Sri Lanka Institute of Information Technology

Web Security – IE 2062

Bug Bounty Report

IT22123404 - WIJESINGHE R P D K N

Table of Contents

Acknowledgment 3
Purpose of the report 3
What is Bug Bounty 3
Reconnaissance 4
Subfinder 5
Sublist3r 6
Vulnerability Assessment 7
Burp Suite 8
Zap 9
Nikto 11
What are available Bug bounty platforms? 11
Reports 12
Vendasta (Report 1) 12
Wise (Report 2) 20
Alshaya (Report 3) 28
Opera (Report 4) 34
FloQast (Report 5) 42
Koelsa group (Report 6) 46
Soundcloud (Report 7) 52
Picsart (Report 8) 57
Trello (Report 9) 63
Rockstar Games (Report 10) 69

Acknowledgment

I'd like to thank Ms.Chethana Liyanapathirana, the Lecturer in charge of the web security module, and our lab instructors Ms. Thriyashi Silva and Ms. Helani Herath for their invaluable advice, assistance, and experience throughout the development of this Bug Bounty report. Their assistance has been genuinely essential.Their commitment to my education and development has been clear at every step of the process.They have patiently answered my questions, provided great insights, and presented real-world examples, all of which have improved my understanding of web security. Their dedication to my accomplishment has motivated me to achieve perfection in my sector.

Purpose of the report

As the final project of the Web Security (IE-2062) The main objective of the Bug Bounty report is to effectively identify and report security vulnerabilities found within the target system or application. This entails providing a detailed and comprehensive account of each discovered vulnerability, ensuring that all relevant information is accurately documented. By fulfilling these objectives, the Bug Bounty report aims to facilitate prompt remediation of the identified vulnerabilities and enhance the overall security posture of the system or application.

What is Bug Bounty

Bug bounty programs are initiatives offered by companies or organizations to incentivize cybersecurity researchers, also known as ethical hackers, to discover and report security vulnerabilities in their software, websites, or systems. These programs typically provide monetary rewards, recognition, or other incentives to individuals who responsibly disclose identified vulnerabilities, thereby helping to improve the overall security posture of the organization. Bug bounty programs not only foster collaboration between security experts and organizations but also help prevent malicious exploitation of vulnerabilities by allowing them to be addressed before they can be exploited by cybercriminals.

What are the Phases of Bug Bounty?

There are mainly 2 phases of bug bounty.

1.Reconnaissance
2. Vulnerability Assessment

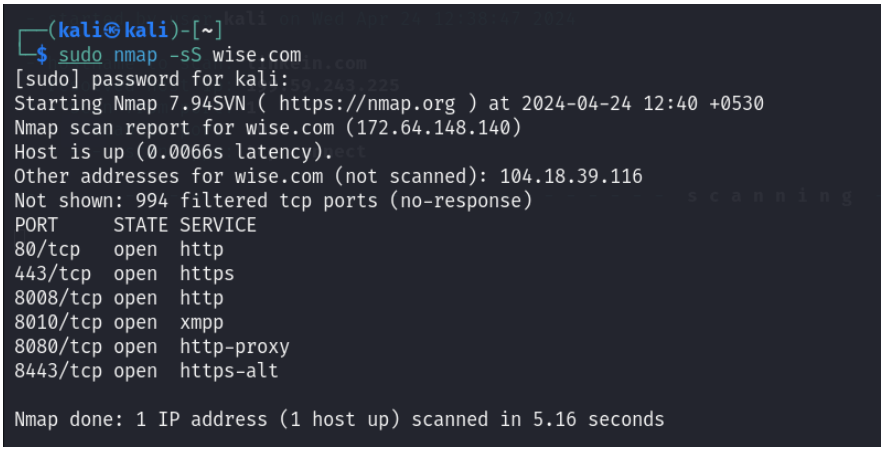
Reconnaissance

Reconnaissance, often referred to as "recon" for short, is the initial phase of a cybersecurity assessment or attack where information is gathered about a target system, network, or organization. It involves passive and active techniques to gather data, such as publicly available information, network scanning, and probing for potential vulnerabilities. Reconnaissance aims to gain insights into the target's infrastructure, assets, security measures, and potential points of entry. This information is crucial for developing a comprehensive understanding of the target and identifying potential attack vectors for further exploitation or testing.

Reconnaissance tools i used

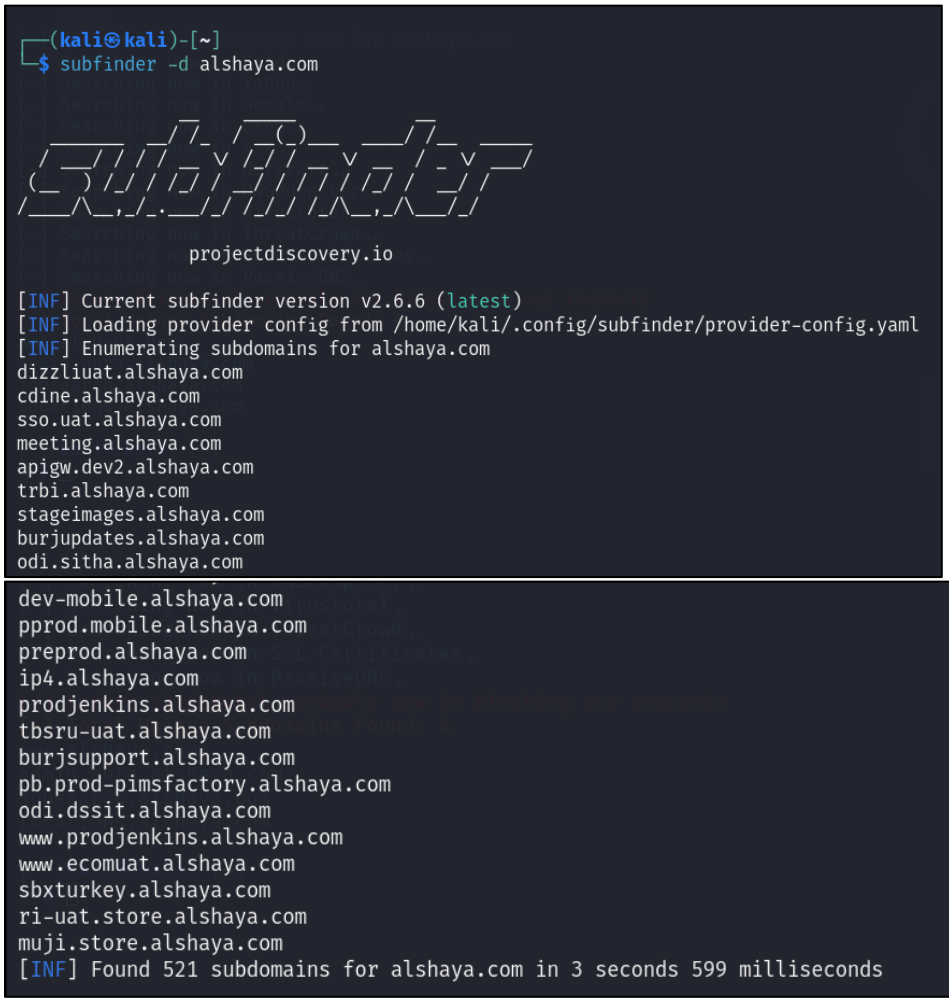
Nmap

Nmap, a staple tool in Kali Linux, is like a digital detective for network exploration and security auditing. It's used by cybersecurity experts to map out networks, discovering devices, services, and open ports. Just like detectives gather clues, Nmap collects information about the network's topology and the software running on it. This helps identify potential entry points for attackers and strengthens defenses by highlighting areas that need attention. With its versatility and precision, Nmap is an indispensable asset in any cybersecurity toolkit.



Subfinder

Subfinder, a potent reconnaissance tool often found in Kali Linux, is akin to a digital scout scouring the internet for subdomains associated with a target domain. Much like exploring the outskirts of a city to uncover hidden paths, Subfinder delves into the vast expanse of the web, discovering subdomains that may have been overlooked. By uncovering these subdomains, which are like hidden entrances to a fortress, Subfinder aids cybersecurity professionals in understanding the full scope of a target's online presence, enabling thorough security assessments and proactive defense measures.



Sublist3r

Sublist3r is an open-source tool used for subdomain enumeration. It helps security researchers, penetration testers, and bug bounty hunters to discover subdomains associated with a target domain. Sublist3r leverages various techniques such as search engines, DNS data, and brute force to enumerate subdomains. By gathering information about these subdomains, security professionals can identify potential entry points or security risks within an organization's infrastructure. Sublist3r is commonly used as part of reconnaissance activities to gather preliminary information about a target's online presence.

2. Vulnerability Assessment

Vulnerability Assessment refers to the process of identifying, quantifying, and prioritizing security vulnerabilities within a system, network, application, or organization. It involves systematic examination of potential weaknesses that could be exploited by attackers to compromise the confidentiality, integrity, or availability of the assets.

The vulnerability assessment process typically includes:

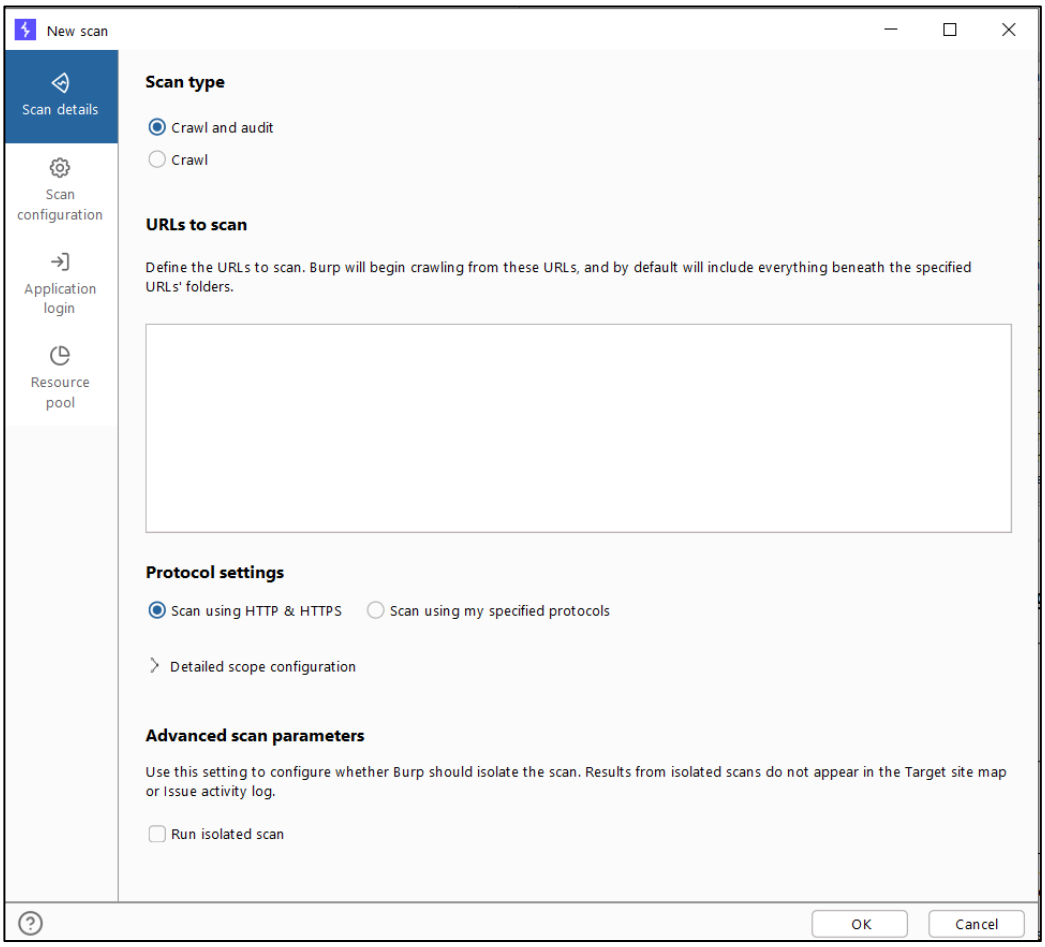
1. **Identification**: This involves discovering and documenting potential vulnerabilities within the target system or environment. This can be achieved through various means such as automated scanning tools, manual inspection, or analysis of system configurations.
2. **Evaluation**: Once vulnerabilities are identified, they are assessed in terms of their severity, potential impact, and likelihood of exploitation. This evaluation helps prioritize which vulnerabilities should be addressed first based on risk assessment.
3. **Remediation**: After vulnerabilities are assessed, appropriate measures are taken to mitigate or remediate them. This may involve applying patches, configuration changes, or implementing additional security controls to reduce the risk of exploitation.
4. **Verification**: Once remediation actions are taken, it's important to verify that the vulnerabilities have been effectively addressed. This often involves retesting the system or environment to ensure that the vulnerabilities have been properly mitigated.

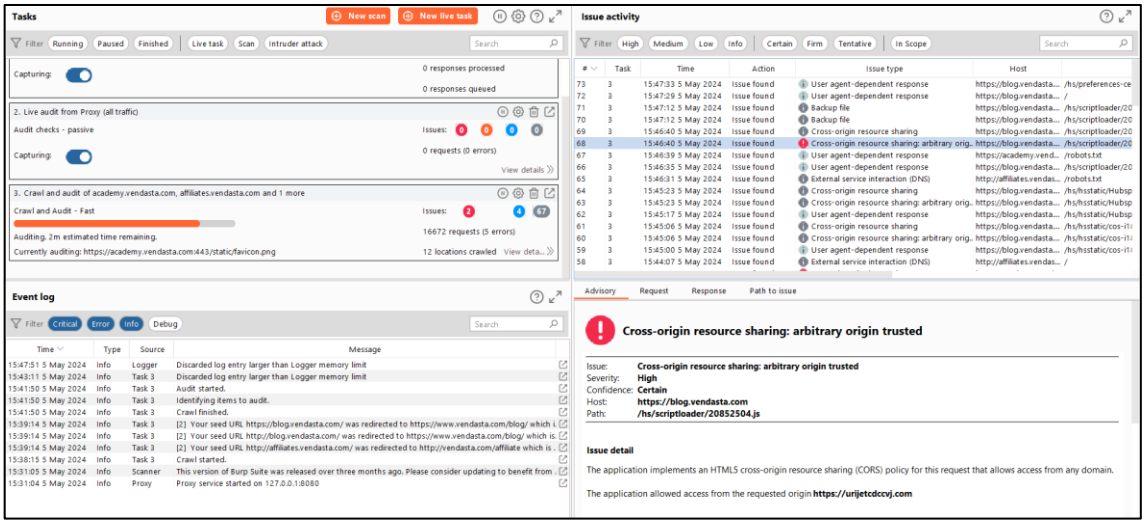
Vulnerability assessments are an essential component of an organization's overall cybersecurity strategy, helping to proactively identify and address potential security risks before they can be exploited by attackers. They are often conducted on a regular basis as part of a comprehensive security program to ensure ongoing protection against emerging threats.

Tools used

Burp Suite

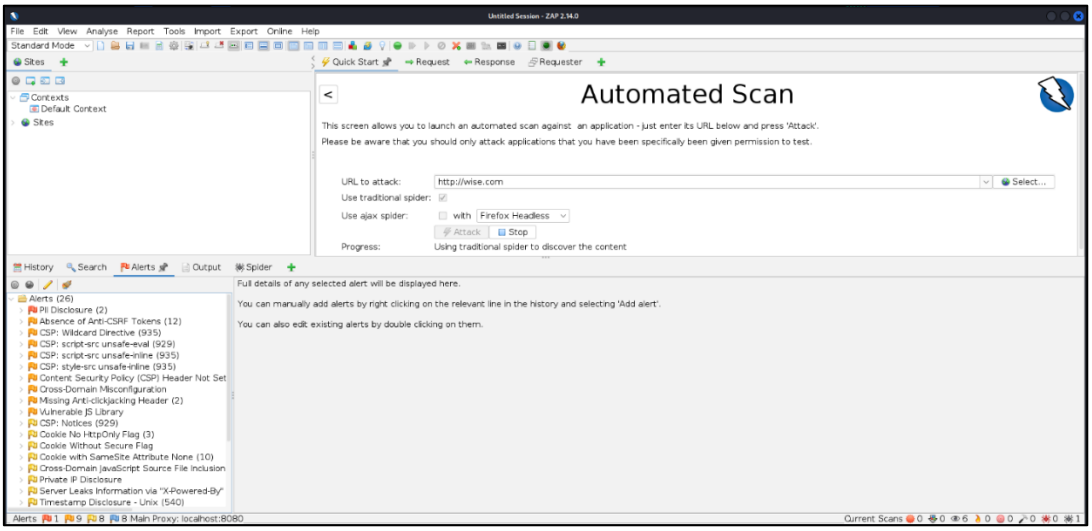
Burp Suite, developed by PortSwigger, is a versatile toolkit for web application security testing. Its comprehensive set of tools includes a Proxy, Scanner, Spider, Intruder, Repeater, Sequencer, and Decoder. These tools allow cybersecurity professionals, penetration testers, and developers to intercept, analyze, and remediate vulnerabilities in web applications. With features such as automated vulnerability detection, manual request modification, and session token analysis, Burp Suite is an indispensable asset for ensuring the security of web applications.

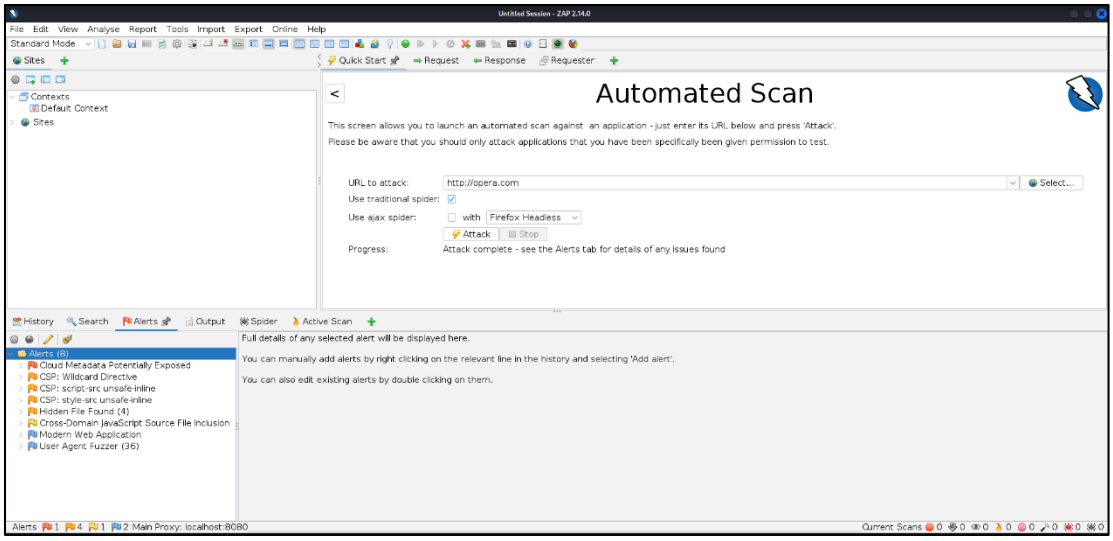


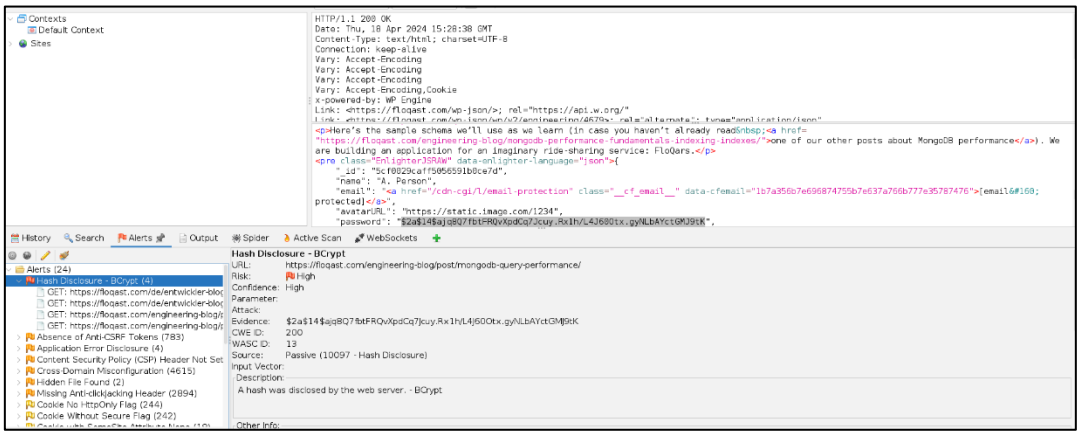


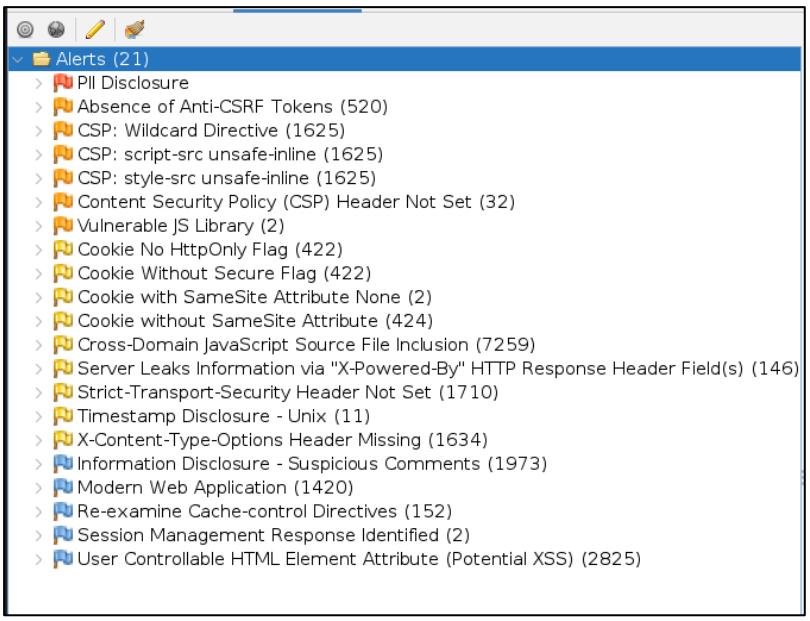
Zap

OWASP ZAP, found in Kali Linux, is a robust security tool trusted by professionals to assess web applications for potential vulnerabilities. similar to Nikto, ZAP scrutinizes websites but goes deeper, examining for a broader range of security flaws like injection attacks, cross-site scripting, and broken authentication. Through its comprehensive scans and intuitive interface, ZAP empowers users to identify and address security weaknesses, fortifying web applications against potential cyber threats.



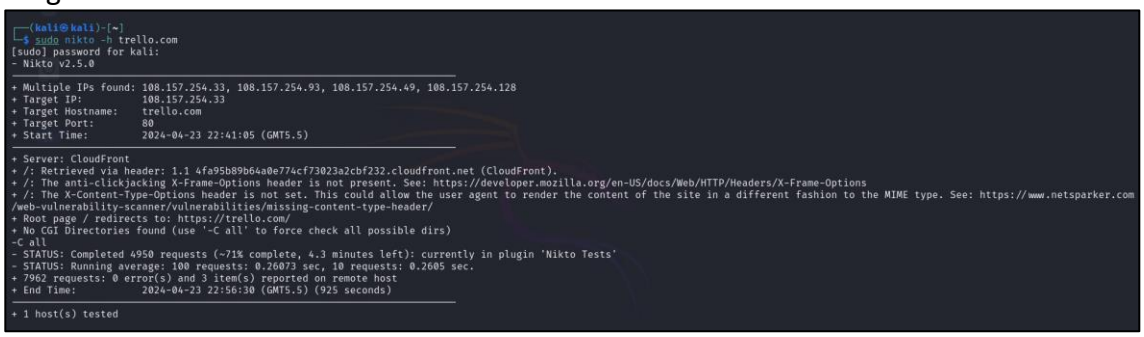

Automated Scan
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack:
http://opera.com
Use traditional spider:
Use ajax spider:
with
Firefox Headless
Attack
Stop
Progress:
Attack complete - see the Alerts tab for details of any issues found




Alerts (21)
PII Disclosure
Absence of Anti-CSRF Tokens (520)
CSP: Wildcard Directive (1625)
CSP: script-src unsafe-inline (1625)
CSP: style-src unsafe-inline (1625)
Content Security Policy (CSP) Header Not Set (32)
Vulnerable JS Library (2)
Cookie No HttpOnly Flag (422)
Cookie Without Secure Flag (422)
Cookie with SameSite Attribute None (2)
Cookie without SameSite Attribute (424)
Cross-Domain JavaScript Source File Inclusion (7259)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (146)
Strict-Transport-Security Header Not Set (1710)
Timestamp Disclosure - Unix (11)
X-Content-Type-Options Header Missing (1634)
Information Disclosure - Suspicious Comments (1973)
Modern Web Application (1420)
Re-examine Cache-control Directives (152)
Session Management Response Identified (2)
User Controllable HTML Element Attribute (Potential XSS) (2825)

Nikto

Nikto is a specialized tool within Kali Linux used by cybersecurity professionals to scan websites for potential vulnerabilities. It searches for common issues like outdated software versions and misconfigurations that could be exploited by attackers. Nikto generates detailed reports that help website owners and administrators understand and address any security risks identified during the scan.



What are available Bug bounty platforms?

1.Hackerone

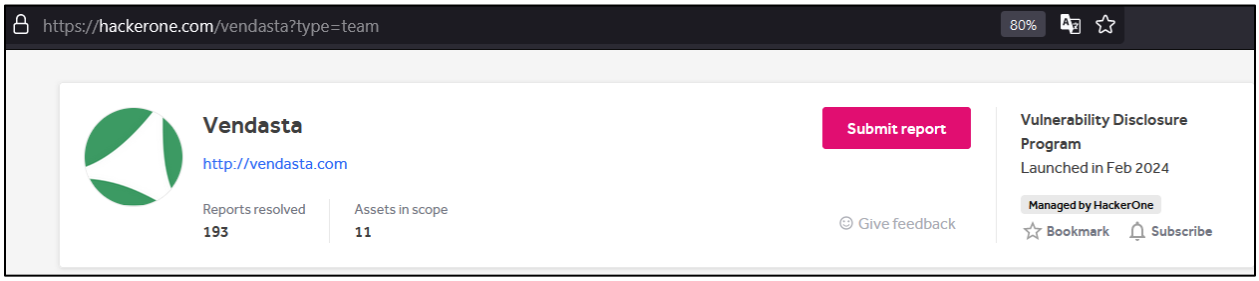
HackerOne is a company specializing in cybersecurity, specifically attack resistance management, which blends the security expertise of ethical hackers with asset discovery, continuous assessment, and process enhancement to find and close gaps in the digital attack surface.

2.Bug crowd

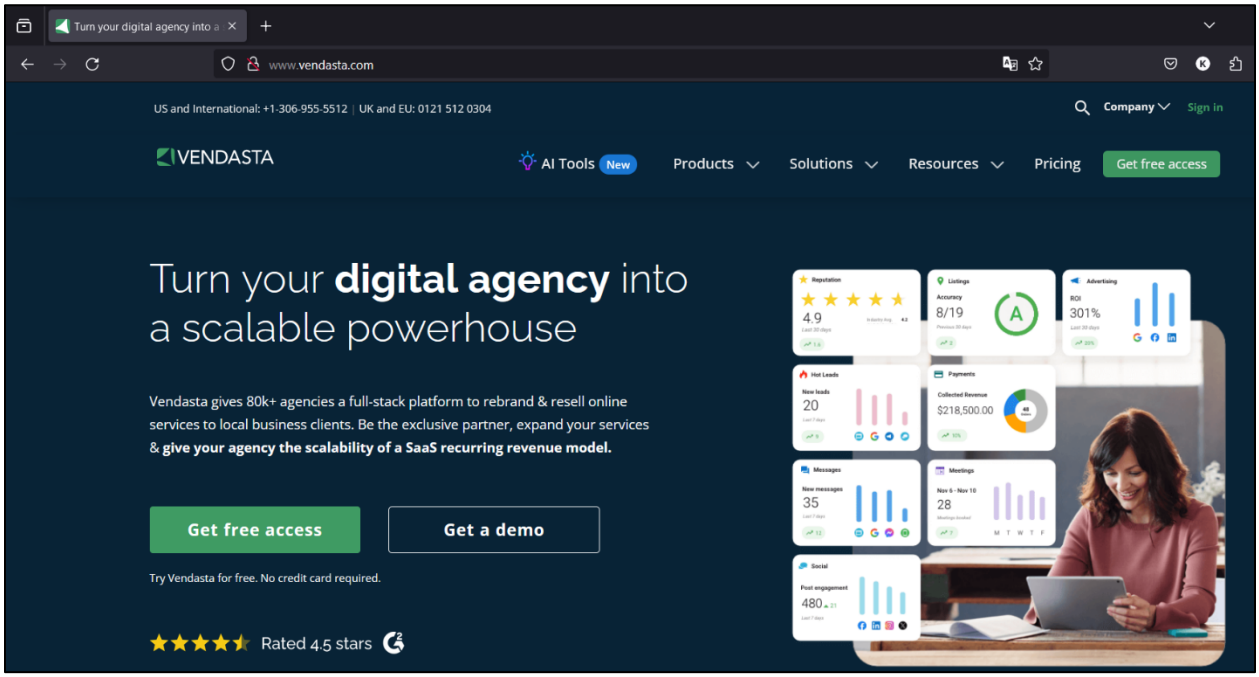
Bugcrowd is a crowdsourced cybersecurity platform that connects organizations with a global community of ethical hackers, often referred to as security researchers or white-hat hackers. These hackers participate in bug bounty programs, where they are incentivized to find and report security vulnerabilities in the organization's software, websites, or applications.
Bugcrowd provides a platform for organizations to run these bug bounty programs, facilitating communication, bug submission, validation, and reward distribution.
Throughout this report,Bug bounty programs that were listed in these two platforms were scanned.

Reports

1.Vendasta (Report 1)



Addressing the target



Vendasta is an end-to-end platform for local experts who market, sell,bill, fulfill, and deliver digital solutions to small and medium businesses.

Scope

In Scope

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
customervoice.biz To access this domain, activate the free-tier version of "Customer Voice" for a test account. For more information on activating products, visit: https://support.vendasta.com/hc/en-us/articles/4406958134807-Activate-Products	Domain	In scope	Critical	Ineligible	Feb 14, 2024	4 (2%)
your-domain.socialsmbs.com To access this domain, activate the free-tier version of "Social Marketing" for a test account. For more information on activating products, visit: https://support.vendasta.com/hc/en-us/articles/4406958134807-Activate-Products	Domain	In scope	Critical	Ineligible	Feb 14, 2024	1 (1%)
your-domain.steprep.com To access this domain, activate the free-tier version of "Reputation Manager" for a test account. For more information on activating products, visit: https://support.vendasta.com/hc/en-us/articles/4406958134807-Activate-Products	Domain	In scope	Critical	Ineligible	Feb 14, 2024	0 (0%)
your-domain.pdqs.mobi To access this domain, activate the free-tier version of "Listing Builder" for a test account. For more information on activating products, visit: https://support.vendasta.com/hc/en-us/articles/4406958134807-Activate-Products	Domain	In scope	Critical	Ineligible	Feb 14, 2024	0 (0%)
your-domain.snapshotreport.biz For activating and testing the Snapshot Report, see our support docs: https://support.vendasta.com/hc/en-us/articles/4406959860887-Create-Snapshot-Reports	Domain	In scope	Critical	Ineligible	Feb 14, 2024	3 (2%)
task-manager.biz	Domain	In scope	Critical	Ineligible	Jan 3, 2022	0 (0%)
your-domain.smblogin.com To access this domain, create a test account in the Business > Accounts page within Partner Center. Select this test account and choose "Business App" from the "Open In" menu. See this support doc for more info: https://support.vendasta.com/hc/en-us/articles/4406958960023-Accessing-Business-App-as-a-Partner-Center-admin	Domain	In scope	Critical	Ineligible	Feb 14, 2024	4 (2%)
***.vendasta-internal.com**	Wildcard	In scope	Critical	Ineligible	May 15, 2023	10 (5%)
***.yesware.com** Sign up to the platform via https://www.yesware.com/sign-up using a Google or Microsoft account. Please note, Wordpress (www.yesware.com) and Zendesk (help.yesware.com) assets are out of scope.	Wildcard	In scope	Critical	Ineligible	May 15, 2023	15 (8%)
***.apigateway.co**	Wildcard	In scope	Critical	Ineligible	May 15, 2023	60 (31%)
partners.vendasta.com Sign up for access to our platform using: https://signup.vendasta.com/?variant=hackerone	Domain	In scope	Critical	Ineligible	Feb 14, 2024	19 (10%)

Out of Scope

Spamming of forms and APIs with automated vulnerability scanners are strictly out of scope	Other	Out of scope	None	Ineligible	Apr 6, 2020	0 (0%)
www.yesware.com	Domain	Out of scope	None	Ineligible	Feb 14, 2023	0 (0%)
help.yesware.com	Domain	Out of scope	None	Ineligible	Feb 14, 2023	0 (0%)
roadmap.vendasta.com Uses a third-party content management system so it is ineligible for VDP.	Domain	Out of scope	None	Ineligible	Mar 1, 2023	0 (0%)
www.vendasta.com	Domain	Out of scope	None	Ineligible	Feb 8, 2024	0 (0%)

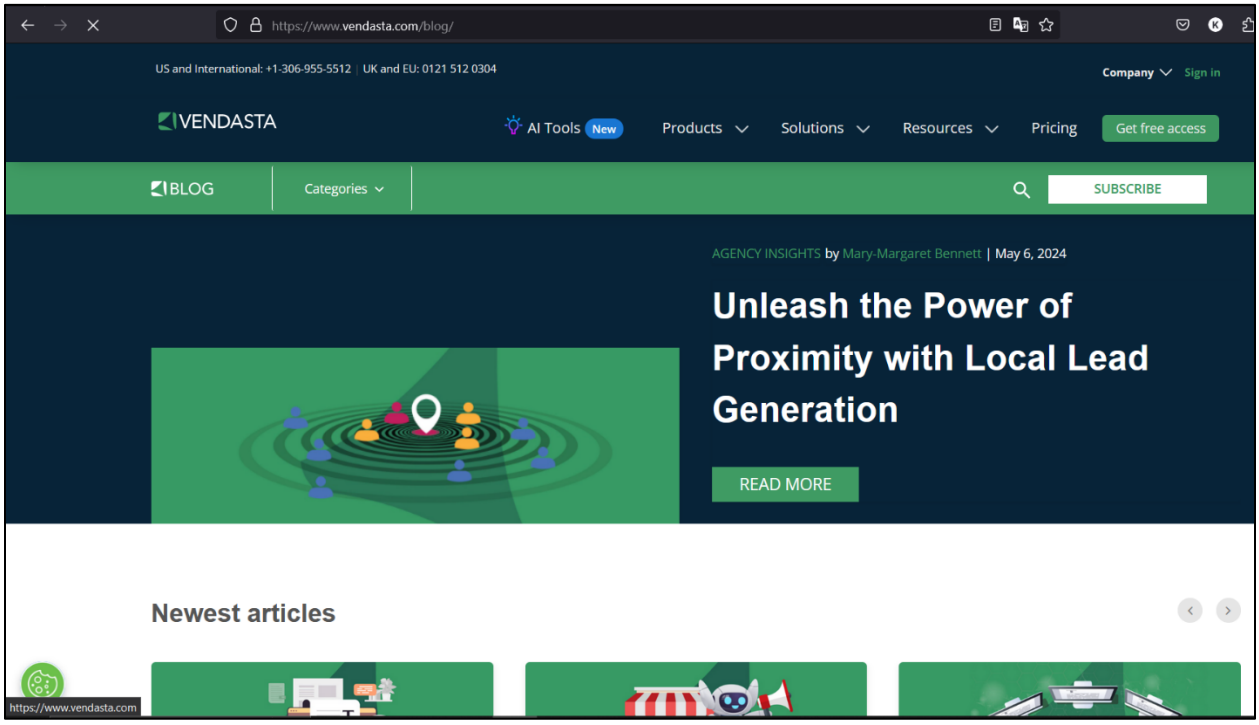
Subdomain hunting using subfinder

```
┌──(kali㉿kali)-[~]
└─$ subfinder -d vendasta.com

                projectdiscovery.io

[INF] Current subfinder version v2.6.6 (latest)
[INF] Loading provider config from /home/kali/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for vendasta.com
pub.vendasta.com
api.vendasta.com
vhs.vendasta.com
sales-test.vendasta.com
techdemos.vendasta.com
dev.vendasta.com
galaxy.vendasta.com
signup.vendasta.com
roadmap.vendasta.com
internal.vendasta.com
academy.vendasta.com
new-blog.vendasta.com
vcafe.vendasta.com
support.vendasta.com
lp.vendasta.com
info.vendasta.com
partner-central-api.vendasta.com
feedback.vendasta.com
sonarqube.vendasta.com
bmo-vpn.vendasta.com
get.vendasta.com
partners.vendasta.com
developers.vendasta.com
```

```
ideas.vendasta.com
gateway.vendasta.com
pcstraining.vendasta.com
affiliates.vendasta.com
blog.vendasta.com
vendors-demo.vendasta.com
vendasta.com
pcsdemo.vendasta.com
salestraining-dev.vendasta.com
email.vendasta.com
dhopkins.ngrok.vendasta.com
www.vendasta.com
staging.vendasta.com
video.vendasta.com
www.lp.vendasta.com
[INF] Found 38 subdomains for vendasta.com in 9 seconds 175 milliseconds
```

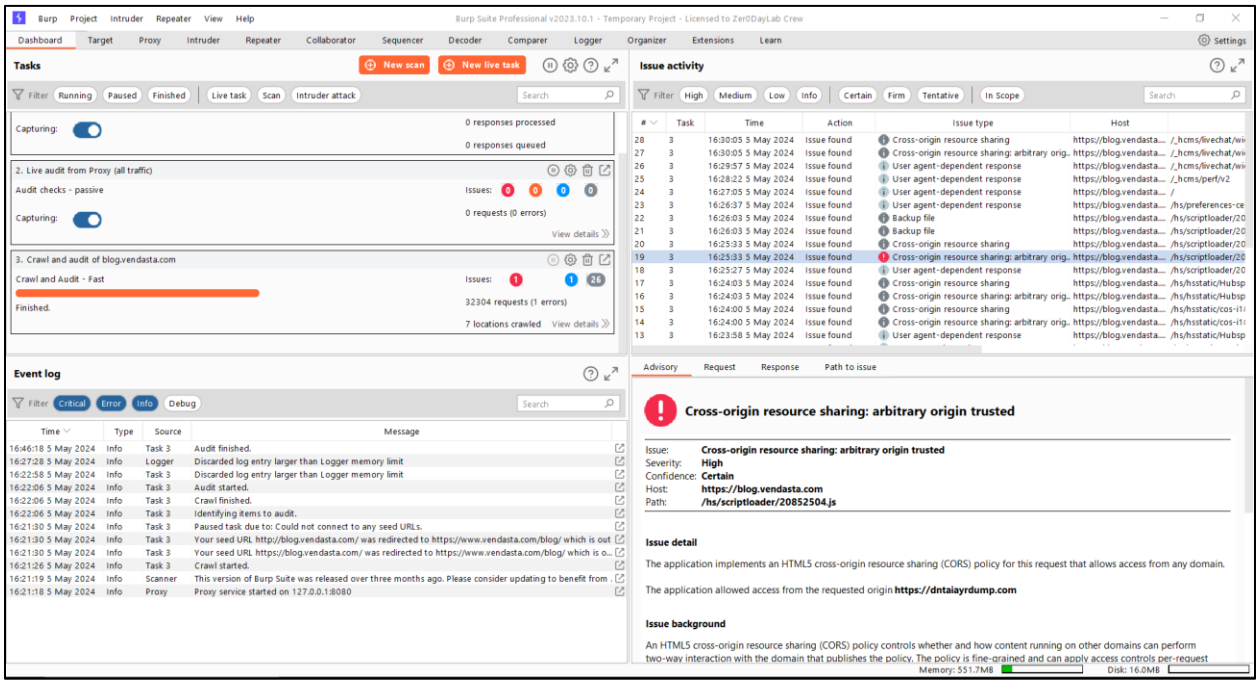
subfinder was able to find 38 subdomains.

Selected sub domain – blog.vendasta.com



Identified Vulnerabilities

1.Cross-origin resource sharing: arbitrary origin trusted (CORS)



Risk Level – High

What is CORS?

Cross-origin resource sharing (CORS) is a browser mechanism which enables controlled access to resources located outside of a given domain. It extends and adds flexibility to the same-origin policy (SOP). However, it also provides potential for cross-domain attacks if a website's CORS policy is poorly configured and implemented. CORS is not a protection against cross-origin attacks such as cross-site request forgery (CSRF).

Impact

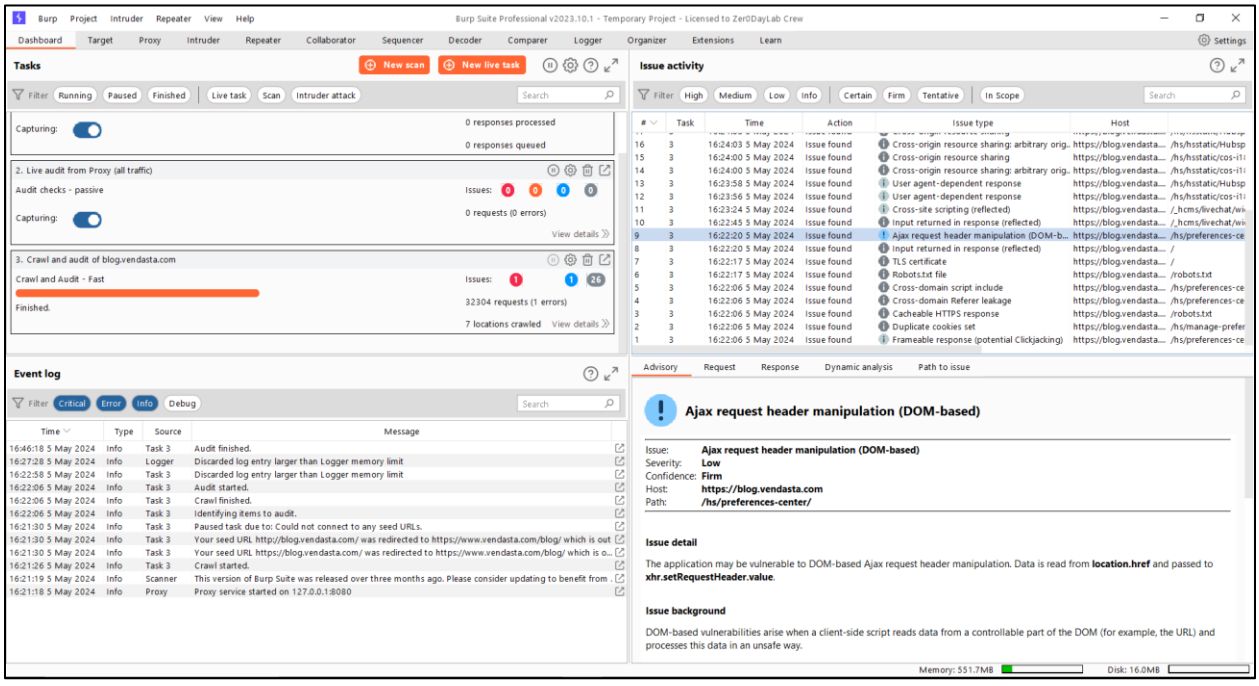
If an attacker realizes an origin that is haphazard about cross-site scripting (XSS) control, then an attacker can use the XSS to inject some JavaScript that via CORS can fetch some sensitive data from the respective site on the other side of the domain boundary.

Remedy

In regards of preventing CORS issues (CORS stands for Cross-Origin Resource Sharing), Here are some of the steps to do it.

- Customize CORS Headers: Response from server with CORS headers should be configured like Access-Control-Allow-Origin.
- Specify Allowed Origins: Articulate allowed domains and origins to connect to server resources, you either list explicitly or use asterisk to allow everyone.
- Handle Preflight Requests: Tackle OPTIONS request from browsers to authorize sequential cross-origin requests via respectable CORS header resolutions.
- Set Credentials Policy: Build Access-Control-Allow-Credentials header for cross-origin ID transmission, set `withCredentials` to true in browser code.
- Testing and Debugging: Thoroughly check applications for CORS issues by using browser developer tools that aid in the diagnosis and solving problems of the cross-origin requests.
- Security Prioritization: Limiting CORS configuration only to have permissive settings, restricting irrelevant methods and headers, and relying on credential transmission would help in securing CORS configuration.
- Update Documentation: It should be well-documented CORS policy with the allowed origins, preflight request handling, or the security concerns to let developers and integrators understand its goals.

2.Ajax request header manipulation (DOM-based)



Risk level - Low

What is Ajax request header manipulation

DOM-based Ajax request header manipulation is a type of security vulnerability found in web applications. It occurs when attackers exploit weaknesses in a web application's JavaScript code to manipulate XMLHttpRequest (XHR) objects directly through the Document Object Model (DOM). By injecting malicious headers into these XHR objects, attackers can perform various malicious actions, potentially compromising the security and integrity of the application.

Impact

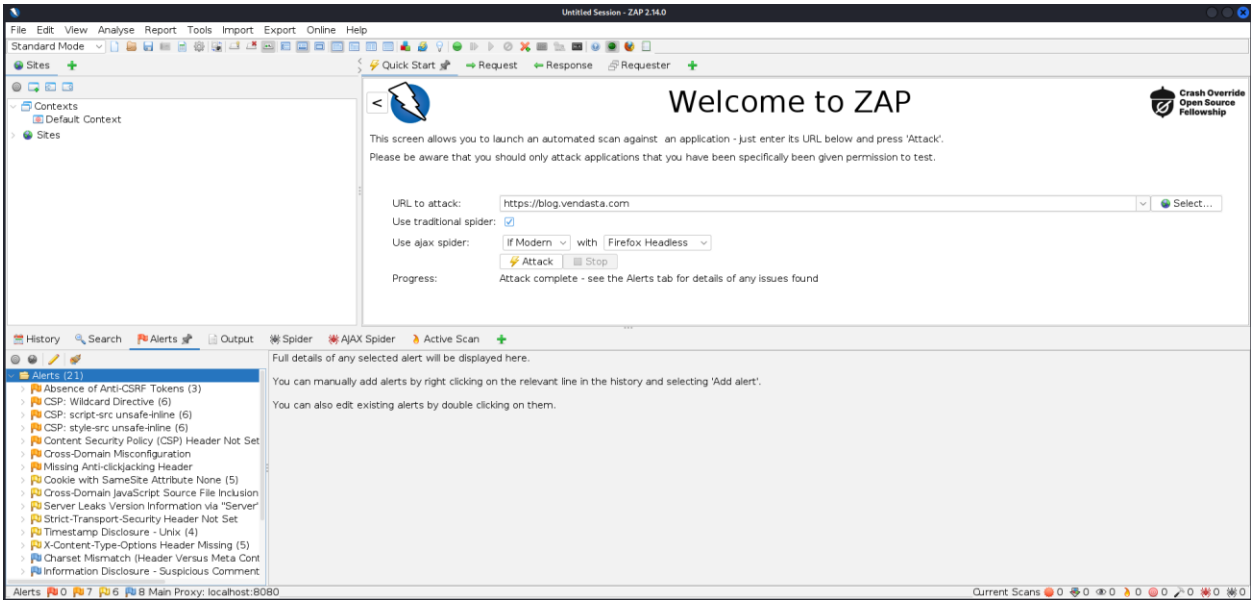
The impact of DOM-based Ajax request header manipulation can be severe and wide-ranging. Attackers can use this vulnerability to steal sensitive data, execute unauthorized actions, or manipulate server responses. Depending on the nature of the injected headers and the server's response to them, the consequences may include unauthorized access to privileged information, data leakage, or even complete compromise of the application's security.

Remedy

Preventing DOM-based Ajax request header manipulation requires a multi-layered approach to web application security:

- Input Validation: Implement strict input validation and sanitization to prevent injection attacks, including malicious code injection via DOM manipulation.
- Cross-Origin Resource Sharing (CORS) Policy: Configure proper CORS policies to restrict access to resources from unauthorized domains, limiting the scope of potential attacks.
- Content Security Policy (CSP): Utilize CSP to control the sources from which scripts can be executed, mitigating the risk of executing malicious scripts injected via DOM manipulation.
- Security Headers: Set appropriate security headers, such as X-Content-Type-Options, X-XSS-Protection, and Content-Security-Policy, to bolster the overall security posture of your web application.
- Regular Security Audits: Conduct regular security audits of your web application's codebase to identify and address vulnerabilities, including DOM-based attacks. Promptly patch any discovered issues to maintain the security and integrity of your application.

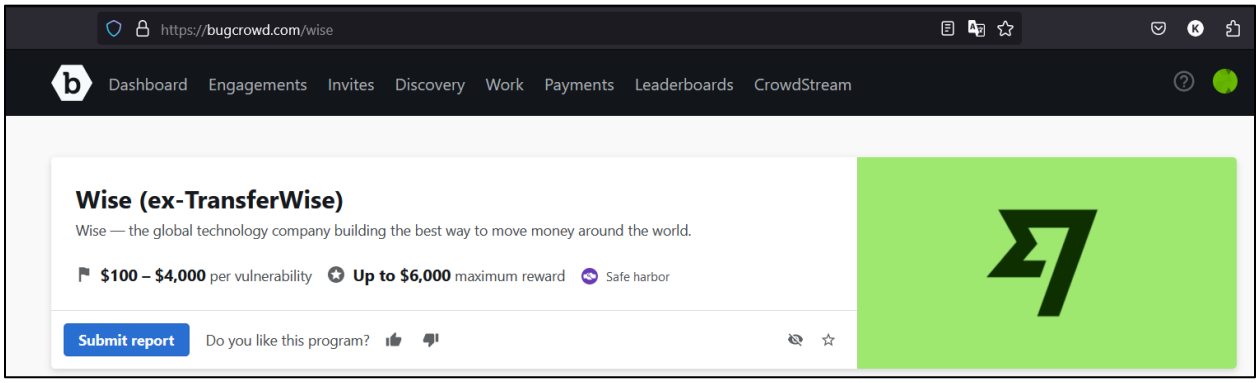
Scanning with Zap



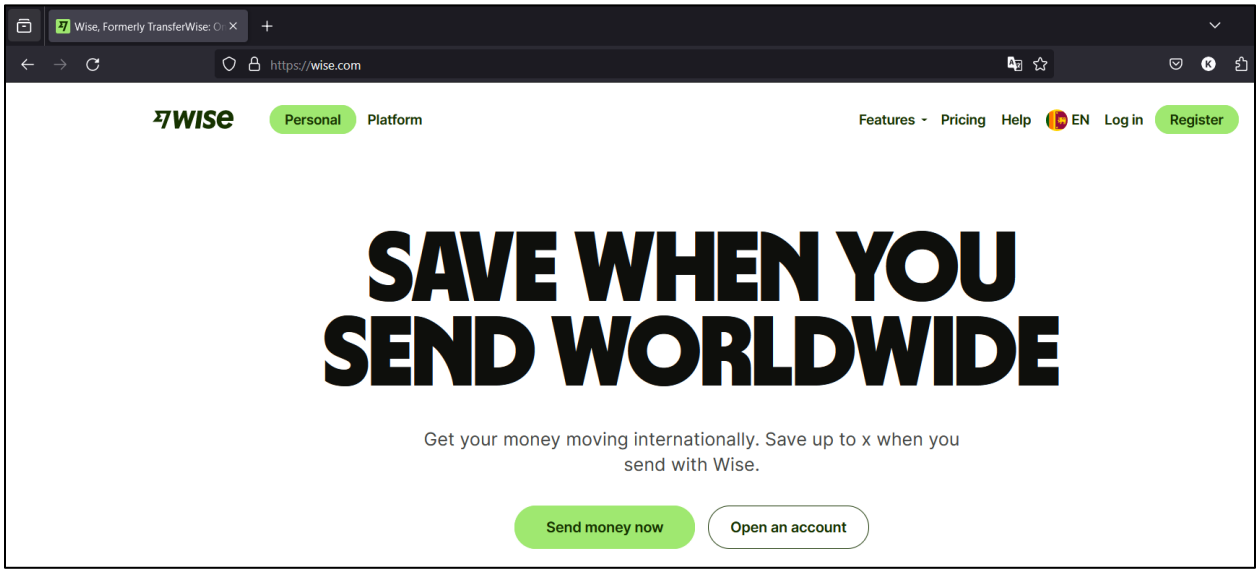
List of Other identified vulnerabilities.

1.Absence of Anti-CSRF Tokens
2.CSP: Wildcard Directive
3.CSP: script-src-unsafe-inline
4.CSP: style-src-unsafe-inline
5.CSP Header Not Set
6.Cross-Domain-Misconfiguration
7.Missing Anti-clickjacking Header

2.Wise (Report 2)



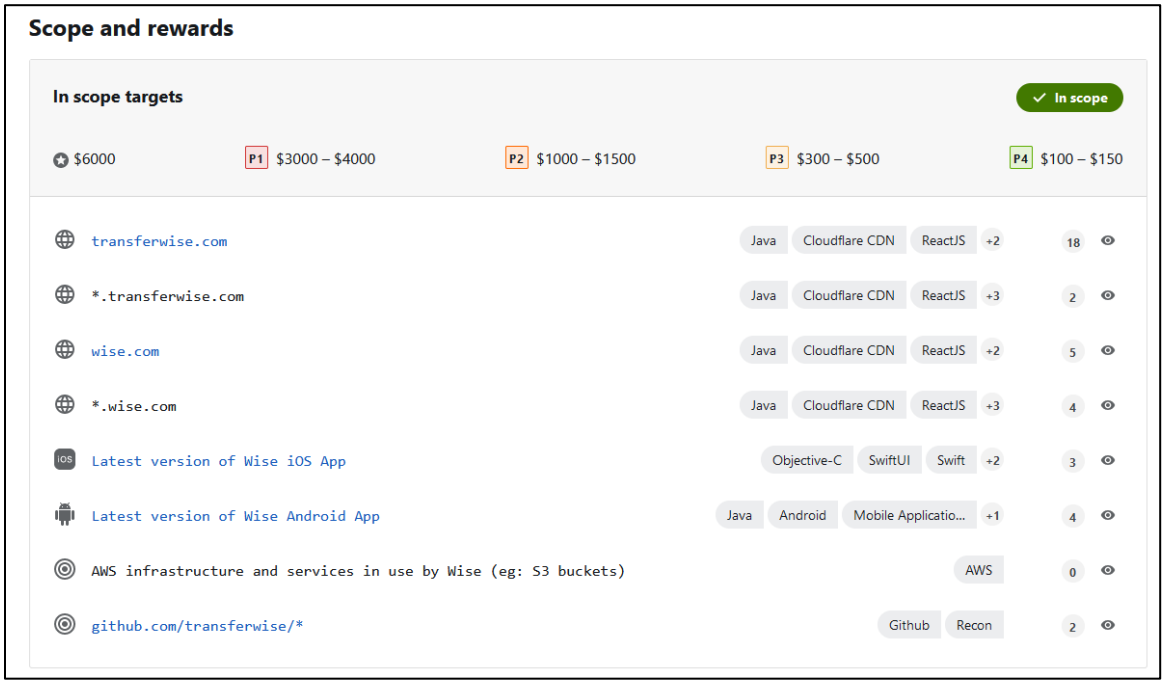
Addressing the target



Wise PLC, previously known as TransferWise, is a financial technology company focused on simplifying global money transfers.

Scope

In Scope



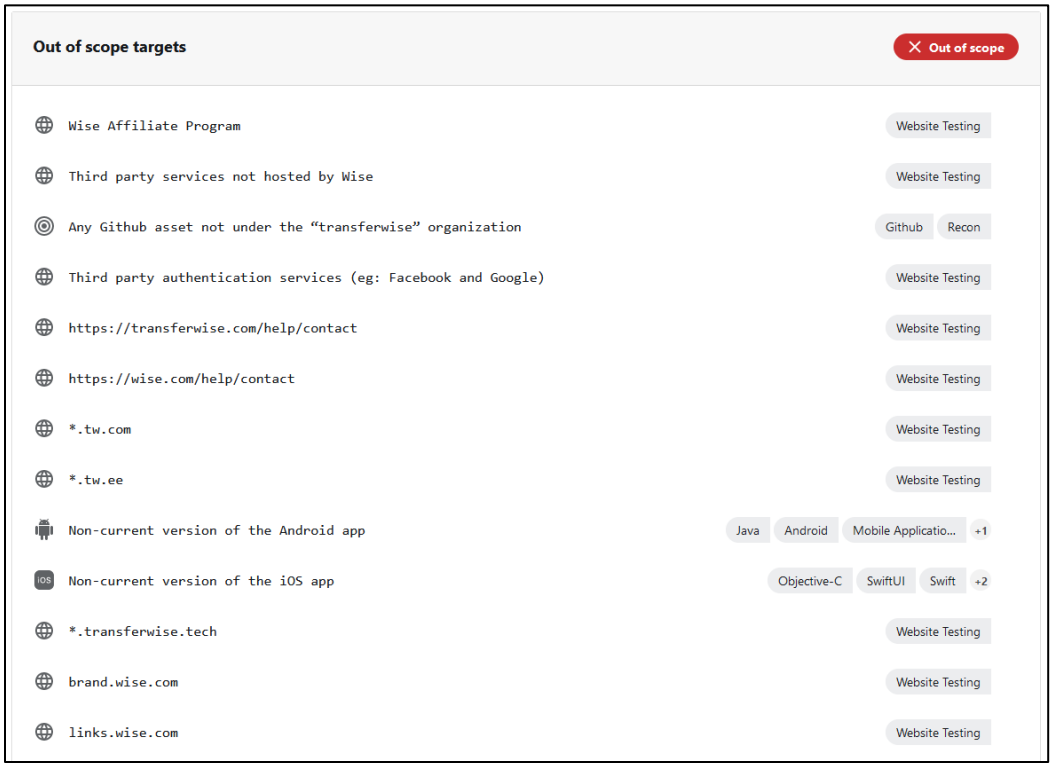
Scope and rewards

In scope targets — In scope

$6000	P1 $3000 – $4000	P2 $1000 – $1500	P3 $300 – $500	P4 $100 – $150

transferwise.com	Java, Cloudflare CDN, ReactJS, +2	18	
*.transferwise.com	Java, Cloudflare CDN, ReactJS, +3	2	
wise.com	Java, Cloudflare CDN, ReactJS, +2	5	
*.wise.com	Java, Cloudflare CDN, ReactJS, +3	4	
Latest version of Wise iOS App	Objective-C, SwiftUI, Swift, +2	3	
Latest version of Wise Android App	Java, Android, Mobile Applicatio..., +1	4	
AWS infrastructure and services in use by Wise (eg: S3 buckets)	AWS	0	
github.com/transferwise/*	Github, Recon	2	

Out of scope



Out of scope targets — Out of scope

Wise Affiliate Program	Website Testing
Third party services not hosted by Wise	Website Testing
Any Github asset not under the “transferwise” organization	Github, Recon
Third party authentication services (eg: Facebook and Google)	Website Testing
https://transferwise.com/help/contact	Website Testing
https://wise.com/help/contact	Website Testing
*.tw.com	Website Testing
*.tw.ee	Website Testing
Non-current version of the Android app	Java, Android, Mobile Applicatio..., +1
Non-current version of the iOS app	Objective-C, SwiftUI, Swift, +2
*.transferwise.tech	Website Testing
brand.wise.com	Website Testing
links.wise.com	Website Testing

Subdomain hunting using Sublist3r

```
┌──(kali㉿kali)-[~]
└─$ sublist3r -d wise.com

                 ____        _ _ _     _____
                / ___| _   _| | (_)___|_   _|__  _ __
                \___ \| | | | | | / __| | |/ _ \| '__|
                 ___) | |_| | | | \__ \ | | (_) | |
                |____/ \__,_|_|_|_|___/ |_|\___/|_|

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for wise.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[!] Error: Google probably now is blocking our requests
[~] Finished now the Google Enumeration ...
[-] Total Unique Subdomains Found: 34
bank--wise.com
www.bank--wise.com
pay.bank--wise.com
wwwtv.bank--wise.com
transferwise.com
api-docs.wise.com
au-cdrbanking-pub.wise.com
brand.wise.com
ablink.feedback.wise.com
gtm.wise.com
www.gtm.wise.com
hdfc-indialinkv2-prod.wise.com
hdfc-indialinkv2-uat.wise.com
hub.wise.com
icici.wise.com
info.wise.com
ablink.info.wise.com
jpm-latam.wise.com
www.jpm-latam.wise.com
jpm-latam-signing.wise.com
www.jpm-latam-signing.wise.com
jpm-latam-uat.wise.com
www.jpm-latam-uat.wise.com
jpm-latam-uat-signing.wise.com
www.jpm-latam-uat-signing.wise.com
neptune.wise.com
newsroom.wise.com
platform.wise.com
email.prco.wise.com
status.wise.com
vpn.wise.com
www2.wise.com
www.www2.wise.com
wwww--wise.com
```

There were 34 unique subdomains found.

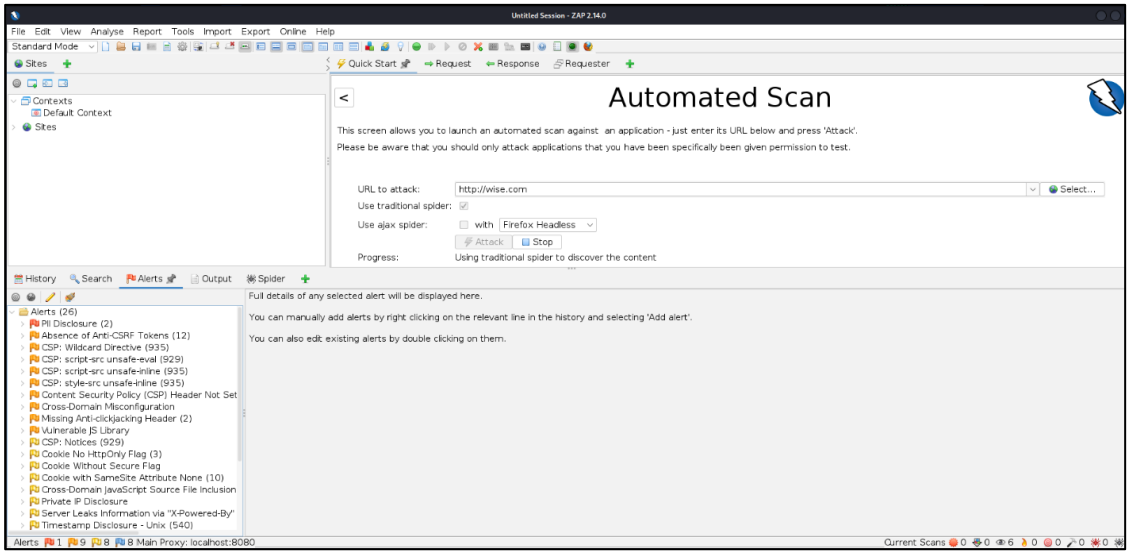
Selected domain – wise.com

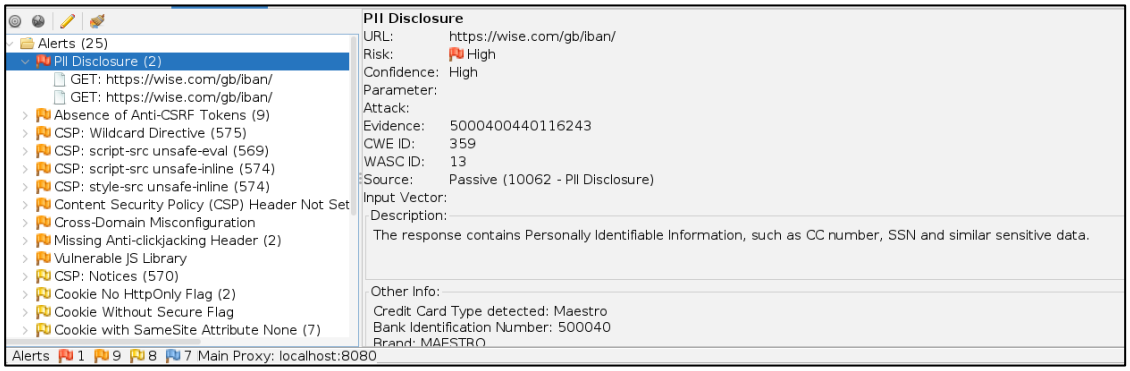
Open Ports scanning with Nmap

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS wise.com
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-24 12:40 +0530
Nmap scan report for wise.com (172.64.148.140)
Host is up (0.0066s latency).
Other addresses for wise.com (not scanned): 104.18.39.116
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8008/tcp open  http
8010/tcp open  xmpp
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 5.16 seconds
```

There we have ports 80,443,8008,8010,8080 and 8443 as open ports.

Scanning with Zap





Identified Vulnerabilities

1.PII Disclosure

Risk Level - High

What is PII Disclosure ?

PII stands in for Personally Identifiable Information, which stands for any information that may be able to pinpoint one person. It can cover a person's name, postal address, phone and cell numbers, email addresses, social security number and the like. PII leakage happens when this highly sensitive information is exposed without permission.

Impact

The impact of PII disclosure can be significant, both for individuals and for the organizations responsible for safeguarding their information. There can be some bad outcomes of PII disclosure.

- Identity Theft: Disclosure of PII creates an opportunity for identity theft to occur, in which criminals acquire personal data which they then use to impersonate unsuspecting victims by making fraudulent purchases or opening new credit accounts in the victim's name all under pretense of that identity.
- Financial Loss: Identity fraud and fraudster activities jeopardize the individual's wealth accumulation efforts by as well harming the credit score and financial reputation. Therefore, it can serve as a legal basis for the imposing of penalties and regulatory fines on organizations who fail to appropriately safeguard PII.
- Privacy Violations: Complete disclosure of personal information raises the issue of an individual's privacy rights as they can possibility go far beyond of just being intrusive into their personal lives, risking even their reputation or safety.
- Loss of Trust: Organizations that suffer at the hands of a PII exposure may experience serious reputation damage and a loss of trust from their major customers, partners and stockholders. The effects of such reputation damage may span over the long term and become obstacles to their business operations.

Remedy

To prevent PII disclosure, organizations can take several proactive measures.

- Data Encryption: Using either the 'encryption in transit' or 'encryption at rest' on confidential information enhances the security of the data by prohibiting any unauthorized access even if the data has been intercepted and compromised.
- Access Controls: The application of a tight access control and authentication methods will guarantee that a privilege is given to just official individuals in the disclosure of the PII; this puts a limit on the inside threats, the unauthorized exposure, and the misuse of the data.
- Data Minimization: Keep and delete only Personal Identifiable Information (PII) needed for business purposes and dispose of it securely after the time it is not needed.

2.Absence of Anti CSRF Tokens

Risk level - Medium

What is absence of anti CSRF tokens?

The absence of Anti-CSRF (Cross-Site Request Forgery) tokens refers to a vulnerability in web applications where they lack protection mechanisms against CSRF attacks. CSRF attacks occur when an attacker tricks a user into unknowingly executing actions on a web application in which the user is authenticated. These attacks can result in unauthorized actions being performed on behalf of the user without the user knowing about it.

Impact

CSRF attacks can lead to unauthorized actions being performed on behalf of the user, such as changing account settings, making purchases, or deleting data. By including Anti-CSRF tokens in an application, we can be protected against CSRF attacks by ensuring that requests are only accepted if they include a valid token that is generated and verified by the server-side code.

Remedy

To mitigate the risk of CSRF attacks, web developers should implement Anti-CSRF tokens as part of their security measures, ensuring that each request made to the server includes a valid token that can be verified to confirm the legitimacy of the request.

3.CSP Wildcard Directive

Risk level - Medium

What is CSP Wildcard Directive?

The Content Security Policy (CSP) wildcard directive (*) is used to allow or restrict content from any origin. When the wildcard is used in a CSP header, it means that the specified policy applies to all origins, including those that are not explicitly defined in the policy.

Impact

The impact of CSP Wildcard Directive can be significant. Here are some of the things that could happen

- Increased Attack Surface: When open to content from any location it can add to the number of potential attack vectors of your site.
- Bypassing CSP Protections: The harasser might utilize the strategy to get out of CSP safeguards.
- Data Leakage: It might be the case that if resources are allowed from different origins, then there is a possibility of unauthorized data dissemination.

Remedy

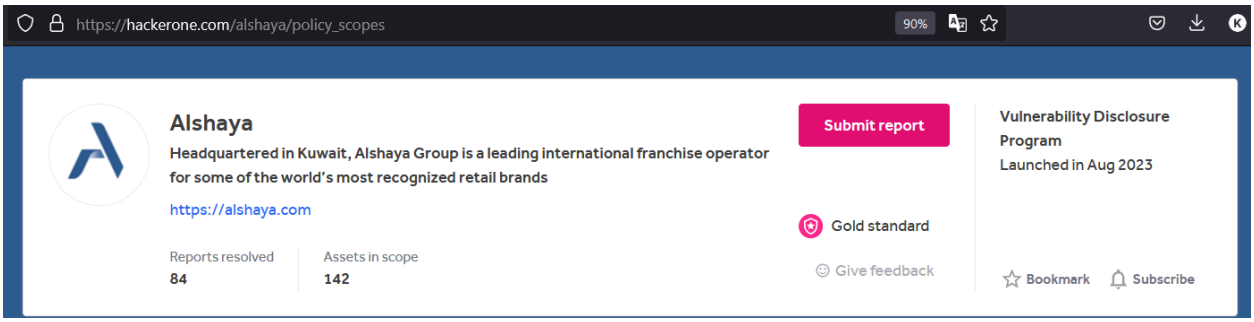
To prevent the negative impact of using the wildcard directive in CSP,following steps can be taken

- Avoid Using the Wildcard Directive: Point to exact locations on the map instead of using asterisk marker.
- Use Nonce or Hash-Based CSP: Implement nonce or hash-based Projected Code Protection to control the script execution.
- Regularly Review and Update CSP Policies: Check and do not put overwriting policies and get rid of wildcard directives.

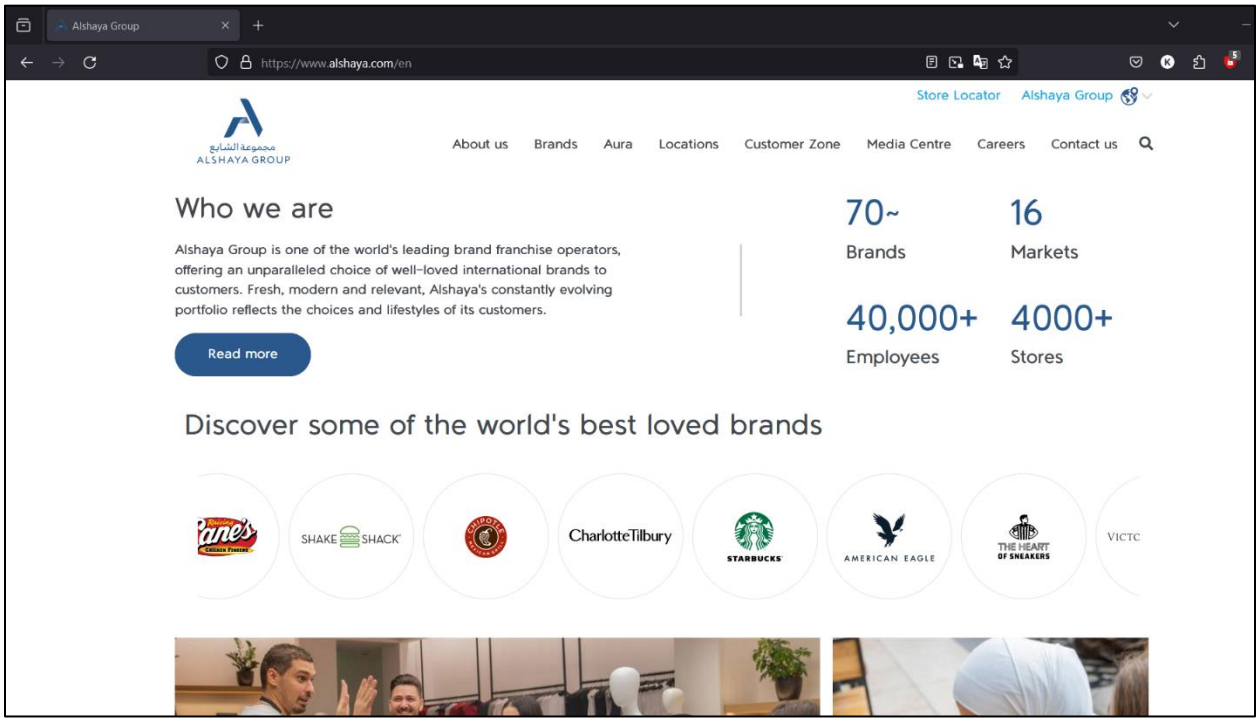
List of Other identified vulnerabilities.

1. CSP: script-src-unsafe-eval
2. CSP: script-src-unsafe-inline
3. CSP: style-src-unsafe-inline
4 .Missing Anti-clickjacking Header
5 .Vulnerable Js library

3.Alshaya (Report 3)



Addressing the target



Headquartered in Kuwait, Alshaya Group is a leading international franchise operator for some of the world's most recognized retail brands.

Scope

In scope

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
*.starbucks.com.kz	Wildcard	In scope	Critical	Ineligible	May 11, 2023	0 (0%)
*.aloyoga.com.kw	Wildcard	In scope	Critical	Ineligible	May 11, 2023	0 (0%)
*.aloyoga.com.qa	Wildcard	In scope	Critical	Ineligible	May 11, 2023	0 (0%)
*.americaneagle.com.bh	Wildcard	In scope	Critical	Ineligible	May 11, 2023	1 (1%)
*.americaneagle.com.eg	Wildcard	In scope	Critical	Ineligible	May 11, 2023	0 (0%)
*.americaneagle.com.jo	Wildcard	In scope	Critical	Ineligible	May 11, 2023	0 (0%)
*.americaneagle.com.kw	Wildcard	In scope	Critical	Ineligible	May 11, 2023	1 (1%)
*.americaneagle.com.qa	Wildcard	In scope	Critical	Ineligible	May 11, 2023	0 (0%)
*.americaneagle.com.sa	Wildcard	In scope	Critical	Ineligible	May 11, 2023	0 (0%)
*.bathandbodyworks.ae	Wildcard	In scope	Critical	Ineligible	May 11, 2023	0 (0%)
*.westelm.com.sa	Wildcard	In scope	Critical	Ineligible	May 11, 2023	0 (0%)
*.westelm.com.kw	Wildcard	In scope	Critical	Ineligible	May 11, 2023	0 (0%)
*.westelm.ae	Wildcard	In scope	Critical	Ineligible	May 11, 2023	0 (0%)

Out of scope

comsuat.carrier.alshaya.com	Domain	In scope	Critical	Ineligible	May 11, 2023	0 (0%)
customercare.alshaya.com	Domain	In scope	Critical	Ineligible	May 11, 2023	1 (1%)
dev.alshaya.com	Domain	In scope	Critical	Ineligible	May 11, 2023	0 (0%)
devimages.alshaya.com	Domain	In scope	Critical	Ineligible	May 11, 2023	0 (0%)
gtmsservice.alshaya.com	Domain	In scope	Critical	Ineligible	May 11, 2023	0 (0%)
internaljobs.alshaya.com This is our internal jobs career site	Domain	In scope	Critical	Ineligible	Aug 4, 2023	0 (0%)

Subdomain hunting using subfinder.

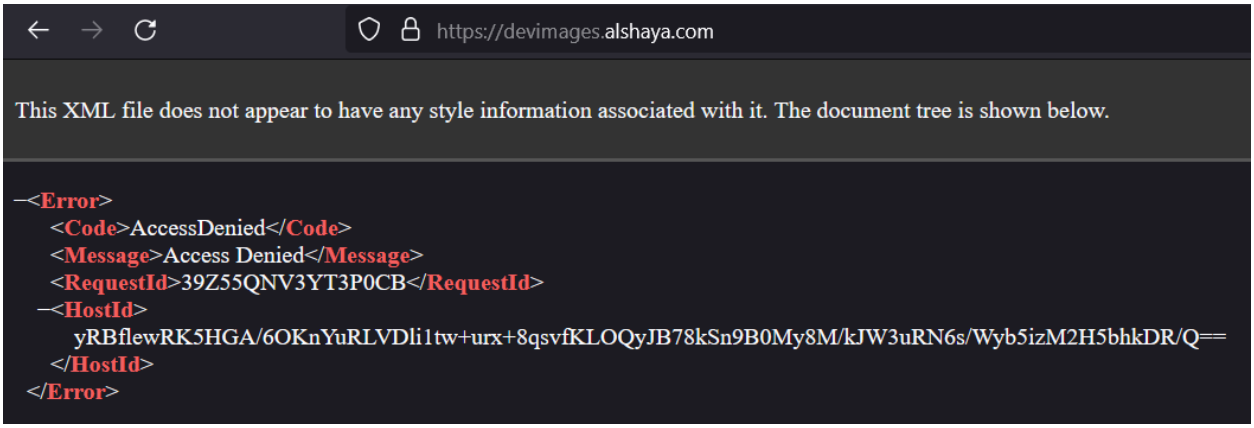
```
┌──(kali㉿kali)-[~]
└─$ subfinder -d alshaya.com

               __    _____           __
   _______  __/ /_  / __(_)___  ____/ /__  _____
  / ___/ / / / __ \/ /_/ / __ \/ __  / _ \/ ___/
 (__  ) /_/ / /_/ / __/ / / / / /_/ /  __/ /
/____/\__,_/_.___/_/ /_/_/ /_/\__,_/\___/_/

                projectdiscovery.io

[INF] Current subfinder version v2.6.6 (latest)
[INF] Loading provider config from /home/kali/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for alshaya.com
www.performans.alshaya.com
www.tbstr-uat.alshaya.com
deb.prod-pimsfactory.alshaya.com
trbi.alshaya.com
alshayaebspub-tst.stg.alshaya.com
sftp.alshaya.com
tbsru-uat.alshaya.com
finprdap-test.alshaya.com
vx.alshaya.com
www.motehrcare.alshaya.com
hps.alshaya.com
apigw.dev.alshaya.com
ilsdatavalidation.alshaya.com
mena.cardtest.alshaya.com
emr.alshaya.com
infra.alshaya.com
expe3.meeting.alshaya.com
kwtprarclog03.alshaya.com
mft.dsuat.alshaya.com
kwtprarclog01.alshaya.com
reim.alshaya.com
goldfpls.alshaya.com
dev.mobile.alshaya.com
store.alshaya.com
```

```
soa.dsuat.alshaya.com
www.lsukadmin.alshaya.com
apigw.trn.alshaya.com
mcprod.cos.store.alshaya.com
wes-training.store.alshaya.com
testpoc.alshaya.com
rmq-store.alshaya.com
www.mothercare.alshaya.com
ecmail.alshaya.com
ksadeveinvoice.alshaya.com
devimages.alshaya.com
mia.alshaya.com
staging-bbw.store.alshaya.com
passwordreset.alshaya.com
bbw.prod-pimsfactory.alshaya.com
alo-pprod.store.alshaya.com
hrssaccess.alshaya.com
dizzliuat.alshaya.com
mc-test.store.alshaya.com
mft.dev.alshaya.com
test.alshaya.com
fl-uat2.store.alshaya.com
fl-pprod.store.alshaya.com
expe.meeting.alshaya.com
trho01.tursbc.alshaya.com
```

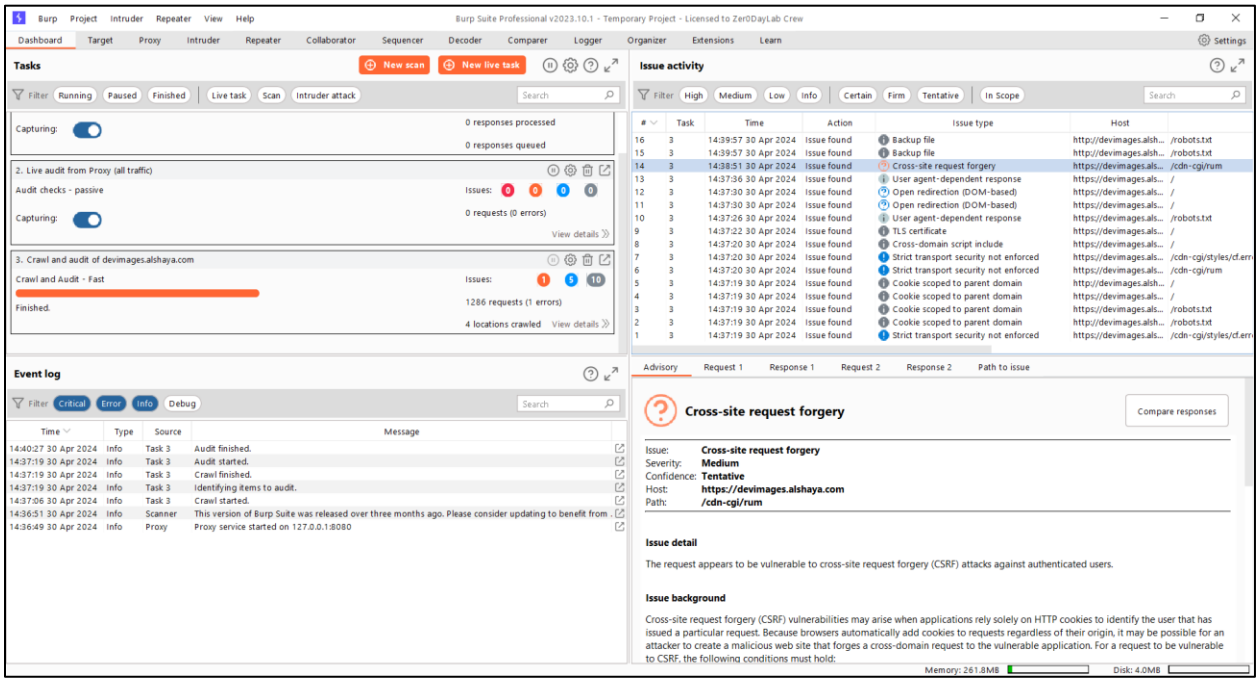
```
www.alshaya.com
pb-pprod.store.alshaya.com
mpos.alshaya.com
ksa-cp-ro-expe-02.meeting.alshaya.com
pb-test.store.alshaya.com
wes-uat.store.alshaya.com
automic.prd.alshaya.com
ksa-cp-ro-expe.meeting.alshaya.com
tbs.store.alshaya.com
dvsum.alshaya.com
sp.uat.alshaya.com
vs.store.alshaya.com
webmail.alshaya.com
autodiscover.alshaya.com
bip.uat.alshaya.com
rmq-qa.store.alshaya.com
odi.dev2.alshaya.com
mft.dssit.alshaya.com
www.ppmtrend.alshaya.com
soa.dssit.alshaya.com
ns2.alshaya.com
aeo.store.alshaya.com
deb-pprod.store.alshaya.com
starbucksb2b.alshaya.com
soa.trn.alshaya.com
www.apimuae-prod.alshaya.com
employeeservices.alshaya.com
deb-uat.store.alshaya.com
ar.coskw-uat.factory.alshaya.com
muji.prod-pimsfactory.alshaya.com
czone.alshaya.com
www.lasenzauat.alshaya.com
[INF] Found 521 subdomains for alshaya.com in 37 seconds 101 milliseconds
```

Subfinder found 521 unique sub domains.

Selected – devimages.alshaya.com



Identified vulnerabilities



1. CSRF

Risk level - High

What is CSRF (Cross-Site Request Forgery)?

Cross-Site Request Forgery (CSRF) is a type of malicious exploit of a web vulnerability that allows an attacker to perform actions on behalf of an authenticated user without their consent. It typically occurs when a user is authenticated on a legitimate website and unknowingly visits a malicious site or clicks on a malicious link. The malicious site generates requests to the legitimate site on which the victim is authenticated, exploiting the fact that the browser automatically includes the user's authentication tokens with the forged requests.

Impact

The impact of CSRF can be severe, potentially leading to unauthorized actions being performed on the victim's behalf on the legitimate website. This could include transferring funds, changing account settings, posting content, or any other action that the authenticated user is authorized to perform. CSRF attacks can compromise the integrity, confidentiality, and availability of the victim's data and resources. Furthermore, they can damage the reputation of the affected website and erode user trust

Remedy

Several measures can be implemented to mitigate the risk of CSRF attacks:

- CSRF Tokens: Include unique tokens in each form or request that are validated by the server to ensure that the request originated from the legitimate site.
- SameSite Cookies: Use the SameSite attribute for cookies to restrict when cookies are sent along with a request, preventing them from being sent on cross-origin requests.
- Referer Header Checking: Verify the Referer header to ensure that requests originate from the expected domain.
- Custom Request Headers: Include custom headers in requests and verify them on the server side to ensure that the request is legitimate.

Scanning with Nikto

The X-Content-Type-Options header is not Set

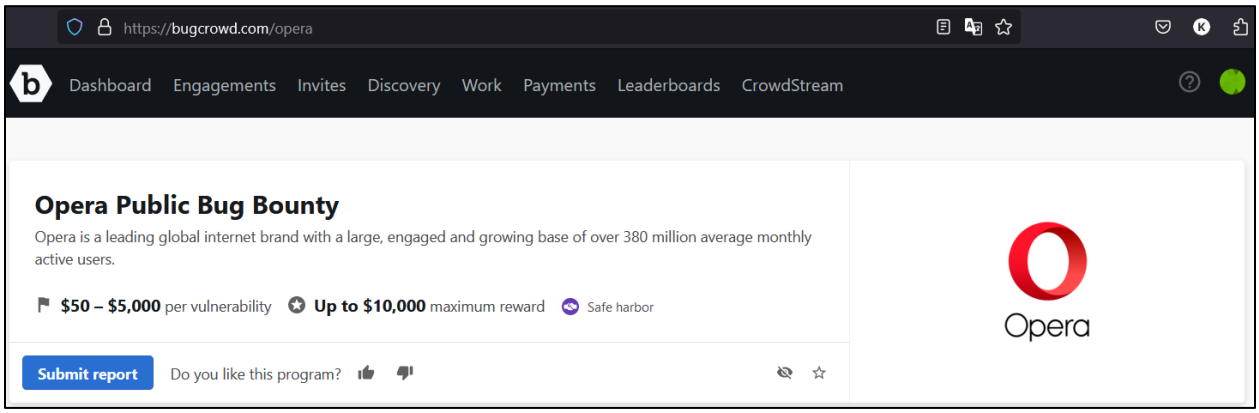
What is it?
The X-Content-Type-Options header is a HTTP header that tells the browser not to perform MIME sniffing but instead to adhere strictly to the Content-Type header provided by the server.

Impact
If this header is missing, it could potentially expose the application to MIME sniffing attacks. This means that an attacker could manipulate the content of a response in such a way that a browser might interpret it as a different MIME type than intended. This could lead to various security vulnerabilities such as cross-site scripting (XSS) attacks or data injection attacks.

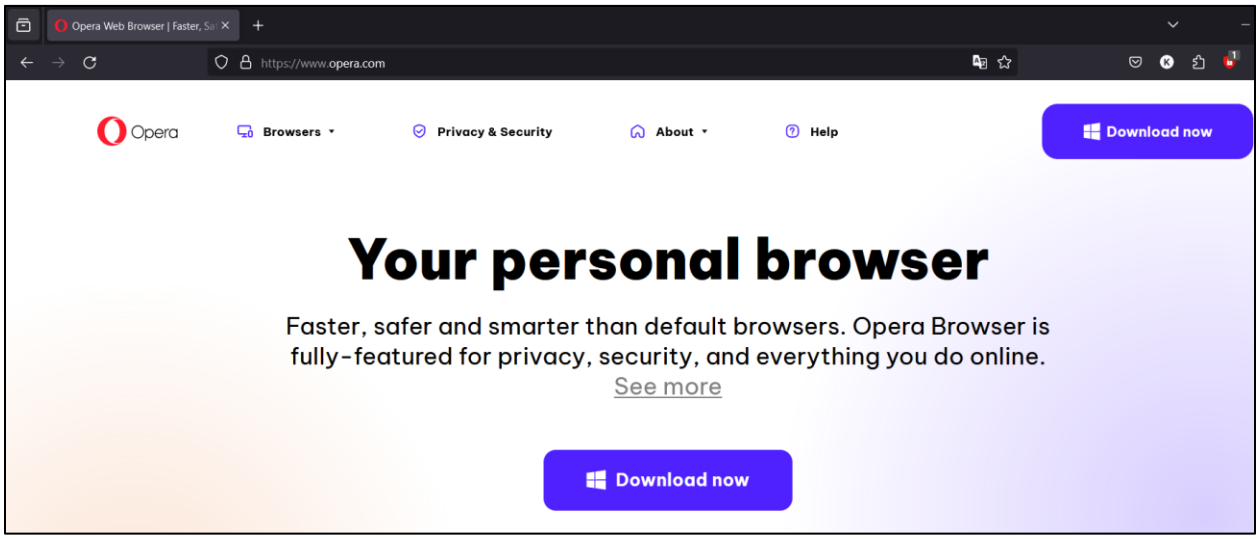
Remedy

To mitigate the risk associated with missing X-Content-Type-Options header, you can add it to your server configuration or web application. You can set the value of this header to "nosniff", which instructs the browser not to perform MIME sniffing.

4.Opera (Report 4)



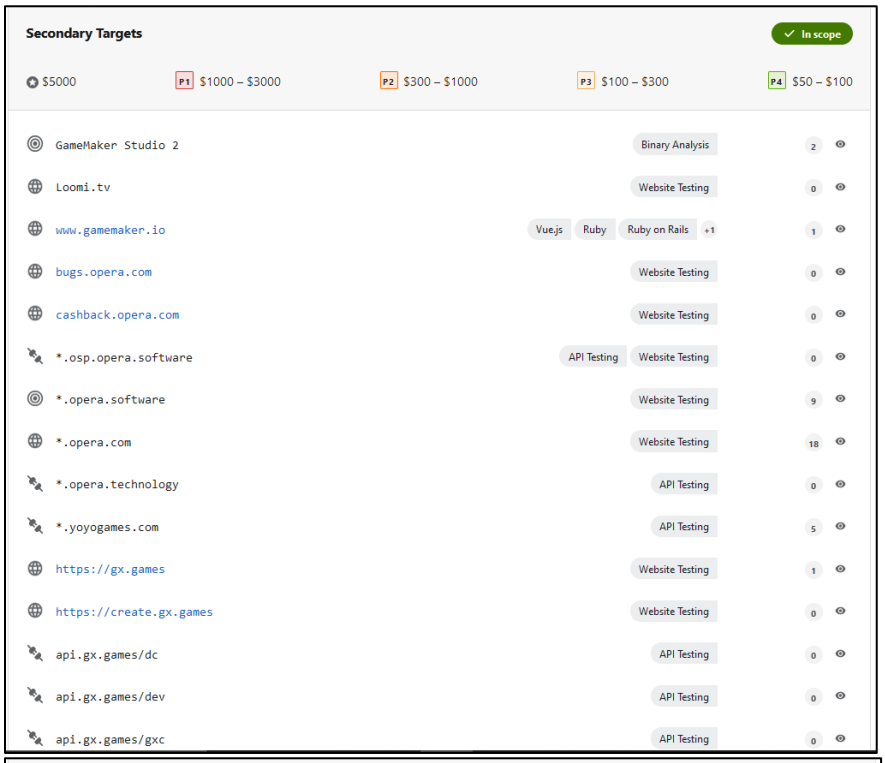
Addressing the target



Opera.com is the official website of Opera Software, a Norwegian company known for its web browsers, primarily the Opera web browser. Opera.com serves as a platform for users to download Opera browsers, access news and updates about the company's products, and explore additional services such as Opera GX, a browser specifically designed for gamers. Additionally, the website provides information about Opera's various features, extensions, and resources for developers.

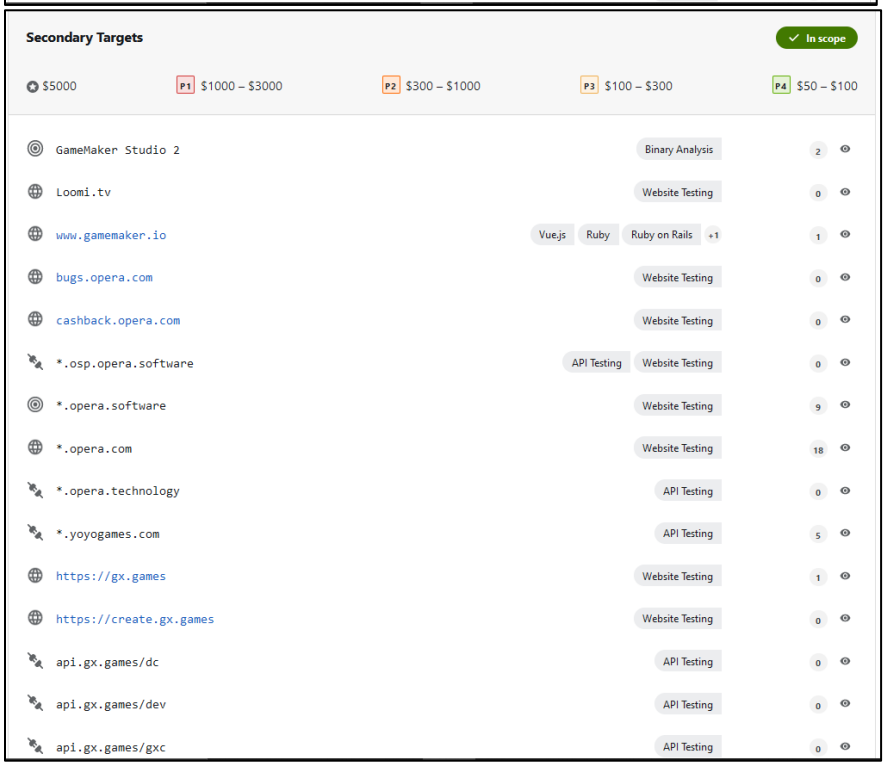
Scope

In scope



Secondary Targets — In scope

$5000	P1 $1000 – $3000	P2 $300 – $1000	P3 $100 – $300	P4 $50 – $100
GameMaker Studio 2			Binary Analysis	2
Loomi.tv			Website Testing	0
www.gamemaker.io			Vue.js Ruby Ruby on Rails +1	1
bugs.opera.com			Website Testing	0
cashback.opera.com			Website Testing	0
*.osp.opera.software			API Testing Website Testing	0
*.opera.software			Website Testing	9
*.opera.com			Website Testing	18
*.opera.technology			API Testing	0
*.yoyogames.com			API Testing	5
https://gx.games			Website Testing	1
https://create.gx.games			Website Testing	0
api.gx.games/dc			API Testing	0
api.gx.games/dev			API Testing	0
api.gx.games/gxc			API Testing	0



Secondary Targets — In scope

$5000	P1 $1000 – $3000	P2 $300 – $1000	P3 $100 – $300	P4 $50 – $100
GameMaker Studio 2			Binary Analysis	2
Loomi.tv			Website Testing	0
www.gamemaker.io			Vue.js Ruby Ruby on Rails +1	1
bugs.opera.com			Website Testing	0
cashback.opera.com			Website Testing	0
*.osp.opera.software			API Testing Website Testing	0
*.opera.software			Website Testing	9
*.opera.com			Website Testing	18
*.opera.technology			API Testing	0
*.yoyogames.com			API Testing	5
https://gx.games			Website Testing	1
https://create.gx.games			Website Testing	0
api.gx.games/dc			API Testing	0
api.gx.games/dev			API Testing	0
api.gx.games/gxc			API Testing	0

Scope and rewards

Primary Targets — In scope

$10000	P1 $3000 – $5000	P2 $500 – $3000	P3 $200 – $500	P4 $100 – $200

Opera PC	macOS, Windows, Binary Analysis	4
Opera GX	macOS, Windows, Binary Analysis	1
www.opera.com	Django, Website Testing, Python	0
auth.opera.com	Django, Website Testing, Python	2
accounts.opera.com	API Testing	0
speeddials.opera.com	API Testing	0
flow.opera.com	API Testing	0
autoupdate.geo.opera.com	API Testing	0
net.geo.opera.com	Website Testing	0
get.geo.opera.com	API Testing, nginx, Website Testing	0
download.opera.com	Django, Website Testing, Python	0
browser-notifications.opera.com	API Testing	0

Out of scope

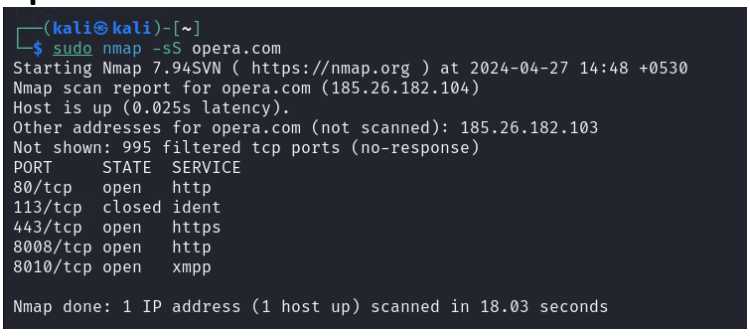
Out of scope — Out of scope

- admanager.opera.com
- accountsstage.yoyogames.com
- bugs.yoyogames.com
- catch.opera.com
- certs.opera.com
- checkout.opera.com
- concurso.opera.com
- contest.opera.com
- control.gx-servers.opera.com
- help.gx-servers.opera.com
- help.yoyogames.com
- interstitial.opera-mini.net
- investor.opera.com
- jobs.opera.com
- s2{1,2}-05-08-v09.opera-mini.net
- tabfulness.opera.com
- verizon-us-seattle.opera-mini.net
- verizon-us-lvs-seattle.opera-mini.net
- verizon-us-lvs-ashburn.opera-mini.net

Subdomain hunting with sublist3r

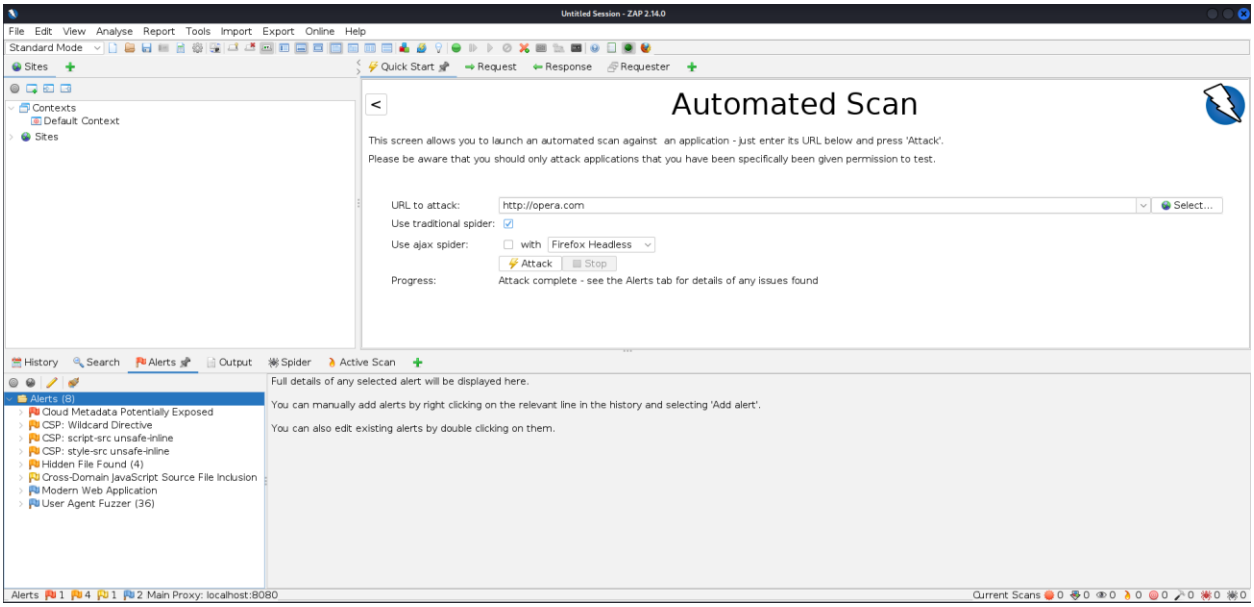
There were 312 unique subdomains.

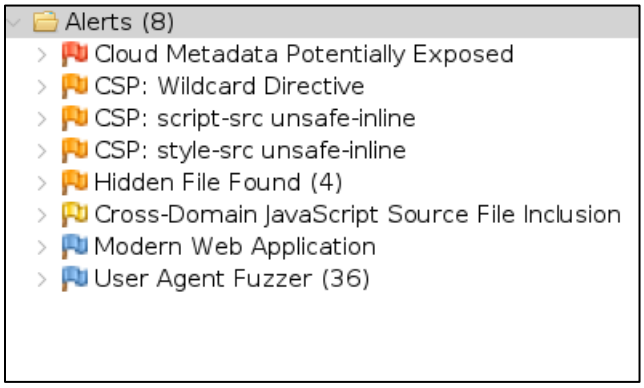
Open Ports

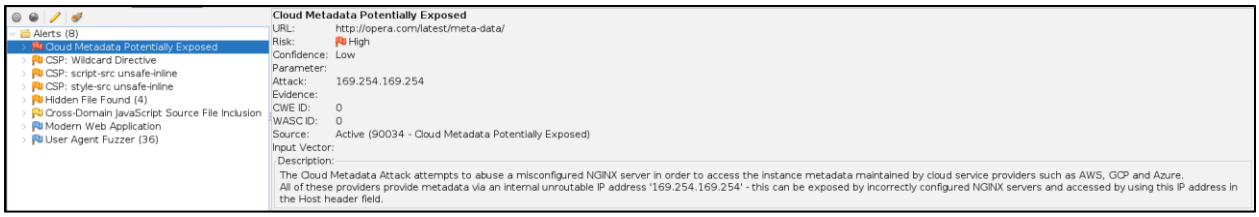


Port 80,113,443,8008 and 8010 was identified as open ports

Zap


Untitled Session - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
Automated Scan
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack:
http://opera.com
Select...
Use traditional spider:
Use ajax spider:
with
Firefox Headless
Attack
Stop
Progress:
Attack complete - see the Alerts tab for details of any issues found
History
Search
Alerts
Output
Spider
Active Scan
Alerts (8)
Cloud Metadata Potentially Exposed
CSP: Wildcard Directive
CSP: script-src unsafe-inline
CSP: style-src unsafe-inline
Hidden File Found (4)
Cross-Domain JavaScript Source File Inclusion
Modern Web Application
User Agent Fuzzer (36)
Full details of any selected alert will be displayed here.
You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.
You can also edit existing alerts by double clicking on them.
Alerts 1 4 1 2 Main Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0 0 0


Alerts (8)
Cloud Metadata Potentially Exposed
CSP: Wildcard Directive
CSP: script-src unsafe-inline
CSP: style-src unsafe-inline
Hidden File Found (4)
Cross-Domain JavaScript Source File Inclusion
Modern Web Application
User Agent Fuzzer (36)


Alerts (8)
Cloud Metadata Potentially Exposed
CSP: Wildcard Directive
CSP: script-src unsafe-inline
CSP: style-src unsafe-inline
Hidden File Found (4)
Cross-Domain JavaScript Source File Inclusion
Modern Web Application
User Agent Fuzzer (36)
Cloud Metadata Potentially Exposed
URL: http://opera.com/latest/meta-data/
Risk: High
Confidence: Low
Parameter:
Attack: 169.254.169.254
Evidence:
CWE ID: 0
WASC ID: 0
Source: Active (90034 - Cloud Metadata Potentially Exposed)
Input Vector:
Description:
The Cloud Metadata Attack attempts to abuse a misconfigured NGINX server in order to access the instance metadata maintained by cloud service providers such as AWS, GCP and Azure.
All of these providers provide metadata via an internal unroutable IP address '169.254.169.254' - this can be exposed by incorrectly configured NGINX servers and accessed by using this IP address in the Host header field.

Scanning with Nikto

Identified vulnerabilities

1.Cloudmetadata Potentially exposed

Risk Level - High

Cloud metadata refers to data about data within a cloud computing environment. It includes information such as the configuration, usage patterns, access controls, and other attributes associated with the resources and services deployed in the cloud.Resource Configurations,Access Control information,Network Topologies and Service Metadata can be exposed with this

Impact

- Security Risks: Exposing sensitive metadata can lead to security breaches, as attackers can leverage this information to identify vulnerabilities, misconfigurations, or valuable targets within the cloud environment.
- Privacy Concerns: Revealing user identities, access permissions, and usage patterns may violate privacy regulations and expose individuals or organizations to risks such as identity theft or unauthorized surveillance.
- Compliance Violations: Failure to adequately protect metadata can result in non-compliance with industry standards and regulatory requirements, leading to legal penalties and reputational damage.

Remedy

- Access Controls: Implement strict access controls to limit who can view and modify metadata within the cloud environment. Use role-based access control (RBAC) and least privilege principles to restrict access only to authorized personnel.
- Encryption: Encrypt sensitive metadata at rest and in transit to prevent unauthorized access even if the data is compromised.
- Monitoring and Auditing: Implement robust monitoring and auditing mechanisms to detect suspicious activities and unauthorized access attempts. Regularly review access logs and perform security assessments to identify and remediate any vulnerabilities.

2.Anti clickjacking x-frame header not found

What is Anti clickjacking x-frame header not found ?

Anti-clickjacking X-Frame-Options header is a security feature implemented on web servers to mitigate clickjacking attacks. Clickjacking is a malicious technique where an attacker tricks a user into clicking on something different from what the user perceives, potentially leading to unintended actions or information disclosure.

Impact:

- Security Vulnerabilities: Without the X-Frame-Options header, the website is vulnerable to clickjacking attacks, where attackers can overlay malicious content over the legitimate site, tricking users into performing actions they didn't intend.
- Data Exposure: Clickjacking attacks can lead to the inadvertent disclosure of sensitive information, such as login credentials, payment details, or personal data.
- Reputation Damage: Successful clickjacking attacks can undermine user trust and tarnish the reputation of the website or application, leading to loss of customers and revenue.

Remedy:

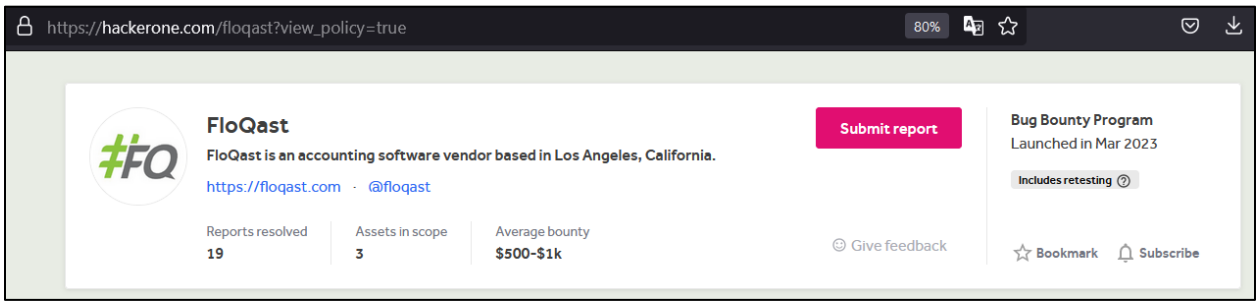
- Implementation of X-Frame-Options Header: Configure the web server to include the X-Frame-Options header in HTTP responses with a value of "DENY" to prevent the page from being rendered in a frame or "SAMEORIGIN" to allow rendering only in frames from the same origin.

- Content Security Policy (CSP): Use CSP to define a policy that restricts which external resources can be loaded by the web page, including the frame-ancestors directive to specify the domains that are allowed to embed the page.
- Frame-busting Scripts: Implement frame-busting scripts within the web page's code to prevent the page from being framed by other sites. These scripts can detect when the page is being loaded within a frame and break out of it or prevent further execution.

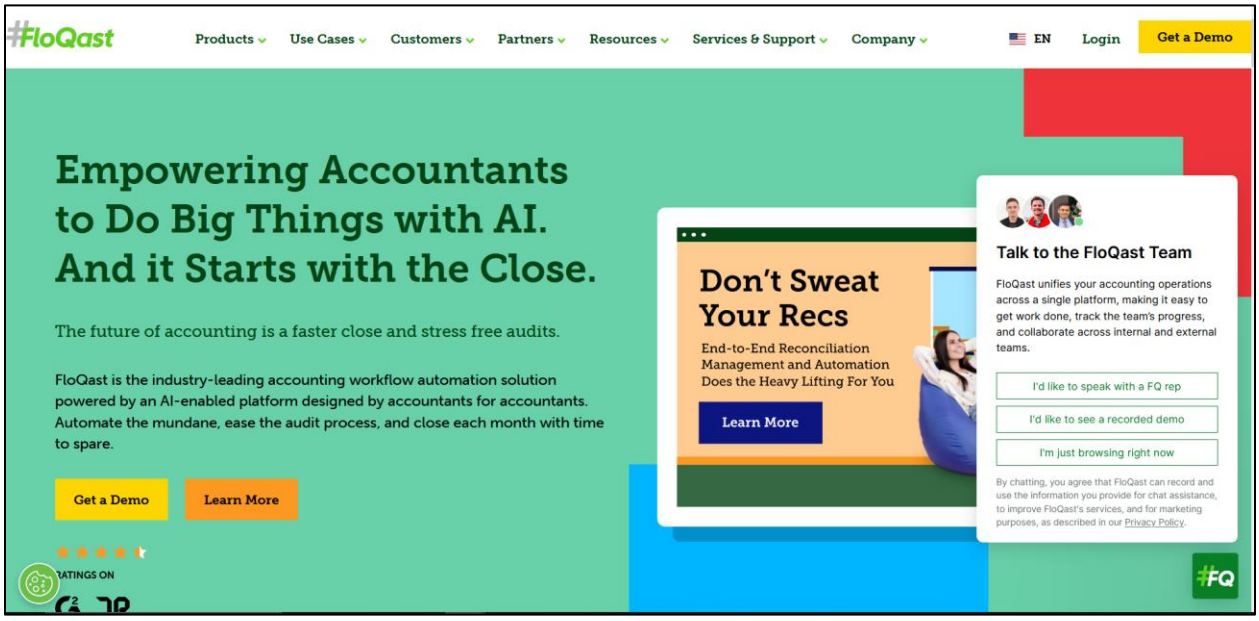
Other identified vulnerabilities

1.CSP : Wildcard Directive
2.CSP: script-src-unsafe-inline
3.CSP: style-src-unsafe-inline
4.Hidden files found

5.FloQast (Report 5)



Addressing the site

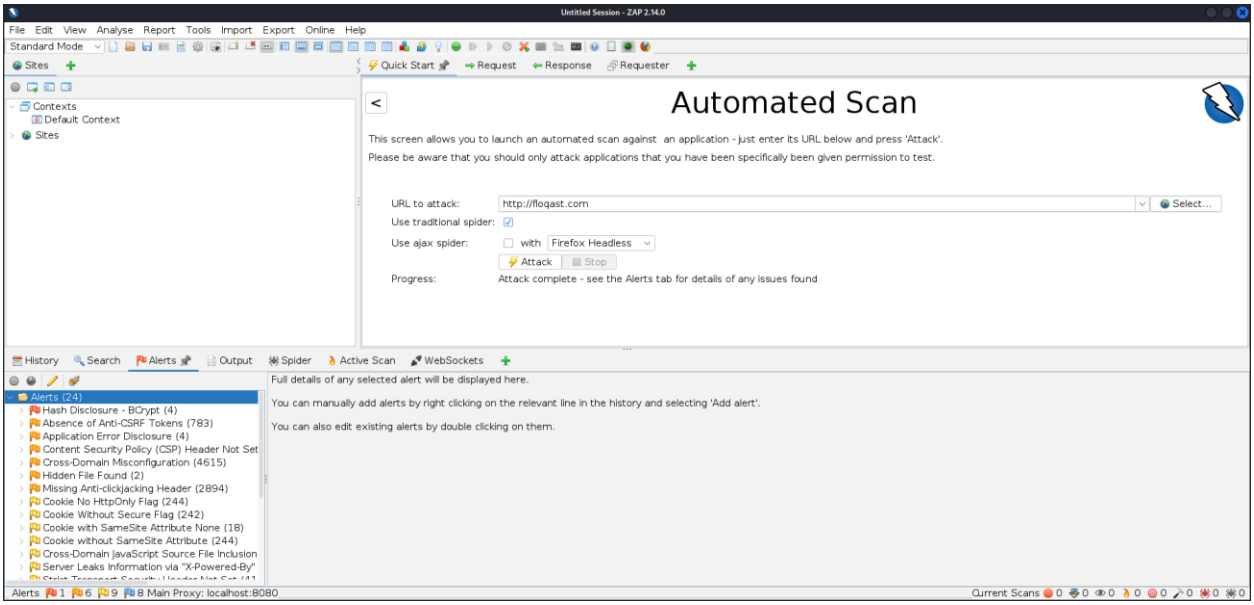


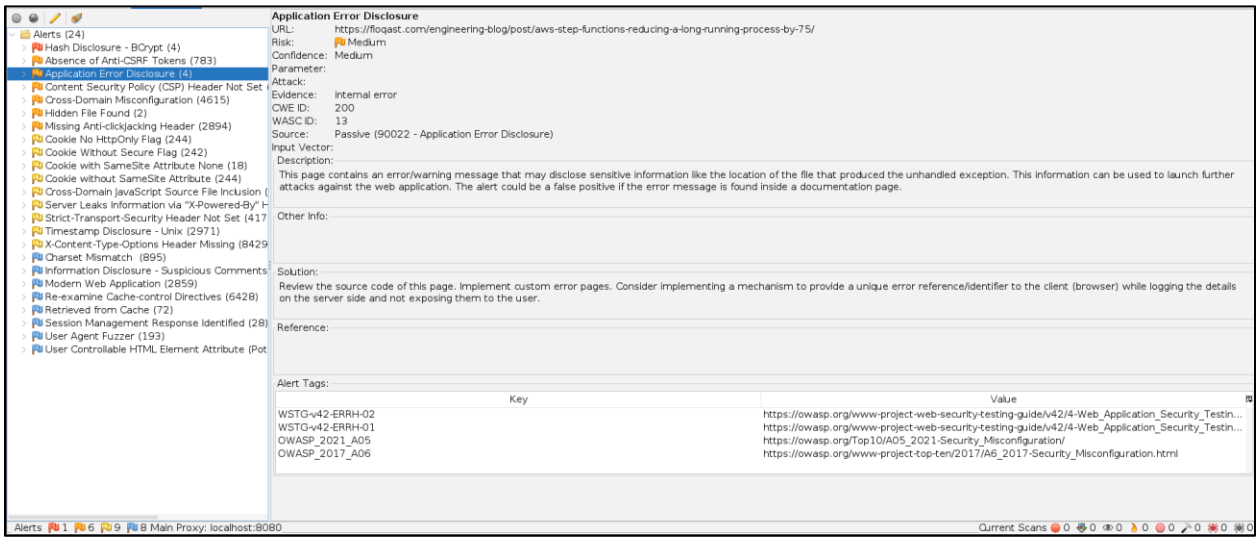
FloQast is an accounting software vendor based in Los Angeles, California. Founded in 2013

Scope

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
***.eu.floqast.app** All domains for FloQast's Core Application for European Customers Amazon Web Services JavaScript MongoDB Node.js React	Wildcard	In scope	Critical	Eligible	May 15, 2023	0 (0%)
api-eu.floqast.app Public API for FloQast's Core Application for European Customers	Domain	In scope	Critical	Eligible	Mar 22, 2023	0 (0%)
***.floqast.app** All domains for FloQast's Core Application for US Customers Amazon Web Services JavaScript MongoDB Node.js React	Wildcard	In scope	Critical	Eligible	May 15, 2023	0 (0%)
***.floqast.com** FloQast's Marketing Website	Wildcard	Out of scope	None	Ineligible	May 15, 2023	0 (0%)
***.floqast.studio** FloQast's Marketing Website for our Digital Entertainment Division	Wildcard	Out of scope	None	Ineligible	May 15, 2023	0 (0%)
Any Asset Not Specifically Listed as In-Scope Any domain, device, or asset not specifically listed as "In-Scope" for this program.	Other	Out of scope	None	Ineligible	Mar 22, 2023	0 (0%)

Scanning with Zap





Identified Vulnerabilities

1.Hash Disclosure in Bcrypt

Risk level - High

What is Hash Disclosure in Bcrypt:

Hash disclosure in bcrypt refers to the unintentional exposure or leakage of bcrypt-hashed passwords or sensitive data. Bcrypt is a cryptographic hashing function known for its strength against brute-force attacks and rainbow table attacks due to its computational intensity.

Impact

- Password Cracking: Exposed bcrypt-hashed passwords can be subjected to cracking attempts, including dictionary attacks and brute-force methods.
- Credential Stuffing: Attackers may use leaked bcrypt-hashed passwords in credential stuffing attacks, exploiting password reuse across multiple platforms.
- Account Takeover: Successful cracking of bcrypt-hashed passwords can lead to unauthorized access to user accounts, enabling attackers to impersonate users and access sensitive information.

Remedy:

- Salting: Always use unique salts for each password hash to mitigate the effectiveness of rainbow table attacks.
- Secure Storage: Store bcrypt-hashed passwords securely with strict access controls and encryption to prevent unauthorized access.
- Hashing Iterations: Configure bcrypt with an appropriate number of iterations to balance security and performance.

2.Application Error Disclosure

Risk Level - Medium

What is Application Error Disclosure?

Application Error Disclosure happens when an application accidentally reveals sensitive details, like internal workings or infrastructure, due to errors or misconfigurations.

Impact

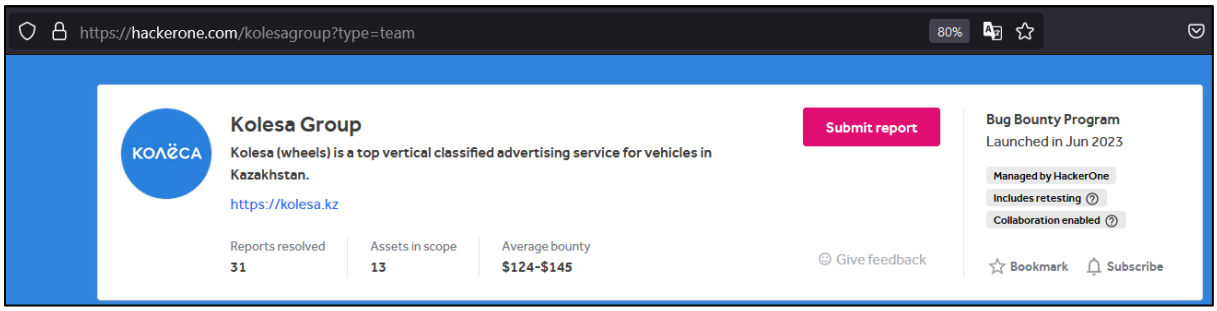
- Information Leakage: Attackers can gather valuable insights about the application's setup, potentially exploiting vulnerabilities.
- Security Risks: It increases the risk of targeted attacks or exploitation.
- Data Exposure: Sensitive user data might be revealed, leading to privacy breaches and compliance issues.

Remedy:

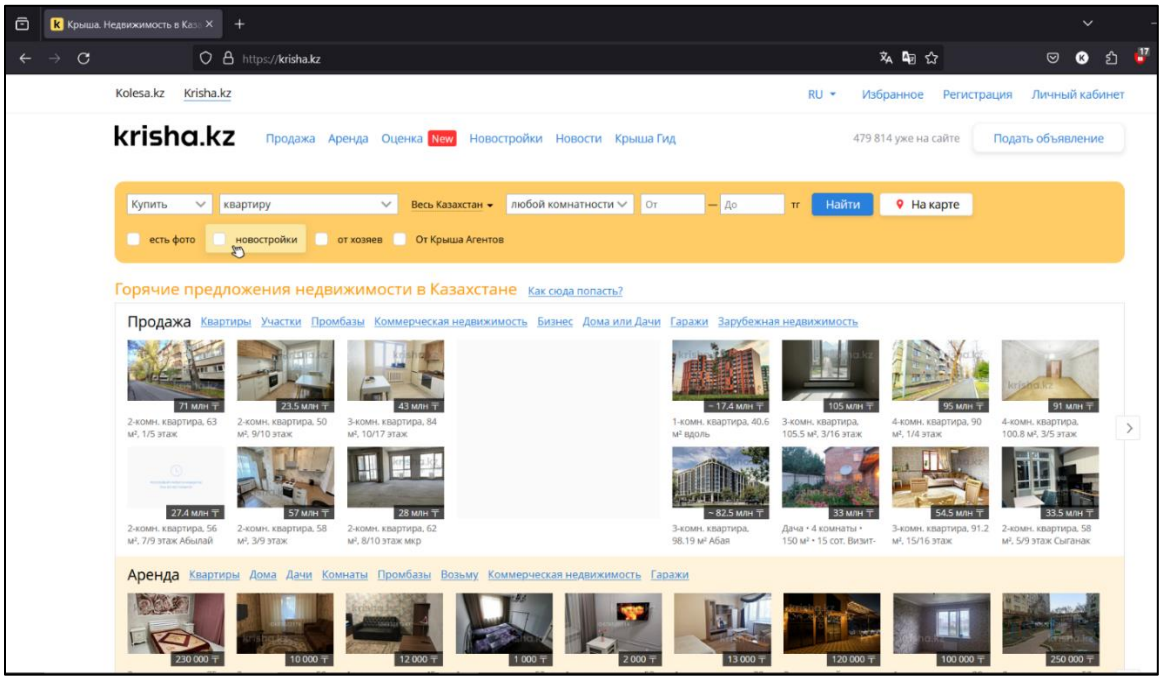
- Custom Error Pages: Developerts can Use generic error messages to users while hiding sensitive information.
- Error Logging and Monitoring: Track and analyze errors, ensuring logs are securely stored and reviewed regularly.
- Input Validation: Validate and sanitize user input to prevent attacks triggering error disclosures.

- ❖ Security Headers: Utilize security headers to enhance application security.
- ❖ Secure Configuration: Review and secure application settings to avoid inadvertent exposure of sensitive information.

6.Koelsa group (Report 6)



Addressing the target



Krisha.kz is a real estate advertising website based on Kazakhstan. There are more than 300,000 current real estate ads. Including apartments, houses, cottages, villas, as well as commercial real estate for every taste, from office to shop.

Scope

In scope

Asset name	Type	Coverage	Max. severity	Bounty	Last update
965180355	iOS: App Store	In scope	Critical	Eligible	Jun 19, 2023
563291345 Any other subdomains under this domain are not in scope ineligible for submission	iOS: App Store	In scope	Critical	Eligible	Nov 17, 2022
kz.kolesa Any other subdomains under this domain are not in scope and ineligible for submission	Android: .apk	In scope	Critical	Eligible	Nov 17, 2022
kolesa.kz Any other subdomains under this domain are not in scope and ineligible for submission	Domain	In scope	Critical	Eligible	Nov 17, 2022
id.kolesa.kz	Domain	In scope	Critical	Eligible	Jun 1, 2023
m.krisha.kz	Domain	In scope	Critical	Eligible	Jun 19, 2023
app.krisha.kz	Domain	In scope	Critical	Eligible	Jun 19, 2023
m.kolesa.kz Any other subdomains under this domain are not in scope and ineligible for submission	Domain	In scope	Critical	Eligible	Nov 17, 2022
api.kolesa.kz	Domain	In scope	Critical	Eligible	Jun 1, 2023
kz.krisha	Android: .apk	In scope	Critical	Eligible	Jul 10, 2023
krisha.kz	Domain	In scope	Critical	Eligible	Jun 19, 2023
api.krisha.kz	Domain	In scope	Critical	Eligible	Jun 19, 2023
app.kolesa.kz	Domain	In scope	Critical	Eligible	Jun 1, 2023

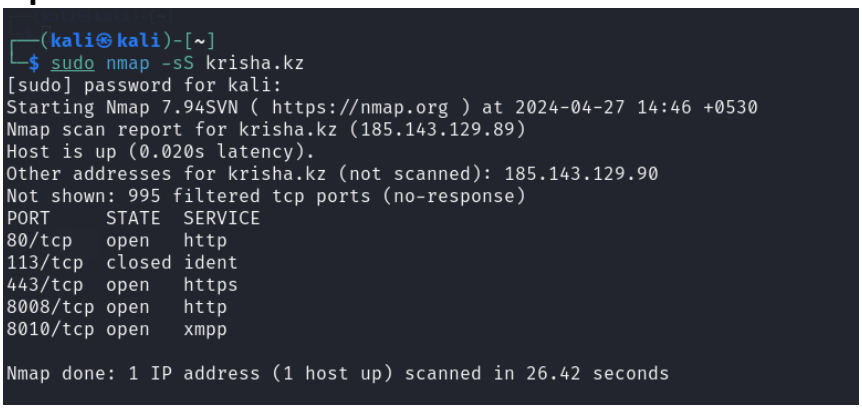
Out of scope

avtoelon.uz	Domain	Out of scope	None	Ineligible	Updated	Apr 10, 2024
api.avtoelon.uz	Domain	Out of scope	None	Ineligible	Updated	Apr 10, 2024
m.avtoelon.uz	Domain	Out of scope	None	Ineligible	Updated	Apr 10, 2024
1431768824	iOS: App Store	Out of scope	None	Ineligible	Updated	Apr 10, 2024
uz.avtoelon	Android: .apk	Out of scope	None	Ineligible	Updated	Apr 10, 2024
id.avtoelon.uz	Domain	Out of scope	None	Ineligible	Updated	Apr 12, 2024
app.avtoelon.uz	Domain	Out of scope	None	Ineligible	Updated	Apr 12, 2024

Subdomain enumeration with subfinder

With subfinder I was able to find 18 subdomains.

Open Ports

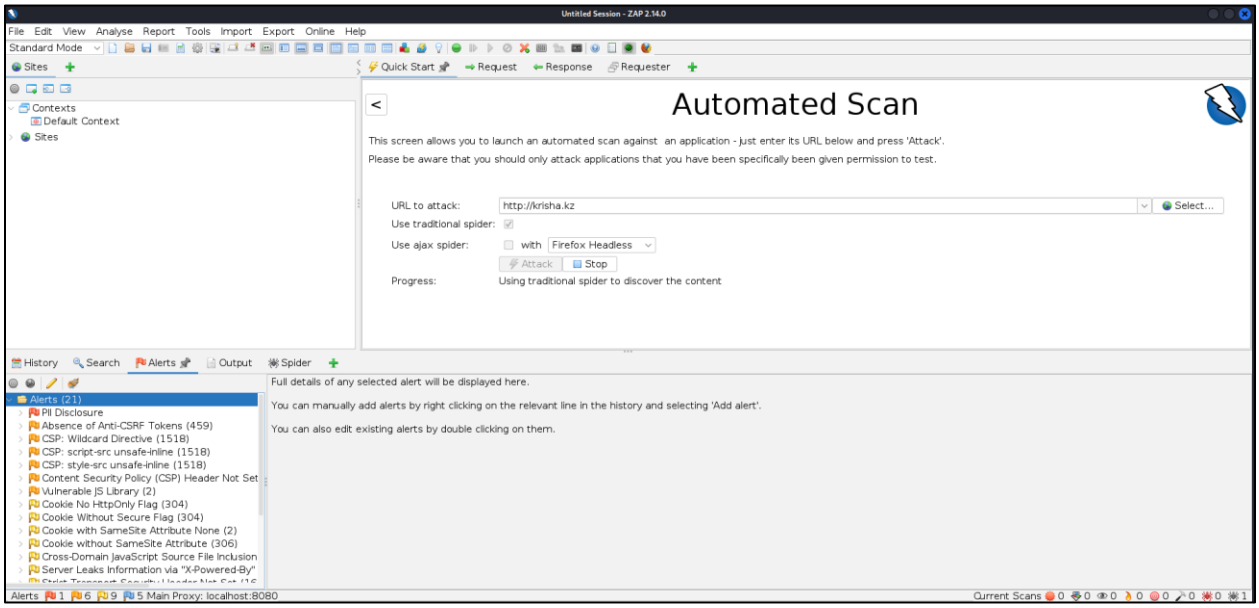


As of the Nmap scan port 80,113,443,8008 and 8010 appears to be open.

Selected domain – Krisha.kz

Scanning with Nikto

Scanning with Zap



Identified Vulnerabilities

1.Absence of Anti CSRF Tokens

Risk level - Medium

What is absence of anti CSRF tokens?

The absence of Anti-CSRF (Cross-Site Request Forgery) tokens refers to a vulnerability in web applications where they lack protection mechanisms against CSRF attacks. CSRF attacks occur when an attacker tricks a user into unknowingly executing actions on a web application in which the user is authenticated. These attacks can result in unauthorized actions being performed on behalf of the user without the user knowing about it.

Impact

CSRF attacks can lead to unauthorized actions being performed on behalf of the user, such as changing account settings, making purchases, or deleting data. By including Anti-CSRF tokens in an application, we can be protected against CSRF attacks by ensuring that requests are only accepted if they include a valid token that is generated and verified by the server-side code.

Remedy

To mitigate the risk of CSRF attacks, web developers should implement Anti-CSRF tokens as part of their security measures, ensuring that each request made to the server includes a valid token that can be verified to confirm the legitimacy of the request.

2.CSP Wildcard Directive

Risk level – Medium

What is CSP Wildcard Directive?

The Content Security Policy (CSP) wildcard directive (*) is used to allow or restrict content from any origin. When the wildcard is used in a CSP header, it means that the specified policy applies to all origins, including those that are not explicitly defined in the policy.

Impact

The impact of CSP Wildcard Directive can be significant. Here are some of the things that could happen.

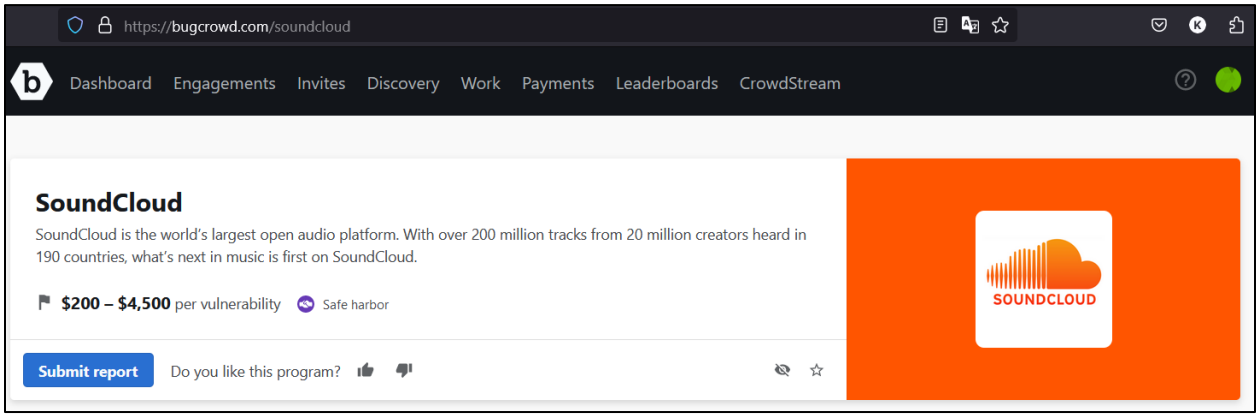
- Increased Attack Surface: When open to content from any location it can add to the number of potential attack vectors of your site.
- Bypassing CSP Protections: The harasser might utilize the strategy to get out of CSP safeguards.
- Data Leakage: It might be the case that if resources are allowed from different origins, then there is a possibility of unauthorized data dissemination.

Remedy

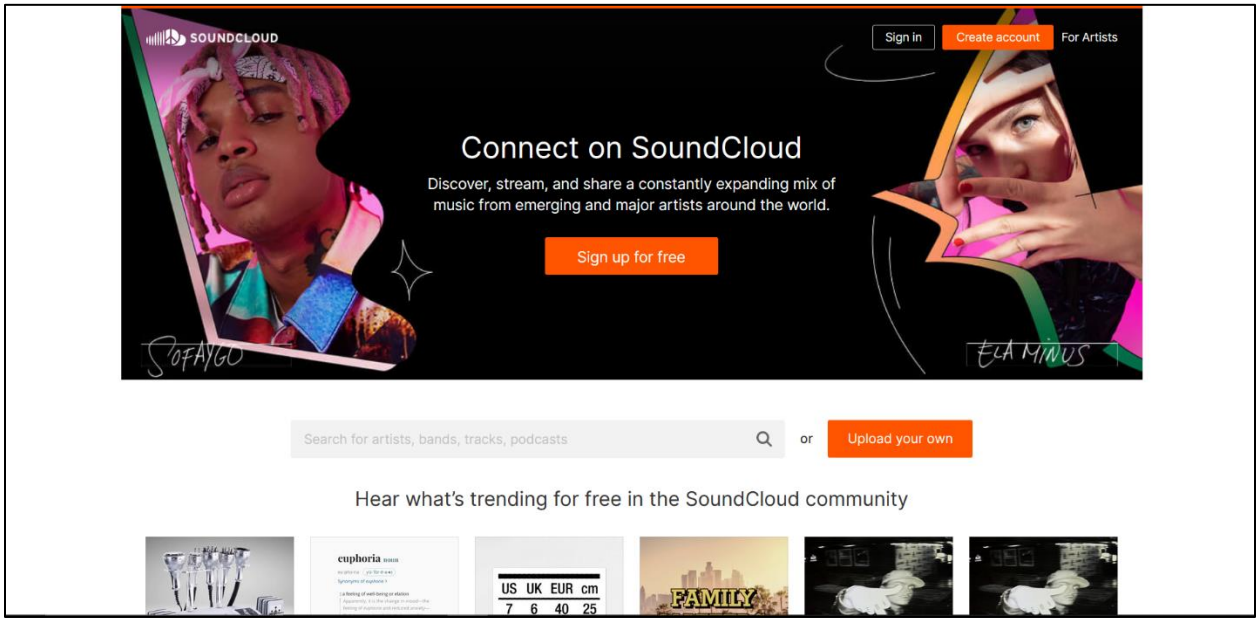
To prevent the negative impact of using the wildcard directive in CSP,following steps can be taken

- Avoid Using the Wildcard Directive: Point to exact locations on the map in stead of using asterisk marker.
- Use Nonce or Hash-Based CSP: Implement nonce or hash-based Projected Code Protection to control the script execution.
- Regularly Review and Update CSP Policies: Check and do not put overwriting policies and get rid of wildcard directives.

7.Soundcloud (Report 7)

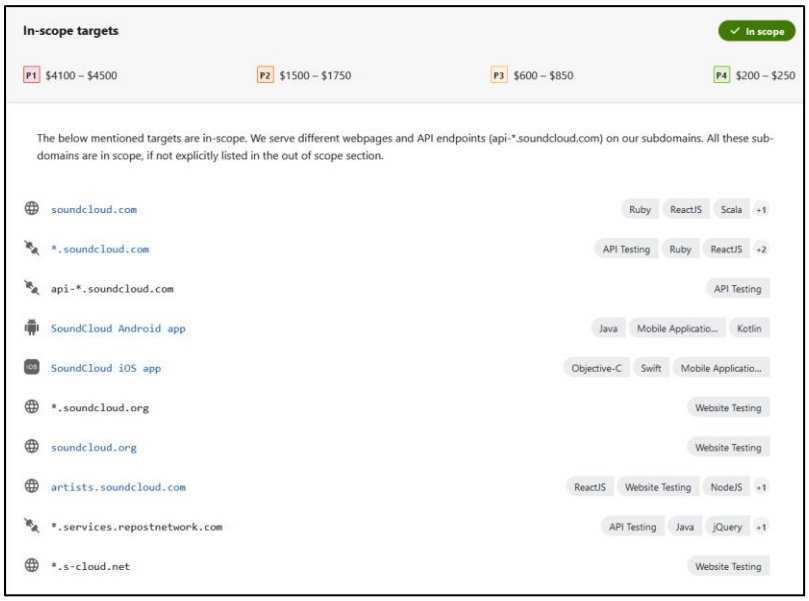


Addressing the target



Founded in 2007, SoundCloud is a German audio streaming service owned and operated by SoundCloud Global Limited & Co. KG. SoundCloud is an artist-first platform powered by a global community of artists and listeners on the pulse of what's new, now and next in music cultureWith over 250 million tracks from 30 million artists from 193 countries on SoundCloud, Soundcloud is one of the largest audio discovery platform in the world.

Scope



Searching for subdomains with sublist3r

```
[-] Total Unique Subdomains Found: 123
www.soundcloud.com
2021playback.soundcloud.com
links.account.soundcloud.com
www.links.account.soundcloud.com
acmetest.soundcloud.com
www.acmetest.soundcloud.com
adidasoriginals5to9.soundcloud.com
links.announcements.soundcloud.com
www.links.announcements.soundcloud.com
api.soundcloud.com
api-partners.soundcloud.com
artist.soundcloud.com
artists.soundcloud.com
axethelabel.soundcloud.com
axethelabelrules.soundcloud.com
backstage.soundcloud.com
links.billing.soundcloud.com
www.links.billing.soundcloud.com
blog.soundcloud.com
campbellssoundsgoodtonight.soundcloud.com
www.campbellssoundsgoodtonight.soundcloud.com
careers.soundcloud.com
checkout.soundcloud.com
community.soundcloud.com
links.confirmation.soundcloud.com
www.links.confirmation.soundcloud.com
contest.soundcloud.com
copyright.soundcloud.com
creator-services.soundcloud.com
```

Selected domain – soundcloud.com

Open Ports

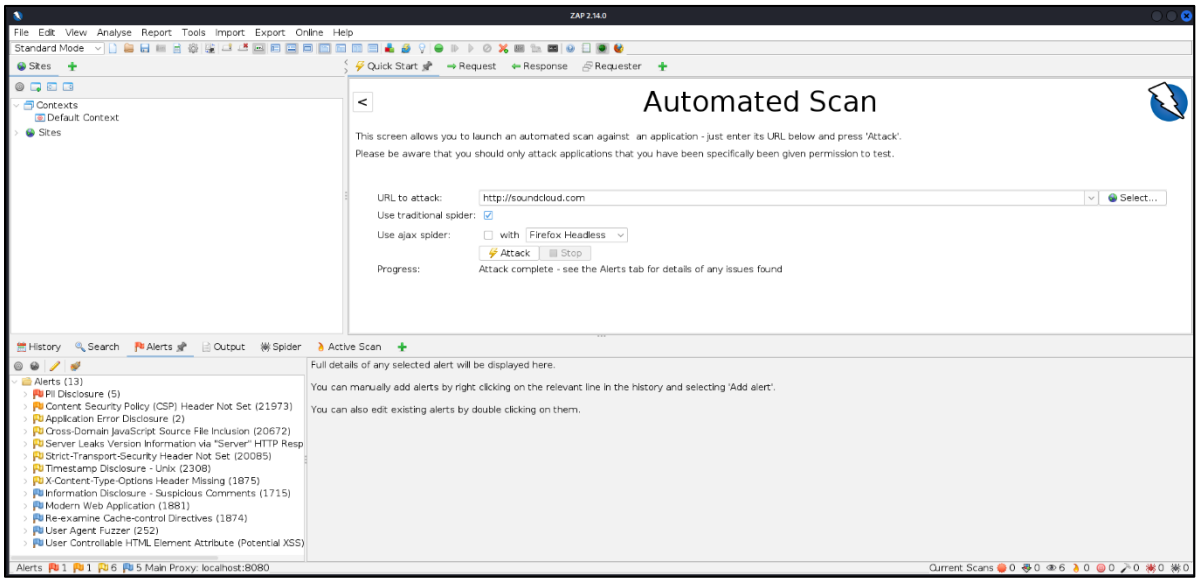
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS soundcloud.com
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-27 14:58 +0530
Nmap scan report for soundcloud.com (13.33.88.80)
Host is up (0.012s latency).
Other addresses for soundcloud.com (not scanned): 13.33.88.55 13.33.88.85 13.33.88.75
rDNS record for 13.33.88.80: server-13-33-88-80.sin2.r.cloudfront.net
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8008/tcp open  http
8010/tcp open  xmpp

Nmap done: 1 IP address (1 host up) scanned in 5.36 seconds
```

With the nmap scan it appears that ports 80,443,8008 and 8010 are open.

Scanning with Nikto

```
┌──(kali㉿kali)-[~]
└─$ sudo nikto -h soundcloud.com
[sudo] password for kali:
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 13.33.88.55, 13.33.88.85, 13.33.88.75, 13.33.88.80
+ Target IP:          13.33.88.55
+ Target Hostname:    soundcloud.com
+ Target Port:        80
+ Start Time:         2024-04-18 13:11:23 (GMT5.5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ /: Retrieved via header: 1.1 6ddfc55dbf10d9a646bfcdba6cd89472.cloudfront.net (CloudFront).
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com
sing-content-type-header/
+ Root page / redirects to: https://soundcloud.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
-C all- STATUS: Completed 340 requests (~5% complete, 33.7 minutes left): currently in plugin 'Site Files'
- STATUS: Running average: 100 requests: 0.26033 sec, 10 requests: 0.2700 sec.

+ /wsman/: Windows Remote Management is enabled.
+ 7964 requests: 2 error(s) and 4 item(s) reported on remote host
+ End Time:           2024-04-18 13:30:18 (GMT5.5) (1135 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Scanning with zap



Identified Vulnerabilites

1.PII Disclosure

Risk Level - High

PII stands in for Personally Identifiable Information, which stands for any information that may be able to pinpoint one person. It can covers a person's name, postal address, phone and cell numbers, email addresses, social security number and the like. PII leakage happens when this highly sensitive information is exposed without permission.

Impact

The impact of PII disclosure can be significant, both for individuals and for the organizations responsible for safeguarding their information. There can be some bad outcomes of PII disclosure.

- Identity Theft: Disclosure of PII creates an opportunity for identity theft to occur, in which criminals acquire personal data which they then use to impersonate unsuspecting victims by making fraudulent purchases or opening new credit accounts in the victim's name all under pretense of that identity.
- Financial Loss: Identity fraud and fraudster activities jeopardize the individual's wealth accumulation efforts by as well harming the credit score and financial reputation. Therefore, it can serve as a legal basis for the imposing of penalties and regulatory fines on organizations who fail to appropriately safeguard PII.
- Privacy Violations: Complete disclosure of personal information raises the issue of an individual's privacy rights as they can possibility go far beyond of just being intrusive into their personal lives, risking even their reputation or safety.
- Loss of Trust: Organizations that suffer at the hands of a PII exposure may experience serious reputation damage and a loss of trust from their major customers, partners and stockholders. The effects of such reputation damage may span over the long term and become obstacles to their business operations.

Remedy

To prevent PII disclosure, organizations can take several proactive measures.

- Data Encryption: Using either the 'encryption in transit' or 'encryption at rest' on confidential information enhances the security of the data by prohibiting any unauthorized access even if the data has been intercepted and compromised.
- Access Controls: The application of a tight access control and authentication methods will guarantee that a privilege is given to just official individuals in the disclosure of the

PII; this puts a limit on the inside threats, the unauthorized exposure, and the misuse of the data.

- Data Minimization: Keep and delete only Personal Identifiable Information (PII) needed for business purposes and dispose of it securely after the time it is not needed.

2.CSP Header Not Set

Risk level – Medium

What is CSP Header not set?

Content Security Policy (CSP) adds a layer of security which helps to detect and mitigate certain types of attacks such as Cross Site Scripting (XSS) and data injection attacks. attackers use XSS attacks to trick trusted websites into delivering malicious content. The browser executes all code from trusted origin and can't differentiate between legitimate and malicious code, so any injected code is executed in that process.

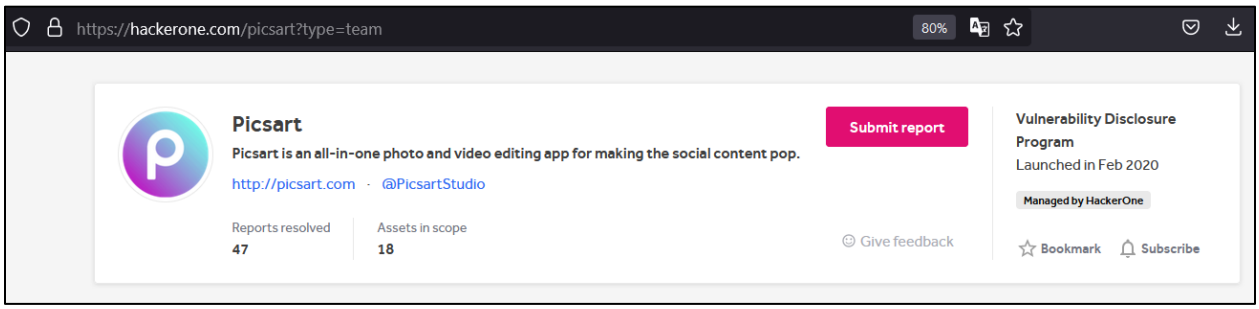
Impact

- XSS Attacks: Without CSP, malicious scripts can be injected into a webpage, leading to the execution of unauthorized code in the context of the website.
- Data Injection: Attackers can inject malicious content or modify the page's content, potentially compromising user data or the integrity of the website.
- Clickjacking: Without proper CSP, attackers can frame a website within a malicious page, tricking users into performing unintended actions.

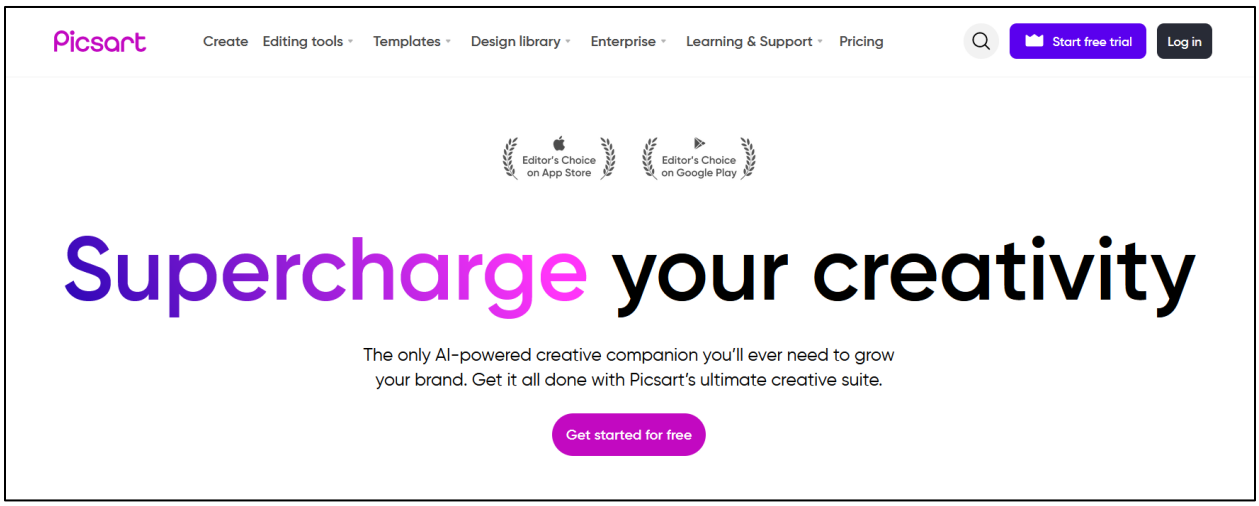
Remedy

- Set CSP Headers: Ensure your server includes CSP headers in HTTP responses, outlining browser policy directions.
- Define Content Sources: Specify allowed domains using CSP directives like default-src, script-src, style-src, img-src, etc., restricting resource loading to these domains.
- Use Nonces and Hashes: Employ CSP nonces or hashes to permit inline script and style execution while maintaining security.
- Regular Audits and Testing: Regularly audit and test CSP configuration to ensure protection against attacks and avoid blocking legitimate content.
- Consider Browser Compatibility: Account for browser compatibility when crafting CSP headers, as certain directives may not function consistently across all browser.

8.Picsart (Report 8)



Addressing the target



PicsArt.com is the official website of PicsArt, where users can access various features and services offered by the platform. On the website, users can create a PicsArt account, explore tutorials and tips for using the app, access the PicsArt blog for creative inspiration, and discover featured artists and their work. Additionally, PicsArt.com serves as a hub for community engagement, allowing users to participate in challenges, contests, and discussions related to photo editing and digital art. Overall, it's a central online destination for all things related to PicsArt and its vibrant creative community.

Scope

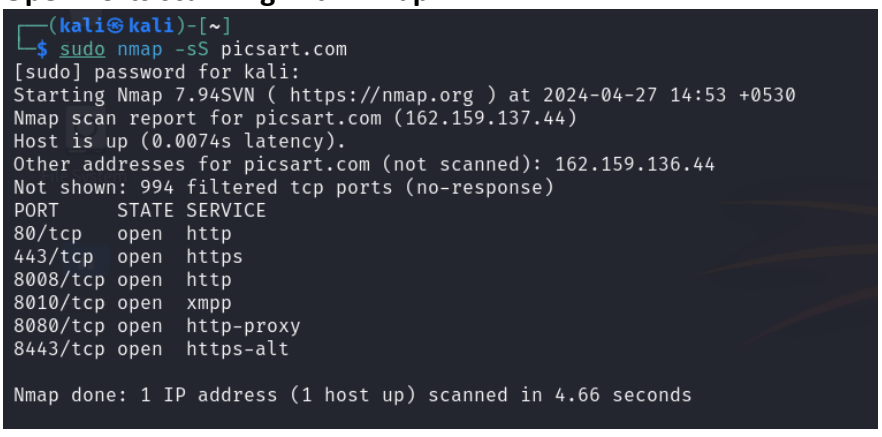
Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
content-discovery.picsart.io	Domain	In scope	Critical	Ineligible	Aug 23, 2023	0 (0%)
video-api.picsart.io	Domain	In scope	Critical	Ineligible	Aug 23, 2023	0 (0%)
revenue-tracking.picsart.io	Domain	In scope	Critical	Ineligible	Aug 23, 2023	0 (0%)
demo.sdk.picsart.io	Domain	In scope	Critical	Ineligible	Aug 23, 2023	0 (0%)
cdn-basic-content-api.picsart.io	Domain	In scope	Critical	Ineligible	Aug 23, 2023	0 (0%)
t.picsart.com	Domain	In scope	Critical	Ineligible	Aug 23, 2023	0 (0%)
stage.optifyr.com	Domain	In scope	Critical	Ineligible	Aug 23, 2023	0 (0%)
optifyr.com	Domain	In scope	Critical	Ineligible	Aug 23, 2023	0 (0%)
upload.picsart.com	Domain	In scope	Critical	Ineligible	Aug 23, 2023	0 (0%)
console.picsart.io	Domain	In scope	Critical	Ineligible	Aug 23, 2023	0 (0%)
api.picsart.io	Domain	In scope	Critical	Ineligible	Jun 10, 2022	0 (0%)
9WZDNCRFJ10M	Windows: Microsoft Store	In scope	Critical	Ineligible	Jun 10, 2022	0 (0%)
587366035	iOS: App Store	In scope	Critical	Ineligible	Feb 17, 2020	0 (0%)
ai.picsart.com	Domain	In scope	Critical	Ineligible	Aug 17, 2023	0 (0%)
picsart.io	Domain	In scope	Critical	Ineligible	Aug 29, 2022	0 (0%)
www.picsart.com	Domain	In scope	Critical	Ineligible	Jun 23, 2021	0 (0%)
api.picsart.com	Domain	In scope	Critical	Ineligible	Aug 23, 2023	0 (0%)
com.picsart.studio	Android: Play Store	In scope	Critical	Ineligible	Feb 17, 2020	0 (0%)

Subdomain hunting with Sublist3r

With sublist3r I was able to find 9 unique subdomains.

Selected domain - picsart.com

Open Ports scanning with Nmap

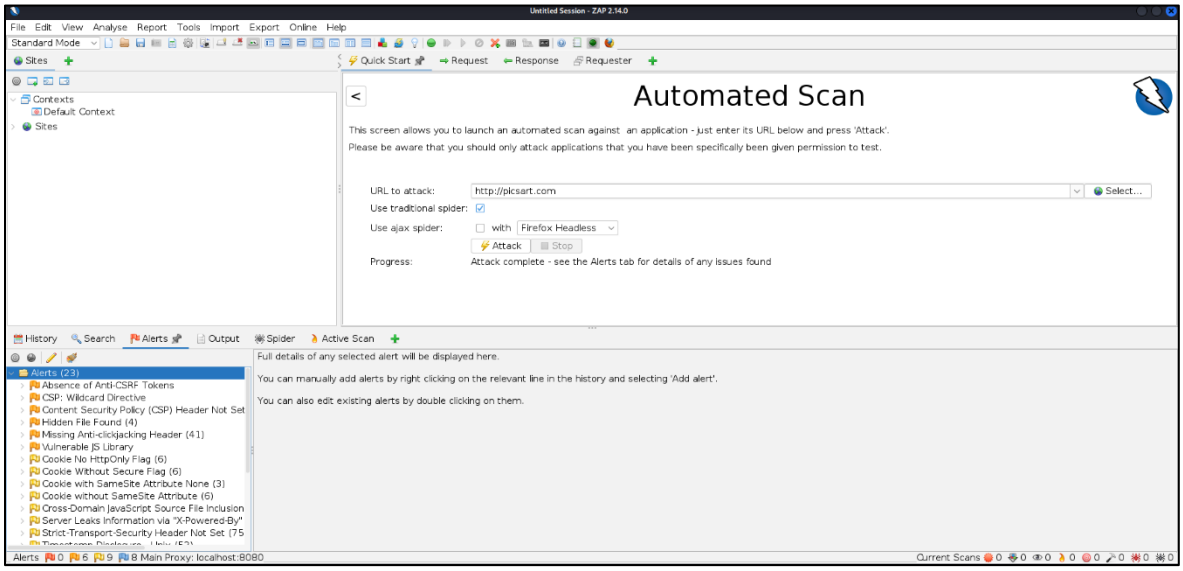


Port 80,443,8008.8010,8080,8443 Was open according to Nmap

Scanning with Nikto

```
┌──(kali㉿kali)-[~]
└─$ sudo nikto -h picsart.com
[sudo] password for kali:
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 162.159.137.44, 162.159.136.44
+ Target IP:          162.159.137.44
+ Target Hostname:    picsart.com
+ Target Port:        80
+ Start Time:         2024-04-23 21:57:40 (GMT5.5)
---------------------------------------------------------------------------
+ Server: cloudflare
+ /: IP address found in the '__cf_bm' cookie. The IP is "1.0.1.1".
+ /: IP address found in the 'set-cookie' header. The IP is "1.0.1.1". See: https://portswigger.net/kb/issues/00600300_private-ip-addresses-disclosed
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Drupal Link header found with value: <https://optifyr.com>; rel="preconnect". See: https://www.drupal.org/
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com
/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: https://picsart.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
-C all
- STATUS: Completed 7520 requests: currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.10043 sec, 10 requests: 0.1014 sec.
+ /cdn-cgi/trace: Retrieved access-control-allow-origin header: *.
+ /cdn-cgi/trace: Cloudflare trace CGI found, which may leak some system information.
+ 7962 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2024-04-23 22:10:53 (GMT5.5) (793 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Scanning with Zap



Identified Vulnerabilites

1.CSP Header Not Set

Risk level – Medium

What is CSP Header not Set?

Content Security Policy (CSP) adds a layer of security which helps to detect and mitigate certain types of attacks such as Cross Site Scripting (XSS) and data injection attacks. attackers use XSS attacks to trick trusted websites into delivering malicious content. The browser executes all code from trusted origin and can't differentiate between legitimate and malicious code, so any injected code is executed in that process.

Impact

- XSS Attacks: Without CSP, malicious scripts can be injected into a webpage, leading to the execution of unauthorized code in the context of the website.
- Data Injection: Attackers can inject malicious content or modify the page's content, potentially compromising user data or the integrity of the website.
- Clickjacking: Without proper CSP, attackers can frame a website within a malicious page, tricking users into performing unintended actions.

Remedy

- Set CSP Headers: Ensure your server includes CSP headers in HTTP responses, outlining browser policy directions.
- Define Content Sources: Specify allowed domains using CSP directives like default-src, script-src, style-src, img-src, etc., restricting resource loading to these domains.
- Use Nonces and Hashes: Employ CSP nonces or hashes to permit inline script and style execution while maintaining security.
- Regular Audits and Testing: Regularly audit and test CSP configuration to ensure protection against attacks and avoid blocking legitimate content.
- Consider Browser Compatibility: Account for browser compatibility when crafting CSP headers, as certain directives may not function consistently across all browsers.

2.Missing Anti Clickjacking Header

Risk level - Medium

What is Missing Anti-clickjacking header?

The absence of an anti-clickjacking header refers to a security vulnerability where web applications fail to include headers such as X-Frame-Options or Content-Security-Policy to prevent clickjacking attacks. Clickjacking is a malicious technique where an attacker tricks a user into clicking on something different from what the user perceives, potentially leading to unintended actions or information disclosure.

Impact

With the anti-clickjacking header missing that can be impactful on many ways.

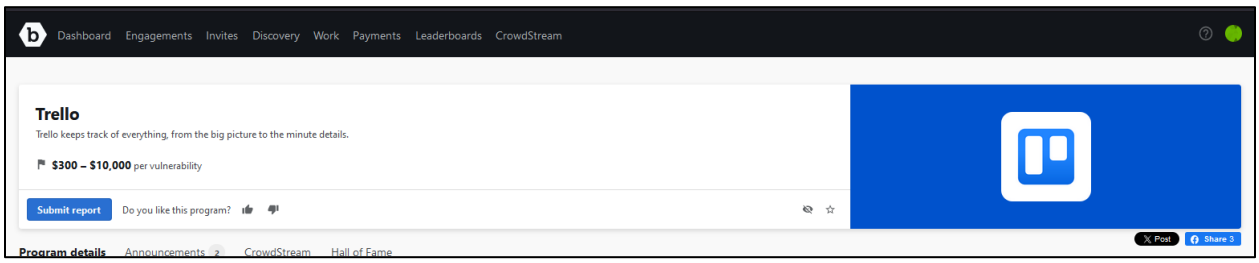
- Security Risks: Without anti-clickjacking headers, websites cannot avoid clickjacking attacks, which means that legitimate webpages may have layers of harmful material between them and their visitors.
- Data Exposure: An example of clickjacking is exposing the user to the risk of accidental divulgence of private data or the execution of any action that the user did not intend.
- Reputation Damage: A clickjacking attack can fool users into clicking on the malicious links which being classified as bait URLs can eventually break their trust towards the website or application.

Remedy

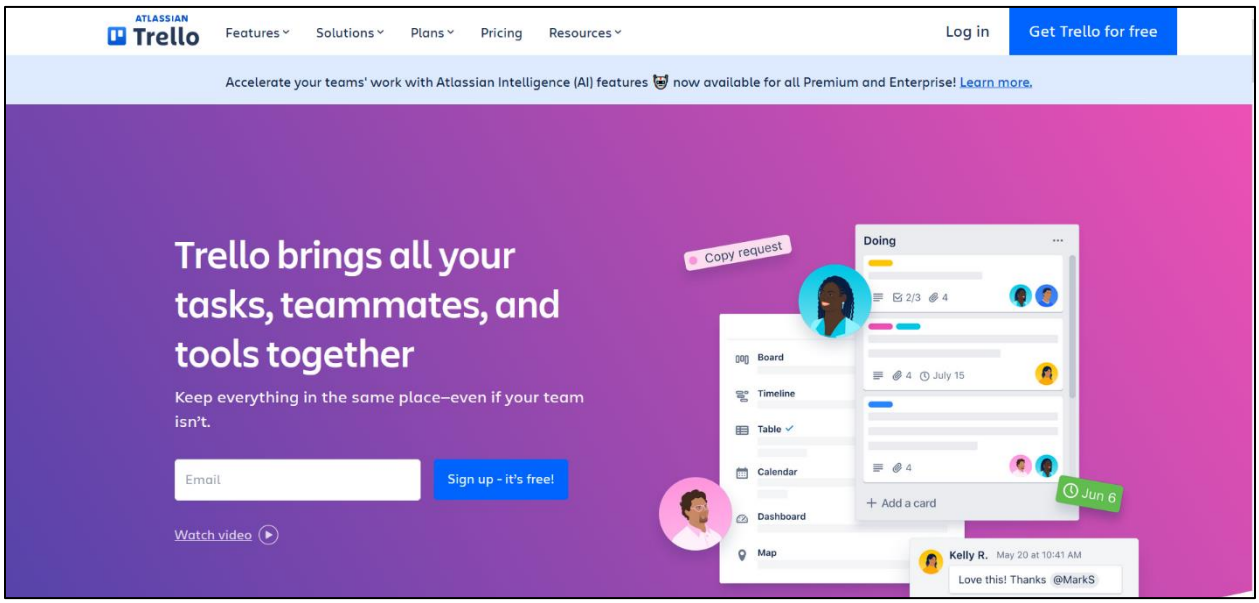
To prevent Attackers from exploiting “Missing anti clickjacking header” there are some steps that can be followed.

- Implement X-Frame-Options: By setting the X-Frame-Options header with values like "DENY" or "SAMEORIGIN", you can control the content areas of your website where iframes are allowed to be embedded without your control.
- Use Content-Security-Policy (CSP): Write down a policy that will limit the internal resources that can be loaded by a web page, including frame-ancestors directives that will determine the allowed pages for framing.
- Regular Security Audits: Run regular audits to make certain that all the anti-clickjacking headers have been implemented correctly and are set up properly.

9.Trello (Report 9)



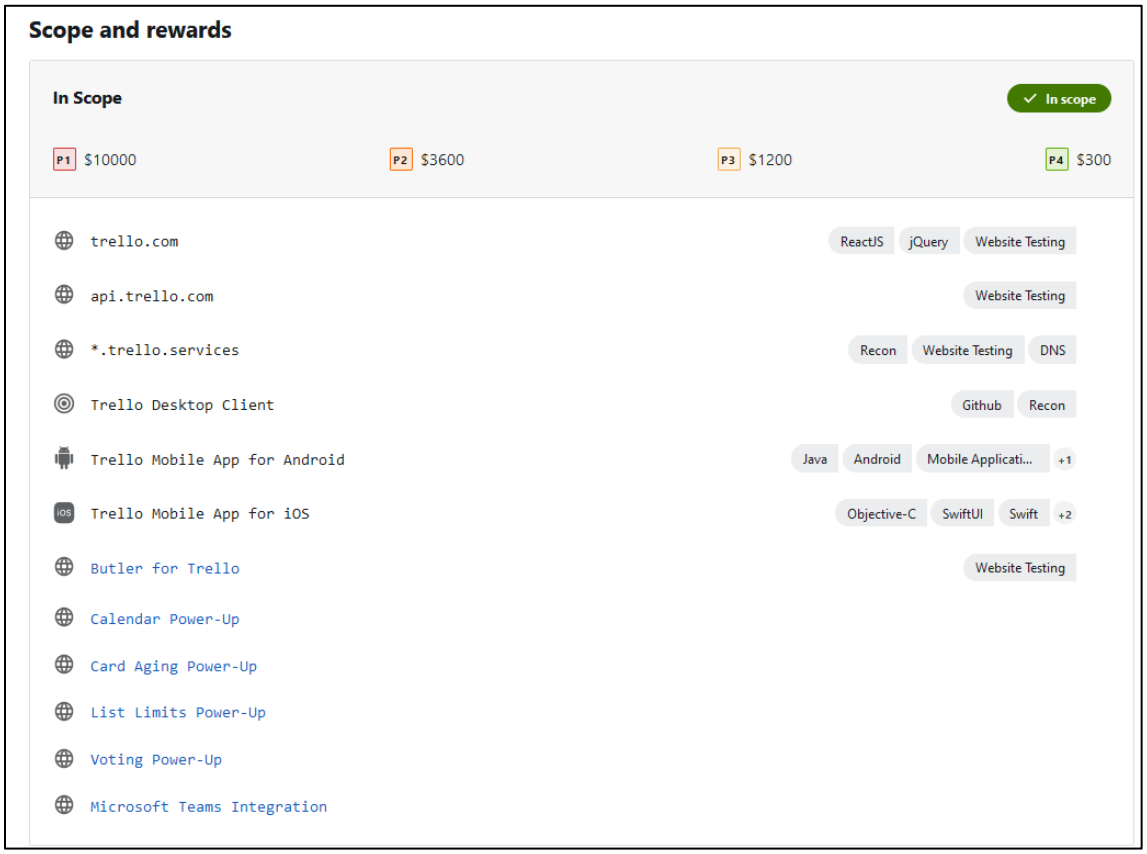
Addressing the target



Trello is a web-based project management application that utilizes boards, lists, and cards to help teams organize and prioritize their tasks and projects in a visually intuitive way. Users can create boards for different projects, then within each board, they can create lists to represent stages or categories, and within those lists, they can create cards for individual tasks or items.

Scope

In Scope



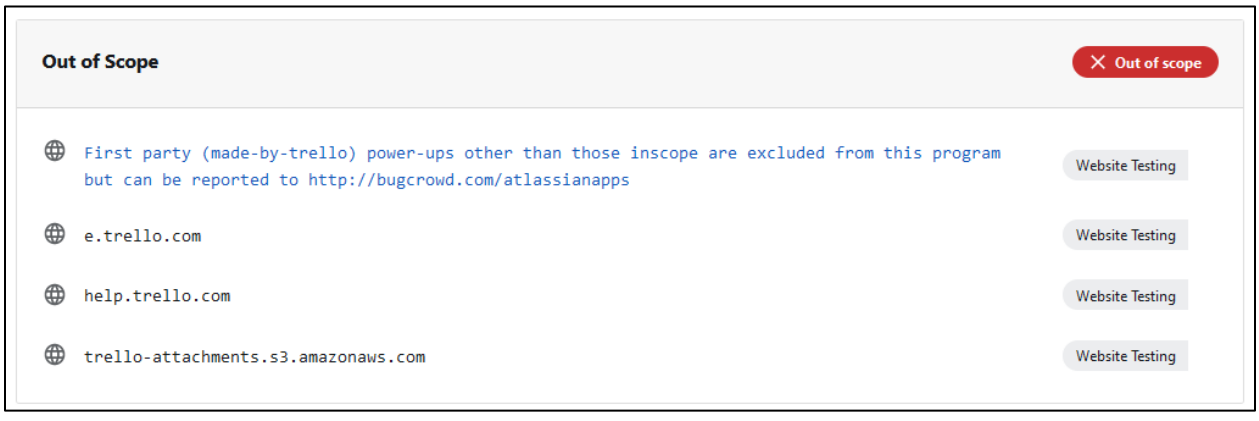
Scope and rewards

In Scope — ✓ In scope

P1 $10000 | P2 $3600 | P3 $1200 | P4 $300

trello.com	ReactJS, jQuery	Website Testing
api.trello.com		Website Testing
*.trello.services	Recon	Website Testing, DNS
Trello Desktop Client		Github, Recon
Trello Mobile App for Android	Java, Android	Mobile Applicati... +1
Trello Mobile App for iOS	Objective-C, SwiftUI, Swift	+2
Butler for Trello		Website Testing
Calendar Power-Up		
Card Aging Power-Up		
List Limits Power-Up		
Voting Power-Up		
Microsoft Teams Integration		

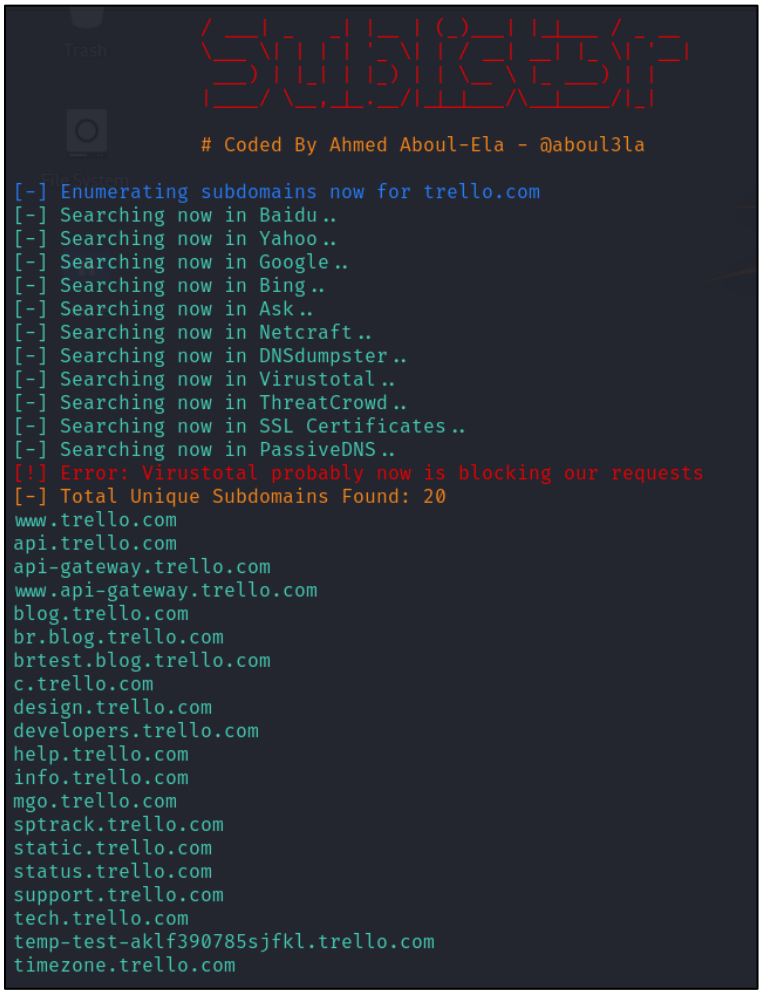
Out of Scope



Out of Scope — ✗ Out of scope

First party (made-by-trello) power-ups other than those inscope are excluded from this program but can be reported to http://bugcrowd.com/atlassianapps	Website Testing
e.trello.com	Website Testing
help.trello.com	Website Testing
trello-attachments.s3.amazonaws.com	Website Testing

Subdomain hunting with Sublist3r



Sublist3r was able to find 20 uniques sub domains.

Selceted - trello.com

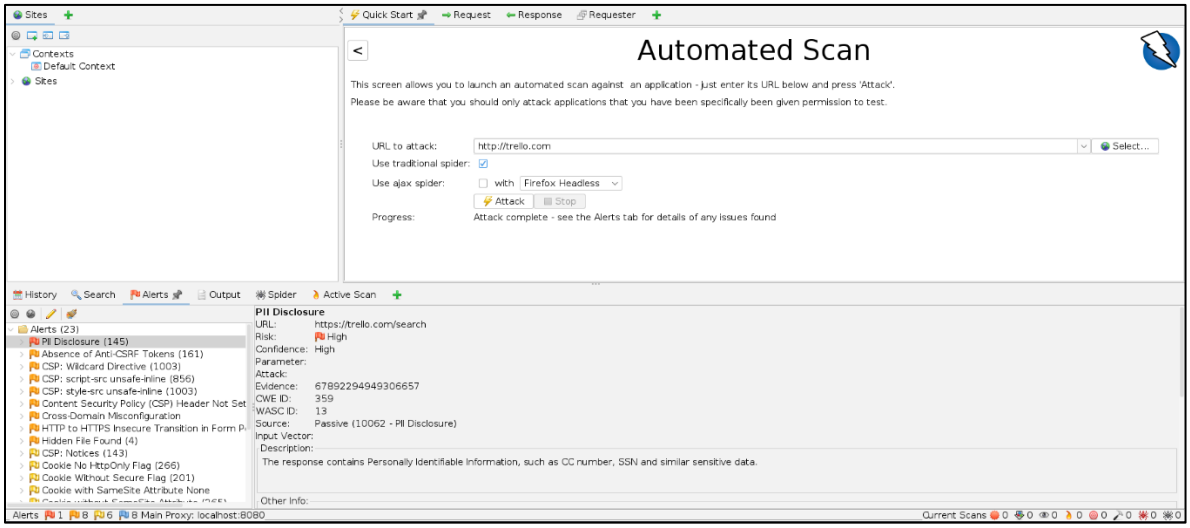
Scanning for open ports with Nmap

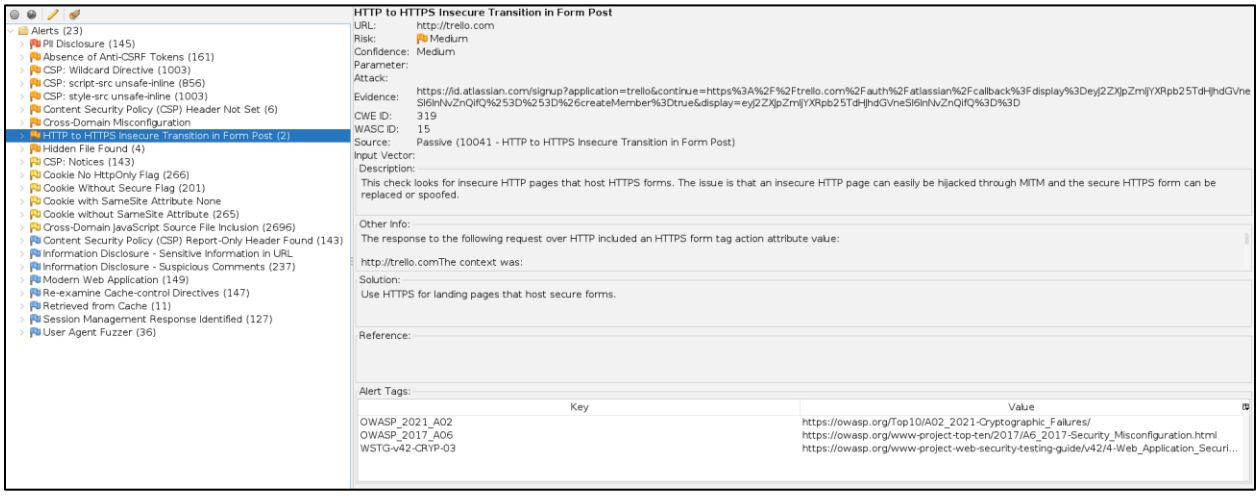
Ports 80,443,8008 and 8010 were open

Scanning with Nikto

```
┌──(kali㉿kali)-[~]
└─$ sudo nikto -h trello.com
[sudo] password for kali:
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 108.157.254.33, 108.157.254.93, 108.157.254.49, 108.157.254.128
+ Target IP:          108.157.254.33
+ Target Hostname:    trello.com
+ Target Port:        80
+ Start Time:         2024-04-23 22:41:05 (GMT5.5)
---------------------------------------------------------------------------
+ Server: CloudFront
+ /: Retrieved via header: 1.1 4fa95b89b64a0e774cf73023a2cbf232.cloudfront.net (CloudFront).
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com
/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: https://trello.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
-C all
- STATUS: Completed 4950 requests (~71% complete, 4.3 minutes left): currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.26073 sec, 10 requests: 0.2605 sec.
+ 7962 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:           2024-04-23 22:56:30 (GMT5.5) (925 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Scanning with Zap





Identified Vulnerabilites

1.PII Disclosure

Risk Level – High

What is PII Disclosure?

PII stands in for Personally Identifiable Information, which stands for any information that may be able to pinpoint one person. It can covers a person's name, postal address, phone and cell numbers, email addresses, social security number and the like. PII leakage happens when this highly sensitive information is exposed without permission.

Impact

The impact of PII disclosure can be significant, both for individuals and for the organizations responsible for safeguarding their information. There can be some bad outcomes of PII disclosure.

- Identity Theft: Disclosure of PII creates an opportunity for identity theft to occur, in which criminals acquire personal data which they then use to impersonate unsuspecting victims by making fraudulent purchases or opening new credit accounts in the victim's name all under pretense of that identity.
- Financial Loss: Identity fraud and fraudster activities jeopardize the individual's wealth accumulation efforts by as well harming the credit score and financial reputation. Therefore, it can serve as a legal basis for the imposing of penalties and regulatory fines on organizations who fail to appropriately safeguard PII.
- Privacy Violations: Complete disclosure of personal information raises the issue of an individual's privacy rights as they can possibility go far beyond of just being intrusive into their personal lives, risking even their reputation or safety.
- Loss of Trust: Organizations that suffer at the hands of a PII exposure may experience serious reputation damage and a loss of trust from their major customers, partners and stockholders. The effects of such reputation damage may span over the long term and become obstacles to their business operations.

Remedy

To prevent PII disclosure, organizations can take several proactive measures.

- Data Encryption: Using either the 'encryption in transit' or 'encryption at rest' on confidential information enhances the security of the data by prohibiting any unauthorized access even if the data has been intercepted and compromised.
- Access Controls: The application of a tight access control and authentication methods will guarantee that a privilege is given to just official individuals in the disclosure of the PII; this puts a limit on the inside threats, the unauthorized exposure, and the misuse of the data.
- Data Minimization: Keep and delete only Personal Identifiable Information (PII) needed for business purposes and dispose of it securely after the time it is not needed.

2.HTTP to HTTPS Insecure transition in Form Post

Risk level – Medium

What is HTTP to HTTPS Insecure transition in Form Post?

When a form is submitted over HTTP (Hypertext Transfer Protocol), the data being sent is not encrypted, making it vulnerable to interception by attackers.This occurs when a user logs in to a website using a secure HTTPS connection, but then is redirected to an insecure HTTP connection when submitting a form.

Impact

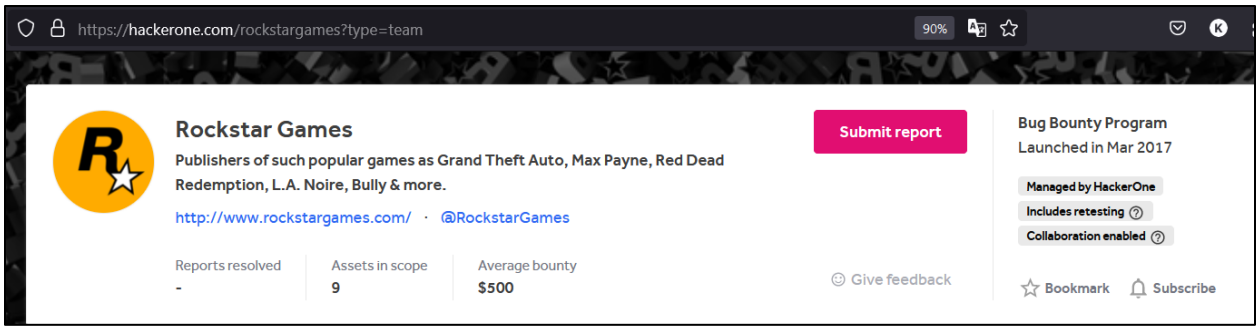
Impact of this vulnerability can lead to various security risks such as Data Interception and Man-in-the-Middle Attacks

Remedy

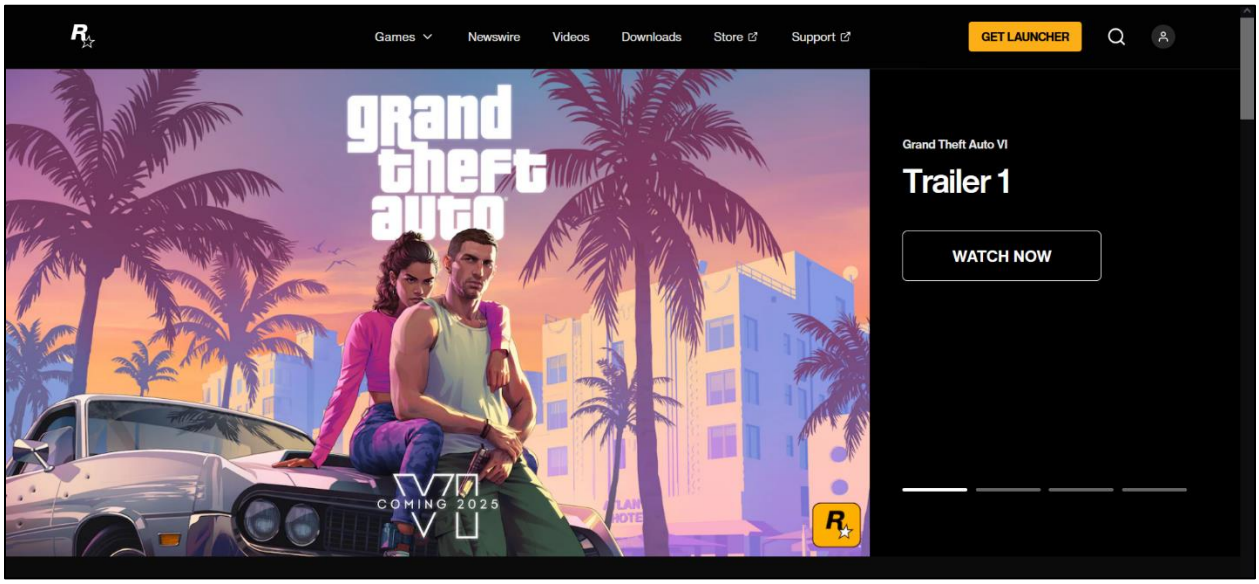
To prevent this from happening following steps can be taken

- Identify All Forms That Are Being Submitted: This means identifying all the forms that are related to the website including login forms,contact forms etc.
- Check the Current Form Submission URLs: Checking the current forms wether they are using HTTP or HTTPs.if HTTP is used it should be upgraded to HTTPs
- Change HTTP URLs to HTTPS URLs: Changing HTTP urls to HTTPs to ensure the security.
- Update Any Associated Links and Resources : any associated resources with form submition such as Css or Js should be updated to load with HTTPs

10.Rockstar Games (Report 10)



Addressing the target



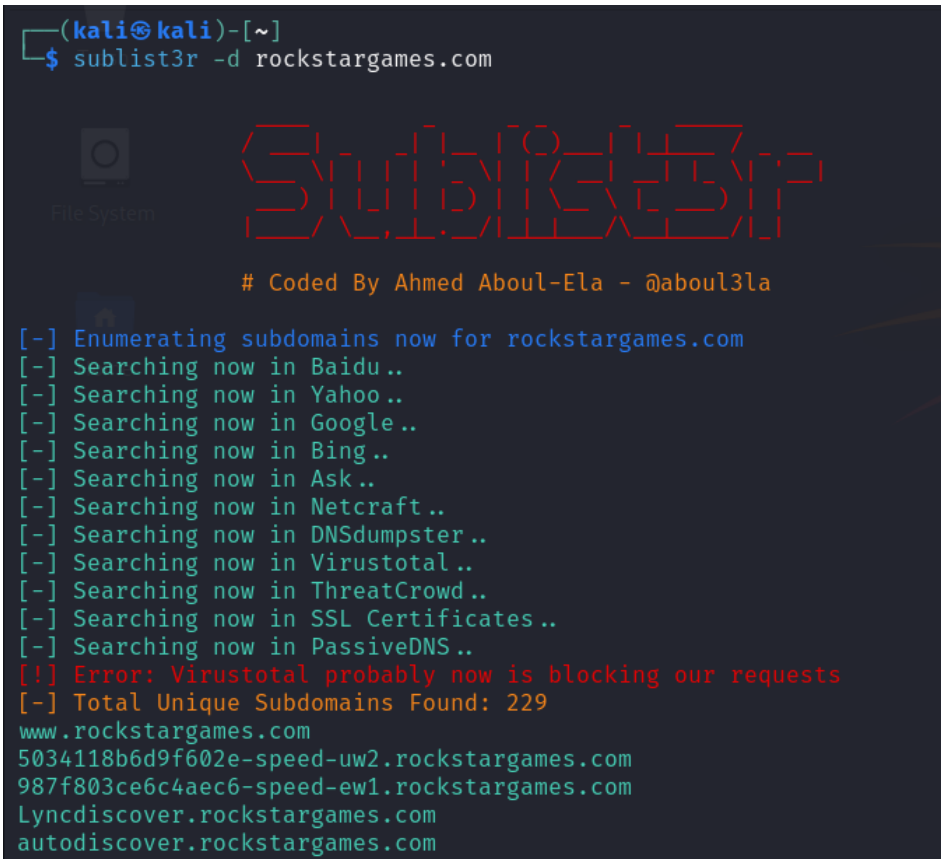
Rockstar games is a American video games company.they are the publishers of the world famous video games like Grand Theft Auto,Red dead redemption,Max payne and much more.

Scope

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
socialclub.rockstargames.com	Domain	In scope	Critical	Eligible	Jan 24, 2023	0 (-)
support.rockstargames.com Vulnerability reports for support.rockstargames.com may not be awarded bounties if it is discovered that the root vulnerability lies in Zendesk's code. Hackers are encouraged to submit such reports to Zendesk's bug bounty program.	Domain	In scope	Critical	Eligible	Jan 24, 2023	0 (-)
store.rockstargames.com Please note that the checkout/payment process go through the Xsolla platform. If you believe you have found a vulnerability in the checkout/payment process, please confirm first whether the vulnerability is in the general Xsolla platform, or our specific implementation.	Domain	In scope	Critical	Eligible	Jan 24, 2023	0 (-)
***.rockstargames.com** Some subdomains excluded. See the rest of the scope table below.	Other	In scope	Critical	Eligible	Jan 24, 2023	0 (-)
prod.ros.rockstargames.com	Domain	In scope	Critical	Eligible	Jan 24, 2023	0 (-)
Rockstar Games Launcher	Executable	In scope	Critical	Eligible	Jan 24, 2023	0 (-)
rockstarnorth.com	Domain	In scope	Medium	Eligible	Jan 24, 2023	0 (-)
circolocorecords.com/	Domain	In scope	Medium	Eligible	Jul 13, 2023	0 (-)
lifeinvader.com	Domain	In scope	Medium	Eligible	Jan 24, 2023	0 (-)

faspex.rockstargames.com	Domain	Out of scope	None	Ineligible	Jan 24, 2023	0 (-)
emailcontent.rockstargames.com We do not have direct control over this subdomain and will not be accepting submissions for it.	Domain	Out of scope	None	Ineligible	Jan 24, 2023	0 (-)
bomgar.rockstargames.com This subdomain is ineligible for bounty at this time.	Domain	Out of scope	None	Ineligible	Jan 24, 2023	0 (-)
any-invalid-domains.rockstargames.com Any subdomain that does NOT contain its own valid content and instead redirects to 'rockstargames.com/?domain-check-failed', UNLESS you can demonstrate an impact to a valid domain or subdomain.	Domain	Out of scope	None	Ineligible	Jul 13, 2023	0 (-)

Subdomain enumeration with Sublist3r



Subfinder was able to 229 unique subdomains.

Selected domain – rockstargames.com

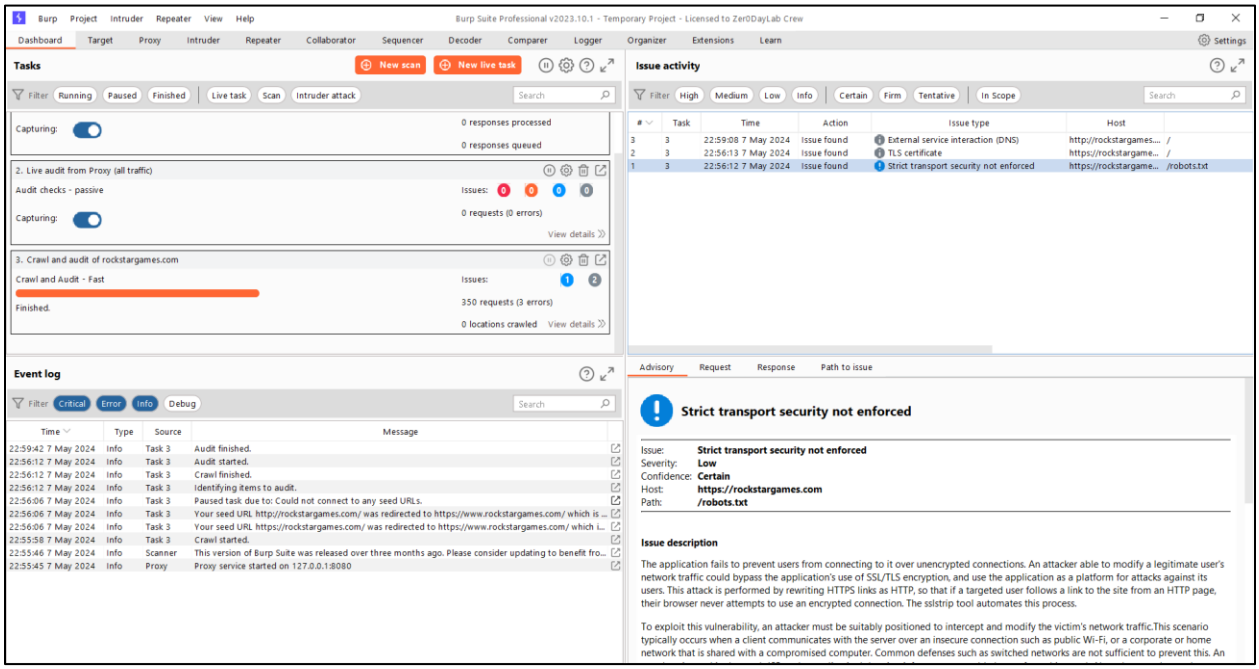
Open Ports

port 80,113,443,8008 and 8010 was found open

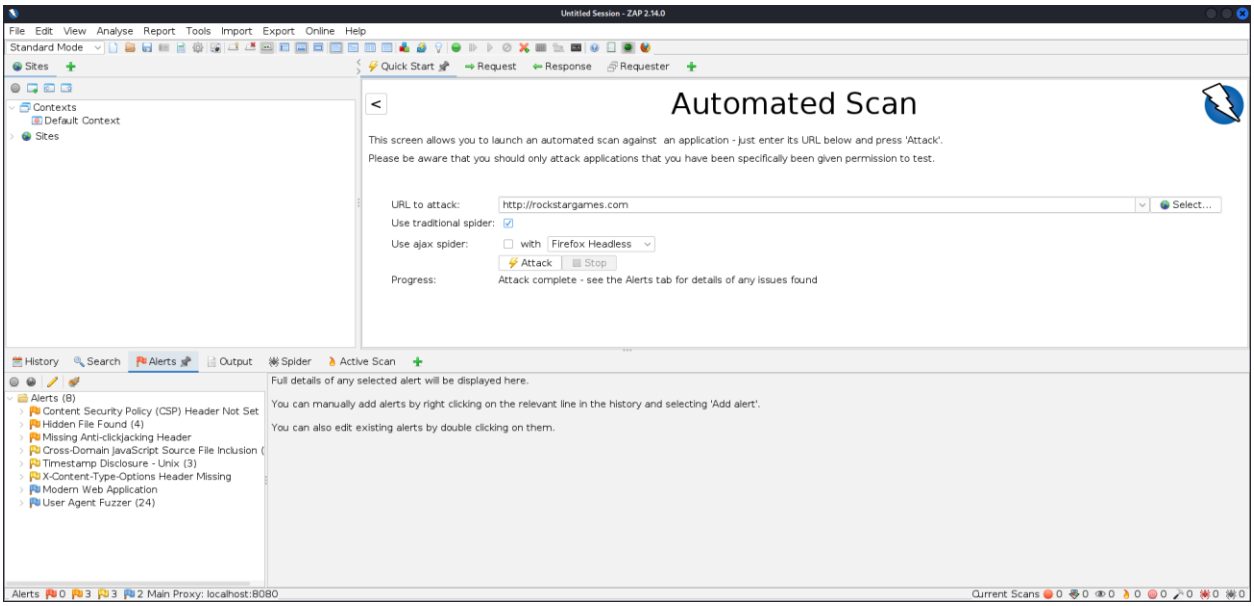
Scanning with Nikto

```
┌──(kali㉿kali)-[~]
└─$ sudo nikto -h rockstargames.com
[sudo] password for kali:
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          23.54.137.66
+ Target Hostname:    rockstargames.com
+ Target Port:        80
+ Start Time:         2024-04-18 10:03:47 (GMT5.5)
---------------------------------------------------------------------------
+ Server: AkamaiGHost
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'akamai-grn' found, with contents: 0.d2d84b17.1713414830.10176071.
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com
/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: https://www.rockstargames.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /nikto-test-HoBYq9Ox.html: Uncommon header 'x-n' found, with contents: S.
+ 7962 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time:           2024-04-18 10:26:25 (GMT5.5) (1358 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Scanning with Burp suite



Scanning with zap



Identified Vulnerabilities

Risk level – Low

Strict Transport Security not enforced

What is "Strict Transport Security not enforced"?

When the Strict Transport Security (HSTS) policy is not enforced, it means that the browser does not strictly adhere to the directives specified by the HSTS header sent by the web server. The HSTS header instructs the browser to communicate with the server only over secure HTTPS connections, even if the user attempts to access the website via HTTP.

Impact

The impact of HSTS not being enforced leads to,

- Increased vulnerability to man-in-the-middle attacks: Without HSTS enforcement, attackers may intercept communication between the user and the server, potentially compromising sensitive data exchanged over the network.
- Higher risk of session hijacking: Attackers can more easily steal session cookies or credentials transmitted over unencrypted HTTP connections, leading to unauthorized access to user accounts.

- Compromised data integrity and confidentiality: The absence of HSTS enforcement exposes transmitted data to eavesdropping and tampering, putting sensitive information at risk.

Remedy

- To address the issue of HSTS not being enforced, the following remedies can be implemented:
- Ensure proper server configuration: Configure the web server to send the HSTS header with appropriate directives in all HTTPS responses.
- Set appropriate "max-age" directive: Specify a suitable duration for the "max-age" directive in the HSTS header to instruct the browser on how long to enforce HTTPS.
- Regularly monitor and test HTTPS configuration: Continuously monitor and test the website's HTTPS configuration to identify and fix any issues that may prevent HSTS enforcement.
- User education: Educate users about the importance of accessing websites over HTTPS and encourage the use of browsers that support and enforce HSTS.
- Consider HSTS preload: Submit the website to browser vendors' HSTS preload lists to ensure that HSTS is enforced by default for all users, even on their first visit to the site.

2.Missing anti clickjacking Header

What is Missing anti clickjacking Header?
The "anti-clickjacking header" typically refers to the "X-Frame-Options" HTTP header, which helps prevent clickjacking attacks. Clickjacking is a malicious technique where an attacker tricks a user into clicking on something different from what the user perceives, potentially leading to unintended actions or information disclosure.

Impact

- Security Risks: Without anti-clickjacking headers, websites cannot avoid clickjacking attacks, which means that legitimate webpages may have layers of harmful material between them and their visitors.
- Data Exposure: An example of clickjacking is exposing the user to the risk of accidental divulgence of private data or the execution of any action that the user did not intend.
- Reputation Damage: A clickjacking attack can fool users into clicking on the malicious links which being classified as bait urls can eventually break their trust towards the website or application.

Remedy

- Implementation of X-Frame-Options Header: Configure the web server to include the X-Frame-Options header in HTTP responses with a value of "DENY" to prevent the page from being rendered in a frame or "SAMEORIGIN" to allow rendering only in frames from the same origin.
- Content Security Policy (CSP): Use CSP to define a policy that restricts which external resources can be loaded by the web page, including the frame-ancestors directive to specify the domains that are allowed to embed the page.

References

https://owasp.org/www-project-top-ten/
https://www.synopsys.com/glossary/what-is-csrf.html
https://en.wikipedia.org/wiki/Cross-site_request_forgery
https://portswigger.net/web-security/csrf
https://portswigger.net/web-security/cors
https://docs.stackhawk.com/vulnerabilities/10062/
https://docs.gitlab.com/ee/user/application_security/dast/browser/checks/352.1.html
https://docs.stackhawk.com/vulnerabilities/10202/
https://www.iothreat.com/blog/csp
https://www.iothreat.com/blog/missing-anti-clickjacking-header
https://www.iothreat.com/blog/cloud-metadata-potentially-exposed
https://turingsecure.com/knowledge-base/issues/password-hash-disclosure/