → Search	Message editor documentation	D highlights
Event log (1) All issues (7)	Proxy interception documentation	Memory: 634.3MB

6. Click on copy HTML

S CSRF PoC generator			- 0	×
Request to:			Option	s ?
Pretty Raw Hex 🗊 🗤 🚍	Inspector		÷	©×
1 POST /Forgotpassword HTTP/2 2 Host: 3 Cookie: JSESSIONID=7EB64CB41ADD61F1096ED0F64FEF9105; _ga=	Request attribute	15	2	~
GAL.3.943308801.1708620187; <u>g</u> a_JHNQ4P1144= GSL.3.1708074205.7.1.1708075424.0.0.0; <u>gid</u> = GAL.3.2146179309.1708794657 User-Agent : Momilla/5.0 (Windows NT 10.0; Win64; x64;	Request query pa	arameters	0	~
<pre>over agenc: noziia/s.o vandow ar A0.0, windy, xey, iv:12:0.0 Gecko/20100101 Firefox/12:0.0 5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/a</pre>	Request body pa	rameters	3	~
vit, image/webp, */*; q=0.8 ? { ? } ← → Search	Request cookies		4	~
<pre>1 chtml> chtml> <form action*<br=""><form action*<br=""><imput name*"password"="" type="hidden" value*"testb123#"<br=""><imput name*"confirm2assword"="" type="hidden" value*"testb123#"<br=""><imput name*"submit="" type="hidden" value*"confirm"=""></imput> <imput name*"submit="" request"="" type="hidden"></imput> <iform> <form> <form> <form> document.forms[0].submit(); document.forms[0].submit();</form></form></form></iform></imput></imput></form></form></pre>		11.>		
14 5 //ttsl>				
⑦ (亞 ← → Search		Q	0 hig	hlights

7. Create HTML file and paste copied script in file



File Ec	lit Selection Find View Goto Tools Project Preferences Help
4 ►	csrf.html ×
	<html></html>
	<pre><!-- CSRF PoC - generated by Burp Suite Professional--></pre>
	<body></body>
	<pre></pre>
	<input name="password" type="hidden" value="Test@123#"/>
	<pre><input name="confirmPassword" type="hidden" value="Test@123#"/></pre>
	<pre><input name="submit" type="hidden" value="Continue"/></pre>
	<input type="submit" value="Submit request"/>
10	<script></th></tr><tr><th>11</th><th>history.pushState('', '', '/');</th></tr><tr><th>12</th><th><pre>document.forms[0].submit();</pre></th></tr><tr><th>13</th><th></script>
14	
15	<pre>//html></pre>
16	

8. Open the created HTML file in the browser and click on Submit button

ō			+
÷	\rightarrow C	file:///C:/Users, //Desktop/csrf.html	습
-Ð Im	nport bookmarks 👈	Getting Started 🛛 🐜 Invia eContracts 🛛 🚥 What is a Magic Byte 🛛 🧣 Android Frida • A w	ю
Subr	nit request		

9. Here we can see the password change page, the password change functionality was not working, if the change password functionality works properly, the password can be changed.

Change/Reset	My Password
Please enter a new pas	sword
The password cont	ains illegal characters.
	* Denotes mandatory field
Password *	Enter Password
Confirm Password *	Confirm Password
	CONTINUE

Resolution of Vulnerability

Several measures can be implemented to mitigate the risk of CSRF attacks and enhance web application security:

- 1. Anti-CSRF Tokens:
 - Include unique, unpredictable tokens in each form or request.



- These tokens are generated on the server side and embedded in web pages or included in requests.
- The server verifies the token's authenticity before processing the request, ensuring it originated from a legitimate source.

2. Same Site Cookie Attribute:

- Set the Same Site attribute for cookies to control when cookies are sent with cross-site requests.
- This attribute helps prevent the browser from sending cookies in requests initiated by third-party websites.

3. Origin Header Checking:

- Validate the origin header to ensure that requests are coming from the expected source.
- This helps verify that requests originate from the same domain and are not forged by malicious actors.

4. Referrer Header Checking:

- Check the referrer header to confirm that the request originated from the same site.
- While this method may have limitations (due to referrer header omission in some cases), it adds an extra layer of validation.

Parameter	Description
Severity	High
Impact	High
Risk Score	8.8
Affected URL	https://demoURL
Threat	 The impact of a successful CSRF attack can be severe, leading to unauthorized actions and potential account takeover: 1. Account Takeover 2. Data Manipulation 3. Privacy Violations

2.2 CSRF on the Claim Create/Update page

Cross-Site Request Forgery (CSRF) is a security vulnerability that arises when an attacker tricks a user's web browser into making unintended and potentially harmful requests on a targeted website where the user is authenticated. This occurs by exploiting the trust that a website places in the user's browser, allowing the attacker to perform actions on behalf of the user without their consent.

It has been observed that an attacker can craft a forged page of the claim update page and send it to a legitimate user to update the user's claim data.

Steps to Reproduce

- 1. Access the URL after logging in with your credentials <u>https://demoURL</u>
- 2. Click the "Make Another Claim" button



► +								~	-	ø	×
← → C O A		<u>ث</u>			۲		. 🕾	e ii e		<i>a</i> e ;	
🕣 Import bookmarks 😆 Getting Started 🐜 Invia eContracts 🚥 What is a Magi	c Byte 🧣 Android Frida • A w	10m									
					Log(Out					
	Your Claim Details			 							
	Claim ID										
	Claim Status	CLAIM - Please mail us your goods									
	Gift	CASHBACK									
	Date Submitted	Tue Feb 20 16:36:02 AEDT 2024									
		UPDATE CLAIM	\supset								
		MAKE ANOTHER CLAIM	\supset								
		Its Terms & Conditions Drivery Delicy									

3. Fill in the blanks

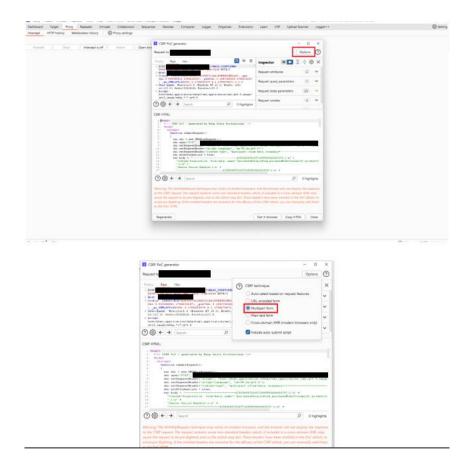
0											
	08				ŵ		۲		8 9		
🖅 Import bookmarks 👋	Getting Started	inve eContracts 🛛 🖶 What is a Magic Byle 💷 🔗 A	ndroid Frida • A wo								
		BSB/Branch Number * '	123456								
		Bank Account Number **	1122334455								
		[*] Please ensure correct entry	of bank account details. Th	e Promoter is not liable for errors. Refer	to terms and condition						
		Questionnaire									
		Please answer the questions I	selows		* Densites manufatory R	rida					
		What is your age?*		25-34		¥.					
		What is your Gender?*		Please Select		÷					
		Why did you return your pr	oduct?*	Upgraded to newer model		÷					
		I have read and accept	ed the promotion Terms 8	Conditions							
		Your data is being collected in	accordance with the Privi	acy Policy. For more details please click I	here.						
				NEXT)					

4. Click on NEXT button and intercept the request in Burp suite, right click on the request, Click on Generate CSRF POC.



HTTP hanny WebSodats hanny @ Proy sets Proved Drop Preval	Open browser							
Forward Drop Intersect is on Action city Rev Hes 2018 water_craships and as water_craships.adu								
Forward Drop Intersect is on Action city Rev Hes 2018 water_craships and as water_craships.adu								
POIN NAME OF A DESCRIPTION OF A DESCRIPT	177-8244-1877-2204-7648-2440 M							
POIN NAME OF A DESCRIPTION OF A DESCRIPT	177-8041-5807-2004-7148-0440 B						D 10 =	
How has compared in the second statistical pression when any marging to the second statistical pression of the second sta		2142					_	
			0.1700426197/	 	1.170007007	4.0.0.0		
Const-Agent: Monthla/1.0 (Windows 37 13.0) Winds; add; svil2.0 Accept: Yest/Dial, application/shial/sal, application/sal.q/0.5.	D deven/20080131 Firefue/122. Deven/artif. in one forder #/*.cold							
Arrept-Language: etc.72, ex. q=2.1								R
Accept-Bacoding: quip, deflate, be	Scan	2						
Control Type: unltipart/form-data; brandarys Context-length: 3170	Do passive scan	1290						Re
Caragan	Do active scan							1.0
Beferrer	Do active scan							
Upperson-Investore-Imparator 1 Ser-Peterb-Dest: decomposition	Send to Intruder 0	tri+1						Re
Ber-Jetch-Bele: nevigete	Send to Repeater C	de R						
Ser-Feldh-Dite: Anne-ortigte Ber-Feldh-Dest: 14								R
Tel Synthese	Send to Sequencer							
	Send to Comparer							
Contem-Dispeniation: form-data; name"purchaseDetailsForm per	Send to Decoder							
content-superiore. Constant and parameterine par								
Cendus Series Randles	Send to Organizer CI	1+0						
Contem-Signation: form-data: name"purchaseSecultSic pur	Insert Collaborator pavioad							
contraction to be and the particulation of the								
4146	Request in browser	2						
42053404701497149704036666669292 Content-disposition: Frem-data; house-beneficientedefecter	Extensions	>						
commentation interact, and personality of part	The second second second	1 Pres	references					
	Engagement tools							
(205360470149714090036666660292 Content-Dispersition: Form-data; mage-"purchase2etails?co.co.	Change request method	Disc	over content					
	Change body encoding	Ste	dule task					
145612								
Contant-Waspenition: from tinta, mann' purchasalat ailaFren eur	Copy URL	Gen	enate CSRF PoC					
	Copy as curl command (bash)							
11/82/2824 1745 3464 781 4771 49780 344444 3197	Copy to file							
Content "Risposition: four-later name-"purchaseDetailsFrom.cor								
Content-Type: application/ortet-stream	Paste from file							
	Save item							
120534047014971409003666669292	Don't intercept requests	2						
Content-Disposition: from data; name*purchaseDetailsTres.rec								
04000	Do intercept	>						
126636047016971698603666683292	Convert selection							
Content-Faspenation: Econ-data: maner'purchase2stailsFrem.cor	URL-encode as you type							
472536047016971699803666663297	Cut C	x++X						
Content-Dispersition: Contributer name-'purchaseDetailsFrem.rec	Copy C							
1441		K+V						

5. Click on Options, select multipart form, and click outside

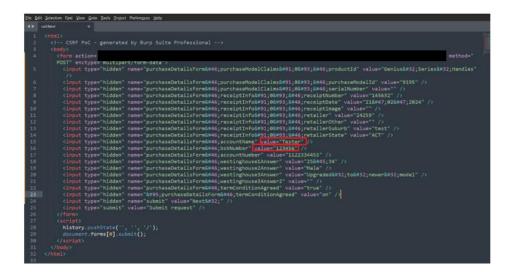


6. Click on Copy HTML to copy the HTML script



S CSRF PoC ge	herator			-	0	· ×
Request to:				0	inoite	0
Putty Raw	Has	🖸 w 🗉	Inspector 🔳 🗖	II	÷¢	×
1 9081 7563-7709-0	Details?0847_010110/ 17-011_007_104-7400-0040 HTTP/C		Request attributes		2	*
0A1.3.043300 / _ps_/02044	oli probinici, giardal 5 lostros Tiss-dol 5 l'Unders't 4 l'indertoit Bostilar5 0 (Winders II 10.0, Winde	08.1705820101	Request query parameter	a -	100	×
1 Accept: text/brail.ep	dre/20100181 Fireder/122.0 plicetion/shtal/sal.eplicetion/sal		Request body parameter	5	20	~
	ster, "Proposition of the second seco	C highlights	Request cookies			*
 Abadys Abadys Abagos Abagos Abagos Abagos Abagos Abagos Abagos 	<pre>type="hidden" max="purtheraPetal type="hidden" max="purtheraPetal type="hidden" max="purtheraPetal type="hidden" max="purtheraPetal type="hidden" max="purtheraPetal</pre>	eFormef46 operat nFormef46 operat aFormef46 operat aFormef46 operat aFormef46 operat	haneffirðel (Jakon Ffl) (Deff haneffirðel (Jakon Ffl) (Deff lýð Saðal Ffl) (Deff) lýð Saðal Ffl) (Deff) (A Ffl)	3-4843-5 3-4843-5 4-443-5 4-443-5 4-443-5 4-443-5 4-443-5 4-443-5 4-443-5 4-443-5 4-443-5 4-443-5 4-443-5 4-443-5 4-443-5 4-443-5 1-44-	nir than mit all mit all at a	alloi mita valv
		a Portas P42, por el a Portas P42, por el a Portas P42, reser- a Portas P42, reser-	have effected if a cancer of Fig. 10 of Fig. monthlink (C. Annue of Fig. 10 of Fig. 20 of the AFF in the Fig. 20 of Fig. 20 of the AFF in the Fig. 20 of Fig. 20 of the AFF in the Fig. 20 of Fig. 20 of the AFF in the Fig. 20 of Fig. 20 of the AFF in the Fig. 20 of Fig. 20 of the AFF in the Fig. 20 of Fig. 20 of Fig. 20 of of Fig. 2	Traffic and a second se	pip then entially whet's ange's state's bibuth's	effor valv Lus+ site valv valv valv valv
Name 1 1-0 CLS 2 -1-0 CLS 3 -10-0 CLS 4 -50-0 -0 5 -10-0 -0 6 -000 -0 7 -000 -0 8 -000 -0 10 -000 -0 11 -000 -0 12 -000 -0 13 -000 -0 14 -000 -0 15 -000 -0 16 -000 -0 17 -000 -0 18 -000 -0 19 -000 -0 10 -000 -0 11 -000 -0 12 -000 -0 12 -000 -0	1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.	eFormetH4 post afformetH4 post afforme	have effected if a man of FL, if of FL manuficies (I a man of FL, if of FL man of FL, if of FL, if of FL, if of FL man of FL, if of FL, if of FL, if of FL man of FL, if of FL, if of FL, if of FL man of FL, if of FL, if of FL, if of FL man of FL, if of FL, if of FL, if of FL man of FL, if of FL, if of FL, if of FL man of FL, if of FL, if of FL, if of FL man of FL, if of FL, if of FL, if of FL man of FL, if of FL, if of FL, if of FL man of FL, if of FL, if of FL, if of FL man of FL, if of FL, if of FL, if of FL man of FL, if of FL, if of FL, if of FL man of FL, if of FL, if of FL, if of FL, if of FL man of FL, if of FL, if of FL, if of FL, if of FL man of FL, if of FL man of FL, if	Traffeling Traffeling traffel	piztban weind weint weint weint weint weint weint ber beint	eSot make valv lus* stis stis valv valv valv valv
	1.000 Copyer-Talafan Samer "procharacteria typer-Talafan Samer "procharacteria	all yona 1940, para di all'oras 1940, para di all'oras 1940, para di all'oras 1940, para di all'ana 1940, para di all'ana 1940, para di all'ana 1940, para di all'ana 1940, anara all'ana 1940, anara	new Hord Li Anna et Li Angel Senti de Li Angel (Li Carlos H), and (Li Carlos H), and (Li	A constant of a constant of the constant of th	piz then en i ald ador " ador " ador " ador " bibari" bibari" bibari bibar bibar bibar bibar bibar bibar bibar bi	eSot make valv lus* stis stis valv valv valv valv

7. Paste the copied script into any notepad and save the with .html extension i.e. csrf.html



8. Open the csrf.html file in the browser and click on Submit request



9. You will see that all the fields are already filled with data



Retailer State/Region * ACT Payment Details Please enter your EFT details for the account you wertered payment details. Enter your Street enter of payment details. Enter your street enteryour	ACT	-	~
Payment Details			
			stem does not
Account Name * *	Tester		
BSB/Branch Number * '	123456		
Please ensure correct entry	of bank account details. 1	The Promoter is not liable for errors. Refer to terms	and conditions
Questionnaire			
Please answer the questions I	below:	* De	notes mandatory fields
What is your age?*		25-34	~
What is your Gender?*		Male	~
Why did you return your pr	oduct?*	Upgraded to newer model	v
I have read and accept	ted the promotion <u>Terms</u>	& Conditions.	
	Contact Us Te	rms & Conditions Privacy Policy	

Resolution of Vulnerability

Several measures can be implemented to mitigate the risk of CSRF attacks and enhance web application security:

1. Anti-CSRF Tokens:

- Include unique, unpredictable tokens in each form or request.
- These tokens are generated on the server side and embedded in web pages or included in requests.
- The server verifies the token's authenticity before processing the request, ensuring it originated from a legitimate source.

2. Same Site Cookie Attribute:

- Set the Same Site attribute for cookies to control when cookies are sent with cross-site requests.
- This attribute helps prevent the browser from sending cookies in requests initiated by third-party websites.

3. Origin Header Checking:

- Validate the origin header to ensure that requests are coming from the expected source.
- This helps verify that requests originate from the same domain and are not forged by malicious actors.

4. Referrer Header Checking:

- Check the referrer header to confirm that the request originated from the same site.
- While this method may have limitations (due to referrer header omission in some cases), it adds an extra layer of validation.



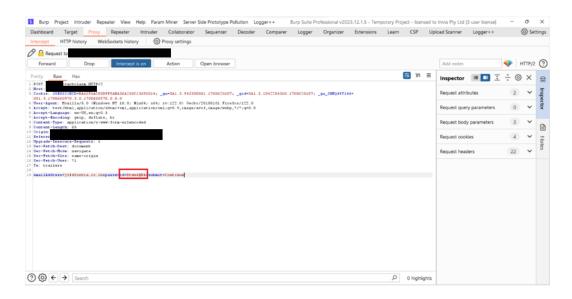
Parameter	Description
Severity	Medium
Impact	Medium
Risk Score	6.5
Affected URL	https://demoURL
Threat	 Eavesdropping: Attackers can intercept and eavesdrop on the communication channel, capturing plaintext passwords during the login process. Credential Theft: Intercepted plaintext passwords can be used for unauthorized access to user accounts.

In a scenario where passwords are transmitted in plaintext, user credentials are sent over the network without encryption or hashing. This means that if an attacker intercepts the communication between the user and the server, they can easily capture and read the plaintext passwords.

It has been observed that the password is transmitting in plain text.

Steps to Reproduce

- 1. Access the URL after logging in with your credentials https://demoURL
- 2. Enter your username and password and intercept the request in Burp Suite



Resolution of Vulnerability

Please follow the following steps to resolve the vulnerability



1. Implement Transport Layer Security (TLS/SSL):

- Enforce the use of HTTPS to encrypt the communication channel between the client (user's browser) and the server.
- Ensure that TLS/SSL certificates are valid and up to date.

2. HSTS (HTTP Strict Transport Security):

• Implement HSTS to instruct browsers to always use a secure, encrypted connection (HTTPS) when communicating with your website.

3. Secure Communication Channels:

- Avoid using unencrypted protocols (e.g., HTTP) for transmitting sensitive information, especially passwords.
- 4. Use Secure Authentication Protocols:
 - If applicable, use secure authentication protocols, such as OAuth or OpenID Connect, that facilitate secure transmission of authentication tokens.

5. Password Hashing and Storage:

• While not directly related to transmission, ensure that passwords are securely hashed and stored on the server to protect them in case of a data breach.

2.4 No Rate Limit

Parameter	Description
Severity	Medium
Impact	Medium
Risk Score	5.0
Affected URL	https://demoURL
Threat	 Brute Force Attacks: Without rate limiting, attackers can perform brute force attacks more efficiently, attempting to guess passwords for user accounts. Account Compromise: Successful brute force attacks can lead to unauthorized access to user accounts, posing risks to sensitive information and potentially allowing attackers to take control of the compromised accounts.

Rate limiting involves controlling the rate or frequency of incoming requests to a specific endpoint, such as a login page. Without rate limiting in place, an attacker could launch automated attacks by making a large number of login attempts in a short period, potentially compromising user accounts through password guessing.

It has been observed that the rate limit is not implemented on the login page.

Steps to Reproduce

- 1. Access the URL https://demoURL
- 2. Enter random email and password



5		× +					*	-	ه ک
	080			Ŷ	S 🖲 🔒	• 🗟	<u>.</u> 0		
Import bookmarks 📦	Getting Started 🐝 Invia eContracts 🖷	What is a Magic Byte 🧖 Android F	rida • A wo						
					Log In				
		To Track Your	Claim, Please Login						
		Please enter your em	ail and password	* Denotes mandatory fields					
		Email Address *	test@test.test						
		Password *							
			CONTINUE						
			FORGOT PASSW						
		c	Contact Us Terms & Condit	ions Drivacy Bolicy					

3. Click on CONTINUE and intercept the request in Burp Suite, right click on the request and click on Send to Intruder to send the request into intruder tool

Dashboard Target Proxy Repeater Intruder	Collaborator Conuencer	Decode	Comparer	Logger Organizer	Extensions	Learn	CSP	Upload Scanner	Logger++		@ Se	itting
Intercept HTTP history WebSockets history @ Pro	Scan	>										
Request to	Do passive scan											
Forward Drop Intercept is on	Do active scan	_						Add notes		-	HTTP/	. 0
Forward Drop Intercept is on	Send to Intruder	Ctrl+I								•	MITP/	- (
Pretty Raw Hex	Send to Repeater	Ctrl+R]\n ≣	Inspector	III 🖬 🗄	: ÷ @	×	-
POST trackclaim HTTP/2	Send to Sequencer											
Cookie: JSESSICNID=036043ESODDF601300DBA2F04D2B267D; _ga GA1.3.2146179309.1708794657	Send to Comparer		471144-GS1.3.1700	794657.6.1.170079469	1.0.0.0; _gid+			Request attr	ibutes	2	~	dsu
User-Agent: Hozilla/5.0 (Windows NT 10.0; Win64; x64; rv Accept: text/html,application/xhtml+xml,application/xml;	Send to Decoder							Request que	ry parameters	0	~	ctor
Accept-Language: en-US, en;q=0.5 Accept-Language: en-US, en;q=0.5	Send to Organizer	Ctrl+O						nedeest doe	ny parametera	0		- 1
Content-Type: application/x-www-form-urlencoded	Insert Collaborator payloa	d						Request boo	ly parameters	3	~	
Content-Length: 59 Origin:	Request in browser	>									~	6
Referer Upgrade-Insecure-Requests: 1	Extensions	>						Request coo	kies	4	~	NOT
Sec-Fetch-Dest: document Sec-Fetch-Mode: navigate	Engagement tools	>						Request hea	ders	22	~	
Sec-Fetch-Site: same-origin Sec-Fetch-User: 71	Change request method											
Te: trailers	Change body encoding											
emailAddress=test%40test.test4password=test4submit=Conti	Copy URL											
	Copy as curl command (ba	ish)										
	Copy to file											
	Paste from file											
-	Save item											
	Don't intercept requests	2										
	Do intercept	>										
	Convert selection											
	URL-encode as you type											
	Cut	Ctrl+X										
	Copy	Ctrl+C										
	Paste	Ctrl+V										

4. Go to Intruder tab, set payloads & dictionary, and click Start attack



Burp Project	ntruder Repeater View				ollution Log	gger++	Burp Suite Pr		3.12.1.5 - Tem			nsed to Invia Pty Ltd		- 0 ×
ashboard Targe	t Proxy Repeater	Intruder	Collaborator	Sequencer	Decoder	Comparer	Logger	Organizer	Extensions	Learn	CSP	Upload Scanner	Logger++	Setting
× 2 × 3	< +													Q
sitions Payloa	is Resource pool S	ttings												
) Payload sets													Г	Start attack
You can define o ways.	ine or more payload sets. Th	e number of pay	yload sets depen	ids on the attac	ck type define	d in the Positio	ons tab. Vario	us payload type	es are available	for each pa	yload set	, and each payload ty	ype can be customi	ized in different
Payload set:	~ ~	Payload coun	nt: 19											
Payload type:	imple list 🗸	Request coun	nt: 0											
Paste Load Remove Clear Deduplicate	root@invia.co.in admin@invia.co.in test@invia.co.in guest@invia.co.in info@invia.co.in adm@invia.co.in		·											
Add	mysol@invia.co.in Enter a new item													
Add from list			~											
	essing ules to perform various pro nabled Rule	essing tasks on	each payload be	fore it is used.										
Edit														

5. Here we can find the true account with unique length and status code

	Showing all items									
Request	Payload 1	Payload 2	Status code	Error	Timeout		Comment			
260	j1@invia.co.in		302			254				
14		root@invia.co.in	200			14038				
33		admin@invia.co.in	200			14038				
52		test@invia.co.in	200			14038				
71		guest@invia.co.in	200			14038				
90		info@invia.co.in	200			14038				
109		adm@invia.co.in	200			14038				
128		mysql@invia.co.in	200			14038				
147		user@invia.co.in	200			14038				
166		administrator@invia.co.in	200	U	U	14038				
Request	Response									:
Pretty	Raw Hex							6	۱n	=
rietty	Naw TIEX							<u> </u>		_

Resolution of Vulnerability

Please follow the following steps to resolve the vulnerability.

Implement rate limiting on the login page to mitigate the risks associated with brute force attacks. Here's how you can approach it:

- 1. Define Thresholds.
- 2. Implement Rate-Limiting Mechanism.



- 3. Incremental Backoff.
- 4. Temporary Lockouts.
- 5. Notify Users.

2.5 Token doesn't implement properly (Token Misconfigured)

Parameter	Description
Severity	Low
Impact	Low
Risk Score	3.1
Affected URL	https://demoURL
Threat	 Security Vulnerabilities: Misconfigured tokens can lead to security vulnerabilities, potentially allowing unauthorized access or exposing sensitive information. Authentication Failures: If tokens are not properly configured, users may face issues with authentication, leading to denial of service or unauthorized access.

A misconfigured or improperly implemented token can indicate issues with how authentication or authorization is handled in a system. Tokens, commonly used in authentication processes (such as JSON Web Tokens or OAuth tokens), are meant to securely convey information about the user or client's identity and permissions.

It has been observed that the token is not implemented properly.

Steps to Reproduce

1. Log in with your credentials and click on update claim.

© × +							
← → C O A ↔			Ŷ	۰ 📲			
🕲 Import bookmanks 🍓 Getting Started 🦠 Initia eConstracts. 🗰 What is a	Magic Tyle						
				Log Out			
				Log Out			
	Your Claim Details						-
	A DE TEL OF A D						
	Claim ID						
		lease mail us your goods					
	Gift CASHBAC	ж					
	Date Submitted						
	UPD	ATE CLAIM)				
	Claim ID						
	Claim Status CLAIM • P	fease mail us your goods					
	Gift CASHBAC	ж					
	Date Submitted						
	UPD	ATE CLAIM					
			-				
	Contact Us Jerms	& Conditions Privacy Policy					

- 2. Fill the blank input field
- 3. Click on NEXT button and intercept the request in Burp Suite



🖾 🗶 +											~		9 >
← → ♂ ○ ○ ○									32	6			
ngport bookmarks 📦 Getting Started 🐜 Invia eContracts	What is a Magic Dyte And Purchase Product * Purchase Model *	droid Frida • A wo											
	Payment Details Please enter your EFT details fo					curity, the syst	em does no	ŧ					
	retrieve previously entered pays Account Name **	ment details. Enter yo	your valid paymen	ent details to	update.								
	BSB/Branch Number * '	123456											
	Bank Account Number **	1122334455											
	Please ensure correct entry of	F bank account details	Is. The Promoter i	r is not liable	for errors. Re	fer to terms a	ind conditie	ins					
	I have read and accepted	d the promotion <u>Term</u>	ms & Conditions	<u>ns.</u>									
	Your data is being collected in a	accordance with the P	Privacy Policy. Fo	For more det	ails please cli	ck here.							
	\square		NEXT					\supset					
		Contact Un 1	Terms & Conditi	litions Dri	warry Dolicy								

4. Remove the OWASP_CSRFTOKEN token and send the request

Jashboard Target Prory Repeater Intruder Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn CSP Upload Scanner Logger++			
ntercept HTTP history WebSockets history ③ Pray settings			
Request to https://mbg.campaign.net.au/43 (52.62.70.38)			
Forward Drop Intercept Is on Action Open browser		Add notes	4
vetty Raw Hex	In ■	Inspector	
NAN		mipector [12] 12	
они и плани определять на правод правод Правод правод		Request attributes	
keept: text/btal,application/ibtal+ml,application/mlop=0.8,image/amif,image/amip,**>py=0.8			
Antroph + Language : env(3), en ; q+0 ; k		Request query parameters	
areget Receiving (mig. deflate, br mateur Type: withings (Tele. And. Beaching)			
Contest-length: 1009		Request body parameters	
Dept add+ Incenter + NeglestL4: 1		Request cookies	
Inter-Part (ch-Dans), documents			
Bar-Fer (wi-Houle) Bar/Spanne Bar-Fer (wi-K), Barrow Same		Request headers	
Rec-Fat, chollon 2 91		The part of the pa	
et trailers			
58405765912 19262102792493565804			
intent-Disposition: form-data; nume*"purchaseDetailsForm.purchaseDode(Claims(D), purchaseBode)[d*			
100			
6840167569279036210290493866804			
Context=Disposition: form=data; mame**purchaseDEtailsPorm.purchaseDEtails20; serialBomber*			
ARABITATION AND AND AND AND AND AND AND AND AND AN			
harred			
AND A CONTRACT AND A CONT			
121446			
Content-Pargonalian Form-data, man-formatilityen average Banders'			
12220944A6			
Content-Disposition: form-data: name="purchaseDetailsForm.termConditionAgreed"			
Nos			
2 F 4 21 5 7 5 6 7 1 7 1 1 2 1 2 1 7 7 1 4 7 3 5 4 5 5 6 5 6 1 4			
Sentent-Disposition: form-dutu: name="_purchaseDetailsForm.ternFormitionAprend"			
ombond-Dispersiblen: Been-dad as manner"submits"			
See			
25 420 576 59 17 19 10 21 02 39 4 536 4 500 4			
) (Ô ← → Search	O highlights		

5. We can see the next page and we can submit this form by removing the OWASP CSRFTOKEN from every request



× +							~		e ×
← → C O A @ Import bookmarks : Ø Getting Started % Invia eContrac	cts 🕶 What is a Magic Byte 🖇	🛱 Android Frida + A wo		û	•	12		0 45	ඞ≡
	Degister		2 Details	3 Theeks					
Γ	Address Details Step 2: Details		Containt.	TRAME.					
	Please enter your contact		C.U. R. 1000.	* Denotos mandatory fiel	4				
	Address Line 2	Address Line 2	e, Golden Beach QLD, Au	ustrana					
	Suburb / City *	sydney							
	State/Region *	ACT							
	Postcode *	0001							
	Country *	Australia		à]				
			NEXT)				
	(BACK)				
		Contact Us	erms & Conditions Pri	ivacy Policy					

Resolution of Vulnerability

Please follow the following steps to resolve the vulnerability.

- 1. **Review Token Generation Code**: Examine the code responsible for token generation. Ensure that it follows security best practices and generates tokens with accurate and necessary information.
- 2. **Secure Token Storage and Transmission**: Implement secure practices for storing and transmitting tokens. This includes encrypting tokens, using secure channels (HTTPS), and avoiding client-side storage of sensitive tokens.
- 3. **Token Validation**: Implement robust token validation mechanisms on the server-side to ensure that incoming tokens are properly formatted, signed, and contain valid information.
- 4. **Token Expiry and Revocation**: Set appropriate expiration times for tokens and consider implementing token revocation mechanisms to invalidate tokens when needed.
- 5. **Use Established Standards**: If implementing authentication and authorization, consider using established standards such as OAuth 2.0 or OpenID Connect. This helps ensure interoperability and adherence to best practices

2.6 Outdated jQuery and Bootstrap

Parameter	Description
Severity	Low
Impact	Low
Risk Score	3.1
Affected URL	https://demoURL
Threat	 Security Vulnerabilities: Outdated frameworks may contain known security vulnerabilities that could be exploited by attackers, leading to potential data breaches or system compromises. Compatibility Issues: Compatibility with modern browsers, devices, and web standards may be



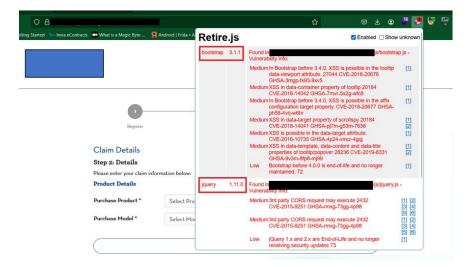
compromised, affecting the functionality and user experience of your application.

Using outdated frameworks refers to employing versions of development frameworks, libraries, or tools that are no longer actively maintained or are significantly behind in updates. These may lack the latest features, optimizations, and crucial security patches.

It has been observed that the application uses multiple outdated components i.e. jQuery & bootstrap.

Steps to Reproduce

1. Check the jQuery and bootstrap



Resolution of Vulnerability

Please follow the following steps to resolve the vulnerability.

- 1. **Regular Framework Updates**: Keep frameworks up to date by applying the latest patches, updates, and security releases. Regularly check for new framework versions and migrate to the latest stable release.
- 2. **Patch Management**: Implement a robust patch management process to promptly apply security patches and updates as soon as they are released. This helps address known vulnerabilities and secure the applications.

2.7 Clickjacking

Parameter	Description
Severity	Low
Impact	Low
Risk Score	4.0
Affected URL	https://demoURL
Threat	1. Unauthorized Actions: Clickjacking can lead users to
	unknowingly perform actions they didn't intend to, such as



2.	liking a post, following someone, or making a purchase. Phishing Attacks: Attackers can use clickjacking to create convincing phishing scenarios, where users might think they are interacting with a legitimate website or application.
3.	Malicious Downloads : Clickjacking can be employed to trick users into unknowingly initiating the download of malware or malicious files.
4.	Credential Theft: In some cases, clickjacking may be combined with other attacks to trick users into entering sensitive information, leading to credential theft.

Clickjacking, also known as a UI (User Interface) redress attack or UI confusion attack, is a malicious technique where an attacker tricks a user into clicking on something different from what the user perceives. This is often achieved by overlaying or embedding transparent elements on a webpage to deceive users into interacting with unintended buttons, links, or content. The term "clickjacking" is a portmanteau of "click" and "hijacking."

It has been observed that the X-Frame-Options header is missing in the application.

Steps to Reproduce

1. Create an IFrame HTML Page containing the target URL and save it as a .html file



2. Open .HTML file in any browser



✓ ③ dick.html × +			
← → C O File C:/Users/	Desktop/click.html		🛧 🛲 🌢 🚓 🍗 🕯
🔀 Android Application 📦 Simple Applicant Tr	F Free Illustrator Onli 🔨 Login 🛛	SSS Hunter	nce X 🔮 offsec.tools - A vast 📀 CTF365 - Capture T
Click Jacking			
			Log In
	1 Register	2 Details	
	Customer Details		
	Step 1: Register		
	Please enter your registration	details. You will be sent an email so you can procee	
	First Name *	First Name	* Denotes mandatory fields
	Last Name *	Last Name	
	Contact Number *	Contact Number	
	Email Address *	Email Address	

Resolution of Vulnerability

Please follow the following steps to resolve the vulnerability.

- 1. X-Frame-Options Header: Set the X-Frame-Options header in HTTP responses to instruct browsers on whether to allow a page to be rendered in a frame.
- 2. Options include DENY (to deny framing altogether) or SAMEORIGIN (to allow framing only by pages on the same origin). "X-Frame-Options: DENY"

2.8 Server Information Disclosed

Parameter	Description
Severity	Low
Impact	Low
Risk Score	3.1
Affected URL	https://demoURL
Threat	 Increased Attack Surface: The disclosed information may provide attackers with insights into the server's software stack, making it easier for them to target specific vulnerabilities associated with known versions. Targeted Attacks: Armed with detailed server information, attackers can launch more targeted and sophisticated attacks, increasing the risk of successful exploitation. Security Misconfigurations: The disclosed details may reveal security misconfigurations, unintentionally aiding attackers in finding weaknesses that could be exploited for unauthorized access or other malicious activities.

When a server inadvertently discloses information about its configuration, software versions, or other sensitive details in its responses, it can be a security concern. This disclosure can occur



through banners, headers, or error messages returned by the server. Attackers often leverage such information to identify potential vulnerabilities and weaknesses in the server's setup.

It has been observed that the application discloses Server Information through the request's response.

Steps to Reproduce

1. Server Disclosed

Send Cancel < Y > Y		0		
quest		Response III III	Inspector	Ξ
etty Raw Hex 🗒	vn ≡	Pretty Raw Hex Render	E Request attributes	
47 - 2777/2 - 7 - 27.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.		1.000002 400 Aud Bageren (1.00002 400 Aud Bageren 1.0000 400 400 400 400 400 400 400 400 40	Request query parameter	ers
<pre>ker-Agent: Mozilla/6.0 (Windows Wf 10.0; Win64; x64; xv:122.0) decko/20101101 Pirefox/122.0 crept: text/Mtml.application/shtml4rml.application/mljq=0.4, image/arif,image/webp.*/*jq=0.4</pre>		6 Conteat-Length: 102 6	Request body parameter	55
competitionary and a second seco		9 etcals theads etcals 400 Rat lequest	Request cookies	
eo-Fetich-Hode: marigate eo-Fetich-Site: mase		<t< td=""><td>Request headers</td><td></td></t<>	Request headers	
er Fischeller († 19. 19. staalier		 stocky stocky	Response headers	

Resolution of Vulnerability

Please follow the following steps to resolve the vulnerability.

1. **Remove or Customize Banners and Headers:** Consider configuring the server to either remove or customize banners, headers, and error messages to minimize the amount of information disclosed. This can be achieved through server settings or configurations.

2.9 HTTP Strict Transport Security (HSTS) Header is Missing

Parameter	Description
Severity	Low
Impact	Low
Risk Score	3.0
Affected URL	https://demoURL
Threat	The lack of HSTS increases the risk of man-in-the-middle attacks, where an attacker could potentially intercept and manipulate communication between the user's browser and the web server. This vulnerability could lead to the compromise of sensitive information, such as login credentials or session tokens, particularly during the initial connection setup.

The absence of the HTTP Strict Transport Security (HSTS) header means that the web server is not instructing the browser to enforce a secure, encrypted connection (HTTPS) when communicating

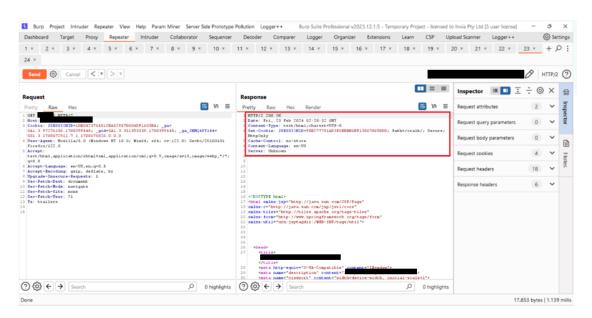


with the website. Without HSTS, there is a potential for attackers to intercept the initial insecure connection and perform attacks like SSL/TLS protocol downgrades or session hijacking.

It has been observed that the HSTS header is not present in the application.

Steps to Reproduce

1. HSTS Header not Present



Resolution of Vulnerability

Please follow the following steps to resolve the vulnerability.

 To mitigate this security risk, website administrators should configure their web servers to include the HTTP Strict Transport Security (HSTS) header in their responses. This header informs the browser to only connect to the website over HTTPS and to block any attempts to establish an insecure connection. An example of an HSTS header is as follows: "Strict-Transport-Security: max-age=31536000; include Subdomains; preload"

2.10 CSP Not Implemented

Parameter	Description
Severity	Low
Impact	Low
Risk Score	3.1
Affected URL	https://demoURL
Threat	The absence of CSP increases the risk of several security threats, including XSS attacks. Without CSP, attackers can inject malicious scripts into web pages, potentially leading to the theft of sensitive user information, session hijacking, defacement of the site, or other malicious activities. Additionally, the lack of CSP makes it more challenging to enforce best practices for resource loading and limits the ability to mitigate the impact of security



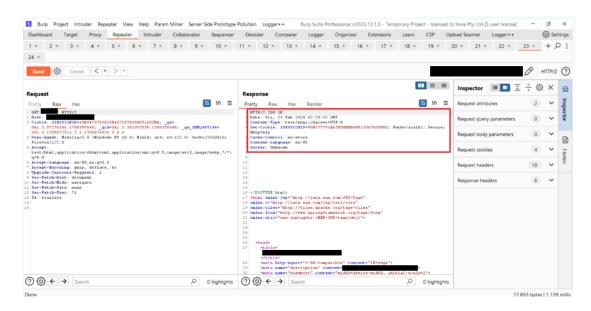
incidents.

When Content Security Policy (CSP) is not implemented, the web application lacks a mechanism to control and restrict the sources from which it can load resources, such as scripts, stylesheets, or images. This absence of CSP opens the site to vulnerabilities, as it becomes more susceptible to malicious scripts or content injected by attackers.

It has been observed that the CSP header is not present in the application.

Steps to Reproduce

1. CSP Header not found



Resolution of Vulnerability

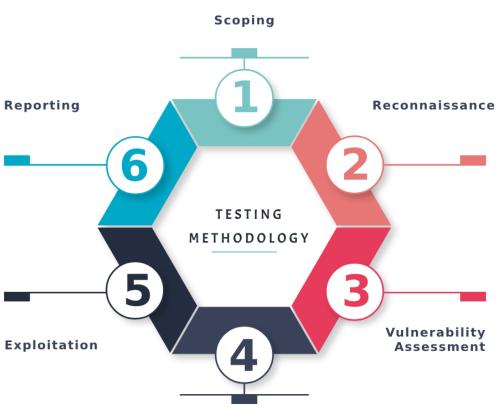
Please follow the following steps to resolve the vulnerability.

 To address the absence of CSP and enhance the security posture of a web application, developers should implement and configure a Content Security Policy. This involves defining and specifying the allowed sources for various types of content, such as scripts, styles, and images.

Testing Methodology

The testing methodology followed during the Web Vulnerability Assessment and Penetration Testing (VAPT) adheres to industry best practices and consists of several key phases. This section provides an overview of the testing methodology employed during the assessment, applicable to various organizations and scenarios.





Manual Testing

Scoping:

- The scoping phase involves defining the scope and objectives of the assessment in collaboration with the client.
- This includes identifying the target web applications, systems, and infrastructure to be tested, as well as specifying any limitations or exclusions.

Reconnaissance:

- The reconnaissance phase focuses on gathering information about the target organization, its systems, and potential vulnerabilities.
- It includes passive and active reconnaissance techniques to identify publicly available information, network infrastructure, and potential entry points.

Vulnerability Assessment:

- The vulnerability assessment phase involves scanning and assessing the target web applications for known vulnerabilities.
- Automated vulnerability scanning tools are utilized to identify common security weaknesses, such as injection flaws, cross-site scripting (XSS), and misconfigurations.

Manual Testing:



- Manual testing is conducted to complement the automated vulnerability assessment and identify vulnerabilities that may not be detected by scanning tools.
- This phase involves a thorough analysis of the target web applications, including input validation, authentication mechanisms, access controls, and session management.

Exploitation:

- The exploitation phase focuses on actively attempting to exploit identified vulnerabilities to determine their potential impact and validate their existence.
- It involves simulating real-world attack scenarios while minimizing any potential impact on the target systems.

Reporting:

- The reporting phase involves documenting the findings, including identified vulnerabilities, their severity, and recommendations for remediation.
- The report provides a clear and concise overview of the assessment results, supporting evidence, and actionable steps for improving the security posture.

Common Vulnerabilities

During manual testing of web applications, various vulnerabilities are commonly tested to identify potential security weaknesses. Here are some vulnerabilities that are typically assessed during web application manual testing:

Input Validation Issues:

- Testing for SQL Injection vulnerabilities by attempting to inject malicious SQL queries.
- Cross-site scripting (XSS) testing by injecting script tags or other HTML/JavaScript payloads.
- Command Injection testing by injecting commands or special characters in user inputs.

Authentication and Session Management:

- Testing for weak or default credentials to identify weak authentication mechanisms.
- Session management testing, including session fixation, session timeout, and session hijacking.

Access Control Issues:

- Testing for access control vulnerabilities such as privilege escalation or unauthorized access to restricted areas.
- Testing for Insecure Direct Object References (IDOR) by manipulating object references or parameters.

Cross-Site Request Forgery (CSRF):

• Testing whether the application is vulnerable to CSRF attacks by crafting malicious requests.



Information Disclosure:

- Testing for sensitive information disclosure, such as error messages revealing system details or stack traces.
- Directory traversal testing to identify if unauthorized file access is possible.

File Upload Vulnerabilities:

• Testing for potential file upload vulnerabilities, such as bypassing file type restrictions or executing malicious files.

Security Misconfigurations:

• Testing for misconfigured security settings, such as default configurations, unnecessary services or ports, or weak encryption algorithms.

Business Logic Flaws:

• Testing for logical vulnerabilities that may allow unauthorized actions or circumvention of intended processes.

Cross-Site Script Inclusion (XSSI):

• Testing for vulnerabilities that may allow the inclusion of external scripts or content from untrusted sources.

API Testing:

• Testing the security of application programming interfaces (APIs) for vulnerabilities like improper access controls or insecure API endpoints.

Error Handling and Input Validation:

• Testing for proper error handling, ensuring that error messages do not disclose sensitive information and inputs are properly validated.

Session Management:

• Testing for session management vulnerabilities, including session fixation, session hijacking, or insufficient session logout mechanisms.

These are just some examples of vulnerabilities typically tested during manual web application testing. The specific vulnerabilities to test depend on the application's functionality, technology stack, and potential attack surface.

Risk Assessment

During the Vulnerability Assessment and Penetration Testing (VAPT), the identified vulnerabilities and findings are categorized into the following risk levels:



Critical:

Critical vulnerabilities pose an immediate and significant threat to the security of web applications and systems. The exploitation of these vulnerabilities can lead to severe consequences, including complete system compromise, unauthorized access to sensitive data, and significant financial or reputational damage.

High-Risk:

High-risk vulnerabilities also represent a significant threat to the security of web applications and systems. The exploitation of these vulnerabilities may result in unauthorized access, data breaches, and potential financial or reputational damage.

Medium-Risk:

Medium-risk vulnerabilities indicate potential security weaknesses that could be exploited by attackers. While the impact may not be as severe as critical or high-risk vulnerabilities, successful exploitation could result in unauthorized access, data leakage, or compromise of sensitive information.

Low-Risk:

Low-risk vulnerabilities represent potential security gaps that may have a limited impact on the overall security posture of web applications. The exploitation of these vulnerabilities is less likely to result in significant harm or compromise.

Informational:

Informational findings provide observations, best practice recommendations, or additional information that may not pose an immediate security risk but offer valuable insights for improving security practices, enhancing system resilience, or adhering to industry standards.

Terms and Conditions

Confidentiality and non-disclosure:

The Provider agrees to treat all information obtained during the engagement as confidential. The Provider will not disclose any findings or sensitive information to unauthorized parties without explicit written consent from the Client. The Client acknowledges that the Provider may share anonymized and aggregated data for statistical or research purposes, provided that it does not disclose sensitive information.

Legal Compliance:

The penetration testing activities will be conducted in compliance with applicable laws, regulations, and ethical standards. The Client agrees to provide accurate and lawful information, ensuring that the testing does not violate any legal or regulatory requirements.

Liability:



Both the Client and the Provider acknowledge that the nature of penetration testing carries inherent risks. The Provider will exercise reasonable care and expertise during the engagement. However, the Provider shall not be held liable for any damages, losses, or claims arising from the penetration testing activities. The Client understands and accepts the risks associated with the engagement.

Ownership of Findings:

The Client retains ownership of all proprietary information and data. The Provider acknowledges that any vulnerabilities discovered during the engagement belong to the Client. The Provider may request permission to include anonymized and sanitized findings in future research or case studies, with the Client's approval.

Remediation and Follow-up:

Upon receiving the penetration testing report, the Client is responsible for promptly addressing and remediating the identified vulnerabilities. The Provider may offer additional support or consulting services to assist with the remediation process if agreed upon separately.