Sri Lanka Institute of Information Technology

IE2072 – WEB SECURITY

Year 2, Semester 2

(Assignment – Individual)-2025

_Bug Bounty Report _

Student Register Number	Student Name
IT23245488	MADUGASWATHTHA A S

Table of Contents

ACKNOLEDGEMENT 3

ABSTRACT 4

WHAT IS OWSPS TOP 10 VULNERABILITIES 5

OWSPS TOP 10 VULNERABILITIES. 6

REPORT 01 7

IN SCOPE 8

REPORT 02 12

REPORT 03 16

REPORT 04 21

REPORT 05 25

REPORT 06 29

REPORT 07 33

REPORT 08 37

REPORT 09 41

REPORT 10 45

ACKNOLEDGEMENT

As a second semester student at SLIIT majoring in cyber security, I (MADUGASWATHTHA A S) was able to take the course Web Security. I was given the task of researching Web Audit as the subject. I received guidance and help from several specialists in order to lead to a great conclusion. I benefited much from the information I learned during the lecture series. This appreciation is extended to Ms.Ayesha Wijesooriya. I appreciate the advice and assistance you provided so that I could complete the task with complete assurance. My family and coworkers, who assisted and provided assistance in several ways, have my sincere gratitude.

ABSTRACT

Through bug bounty programs, businesses may crowdsource security testing to find and fix flaws. Although the idea of crowdsourcing security testing is relatively new, the fundamental origins may be found in penetration testing efforts. In the past five years, bug bounty schemes have begun to take off in the information security sector. Evaluations of both bug bounty programs and the platforms they are run on are necessary as bug bounty programs continue to spread. This study looked into the development, upkeep, and viability of bug bounty schemes. The bulk of bug bounty programs are managed by a small number of bug bounty platforms. These systems might be difficult to set up initially and keep up, but they provide many security advantages to any firm willing to use them. The results of this study finally showed that a bug reward oversight committee was required, and that there should be more public vulnerability reports.Most often, hackers taking part in bug bounty schemes are hired to find vulnerabilities. Since 2015, programs advertised on bug bounty sites like HackerOne have been responsible for the discovery of tens of thousands of vulnerabilities. As of July 2020, these platforms feature over 200 publicly listed programs. We provide the findings of an empirical research that was conducted utilizing data from two bug bounty platforms in order to comprehend the expenses and advantages of bug bounty programs for both individuals and organizations. We examine the costs and advantages of running bug bounty programs as well as the incentives offered to hackers who contribute to the discovery of vulnerabilities. The average expense of running a bug bounty program for a year is now less than the cost of hiring 2 additional software engineers.

What is OWSPS top 10 vulnerabilities

OWASP creates an updated compilation of the top 10 web application risks every three to four years. The management team uses Open Web Application Security Project as its formal designation. OWASP releases documents that present the ten most dangerous web application threats with descriptions highlighting how they affect web applications and how organizations can prevent them. OWASP stands as a nonprofit organization which dedicates its resources to better internet application security. The complete list was created through information gathered from multiple specialized sources like security consultants and security suppliers and security teams representing different kinds of businesses. The safety management tool stands as an essential practice instrument for online application security standards.

Application developers and security teams are now using the following OWASP TOP 10 web vulnerabilities:

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXE)
5. Broken Access Control
6. Security Misconfiguration
7. Cross-Site Scripting
8. Insecure Deserialization
9. Using Components with Known Vulnerabilities
10. Insufficient Logging and Monitoring

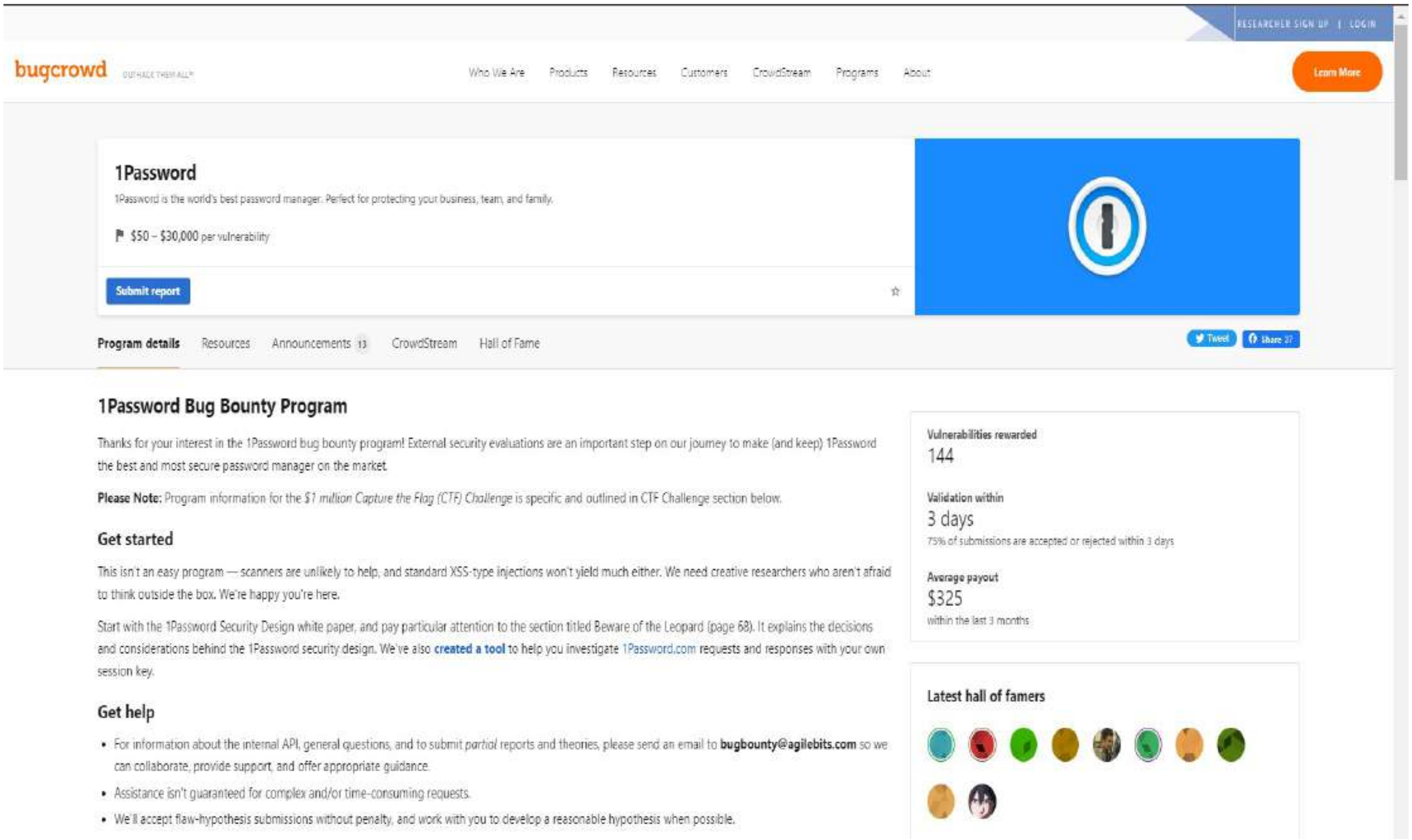
OWSPS top 10 vulnerabilities

1. The insertion of illicit data into command inquiries or queries produces an injection fault which grants attackers unrestricted control of databases or data access privileges.
2. Unsecured authentication mechanisms that include poor session management policies and weak password storage practices and flawed credential management generate entry points for unauthorized users who endanger user account security.
3. Sensitive data exposure occurs through poor encryption and bad storage practices as well as unsecured transfer methods which culminates in sensitive data disclosure.
4. XML External Entities (XXE) vulnerabilities appear when XML inputs receive improper processing from applications which enables attackers to obtain private files and execute server-side request forgery attacks (SSRF) and run unwanted code.
5. Impaired access control systems lead to unauthorized access of sensitive information and restricted features when authorization verification fails to occur.
6. Security misconfigurations cause various deficiencies by creating vulnerabilities from imprecise system configuration which lets sensitive data become exposed together with inactive functionalities and default setup parameters.
7. XSS flaws enable hackers to embed harmful scripts inside web pages thereby exposing other users to data theft and session hijackings or page defacement attacks.
8. The security vulnerability in insecure deserialization enables hackers to modify serialized objects and results in remote code execution or denial of service attacks and data manipulation incidents.
9. Amino acid sequences bearing known vulnerabilities within their components (such as libraries or frameworks) make applications susceptible to both known vulnerabilities and attacks.
10. A lack of complete logging systems combined with inadequate monitoring makes it difficult to detect security issues thus allowing attackers additional time to create damage.

Report 01

1password.com

Scope of the security audit according to https://hackerone.com/crowdstrike/policy_scopes is as follows,



1Password

1Password is the world's best password manager. Perfect for protecting your business, team, and family.

$50 – $30,000 per vulnerability

1Password Bug Bounty Program

Thanks for your interest in the 1Password bug bounty program! External security evaluations are an important step on our journey to make (and keep) 1Password the best and most secure password manager on the market.

Please Note: Program information for the *$1 million Capture the Flag (CTF) Challenge* is specific and outlined in CTF Challenge section below.

Get started

This isn't an easy program — scanners are unlikely to help, and standard XSS-type injections won't yield much either. We need creative researchers who aren't afraid to think outside the box. We're happy you're here.

Start with the 1Password Security Design white paper, and pay particular attention to the section titled Beware of the Leopard (page 68). It explains the decisions and considerations behind the 1Password security design. We've also **created a tool** to help you investigate 1Password.com requests and responses with your own session key.

Get help

- For information about the internal API, general questions, and to submit *partial* reports and theories, please send an email to **bugbounty@agilebits.com** so we can collaborate, provide support, and offer appropriate guidance.
- Assistance isn't guaranteed for complex and/or time-consuming requests.
- We'll accept flaw-hypothesis submissions without penalty, and work with you to develop a reasonable hypothesis when possible.

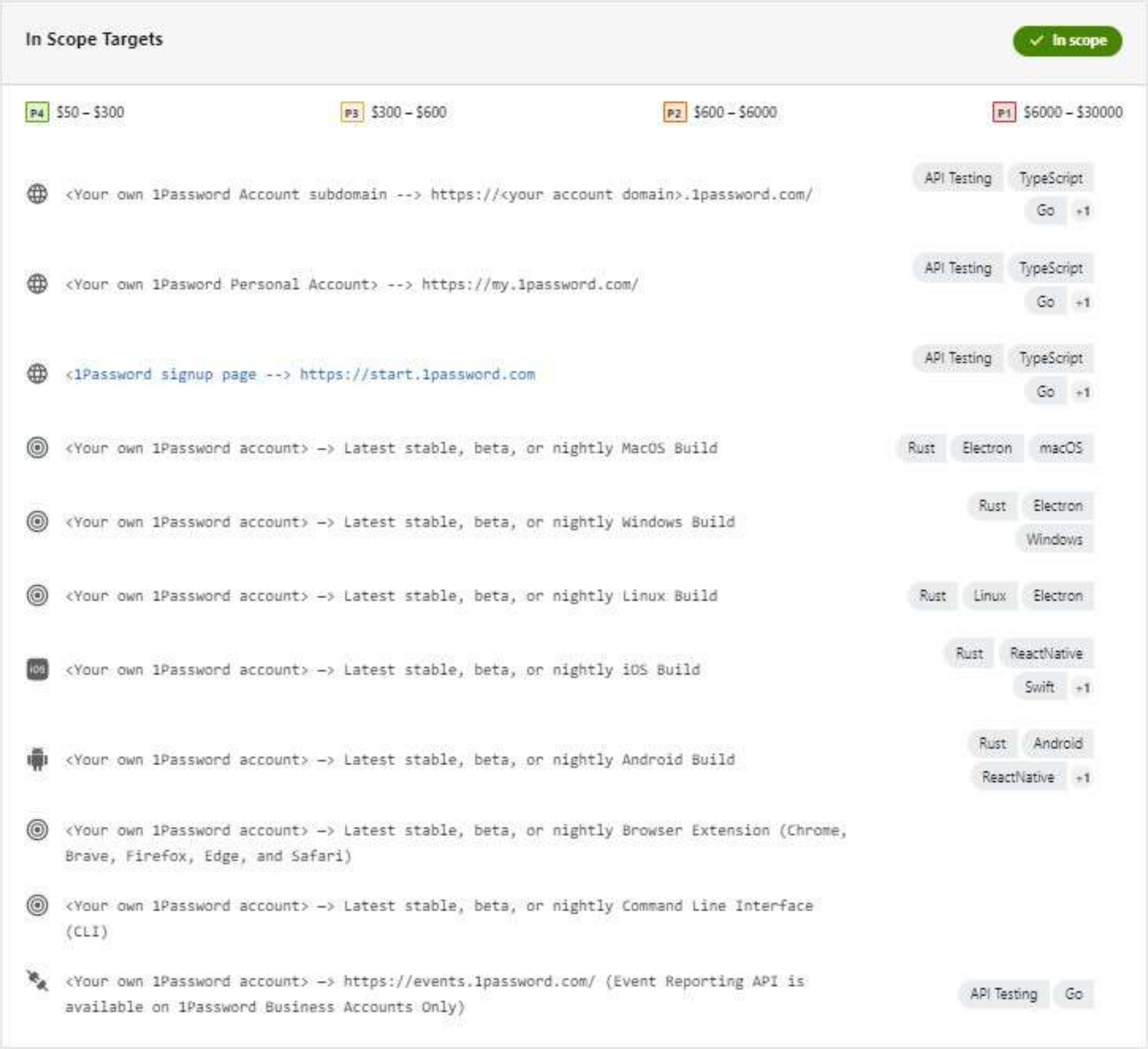
Vulnerabilities rewarded
144

Validation within
3 days
75% of submissions are accepted or rejected within 3 days

Average payout
$325
within the last 3 months

Latest hall of famers

In Scope

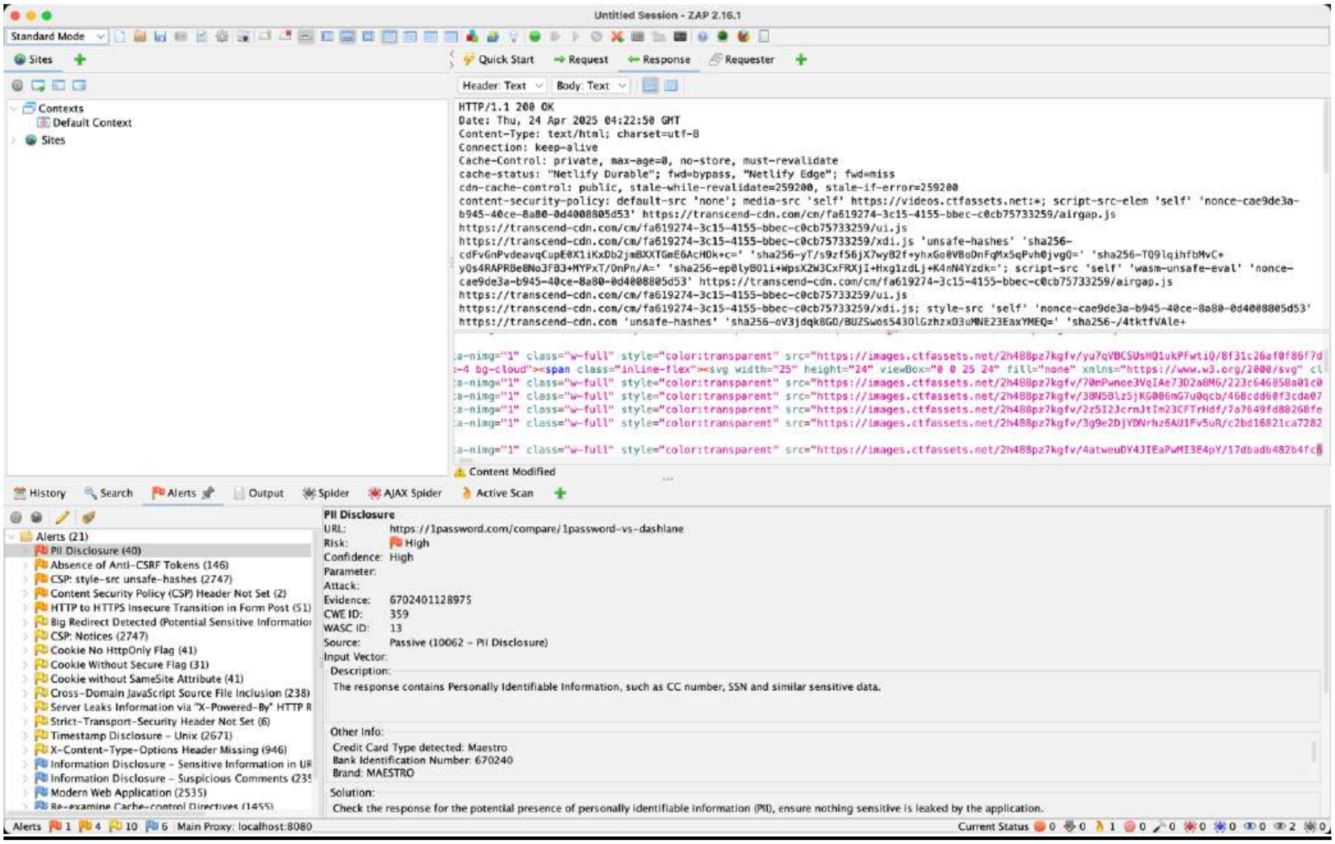


In Scope Targets ✓ In scope

P4 $50 – $300   P3 $300 – $600   P2 $600 – $6000   P1 $6000 – $30000

<Your own 1Password Account subdomain --> https://<your account domain>.1password.com/	API Testing TypeScript Go +1
<Your own 1Pasword Personal Account> --> https://my.1password.com/	API Testing TypeScript Go +1
<1Password signup page --> https://start.1password.com	API Testing TypeScript Go +1
<Your own 1Password account> –> Latest stable, beta, or nightly MacOS Build	Rust Electron macOS
<Your own 1Password account> –> Latest stable, beta, or nightly Windows Build	Rust Electron Windows
<Your own 1Password account> –> Latest stable, beta, or nightly Linux Build	Rust Linux Electron
<Your own 1Password account> –> Latest stable, beta, or nightly iOS Build	Rust ReactNative Swift +1
<Your own 1Password account> –> Latest stable, beta, or nightly Android Build	Rust Android ReactNative +1
<Your own 1Password account> –> Latest stable, beta, or nightly Browser Extension (Chrome, Brave, Firefox, Edge, and Safari)	
<Your own 1Password account> –> Latest stable, beta, or nightly Command Line Interface (CLI)	
<Your own 1Password account> –> https://events.1password.com/ (Event Reporting API is available on 1Password Business Accounts Only)	API Testing Go

Scanned Vulnerabilities Using ZAP



```
HTTP/1.1 200 OK
Date: Thu, 24 Apr 2025 04:22:50 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Cache-Control: private, max-age=0, no-store, must-revalidate
cache-status: "Netlify Durable"; fwd=bypass, "Netlify Edge"; fwd=miss
cdn-cache-control: public, stale-while-revalidate=259200, stale-if-error=259200
content-security-policy: default-src 'none'; media-src 'self' https://videos.ctfassets.net:*; script-src-elem 'self' 'nonce-cae9de3a-
b945-40ce-8a80-0d4008805d53' https://transcend-cdn.com/cm/fa619274-3c15-4155-bbec-c0cb75733259/airgap.js
https://transcend-cdn.com/cm/fa619274-3c15-4155-bbec-c0cb75733259/ui.js
https://transcend-cdn.com/cm/fa619274-3c15-4155-bbec-c0cb75733259/xdi.js 'unsafe-hashes' 'sha256-
cdFvGnPvdeavqCupE0X1iKxDb2jmBXXTGmE6AcHOk+c=' 'sha256-yT/s9zf56jX7wyB2f+yhxGo0VBoDnFqMx5qPvh0jvgQ=' 'sha256-TQ9lqihfbMvC+
yOs4RAPRBe8No3FB3+MYPxT/OnPn/A=' 'sha256-ep0lyB01i+WpsX2W3CxFRXjI+Hxg1zdLj+K4nN4Yzdk='; script-src 'self' 'wasm-unsafe-eval' 'nonce-
cae9de3a-b945-40ce-8a80-0d4008805d53' https://transcend-cdn.com/cm/fa619274-3c15-4155-bbec-c0cb75733259/airgap.js
https://transcend-cdn.com/cm/fa619274-3c15-4155-bbec-c0cb75733259/ui.js
https://transcend-cdn.com/cm/fa619274-3c15-4155-bbec-c0cb75733259/xdi.js; style-src 'self' 'nonce-cae9de3a-b945-40ce-8a80-0d4008805d53'
https://transcend-cdn.com 'unsafe-hashes' 'sha256-oV3jdqk8GO/BUZSwos543OlGzhzxD3uMNE23EaxYMEQ=' 'sha256-/4tktfVAle+
```

```
:a-nimg="1" class="w-full" style="color:transparent" src="https://images.ctfassets.net/2h488pz7kgfv/yu7qVBCSUsHQ1ukPFwtiQ/8f31c26af0f86f7d
:-4 bg-cloud"><span class="inline-flex"><svg width="25" height="24" viewBox="0 0 25 24" fill="none" xmlns="https://www.w3.org/2000/svg" cl
:a-nimg="1" class="w-full" style="color:transparent" src="https://images.ctfassets.net/2h488pz7kgfv/70mPwnoe3VqIAe73D2a8M6/223c646858a01c0
:a-nimg="1" class="w-full" style="color:transparent" src="https://images.ctfassets.net/2h488pz7kgfv/38N5Blz5jKG086mG7u0qcb/468cdd60f3cda07
:a-nimg="1" class="w-full" style="color:transparent" src="https://images.ctfassets.net/2h488pz7kgfv/2z5I2JcrnJtIm23CFTrHdf/7a7649fd88268fe
:a-nimg="1" class="w-full" style="color:transparent" src="https://images.ctfassets.net/2h488pz7kgfv/3g9e2DjYDNrhz6AU1Fv5uR/c2bd16821ca7282

:a-nimg="1" class="w-full" style="color:transparent" src="https://images.ctfassets.net/2h488pz7kgfv/4atweuDY4JIEaPwMI3E4pY/17dbadb482b4fc6
```

Alerts (21)
- PII Disclosure (40)
- Absence of Anti-CSRF Tokens (146)
- CSP: style-src unsafe-hashes (2747)
- Content Security Policy (CSP) Header Not Set (2)
- HTTP to HTTPS Insecure Transition in Form Post (51)
- Big Redirect Detected (Potential Sensitive Informatior
- CSP: Notices (2747)
- Cookie No HttpOnly Flag (41)
- Cookie Without Secure Flag (31)
- Cookie without SameSite Attribute (41)
- Cross-Domain JavaScript Source File Inclusion (238)
- Server Leaks Information via "X-Powered-By" HTTP R
- Strict-Transport-Security Header Not Set (6)
- Timestamp Disclosure - Unix (2671)
- X-Content-Type-Options Header Missing (946)
- Information Disclosure - Sensitive Information in UR
- Information Disclosure - Suspicious Comments (235
- Modern Web Application (2535)
- Re-examine Cache-control Directives (1455)

PII Disclosure
URL: https://1password.com/compare/1password-vs-dashlane
Risk: High
Confidence: High
Parameter:
Attack:
Evidence: 6702401128975
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: 670240
Brand: MAESTRO
Solution:
Check the response for the potential presence of personally identifiable information (PII), ensure nothing sensitive is leaked by the application.

Alerts 1 4 10 6 Main Proxy: localhost:8080 Current Status 0 0 1 0 0 0 0 0 2 0

Vulnerability Title Vulnerability Title

- PII Disclosure

Risk type

- High

- PII Disclosure represents a security vulnerability through which personally identifiable information gets revealed to unauthorized users. A response from the application revealed credit card data to OWASP ZAP during its security scan.

Affected Components

- A comparison page located at https://1password.com/compare/1password-vs-dashlane exposes URL as an affected risk vector. Users should avoid viewing the sensitive information found within the HTTP response. Visible HTTP header data indicates that the vulnerability exists within CDN service content delivered by transcend-cdn.com and potentially impacts media content found on images.ctfassets.net.

Impact Assessment

The ZAP scanner issues a "High" rating with "High" confidence for the severity of this vulnerability. The exposure of this PII information can trigger the following possible adverse effects:

- Personal information exposed to identity thieves allows them to commit financial fraud by using the provided credit card information.
- Data protection violations create the risk for organizations to receive monetary penalties and legal disputes that can harm their reputation.
- The disclosure of PII data results in customers losing their trust because organizations fail to safeguard sensitive information.
- Commercial entities could face substantial regulatory financial penalties based on relevant privacy laws such us GDPR along with HIPAA.

Steps to Reproduce

- The detection system marks the data as PII.
- According to the "Content Modified" warning the page content includes the detected sensitive information.

Mitigation

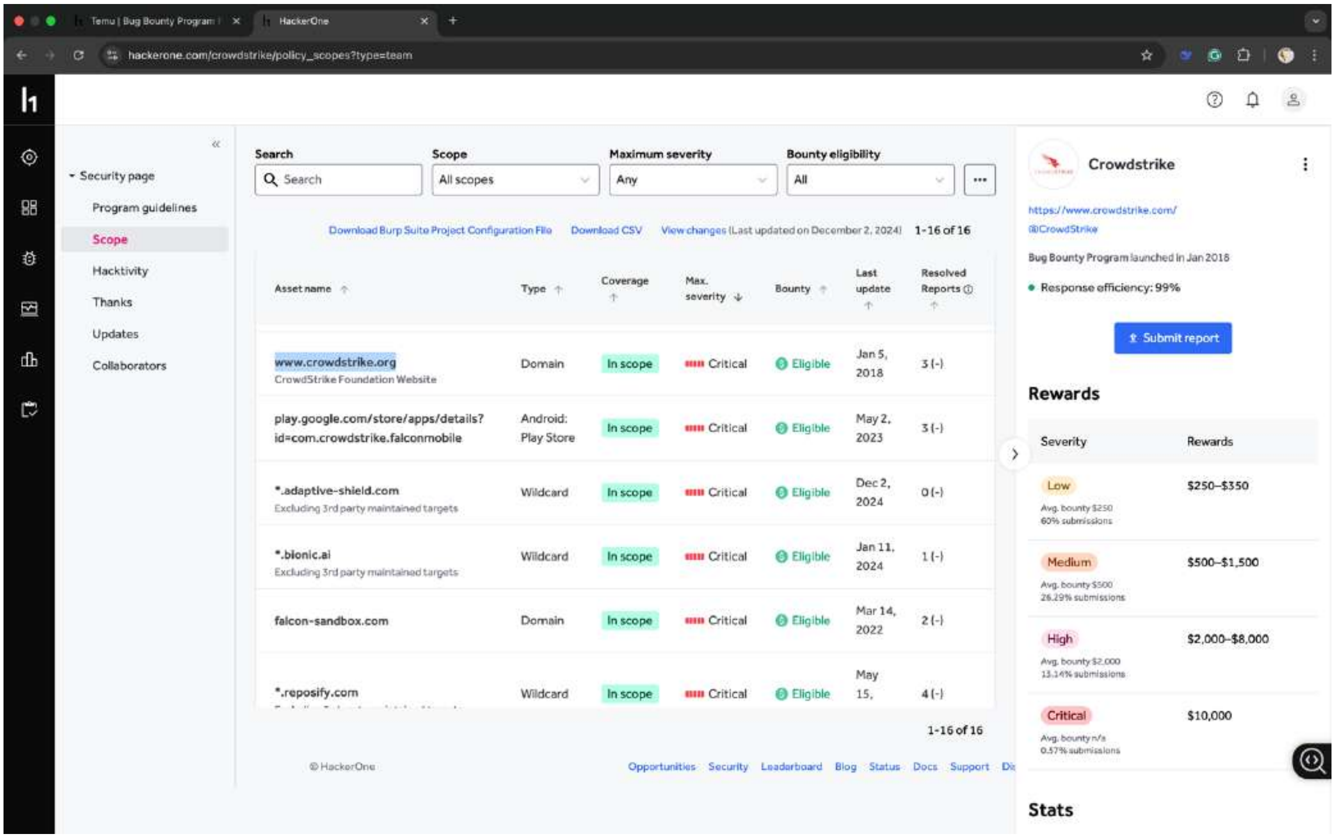
- A four-step mitigation process should be applied to prevent PII disclosure vulnerabilities.
- Data discovery techniques should be implemented to keep sensitive data hidden while it is out of use.
- Strong encryption algorithms must be used to protect both financial information (e.g. credit card details) and all other PII data sets.

- The proper implementation of access controls should accompany PII protection through limiting exposure with authorization management and access restriction.
- Business operations require the minimum amount of PII needed for processing because you should exercise data minimization practices.
- Make sure PII data transmission stays secure through using secure communication protocols (HTTPS) which are set up correctly
- Tests must be conducted to validate that system errors produce messages which avoid revealing sensitive data to users.

Report 02

CrowdStrike

Scope of the security audit according to https://hackerone.com/crowdstrike/policy_scopes is as follows.



hackerone.com/crowdstrike/policy_scopes?type=team

Search: Search | Scope: All scopes | Maximum severity: Any | Bounty eligibility: All

(Last updated on December 2, 2024) 1-16 of 16

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
www.crowdstrike.org CrowdStrike Foundation Website	Domain	In scope	Critical	Eligible	Jan 5, 2018	3 (-)
play.google.com/store/apps/details?id=com.crowdstrike.falconmobile	Android: Play Store	In scope	Critical	Eligible	May 2, 2023	3 (-)
*.adaptive-shield.com Excluding 3rd party maintained targets	Wildcard	In scope	Critical	Eligible	Dec 2, 2024	0 (-)
*.bionic.ai Excluding 3rd party maintained targets	Wildcard	In scope	Critical	Eligible	Jan 11, 2024	1 (-)
falcon-sandbox.com	Domain	In scope	Critical	Eligible	Mar 14, 2022	2 (-)
*.reposify.com	Wildcard	In scope	Critical	Eligible	May 15,	4 (-)

1-16 of 16

Crowdstrike

https://www.crowdstrike.com/

@CrowdStrike

Bug Bounty Program launched in Jan 2018

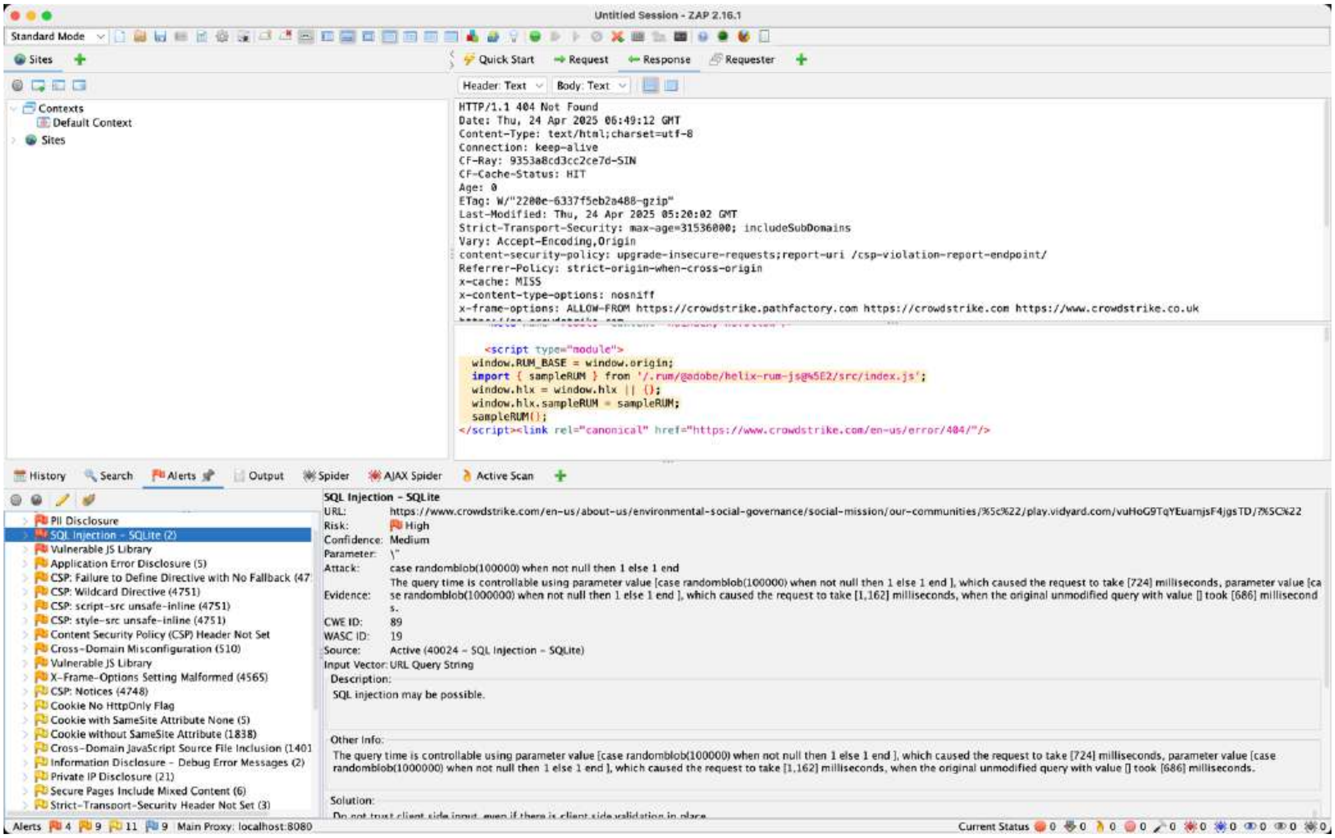
- Response efficiency: 99%

Rewards

Severity	Rewards
Low Avg. bounty $250 60% submissions	$250–$350
Medium Avg. bounty $500 26.29% submissions	$500–$1,500
High Avg. bounty $2,000 13.14% submissions	$2,000–$8,000
Critical Avg. bounty n/a 0.57% submissions	$10,000

Stats

Scanned Vulnerabilities Using ZAP



```
HTTP/1.1 404 Not Found
Date: Thu, 24 Apr 2025 06:49:12 GMT
Content-Type: text/html;charset=utf-8
Connection: keep-alive
CF-Ray: 9353a8cd3cc2ce7d-SIN
CF-Cache-Status: HIT
Age: 0
ETag: W/"2200e-6337f5eb2a488-gzip"
Last-Modified: Thu, 24 Apr 2025 05:20:02 GMT
Strict-Transport-Security: max-age=31536000; includeSubDomains
Vary: Accept-Encoding,Origin
content-security-policy: upgrade-insecure-requests;report-uri /csp-violation-report-endpoint/
Referrer-Policy: strict-origin-when-cross-origin
x-cache: MISS
x-content-type-options: nosniff
x-frame-options: ALLOW-FROM https://crowdstrike.pathfactory.com https://crowdstrike.com https://www.crowdstrike.co.uk
```

```
    <script type="module">
  window.RUM_BASE = window.origin;
  import { sampleRUM } from '/.rum/@adobe/helix-rum-js@%5E2/src/index.js';
  window.hlx = window.hlx || {};
  window.hlx.sampleRUM = sampleRUM;
  sampleRUM();
</script><link rel="canonical" href="https://www.crowdstrike.com/en-us/error/404/"/>
```

- PII Disclosure
- SQL Injection - SQLite (2)
- Vulnerable JS Library
- Application Error Disclosure (5)
- CSP: Failure to Define Directive with No Fallback (47
- CSP: Wildcard Directive (4751)
- CSP: script-src unsafe-inline (4751)
- CSP: style-src unsafe-inline (4751)
- Content Security Policy (CSP) Header Not Set
- Cross-Domain Misconfiguration (510)
- Vulnerable JS Library
- X-Frame-Options Setting Malformed (4565)
- CSP: Notices (4748)
- Cookie No HttpOnly Flag
- Cookie with SameSite Attribute None (5)
- Cookie without SameSite Attribute (1838)
- Cross-Domain JavaScript Source File Inclusion (1401
- Information Disclosure - Debug Error Messages (2)
- Private IP Disclosure (21)
- Secure Pages Include Mixed Content (6)
- Strict-Transport-Security Header Not Set (3)

Alerts 4 9 11 9 Main Proxy: localhost:8080

SQL Injection - SQLite

URL: https://www.crowdstrike.com/en-us/about-us/environmental-social-governance/social-mission/our-communities/%5c%22/play.vidyard.com/vuHoG9TqYEuamjsF4jgsTD/?%5C%22
Risk: High
Confidence: Medium
Parameter: \"
Attack: case randomblob(100000) when not null then 1 else 1 end
Evidence: The query time is controllable using parameter value [case randomblob(100000) when not null then 1 else 1 end], which caused the request to take [724] milliseconds, parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [1,162] milliseconds, when the original unmodified query with value [] took [686] milliseconds.
CWE ID: 89
WASC ID: 19
Source: Active (40024 - SQL Injection - SQLite)
Input Vector: URL Query String

Description:
SQL injection may be possible.

Other Info:
The query time is controllable using parameter value [case randomblob(100000) when not null then 1 else 1 end], which caused the request to take [724] milliseconds, parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [1,162] milliseconds, when the original unmodified query with value [] took [686] milliseconds.

Solution:
Do not trust client side input, even if there is client side validation in place.

Current Status 0 0 0 0 0 0 0 0 0 0

Vulnerability Title Vulnerability Title

- SQL Injection (SQLite)

Risk type

- High

Vulnerability Description

- An SQL injection vulnerability actively affects the CrowdStrike website which lets attackers change database queries through injected SQL code. The SQL injection vulnerability depends on time-based blind SQL injection through SQLite randomblob which allows attackers to extend query execution time for verification purposes. This vulnerability belongs to the SQL Injection category using CWE-89 and WASC-19 standards.

URL

- https://www.crowdstrike.com/en-us/about-us/environmental-social-governance/social-mission/our-communities/

Affected Components

- Web server hosting CrowdStrike's environmental and social governance content
- Backend database system (SQLite database)
- Parameter handling within the URL query string

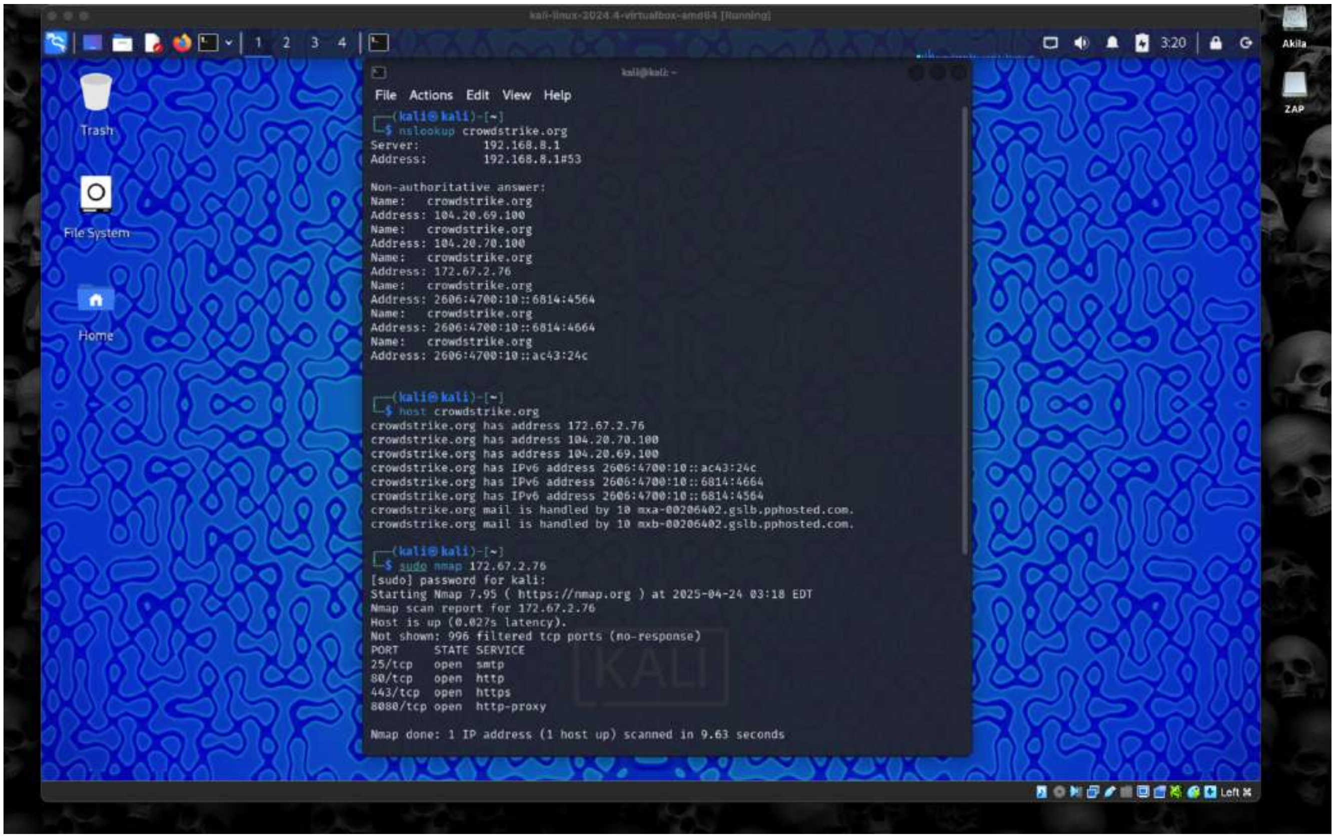
Impact Assessment

- This vulnerability poses significant risks to the organization:
- Unauthorized access to sensitive database information
- Potential exfiltration of confidential data
- Database corruption or unauthorized modifications
- Authentication bypass possibilities
- Compromise of application integrity
- Potential regulatory compliance violations

Steps to Reproduce

- Navigate to https://www.crowdstrike.com/en-us/about-us/environmental-social-governance/social-mission/our-communities/
- Insert the following payload into the URL parameter: case randomblob(100000) when not null then 1 else 1 end
- Observe the delayed response time
- Compare with unmodified query response time
- The significant time difference confirms the SQL injection vulnerability

Proof of Concept



```
┌──(kali㉿kali)-[~]
└─$ nslookup crowdstrike.org
Server:         192.168.8.1
Address:        192.168.8.1#53

Non-authoritative answer:
Name:   crowdstrike.org
Address: 104.20.69.100
Name:   crowdstrike.org
Address: 104.20.70.100
Name:   crowdstrike.org
Address: 172.67.2.76
Name:   crowdstrike.org
Address: 2606:4700:10::6814:4564
Name:   crowdstrike.org
Address: 2606:4700:10::6814:4664
Name:   crowdstrike.org
Address: 2606:4700:10::ac43:24c


┌──(kali㉿kali)-[~]
└─$ host crowdstrike.org
crowdstrike.org has address 172.67.2.76
crowdstrike.org has address 104.20.70.100
crowdstrike.org has address 104.20.69.100
crowdstrike.org has IPv6 address 2606:4700:10::ac43:24c
crowdstrike.org has IPv6 address 2606:4700:10::6814:4664
crowdstrike.org has IPv6 address 2606:4700:10::6814:4564
crowdstrike.org mail is handled by 10 mxa-00206402.gslb.pphosted.com.
crowdstrike.org mail is handled by 10 mxb-00206402.gslb.pphosted.com.

┌──(kali㉿kali)-[~]
└─$ sudo nmap 172.67.2.76
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-24 03:18 EDT
Nmap scan report for 172.67.2.76
Host is up (0.027s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
25/tcp   open  smtp
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 9.63 seconds
```

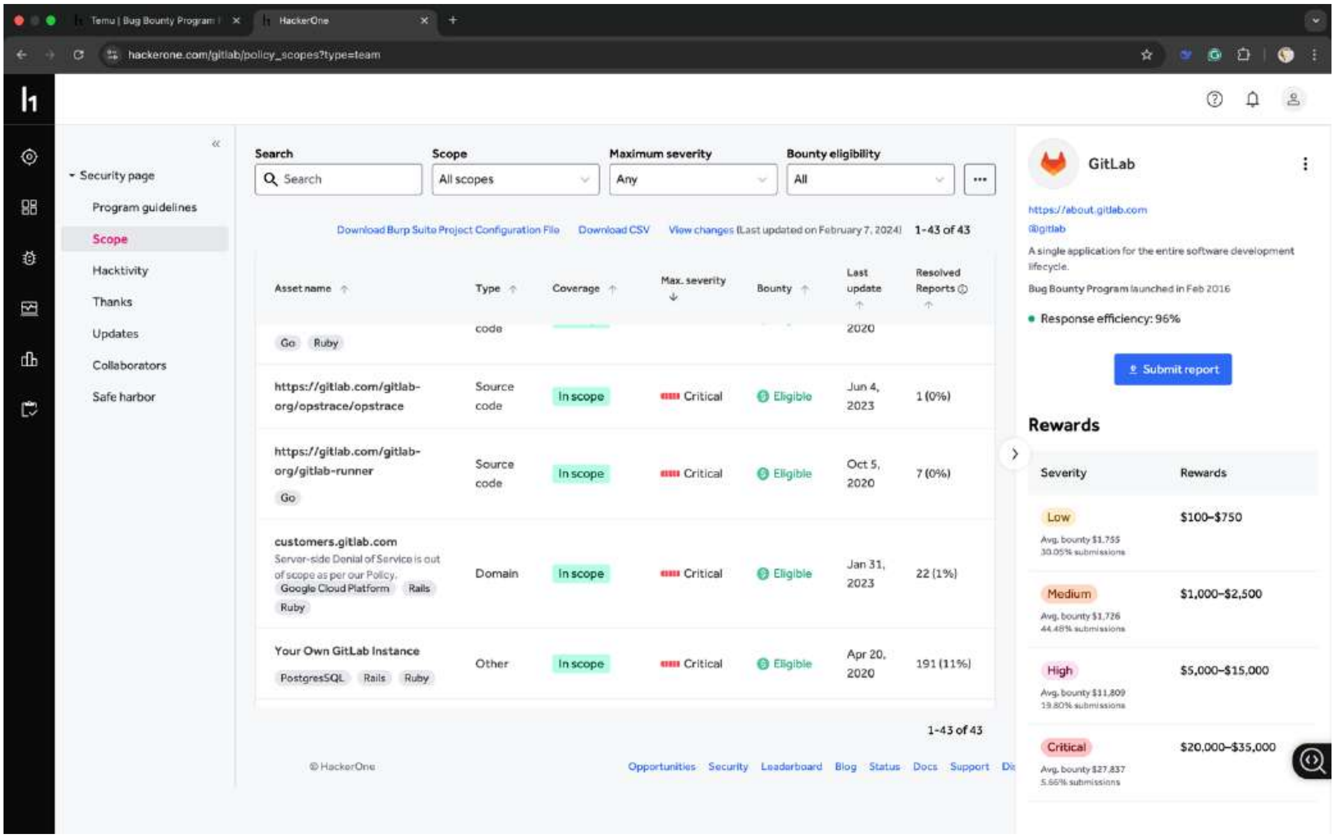
Proposed Mitigation or Fix

- The implementation of parameterized queries eliminates dynamic SQL by using prepared statements for creating a clear distinction between code and data content.
- All user inputs need approval through strict validation tests before system processing occurs.
- Programs should use ORM frameworks which perform automatic SQL escaping operations.
- The database must have permission systems which distribute minimum required access to each database user for operational purposes.
- The installation of Web Application Firewalls allows for detection and blocking of SQL injection attempts.
- Organization of error handling must include customized messages that do not reveal sensitive database information to unauthorized persons.
- A full security test must be conducted through periodic testing that detects and fixes procedural weaknesses.
- Radically examine the database interaction code as part of code review operations to detect additional vulnerabilities.

Report 03

GitLab

Scope of the security audit according to https://hackerone.com/gitlab/policy_scopes is as follows.



(Last updated on February 7, 2024) 1-43 of 43

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
Go Ruby	code				2020	
https://gitlab.com/gitlab-org/opstrace/opstrace	Source code	In scope	Critical	Eligible	Jun 4, 2023	1 (0%)
https://gitlab.com/gitlab-org/gitlab-runner Go	Source code	In scope	Critical	Eligible	Oct 5, 2020	7 (0%)
customers.gitlab.com Server-side Denial of Service is out of scope as per our Policy. Google Cloud Platform Rails Ruby	Domain	In scope	Critical	Eligible	Jan 31, 2023	22 (1%)
Your Own GitLab Instance PostgresSQL Rails Ruby	Other	In scope	Critical	Eligible	Apr 20, 2020	191 (11%)

1-43 of 43

GitLab

https://about.gitlab.com

@gitlab

A single application for the entire software development lifecycle.

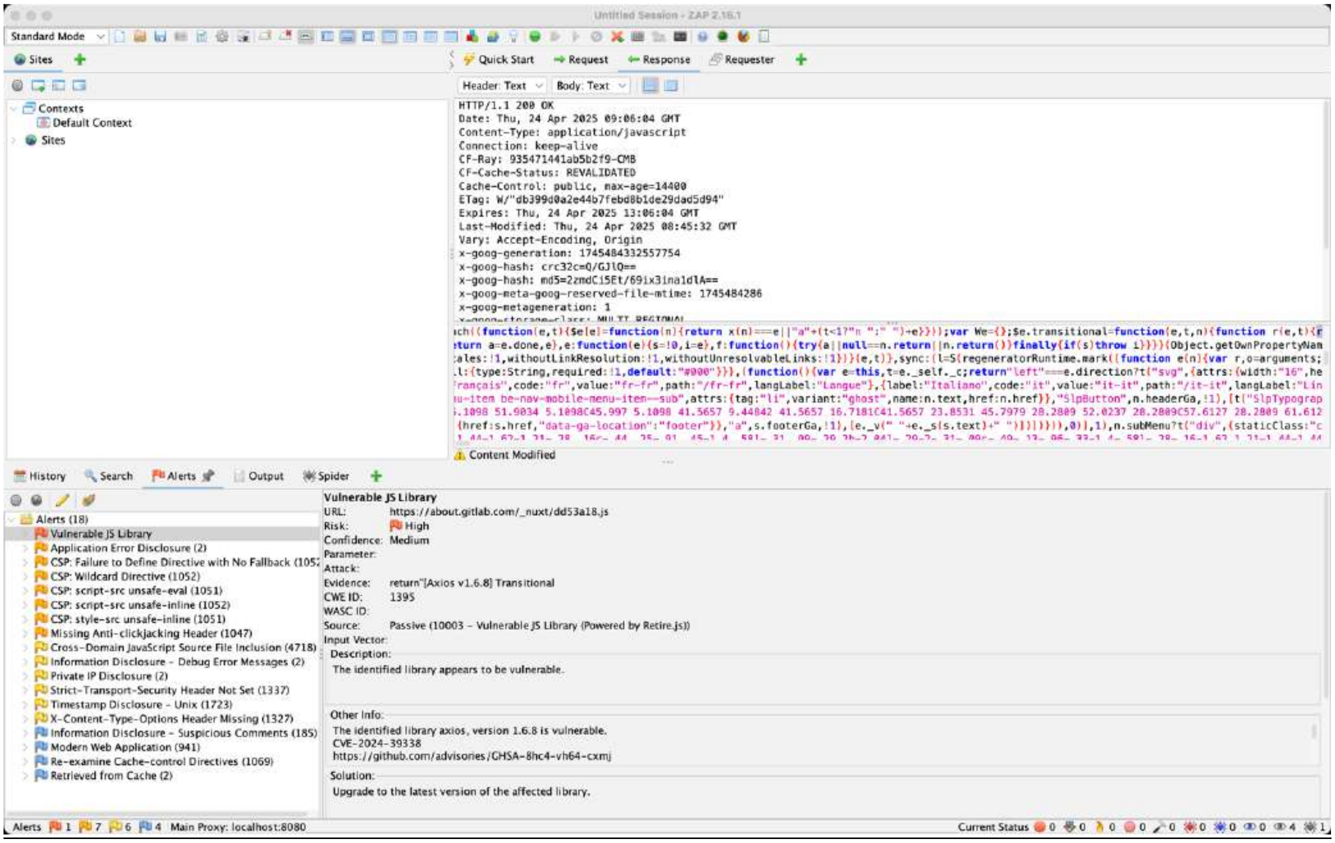
Bug Bounty Program launched in Feb 2016

- Response efficiency: 96%

Rewards

Severity	Rewards
Low Avg. bounty $1,755 30.05% submissions	$100–$750
Medium Avg. bounty $1,726 44.48% submissions	$1,000–$2,500
High Avg. bounty $11,809 19.80% submissions	$5,000–$15,000
Critical Avg. bounty $27,837 5.66% submissions	$20,000–$35,000

Scanned Vulnerabilities Using ZAP



```
HTTP/1.1 200 OK
Date: Thu, 24 Apr 2025 09:06:04 GMT
Content-Type: application/javascript
Connection: keep-alive
CF-Ray: 935471441ab5b2f9-CMB
CF-Cache-Status: REVALIDATED
Cache-Control: public, max-age=14400
ETag: W/"db399d0a2e44b7febd8b1de29dad5d94"
Expires: Thu, 24 Apr 2025 13:06:04 GMT
Last-Modified: Thu, 24 Apr 2025 08:45:32 GMT
Vary: Accept-Encoding, Origin
x-goog-generation: 1745484332557754
x-goog-hash: crc32c=Q/GJlQ==
x-goog-hash: md5=2zmdCi5Et/69ix3ina1dlA==
x-goog-meta-goog-reserved-file-mtime: 1745484286
x-goog-metageneration: 1
```

```
ach((function(e,t){$e[e]=function(n){return x(n)===e||"a"+(t<1?"n ":" ")+e}}));var We={};$e.transitional=function(e,t,n){function r(e,t){r
eturn a=e.done,e},e:function(e){s=!0,i=e},f:function(){try{a||null==n.return||n.return()}finally{if(s)throw i}}}(Object.getOwnPropertyNam
tales:!1,withoutLinkResolution:!1,withoutUnresolvableLinks:!1}}}(e,t)},sync:[l=S(regeneratorRuntime.mark((function e(n){var r,o=arguments;
.l:{type:String,required:!1,default:"#000"}}},(function(){var e=this,t=e._self._c;return"left"===e.direction?t("svg",{attrs:{width:"16",he
rançais",code:"fr",value:"fr-fr",path:"/fr-fr",langLabel:"Langue"},{label:"Italiano",code:"it",value:"it-it",path:"/it-it",langLabel:"Lin
u-item be-nav-mobile-menu-item--sub",attrs:{tag:"li",variant:"ghost",name:n.text,href:n.href}},"SlpButton",n.headerGa,!1),[t("SlpTypograp
5.1098 51.9034 5.1098C45.997 5.1098 41.5657 9.44842 41.5657 16.7181C41.5657 23.8531 45.7979 28.2809 52.0237 28.2809C57.6127 28.2809 61.612
{href:s.href,"data-ga-location":"footer"}},"a",s.footerGa,!1),[e._v(" "+e._s(s.text)+" ")])])}})),0)],1),n.subMenu?t("div",{staticClass:"c
```

Alerts (18)
- Vulnerable JS Library
- Application Error Disclosure (2)
- CSP: Failure to Define Directive with No Fallback (1052
- CSP: Wildcard Directive (1052)
- CSP: script-src unsafe-eval (1051)
- CSP: script-src unsafe-inline (1052)
- CSP: style-src unsafe-inline (1051)
- Missing Anti-clickjacking Header (1047)
- Cross-Domain JavaScript Source File Inclusion (4718)
- Information Disclosure - Debug Error Messages (2)
- Private IP Disclosure (2)
- Strict-Transport-Security Header Not Set (1337)
- Timestamp Disclosure - Unix (1723)
- X-Content-Type-Options Header Missing (1327)
- Information Disclosure - Suspicious Comments (185)
- Modern Web Application (941)
- Re-examine Cache-control Directives (1069)
- Retrieved from Cache (2)

Alerts 1 7 6 4 Main Proxy: localhost:8080

Vulnerable JS Library

URL:	https://about.gitlab.com/_nuxt/dd53a18.js
Risk:	High
Confidence:	Medium
Parameter:	
Attack:	
Evidence:	return"[Axios v1.6.8] Transitional
CWE ID:	1395
WASC ID:	
Source:	Passive (10003 - Vulnerable JS Library (Powered by Retire.js))
Input Vector:	

Description:

The identified library appears to be vulnerable.

Other Info:

The identified library axios, version 1.6.8 is vulnerable.
CVE-2024-39338
https://github.com/advisories/GHSA-8hc4-vh64-cxmj

Solution:

Upgrade to the latest version of the affected library.

Vulnerability Title Vulnerability Title

- Vulnerable JavaScript Library

Risk type

- High

Vulnerability Description

- Security professionals have discovered that the application runs Axios JavaScript library version 1.6.8 which contains security vulnerabilities. Workers have identified CVE-2024-39338 as a security vulnerability affecting this Axios JavaScript library within the version v1.6.8. The vulnerability detected by OWASP ZAP security tool was classified as CWE-1395 in the Axios JavaScript library version 1.6.8.

Attackers may exploit the "Transitional" functionality of Axios as it stands as the specific vulnerability affecting the application's systems.

URL

- https://about.gitlab.com/_nuxt/dd53a18.js

Affected Components

- Axios library version 1.6.8
- GitLab website or application using the vulnerable Axios version
- Any functionality that depends on this JavaScript library for making HTTP requests

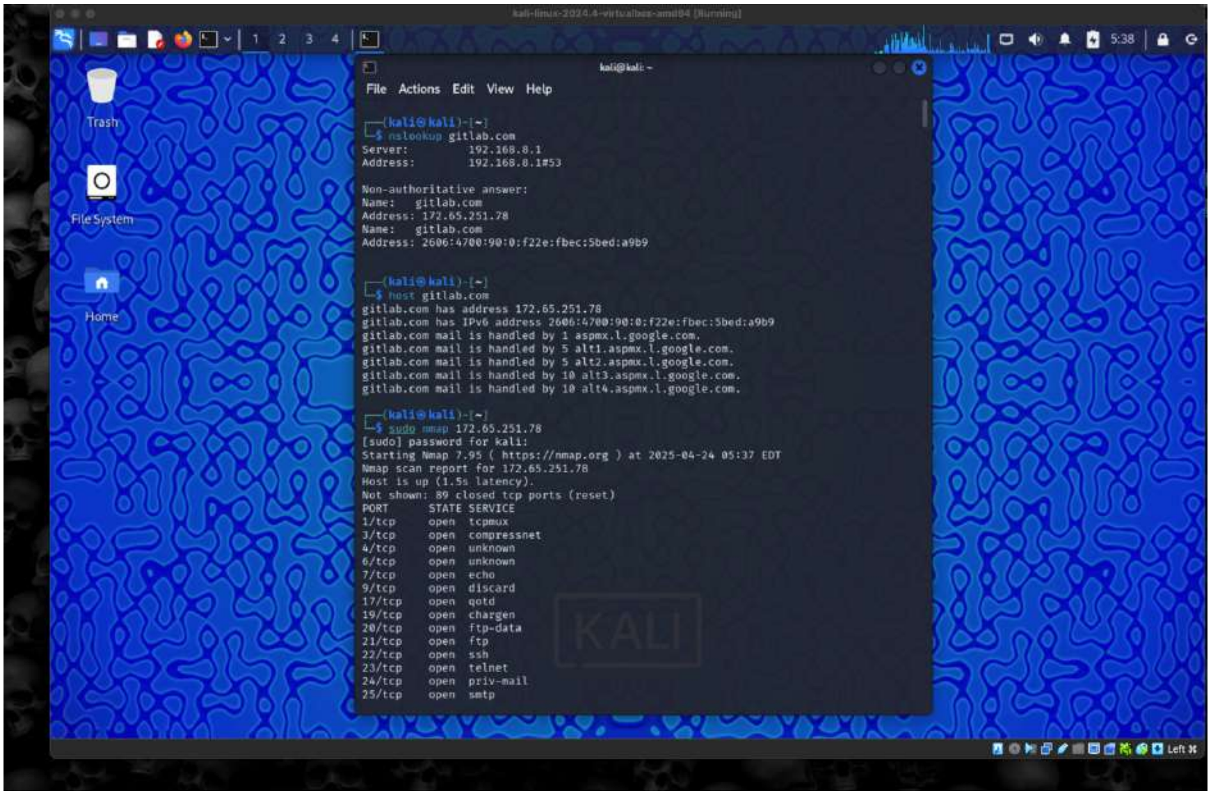
Impact Assessment

- Execute malicious code
- Compromise data integrity
- Bypass security controls
- Potentially gain unauthorized access to system resources

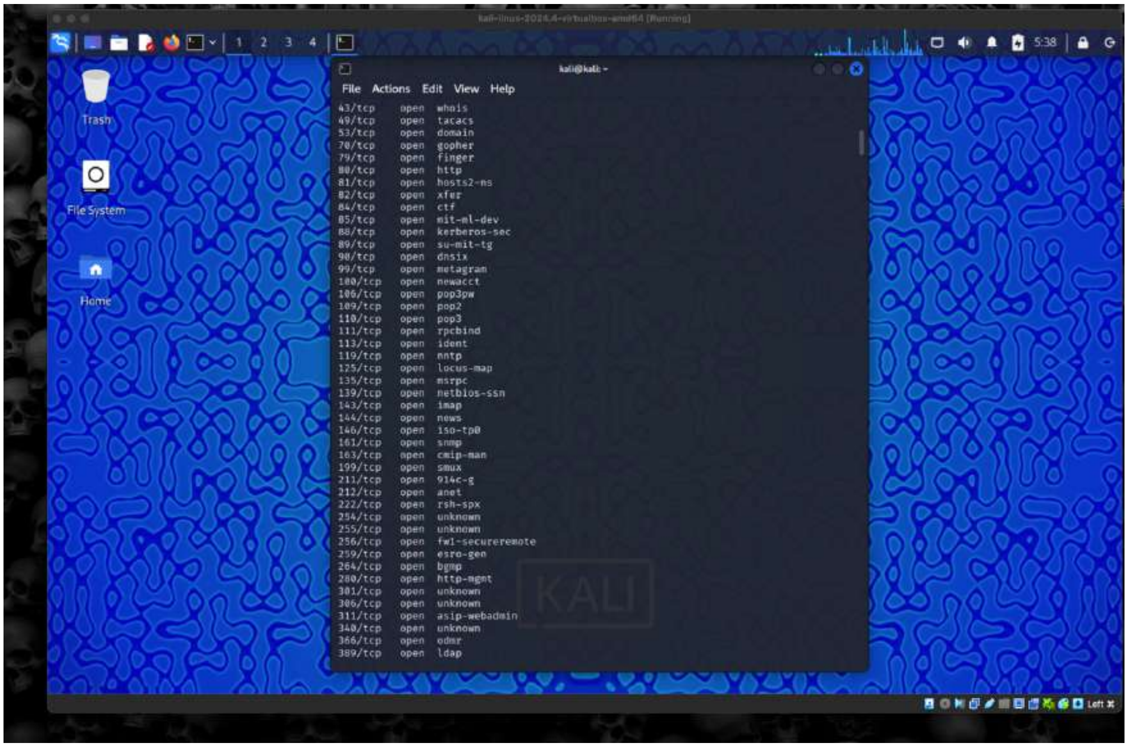
Steps to Reproduce

- Navigate to the GitLab website that loads the affected JavaScript file
- Inspect the loaded JavaScript resources in the browser's developer tools
- Locate the Axios library loaded from https://about.gitlab.com/_nuxt/dd53a18.js
- Verify the version of Axios being used (v1.6.8)
- Confirm the presence of the vulnerable code by searching for the "[Axios v1.6.8] Transitional" string

Proof of Concept



```
┌──(kali㉿kali)-[~]
└─$ nslookup gitlab.com
Server:         192.168.8.1
Address:        192.168.8.1#53

Non-authoritative answer:
Name:   gitlab.com
Address: 172.65.251.78
Name:   gitlab.com
Address: 2606:4700:90:0:f22e:fbec:5bed:a9b9


┌──(kali㉿kali)-[~]
└─$ host gitlab.com
gitlab.com has address 172.65.251.78
gitlab.com has IPv6 address 2606:4700:90:0:f22e:fbec:5bed:a9b9
gitlab.com mail is handled by 1 aspmx.l.google.com.
gitlab.com mail is handled by 5 alt1.aspmx.l.google.com.
gitlab.com mail is handled by 5 alt2.aspmx.l.google.com.
gitlab.com mail is handled by 10 alt3.aspmx.l.google.com.
gitlab.com mail is handled by 10 alt4.aspmx.l.google.com.

┌──(kali㉿kali)-[~]
└─$ sudo nmap 172.65.251.78
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-24 05:37 EDT
Nmap scan report for 172.65.251.78
Host is up (1.5s latency).
Not shown: 89 closed tcp ports (reset)
PORT      STATE SERVICE
1/tcp     open  tcpmux
3/tcp     open  compressnet
4/tcp     open  unknown
6/tcp     open  unknown
7/tcp     open  echo
9/tcp     open  discard
17/tcp    open  qotd
19/tcp    open  chargen
20/tcp    open  ftp-data
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
24/tcp    open  priv-mail
25/tcp    open  smtp
```



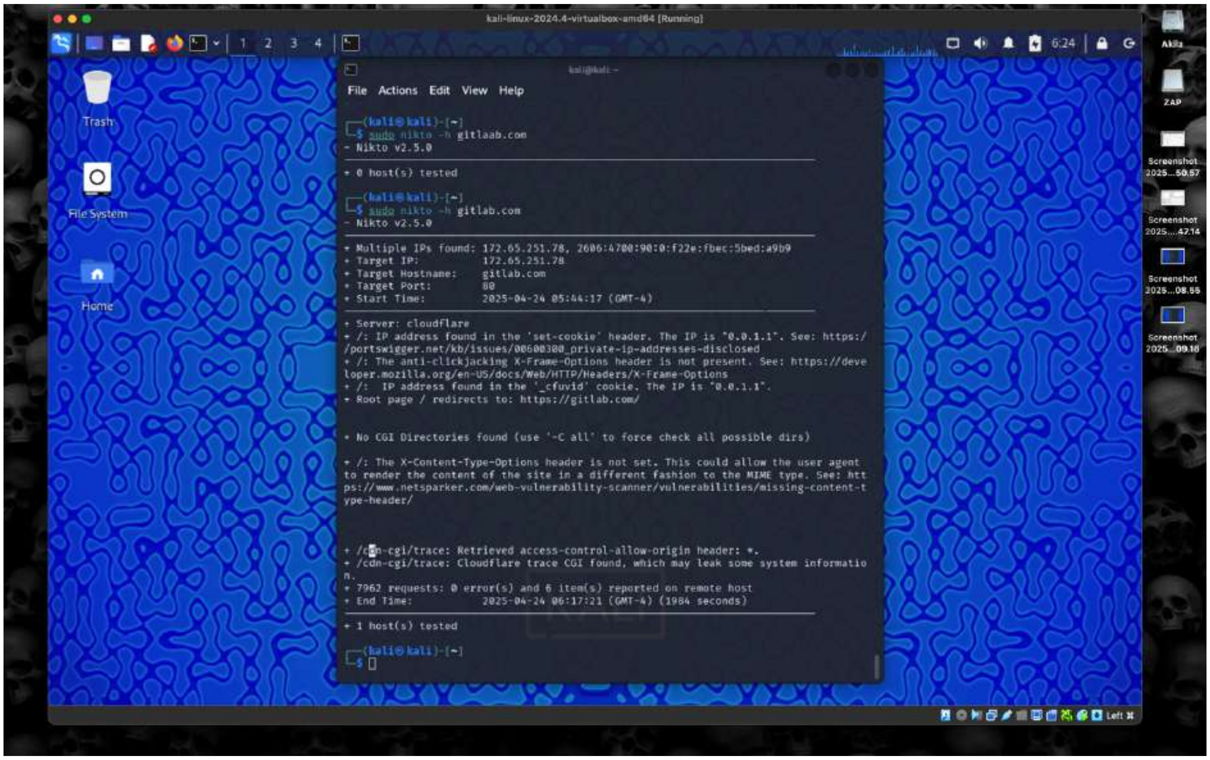
```
43/tcp    open  whois
49/tcp    open  tacacs
53/tcp    open  domain
70/tcp    open  gopher
79/tcp    open  finger
80/tcp    open  http
81/tcp    open  hosts2-ns
82/tcp    open  xfer
84/tcp    open  ctf
85/tcp    open  mit-ml-dev
88/tcp    open  kerberos-sec
89/tcp    open  su-mit-tg
90/tcp    open  dnsix
99/tcp    open  metagram
100/tcp   open  newacct
106/tcp   open  pop3pw
109/tcp   open  pop2
110/tcp   open  pop3
111/tcp   open  rpcbind
113/tcp   open  ident
119/tcp   open  nntp
125/tcp   open  locus-map
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
143/tcp   open  imap
144/tcp   open  news
146/tcp   open  iso-tp0
161/tcp   open  snmp
163/tcp   open  cmip-man
199/tcp   open  smux
211/tcp   open  914c-g
212/tcp   open  anet
222/tcp   open  rsh-spx
254/tcp   open  unknown
255/tcp   open  unknown
256/tcp   open  fw1-secureremote
259/tcp   open  esro-gen
264/tcp   open  bgmp
280/tcp   open  http-mgmt
301/tcp   open  unknown
306/tcp   open  unknown
311/tcp   open  asip-webadmin
340/tcp   open  unknown
366/tcp   open  odmr
389/tcp   open  ldap
```

Proposed Mitigation or Fix

- Moving to the most recent Axios library version ensures the patching of this vulnerability.
- Content Security Policy headers should be added to implement restrictions against potentially harmful script execution.
- The deployment process must include automatic third-party library scanning which detects vulnerabilities before product release.
- Third-party scripts require implementation of Subresource Integrity to verify their unaltered status.
- The application needs a monitoring procedure to track security notifications from all third-party system components which the application utilizes.
- A complete assessment of Axios library utilization throughout the application needs to be carried out by reviewing its implementation patterns to ensure security measures.

Scanned Vulnerabilities Using NIKTO

Nikto scan results from gitlab.com revealed three security problems including Cloudflare service use and cookies containing "0.0.1.1" internal IP address and the absence of critical X-Frame-Options and X-Content-Type-Options headers which creates clickjacking and MIME-type attack vulnerabilities as well as the /cdn-cgi/trace endpoint accepting any origin and exposing system data. The discovered misconfigurations demonstrate ways in which the site could become more exposed to possible attacks.



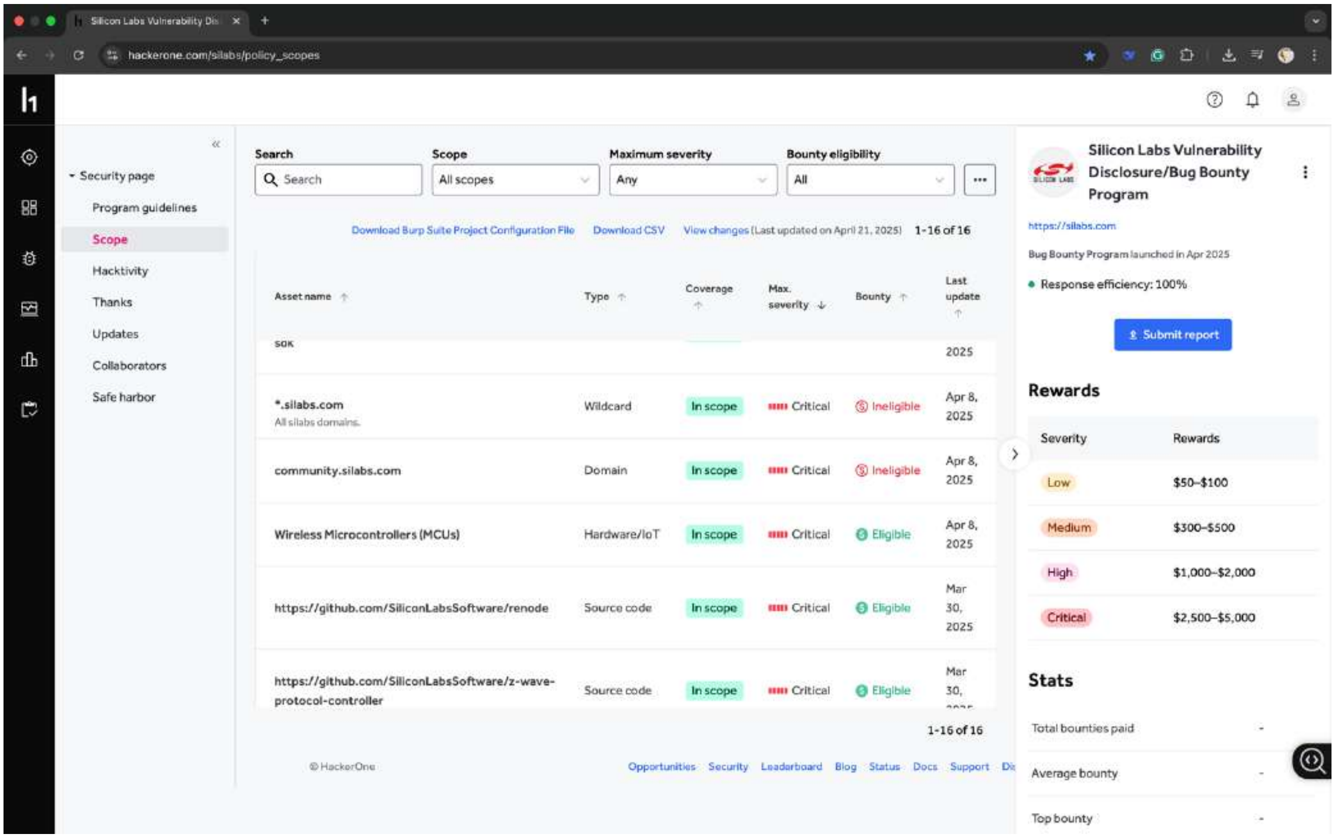
```
┌──(kali㉿kali)-[~]
└─$ sudo nikto -h gitlaab.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ 0 host(s) tested

┌──(kali㉿kali)-[~]
└─$ sudo nikto -h gitlab.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 172.65.251.78, 2606:4700:90:0:f22e:fbec:5bed:a9b9
+ Target IP:          172.65.251.78
+ Target Hostname:    gitlab.com
+ Target Port:        80
+ Start Time:         2025-04-24 05:44:17 (GMT-4)
---------------------------------------------------------------------------
+ Server: cloudflare
+ /: IP address found in the 'set-cookie' header. The IP is "0.0.1.1". See: https:/
/portswigger.net/kb/issues/00600300_private-ip-addresses-disclosed
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://deve
loper.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /:  IP address found in the '_cfuvid' cookie. The IP is "0.0.1.1".
+ Root page / redirects to: https://gitlab.com/


+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ /: 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: htt
ps://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-t
ype-header/



+ /cdn-cgi/trace: Retrieved access-control-allow-origin header: *.
+ /cdn-cgi/trace: Cloudflare trace CGI found, which may leak some system informatio
n.
+ 7962 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time:           2025-04-24 06:17:21 (GMT-4) (1984 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(kali㉿kali)-[~]
└─$ 
```

Report 04

Silabs.com

SILICON LABS

Scope of the security audit according to https://hackerone.com/silabs/policy_scopes is as follows.



Search: Search | Scope: All scopes | Maximum severity: Any | Bounty eligibility: All

Download Burp Suite Project Configuration File   Download CSV   View changes (Last updated on April 21, 2025)   1-16 of 16

Asset name	Type	Coverage	Max. severity	Bounty	Last update
sdk					2025
*.silabs.com All silabs domains.	Wildcard	In scope	Critical	Ineligible	Apr 8, 2025
community.silabs.com	Domain	In scope	Critical	Ineligible	Apr 8, 2025
Wireless Microcontrollers (MCUs)	Hardware/IoT	In scope	Critical	Eligible	Apr 8, 2025
https://github.com/SiliconLabsSoftware/renode	Source code	In scope	Critical	Eligible	Mar 30, 2025
https://github.com/SiliconLabsSoftware/z-wave-protocol-controller	Source code	In scope	Critical	Eligible	Mar 30,

1-16 of 16

Silicon Labs Vulnerability Disclosure/Bug Bounty Program

https://silabs.com

Bug Bounty Program launched in Apr 2025

- Response efficiency: 100%

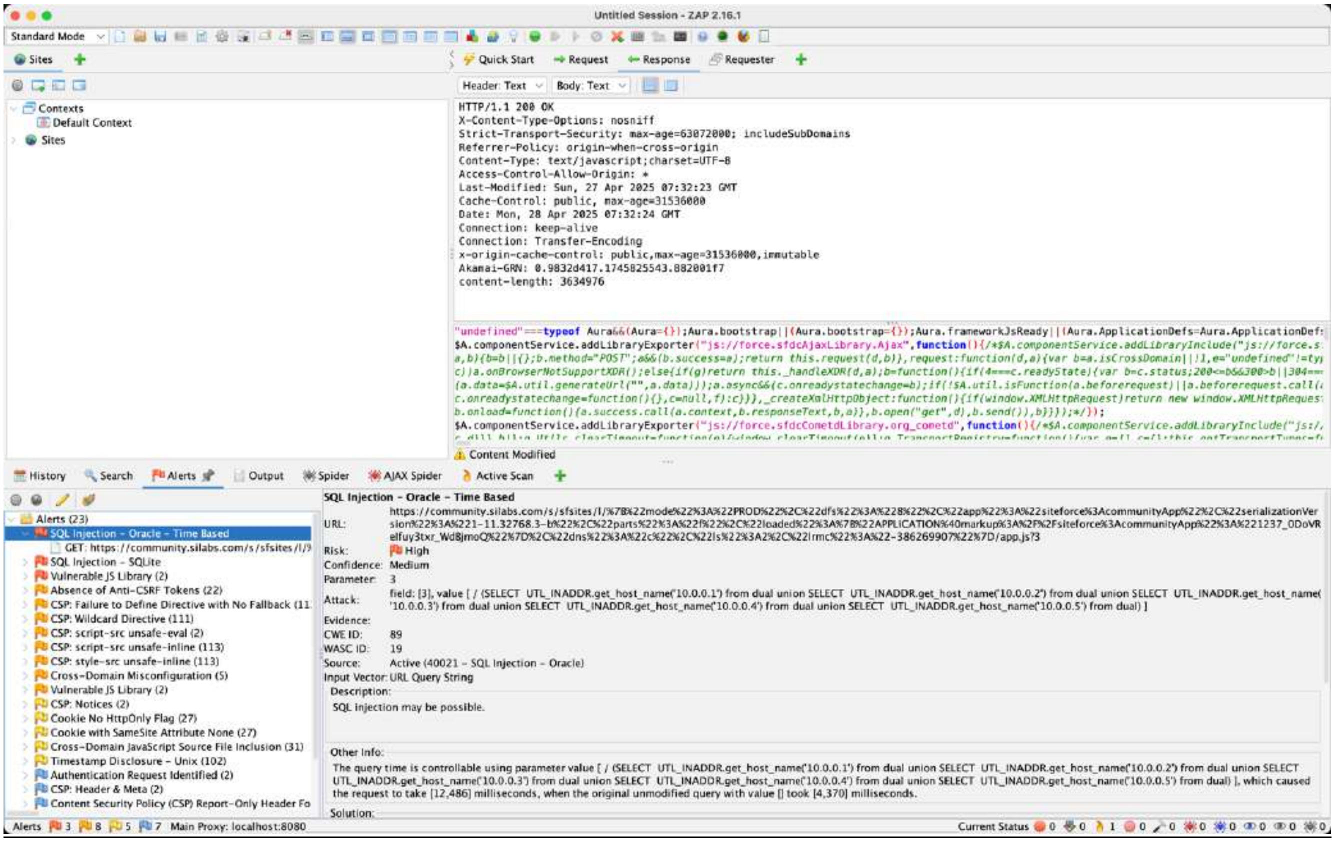
Rewards

Severity	Rewards
Low	\$50–\$100
Medium	\$300–\$500
High	\$1,000–\$2,000
Critical	\$2,500–\$5,000

Stats

Total bounties paid	-
Average bounty	-
Top bounty	-

Scanned Vulnerabilities Using ZAP



```
HTTP/1.1 200 OK
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains
Referrer-Policy: origin-when-cross-origin
Content-Type: text/javascript;charset=UTF-8
Access-Control-Allow-Origin: *
Last-Modified: Sun, 27 Apr 2025 07:32:23 GMT
Cache-Control: public, max-age=31536000
Date: Mon, 28 Apr 2025 07:32:24 GMT
Connection: keep-alive
Connection: Transfer-Encoding
x-origin-cache-control: public,max-age=31536000,immutable
Akamai-GRN: 0.9832d417.1745825543.882001f7
content-length: 3634976
```

```
"undefined"===typeof Aura&&(Aura={});Aura.bootstrap||(Aura.bootstrap={});Aura.frameworkJsReady||(Aura.ApplicationDefs=Aura.ApplicationDef:
$A.componentService.addLibraryExporter("js://force.sfdcAjaxLibrary.Ajax",function(){/*$A.componentService.addLibraryInclude("js://force.s
a,b){b=b||{};b.method="POST";a&&(b.success=a);return this.request(d,b)},request:function(d,a){var b=a.isCrossDomain||!1,e="undefined"!=typ
c))a.onBrowserNotSupportXDR();else{if(g)return this._handleXDR(d,a);b=function(){if(4===c.readyState){var b=c.status;200<=b&&300>b||304==
(a.data=$A.util.generateUrl("",a.data)));a.async&&(c.onreadystatechange=b);if(!$A.util.isFunction(a.beforerequest)||a.beforerequest.call(
c.onreadystatechange=function(){},c=null,f):c}}},_createXmlHttpObject:function(){if(window.XMLHttpRequest)return new window.XMLHttpReques
b.onload=function(){a.success.call(a.context,b.responseText,b,a)},b.open("get",d),b.send()),b}}});*/});
$A.componentService.addLibraryExporter("js://force.sfdcCometdLibrary.org_cometd",function(){/*$A.componentService.addLibraryInclude("js:/,
```

Alerts (23)
- SQL Injection - Oracle - Time Based
  - GET: https://community.silabs.com/s/sfsites/l/9
- SQL Injection - SQLite
- Vulnerable JS Library (2)
- Absence of Anti-CSRF Tokens (22)
- CSP: Failure to Define Directive with No Fallback (11
- CSP: Wildcard Directive (111)
- CSP: script-src unsafe-eval (2)
- CSP: script-src unsafe-inline (113)
- CSP: style-src unsafe-inline (113)
- Cross-Domain Misconfiguration (5)
- Vulnerable JS Library (2)
- CSP: Notices (2)
- Cookie No HttpOnly Flag (27)
- Cookie with SameSite Attribute None (27)
- Cross-Domain JavaScript Source File Inclusion (31)
- Timestamp Disclosure - Unix (102)
- Authentication Request Identified (2)
- CSP: Header & Meta (2)
- Content Security Policy (CSP) Report-Only Header Fo

Alerts 🟥 3 🟧 8 🟨 5 🟦 7 Main Proxy: localhost:8080

SQL Injection - Oracle - Time Based

URL: https://community.silabs.com/s/sfsites/l/%7B%22mode%22%3A%22PROD%22%2C%22dfs%22%3A%228%22%2C%22app%22%3A%22siteforce%3AcommunityApp%22%2C%22serializationVersion%22%3A%221-11.32768.3-b%22%2C%22parts%22%3A%22f%22%2C%22loaded%22%3A%7B%22APPLICATION%40markup%3A%2F%2Fsiteforce%3AcommunityApp%22%3A%221237_0DoVRelfuy3txr_WdBjmoQ%22%7D%2C%22dns%22%3A%22c%22%2C%22ls%22%3A2%2C%22lrmc%22%3A%22-386269907%22%7D/app.js?3

Risk: High

Confidence: Medium

Parameter: 3

Attack: field: [3], value [/ (SELECT UTL_INADDR.get_host_name('10.0.0.1') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.2') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.3') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.4') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.5') from dual)]

Evidence:

CWE ID: 89

WASC ID: 19

Source: Active (40021 - SQL Injection - Oracle)

Input Vector: URL Query String

Description:

SQL injection may be possible.

Other Info:

The query time is controllable using parameter value [/ (SELECT UTL_INADDR.get_host_name('10.0.0.1') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.2') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.3') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.4') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.5') from dual)], which caused the request to take [12,486] milliseconds, when the original unmodified query with value [] took [4,370] milliseconds.

Solution:

Current Status 0 0 1 0 0 0 0 0 0 0

Vulnerability Title Vulnerability Title

- SQL Injection – Oracle (Time-Based)

Risk type

- High

Vulnerability Description

- An attack through time-based SQL injection can target the URL query string parameter at https://community.silabs.com/s/sfsites/. The attack technique enables an attacker to embed any desired SQL commands into database queries that could result in unauthorized data access as well as data modification or service disruption through delayed server responses

URL

- https://community.silabs.com/s/sfsites/

Affected Components

- User-supplied inputs passed through URL query strings get processed at Oracle database backend systems.

Impact Assessment

- The database suffers from unauthorized access to its critical stored sensitive data.
- Data exfiltration or manipulation
- Service disruption through time-based attacks
- Exploiters would continue to abuse backend applications along with the connected database.

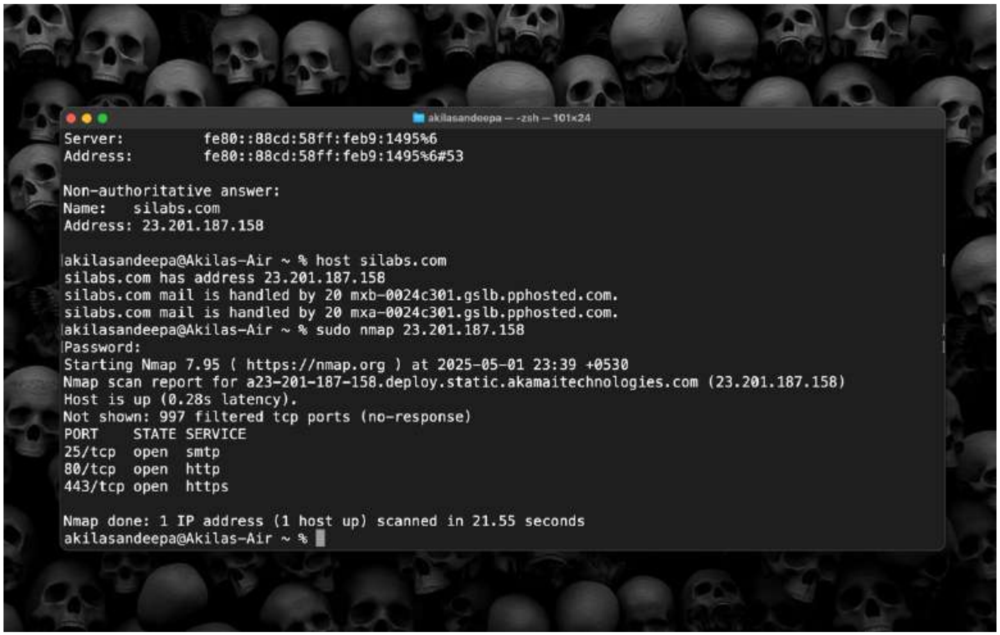
Steps to Reproduce

- A time-based SQL payload must be inserted into the URL query string parameter by modifying it to function properly.
- Observe the response time. The delayed response after a successful SQL injection attack will reveal the SQL vulnerability of the target system.

Proposed Mitigation or Fix

- The system must enforce robust input validation together with sanitization practices on each piece of user-supplied data that enters URL query strings.
- The prevention of SQL injection attacks can be achieved through parameterized queries or prepared statements.
- Apply least privilege rights policies to control the privileges of application access accounts that work with the database.
- Update and patch all application software components at regular intervals as well as the database and application frameworks.
- For SQL injection detection and blocking WAF web application firewalls should be employed.

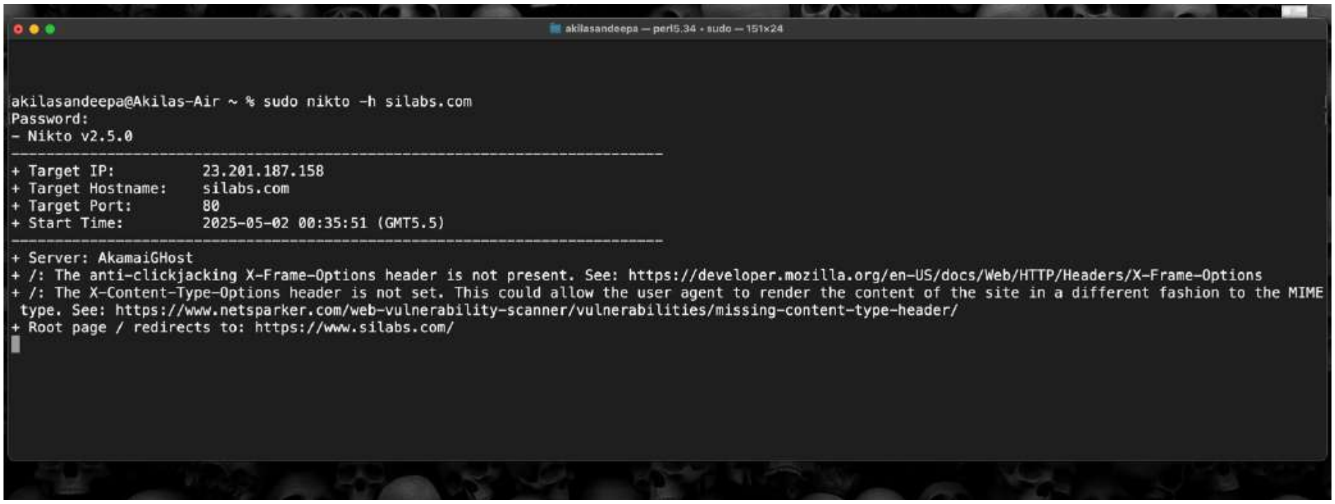
Proof of Concept



```
Server:         fe80::88cd:58ff:feb9:1495%6
Address:        fe80::88cd:58ff:feb9:1495%6#53

Non-authoritative answer:
Name:   silabs.com
Address: 23.201.187.158

akilasandeepa@Akilas-Air ~ % host silabs.com
silabs.com has address 23.201.187.158
silabs.com mail is handled by 20 mxb-0024c301.gslb.pphosted.com.
silabs.com mail is handled by 20 mxa-0024c301.gslb.pphosted.com.
akilasandeepa@Akilas-Air ~ % sudo nmap 23.201.187.158
Password:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-01 23:39 +0530
Nmap scan report for a23-201-187-158.deploy.static.akamaitechnologies.com (23.201.187.158)
Host is up (0.28s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 21.55 seconds
akilasandeepa@Akilas-Air ~ %
```

Scanned Vulnerabilities Using NIKTO

Silabs.com has multiple security header vulnerabilities per a Nikto scan because it lacks both X-Frame-Options protection against clickjacking attacks as well as X-Content-Type-Options protection against browser MIME type misinterpretation making it more prone to web-based attacks.

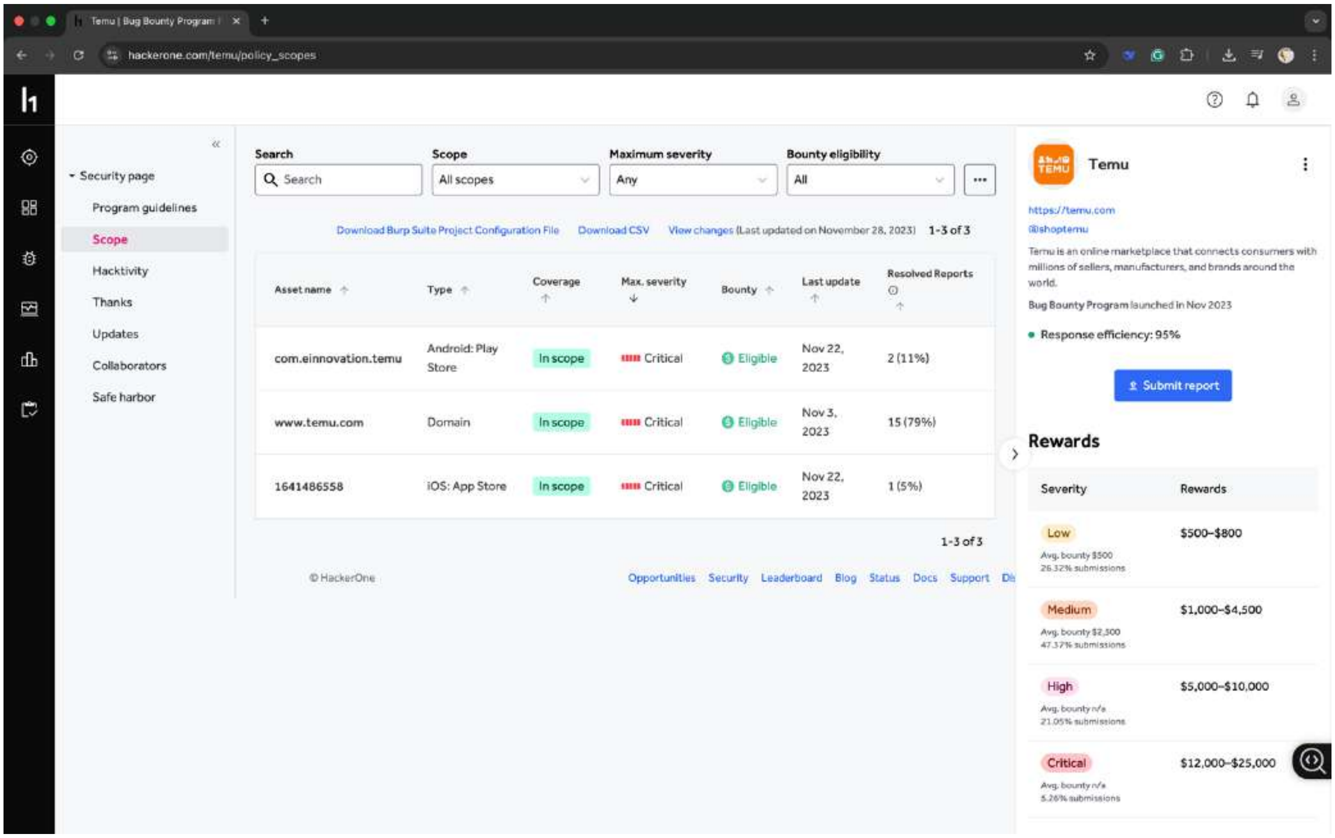


```
akilasandeepa@Akilas-Air ~ % sudo nikto -h silabs.com
Password:
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          23.201.187.158
+ Target Hostname:    silabs.com
+ Target Port:        80
+ Start Time:         2025-05-02 00:35:51 (GMT5.5)
---------------------------------------------------------------------------
+ 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
+ /: 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.silabs.com/
```

Report 05

Temu.com

Scope of the security audit according to https://hackerone.com/temu/policy_scopes as follows.



Search: Search | Scope: All scopes | Maximum severity: Any | Bounty eligibility: All

Download Burp Suite Project Configuration File Download CSV View changes (Last updated on November 28, 2023) 1-3 of 3

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
com.einnovation.temu	Android: Play Store	In scope	Critical	Eligible	Nov 22, 2023	2 (11%)
www.temu.com	Domain	In scope	Critical	Eligible	Nov 3, 2023	15 (79%)
1641486558	iOS: App Store	In scope	Critical	Eligible	Nov 22, 2023	1 (5%)

1-3 of 3

© HackerOne

Temu

https://temu.com
@shoptemu

Temu is an online marketplace that connects consumers with millions of sellers, manufacturers, and brands around the world.

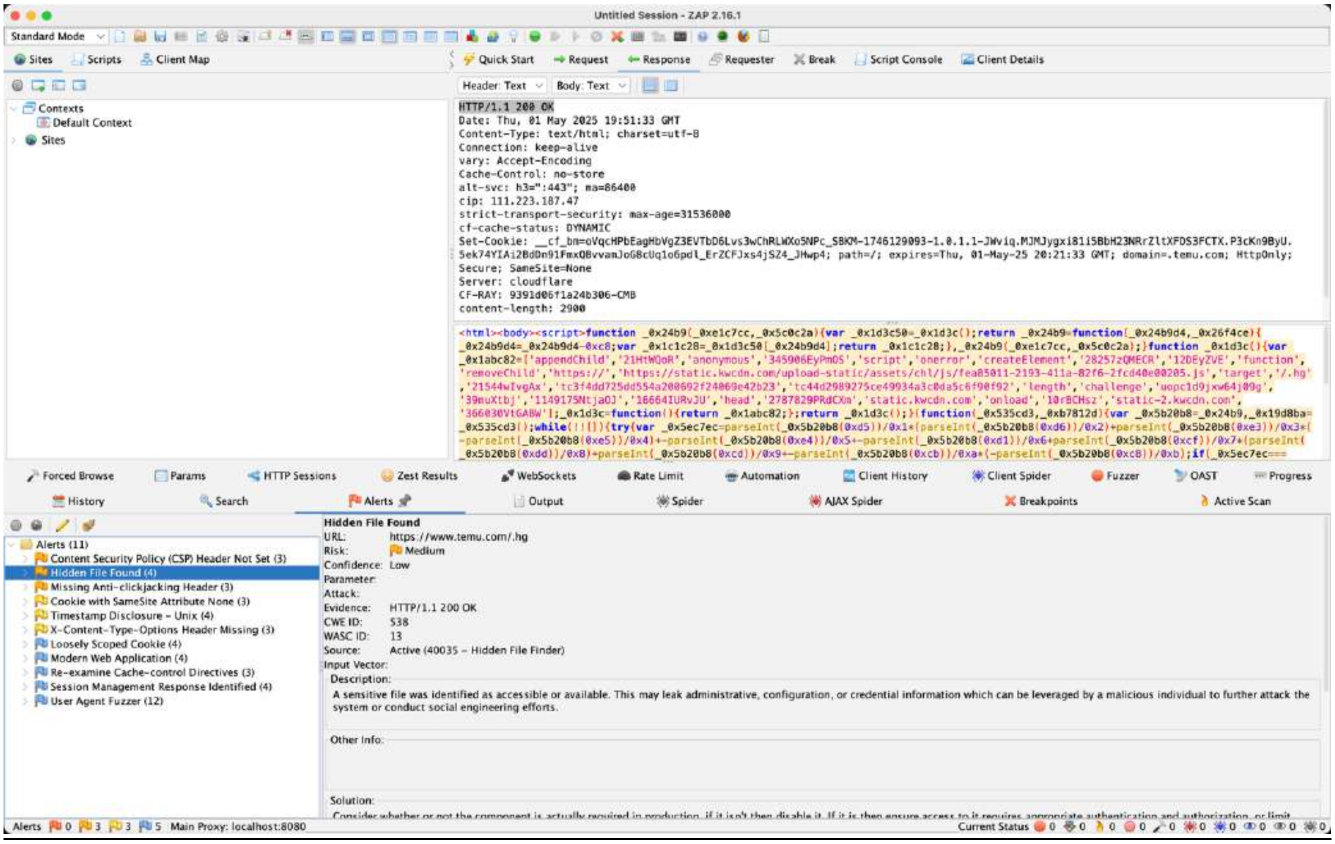
Bug Bounty Program launched in Nov 2023

- Response efficiency: 95%

Rewards

Severity	Rewards
Low Avg. bounty $500 26.32% submissions	$500–$800
Medium Avg. bounty $2,300 47.37% submissions	$1,000–$4,500
High Avg. bounty n/a 21.05% submissions	$5,000–$10,000
Critical Avg. bounty n/a 5.26% submissions	$12,000–$25,000

Scanned Vulnerabilities Using ZAP



```
HTTP/1.1 200 OK
Date: Thu, 01 May 2025 19:51:33 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
vary: Accept-Encoding
Cache-Control: no-store
alt-svc: h3=":443"; ma=86400
cip: 111.223.187.47
strict-transport-security: max-age=31536000
cf-cache-status: DYNAMIC
Set-Cookie: __cf_bm=oVqcHPbEagHbVgZ3EVTbD6Lvs3wChRLWXo5NPc_SBKM-1746129093-1.0.1.1-JWviq.MJMJygxi81i5BbH23NRrZltXFDS3FCTX.P3cKn9ByU.
5ek74YIAi2BdDn91FmxQBvvamJoG8cUq1o6pdl_ErZCFJxs4jSZ4_JHwp4; path=/; expires=Thu, 01-May-25 20:21:33 GMT; domain=.temu.com; HttpOnly;
Secure; SameSite=None
Server: cloudflare
CF-RAY: 9391d06f1a24b306-CMB
content-length: 2900
```

```
<html><body><script>function _0x24b9(_0xe1c7cc,_0x5c0c2a){var _0x1d3c50=_0x1d3c();return _0x24b9=function(_0x24b9d4,_0x26f4ce){
_0x24b9d4=_0x24b9d4-0xc8;var _0x1c1c28=_0x1d3c50[_0x24b9d4];return _0x1c1c28;},_0x24b9(_0xe1c7cc,_0x5c0c2a);}function _0x1d3c(){var
_0x1abc82=['appendChild','21HtWQoR','anonymous','345906EyPmOS','script','onerror','createElement','28257zQMECR','12DEyZVE','function',
'removeChild','https://','https://static.kwcdn.com/upload-static/assets/chl/js/fea85011-2193-411a-82f6-2fcd40e00205.js','target','/.hg'
,'21544wIvgAx','tc3f4dd725dd554a200692f24069e42b23','tc44d2989275ce49934a3c0da5c6f90f92','length','challenge','uopc1d9jxw64j09g',
'39muXtbj','1149175NtjaOJ','16664IURvJU','head','2787829PRdCXm','static.kwcdn.com','onload','10rBCHsz','static-2.kwcdn.com',
'366030VtGABW'];_0x1d3c=function(){return _0x1abc82;};return _0x1d3c();}(function(_0x535cd3,_0xb7812d){var _0x5b20b8=_0x24b9,_0x19d8ba=
_0x535cd3();while(!![]){try{var _0x5ec7ec=parseInt(_0x5b20b8(0xd5))/0x1*(parseInt(_0x5b20b8(0xd6))/0x2)+parseInt(_0x5b20b8(0xe3))/0x3*(
-parseInt(_0x5b20b8(0xe5))/0x4)+-parseInt(_0x5b20b8(0xe4))/0x5+-parseInt(_0x5b20b8(0xd1))/0x6+parseInt(_0x5b20b8(0xcf))/0x7*(parseInt(
_0x5b20b8(0xdd))/0x8)+parseInt(_0x5b20b8(0xcd))/0x9+-parseInt(_0x5b20b8(0xcb))/0xa*(-parseInt(_0x5b20b8(0xc8))/0xb);if(_0x5ec7ec===
```

Alerts (11)
- Content Security Policy (CSP) Header Not Set (3)
- Hidden File Found (4)
- Missing Anti-clickjacking Header (3)
- Cookie with SameSite Attribute None (3)
- Timestamp Disclosure - Unix (4)
- X-Content-Type-Options Header Missing (3)
- Loosely Scoped Cookie (4)
- Modern Web Application (4)
- Re-examine Cache-control Directives (3)
- Session Management Response Identified (4)
- User Agent Fuzzer (12)

Hidden File Found
URL: https://www.temu.com/.hg
Risk: Medium
Confidence: Low
Parameter:
Attack:
Evidence: HTTP/1.1 200 OK
CWE ID: 538
WASC ID: 13
Source: Active (40035 – Hidden File Finder)
Input Vector:

Description:
A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.

Other Info:

Solution:
Consider whether or not the component is actually required in production, if it isn't then disable it. If it is then ensure access to it requires appropriate authentication and authorization, or limit

Alerts 0 3 3 5 Main Proxy: localhost:8080
Current Status 0 0 0 0 0 0 0 0 0 0

Vulnerability Title Vulnerability Title

- Hidden File Disclosure –. hg File Accessible

Risk type

- Medium

Vulnerability Description

- Accessibility of the hidden .hg file was identified at the URL https://www.temu.com/.hg. The system uses Mercurial as its version control solution through this .hg file or directory which risks revealing its administrative and configuration settings and credentials. The exposed file helps attackers execute two different types of attacks: information disclosure and social engineering.

URL

- www.temu.com

Affected Components

- Web server hosting www.temu.com
- File system and directory structure, specifically the .hg directory or file

Impact Assessment

- A successful attack enables attackers to recover important data stored in the repository, including history records and configuration details, along with credentials, which could lead to more cyberattacks or privileged access or social engineering capabilities.

Steps to Reproduce

- Open a browser or use a tool like curl to access:

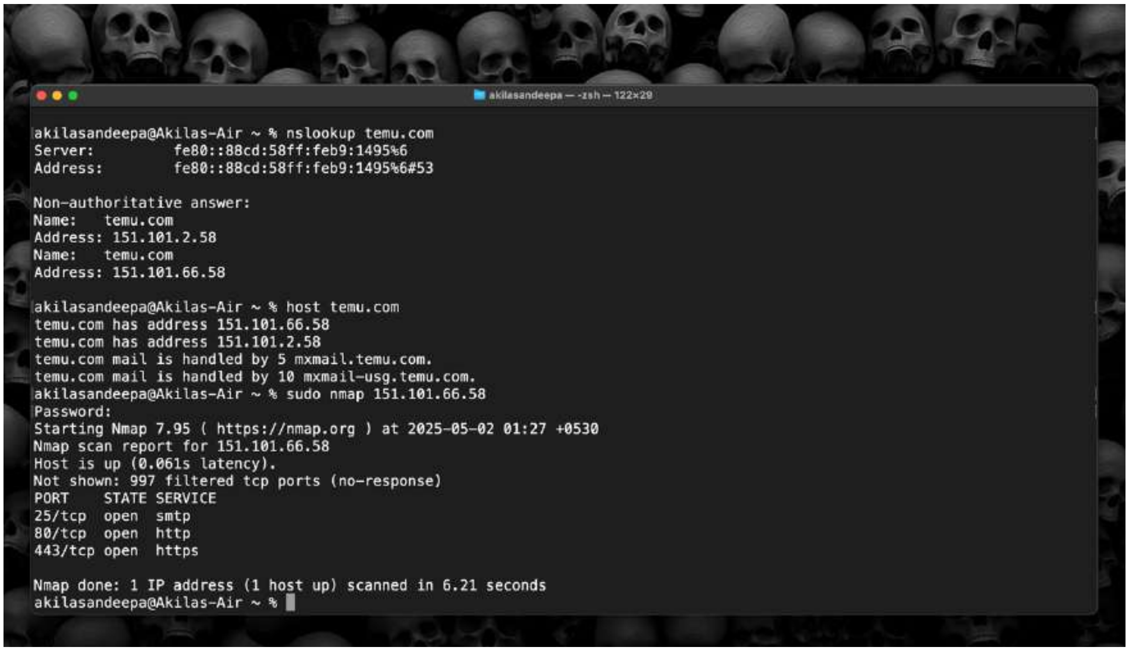
  https://www.temu.com/.hg

- If the file or directory is accessible, the server will respond with HTTP 200 OK and display its contents

Proposed Mitigation or Fix

- Worldwide visibility of the .hg file or directory needs to be blocked from the web root.
- Web server administrators should restrict access to all hidden files and directories which begin with a dot through proper configuration updates.
- Sensitive files and version control data should be monitored in web root audits to stop their accidental release

Proof of Concept

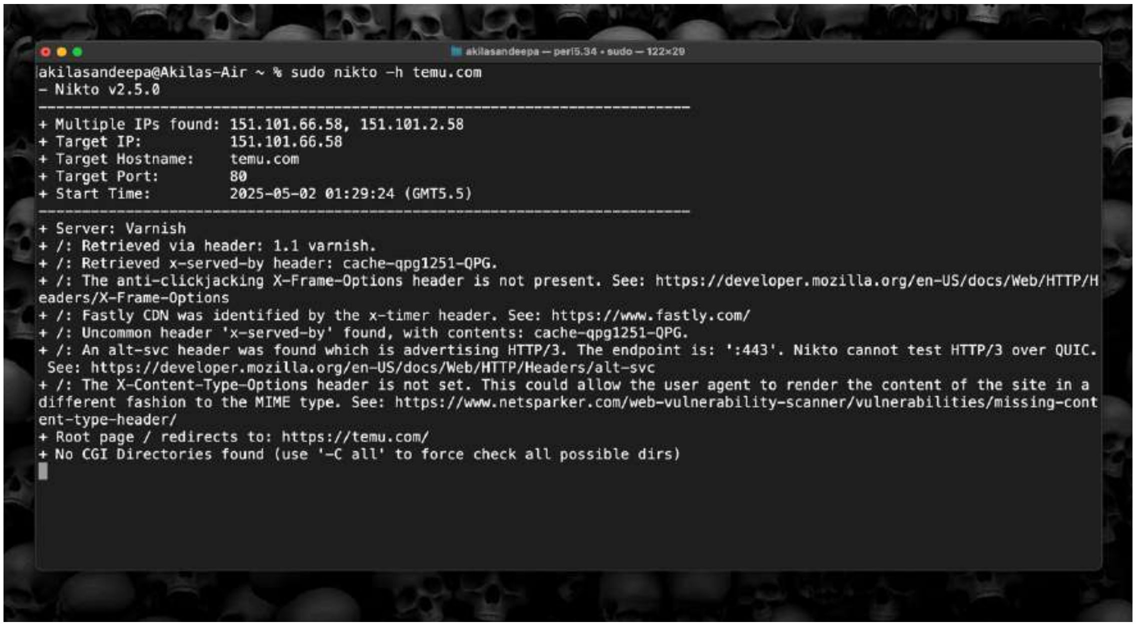


akilasandeepa — -zsh — 122×29

```
akilasandeepa@Akilas-Air ~ % nslookup temu.com
Server:         fe80::88cd:58ff:feb9:1495%6
Address:        fe80::88cd:58ff:feb9:1495%6#53

Non-authoritative answer:
Name:   temu.com
Address: 151.101.2.58
Name:   temu.com
Address: 151.101.66.58

akilasandeepa@Akilas-Air ~ % host temu.com
temu.com has address 151.101.66.58
temu.com has address 151.101.2.58
temu.com mail is handled by 5 mxmail.temu.com.
temu.com mail is handled by 10 mxmail-usg.temu.com.
akilasandeepa@Akilas-Air ~ % sudo nmap 151.101.66.58
Password:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-02 01:27 +0530
Nmap scan report for 151.101.66.58
Host is up (0.061s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 6.21 seconds
akilasandeepa@Akilas-Air ~ %
```

Scanned Vulnerabilities Using NIKTO

- The X-Frame-Options header together with the X-Content-Type-Options header are missing from temu.com during a Nikto scan making the site vulnerable to specific web-based attacks.



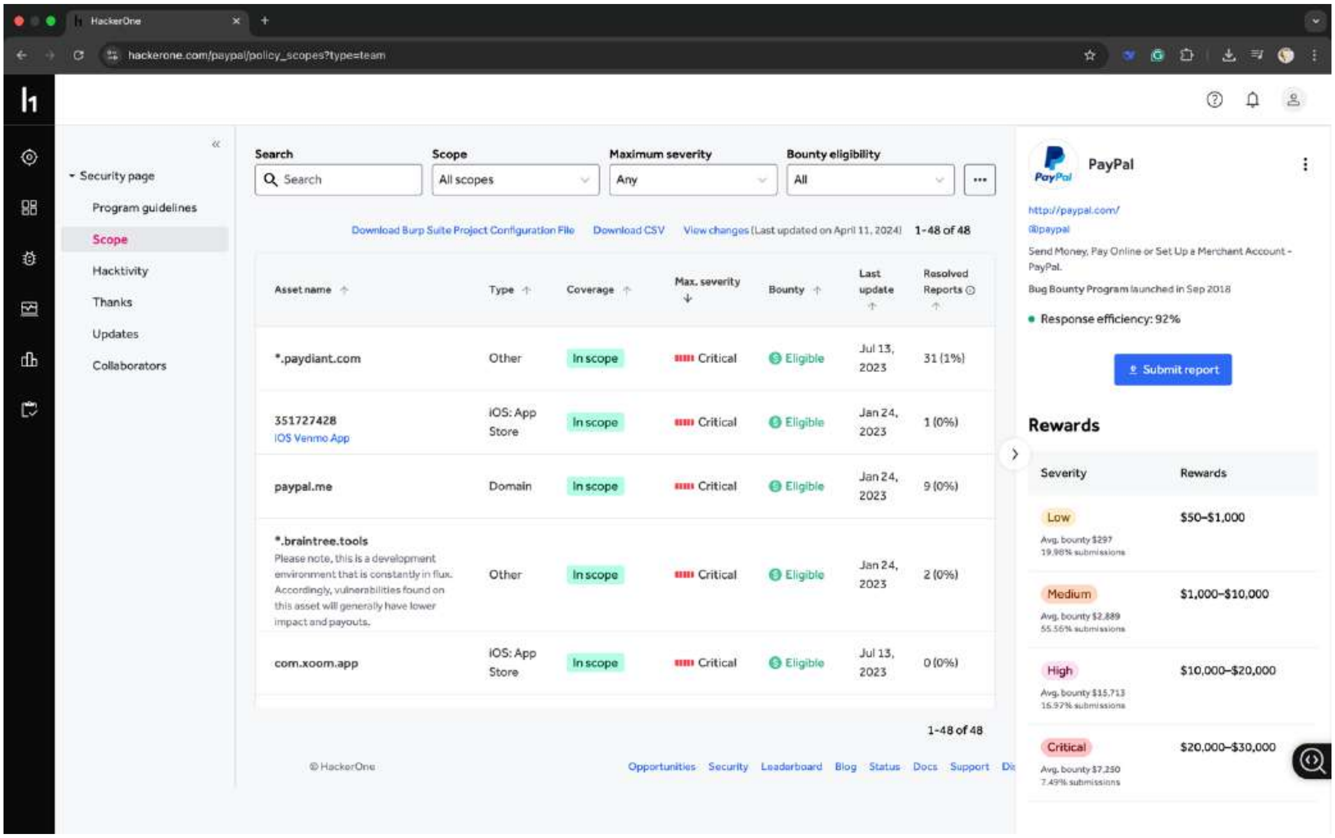
akilasandeepa — perl5.34 • sudo — 122×29

```
akilasandeepa@Akilas-Air ~ % sudo nikto -h temu.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 151.101.66.58, 151.101.2.58
+ Target IP:          151.101.66.58
+ Target Hostname:    temu.com
+ Target Port:        80
+ Start Time:         2025-05-02 01:29:24 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Varnish
+ /: Retrieved via header: 1.1 varnish.
+ /: Retrieved x-served-by header: cache-qpg1251-QPG.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/H
eaders/X-Frame-Options
+ /: Fastly CDN was identified by the x-timer header. See: https://www.fastly.com/
+ /: Uncommon header 'x-served-by' found, with contents: cache-qpg1251-QPG.
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 over QUIC.
 See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
+ /: 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-cont
ent-type-header/
+ Root page / redirects to: https://temu.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

Report 06

Paypal

Scope of the security audit according to https://hackerone.com/paypal/policy_scopes is as follows.



Search: Search | Scope: All scopes | Maximum severity: Any | Bounty eligibility: All

Download Burp Suite Project Configuration File   Download CSV   View changes (Last updated on April 11, 2024)   1-48 of 48

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
*.paydiant.com	Other	In scope	Critical	Eligible	Jul 13, 2023	31 (1%)
351727428 iOS Venmo App	iOS: App Store	In scope	Critical	Eligible	Jan 24, 2023	1 (0%)
paypal.me	Domain	In scope	Critical	Eligible	Jan 24, 2023	9 (0%)
*.braintree.tools Please note, this is a development environment that is constantly in flux. Accordingly, vulnerabilities found on this asset will generally have lower impact and payouts.	Other	In scope	Critical	Eligible	Jan 24, 2023	2 (0%)
com.xoom.app	iOS: App Store	In scope	Critical	Eligible	Jul 13, 2023	0 (0%)

1-48 of 48

PayPal

http://paypal.com/
@paypal

Send Money, Pay Online or Set Up a Merchant Account - PayPal.

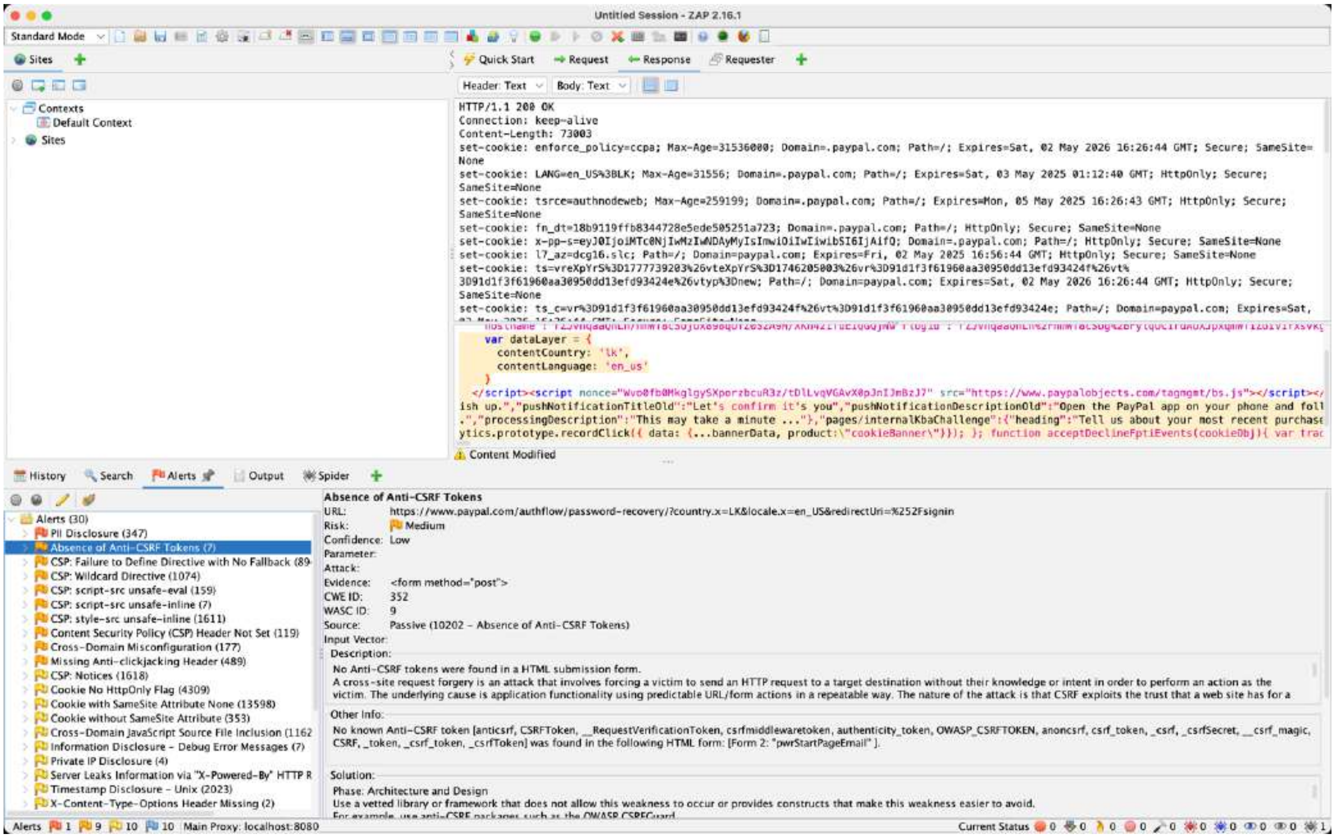
Bug Bounty Program launched in Sep 2018

Response efficiency: 92%

Rewards

Severity	Rewards
Low Avg. bounty $297 19.98% submissions	$50–$1,000
Medium Avg. bounty $2,889 55.56% submissions	$1,000–$10,000
High Avg. bounty $15,713 16.97% submissions	$10,000–$20,000
Critical Avg. bounty $7,250 7.49% submissions	$20,000–$30,000

Scanned Vulnerabilities Using ZAP



```
HTTP/1.1 200 OK
Connection: keep-alive
Content-Length: 73003
set-cookie: enforce_policy=ccpa; Max-Age=31536000; Domain=.paypal.com; Path=/; Expires=Sat, 02 May 2026 16:26:44 GMT; Secure; SameSite=
None
set-cookie: LANG=en_US%3BLK; Max-Age=31556; Domain=.paypal.com; Path=/; Expires=Sat, 03 May 2025 01:12:40 GMT; HttpOnly; Secure;
SameSite=None
set-cookie: tsrce=authnodeweb; Max-Age=259199; Domain=.paypal.com; Path=/; Expires=Mon, 05 May 2025 16:26:43 GMT; HttpOnly; Secure;
SameSite=None
set-cookie: fn_dt=18b9119ffb8344728e5ede505251a723; Domain=.paypal.com; Path=/; HttpOnly; Secure; SameSite=None
set-cookie: x-pp-s=eyJ0IjoiMTc0NjIwMzIwNDAyMyIsImwiOiIwIiwibSI6IjAifQ; Domain=.paypal.com; Path=/; HttpOnly; Secure; SameSite=None
set-cookie: l7_az=dcg16.slc; Path=/; Domain=paypal.com; Expires=Fri, 02 May 2025 16:56:44 GMT; HttpOnly; Secure; SameSite=None
set-cookie: ts=vreXpYrS%3D1777739203%26vteXpYrS%3D1746205003%26vr%3D91d1f3f61960aa30950dd13efd93424f%26vt%
3D91d1f3f61960aa30950dd13efd93424e%26vtyp%3Dnew; Path=/; Domain=paypal.com; Expires=Sat, 02 May 2026 16:26:44 GMT; HttpOnly; Secure;
SameSite=None
set-cookie: ts_c=vr%3D91d1f3f61960aa30950dd13efd93424f%26vt%3D91d1f3f61960aa30950dd13efd93424e; Path=/; Domain=paypal.com; Expires=Sat,
```

```
    var dataLayer = {
      contentCountry: 'lk',
      contentLanguage: 'en_us'
    }
  </script><script nonce="Wvo0fb0MkglgySXporzbcuR3z/tDlLvqVGAvX0pJnIJmBzJ7" src="https://www.paypalobjects.com/tagmgt/bs.js"></script></
ish up.","pushNotificationTitleOld":"Let's confirm it's you","pushNotificationDescriptionOld":"Open the PayPal app on your phone and foll
.","processingDescription":"This may take a minute ..."},"pages/internalKbaChallenge":{"heading":"Tell us about your most recent purchase
ytics.prototype.recordClick({ data: {...bannerData, product:\"cookieBanner\"}}); }; function acceptDeclineFptiEvents(cookieObj){ var trac
```

⚠ Content Modified

- Alerts (30)
  - PII Disclosure (347)
  - Absence of Anti-CSRF Tokens (7)
  - CSP: Failure to Define Directive with No Fallback (89
  - CSP: Wildcard Directive (1074)
  - CSP: script-src unsafe-eval (159)
  - CSP: script-src unsafe-inline (7)
  - CSP: style-src unsafe-inline (1611)
  - Content Security Policy (CSP) Header Not Set (119)
  - Cross-Domain Misconfiguration (177)
  - Missing Anti-clickjacking Header (489)
  - CSP: Notices (1618)
  - Cookie No HttpOnly Flag (4309)
  - Cookie with SameSite Attribute None (13598)
  - Cookie without SameSite Attribute (353)
  - Cross-Domain JavaScript Source File Inclusion (1162
  - Information Disclosure - Debug Error Messages (7)
  - Private IP Disclosure (4)
  - Server Leaks Information via "X-Powered-By" HTTP R
  - Timestamp Disclosure - Unix (2023)
  - X-Content-Type-Options Header Missing (2)

Absence of Anti-CSRF Tokens

URL:	https://www.paypal.com/authflow/password-recovery/?country.x=LK&locale.x=en_US&redirectUri=%252Fsignin
Risk:	Medium
Confidence:	Low
Parameter:	
Attack:	
Evidence:	<form method="post">
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

Other Info:

No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 2: "pwrStartPageEmail"].

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.

Alerts 1 9 10 10 Main Proxy: localhost:8080

Current Status 0 0 0 0 0 0 0 0 0 1

Vulnerability Title Vulnerability Title

- Absence of Anti-CSRF Tokens

Risk type

- Medium

Vulnerability Description

- A CSRF defense through the implementation of anti-CSRF (Cross-Site Request Forgery) tokens is absent from all HTML submission forms within the application. CSRF attacks become possible when authentication tokens are absent because attackers can make users mistakenly send undesirable requests to the web application that executes commands on behalf of the user without authorization. The lack of this security measure breaches the protective layer between users and their applications by allowing CSRF attacks to abuse sessions which are already authenticated.

Affected Components

- HTML forms, specifically the password recovery endpoint:
  /authflow/password-recovery/?country.x=LK&locale.x=en_US&redirectUri=%2Fsignin
- Any other forms lacking anti-CSRF tokens

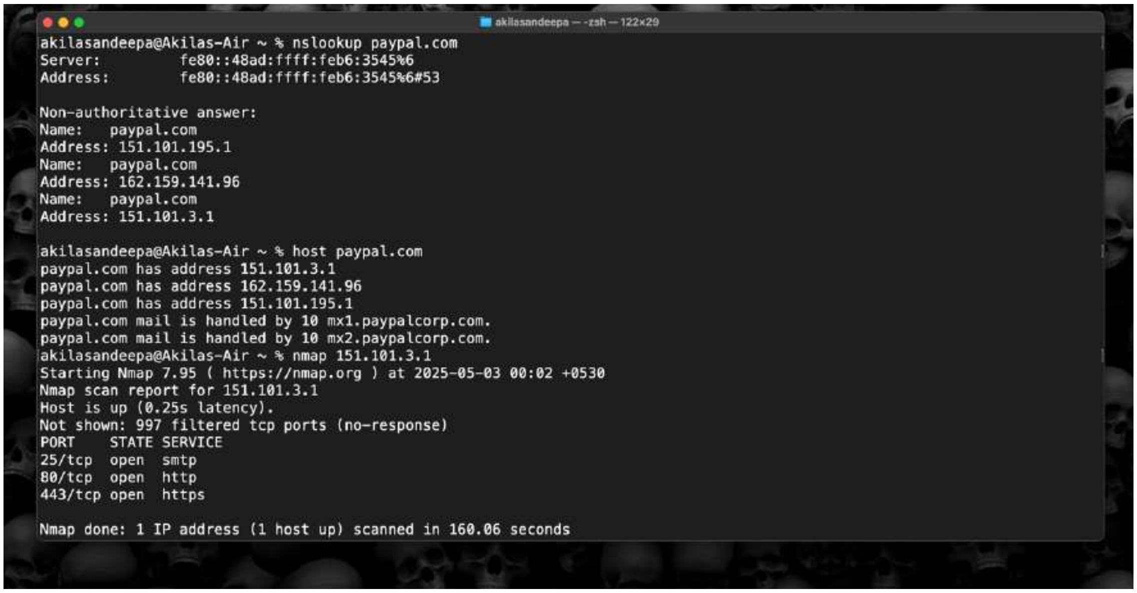
Impact Assessment

- Users could become victims to attackers who would induce them to send malicious requests that enable attackers to execute sensitive actions like password resets and account changes. The unauthorized execution could result in unwanted access and both data alteration and compromised accounts

Steps to Reproduce

- The user needs to access the impacted form such as password recovery form.
- The form submission should not contain any anti-CSRF tokens including csrf_token or CSRFToken and other similar identifiers.
- Create an easy HTML page which sends a POST request to the identical API while providing handpicked parameters.
- Users should access the malicious HTML page under their victim account authentication.
- The server confirms the request which proves the website has no anti-CSRF protection enabled.

Proof of Concept



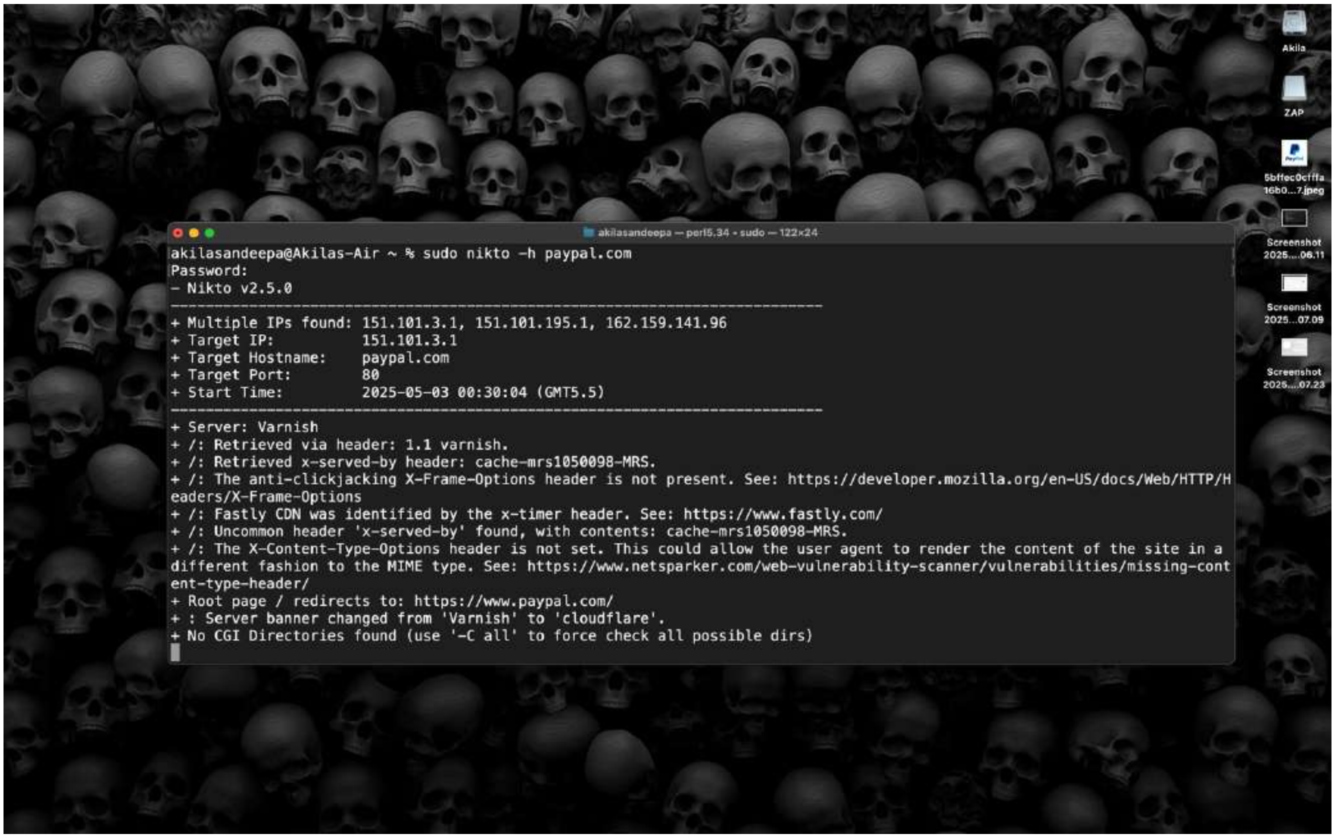
```
akilasandeepa@Akilas-Air ~ % nslookup paypal.com
Server:         fe80::48ad:ffff:feb6:3545%6
Address:        fe80::48ad:ffff:feb6:3545%6#53

Non-authoritative answer:
Name:   paypal.com
Address: 151.101.195.1
Name:   paypal.com
Address: 162.159.141.96
Name:   paypal.com
Address: 151.101.3.1

akilasandeepa@Akilas-Air ~ % host paypal.com
paypal.com has address 151.101.3.1
paypal.com has address 162.159.141.96
paypal.com has address 151.101.195.1
paypal.com mail is handled by 10 mx1.paypalcorp.com.
paypal.com mail is handled by 10 mx2.paypalcorp.com.
akilasandeepa@Akilas-Air ~ % nmap 151.101.3.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-03 00:02 +0530
Nmap scan report for 151.101.3.1
Host is up (0.25s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 160.06 seconds
```

Proposed Mitigation or Fix

- All state-changing requests and sensitive forms need to incorporate anti-CSRF tokens for protection.
- Every form needs a distinct unpredictable verification token which must be validated by the server upon user submission.
- Making use of well-known frameworks or libraries which include native protection methods against CSRF weak points helps eliminate this vulnerability

Scanned Vulnerabilities Using NIKTO

The X-Frame-Options header and X-Content-Type-Options header are missing from paypal.com during the Nikto scan because these security headers protect users from clickjacking vulnerabilities and prevent browsers from misinterpreting file types respectively. The scan detected uncommon HTTP headers as well as Fastly CDN and server banner changes yet did not discover any CGI directories or critical vulnerabilities. The security header misconfigurations were identified by the scan without the presence of critical vulnerabilities.

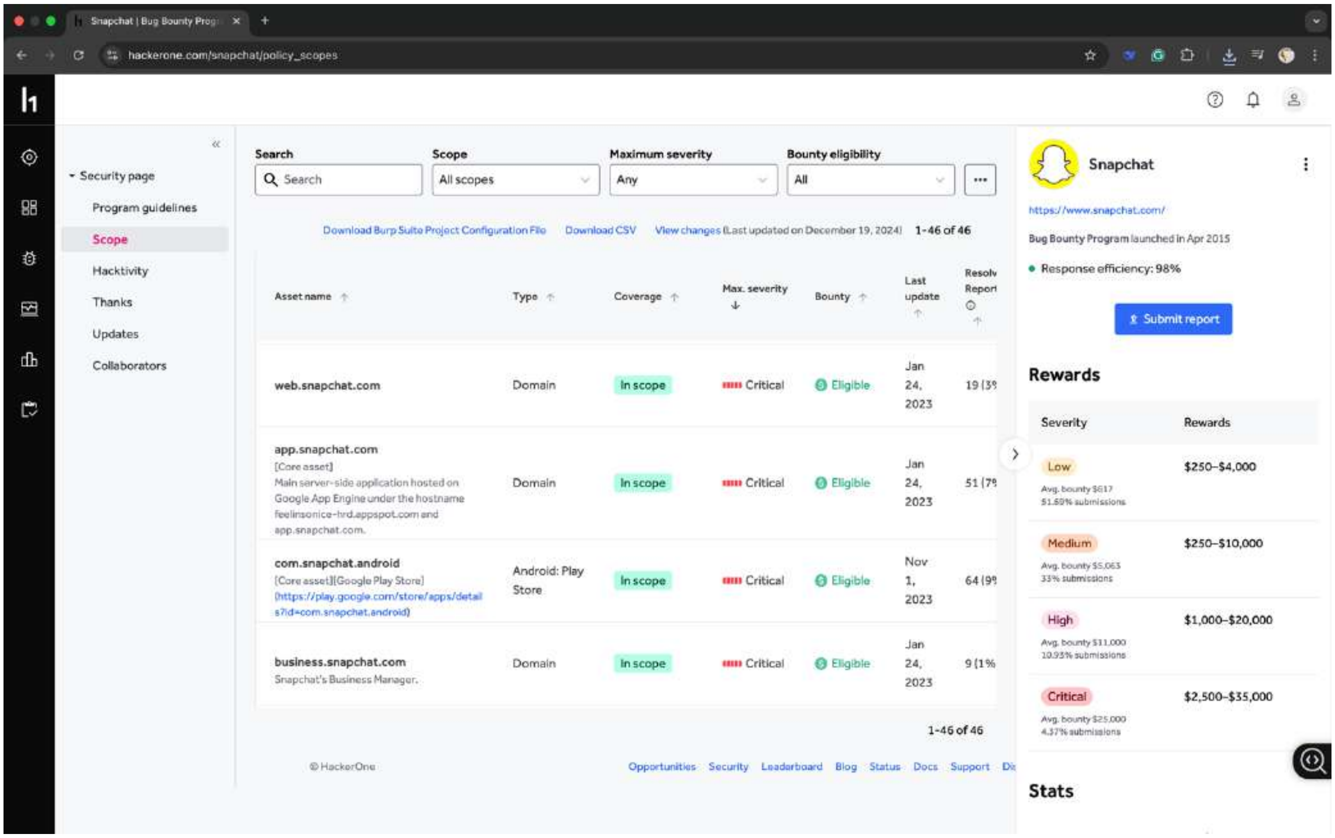


```
akilasandeepa@Akilas-Air ~ % sudo nikto -h paypal.com
Password:
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 151.101.3.1, 151.101.195.1, 162.159.141.96
+ Target IP:          151.101.3.1
+ Target Hostname:    paypal.com
+ Target Port:        80
+ Start Time:         2025-05-03 00:30:04 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Varnish
+ /: Retrieved via header: 1.1 varnish.
+ /: Retrieved x-served-by header: cache-mrs1050098-MRS.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/H
eaders/X-Frame-Options
+ /: Fastly CDN was identified by the x-timer header. See: https://www.fastly.com/
+ /: Uncommon header 'x-served-by' found, with contents: cache-mrs1050098-MRS.
+ /: 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-cont
ent-type-header/
+ Root page / redirects to: https://www.paypal.com/
+ : Server banner changed from 'Varnish' to 'cloudflare'.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

Report 07

Snapchat

Scope of the security audit according to https://hackerone.com/snapchat/policy_scopes is as follows.



Snapchat | Bug Bounty Prog
hackerone.com/snapchat/policy_scopes
Security page
Program guidelines
Scope
Hacktivity
Thanks
Updates
Collaborators
Submit report
Opportunities Security Leaderboard Blog Status Docs Support Di

Search: Search
Scope: All scopes
Maximum severity: Any
Bounty eligibility: All

Download Burp Suite Project Configuration File Download CSV View changes (Last updated on December 19, 2024) 1-46 of 46

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolv Report
web.snapchat.com	Domain	In scope	Critical	Eligible	Jan 24, 2023	19 (3!
app.snapchat.com [Core asset] Main server-side application hosted on Google App Engine under the hostname feelinsonice-hrd.appspot.com and app.snapchat.com.	Domain	In scope	Critical	Eligible	Jan 24, 2023	51 (7!
com.snapchat.android [Core asset][Google Play Store] (https://play.google.com/store/apps/details?id=com.snapchat.android)	Android: Play Store	In scope	Critical	Eligible	Nov 1, 2023	64 (9!
business.snapchat.com Snapchat's Business Manager.	Domain	In scope	Critical	Eligible	Jan 24, 2023	9 (1%

1-46 of 46

© HackerOne

Snapchat

https://www.snapchat.com/

Bug Bounty Program launched in Apr 2015

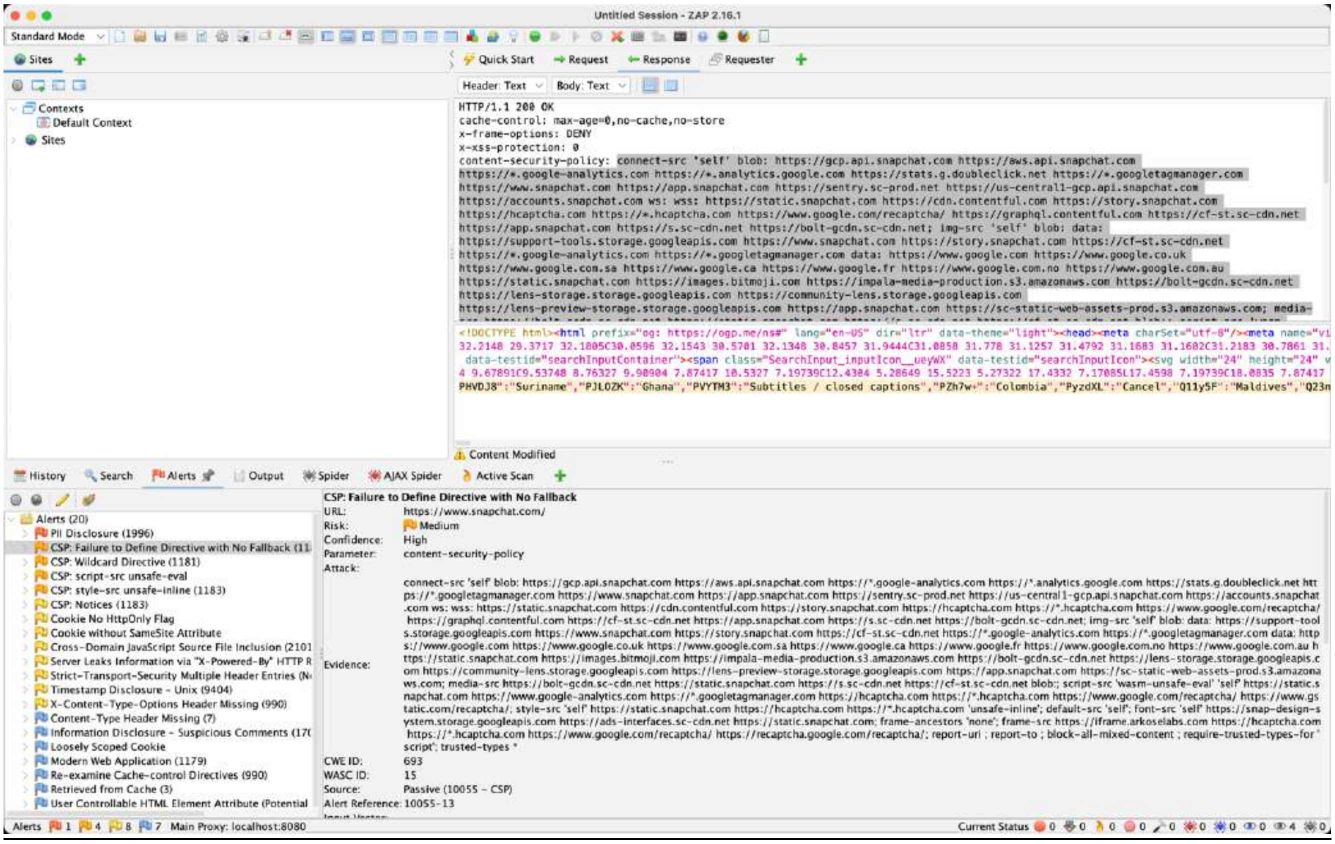
- Response efficiency: 98%

Rewards

Severity	Rewards
Low Avg. bounty $617 51.69% submissions	$250–$4,000
Medium Avg. bounty $5,063 33% submissions	$250–$10,000
High Avg. bounty $11,000 10.93% submissions	$1,000–$20,000
Critical Avg. bounty $25,000 4.37% submissions	$2,500–$35,000

Stats

Scanned Vulnerabilities Using ZAP



```
HTTP/1.1 200 OK
cache-control: max-age=0,no-cache,no-store
x-frame-options: DENY
x-xss-protection: 0
content-security-policy: connect-src 'self' blob: https://gcp.api.snapchat.com https://aws.api.snapchat.com
https://*.google-analytics.com https://*.analytics.google.com https://stats.g.doubleclick.net https://*.googletagmanager.com
https://www.snapchat.com https://app.snapchat.com https://sentry.sc-prod.net https://us-central1-gcp.api.snapchat.com
https://accounts.snapchat.com ws: wss: https://static.snapchat.com https://cdn.contentful.com https://story.snapchat.com
https://hcaptcha.com https://*.hcaptcha.com https://www.google.com/recaptcha/ https://graphql.contentful.com https://cf-st.sc-cdn.net
https://app.snapchat.com https://s.sc-cdn.net https://bolt-gcdn.sc-cdn.net; img-src 'self' blob: data:
https://support-tools.storage.googleapis.com https://www.snapchat.com https://story.snapchat.com https://cf-st.sc-cdn.net
https://*.google-analytics.com https://*.googletagmanager.com data: https://www.google.com https://www.google.co.uk
https://www.google.com.sa https://www.google.ca https://www.google.fr https://www.google.com.no https://www.google.com.au
https://static.snapchat.com https://images.bitmoji.com https://impala-media-production.s3.amazonaws.com https://bolt-gcdn.sc-cdn.net
https://lens-storage.storage.googleapis.com https://community-lens.storage.googleapis.com
https://lens-preview-storage.storage.googleapis.com https://app.snapchat.com https://sc-static-web-assets-prod.s3.amazonaws.com; media-
```

```
<!DOCTYPE html><html prefix="og: https://ogp.me/ns#" lang="en-US" dir="ltr" data-theme="light"><head><meta charSet="utf-8"/><meta name="vi
32.2148 29.3717 32.1805C30.0596 32.1543 30.5701 32.1348 30.8457 31.9444C31.0858 31.778 31.1257 31.4792 31.1683 31.1602C31.2183 30.7861 31.
 data-testid="searchInputContainer"><span class="SearchInput_inputIcon__ueyWX" data-testid="searchInputIcon"><svg width="24" height="24" v
4 9.67891C9.53748 8.76327 9.90904 7.87417 10.5327 7.19739C12.4384 5.28649 15.5223 5.27322 17.4332 7.17085L17.4598 7.19739C18.0835 7.87417
PHVDJ8":"Suriname","PJLOZK":"Ghana","PVYTM3":"Subtitles / closed captions","PZh7w+":"Colombia","PyzdXL":"Cancel","Q11y5F":"Maldives","Q23n
```

Alerts (20)
- PII Disclosure (1996)
- CSP: Failure to Define Directive with No Fallback (11
- CSP: Wildcard Directive (1181)
- CSP: script-src unsafe-eval
- CSP: style-src unsafe-inline (1183)
- CSP: Notices (1183)
- Cookie No HttpOnly Flag
- Cookie without SameSite Attribute
- Cross-Domain JavaScript Source File Inclusion (2101
- Server Leaks Information via "X-Powered-By" HTTP R
- Strict-Transport-Security Multiple Header Entries (N
- Timestamp Disclosure - Unix (9404)
- X-Content-Type-Options Header Missing (990)
- Content-Type Header Missing (7)
- Information Disclosure - Suspicious Comments (17(
- Loosely Scoped Cookie
- Modern Web Application (1179)
- Re-examine Cache-control Directives (990)
- Retrieved from Cache (3)
- User Controllable HTML Element Attribute (Potential

CSP: Failure to Define Directive with No Fallback

URL: https://www.snapchat.com/
Risk: Medium
Confidence: High
Parameter: content-security-policy
Attack:
Evidence: connect-src 'self' blob: https://gcp.api.snapchat.com https://aws.api.snapchat.com https://*.google-analytics.com https://*.analytics.google.com https://stats.g.doubleclick.net https://*.googletagmanager.com https://www.snapchat.com https://app.snapchat.com https://sentry.sc-prod.net https://us-central1-gcp.api.snapchat.com https://accounts.snapchat.com ws: wss: https://static.snapchat.com https://cdn.contentful.com https://story.snapchat.com https://hcaptcha.com https://*.hcaptcha.com https://www.google.com/recaptcha/ https://graphql.contentful.com https://cf-st.sc-cdn.net https://app.snapchat.com https://s.sc-cdn.net https://bolt-gcdn.sc-cdn.net; img-src 'self' blob: data: https://support-tools.storage.googleapis.com https://www.snapchat.com https://story.snapchat.com https://cf-st.sc-cdn.net https://*.google-analytics.com https://*.googletagmanager.com data: https://www.google.com https://www.google.co.uk https://www.google.com.sa https://www.google.ca https://www.google.fr https://www.google.com.no https://www.google.com.au https://static.snapchat.com https://images.bitmoji.com https://impala-media-production.s3.amazonaws.com https://bolt-gcdn.sc-cdn.net https://lens-storage.storage.googleapis.com https://community-lens.storage.googleapis.com https://lens-preview-storage.storage.googleapis.com https://app.snapchat.com https://sc-static-web-assets-prod.s3.amazonaws.com; media-src https://bolt-gcdn.sc-cdn.net https://static.snapchat.com https://s.sc-cdn.net https://cf-st.sc-cdn.net blob:; script-src 'wasm-unsafe-eval' 'self' https://static.snapchat.com https://www.google-analytics.com https://*.googletagmanager.com https://hcaptcha.com https://*.hcaptcha.com https://www.google.com/recaptcha/ https://www.gstatic.com/recaptcha/; style-src 'self' https://static.snapchat.com https://hcaptcha.com https://*.hcaptcha.com 'unsafe-inline'; default-src 'self'; font-src 'self' https://snap-design-system.storage.googleapis.com https://ads-interfaces.sc-cdn.net https://static.snapchat.com; frame-ancestors 'none'; frame-src https://iframe.arkoselabs.com https://hcaptcha.com https://*.hcaptcha.com https://www.google.com/recaptcha/ https://recaptcha.google.com/recaptcha/; report-uri ; report-to ; block-all-mixed-content ; require-trusted-types-for 'script'; trusted-types *
CWE ID: 693
WASC ID: 15
Source: Passive (10055 - CSP)
Alert Reference: 10055-13

Alerts 1 4 8 7 Main Proxy: localhost:8080

Current Status 0 0 0 0 0 0 0 0 4 0

Vulnerability Title Vulnerability Title

- CSP: Failure to Define Directive with No Fallback

Risk type

- Medium

Vulnerability Description

- The Content Security Policy (CSP) of the site has an incomplete configuration by withholding essential explicit instructions while dropping default-src as backup. Browsers allow content from various sources for missing directives that would otherwise protect the application from web-based attacks including XSS and clickjacking

URL

- https://www.snapchat.com/

Affected Components

- HTTP response headers for https://www.snapchat.com/
- Specifically, the Content-Security-Policy header and its configuration

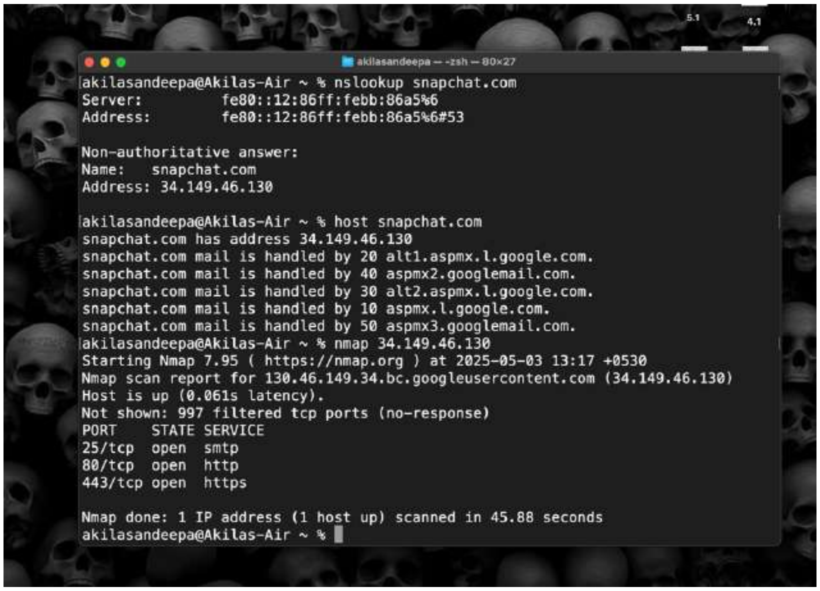
Impact Assessment

- Absence of proper CSP directives allows attackers to inject harmful scripts and load dangerous resources and embed sites within iframes which creates conditions for XSS attacks, data theft and clickjacking vulnerabilities.

Steps to Reproduce

- Access https://www.snapchat.com/ in a browser or use a web proxy tool (e.g., OWASP ZAP).
- The Content-Security-Policy header must be examined in HTTP response headers.
- Notice how several directives (including frame-ancestors) either have not been explicitly specified or they are absent from the policy.
- Ensure that these directives avoid settings that would result in default-src deactivated policies which leave domains open without restrictions

Proof of Concept



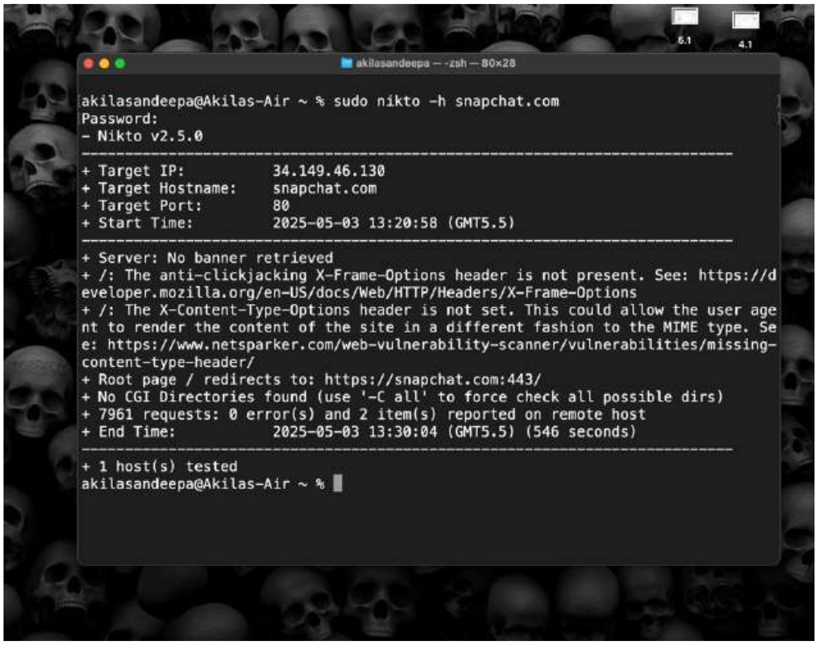
```
akilasandeepa@Akilas-Air ~ % nslookup snapchat.com
Server:         fe80::12:86ff:febb:86a5%6
Address:        fe80::12:86ff:febb:86a5%6#53

Non-authoritative answer:
Name:   snapchat.com
Address: 34.149.46.130

akilasandeepa@Akilas-Air ~ % host snapchat.com
snapchat.com has address 34.149.46.130
snapchat.com mail is handled by 20 alt1.aspmx.l.google.com.
snapchat.com mail is handled by 40 aspmx2.googlemail.com.
snapchat.com mail is handled by 30 alt2.aspmx.l.google.com.
snapchat.com mail is handled by 10 aspmx.l.google.com.
snapchat.com mail is handled by 50 aspmx3.googlemail.com.
akilasandeepa@Akilas-Air ~ % nmap 34.149.46.130
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-03 13:17 +0530
Nmap scan report for 130.46.149.34.bc.googleusercontent.com (34.149.46.130)
Host is up (0.061s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 45.88 seconds
akilasandeepa@Akilas-Air ~ % 
```

Proposed Mitigation or Fix

- Explicitly define all CSP directives that do not fallback to default-src, such as frame-ancestors, in the Content-Security-Policy header.

Scanned Vulnerabilities Using NIKTO

Nikto revealed that snapchat.com lacks two critical security headers including X-Frame-Options for clickjacking protection as well as X-Content-Type-Options for content-sniffing defense. The website lacks necessary security headers which presents possible web-based vulnerabilities but the scan did not identify any critical vulnerabilities or CGI directories.

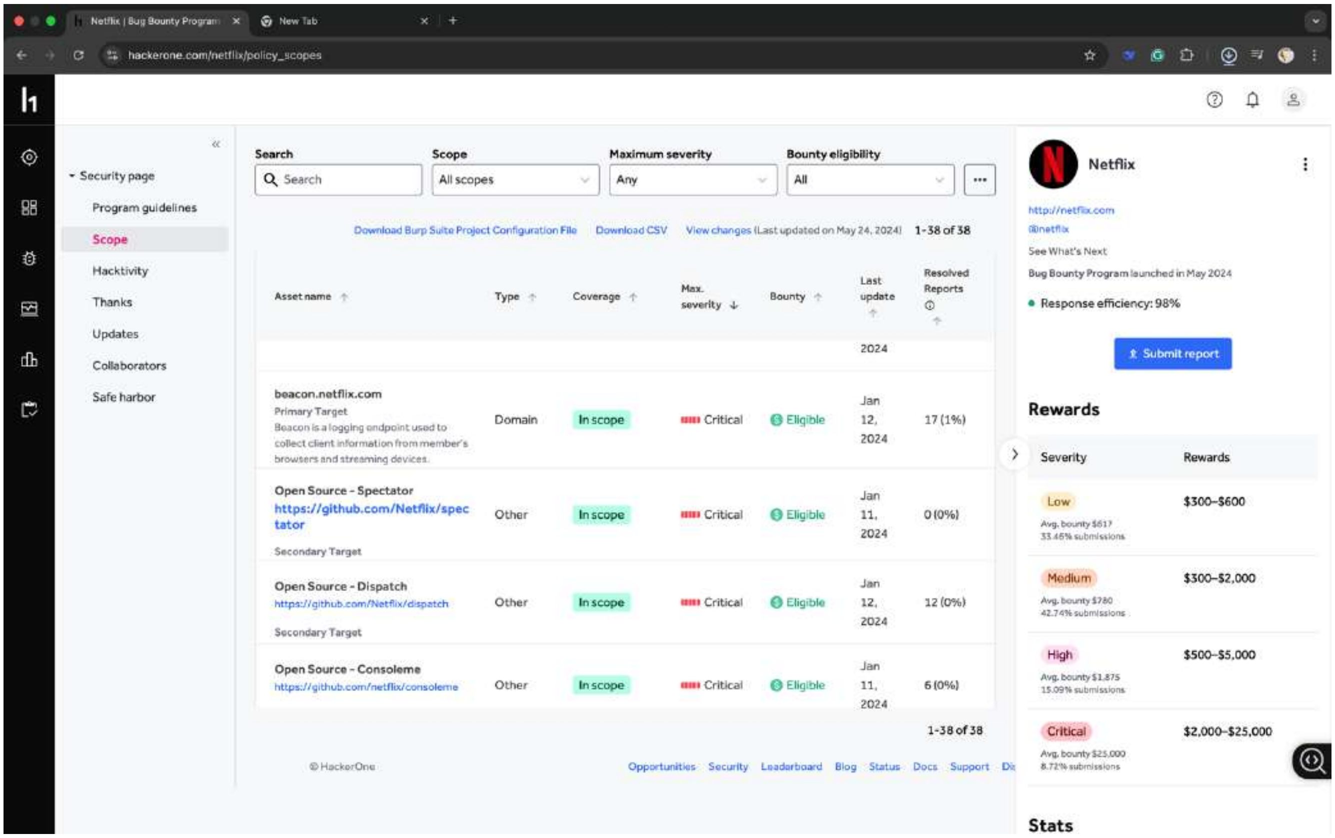


```
akilasandeepa@Akilas-Air ~ % sudo nikto -h snapchat.com
Password:
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          34.149.46.130
+ Target Hostname:    snapchat.com
+ Target Port:        80
+ Start Time:         2025-05-03 13:20:58 (GMT5.5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://d
eveloper.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 age
nt to render the content of the site in a different fashion to the MIME type. Se
e: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-
content-type-header/
+ Root page / redirects to: https://snapchat.com:443/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7961 requests: 0 error(s) and 2 item(s) reported on remote host
+ End Time:           2025-05-03 13:30:04 (GMT5.5) (546 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
akilasandeepa@Akilas-Air ~ %
```

Report 08

Netflix

Scope of the security audit according to https://hackerone.com/netflix/policy_scopes is as follows.



Search	Scope	Maximum severity	Bounty eligibility
Search	All scopes	Any	All

(Last updated on May 24, 2024) 1-38 of 38

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
					2024	
beacon.netflix.com Primary Target Beacon is a logging endpoint used to collect client information from member's browsers and streaming devices.	Domain	In scope	Critical	Eligible	Jan 12, 2024	17 (1%)
Open Source - Spectator https://github.com/Netflix/spectator Secondary Target	Other	In scope	Critical	Eligible	Jan 11, 2024	0 (0%)
Open Source - Dispatch https://github.com/Netflix/dispatch Secondary Target	Other	In scope	Critical	Eligible	Jan 12, 2024	12 (0%)
Open Source - Consoleme https://github.com/netflix/consoleme	Other	In scope	Critical	Eligible	Jan 11, 2024	6 (0%)

1-38 of 38

Netflix

http://netflix.com

@netflix

See What's Next

Bug Bounty Program launched in May 2024

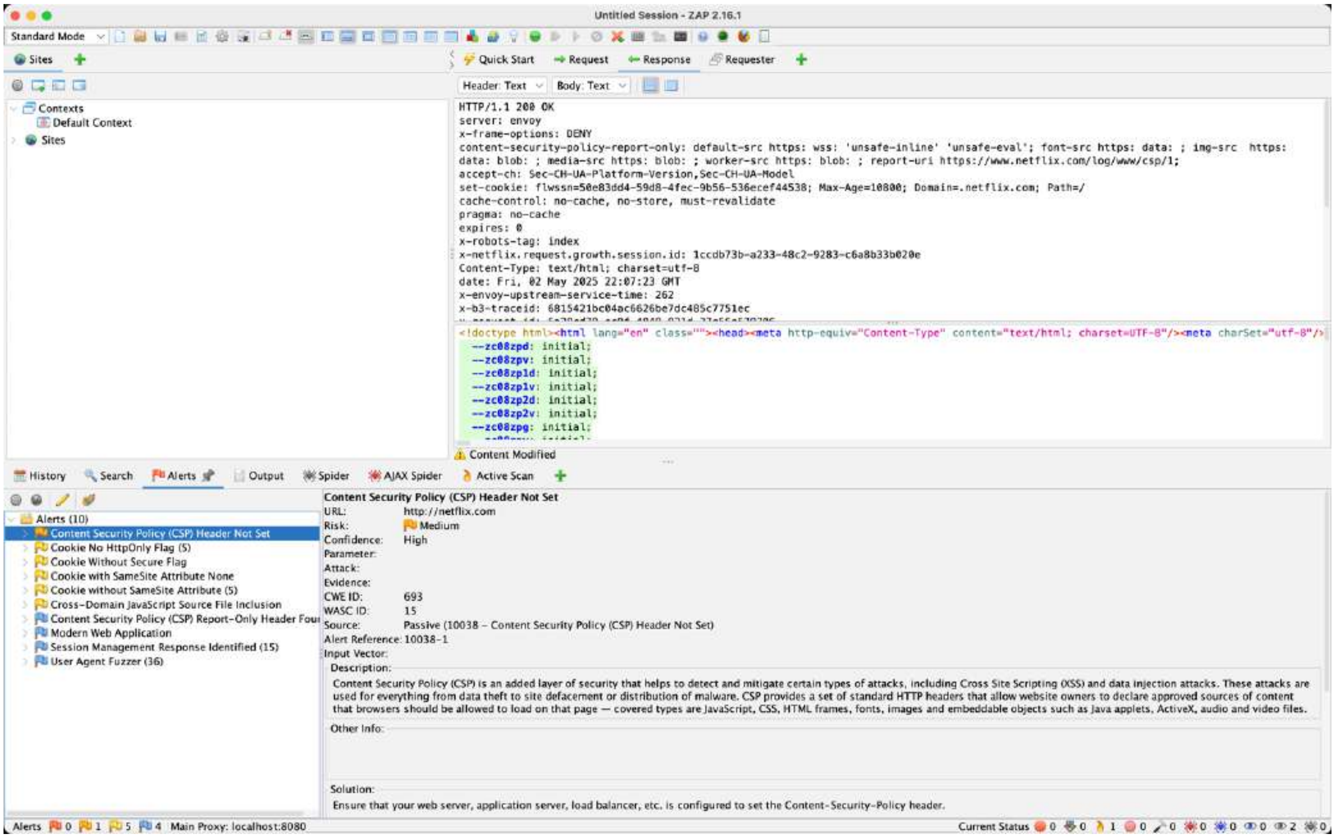
- Response efficiency: 98%

Rewards

Severity	Rewards
Low Avg. bounty $617 33.45% submissions	$300–$600
Medium Avg. bounty $780 42.74% submissions	$300–$2,000
High Avg. bounty $1,875 15.09% submissions	$500–$5,000
Critical Avg. bounty $25,000 8.72% submissions	$2,000–$25,000

Stats

Scanned Vulnerabilities Using ZAP



```
HTTP/1.1 200 OK
server: envoy
x-frame-options: DENY
content-security-policy-report-only: default-src https: wss: 'unsafe-inline' 'unsafe-eval'; font-src https: data: ; img-src  https:
data: blob: ; media-src https: blob: ; worker-src https: blob: ; report-uri https://www.netflix.com/log/www/csp/1;
accept-ch: Sec-CH-UA-Platform-Version,Sec-CH-UA-Model
set-cookie: flwssn=50e83dd4-59d8-4fec-9b56-536ecef44538; Max-Age=10800; Domain=.netflix.com; Path=/
cache-control: no-cache, no-store, must-revalidate
pragma: no-cache
expires: 0
x-robots-tag: index
x-netflix.request.growth.session.id: 1ccdb73b-a233-48c2-9283-c6a8b33b020e
Content-Type: text/html; charset=utf-8
date: Fri, 02 May 2025 22:07:23 GMT
x-envoy-upstream-service-time: 262
x-b3-traceid: 6815421bc04ac6626be7dc485c7751ec
```

```
<!doctype html><html lang="en" class=""><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/><meta charSet="utf-8"/>
  --zc08zpd: initial;
  --zc08zpv: initial;
  --zc08zp1d: initial;
  --zc08zp1v: initial;
  --zc08zp2d: initial;
  --zc08zp2v: initial;
  --zc08zpg: initial;
```

Alerts (10)
- Content Security Policy (CSP) Header Not Set
- Cookie No HttpOnly Flag (5)
- Cookie Without Secure Flag
- Cookie with SameSite Attribute None
- Cookie without SameSite Attribute (5)
- Cross-Domain JavaScript Source File Inclusion
- Content Security Policy (CSP) Report-Only Header Four
- Modern Web Application
- Session Management Response Identified (15)
- User Agent Fuzzer (36)

Content Security Policy (CSP) Header Not Set
URL: http://netflix.com
Risk: Medium
Confidence: High
Parameter:
Attack:
Evidence:
CWE ID: 693
WASC ID: 15
Source: Passive (10038 – Content Security Policy (CSP) Header Not Set)
Alert Reference: 10038-1
Input Vector:
Description:
Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Other Info:
Solution:
Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Alerts 0 1 5 4 Main Proxy: localhost:8080 Current Status 0 0 1 0 0 0 0 0 2 0

Vulnerability Title Vulnerability Title

- Content Security Policy (CSP) Header Not Set

Risk type

- Medium

Vulnerability Description

- The web server of netflix.com fails to present the Content Security Policy (CSP) HTTP header in its generated responses. CSP functions as a security standard which stops multiple attacks like XSS and data injection through browser restrictions on source content loading and execution. The site becomes more vulnerable to client-side attacks because it lacks the Content Security Policy header which protects against such threats

Affected Components

- Web server and HTTP response configuration for netflix.com

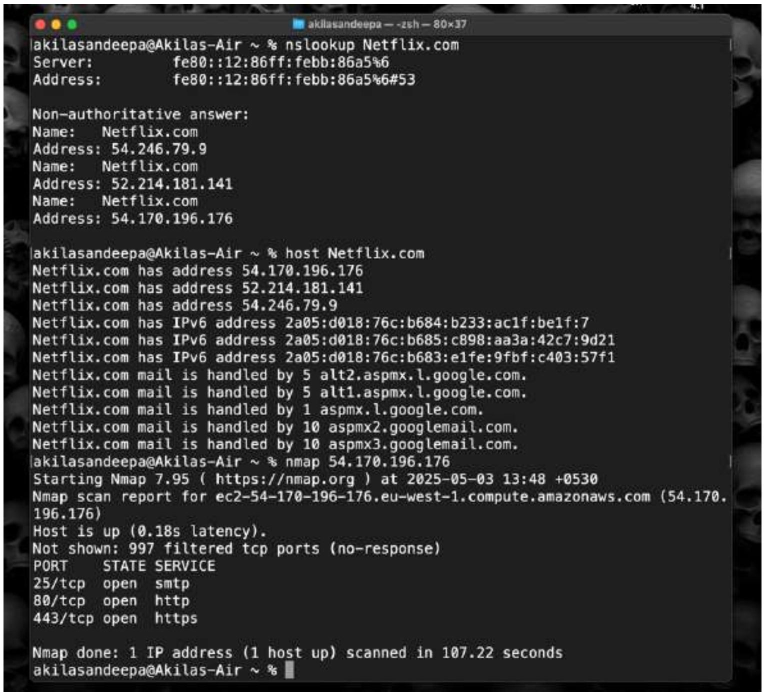
Impact Assessment

- The website faces threats from attackers who could undertake malicious actions by injecting dangerous code while stealing data and damaging its appearance.
- Browsers receive unrestricted access to load any resources (scripts, styles, images) without administrator control

Steps to Reproduce

- The OWASP ZAP or similar web proxy tool should intercept HTTP responses that originate from netflix.com.
- Proceed to check HTTP headers for the absence of Content-Security-Policy header

Proof of Concept



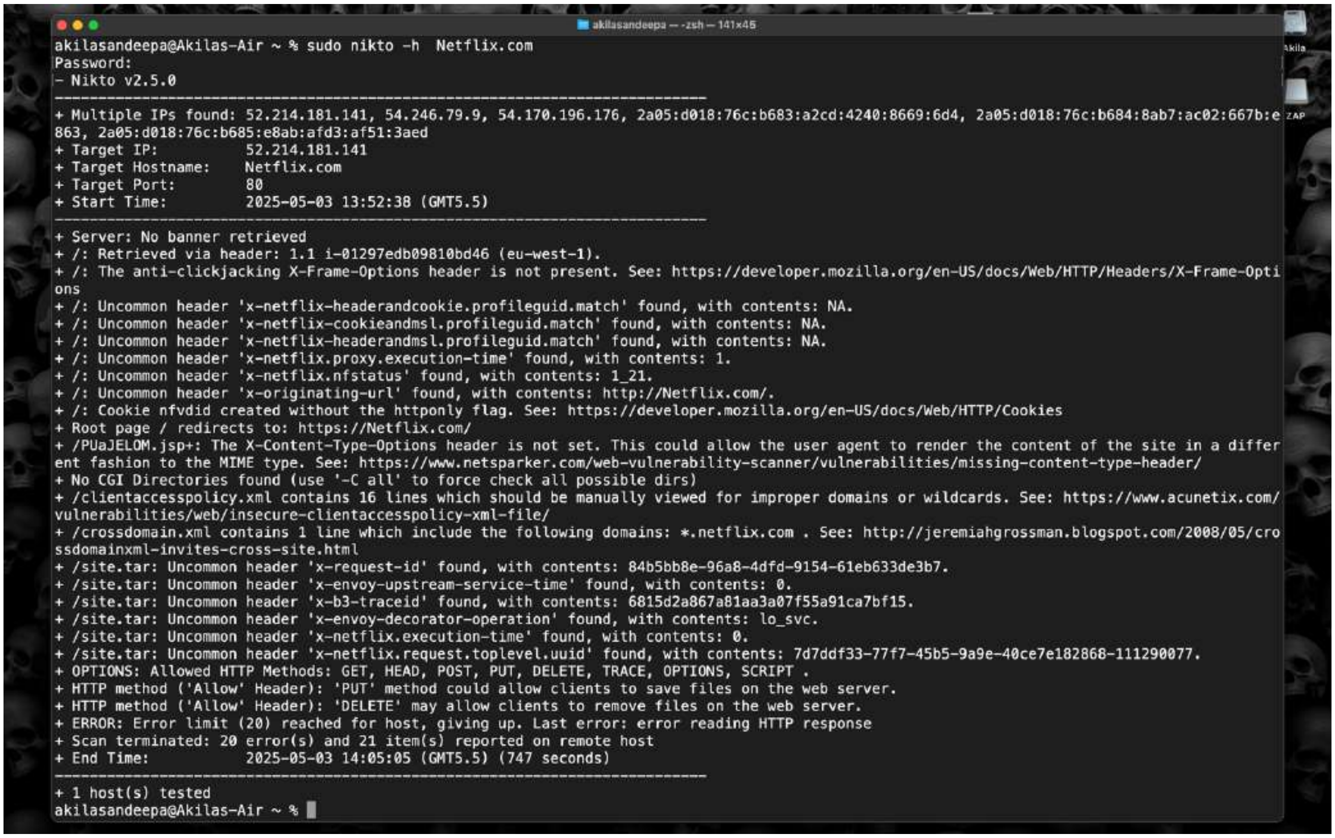
```
akilasandeepa@Akilas-Air ~ % nslookup Netflix.com
Server:         fe80::12:86ff:febb:86a5%6
Address:        fe80::12:86ff:febb:86a5%6#53

Non-authoritative answer:
Name:   Netflix.com
Address: 54.246.79.9
Name:   Netflix.com
Address: 52.214.181.141
Name:   Netflix.com
Address: 54.170.196.176

akilasandeepa@Akilas-Air ~ % host Netflix.com
Netflix.com has address 54.170.196.176
Netflix.com has address 52.214.181.141
Netflix.com has address 54.246.79.9
Netflix.com has IPv6 address 2a05:d018:76c:b684:b233:ac1f:be1f:7
Netflix.com has IPv6 address 2a05:d018:76c:b685:c898:aa3a:42c7:9d21
Netflix.com has IPv6 address 2a05:d018:76c:b683:e1fe:9fbf:c403:57f1
Netflix.com mail is handled by 5 alt2.aspmx.l.google.com.
Netflix.com mail is handled by 5 alt1.aspmx.l.google.com.
Netflix.com mail is handled by 1 aspmx.l.google.com.
Netflix.com mail is handled by 10 aspmx2.googlemail.com.
Netflix.com mail is handled by 10 aspmx3.googlemail.com.
akilasandeepa@Akilas-Air ~ % nmap 54.170.196.176
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-03 13:48 +0530
Nmap scan report for ec2-54-170-196-176.eu-west-1.compute.amazonaws.com (54.170.
196.176)
Host is up (0.18s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 107.22 seconds
akilasandeepa@Akilas-Air ~ %
```

Proposed Mitigation or Fix

- All outgoing HTTP responses should contain a strict Content-Security-Policy header through configuration of either the web server or application.
- Implement ongoing CSP monitoring to allow necessary resources through updates that minimize client-side security dangers.

Scanned Vulnerabilities Using NIKTO

The security header X-Frame-Options is absent from netflix.com alongside X-Content-Type-Options which protects against incorrect browser file interpretation thus causing greater vulnerabilities to web-based attacks and misconfigurations.

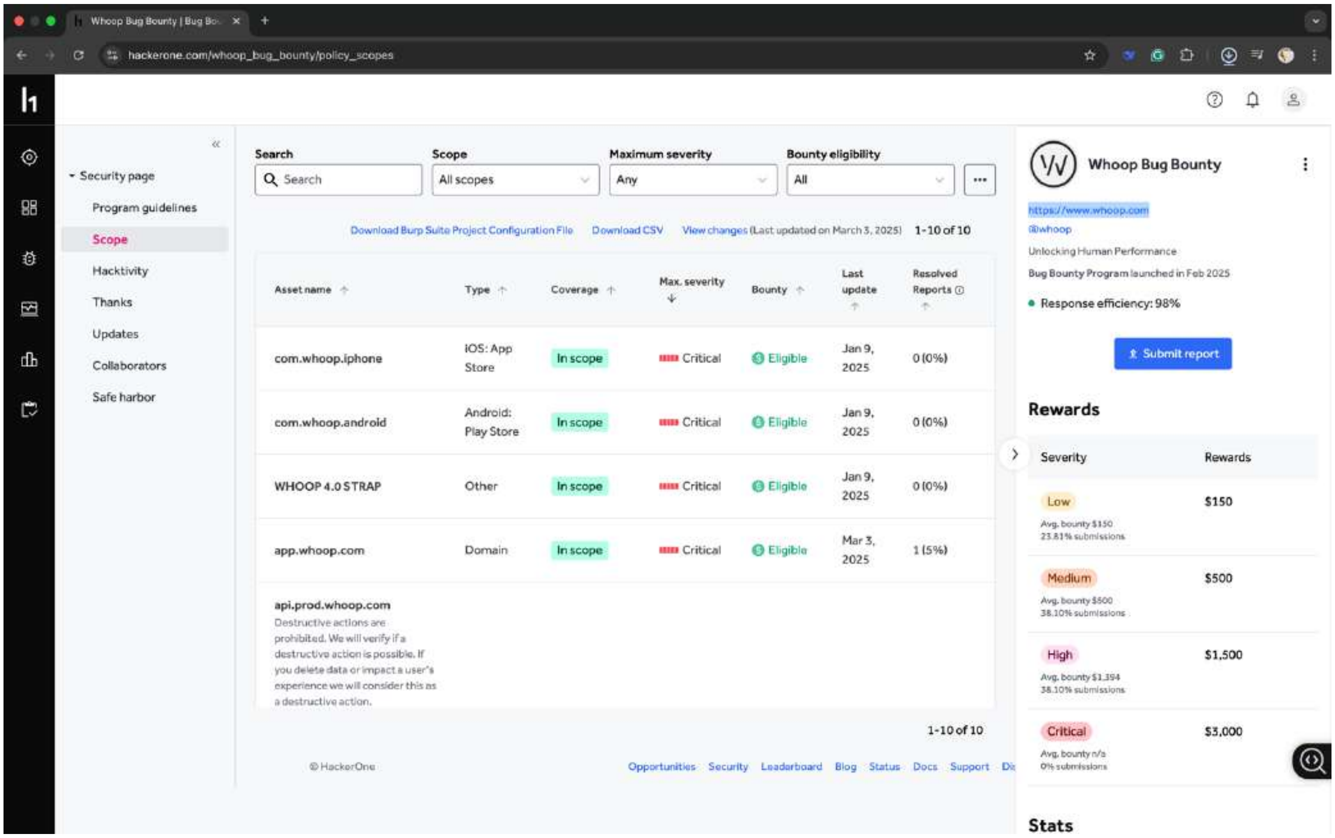


```
akilasandeepa@Akilas-Air ~ % sudo nikto -h  Netflix.com
Password:
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 52.214.181.141, 54.246.79.9, 54.170.196.176, 2a05:d018:76c:b683:a2cd:4240:8669:6d4, 2a05:d018:76c:b684:8ab7:ac02:667b:e
863, 2a05:d018:76c:b685:e8ab:afd3:af51:3aed
+ Target IP:          52.214.181.141
+ Target Hostname:    Netflix.com
+ Target Port:        80
+ Start Time:         2025-05-03 13:52:38 (GMT5.5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ /: Retrieved via header: 1.1 i-01297edb09810bd46 (eu-west-1).
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Opti
ons
+ /: Uncommon header 'x-netflix-headerandcookie.profileguid.match' found, with contents: NA.
+ /: Uncommon header 'x-netflix-cookieandmsl.profileguid.match' found, with contents: NA.
+ /: Uncommon header 'x-netflix-headerandmsl.profileguid.match' found, with contents: NA.
+ /: Uncommon header 'x-netflix.proxy.execution-time' found, with contents: 1.
+ /: Uncommon header 'x-netflix.nfstatus' found, with contents: 1_21.
+ /: Uncommon header 'x-originating-url' found, with contents: http://Netflix.com/.
+ /: Cookie nfvdid created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ Root page / redirects to: https://Netflix.com/
+ /PUaJELOM.jsp+: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a differ
ent fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /clientaccesspolicy.xml contains 16 lines which should be manually viewed for improper domains or wildcards. See: https://www.acunetix.com/
vulnerabilities/web/insecure-clientaccesspolicy-xml-file/
+ /crossdomain.xml contains 1 line which include the following domains: *.netflix.com . See: http://jeremiahgrossman.blogspot.com/2008/05/cro
ssdomainxml-invites-cross-site.html
+ /site.tar: Uncommon header 'x-request-id' found, with contents: 84b5bb8e-96a8-4dfd-9154-61eb633de3b7.
+ /site.tar: Uncommon header 'x-envoy-upstream-service-time' found, with contents: 0.
+ /site.tar: Uncommon header 'x-b3-traceid' found, with contents: 6815d2a867a81aa3a07f55a91ca7bf15.
+ /site.tar: Uncommon header 'x-envoy-decorator-operation' found, with contents: lo_svc.
+ /site.tar: Uncommon header 'x-netflix.execution-time' found, with contents: 0.
+ /site.tar: Uncommon header 'x-netflix.request.toplevel.uuid' found, with contents: 7d7ddf33-77f7-45b5-9a9e-40ce7e182868-111290077.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS, SCRIPT .
+ HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 21 item(s) reported on remote host
+ End Time:           2025-05-03 14:05:05 (GMT5.5) (747 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
akilasandeepa@Akilas-Air ~ % █
```

Report 09

Whoop Bug Bounty

Scope of the security audit according to https://hackerone.com/whoop_bug_bounty/policy_scopes is as follows.



(Last updated on March 3, 2025) 1-10 of 10

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
com.whoop.iphone	iOS: App Store	In scope	Critical	Eligible	Jan 9, 2025	0 (0%)
com.whoop.android	Android: Play Store	In scope	Critical	Eligible	Jan 9, 2025	0 (0%)
WHOOP 4.0 STRAP	Other	In scope	Critical	Eligible	Jan 9, 2025	0 (0%)
app.whoop.com	Domain	In scope	Critical	Eligible	Mar 3, 2025	1 (5%)
api.prod.whoop.com Destructive actions are prohibited. We will verify if a destructive action is possible. If you delete data or impact a user's experience we will consider this as a destructive action.						

1-10 of 10

Whoop Bug Bounty

https://www.whoop.com
@whoop
Unlocking Human Performance
Bug Bounty Program launched in Feb 2025

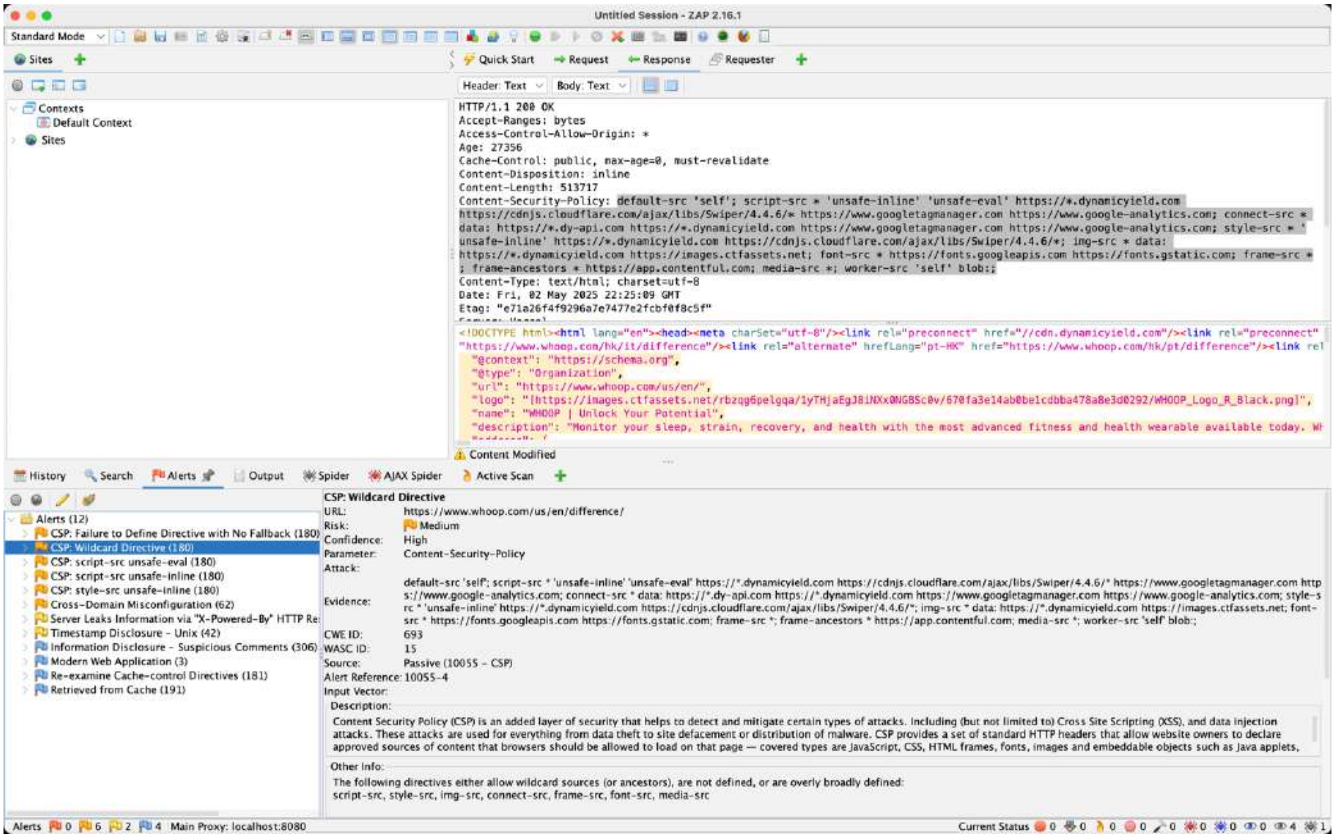
- Response efficiency: 98%

Rewards

Severity	Rewards
Low Avg. bounty $150 23.81% submissions	$150
Medium Avg. bounty $500 38.10% submissions	$500
High Avg. bounty $1,394 38.10% submissions	$1,500
Critical Avg. bounty n/a 0% submissions	$3,000

Stats

Scanned Vulnerabilities Using ZAP



```
HTTP/1.1 200 OK
Accept-Ranges: bytes
Access-Control-Allow-Origin: *
Age: 27356
Cache-Control: public, max-age=0, must-revalidate
Content-Disposition: inline
Content-Length: 513717
Content-Security-Policy: default-src 'self'; script-src * 'unsafe-inline' 'unsafe-eval' https://*.dynamicyield.com
https://cdnjs.cloudflare.com/ajax/libs/Swiper/4.4.6/* https://www.googletagmanager.com https://www.google-analytics.com; connect-src *
data: https://*.dy-api.com https://*.dynamicyield.com https://www.googletagmanager.com https://www.google-analytics.com; style-src * '
unsafe-inline' https://*.dynamicyield.com https://cdnjs.cloudflare.com/ajax/libs/Swiper/4.4.6/*; img-src * data:
https://*.dynamicyield.com https://images.ctfassets.net; font-src * https://fonts.googleapis.com https://fonts.gstatic.com; frame-src *
; frame-ancestors * https://app.contentful.com; media-src *; worker-src 'self' blob:;
Content-Type: text/html; charset=utf-8
Date: Fri, 02 May 2025 22:25:09 GMT
Etag: "e71a26f4f9296a7e7477e2fcbf0f8c5f"
```

```
<!DOCTYPE html><html lang="en"><head><meta charSet="utf-8"/><link rel="preconnect" href="//cdn.dynamicyield.com"/><link rel="preconnect"
"https://www.whoop.com/hk/it/difference"/><link rel="alternate" hrefLang="pt-HK" href="https://www.whoop.com/hk/pt/difference"/><link rel
  "@context": "https://schema.org",
  "@type": "Organization",
  "url": "https://www.whoop.com/us/en/",
  "logo": "[https://images.ctfassets.net/rbzqg6pelgqa/1yTHjaEgJ8iNXx0NGBSc0v/670fa3e14ab0be1cdbba478a8e3d0292/WHOOP_Logo_R_Black.png]",
  "name": "WHOOP | Unlock Your Potential",
  "description": "Monitor your sleep, strain, recovery, and health with the most advanced fitness and health wearable available today. Wh
```

Alerts (12)
- CSP: Failure to Define Directive with No Fallback (180)
- CSP: Wildcard Directive (180)
- CSP: script-src unsafe-eval (180)
- CSP: script-src unsafe-inline (180)
- CSP: style-src unsafe-inline (180)
- Cross-Domain Misconfiguration (62)
- Server Leaks Information via "X-Powered-By" HTTP Re
- Timestamp Disclosure - Unix (42)
- Information Disclosure - Suspicious Comments (306)
- Modern Web Application (3)
- Re-examine Cache-control Directives (181)
- Retrieved from Cache (191)

CSP: Wildcard Directive
URL: https://www.whoop.com/us/en/difference/
Risk: Medium
Confidence: High
Parameter: Content-Security-Policy
Attack:
Evidence: default-src 'self'; script-src * 'unsafe-inline' 'unsafe-eval' https://*.dynamicyield.com https://cdnjs.cloudflare.com/ajax/libs/Swiper/4.4.6/* https://www.googletagmanager.com https://www.google-analytics.com; connect-src * data: https://*.dy-api.com https://*.dynamicyield.com https://www.googletagmanager.com https://www.google-analytics.com; style-src * 'unsafe-inline' https://*.dynamicyield.com https://cdnjs.cloudflare.com/ajax/libs/Swiper/4.4.6/*; img-src * data: https://*.dynamicyield.com https://images.ctfassets.net; font-src * https://fonts.googleapis.com https://fonts.gstatic.com; frame-src *; frame-ancestors * https://app.contentful.com; media-src *; worker-src 'self' blob:;
CWE ID: 693
WASC ID: 15
Source: Passive (10055 - CSP)
Alert Reference: 10055-4
Input Vector:
Description:
Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets,
Other Info:
The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined:
script-src, style-src, img-src, connect-src, frame-src, font-src, media-src

Vulnerability Title Vulnerability Title

- CSP Wildcard Directive and Unsafe Source Allowance

Risk type

- Medium

Vulnerability Description

- Whoop.com executes its Content Security Policy on its URL /en/difference/ using wildcard policies which admit both 'unsafe-inline' and 'unsafe-eval' source categories. The weak configuration of the CSP policy weakens security effectiveness making https://www.whoop.com/en/difference/ susceptible to attacks through XSS and data injection vectors because attackers can inject malicious scripts

Affected Components

- HTTP response headers, specifically the Content-Security-Policy header

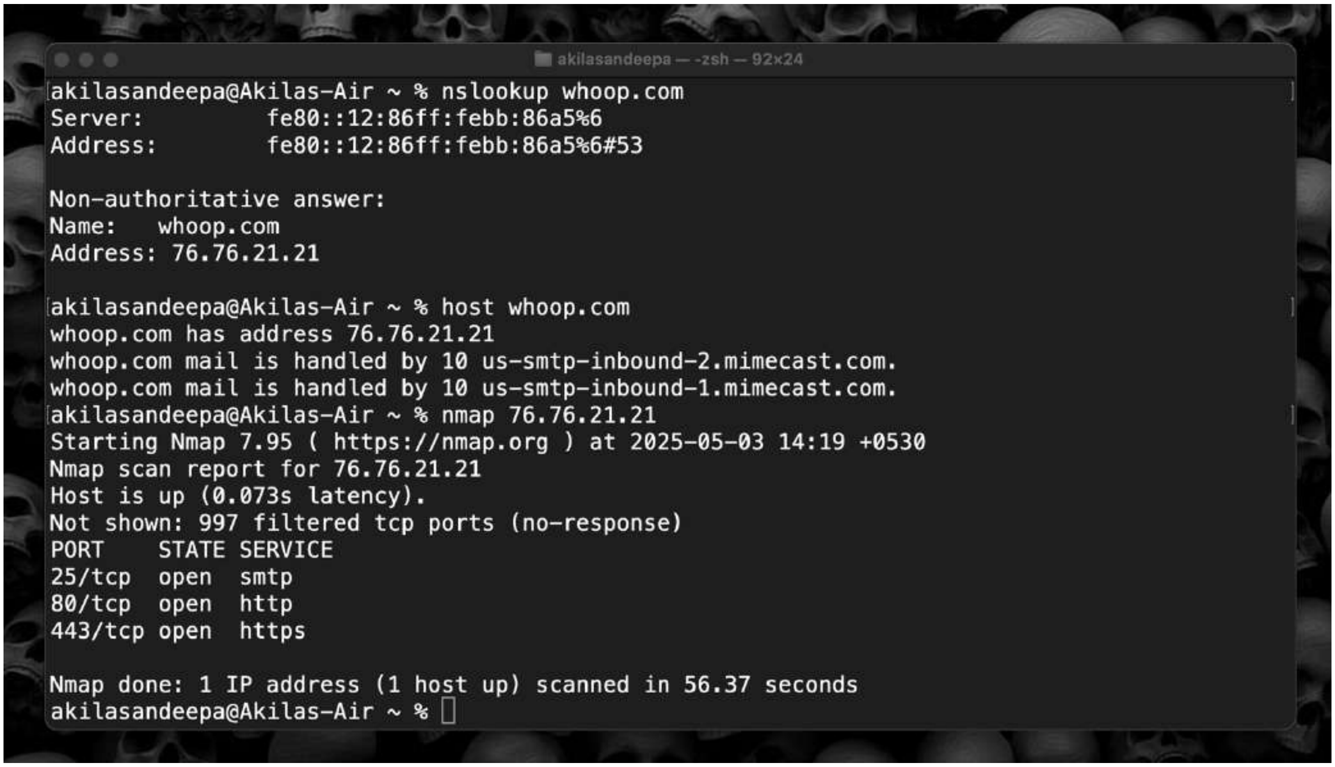
Impact Assessment

- Attackers use such security flaws to execute unauthorized browser scripts that target users' systems

Steps to Reproduce

- can reach www.whoop.com/en/difference/ through any browser but also through a proxy tool like OWASP ZAP.
- Check whether the HTTP response headers contain a Content-Security-Policy header.
- Examine how the policy makes use of wildcard sources (*) while containing two unsafe directives ('unsafe-inline', 'unsafe-eval')

Proof of Concept



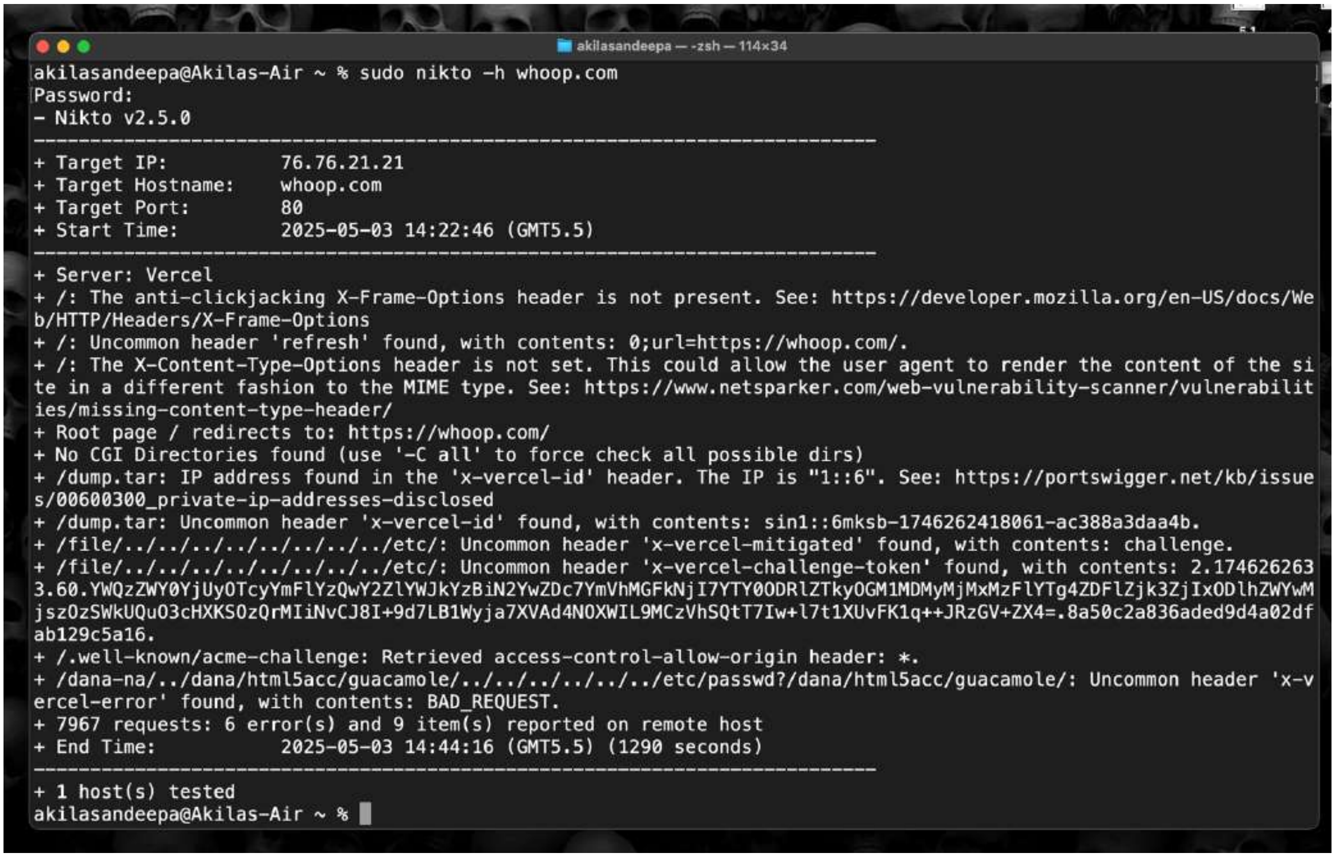
```
akilasandeepa@Akilas-Air ~ % nslookup whoop.com
Server:         fe80::12:86ff:febb:86a5%6
Address:        fe80::12:86ff:febb:86a5%6#53

Non-authoritative answer:
Name:   whoop.com
Address: 76.76.21.21

akilasandeepa@Akilas-Air ~ % host whoop.com
whoop.com has address 76.76.21.21
whoop.com mail is handled by 10 us-smtp-inbound-2.mimecast.com.
whoop.com mail is handled by 10 us-smtp-inbound-1.mimecast.com.
akilasandeepa@Akilas-Air ~ % nmap 76.76.21.21
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-03 14:19 +0530
Nmap scan report for 76.76.21.21
Host is up (0.073s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 56.37 seconds
akilasandeepa@Akilas-Air ~ %
```

Proposed Mitigation or Fix

- The access allowed by CSP must exclude wildcard (*). Additionally the 'unsafe-inline' and 'unsafe-eval' script directive values must not be used in the policy.
- Each CSP directive should contain its sources limited to only verified domains.
- The CSP requires frequent assessments to maintain its effectiveness by establishing strict limitations for script and style and image and additional resource sources.
- Check the enhanced policy to make sure it maintains all functional aspects of the site without compromising security measures

Scanned Vulnerabilities Using NIKTO

A Nikto scan of whoop.com reveals security header deficiencies which include X-Frame-Options and X-Content-Type-Options because these protections prevent clickjacking vulnerabilities and browser security issues.



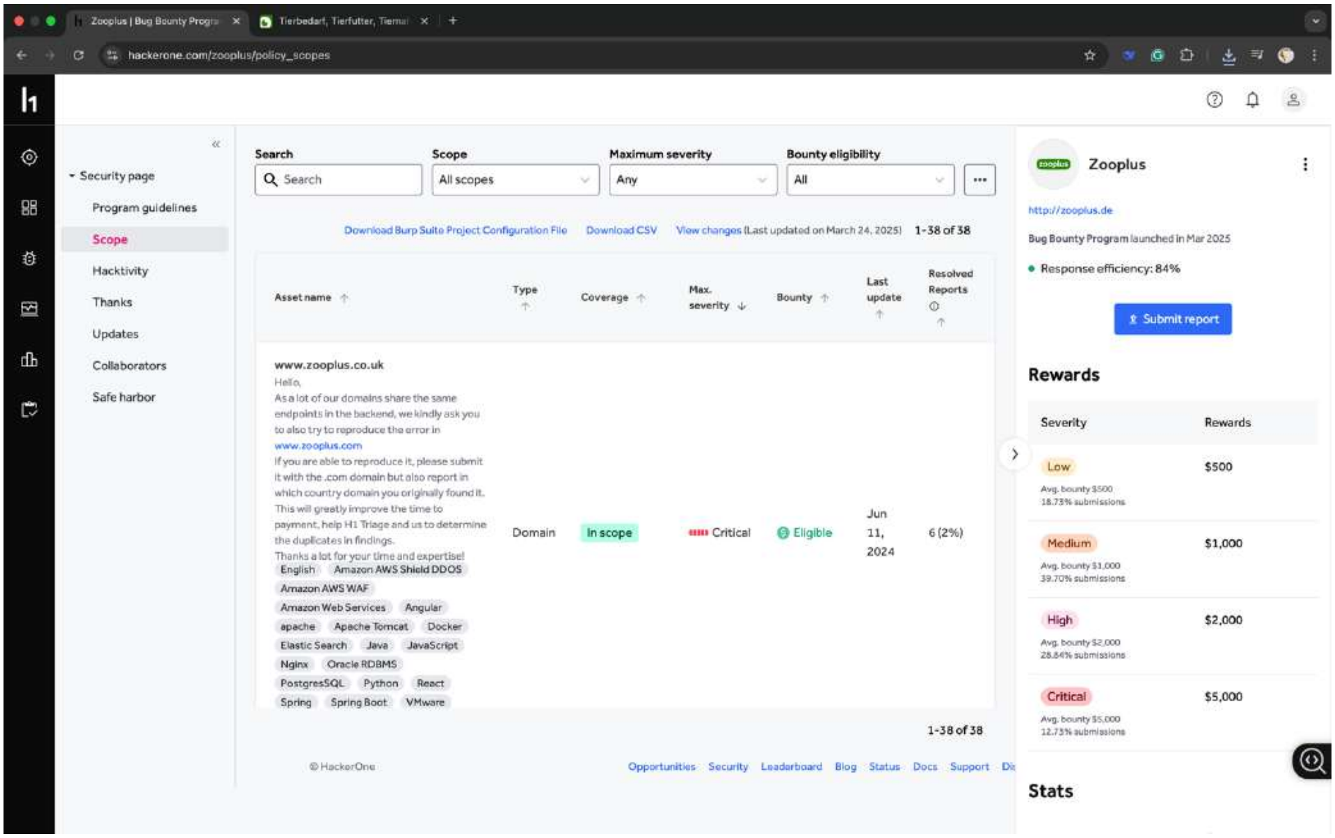
```
akilasandeepa@Akilas-Air ~ % sudo nikto -h whoop.com
Password:
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          76.76.21.21
+ Target Hostname:    whoop.com
+ Target Port:        80
+ Start Time:         2025-05-03 14:22:46 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Vercel
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/We
b/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'refresh' found, with contents: 0;url=https://whoop.com/.
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the si
te in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilit
ies/missing-content-type-header/
+ Root page / redirects to: https://whoop.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /dump.tar: IP address found in the 'x-vercel-id' header. The IP is "1::6". See: https://portswigger.net/kb/issue
s/00600300_private-ip-addresses-disclosed
+ /dump.tar: Uncommon header 'x-vercel-id' found, with contents: sin1::6mksb-1746262418061-ac388a3daa4b.
+ /file/../../../../../../../../etc/: Uncommon header 'x-vercel-mitigated' found, with contents: challenge.
+ /file/../../../../../../../../etc/: Uncommon header 'x-vercel-challenge-token' found, with contents: 2.174626263
3.60.YWQzZWY0YjUyOTcyYmFlYzQwY2ZlYWJkYzBiN2YwZDc7YmVhMGFkNjI7YTY0ODRlZTkyOGM1MDMyMjMxMzFlYTg4ZDFlZjk3ZjIxODlhZWYwM
jszOzSWkUQuO3cHXKSOzQrMIiNvCJ8I+9d7LB1Wyja7XVAd4NOXWIL9MCzVhSQtT7Iw+l7t1XUvFK1q++JRzGV+ZX4=.8a50c2a836aded9d4a02df
ab129c5a16.
+ /.well-known/acme-challenge: Retrieved access-control-allow-origin header: *.
+ /dana-na/../dana/html5acc/guacamole/../../../../../../etc/passwd?/dana/html5acc/guacamole/: Uncommon header 'x-v
ercel-error' found, with contents: BAD_REQUEST.
+ 7967 requests: 6 error(s) and 9 item(s) reported on remote host
+ End Time:           2025-05-03 14:44:16 (GMT5.5) (1290 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
akilasandeepa@Akilas-Air ~ %
```

Report 10

Zooplus

zooplus

Scope of the security audit according to https://hackerone.com/zooplus/policy_scopes is as follows.



Zooplus | Bug Bounty Progra

Tierbedarf, Tierfutter, Tiernal

hackerone.com/zooplus/policy_scopes

- Security page
  - Program guidelines
  - Scope
  - Hacktivity
  - Thanks
  - Updates
  - Collaborators
  - Safe harbor

Search: Search

Scope: All scopes

Maximum severity: Any

Bounty eligibility: All

Download Burp Suite Project Configuration File · Download CSV · View changes (Last updated on March 24, 2025) 1-38 of 38

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
www.zooplus.co.uk Hello, As a lot of our domains share the same endpoints in the backend, we kindly ask you to also try to reproduce the error in www.zooplus.com If you are able to reproduce it, please submit it with the .com domain but also report in which country domain you originally found it. This will greatly improve the time to payment, help H1 Triage and us to determine the duplicates in findings. Thanks a lot for your time and expertise! English · Amazon AWS Shield DDOS · Amazon AWS WAF · Amazon Web Services · Angular · apache · Apache Tomcat · Docker · Elastic Search · Java · JavaScript · Nginx · Oracle RDBMS · PostgresSQL · Python · React · Spring · Spring Boot · VMware	Domain	In scope	Critical	Eligible	Jun 11, 2024	6 (2%)

1-38 of 38

© HackerOne

Opportunities · Security · Leaderboard · Blog · Status · Docs · Support · Di

Zooplus

http://zooplus.de

Bug Bounty Program launched in Mar 2025

● Response efficiency: 84%

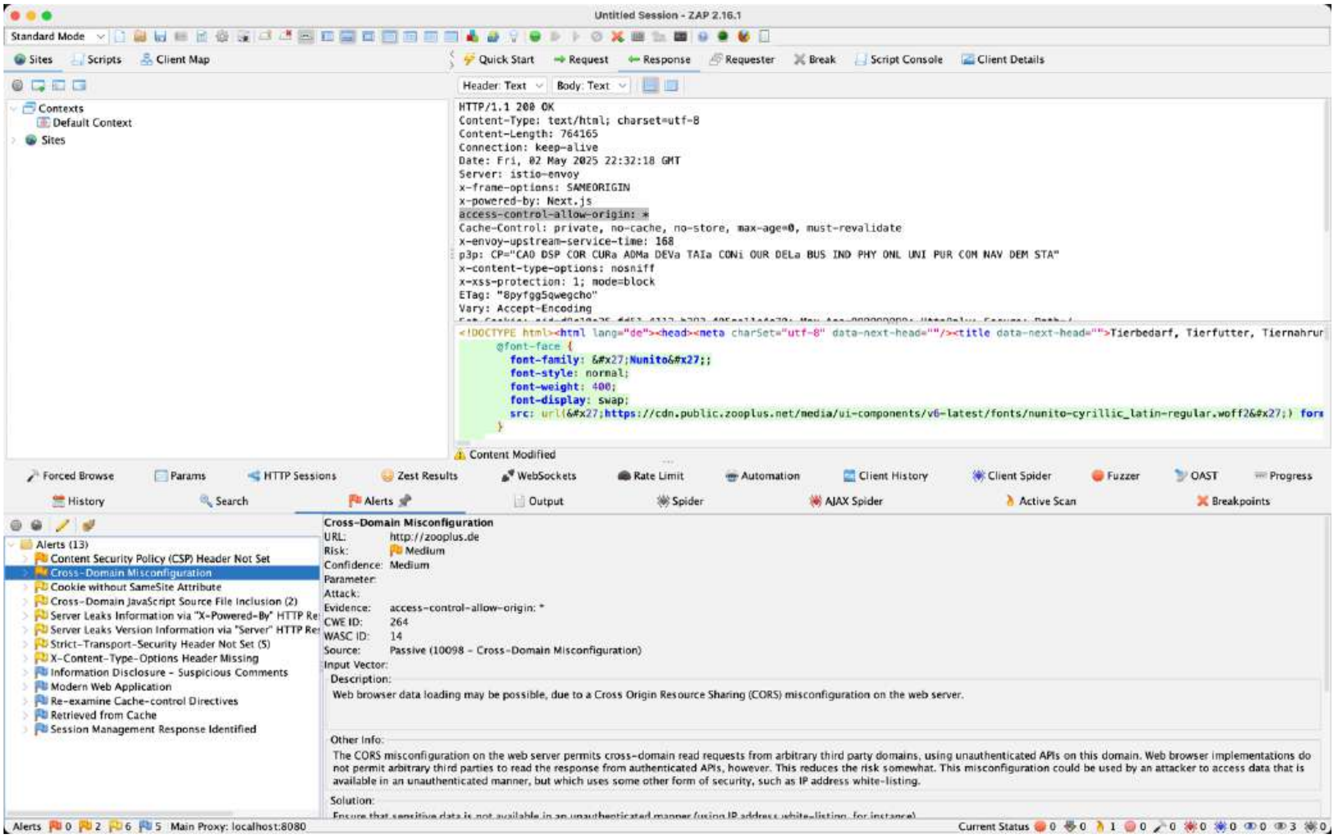
Submit report

Rewards

Severity	Rewards
Low Avg. bounty $500 18.73% submissions	$500
Medium Avg. bounty $1,000 39.70% submissions	$1,000
High Avg. bounty $2,000 28.84% submissions	$2,000
Critical Avg. bounty $5,000 12.73% submissions	$5,000

Stats

Scanned Vulnerabilities Using ZAP



```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 764165
Connection: keep-alive
Date: Fri, 02 May 2025 22:32:18 GMT
Server: istio-envoy
x-frame-options: SAMEORIGIN
x-powered-by: Next.js
access-control-allow-origin: *
Cache-Control: private, no-cache, no-store, max-age=0, must-revalidate
x-envoy-upstream-service-time: 168
p3p: CP="CAO DSP COR CURa ADMa DEVa TAIa CONi OUR DELa BUS IND PHY ONL UNI PUR COM NAV DEM STA"
x-content-type-options: nosniff
x-xss-protection: 1; mode=block
ETag: "8pyfgg5qwegcho"
Vary: Accept-Encoding
```

```
<!DOCTYPE html><html lang="de"><head><meta charSet="utf-8" data-next-head=""/><title data-next-head="">Tierbedarf, Tierfutter, Tiernahrur
      @font-face {
        font-family: &#x27;Nunito&#x27;;
        font-style: normal;
        font-weight: 400;
        font-display: swap;
        src: url(&#x27;https://cdn.public.zooplus.net/media/ui-components/v6-latest/fonts/nunito-cyrillic_latin-regular.woff2&#x27;) form
      }
```

Alerts (13)
- Content Security Policy (CSP) Header Not Set
- Cross-Domain Misconfiguration
- Cookie without SameSite Attribute
- Cross-Domain JavaScript Source File Inclusion (2)
- Server Leaks Information via "X-Powered-By" HTTP Re
- Server Leaks Version Information via "Server" HTTP Re
- Strict-Transport-Security Header Not Set (5)
- X-Content-Type-Options Header Missing
- Information Disclosure - Suspicious Comments
- Modern Web Application
- Re-examine Cache-control Directives
- Retrieved from Cache
- Session Management Response Identified

Cross-Domain Misconfiguration

URL: http://zooplus.de
Risk: Medium
Confidence: Medium
Parameter:
Attack:
Evidence: access-control-allow-origin: *
CWE ID: 264
WASC ID: 14
Source: Passive (10098 - Cross-Domain Misconfiguration)
Input Vector:

Description:

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

Other Info:

The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.

Solution:

Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).

Vulnerability Title Vulnerability Title

- Cross-Domain Misconfiguration (CORS)

Risk type

- Medium

Vulnerability Description

- The web server at zooplus.de contains a weak Cross-Origin Resource Sharing (CORS) configuration that allows third-party origins through its access-control-allow-origin: * header. The server misconfiguration allows web browsers to load cross-domain data from any third-party origin site which may disclose sensitive information to unauthorized external domains

Affected Components

- Web server at zooplus.de
- HTTP response headers, particularly CORS configuration

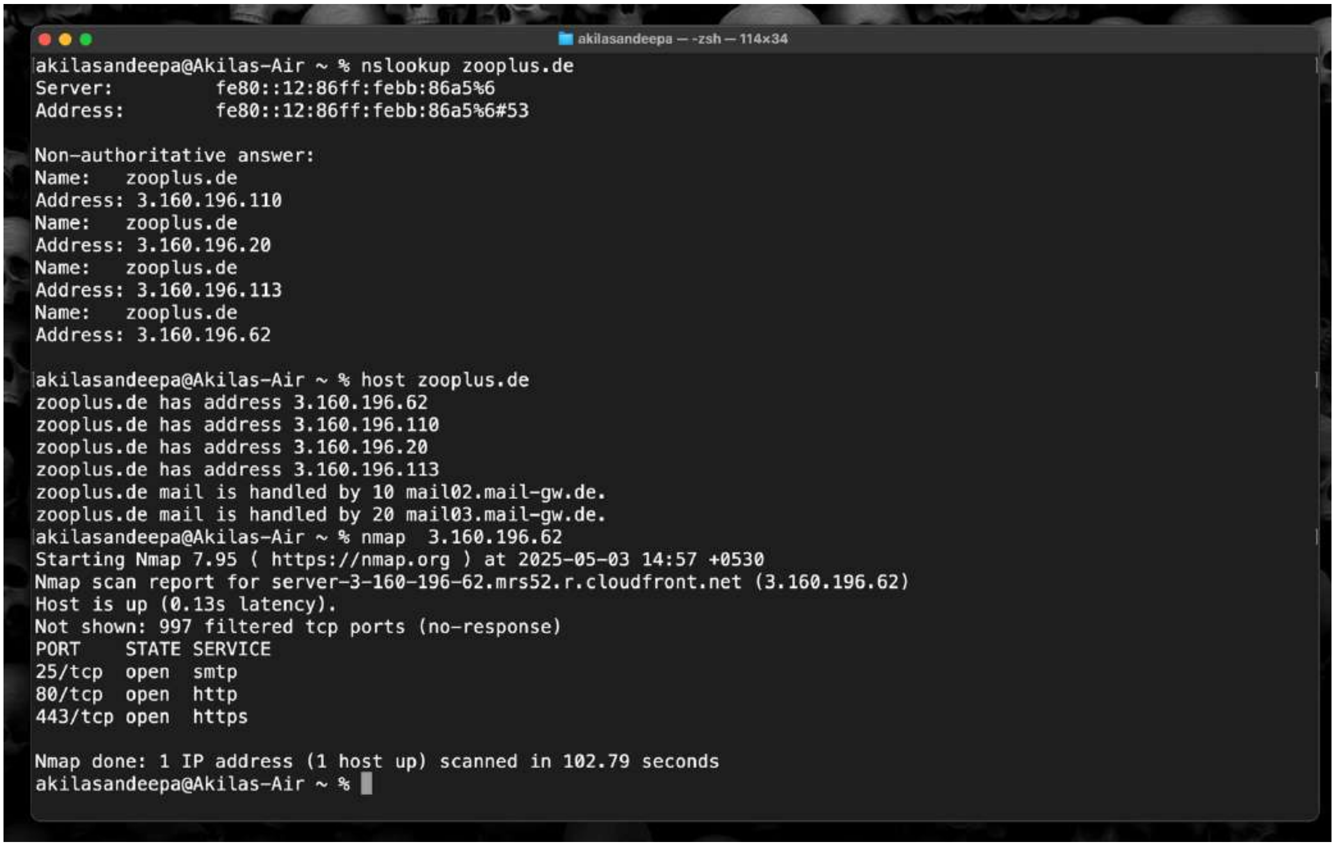
Impact Assessment

- Unauthorized third-party domains which make API requests plus access responses result in increased data exposure risks.
- A lack of proper security measures allows attackers to acquire protected data or carry out actions under user identities when this occurs.

Steps to Reproduce

- Through OWASP ZAP users can intercept HTTP responses which transmit from http://zooplus.de.
- Verify if the HTTP response headers stay visible while looking for access-control-allow-origin: * in the header section.

Proof of Concept



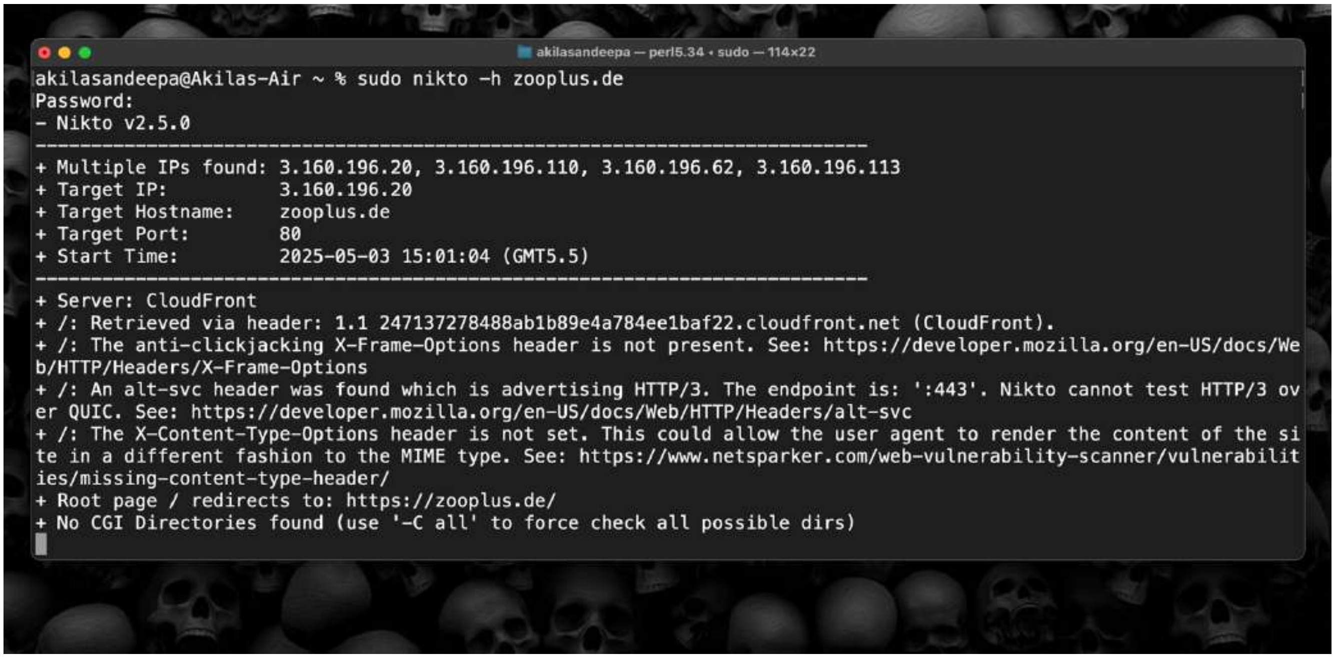
```
akilasandeepa@Akilas-Air ~ % nslookup zooplus.de
Server:         fe80::12:86ff:febb:86a5%6
Address:        fe80::12:86ff:febb:86a5%6#53

Non-authoritative answer:
Name:   zooplus.de
Address: 3.160.196.110
Name:   zooplus.de
Address: 3.160.196.20
Name:   zooplus.de
Address: 3.160.196.113
Name:   zooplus.de
Address: 3.160.196.62

akilasandeepa@Akilas-Air ~ % host zooplus.de
zooplus.de has address 3.160.196.62
zooplus.de has address 3.160.196.110
zooplus.de has address 3.160.196.20
zooplus.de has address 3.160.196.113
zooplus.de mail is handled by 10 mail02.mail-gw.de.
zooplus.de mail is handled by 20 mail03.mail-gw.de.
akilasandeepa@Akilas-Air ~ % nmap  3.160.196.62
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-03 14:57 +0530
Nmap scan report for server-3-160-196-62.mrs52.r.cloudfront.net (3.160.196.62)
Host is up (0.13s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 102.79 seconds
akilasandeepa@Akilas-Air ~ %
```

Proposed Mitigation or Fix

- The Access-Control-Allow-Origin header should contain restricted domains instead of using the wildcard format.
- Organizations must enforce CORS policies that limit permissions by origin sites as well as by HTTP methods and response headers.
- Regular tests and audits of CORS configurations must be performed to confirm the admission of proper cross-origin request permissions.

Scanned Vulnerabilities Using NIKTO

During the Nikto scan of zooplus.de multiple security vulnerabilities emerged because the website lacked essential X-Frame-Options protection and did not implement X-Content-Type-Options and had an alt-svc header revealing HTTP/3 although QUIC testing was unavailable while no CGI directories existed alongside root page redirection to HTTPS.



```
akilasandeepa@Akilas-Air ~ % sudo nikto -h zooplus.de
Password:
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 3.160.196.20, 3.160.196.110, 3.160.196.62, 3.160.196.113
+ Target IP:          3.160.196.20
+ Target Hostname:    zooplus.de
+ Target Port:        80
+ Start Time:         2025-05-03 15:01:04 (GMT5.5)
---------------------------------------------------------------------------
+ Server: CloudFront
+ /: Retrieved via header: 1.1 247137278488ab1b89e4a784ee1baf22.cloudfront.net (CloudFront).
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/We
b/HTTP/Headers/X-Frame-Options
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 ov
er QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the si
te in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilit
ies/missing-content-type-header/
+ Root page / redirects to: https://zooplus.de/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```