

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.

```
(kali㉿kali)-[~] kali on wed apr 24 12:38:47 2024
└─$ sudo nmap -sS wise.com
[sudo] password for kali:          243 325
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).          .scanning
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
```

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.

```
[kali㉿kali)-[~] ~$ subfinder -d alshaya.com
[!] Searching now in Google...
[!] Searching now in Shodan...
[!] Searching now in Censys...
[!] Searching now in crt.sh...
[!] Searching now in sublist3r...
[!] Searching now in subfinder...
[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
dizzliuat.alshaya.com
cdine.alshaya.com
sso.uat.alshaya.com
meeting.alshaya.com
apigw.dev2.alshaya.com
trbi.alshaya.com
stageimages.alshaya.com
burjupdates.alshaya.com
odi.sitha.alshaya.com

dev-mobile.alshaya.com [1] 100% total...
pprod.mobile.alshaya.com [2] Crowd...
preprod.alshaya.com [3] SSL certificates...
ip4.alshaya.com [4] PassiveDNS...
prodjenkins.alshaya.com [5] Malicious by Blocking our requests
tbsru-uat.alshaya.com [6] 0 hosts Found: 4
burjsupport.alshaya.com
pb.prod-pimsfactory.alshaya.com
odi.dssit.alshaya.com
www.prodjenkins.alshaya.com
www.ecomuat.alshaya.com
sbxturkey.alshaya.com
ri-uat.store.alshaya.com
muji.store.alshaya.com
[INF] Found 521 subdomains for alshaya.com in 3 seconds 599 milliseconds
```

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.

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

File System
└── [REDACTED]

# 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
[-] 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
```

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:

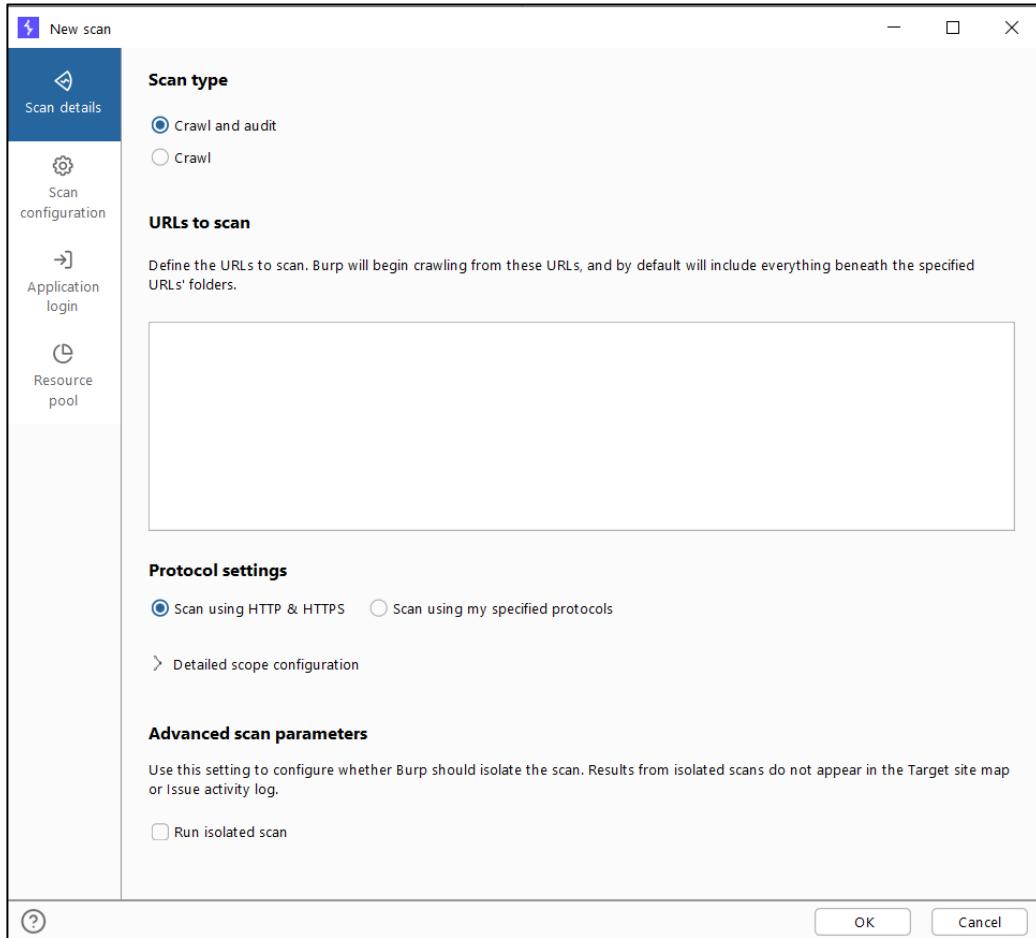
1. **Identification:** This involves discovering and documenting potential vulnerabilities within the target system or environment. This can be achieved through various means such as automated scanning tools, manual inspection, or analysis of system configurations.
2. **Evaluation:** Once vulnerabilities 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.



The screenshot shows the OWASP ZAP interface with three main panels:

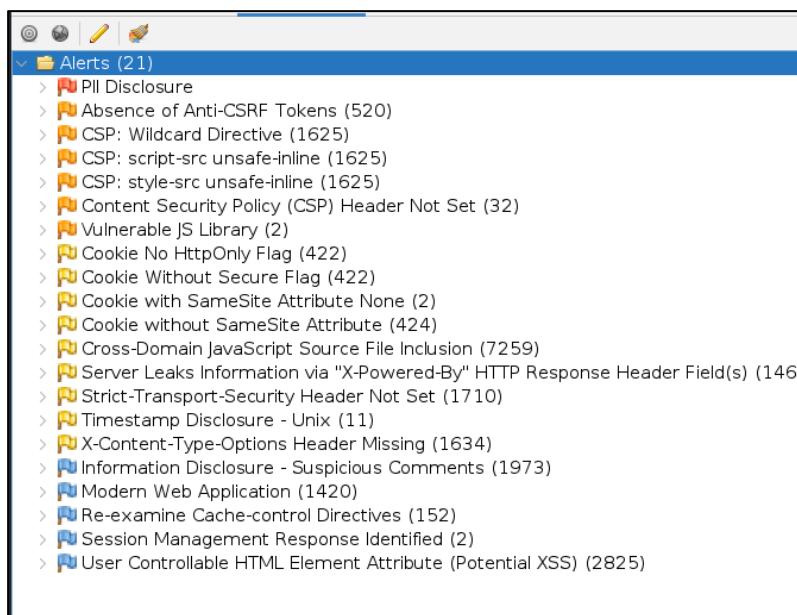
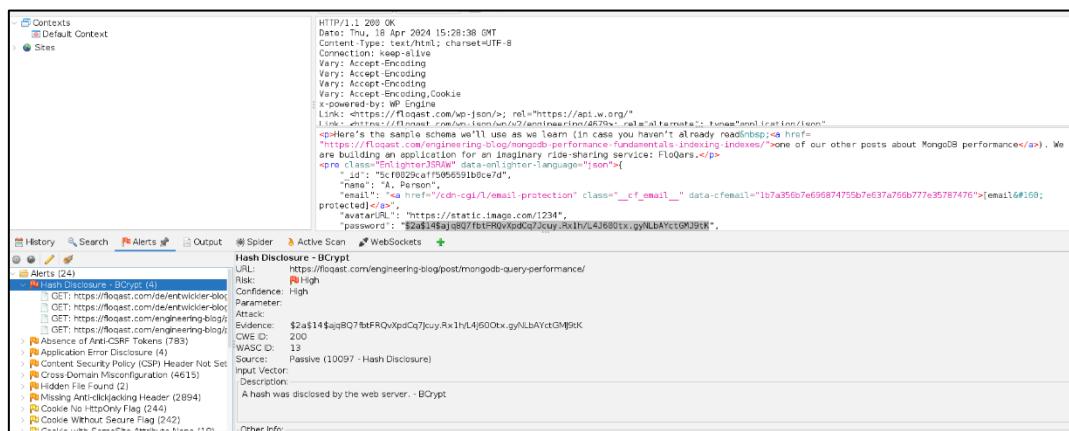
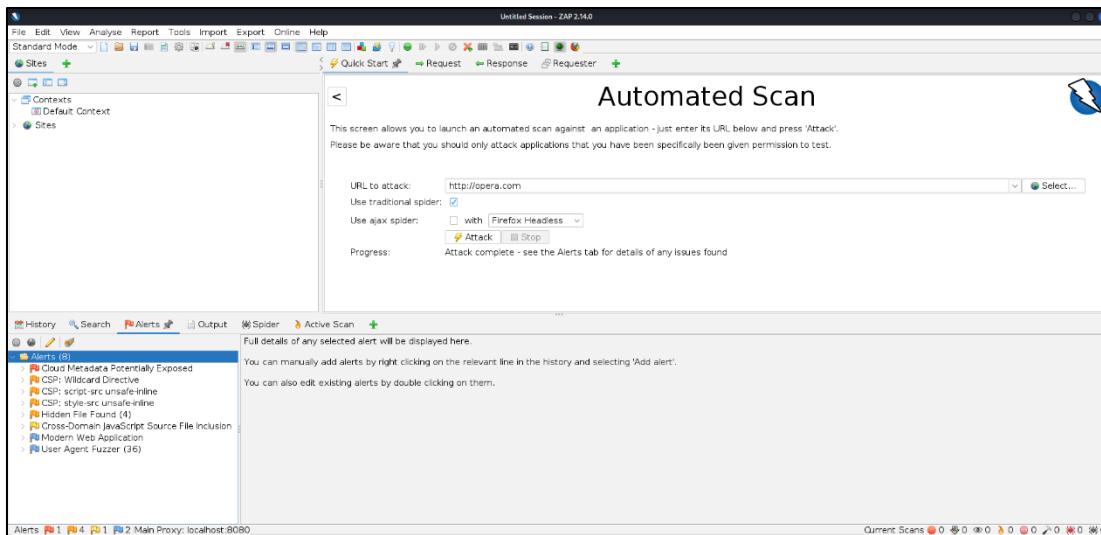
- Tasks**: Shows a live audit from a proxy, crawl and audit of academy.vendasta.com, and a currently auditing session.
- Issue activity**: A table listing issues found during the audit, including cross-origin resource sharing and user agent-dependent responses.
- Event log**: A detailed log of events, including audit starts, task completion, and proxy service startup.

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.

The screenshot shows the OWASP ZAP interface with the following components:

- Top Bar**: File, Edit, View, Analyse, Report, Tools, Import, Export, Online, Help.
- Left Sidebar**: Contexts (Default Context), Sites.
- Central Panel**:
 - Automated Scan** section: URL to attack: http://wise.com, Attack button.
 - Alerts** section: Displays a list of alerts found during the scan, such as XSS, CSRF, and various CSP violations.
 - Output** section: Displays the results of the automated scan.
- Bottom Status Bar**: Alerts (26), Current Scans (0/0/0/0/0/0/0/1).



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.

```
(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 4fa95bb89b64a0e774cf73023a2cbf232.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-interpreter/scanner/headers/malicious-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 (~7% 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
```

```
(kali㉿kali)-[~]
$ sudo nikto -h krisha.kz
[sudo] password for kali:
- Nikto v2.5.0

+ Multiple IPs found: 185.143.129.90, 185.143.129.89
+ Target IP: 185.143.129.90
+ Target Hostname: krisha.kz
+ Target Port: 80
+ Start Time: 2024-04-25 21:07:08 (GMT5.5)

+ Server: nginx
+ /: 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-interpreter/scanner/headers/malicious-content-type-header/
+ Root page / redirects to: https://krisha.kz/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
-C all
- STATUS: Completed 380 requests (~5% complete, 35.8 minutes left): currently in plugin 'Site Files'
- STATUS: Running average: 100 requests: 0.38515 sec, 10 requests: 0.3868 sec.
+ 7964 requests: 0 error(s) and 2 item(s) reported on remote host
+ End Time: 2024-04-25 22:00:08 (GMT5.5) (3180 seconds)

+ 1 host(s) tested
```

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

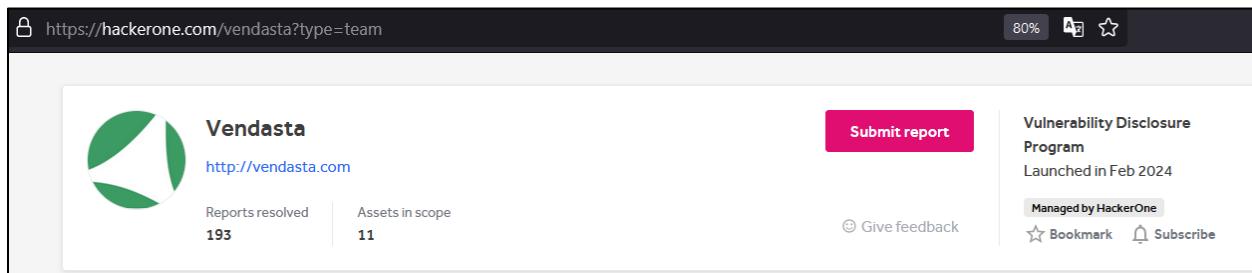
Bugcrowd is a crowdsourced cybersecurity platform that connects organizations with a global community of ethical hackers, often referred to as security researchers or white-hat hackers. These hackers participate in bug bounty programs, where they are incentivized to find and report security vulnerabilities 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

A screenshot of the Vendasta homepage. The top navigation bar includes a search bar, company name, and sign-in options. The main headline reads "Turn your **digital agency** into a scalable powerhouse". Below this, a sub-headline states: "Vendasta gives 80k+ agencies a full-stack platform to rebrand & resell online services to local business clients. Be the exclusive partner, expand your services & give your agency the scalability of a SaaS recurring revenue model." Two call-to-action buttons are present: "Get free access" and "Get a demo". A sidebar on the right displays various performance metrics in cards, such as Reputation (4.9), Listings (Accuracy 8/19), Advertising (ROI 301%), and Social (Post engagement 480). A woman is shown working on a tablet, illustrating the platform's use.

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.stepprep.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: Create-Snapshot-Reports">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

[INFO] Current subfinder version v2.6.6 (latest)
[INFO] Loading provider config from /home/kali/.config/subfinder/provider-config.yaml
[INFO] 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

The screenshot shows a web browser displaying the URL <https://www.vendasta.com/blog/>. The page has a dark blue header with the Vendasta logo, a search bar, and navigation links for AI Tools, Products, Solutions, Resources, Pricing, and a 'Get free access' button. A banner at the top features a green background with a graphic of people icons and a location pin, and the text 'Unleash the Power of Proximity with Local Lead Generation'. Below the banner, there's a section titled 'Newest articles' with a small thumbnail image of a person icon.

Identified Vulnerabilities

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

The screenshot shows the Burp Suite Professional interface with the following details:

- Task Overview:** Capturing is turned off. There are 0 responses processed and 0 responses queued.
- Audit Checks - passive:** 2. Live audit from Proxy (all traffic) is selected. Issues found: 0 errors, 0 warnings, 0 info.
- Crawl and Audit - Fast:** Crawl and Audit - Fast is selected. Issues found: 1 error, 0 warnings, 0 info. 32304 requests (1 errors). 7 locations crawled.
- Event Log:** Filtered by Critical, Error, Info, Debug. Shows log entries from Task 3 and Scanner.
- Issue Activity:** A table listing issues found during the audit. The first issue is highlighted:

#	Task	Time	Action	Issue type	Host
28	3	16:30:05 5 May 2024	issue found	① Cross-origin resource sharing	https://blog.vendasta.../hms/livechat/wi...
27	3	16:30:05 5 May 2024	issue found	① Cross-origin resource sharing: arbitrary orig...	https://blog.vendasta.../hms/livechat/wi...
26	3	16:29:57 5 May 2024	issue found	① User agent-dependent response	https://blog.vendasta.../hms/livechat/wi...
25	3	16:29:57 5 May 2024	issue found	① User agent-dependent response	https://blog.vendasta.../hms/perf/v2...
24	3	16:29:57 5 May 2024	issue found	① User agent-dependent response	https://blog.vendasta.../hms/perf/v2...
23	3	16:29:57 5 May 2024	issue found	① User agent-dependent response	https://blog.vendasta.../hms/scriptloader/20...
22	3	16:29:57 5 May 2024	issue found	① Backup file	https://blog.vendasta.../hms/scriptloader/20...
21	3	16:29:57 5 May 2024	issue found	① Backup file	https://blog.vendasta.../hms/scriptloader/20...
20	3	16:29:53 5 May 2024	issue found	① Cross-origin resource sharing	https://blog.vendasta.../hms/scriptloader/20...
19	3	16:29:53 5 May 2024	issue found	① Cross-origin resource sharing: arbitrary orig...	https://blog.vendasta.../hms/scriptloader/20...
18	3	16:29:57 5 May 2024	issue found	① User agent-dependent response	https://blog.vendasta.../hms/scriptloader/20...
17	3	16:29:57 5 May 2024	issue found	① Cross-origin resource sharing	https://blog.vendasta.../hms/static/Hubsp...
16	3	16:29:57 5 May 2024	issue found	① Cross-origin resource sharing: arbitrary orig...	https://blog.vendasta.../hms/static/Hubsp...
15	3	16:29:57 5 May 2024	issue found	① Cross-origin resource sharing	https://blog.vendasta.../hms/static/cos-111...
14	3	16:29:57 5 May 2024	issue found	① Cross-origin resource sharing: arbitrary orig...	https://blog.vendasta.../hms/static/cos-111...
13	3	16:29:57 5 May 2024	issue found	① User agent-dependent response	https://blog.vendasta.../hms/static/Hubsp...
- Issue Detail:** Cross-origin resource sharing: arbitrary origin trusted. Severity: High. Confidence: Certain. Host: https://blog.vendasta.com. Path: /hs/scriptloader/20852504.js. Description: The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain. The application allowed access from the requested origin https://dntaiayrdump.com.
- Issue Background:** An HTML5 cross-origin resource sharing (CORS) policy controls whether and how content running on other domains can perform two-way interaction with the domain that publishes the policy. The policy is fine-grained and can apply access controls per-request.

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)

The screenshot shows the Burp Suite Professional interface with the following details:

- Issue activity:** A table listing findings related to Ajax request header manipulation (DOM-based). The first few rows include:
 - Issue found: Cross-origin resource sharing arbitrary orig. https://blog.vendasta... /hs/static/Hubsp
 - Issue found: Cross-origin resource sharing arbitrary orig. https://blog.vendasta... /hs/static/cos-i11
 - Issue found: Cross-origin resource sharing arbitrary orig. https://blog.vendasta... /hs/static/cos-i11
 - Issue found: User agent-dependent response https://blog.vendasta... /hs/static/Hubsp
 - Issue found: Cross-site scripting (reflected) https://blog.vendasta... /hs/manage-prefer
 - Issue found: Input returned in response (reflected) https://blog.vendasta... /hs/manage-prefer
 - Issue found: Ajax request header manipulation (DOM-based) https://blog.vendasta... /hs/preferences-ce
 - Issue found: Input returned in response (reflected) https://blog.vendasta... /
 - Issue found: Certificate https://blog.vendasta... /
 - Issue found: Robotstat file https://blog.vendasta... /robotstat
 - Issue found: Cross-domain script include https://blog.vendasta... /hs/preferences-ce
 - Issue found: Cross-domain Referer leakage https://blog.vendasta... /hs/preferences-ce
 - Issue found: Cacheable HTTPS response https://blog.vendasta... /robots.txt
 - Issue found: Duplicate cookies set https://blog.vendasta... /hs/manage-prefer
 - Issue found: Frameable response (potential Clickjacking) https://blog.vendasta... /hs/preferences-ce
- Event log:** A table showing logs from 16:46:18 to 16:21:18. Key entries include:
 - Task 3 Audit finished.
 - Discarded log entry larger than Logger memory limit
 - Discarded log entry larger than Logger memory limit
 - Task 3 Audit finished.
 - Crawl finished.
 - Identifying items to audit.
 - Paused task due to: Could not connect to any seed URLs.
 - Your seed URL https://blog.vendasta.com/ was redirected to https://www.vendasta.com/blog/ which is out
 - Your seed URL https://blog.vendasta.com/ was redirected to https://www.vendasta.com/blog/ which is out
 - Crawl started.
 - This version of Burp Suite was released over three months ago. Please consider updating to benefit from
 - Proxy service started on 127.0.0.1:8080

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

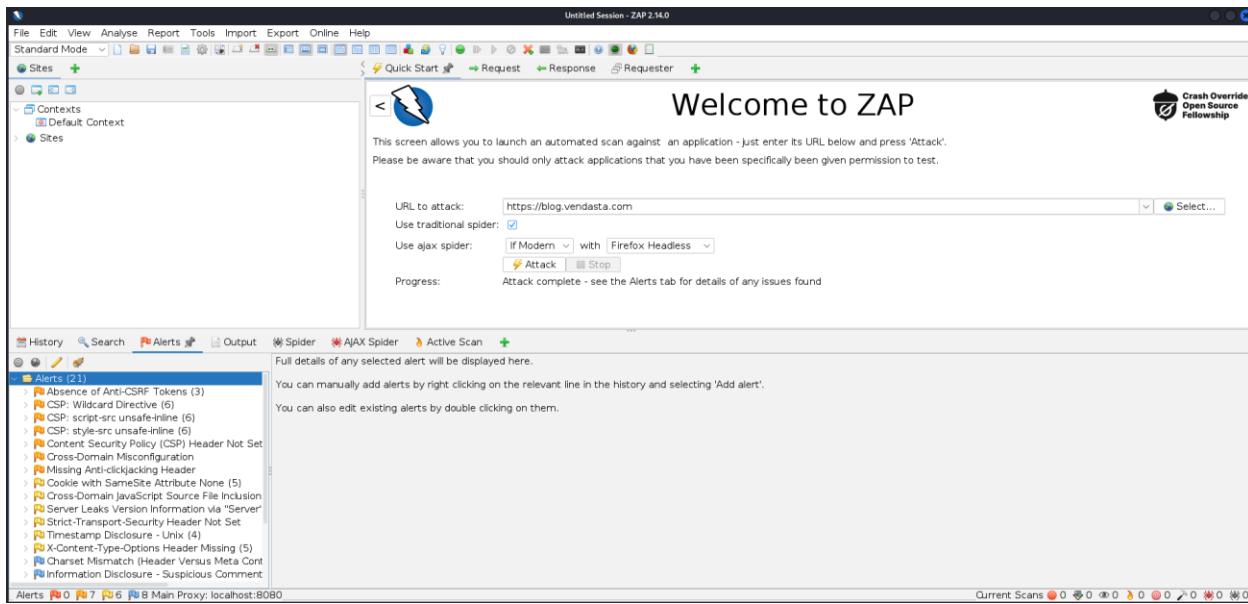
The impact of DOM-based Ajax request header manipulation can be severe and wide-ranging. Attackers can use this vulnerability to steal sensitive data, execute unauthorized actions, or manipulate server responses. Depending on the nature of the injected headers and the server's response to them, the consequences 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)

Wise (ex-TransferWise)
Wise — the global technology company building the best way to move money around the world.

\$100 – \$4,000 per vulnerability | Up to \$6,000 maximum reward | Safe harbor

Submit report | Do you like this program? |

Σ

Addressing the target

ΣWISE Personal Platform Features Pricing Help EN Log in Register

SAVE WHEN YOU SEND WORLDWIDE

Get your money moving internationally. Save up to x when you send with Wise.

[Send money now](#) [Open an account](#)

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

Value	Rewards
★ \$6000	P1 \$3000 – \$4000
	P2 \$1000 – \$1500
	P3 \$300 – \$500
	P4 \$100 – \$150

Targets:

- 🌐 transferwise.com
- 🌐 *.transferwise.com
- 🌐 wise.com
- 🌐 *.wise.com
- iOS Latest version of Wise iOS App
- Android Latest version of Wise Android App
- 🌐 AWS infrastructure and services in use by Wise (eg: S3 buckets)
- 🌐 github.com/transferwise/*

Tags:

- Java
- Cloudflare CDN
- ReactJS
- +2
- 18
- 🔗

- Java
- Cloudflare CDN
- ReactJS
- +3
- 2
- 🔗

- Java
- Cloudflare CDN
- ReactJS
- +2
- 5
- 🔗

- Java
- Cloudflare CDN
- ReactJS
- +3
- 4
- 🔗

- Objective-C
- SwiftUI
- Swift
- +2
- 3
- 🔗

- Java
- Android
- Mobile Application
- +1
- 4
- 🔗

- AWS
- 0
- 🔗

- Github
- Recon
- 2
- 🔗

Out of scope

Out of scope targets

✗ Out of scope

Targets:

- 🌐 Wise Affiliate Program
- 🌐 Third party services not hosted by Wise
- 🌐 Any Github asset not under the “transferwise” organization
- 🌐 Third party authentication services (eg: Facebook and Google)
- 🌐 https://transferwise.com/help/contact
- 🌐 https://wise.com/help/contact
- 🌐 *.tw.com
- 🌐 *.tw.ee
- 📱 Non-current version of the Android app
- iOS Non-current version of the iOS app
- 🌐 *.transferwise.tech
- 🌐 brand.wise.com
- 🌐 links.wise.com

Tags:

- Website Testing

- Website Testing

- Github
- Recon

- Website Testing

- Java
- Android
- Mobile Application
- +1

- Objective-C
- SwiftUI
- Swift
- +2

- Website Testing

- Website Testing

- Website Testing

Subdomain hunting using Sublist3r

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

File System
└── [!] 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
www--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:59 247 225
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).ect
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
```

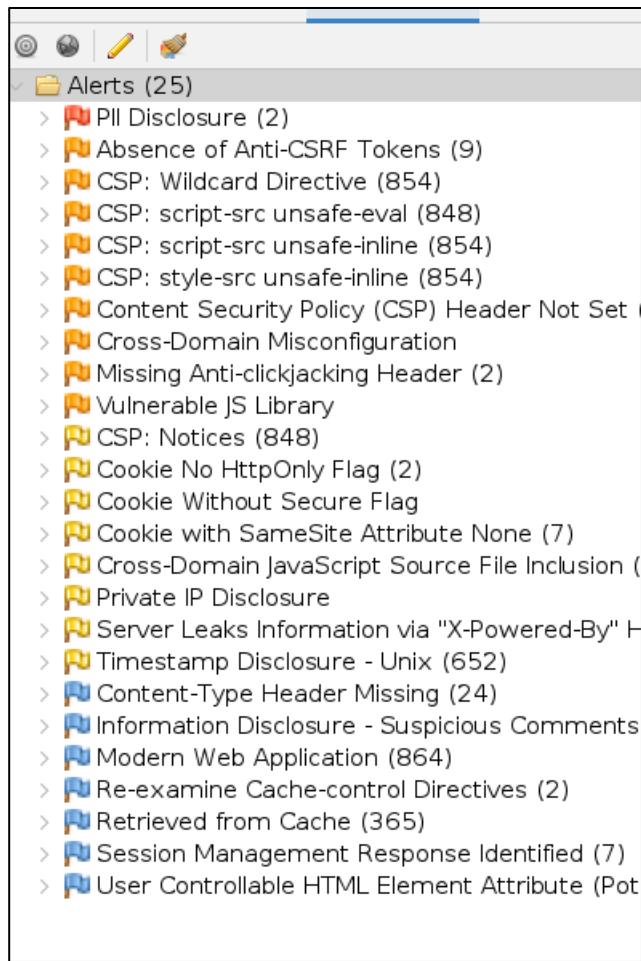
There we have ports 80,443,8008,8010,8080 and 8443 as open ports.

Scanning with Zap

The screenshot shows the ZAP interface with an 'Automated Scan' in progress against the URL <http://wise.com>. The 'Alerts' panel on the left lists 26 PII Disclosure vulnerabilities, including details like URL, Risk level (High), and Evidence ID. The main pane displays the results of the scan.

PII Disclosure	
URL:	https://wise.com/gb/iban/
Risk:	High
Confidence:	High
Parameter:	
Attack:	
Evidence:	5000400440116243
CWE ID:	359
WASC ID:	13
Source:	Passive (10062 - PII Disclosure)
Input Vector:	
Description:	The response contains Personally Identifiable Information, such as CC number, SSN and similar sensitive data.
Other Info:	
Credit Card Type detected:	Maestro
Bank Identification Number:	500040
Brand:	MAESTRO

Alerts 1 9 8 7 Main Proxy: localhost:8080



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 possibly 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.
- ❖ UseNonce 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)

Alshaya

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

<https://alshaya.com>

Reports resolved: 84 Assets in scope: 142

Submit report

Vulnerability Disclosure Program
Launched in Aug 2023

Gold standard

Give feedback

Bookmark Subscribe

Addressing the target

Ashaya Group

About us Brands Aura Locations Customer Zone Media Centre Careers Contact us

Who we are

Alshaya Group is one of the world's leading brand franchise operators, offering an unparalleled choice of well-loved international brands to customers. Fresh, modern and relevant, Alshaya's constantly evolving portfolio reflects the choices and lifestyles of its customers.

Read more

70~ 16

Brands Markets

40,000+ 4000+

Employees Stores

Discover some of the world's best loved brands

Panes SHAKE SHACK Sephora CharlotteTilbury Starbucks AMERICAN EAGLE THE HEART OF SNEAKERS VICTORINOX

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

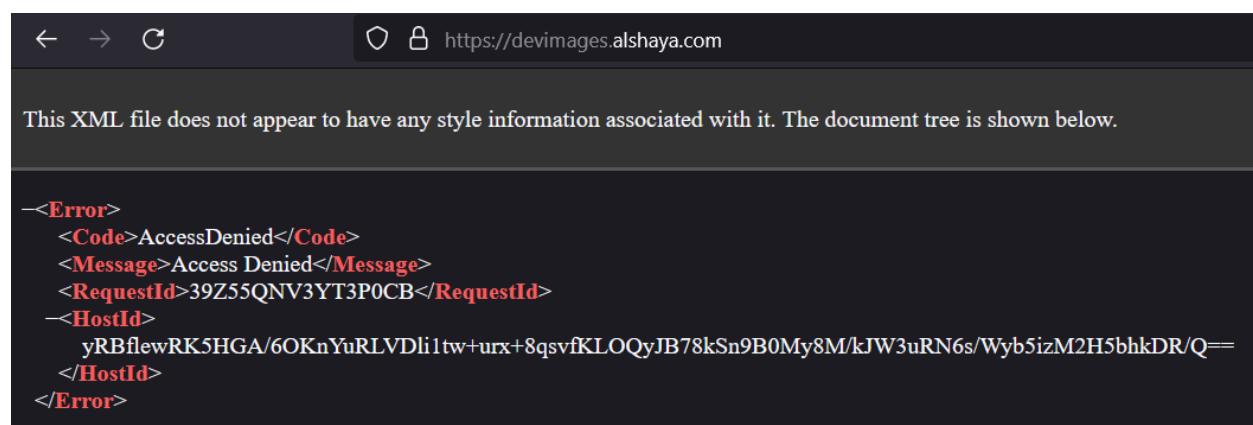
[INF] Current subfinder version v2.6.6 (latest)
[INF] Loading provider config from /home/kali/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for alshaya.com
www.performans.alshaya.com
www.tbstr-uat.alshaya.com
deb.prod-pimsfactory.alshaya.com
trbi.alshaya.com
alshayaebspub-tst.stg.alshaya.com
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
email.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
rssaccess.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
starbucks2b.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



The screenshot shows a web browser window with the URL <https://devimages.alshaya.com> in the address bar. The page content is an XML error response:

```
<Error>
<Code>AccessDenied</Code>
<Message>Access Denied</Message>
<RequestId>39Z55QNV3YT3P0CB</RequestId>
<HostId>
    yRBflewRK5HGA/6OKnYuRLVDli1tw+urx+8qsvfKLOQyJB78kSn9B0My8M/kJW3uRN6s/Wyb5izM2H5bhkDR/Q==
</HostId>
</Error>
```

Identified vulnerabilities

The screenshot shows the Burp Suite Professional interface with several panels:

- Dashboard:** Shows tasks like "Capturing" (0 responses processed), "Audit from Proxy (all traffic)" (Issues: 0 errors), and "Crawl and audit of devimages.alshaya.com" (Issues: 1 error, 1286 requests, 4 locations crawled).
- Issue activity:** A table listing vulnerabilities found during the crawl. One entry is highlighted: "Cross-site request forgery" at <http://devimages.alshaya.com/cdn-cgi/rum>.
- Event log:** A table of log entries showing events like "Audit finished", "Audit started", "Crawl finished", and "Scanner started".
- Details pane:** Expanded view of the "Cross-site request forgery" issue, showing details like Issue: Cross-site request forgery, Severity: Medium, Confidence: Tentative, Host: <https://devimages.alshaya.com>, and Path: /cdn-cgi/rum.

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

```
(kali㉿kali)-[~]
$ nikto -h devimages.alshaya.com
- Nikto v2.5.0

+ Multiple IPs found: 104.18.40.190, 172.64.147.66, 2606:4700:4400::ac40:9342, 2606:4700:4400::6812:28be
+ Target IP: 104.18.40.190
+ Target Hostname: devimages.alshaya.com
+ Target Port: 80
+ Start Time: 2024-05-08 17:46:58 (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 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/img/content-type-header/
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 3 item(s) reported on remote host
+ End Time: 2024-05-08 17:48:49 (GMT5.5) (111 seconds)

+ 1 host(s) tested
```

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)

The screenshot shows a web browser window with the URL <https://bugcrowd.com/operaprogram>. The page title is "Opera Public Bug Bounty". It features a large red "O" Opera logo on the right. Key information includes: "\$50 – \$5,000 per vulnerability", "Up to \$10,000 maximum reward", and "Safe harbor". There are buttons for "Submit report" and "Do you like this program?". The Bugcrowd navigation bar at the top includes links for Dashboard, Engagements, Invites, Discovery, Work, Payments, Leaderboards, and CrowdStream.

Addressing the target

The screenshot shows the official Opera website at <https://www.opera.com>. The main headline is "Your personal browser". Below it, a sub-headline reads: "Faster, safer and smarter than default browsers. Opera Browser is fully-featured for privacy, security, and everything you do online." A "See more" link and a "Download now" button are present. The top navigation bar includes links for Opera, Browsers, Privacy & Security, About, and Help. A prominent purple "Download now" button is located in the center of the page.

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

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

Scope and rewards

Primary Targets

✓ In scope

Value	Count
\$10000	1
\$3000 – \$5000	1
\$500 – \$3000	1
\$200 – \$500	1
\$100 – \$200	1

Targets

- 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

```
(kali㉿kali)-[~]
$ sublist3r -d opera.com

File System

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for opera.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
[-] Total Unique Subdomains Found: 312
bugs.coastbyopera.com
myopera.com
www.myopera.com
mail.myopera.com
www.opera.com
addons.opera.com
admanager.opera.com
ads.opera.com
www.ads.opera.com
adx.opera.com
b-ca.adx.opera.com
b-eu.adx.opera.com
b-gb.adx.opera.com
b-sg.adx.opera.com
b-us.adx.opera.com
b-usc.adx.opera.com
bz.adx.opera.com
```

There were 312 unique subdomains.

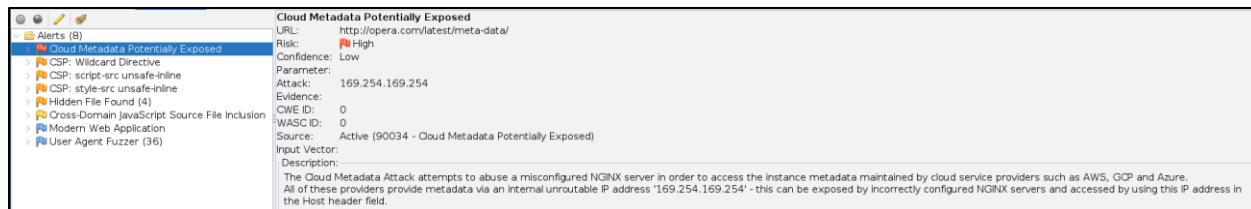
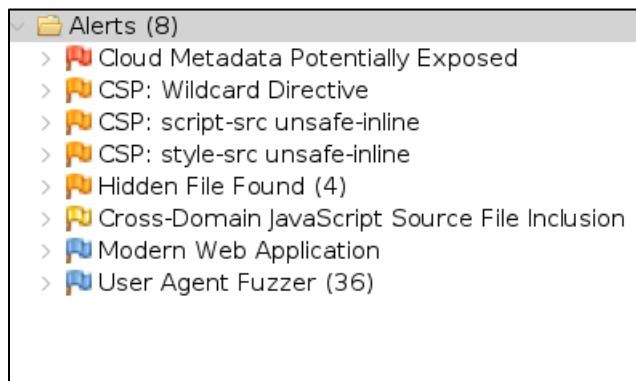
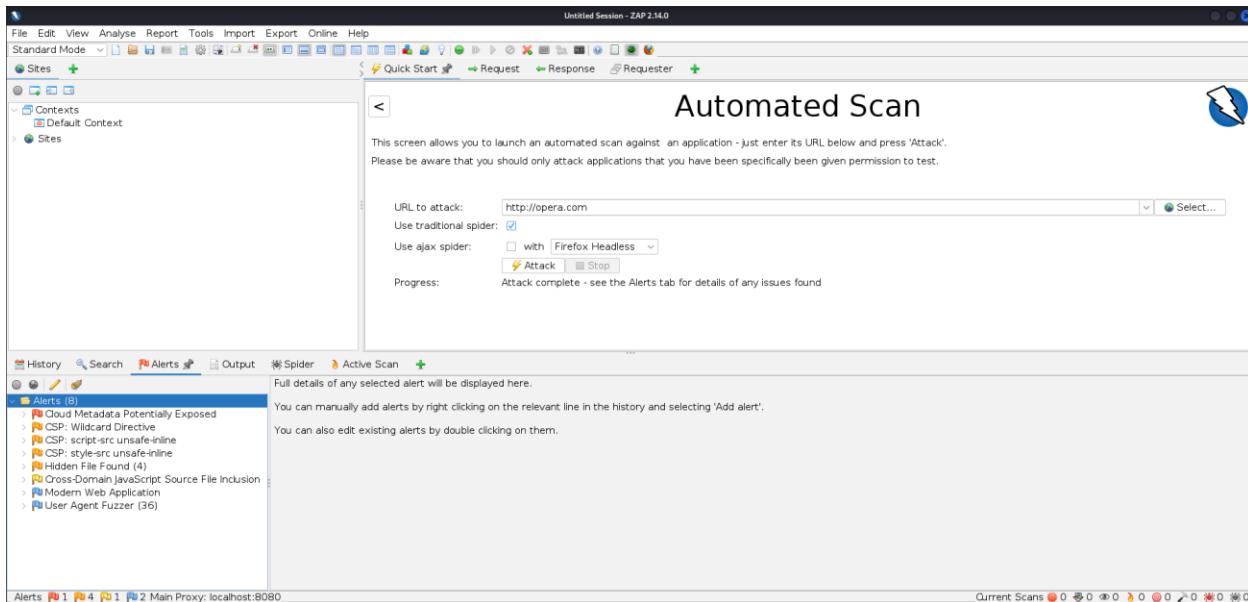
Open Ports

```
(kali㉿kali)-[~]
$ sudo nmap -sS opera.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-27 14:48 +0530
Nmap scan report for opera.com (185.26.182.104)
Host is up (0.025s latency).
Other addresses for opera.com (not scanned): 185.26.182.103
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE    SERVICE
80/tcp     open     http
113/tcp    closed   ident
443/tcp    open     https
8008/tcp   open     http
8010/tcp   open     xmpp

Nmap done: 1 IP address (1 host up) scanned in 18.03 seconds
```

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

Zap



Scanning with Nikto

```
(kali㉿kali)-[~]
$ sudo nikto -h opera.com
[sudo] password for kali:
- Nikto v2.5.0

+ Multiple IPs found: 185.26.182.104, 185.26.182.103
+ Target IP:          185.26.182.104
+ Target Hostname:   opera.com
+ Target Port:        80
+ Start Time:        2024-04-18 15:48:32 (GMT5.5)

+ Server: nginx
+ /: 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://opera.com/
+ No CGI Directories found (use '-c all' to force check all possible dirs)
-C [all]
- STATUS: Completed 310 requests (~4% complete, 30.4 minutes left): currently in plugin 'HTTP Headers'
- STATUS: Running average: 100 requests: 0.24397 sec, 10 requests: 0.2474 sec.
+ 7963 requests: 0 error(s) and 2 item(s) reported on remote host
+ End Time:      2024-04-18 16:24:37 (GMT5.5) (2165 seconds)

+ 1 host(s) tested
```

Identified vulnerabilities

1. Cloud metadata 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)

The screenshot shows a browser window with the URL https://hackerone.com/floqast?view_policy=true. The page title is "FloQast". Below the title, it says "FloQast is an accounting software vendor based in Los Angeles, California." and provides the URL <https://floqast.com> and handle @floqast. There are three metrics displayed: "Reports resolved 19", "Assets in scope 3", and "Average bounty \$500-\$1k". A pink button labeled "Submit report" is visible. To the right, there's a "Bug Bounty Program" section stating "Launched in Mar 2023" and "Includes retesting". Buttons for "Bookmark" and "Subscribe" are also present.

Addressing the site

The screenshot shows the FloQast homepage. The main headline reads "Empowering Accountants to Do Big Things with AI. And it Starts with the Close." Below it, a sub-headline states "The future of accounting is a faster close and stress free audits." A text block explains that FloQast is an industry-leading accounting workflow automation solution powered by an AI-enabled platform designed by accountants for accountants. It highlights the ability to automate mundane tasks and ease the audit process. Two buttons are visible: "Get a Demo" and "Learn More". On the right side, there's a "Talk to the FloQast Team" section featuring a team photo and three options: "I'd like to speak with a FQ rep", "I'd like to see a recorded demo", and "I'm just browsing right now". A small note at the bottom of this section states: "By chatting, you agree that FloQast can record and use the information you provide for chat assistance, to improve FloQast's services, and for marketing purposes, as described in our [Privacy Policy](#)".

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	Wildcard	In scope	Critical	\$ Eligible	May 15, 2023	0 (0%)
Amazon Web Services JavaScript MongoDB Node.js React						
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	Wildcard	In scope	Critical	\$ Eligible	May 15, 2023	0 (0%)
Amazon Web Services JavaScript MongoDB Node.js React						
*.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

The screenshot shows the ZAP 2.14.0 interface with an 'Automated Scan' in progress against the URL <http://floqast.com>. The 'Alerts' tab is active, listing 24 findings across various categories such as security headers, file extensions, and cookie handling. The 'Spider' tab is also visible at the bottom.

Category	Count
Hash Disclosure - BCrypt	4
Absence of Anti-CSRF Tokens	783
Application Error Disclosure	4
Content Security Policy (CSP) Header Not Set	1
Cross-Domain CSP Configuration	4615
Missing File Extension	2
Missing Anti-clickjacking Header	2894
Cookie No HttpOnly Flag	244
Cookie Without Secure Flag	242
Cookie with SameSite Attribute None	18
Cookie without SameSite Attribute	244
Cross-Domain JavaScript Source File Inclusion	1
Server Leaks Information via 'X-Powered-By'	1
Cookie Transport Security Header Not Set	1

Hash Disclosure - BCrypt

URL: <https://floast.com/engineering-blog/post/mongodb-query-performance/>
Risk: High
Confidence: High
Parameter:
Attack:
Evidence: \$2a\$14\$ajqBQ7btFRQvXpdCq7juy.Rx1h/L4j60Otx.gyNLbAYctGMj9tK
CWE ID: 200
WASC ID: 13
Source: Passive (10097 - Hash Disclosure)
Input Vector:
Description: A hash was disclosed by the web server. - BCrypt
Other Info:
Solution: Ensure that hashes that are used to protect credentials or other resources are not leaked by the web server or database. There is typically no requirement for password hashes to be accessible by the web browser.
Reference: <http://projects.webappsec.org/w/page/13246936/Information%20Leakage>
<http://openwall.info/wiki/john/sample-hashes>
Alert Tags:

Key	Value
OWASP_2021_A04	https://owasp.org/Top10/A04_2021-Insecure_Design/
OWASP_2017_A03	https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html

Application Error Disclosure

URL: <https://floast.com/engineering-blog/post/aws-step-functions-reducing-a-long-running-process-by-75/>
Risk: Medium
Confidence: Medium
Parameter:
Attack:
Evidence: Internal error
CWE ID: 200
WASC ID: 13
Source: Passive (90022 - Application Error Disclosure)
Input Vector:
Description: This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.
Other Info:
Solution: Review the source code of this page. Implement custom error pages. Consider implementing a mechanism to provide a unique error reference/identifier to the client (browser) while logging the details on the server side and not exposing them to the user.
Reference:
Alert Tags:

Key	Value
WSTG-v42-ERRH-02	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testin...
WSTG-v42-ERRH-01	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testin...
OWASP_2021_A05	https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
OWASP_2017_A06	https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html

Alerts: 1 6 9 8 Main Proxy: localhost:8080 Current Scans: 0 0 0 0 0 0 0 0 0 0 0 0

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: Developers 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)

Kolesa Group
Kolesa (wheels) is a top vertical classified advertising service for vehicles in Kazakhstan.
<https://kolesa.kz>

Reports resolved: 31 | Assets in scope: 13 | Average bounty: \$124-\$145

[Submit report](#) | Bug Bounty Program
Launched in Jun 2023
Managed by HackerOne | Includes retesting | Collaboration enabled
[Give feedback](#) | [Bookmark](#) | [Subscribe](#)

Addressing the target

Kolesa.kz Krisha.kz

krisha.kz Продажа Аренда Оценка **New** Новостройки Новости Крыша Гид 479 814 уже на сайте [Подать объявление](#)

Купить квартиру Весь Казахстан любой комнатности От До Найти На карте
 есть фото новостройки от хозяев От Крыша Агентов

Горячие предложения недвижимости в Казахстане [Как сюда попасть?](#)

Продажа	Аренда	Квартиры	Участки	Промбазы	Коммерческая недвижимость	Бизнес	Дома или Дачи	Гаражи	Зарубежная недвижимость
 2-комн. квартира, 63 м², 1/5 этаж 71 млн ₮ 27.4 млн ₮	 2-комн. квартира, 50 м², 9/10 этаж 23.5 млн ₮ 57 млн ₮	 3-комн. квартира, 84 м², 10/17 этаж 43 млн ₮ 28 млн ₮	 1-комн. квартира, 40.6 м², вид на горы 17.4 млн ₮	 3-комн. квартира, 105.5 м², 3/16 этаж 105 млн ₮ 33 млн ₮	 4-комн. квартира, 90 м², 1/4 этаж 95 млн ₮ 44.5 млн ₮	 4-комн. квартира, 100.8 м², 3/5 этаж 91 млн ₮ 35.5 млн ₮			
 2-комн. квартира, 56 м², 7/9 этаж Абайский 71.5 млн ₮ 23.000 ₮	 2-комн. квартира, 58 м², 3/9 этаж 73.5 млн ₮ 10 000 ₮	 2-комн. квартира, 62 м², 8/10 этаж микр 78.5 млн ₮ 12 000 ₮	 3-комн. квартира, 98.19 м² Абайка 82.5 млн ₮ 1 000 ₮	 Дача + 4 комнаты + 150 м² + 15 сот. Бизимт 105.5 млн ₮ 2 000 ₮	 3-комн. квартира, 91.2 м², 15/16 этаж 100 000 ₮ 13 000 ₮	 2-комн. квартира, 58 м², 15/16 этаж Сыганак 100 000 ₮ 120 000 ₮			

Krishna.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 and 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

```
└─(kali㉿kali)-[~]
$ subfinder -d krisha.kz

projectdiscovery.io

[INF] Current subfinder version v2.6.0 (outdated)
[INF] Loading provider config from /home/kali/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for krisha.kz
sales.krisha.kz
krisha.kz
support.krisha.kz
guide.krisha.kz
api.krisha.kz
srv.krisha.kz
special.krisha.kz
www.special.krisha.kz
m.krisha.kz
app.krisha.kz
pay.krisha.kz
links.e.krisha.kz
chat.krisha.kz
ws.krisha.kz
bff.krisha.kz
www.krisha.kz
khvcux.krisha.kz
www.sales.krisha.kz
[INF] Found 18 subdomains for krisha.kz in 30 seconds 3 milliseconds
```

With subfinder I was able to find 18 subdomains.

Open Ports

```
└─(kali㉿kali)-[~]
$ sudo nmap -sS krisha.kz
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-27 14:46 +0530
Nmap scan report for krisha.kz (185.143.129.89)
Host is up (0.020s latency).
Other addresses for krisha.kz (not scanned): 185.143.129.90
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
113/tcp   closed ident
443/tcp   open  https
8008/tcp  open  http
8010/tcp  open  xmpp

Nmap done: 1 IP address (1 host up) scanned in 26.42 seconds
```

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

Selected domain – Krisha.kz

Scanning with Nikto

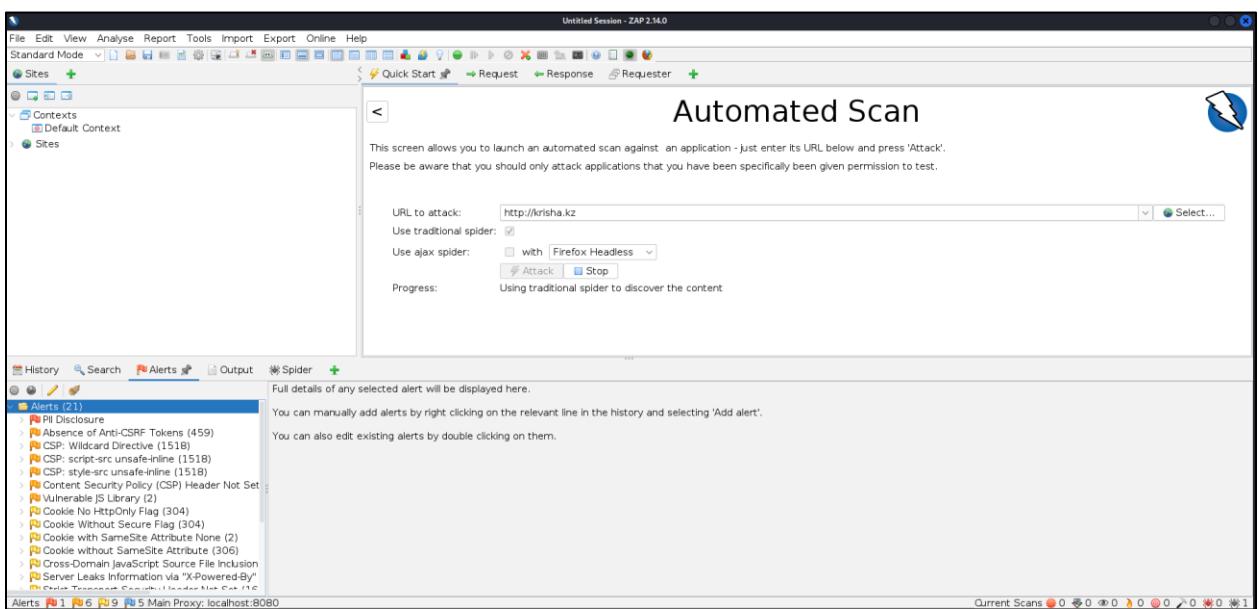
```
(kali㉿kali)-[~]
└─$ sudo nikto -h krisha.kz
[sudo] password for kali:
    Nikto v2.5.0

+ Multiple IPs found: 185.143.129.90, 185.143.129.89
+ Target IP:          185.143.129.90
+ Target Hostname:   krisha.kz
+ Target Port:        80
+ Start Time:        2024-04-25 21:07:08 (GMT5.5)

+ Server: nginx
+ /: 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://krisha.kz/
+ No CGI Directories found (use '-c all' to force check all possible dirs)
-C all
- STATUS: Completed 380 requests (~5% complete, 35.8 minutes left); currently in plugin 'Site Files'
- STATUS: Running average: 100 requests: 0.38515 sec, 10 requests: 0.3868 sec.
+ 7964 requests: 0 error(s) and 2 item(s) reported on remote host
+ End Time:        2024-04-25 22:00:08 (GMT5.5) (3180 seconds)

+ 1 host(s) tested
```

Scanning with Zap



Absence of Anti-CSRF Tokens

URL: http://krisha.kz
Risk: Medium
Confidence: Low

Parameter: cookie
Evidence: <form id="search-form" action="/prodazha/kvartiry/" method="get">
CWE ID: 352
WASC ID: 9
Source: Passive (10202 - Absence of Anti-CSRF Tokens)
Input Vector:
Description: No Anti-CSRF tokens were found in a HTML submission form.
A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast,
Other Info: No known Anti-CSRF token [`anticsrf_CSRFToken__RequestVerificationToken`, `csrfmiddlewaretoken`, `authenticity_token`, `OWASP_CSRFTOKEN`, `anoncsrf csrf_token csrf_secret csrf_magic`, `CSRF_token csrf_token`] was found in the following HTML form: [Form 1: "das[sys.fromAgent]checkbox-0" "das[sys.hasphoto]checkbox-0" "das[com.square][from]" "das[com.square][to]" "das[land.square][from]" "das[land.square][to]" "das[price][from]" "das[price][to]" "das[who]checkbox-0" "novostroiki-checkbox-0" "region"].
Solution: Phase: Architecture and Design
Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.
For example, use anti-CSRF packages such as the OWASP CSRFGuard.
Reference: <http://projects.webappsec.org/Cross-Site-Request-Forgery> <https://cwe.mitre.org/data/definitions/352.html>

Alert Tags:	Key	Value
OWASP_2021_A01		https://owasp.org/Top10/A01_2021-Broken_Access_Control/
WSTG-v42-SESS-05		https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/Broken_Access_Control
OWASP_2017_A05		https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html

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.
- ❖ UseNonce 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)

The screenshot shows a browser window with the URL <https://bugcrowd.com/soundcloud>. The page title is "SoundCloud". Below it, a sub-headline states: "SoundCloud is the world's largest open audio platform. With over 200 million tracks from 20 million creators heard in 190 countries, what's next in music is first on SoundCloud." A reward section indicates "\$200 – \$4,500 per vulnerability" and "Safe harbor". On the right, there is a large orange button featuring the SoundCloud logo. At the bottom left, there is a "Submit report" button and a "Do you like this program?" poll with thumbs up and down icons.

Addressing the target

The screenshot shows the official SoundCloud homepage. It features a large banner with two artists: Sofaygo and Ela Minus. The banner text reads: "Connect on SoundCloud. Discover, stream, and share a constantly expanding mix of music from emerging and major artists around the world." Below the banner is a "Sign up for free" button. A search bar at the top allows users to "Search for artists, bands, tracks, podcasts" or "Upload your own". Below the search bar, a section titled "Hear what's trending for free in the SoundCloud community" displays several thumbnail images of tracks, including one for "c euphoria" and another for "FAMILY".

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 culture. With over 250 million tracks from 30 million artists from 193 countries on SoundCloud, SoundCloud is one of the largest audio discovery platforms in the world.

Scope

The screenshot shows a list of in-scope targets for the SoundCloud domain. At the top, there are four color-coded boxes representing different price ranges: P1 (\$400 - \$4500), P2 (\$1500 - \$1750), P3 (\$600 - \$850), and P4 (\$200 - \$250). A green button labeled 'In scope' is visible. Below the boxes, a note states: "The below mentioned targets are in-scope. We serve different webpages and API endpoints (api-*.soundcloud.com) on our subdomains. All these sub-domains are in scope, if not explicitly listed in the out of scope section." The list includes:

- soundcloud.com: Ruby, ReactJS, Scala, +1
- *.soundcloud.com: API Testing, Ruby, ReactJS, +2
- api-* soundcloud.com: API Testing
- SoundCloud Android app: Java, Mobile Application..., Kotlin
- SoundCloud iOS app: Objective-C, Swift, Mobile Application...
- *.soundcloud.org: Website Testing
- soundcloud.org: Website Testing
- artists.soundcloud.com: ReactJS, Website Testing, NodeJS, +1
- *.services.repostnetwork.com: API Testing, Java, jQuery, +1
- *.s-cloud.net: Website Testing

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

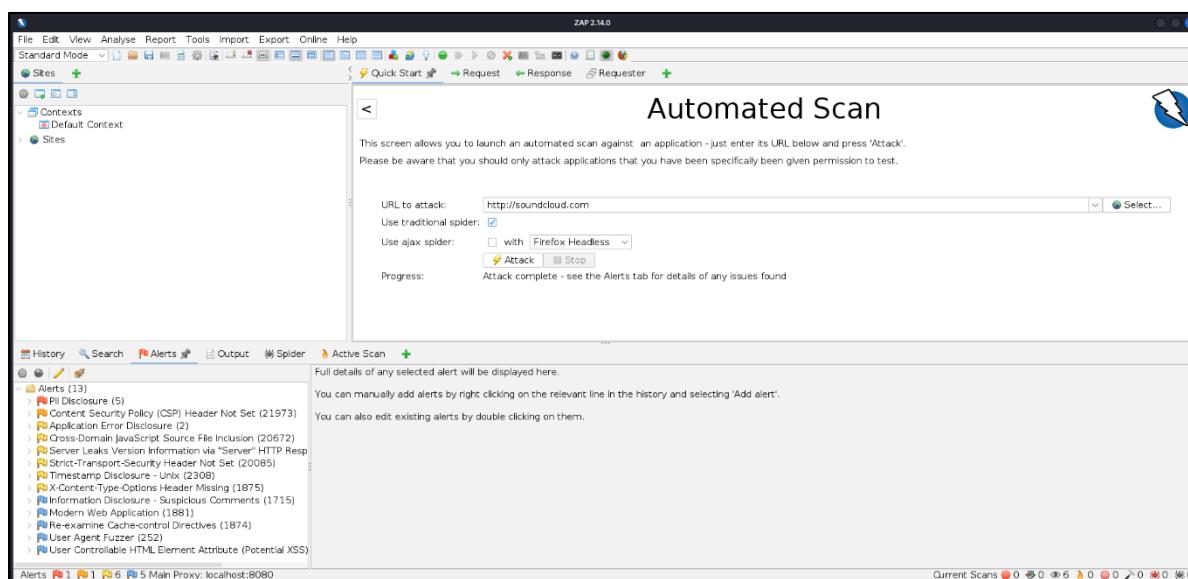
```
[+] (kali㉿kali) [-] $ sudo nikto -h soundcloud.com
[sudo] password for kali:
- Nikto v2.5.0

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 6ddf55dbf1d9a646bfcdb46cd89472.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
+ Site Map types found:
  Root page / redirects to: https://soundcloud.com/
  /wsmans/: 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 Vulnerabilities

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 browsers.

8.Picsart (Report 8)

The screenshot shows the HackerOne platform interface for the 'Picsart' team. At the top, there's a navigation bar with a shield icon, a lock icon, the URL 'https://hackerone.com/picsart?type=team', a zoom level indicator '80%', and several other icons. Below the header, the 'Picsart' logo is displayed, followed by a brief description: 'Picsart is an all-in-one photo and video editing app for making the social content pop.' A 'Submit report' button is prominently featured. To the right, there's a section titled 'Vulnerability Disclosure Program' with the note 'Launched in Feb 2020' and a 'Managed by HackerOne' badge. On the left, there are two status boxes: 'Reports resolved 47' and 'Assets in scope 18'. On the right, there are links for 'Give feedback', 'Bookmark', and 'Subscribe'. The overall theme is dark with purple and white text.

Addressing the target

The screenshot shows the official Picsart website. At the top, the 'Picsart' logo is on the left, and a navigation bar with links like 'Create', 'Editing tools', 'Templates', 'Design library', 'Enterprise', 'Learning & Support', and 'Pricing' is on the right. There's also a search icon, a 'Start free trial' button, and a 'Log in' button. Below the navigation, two 'Editor's Choice' awards from the App Store and Google Play are shown. The main headline reads 'Supercharge your creativity' in large, bold, purple and black text. A subtext below it says, 'The only AI-powered creative companion you'll ever need to grow your brand. Get it all done with Picsart's ultimate creative suite.' A 'Get started for free' button is at the bottom of this section. The overall design is clean with a white background and purple accents.

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	⑤ Ineligible	Aug 23, 2023	0 (0%)
video-api.picsart.io	Domain	In scope	Critical	⑤ Ineligible	Aug 23, 2023	0 (0%)
revenue-tracking.picsart.io	Domain	In scope	Critical	⑤ Ineligible	Aug 23, 2023	0 (0%)
demo.sdk.picsart.io	Domain	In scope	Critical	⑤ Ineligible	Aug 23, 2023	0 (0%)
cdn-basic-content-api.picsart.io	Domain	In scope	Critical	⑤ Ineligible	Aug 23, 2023	0 (0%)
t.picsart.com	Domain	In scope	Critical	⑤ Ineligible	Aug 23, 2023	0 (0%)
stage.optifyr.com	Domain	In scope	Critical	⑤ Ineligible	Aug 23, 2023	0 (0%)
optifyr.com	Domain	In scope	Critical	⑤ Ineligible	Aug 23, 2023	0 (0%)
upload.picsart.com	Domain	In scope	Critical	⑤ Ineligible	Aug 23, 2023	0 (0%)
console.picsart.io	Domain	In scope	Critical	⑤ Ineligible	Aug 23, 2023	0 (0%)
api.picsart.io	Domain	In scope	Critical	⑤ Ineligible	Jun 10, 2022	0 (0%)
9WZDNCRFJ10M	Windows: Microsoft Store	In scope	Critical	⑤ Ineligible	Jun 10, 2022	0 (0%)
587366035	iOS: App Store	In scope	Critical	⑤ Ineligible	Feb 17, 2020	0 (0%)
ai.picsart.com	Domain	In scope	Critical	⑤ Ineligible	Aug 17, 2023	0 (0%)
picsart.io	Domain	In scope	Critical	⑤ Ineligible	Aug 29, 2022	0 (0%)
www.picsart.com	Domain	In scope	Critical	⑤ Ineligible	Jun 23, 2021	0 (0%)
api.picsart.com	Domain	In scope	Critical	⑤ Ineligible	Aug 23, 2023	0 (0%)
com.picsart.studio	Android: Play Store	In scope	Critical	⑤ 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

```
└─[kali㉿kali]-[~]
$ sudo nmap -sS picsart.com
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-27 14:53 +0530
Nmap scan report for picsart.com (162.159.137.44)
Host is up (0.0074s latency).
Other addresses for picsart.com (not scanned): 162.159.136.44
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 4.66 seconds
```

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 'setcf.bm' cookie. The IP is "1.0.1.1".
+ /: IP address found in the 'setcookie' 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://optimizely.com>; rel="preconnect". See: https://www.drupal.org/web-security-best-practices/preloading-content-type-header/
+ /: 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-security-best-practices/preloading-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
STATS: Completed 7962 requests: currently in plugin 'Nikto Tests'
STATUS: Running average: 100 requests / 100.4 sec; 10 headers / 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 errors(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

The screenshot shows the ZAP interface during an automated scan. The main window displays the 'Automated Scan' configuration with the URL `http://picsart.com` entered. Below the configuration, the 'Alerts' tab is selected, showing a list of 23 detected vulnerabilities. The findings include common security issues such as CSRF protection absence, CSP misconfigurations, and various cookie handling problems.

Category	Count
Absence of Anti-CSRF Tokens	1
CSP: Wildcard Directive	1
Content Security Policy (CSP) Header Not Set	1
Hidden File Found	4
Missing Anti-clickjacking Header	41
Vulnerable JS Library	1
Cookie No HttpOnly Flag	6
Cookie Without Secure Flag	6
Cookie with SameSite Attribute None	3
Cookie without SameSite Attribute	6
Cross-Domain JavaScript Source File Inclusion	1
Server Leaks Information via "X-Powered-By"	1
Strict-Transport-Security Header Not Set	75
Timestamp Disclosure - Unix	53
X-Content-Type-Options Header Missing	63
Content-Type Header Missing	8
Information Disclosure - Suspicious Comments	1
Modern Web Application	50
Re-examine Cache-control Directives	36
Retrieved from Cache	14
Session Management Response Identified	6
User Agent Fuzzer	36
User Controllable HTML Element Attribute (Pot)	1

This is a detailed view of the 'Alerts' list in ZAP. The list contains 23 items, each with a severity icon (orange) and a brief description. The findings are categorized as follows:

- Absence of Anti-CSRF Tokens (1)
- CSP: Wildcard Directive (1)
- Content Security Policy (CSP) Header Not Set (1)
- Hidden File Found (4)
- Missing Anti-clickjacking Header (41)
- Vulnerable JS Library (1)
- Cookie No HttpOnly Flag (6)
- Cookie Without Secure Flag (6)
- Cookie with SameSite Attribute None (3)
- Cookie without SameSite Attribute (6)
- Cross-Domain JavaScript Source File Inclusion (1)
- Server Leaks Information via "X-Powered-By" (1)
- Strict-Transport-Security Header Not Set (75)
- Timestamp Disclosure - Unix (53)
- X-Content-Type-Options Header Missing (63)
- Content-Type Header Missing (8)
- Information Disclosure - Suspicious Comments (1)
- Modern Web Application (50)
- Re-examine Cache-control Directives (36)
- Retrieved from Cache (14)
- Session Management Response Identified (6)
- User Agent Fuzzer (36)
- User Controllable HTML Element Attribute (Pot) (1)

Identified Vulnerabilities

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.

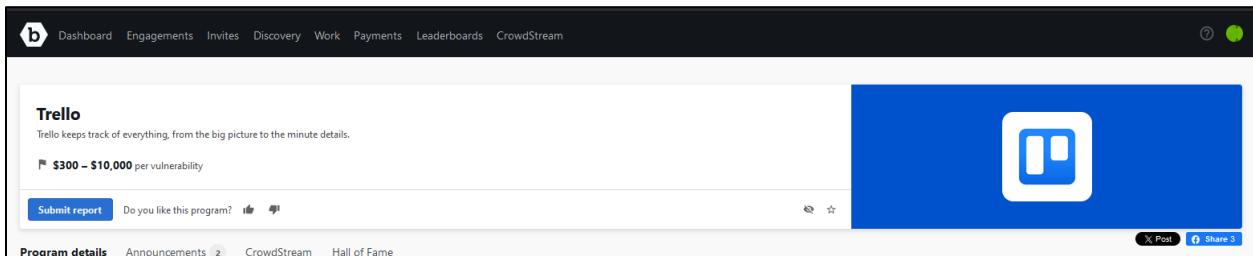
- ❖ Security Risks: Without anti-clickjacking headers, websites cannot avoid clickjacking attacks, which means that legitimate webpages may have layers of harmful material between them and their visitors.
- ❖ Data Exposure: An example of clickjacking is exposing the user to the risk of accidental divulgence 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

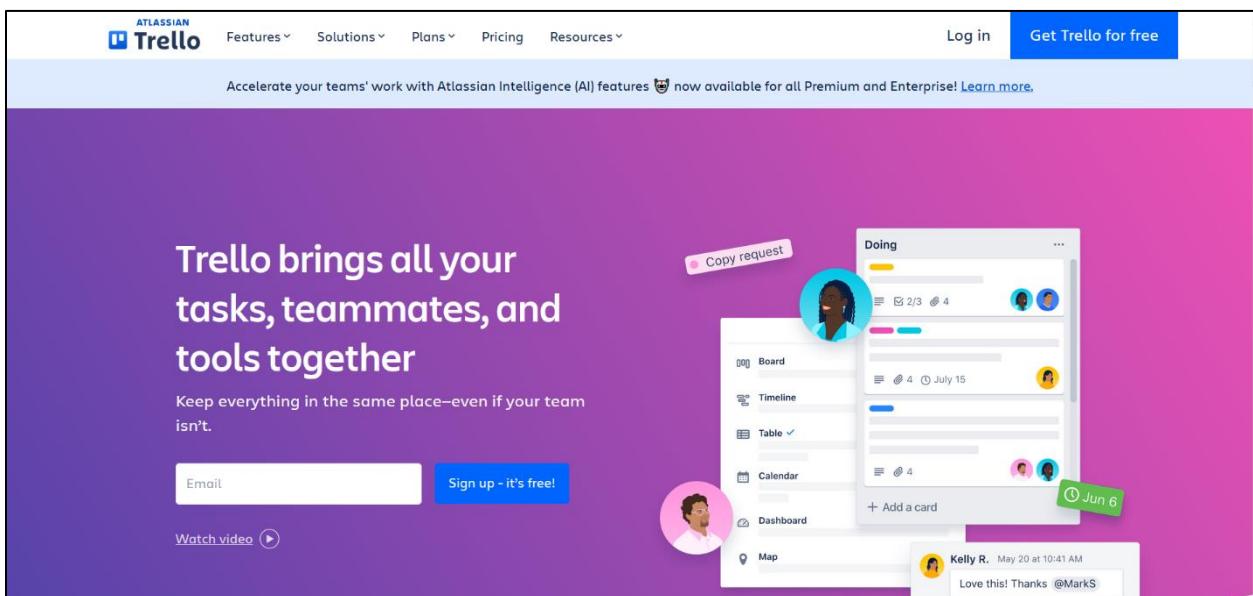
To prevent Attackers from exploiting “Missing anti clickjacking header” there are some steps that can be followed.

- ❖ 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

P1 \$10000 **P2** \$3600 **P3** \$1200 **P4** \$300 **In scope**

Scope Item	Tags
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 Application... +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

Scope Item	Notes	Tags
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

```
Trash

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for trello.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
[-] Total Unique Subdomains Found: 20
www.trello.com
api.trello.com
api-gateway.trello.com
www.api-gateway.trello.com
blog.trello.com
br.blog.trello.com
brtest.blog.trello.com
c.trello.com
design.trello.com
developers.trello.com
help.trello.com
info.trello.com
mgo.trello.com
sptrack.trello.com
static.trello.com
status.trello.com
support.trello.com
tech.trello.com
temp-test-aklf390785sjfkl.trello.com
timezone.trello.com
```

Sublist3r was able to find 20 uniques sub domains.

Selected - trello.com

Scanning for open ports with Nmap

```
(kali㉿kali)-[~]
└─$ sudo nmap -sS trello.com
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-27 15:00 +0530
Nmap scan report for trello.com (108.157.254.49)
Host is up (0.012s latency).
Other addresses for trello.com (not scanned): 108.157.254.33 108.157.254.93 108.157.254.128
rDNS record for 108.157.254.49: server-108-157-254-49.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 5.52 seconds
```

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.
+ 7952 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

The screenshot shows the ZAP interface with an 'Automated Scan' in progress. The URL 'http://trello.com' is entered in the 'URL to attack' field. The 'Attack' button is highlighted. The 'Alerts' tab is selected, displaying 231 findings, including 145 PII Disclosure alerts. One specific alert is expanded, detailing a 'Hidden File Found' issue at <https://trello.com/search>. The alert has a 'High' risk rating and is from 'Evidence: 67992294949306657'. The 'Attack' button is also visible here.

This screenshot shows the detailed view of a 'Hidden File Found' alert. The alert is triggered by a request to <https://atlassian.com/slurm?application=trello&continue=https%3A%2F%2Ftrello.com%2Fauth%2Fatlassian%2Fcallback%3Fdisplay%3DryZjpb25TdjhGvneSl6hNvZnQifQ%253D%253D%26createMember%3Dtrue&display=eyJ2Zjpb25TdjhGvneSl6hNvZnQifQ%3D%3D>. The alert has a 'Medium' risk rating and is from 'Evidence: 319'. It includes a 'Solution:' section suggesting using HTTPS for landing pages that host secure forms.

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 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

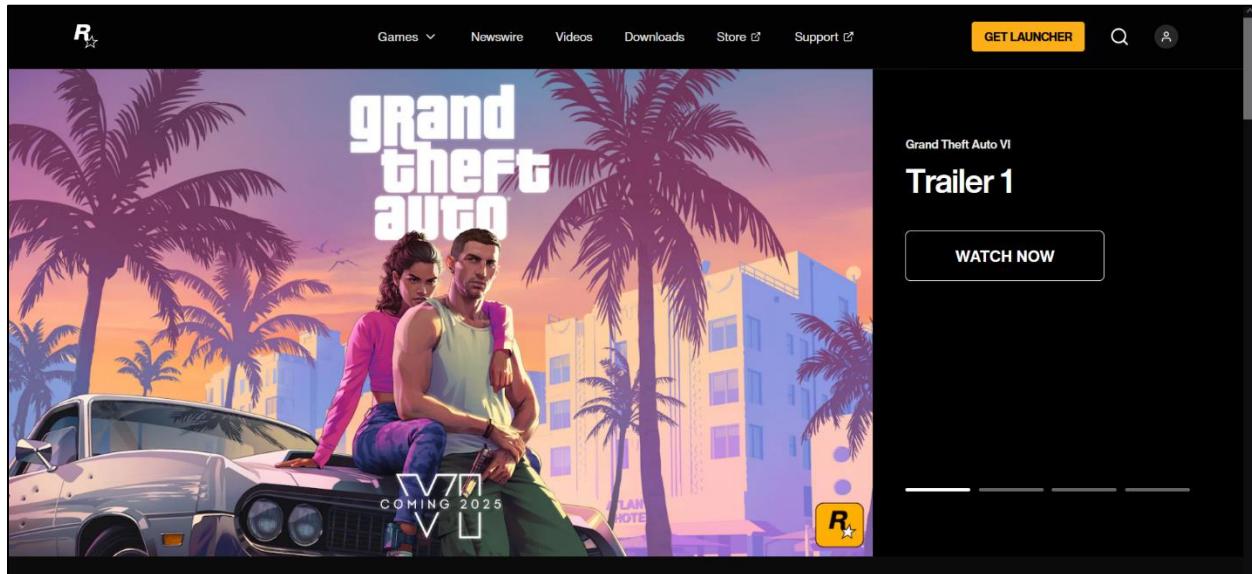
To prevent this from happening following steps can be taken

- ❖ 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 whether 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 submission such as Css or Js should be updated to load with HTTPS

10.Rockstar Games (Report 10)

The screenshot shows the Rockstar Games profile on the HackerOne platform. The page includes the company logo, a brief description of their popular games (Grand Theft Auto, Max Payne, Red Dead Redemption, L.A. Noire, Bully & more), and links to their website and social media. It also displays metrics like reports resolved (0), assets in scope (9), and average bounty (\$500). A pink 'Submit report' button is prominent. To the right, there's information about the Bug Bounty Program, which was launched in March 2017, and options to manage it, include retesting, and enable collaboration.

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 goes 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

```
(kali㉿kali)-[~]
$ sublist3r -d rockstargames.com

File System
S U B D O M A I N S
# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for rockstargames.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
[-] Total Unique Subdomains Found: 229
www.rockstargames.com
5034118b6d9f602e-speed-uw2.rockstargames.com
987f803ce6c4aec6-speed-ew1.rockstargames.com
Lyncdiscover.rockstargames.com
autodiscover.rockstargames.com
```

Subfinder was able to 229 unique subdomains.

Selected domain – rockstargames.com

Open Ports

```
(kali㉿kali)-[~]
$ sudo nmap -sS rockstargames.com
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-27 14:08 +0530
Nmap scan report for rockstargames.com (23.15.24.13)
Host is up (0.016s latency).
rDNS record for 23.15.24.13: a23-15-24-13.deploy.static.akamaitechnologies.com
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
113/tcp   closed ident
443/tcp   open  https
8008/tcp  open  http
8010/tcp  open  xmpp

Nmap done: 1 IP address (1 host up) scanned in 11.17 seconds
```

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 'akami-grn' found, with contents: 0.0d284b17.1713414830.10176071.
+ /: 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
```

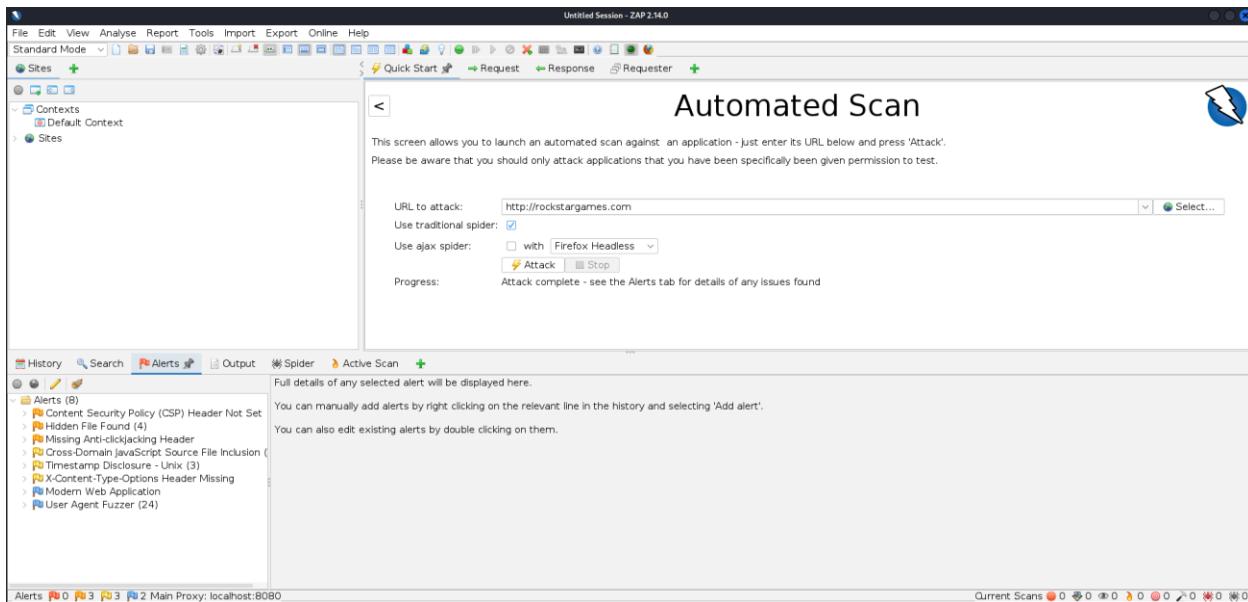
Scanning with Burp suite

The screenshot shows the Burp Suite Professional interface. The top navigation bar includes Project, Intruder, Repeater, View, Help, and several tabs like Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Comparer, Logger, Organizer, Extensions, and Learn. The main window is divided into several panels:

- Tasks:** Shows three active tasks:
 - Capturing:** 0 responses processed, 0 responses queued.
 - 2. Live audit from Proxy (all traffic):** Audit checks - passive, Issues: 0, 0 requests (0 errors).
 - 3. Crawl and audit of rockstargames.com:** Crawl and Audit - Fast, Issues: 1, 350 requests (3 errors), 0 locations crawled.
- Issue activity:** A table listing findings:

#	Task	Time	Action	Issue type	Host
3	3	22:59:08 7 May 2024	Issue found	External service interaction (DNS)	http://rockstargame... /
2	3	22:56:13 7 May 2024	Issue found	TLS certificate	https://rockstargame... /
1	3	22:56:12 7 May 2024	Issue found	Strict transport security not enforced	https://rockstargame... /robots.txt
- Event log:** A table of log entries showing audit and crawl progress.
- Advisory:** A detailed view of the "Strict transport security not enforced" issue, including severity (Low), confidence (Certain), host (https://rockstargames.com), and path (/robots.txt). It also includes an "Issue description" section explaining the vulnerability.

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/>