Sri Lanka Institute of Information Technology

BSc Honors in Information Technology

Specializing in Cyber Security

IE2062 - Web Security

Bug Bounty Assignment

Final Report

Student Register Number	Student Name
IT 22083678	SAHAN H.P.T

Tabel of Contents

Acknowledgement

In the huge globe of international trade, well-known companies constantly reinforce their digital walls with bug bounty programs, depending on ethical hacker's skills to find weaknesses in their online systems. These partnerships create a mutually beneficial relationships as white hat hackers find vulnerabilities and help companies strengthen their defenses and protect user data. To honor this collaboration, we must recognize and give reward to those whose hard work and expertise strengthen the overall security posture of the digital space.

The fact bug reward programs are so widely used is evidence that ethical hacking is becoming increasingly important for preserving cyber resilience. I'll provide ten reports covering topics such how I got started with bug bounty programs and how I researched web apps as a student, and we'll discuss the tools we can apply for bug bounties.

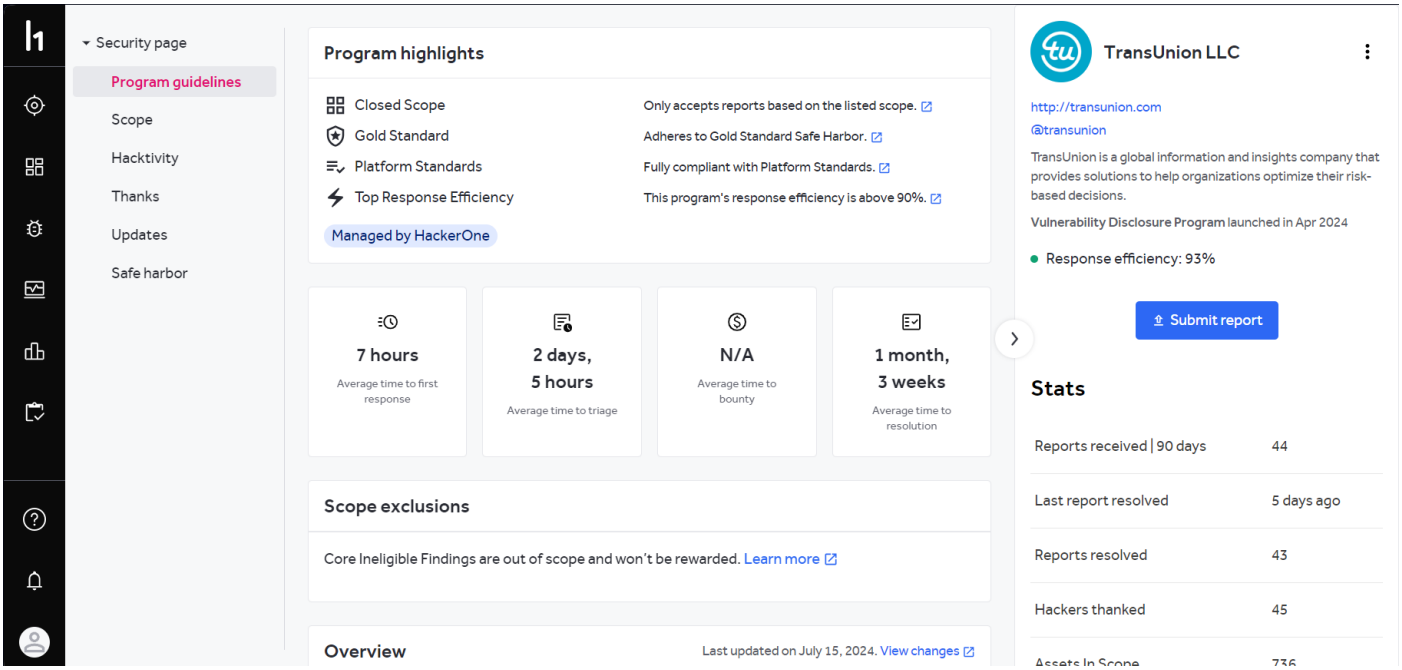
Introduction

The requirements of cybersecurity acts as sentinel guardians against the advancing tide of malicious exploits in the constantly growing world of digital interconnection, where the online and physical domains merge smoothly. Bug bounty programs become true fortresses of proactive defense in this ever-changing landscape, creating a mutually beneficial alliance between organizations and ethical hackers who share the same goal of digital resilience.Business establish bug bounties to offer monetary rewards to self-employed bug bounty hunters who uncover system flaws and security vulnerabilities. Business compensate bounty hunters for identifying security flaws before malevolent actors do when they report legitimate bugs . Bug bounty programs are sign of a major change in the cybersecurity landscape.

This change has been sparked by an awareness among businesses of all sizes, from industry titans to up-and-coming innovators, that the traditional security bastions are inadequate of navigating the dangerous waters of a constantly changing threats landscape. The days of enterprises being able to secure their digital estates only with walls and defenses that never changed are long gone. Conventional security paradigms are no loner relevant due to the explosive growth of sophisticated cyber threats, which are being driven by the devious schemes of actors acting with never-before-seen stealth and agility.

Fundamentally, a bug bounty program is a collaboration between organizations and ethical hackers in the common goal of strengthening the digital space against constantly changing threats. Admired as the brave guardians of the internet, ethical hackers respond to the call to duty by examining the complex subtleties of online apps in an effort to find difficult vulnerabilities. They do this nothing more than their creativity and moral determination.

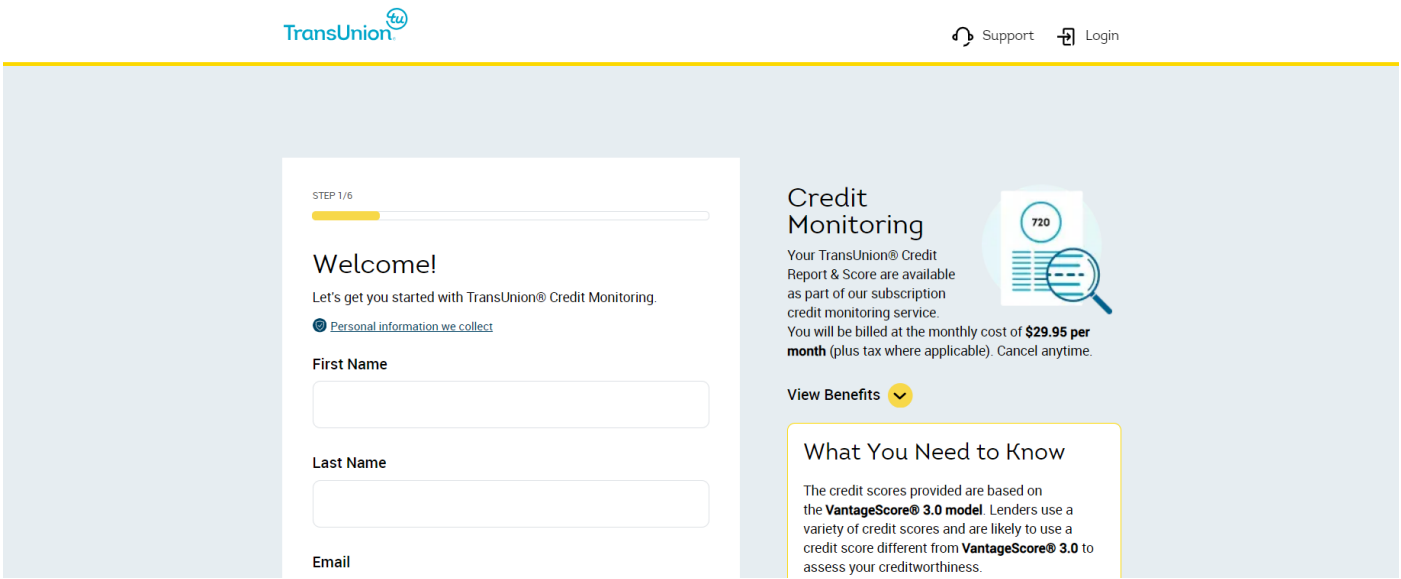
Report 01 Target Details



The target for this Bug Bounty report is TransUnion (https://www.transunion.com), a leading global provider of credit information and analytics services. The company offers various digital services, including credit reports, fraud detection, identity management, and personalized financial insights. The platform aims to make financial information more accessible and secure by leveraging technology to provide critical data services.

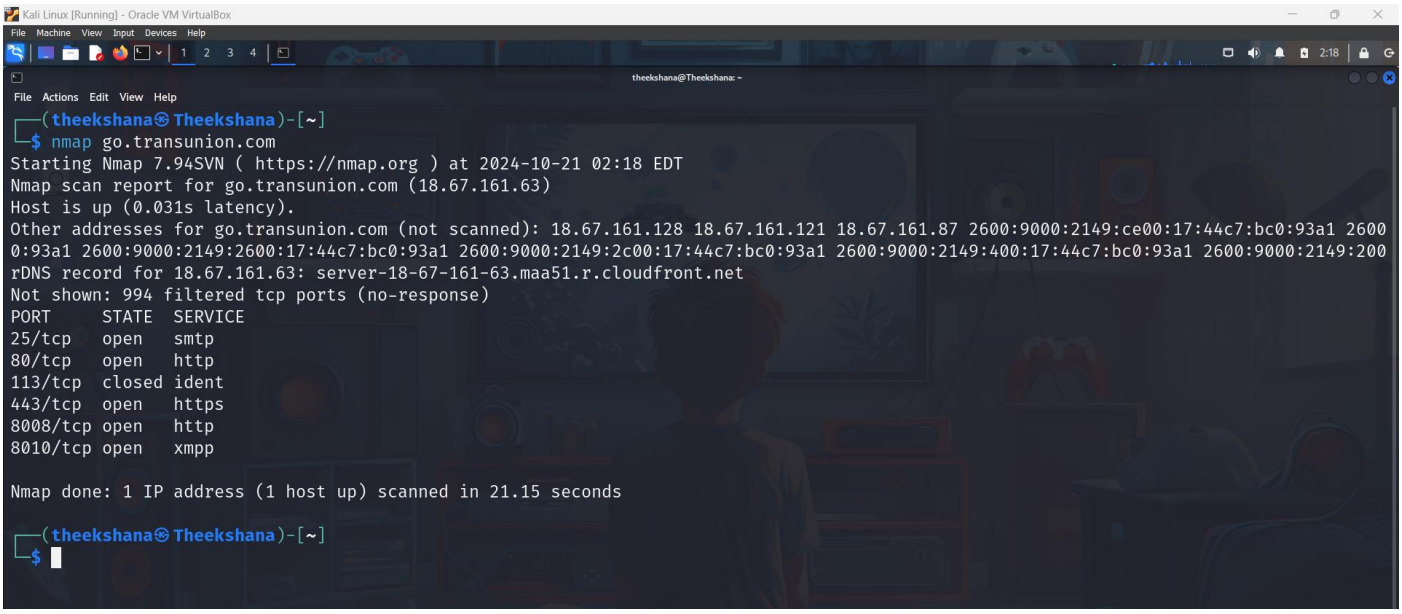
In this report, I have chosen to focus on 10 subdomains under the main domain transunion.com. Each subdomain may offer distinct functionalities or services, which can potentially introduce different security risks. The subdomains were selected based on their relevance and the likelihood of containing vulnerabilities, particularly in development or user-related functionalities.

This report covers the findings for the subdomain: go.transunion.com



Target Reconnaissance

Nmap Scan

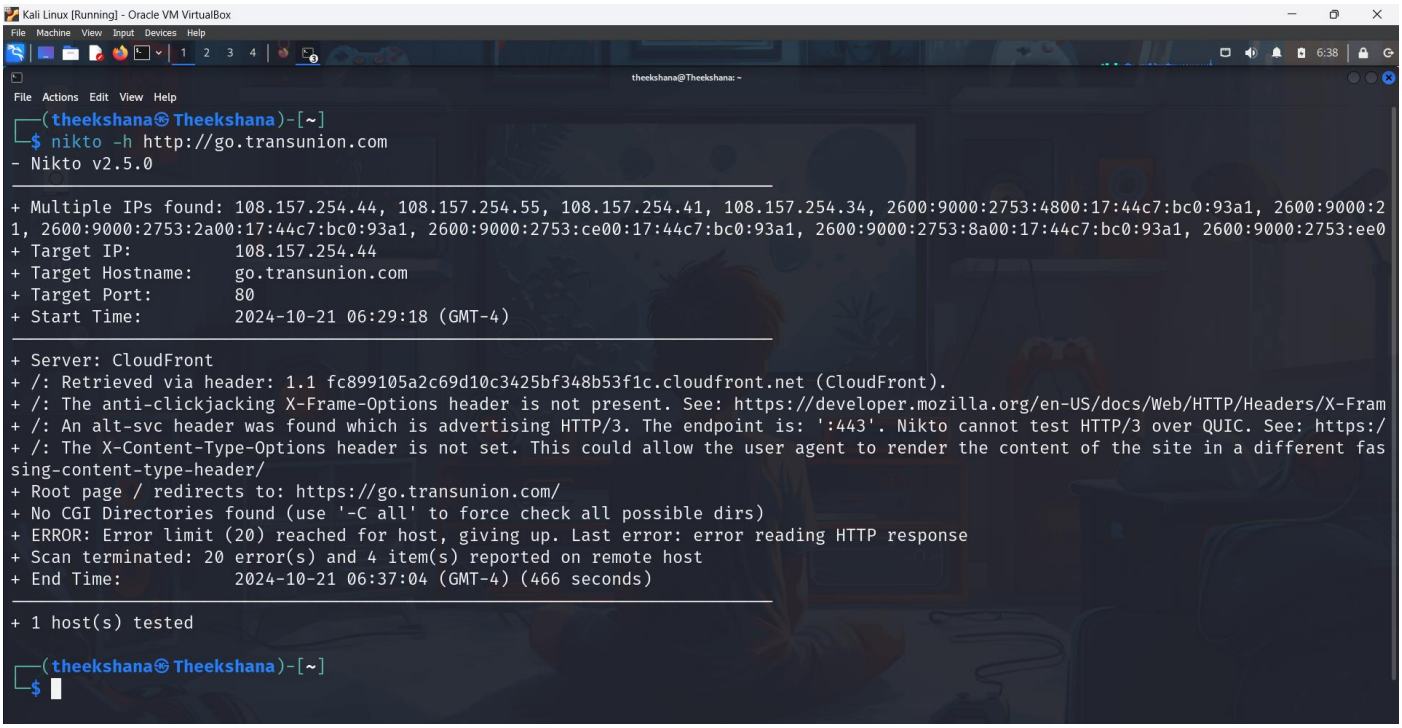


By scanning go.transunion.com with Nmap I found out these information.

Port	State	Service
25/tcp	Open	SMTP
80/tcp	Open	HTTP
443/tcp	Open	HTTPS
8080/tcp	Open	HTTP
8001/tcp	Open	XMPP

Port	Service	Potential Vulnerabilities
25/tcp	SMTP	Vulnerable to spam, open relay attacks, and email-based exploits (phishing, malware). Could be abused for email spoofing.
80/tcp	HTTP	Unencrypted traffic could be intercepted (MITM attacks). Vulnerabilities in web server software (Apache or Nginx) may be exploited.
443/tcp	HTTP	Possible SSL/TLS vulnerabilities (weak ciphers, outdated protocols) or certificate misconfigurations that could be exploited.
8080/tcp	HTTP	Alternative HTTP port often used for testing or secondary services, which may be less secure or outdated. Could be an attack vector.
8001/tcp	XMPP	Vulnerable to DoS attacks, unauthorized message interception, and account hijacking if not properly secured.

Nikto Scan



The screenshot shows the output of a Nikto scan against the target go.transunion.com, which reveals several potential security issues and misconfigurations.

1. X-Frame-Options Header Missing:

- The X-Frame-Options header is not present. This header is important for preventing clickjacking attacks, where a malicious website can trick users into clicking something different from what they perceive.
- Vulnerability: Without this header, the site is vulnerable to clickjacking, where an attacker could embed the site within an iframe on a malicious site and trick users into interacting with the hidden site.
- Mitigation: Implement the X-Frame-Options header with a value of "DENY" or "SAMEORIGIN" to prevent framing from untrusted sites.

2. Missing X-Content-Type-Options Header:

- The X-Content-Type-Options header is not set. This header is used to prevent browsers from interpreting files as a different MIME type than what is specified by the server.
- Vulnerability: Without this header, the site could be vulnerable to MIME-sniffing attacks, where an attacker might manipulate how content is rendered, potentially leading to cross-site scripting (XSS) or other attacks.
- Mitigation: Implement the X-Content-Type-Options header with the value "nosniff" to ensure browsers honor the declared MIME types.

3. HTTP/3 Alt-Svc Header Found:

- An "alt-svc" header was found advertising support for HTTP/3. While this isn't inherently a vulnerability, it is noted that Nikto cannot test HTTP/3 over QUIC, which could leave certain aspects of the server's configuration untested.

- Vulnerability: Potential misconfigurations in HTTP/3 settings or weaknesses in older implementations of QUIC could introduce risks. However, there are no direct issues flagged in this scan.

- Mitigation: Ensure that your HTTP/3 configuration is secure, and test it separately for security vulnerabilities if not covered by Nikto.

4. Root Page Redirects to HTTPS:

- The root page ("/") redirects to `https://go.transunion.com/`, which is a good practice as it ensures that users are directed to the secure HTTPS version of the site.

- Mitigation: No direct issue here. However, you should ensure that the HTTPS configuration is strong and up-to-date (e.g., supporting only secure protocols like TLS 1.2 or 1.3).

5. No CGI Directories Found:

- Nikto did not find any CGI directories. CGI (Common Gateway Interface) scripts can often be vulnerable to a wide range of attacks, so this is a positive finding.

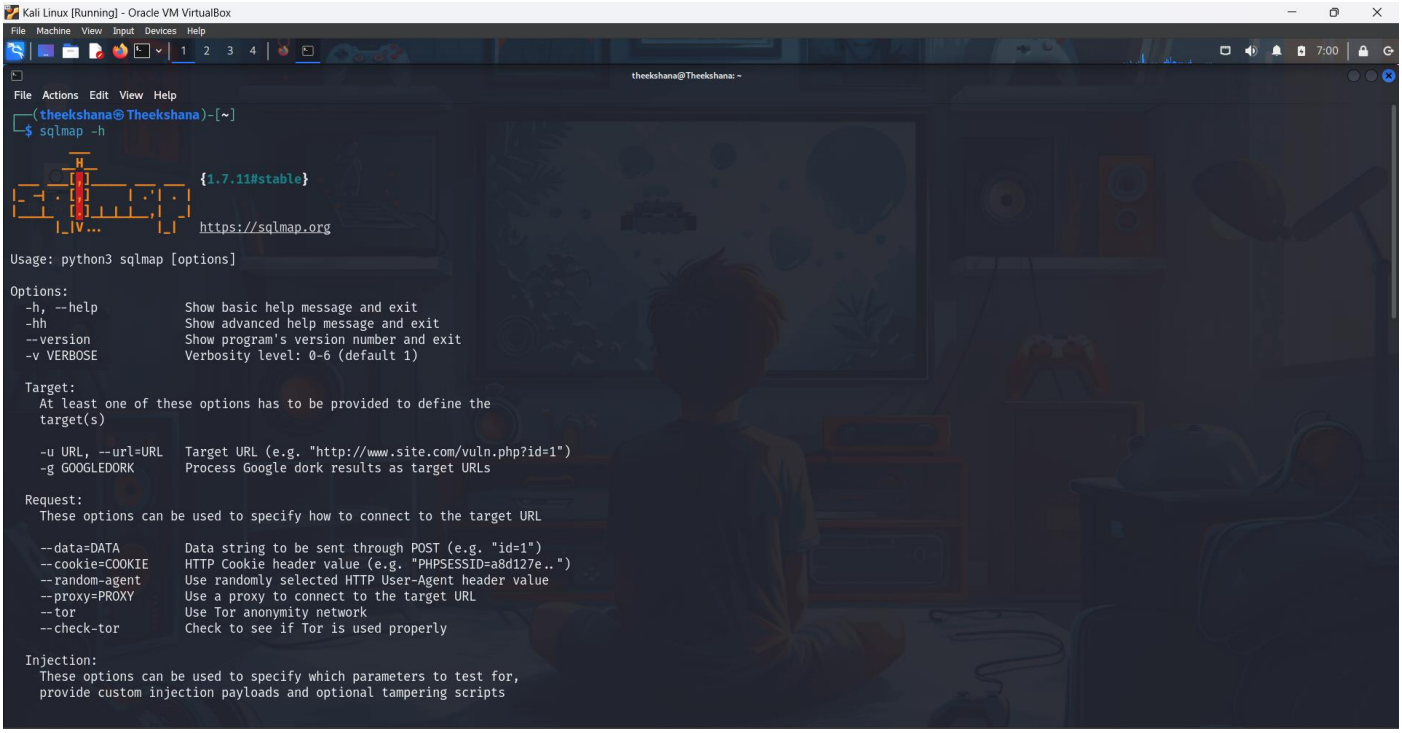
- Mitigation: Ensure any dynamic scripts or services running on the server are secured and regularly updated to avoid vulnerabilities.

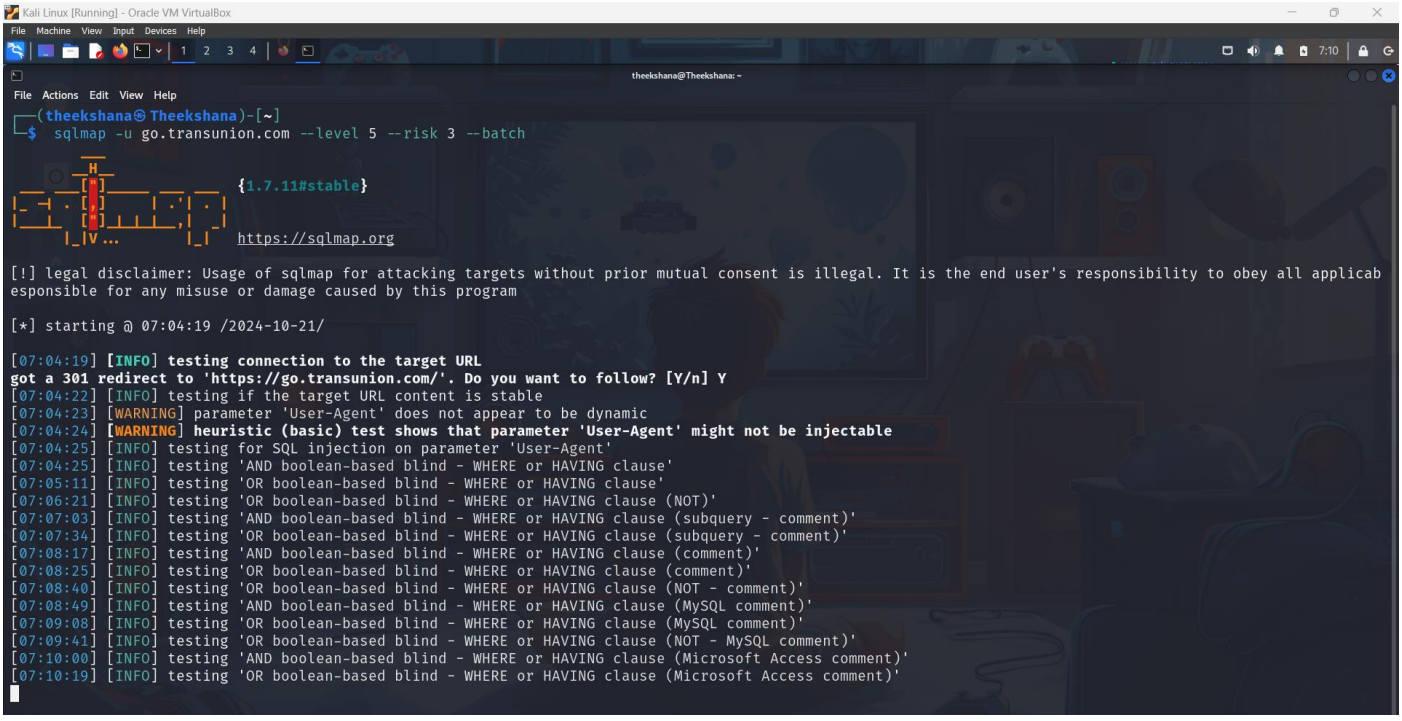
6. Error: Error Limit Reached:

- The scan encountered multiple errors (20 in total) while attempting to interact with the host, leading to an error limit being reached. The specific errors aren’t detailed here, but they may indicate that the server was blocking some of the scan's requests or that there were network-related issues.

- Vulnerability: Errors during scanning could obscure potential vulnerabilities. Ensure that security mechanisms like firewalls or rate-limiting are not overly restrictive to prevent missing vulnerabilities in security tests.
- Mitigation: Conduct further manual or tool-based testing to ensure no critical issues were missed due to the errors.

SQLmap Scaner

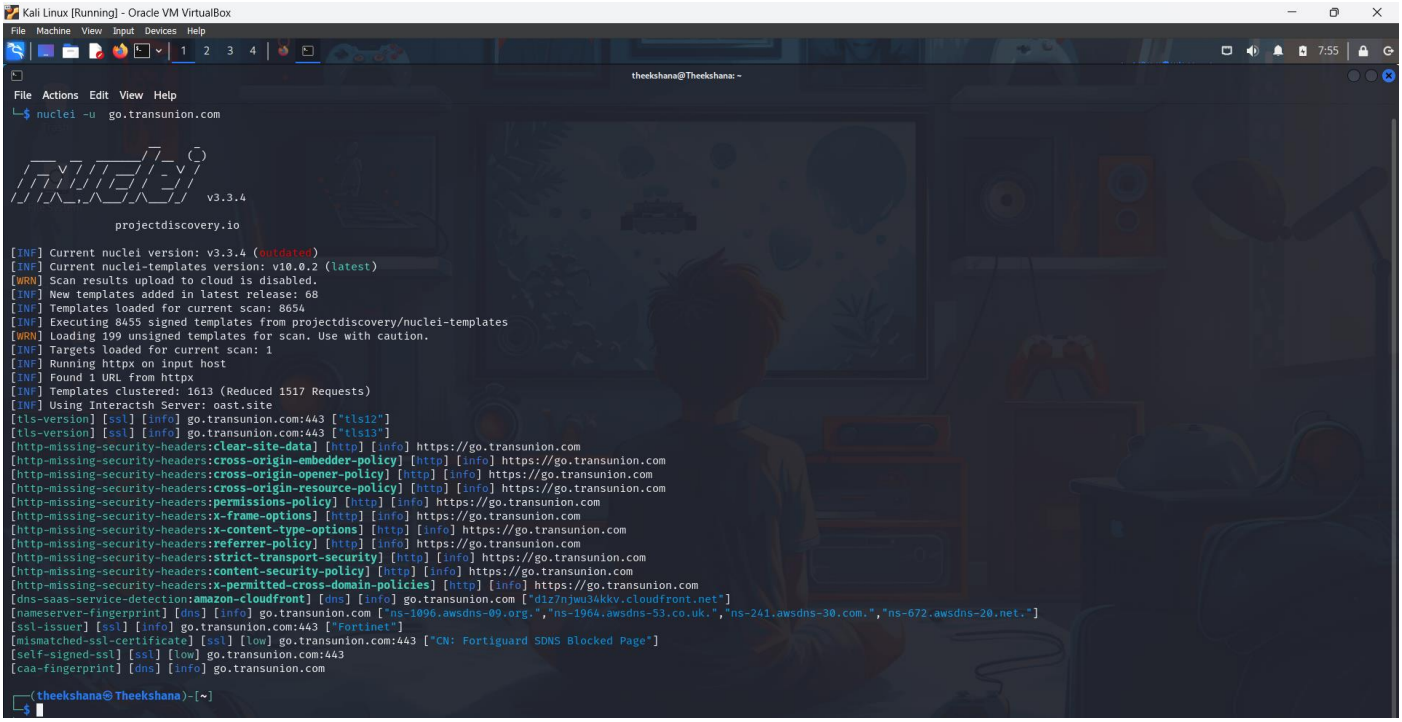




Vulnerabilities Detected:

- Potential SQL Injection Risk in User-Agent Parameter
- 301 Redirect (Not a vulnerability but a redirection)
- Boolean-Based Blind SQL Injection:
  This technique is used to determine if the web application is vulnerable to SQL injection by observing changes in the application's behavior based on true or false SQL conditions. The fact that SQLmap is performing this indicates potential vulnerabilities, but in this specific case, the User-Agent parameter did not immediately show a clear vulnerability during the automated test.

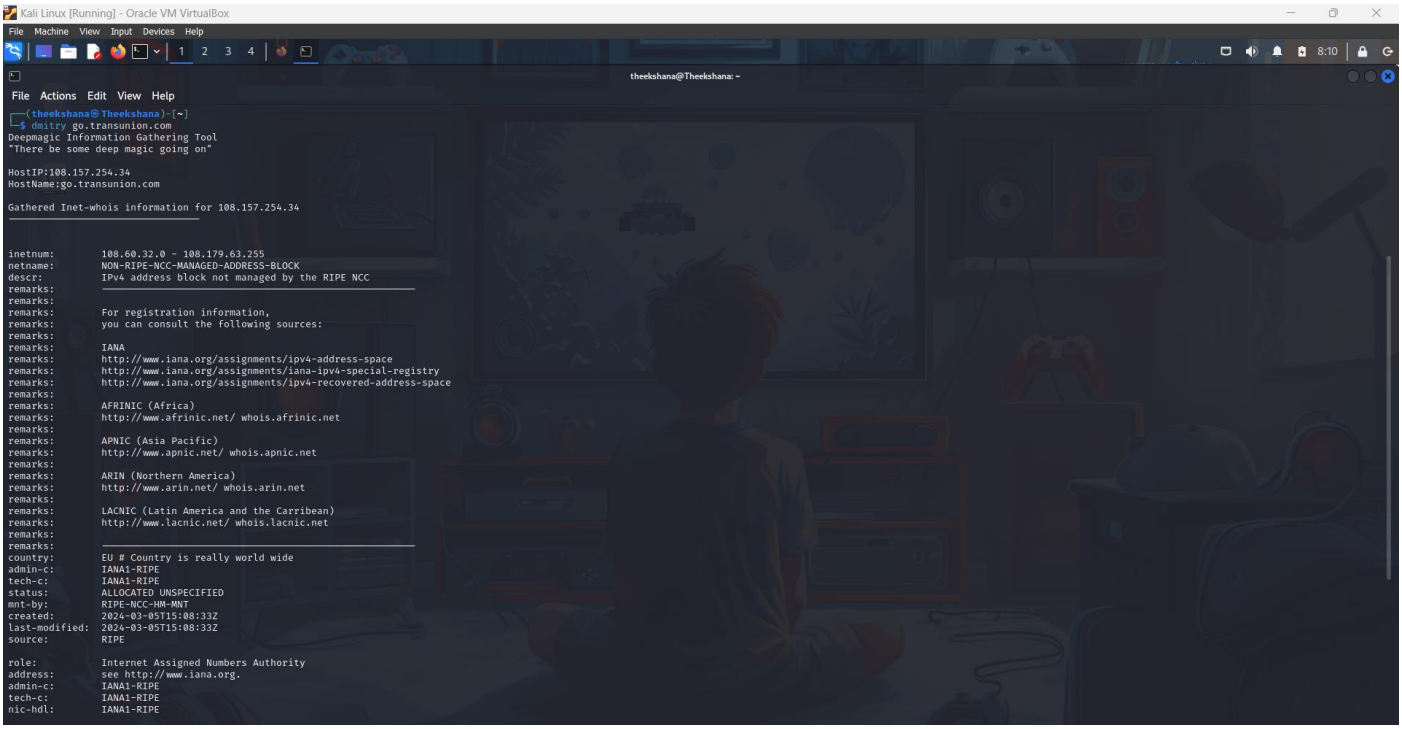
Nuclei Scan

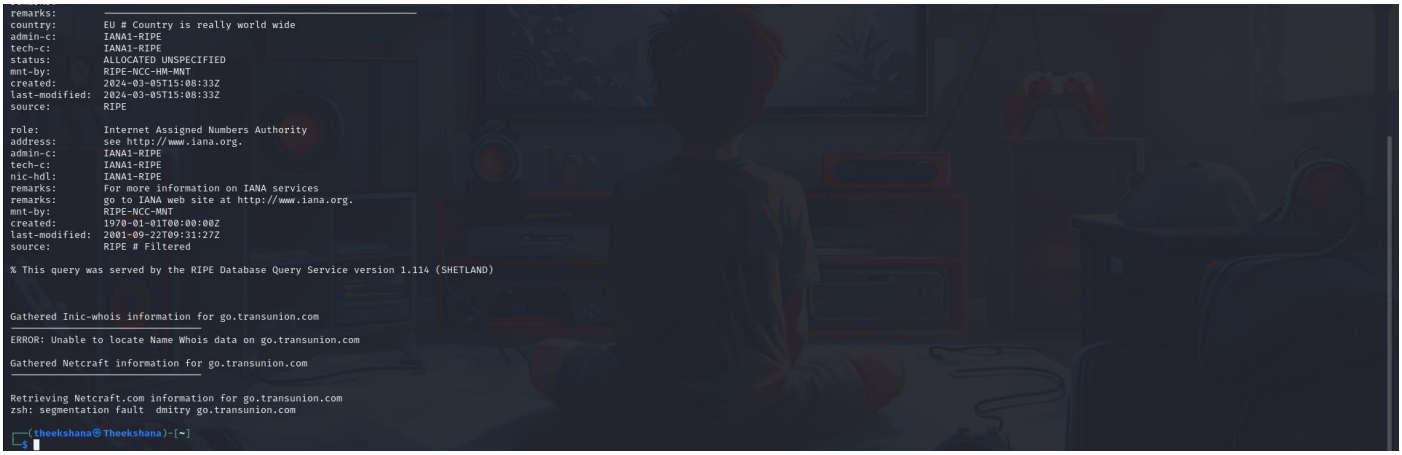


Important Findings:

Vulnerability Type	Description	Risk
Mismatched SSL Certificate	The SSL certificate's domain does not match the actual domain, indicating a configuration issue.	Man-in-the-middle attacks
Self-signed SSL Certificate	The certificate is not signed by a trusted Certificate Authority (CA), which makes the connection less secure.	Reduced trustworthiness
Missing clear-site-data Header	This header is missing, which helps ensure that user data is properly cleared when logging out or switching sessions.	Privacy risk
Missing cross-origin-embedder-policy	Lack of this header may leave the site vulnerable to cross-origin resource sharing attacks.	Cross-site scripting (XSS)
Missing cross-origin-opener-policy	Without this, the site could be exposed to cross-origin data leaks or attacks like cross-window communication hijacking.	Data leakage, security risk
Missing cross-origin-resource-policy	This prevents unauthorized sites from embedding the site's resources, reducing potential for XSS attacks.	Data exposure
Missing permissions-policy Header	Controls browser features like camera, microphone, etc., limiting potential attack surface.	Reduced security control
Missing x-frame-options Header	Prevents clickjacking by stopping the site from being embedded in frames on other sites.	Clickjacking attacks
Missing x-content-type-options Header	Prevents MIME-type mismatch attacks where files could be executed as different file types than intended.	MIME-type attacks

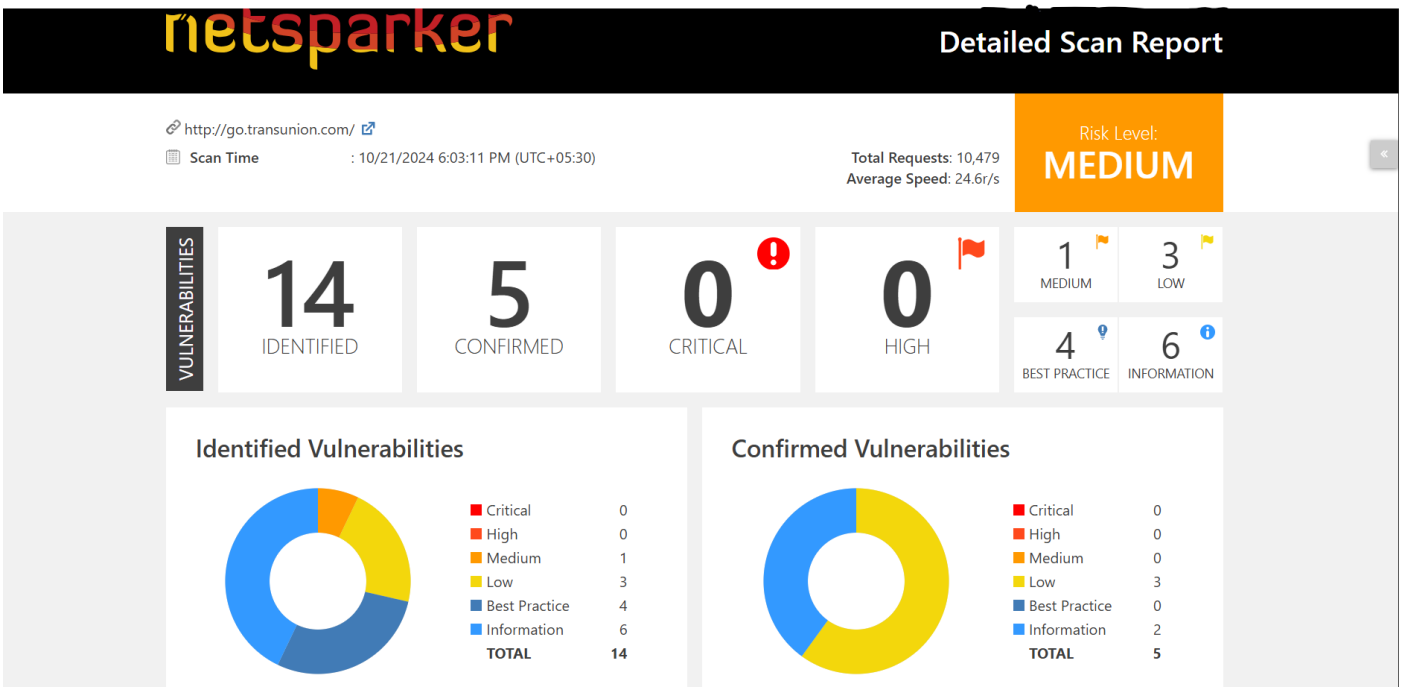
Dmitry Scan





Field	Details
Host IP	108.157.254.34
Host Name	go.transunion.com
Inetnum	108.60.32.0 - 108.179.63.255
Netname	NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
Description	IPv4 address block not managed by the RIPE NCC
Country	EU (European Union, globally worldwide)
Admin-C / Tech-C	IANA1-RIPE
Status	ALLOCATED UNSPECIFIED
Created	2024-03-05T15:08:33Z
Source	RIPE
Remarks	IPv4 block registration information can be found at AFRINIC (Africa), APNIC (Asia Pacific), ARIN (Northern America), LACNIC (Latin America and the Caribbean)

Netsparker



Vulnerability Summary

SEVERITY FILTER : CRITICAL HIGH MEDIUM LOW BEST PRACTICE INFORMATION

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://go.transunion.com/	
	Cookie Not Marked as HttpOnly	GET	https://go.transunion.com/	
	Cookie Not Marked as Secure	GET	https://go.transunion.com/	
	Insecure Frame (External)	GET	https://go.transunion.com/	
	Expect-CT Not Enabled	GET	https://go.transunion.com/.well-known/	
	Missing X-XSS-Protection Header	GET	https://go.transunion.com/_next/static/chunks/main-app-73c201cc0b2119e4.js	
	SameSite Cookie Not Implemented	GET	https://go.transunion.com/	
	Subresource Integrity (SRI) Not Implemented	GET	https://go.transunion.com/.svn/wc.db	
	[Possible] Internal Path Disclosure (*nix)	GET	https://go.transunion.com/etc/static/	
	[Possible] Internal Path Disclosure (Windows)	GET	https://go.transunion.com/c:/static/	
	An Unsafe Content Security Policy (CSP) Directive in Use	GET	https://go.transunion.com/	

HTTP Strict Transport Security (HSTS) Policy Not Enabled

MEDIUM 1

Netsparker identified that HTTP Strict Transport Security (HSTS) policy is not enabled.

The target website is being served from not only HTTPS but also HTTP and it lacks of HSTS policy implementation.

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period of time during which the user agent shall access the server in only secure fashion.

When a web application issues HSTS Policy to user agents, conformant user agents behave as follows:

- Automatically turn any insecure (HTTP) links referencing the web application into secure (HTTPS) links. (For instance, http://example.com/some/page/ will be modified to https://example.com/some/page/ before accessing the server.)
- If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), user agents show an error message and do not allow the user to access the web application.

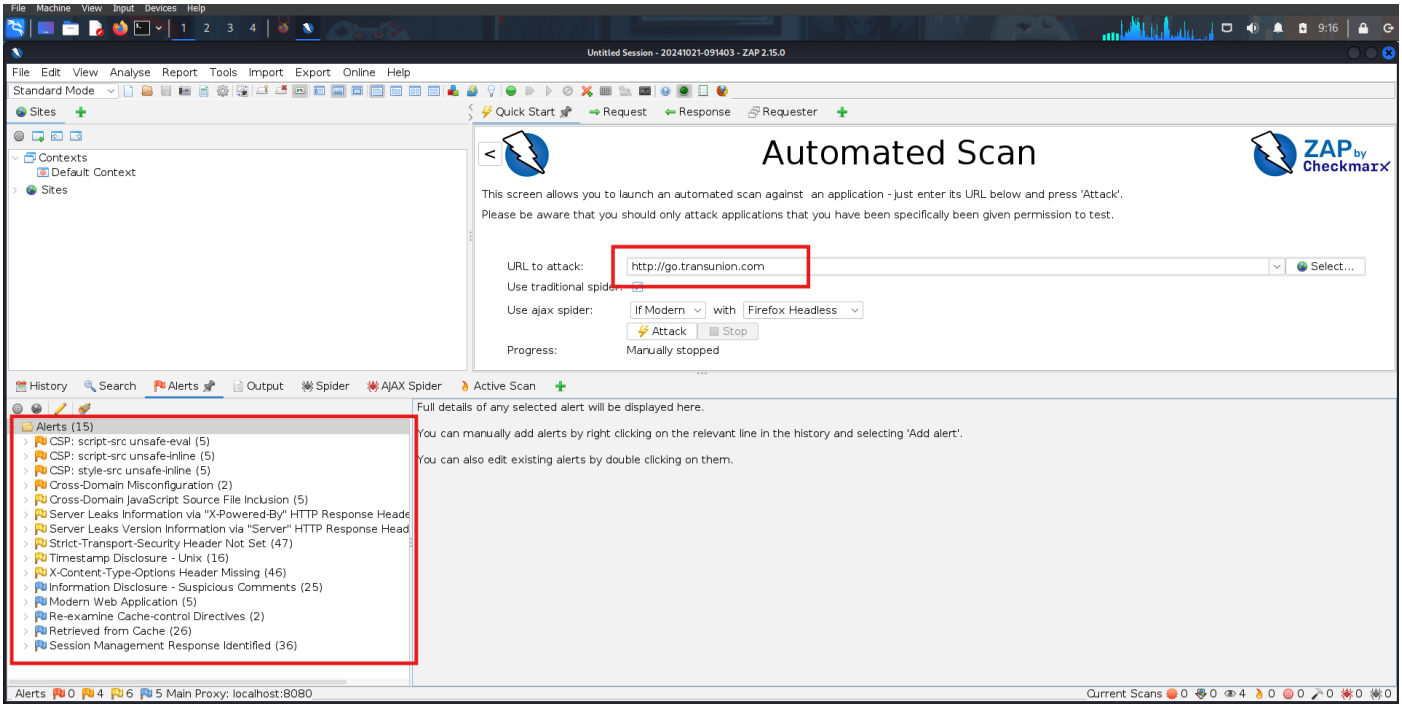
Vulnerabilities

1.1. https://go.transunion.com/

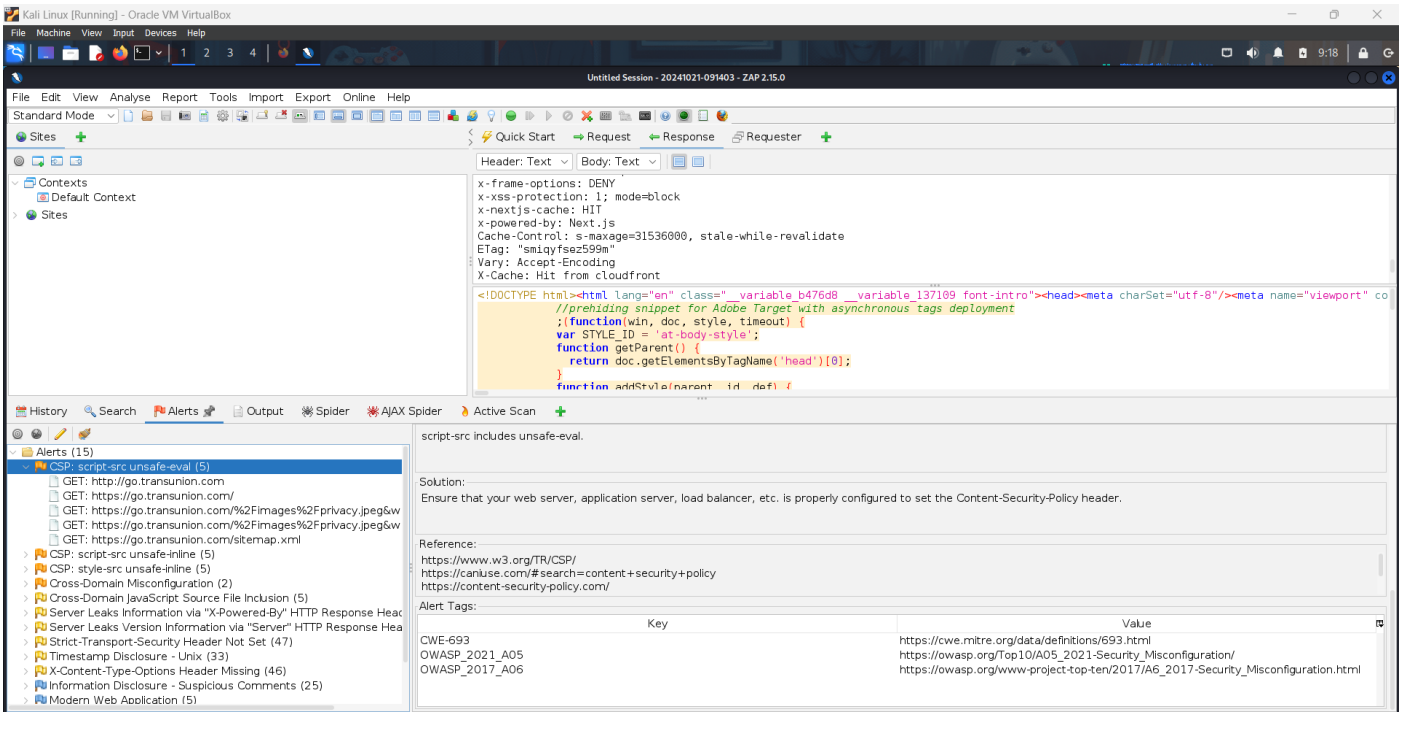
Certainty

Request Response

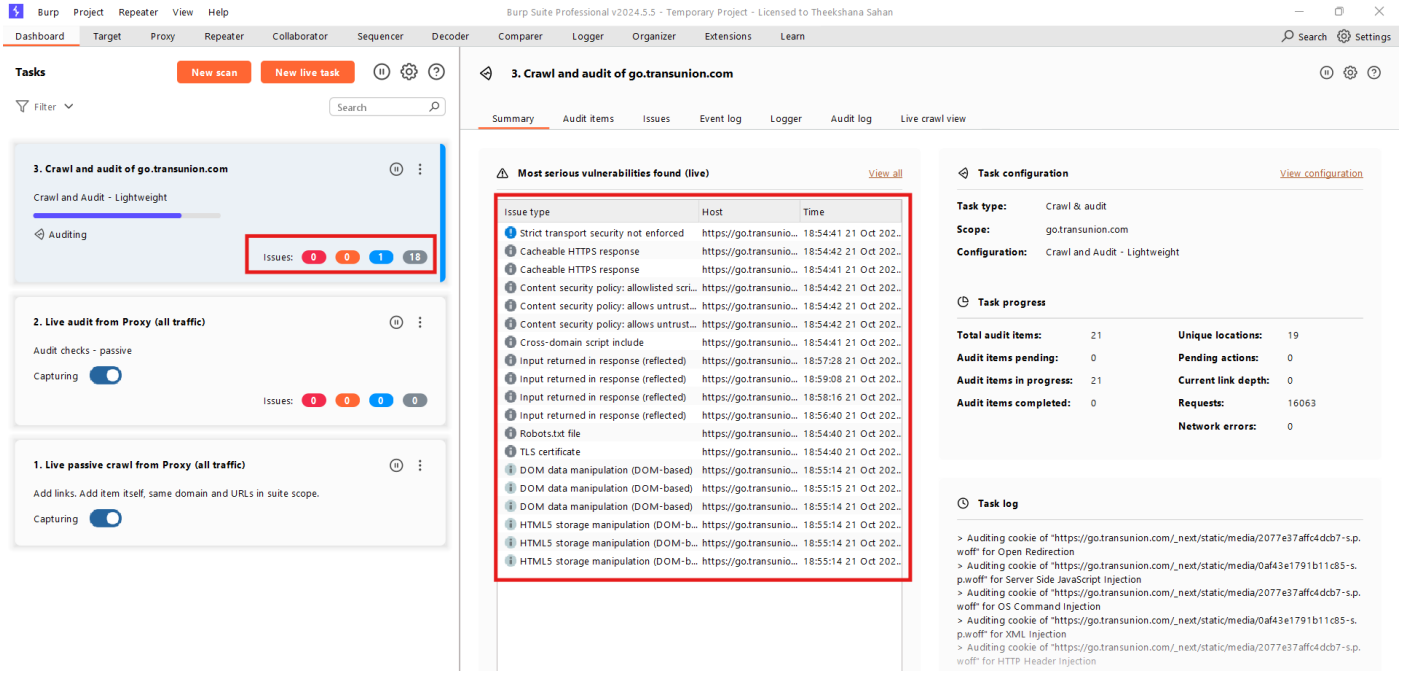
OWASP ZAP

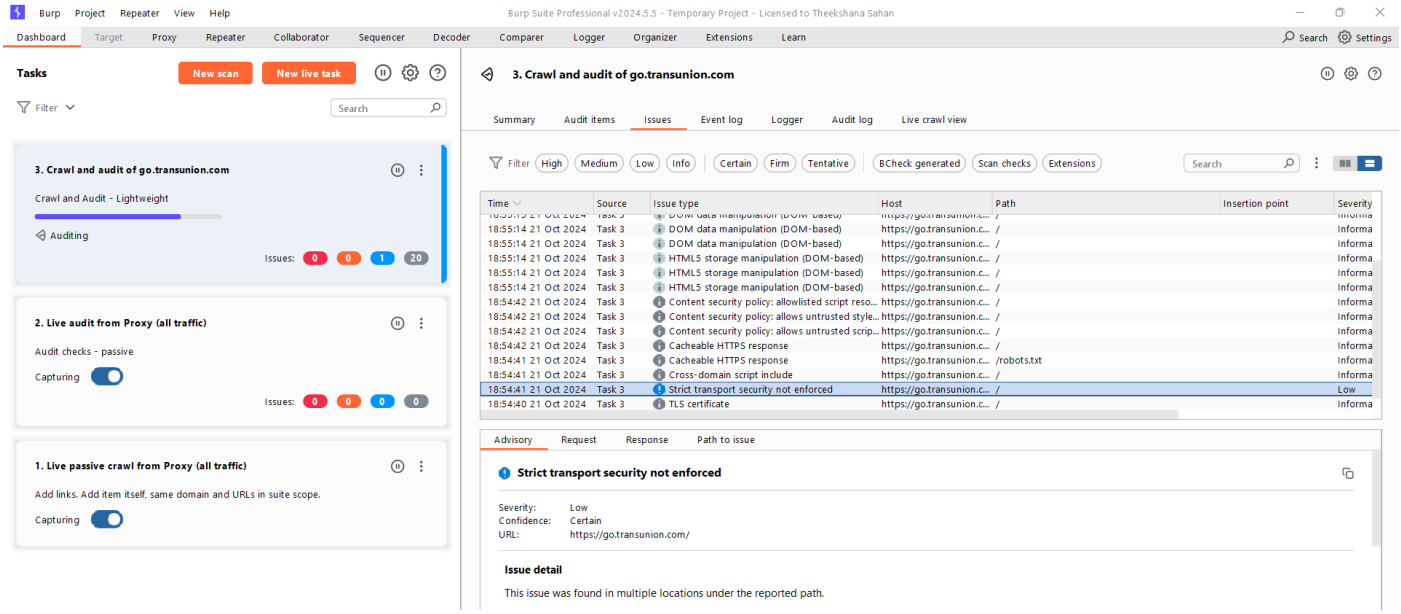

Untitled Session - 20241021-091403 - ZAP 2.15.0
Automated Scan
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack: http://go.transunion.com
Use traditional spider:
Use ajax spider: If Modern with Firefox Headless
Attack
Stop
Progress: Manually stopped
Alerts (15)
CSP: script-src unsafe-eval (5)
CSP: script-src unsafe-inline (5)
CSP: style-src unsafe-inline (5)
Cross-Domain Misconfiguration (2)
Cross-Domain JavaScript Source File Inclusion (5)
Server Leaks Information via "X-Powered-By" HTTP Response Header
Server Leaks Version Information via "Server" HTTP Response Header
Strict-Transport-Security Header Not Set (47)
Timestamp Disclosure - Unix (16)
X-Content-Type-Options Header Missing (46)
Information Disclosure - Suspicious Comments (25)
Modern Web Application (5)
Re-examine Cache-control Directives (2)
Retrieved from Cache (26)
Session Management Response Identified (36)
Full details of any selected alert will be displayed here.
You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.
You can also edit existing alerts by double clicking on them.

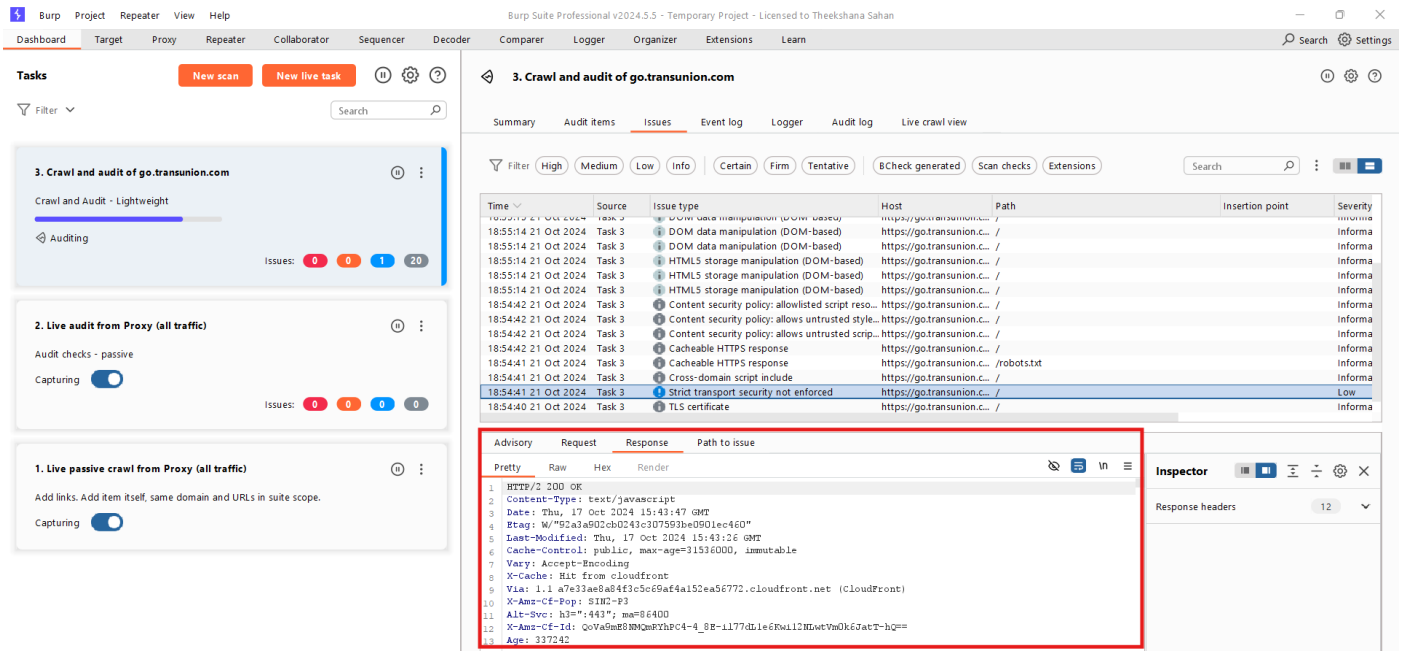

CSP: script-src unsafe-eval
URL: http://go.transunion.com
Risk: Medium
Confidence: High
Parameter: content-security-policy
Attack:
Evidence: :m.com dpm.demdex.net api.company-target.com t.teads.tv transunion.tt.omtrdc.net googleads.g.doubleclick.net ; block-all-mixed-content; upgrade-insecure-requests;
CWE ID: 693
WASC ID: 15
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, ActiveX, audio and video files.
Other Info:
script-src includes unsafe-eval.
Solution:
Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference:
https://www.w3.org/TR/CSP/
https://caniuse.com/#search=content+security+policy
Cancel
Save


Kali Linux [Running] - Oracle VM VirtualBox
Untitled Session - 20241021-091403 - ZAP 2.15.0
x-frame-options: DENY
x-xss-protection: 1; mode=block
x-nextjs-cache: HIT
x-powered-by: Next.js
Cache-Control: s-maxage=31536000, stale-while-revalidate
ETag: "smiqyfsez599m"
Vary: Accept-Encoding
X-Cache: Hit from cloudfront
script-src includes unsafe-eval.
Solution:
Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference:
https://www.w3.org/TR/CSP/
https://caniuse.com/#search=content+security+policy
https://content-security-policy.com/
Alert Tags:
Key
Value
CWE-693
https://cwe.mitre.org/data/definitions/693.html
OWASP_2021_A05
https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
OWASP_2017_A06
https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html

Burp Suite


Burp Project Repeater View Help
Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan
Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Tasks
New scan
New live task
3. Crawl and audit of go.transunion.com
Crawl and Audit - Lightweight
Auditing
Issues: 0 0 1 18
2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing
Issues: 0 0 0 0
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing
3. Crawl and audit of go.transunion.com
Summary Audit items Issues Event log Logger Audit log Live crawl view
Most serious vulnerabilities found (live)
View all
Issue type Host Time
Strict transport security not enforced https://go.transunio... 18:54:41 21 Oct 202...
Cacheable HTTPS response https://go.transunio... 18:54:42 21 Oct 202...
Cacheable HTTPS response https://go.transunio... 18:54:41 21 Oct 202...
Content security policy: allowlisted scri... https://go.transunio... 18:54:42 21 Oct 202...
Content security policy: allows untrust... https://go.transunio... 18:54:42 21 Oct 202...
Content security policy: allows untrust... https://go.transunio... 18:54:42 21 Oct 202...
Cross-domain script include https://go.transunio... 18:54:41 21 Oct 202...
Input returned in response (reflected) https://go.transunio... 18:57:28 21 Oct 202...
Input returned in response (reflected) https://go.transunio... 18:59:08 21 Oct 202...
Input returned in response (reflected) https://go.transunio... 18:58:16 21 Oct 202...
Input returned in response (reflected) https://go.transunio... 18:56:40 21 Oct 202...
Robots.txt file https://go.transunio... 18:54:40 21 Oct 202...
TLS certificate https://go.transunio... 18:54:40 21 Oct 202...
DOM data manipulation (DOM-based) https://go.transunio... 18:55:14 21 Oct 202...
DOM data manipulation (DOM-based) https://go.transunio... 18:55:15 21 Oct 202...
DOM data manipulation (DOM-based) https://go.transunio... 18:55:14 21 Oct 202...
HTML5 storage manipulation (DOM-b... https://go.transunio... 18:55:14 21 Oct 202...
HTML5 storage manipulation (DOM-b... https://go.transunio... 18:55:14 21 Oct 202...
HTML5 storage manipulation (DOM-b... https://go.transunio... 18:55:14 21 Oct 202...
Task configuration
View configuration
Task type: Crawl & audit
Scope: go.transunion.com
Configuration: Crawl and Audit - Lightweight
Task progress
Total audit items: 21
Audit items pending: 0
Audit items in progress: 21
Audit items completed: 0
Unique locations: 19
Pending actions: 0
Current link depth: 0
Requests: 16063
Network errors: 0
Task log
> Auditing cookie of "https://go.transunion.com/_next/static/media/2077e37affc4dcb7-s.p.woff" for Open Redirection
> Auditing cookie of "https://go.transunion.com/_next/static/media/0af43e1791b11c85-s.p.woff" for Server Side JavaScript Injection
> Auditing cookie of "https://go.transunion.com/_next/static/media/2077e37affc4dcb7-s.p.woff" for OS Command Injection
> Auditing cookie of "https://go.transunion.com/_next/static/media/0af43e1791b11c85-s.p.woff" for XML Injection
> Auditing cookie of "https://go.transunion.com/_next/static/media/2077e37affc4dcb7-s.p.woff" for HTTP Header Injection


Burp Project Repeater View Help
Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan
Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Tasks
New scan
New live task
3. Crawl and audit of go.transunion.com
Crawl and Audit - Lightweight
Auditing
Issues: 0 0 1 20
2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing
Issues: 0 0 0 0
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing
3. Crawl and audit of go.transunion.com
Summary Audit items Issues Event log Logger Audit log Live crawl view
Filter High Medium Low Info Certain Firm Tentative BCheck generated Scan checks Extensions
Search
Time Source Issue type Host Path Insertion point Severity
18:55:14 21 Oct 2024 Task 3 DOM data manipulation (DOM-based) https://go.transunion.c... / Informa
18:55:14 21 Oct 2024 Task 3 DOM data manipulation (DOM-based) https://go.transunion.c... / Informa
18:55:14 21 Oct 2024 Task 3 HTML5 storage manipulation (DOM-based) https://go.transunion.c... / Informa
18:55:14 21 Oct 2024 Task 3 HTML5 storage manipulation (DOM-based) https://go.transunion.c... / Informa
18:55:14 21 Oct 2024 Task 3 HTML5 storage manipulation (DOM-based) https://go.transunion.c... / Informa
18:54:42 21 Oct 2024 Task 3 Content security policy: allowlisted script reso... https://go.transunion.c... / Informa
18:54:42 21 Oct 2024 Task 3 Content security policy: allows untrusted style... https://go.transunion.c... / Informa
18:54:42 21 Oct 2024 Task 3 Content security policy: allows untrusted scrip... https://go.transunion.c... / Informa
18:54:42 21 Oct 2024 Task 3 Cacheable HTTPS response https://go.transunion.c... / Informa
18:54:41 21 Oct 2024 Task 3 Cacheable HTTPS response https://go.transunion.c... /robots.txt Informa
18:54:41 21 Oct 2024 Task 3 Cross-domain script include https://go.transunion.c... / Informa
18:54:41 21 Oct 2024 Task 3 Strict transport security not enforced https://go.transunion.c... / Low
18:54:40 21 Oct 2024 Task 3 TLS certificate https://go.transunion.c... / Informa
Advisory Request Response Path to issue
Strict transport security not enforced
Severity: Low
Confidence: Certain
URL: https://go.transunion.com/
Issue detail
This issue was found in multiple locations under the reported path.


Burp Project Repeater View Help
Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan
Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Tasks
New scan
New live task
3. Crawl and audit of go.transunion.com
Crawl and Audit - Lightweight
Auditing
Issues: 0 0 1 20
2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing
Issues: 0 0 0 0
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing
3. Crawl and audit of go.transunion.com
Summary Audit items Issues Event log Logger Audit log Live crawl view
Filter High Medium Low Info Certain Firm Tentative BCheck generated Scan checks Extensions
Search
Time Source Issue type Host Path Insertion point Severity
18:55:14 21 Oct 2024 Task 3 DOM data manipulation (DOM-based) https://go.transunion.c... / Informa
18:55:14 21 Oct 2024 Task 3 DOM data manipulation (DOM-based) https://go.transunion.c... / Informa
18:55:14 21 Oct 2024 Task 3 HTML5 storage manipulation (DOM-based) https://go.transunion.c... / Informa
18:55:14 21 Oct 2024 Task 3 HTML5 storage manipulation (DOM-based) https://go.transunion.c... / Informa
18:55:14 21 Oct 2024 Task 3 HTML5 storage manipulation (DOM-based) https://go.transunion.c... / Informa
18:54:42 21 Oct 2024 Task 3 Content security policy: allowlisted script reso... https://go.transunion.c... / Informa
18:54:42 21 Oct 2024 Task 3 Content security policy: allows untrusted style... https://go.transunion.c... / Informa
18:54:42 21 Oct 2024 Task 3 Content security policy: allows untrusted scrip... https://go.transunion.c... / Informa
18:54:42 21 Oct 2024 Task 3 Cacheable HTTPS response https://go.transunion.c... / Informa
18:54:41 21 Oct 2024 Task 3 Cacheable HTTPS response https://go.transunion.c... /robots.txt Informa
18:54:41 21 Oct 2024 Task 3 Cross-domain script include https://go.transunion.c... / Informa
18:54:41 21 Oct 2024 Task 3 Strict transport security not enforced https://go.transunion.c... / Low
18:54:40 21 Oct 2024 Task 3 TLS certificate https://go.transunion.c... / Informa
Advisory Request Response Path to issue
Pretty Raw Hex Render
HTTP/2 200 OK
Content-Type: text/javascript
Date: Thu, 17 Oct 2024 15:43:47 GMT
Etag: W/"92a3a902cb0243c307593be0901ec460"
Last-Modified: Thu, 17 Oct 2024 15:43:26 GMT
Cache-Control: public, max-age=31536000, immutable
Vary: Accept-Encoding
X-Cache: Hit from cloudfront
Via: 1.1 a7e33ae8a84f3c5c69af4a152ea56772.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: SIN2-P3
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: QoVa9mE8XMQmRYhPC4-4_8E-il77dL1e6Kwil2NLwtVmOk6JatT-hQ==
Age: 337242
Inspector
Response headers 12

Vulnerabilities:

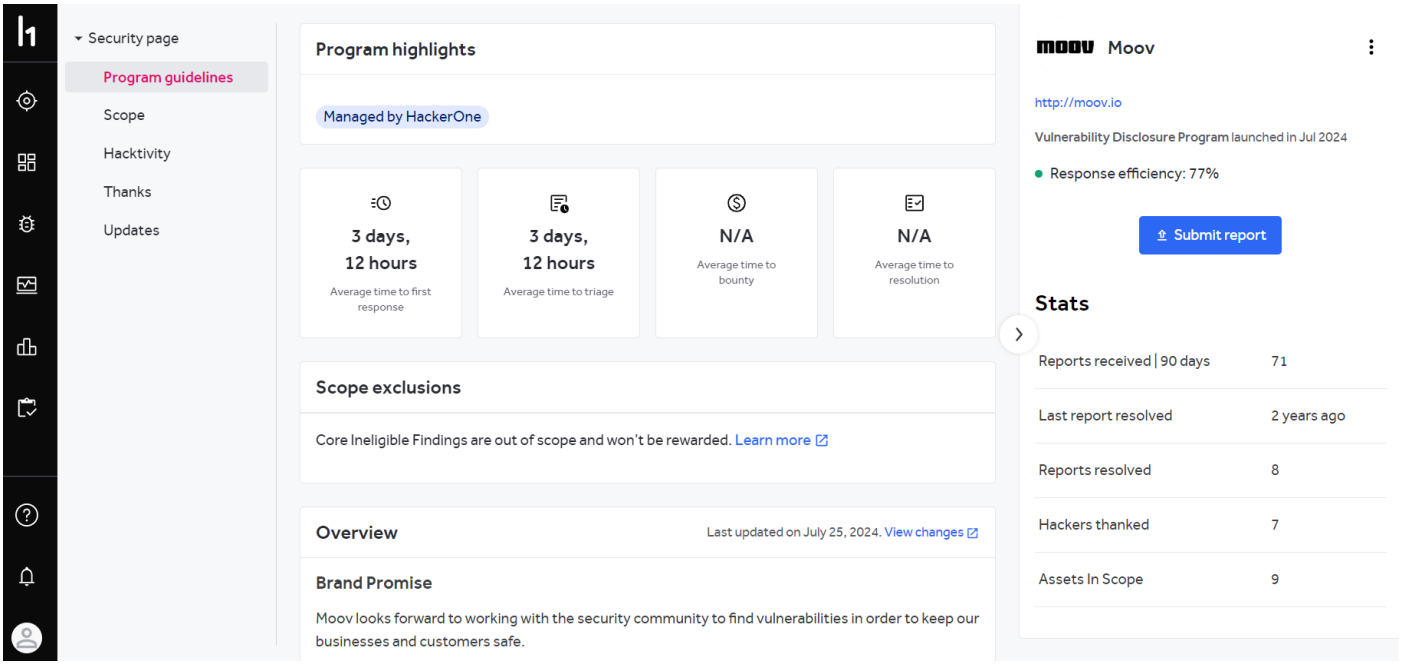
1 HTTP Strict Transport Security Policy Not Enabled

Vulnerability Title	**HTTP Strict Transport Security (HSTS) Policy Not Enabled**
Vulnerability Description	HSTS is a security feature that forces web browsers to communicate with servers only via secure HTTPS connections. The lack of HSTS increases the risk of Man-in-the-Middle (MITM) attacks, as users could be tricked into accessing the site over an insecure HTTP connection.
Affected Components	Web server configuration, specifically the response headers for **go.transunion.com** Any external site linked from a vulnerable website can receive the referrer URL, which may include sensitive or confidential information.
Impact Assessment	Without HSTS, users may accidentally connect over HTTP, exposing sensitive data to interception. Attackers could exploit this to steal session cookies, login credentials, or other confidential information through downgrading attacks.
Steps to Reproduce	1.Open a browser and attempt to connect to **http://go.transunion.com** (without HTTPS). 2. Observe that the connection is not automatically upgraded to HTTPS. 3. Inspect the HTTP response headers and note the absence of the **Strict-Transport-Security** header.
Proof of Concept	**http://go.transunion.com** in an unsecured network. Use network analysis tools (e.g., Wireshark) to observe traffic and confirm it's unencrypted.
Proposed Mitigation or Fix	Enable the HSTS policy on the server by adding the **Strict-Transport-Security** header. This header enforces HTTPS, prevents downgrade attacks, and sets a max age to enforce the policy. Ensure the site supports HTTPS properly before enabling this policy.

2 Cross-site Referrer Leakage through Referrer-Policy

Vulnerability Title	**Cross-site Referrer Leakage through Referrer-Policy**
Vulnerability Description	Cross-site Referrer Leakage vulnerability occurs when a website's Referrer-Policy allows the Referer header to expose sensitive URL information when users navigate from the website to another domain. The Referer header is an HTTP header that tells the destination website the URL of the page that the user was on before clicking a link. When misconfigured, sensitive data, such as session tokens, user IDs, or other sensitive query parameters included in the URL, may be shared with third-party domains.
Affected Components	Web Application Configuration: Specifically, the Referrer-Policy setting within the HTTP response headers. Browsers and HTTP Requests: Web browsers include the Referer header by default when users click on a link, and it is up to the site's policy to control what information is sent. Third-party Sites: Any external site linked from a vulnerable website can receive the referrer URL, which may include sensitive or confidential information.
Impact Assessment	Information Leakage: Sensitive details, such as internal URL paths, session identifiers, or even user-specific data embedded in the URL, may be leaked to external sites. This is particularly dangerous when users follow links to untrusted domains.
Steps to Reproduce	1. Visit the http://go.transunion.com 2. Inspect outgoing HTTP requests to external sites. 3. Note that the Referer header contains sensitive data.
Proof of Concept	Use browser developer tools or a network tool to capture an outgoing HTTP request and observe the full URL (or part of it) in the Referer header.
Proposed Mitigation or Fix	Implement a stricter Referrer-Policy, such as no-referrer or strict-origin-when-cross-origin, to prevent referrer information from being exposed to external sites.

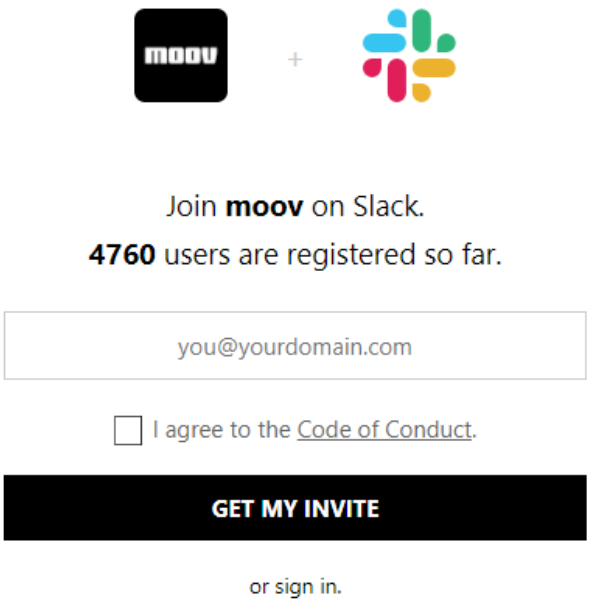
Report 02 Target Details



The target for this Bug Bounty report is Moov.io (https://www.moov.io), a platform providing modern payment solutions and infrastructure. The company offers various digital services, including payment processing, real-time payment tracking, and APIs for financial integrations. The platform is designed to make financial services more efficient, secure, and scalable by leveraging advanced technology.

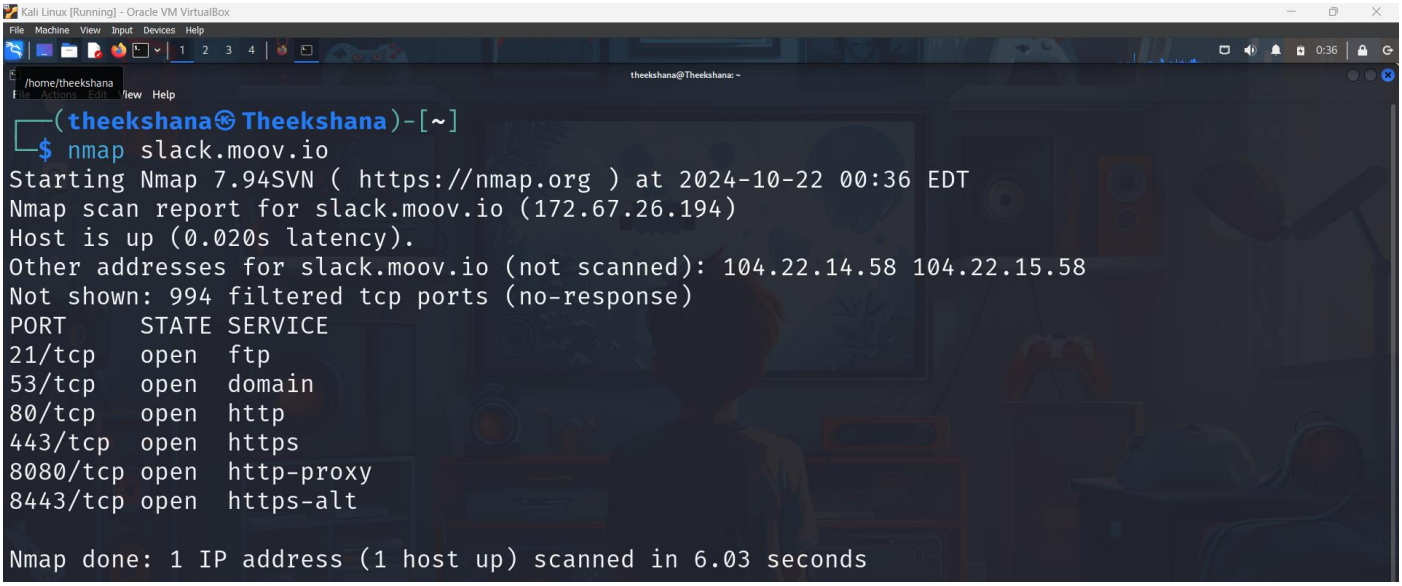
In this report, I have chosen to focus on 10 subdomains under the main domain moov.io. Each subdomain may offer distinct functionalities or services, which can potentially introduce different security risks. The subdomains were selected based on their relevance and the likelihood of containing vulnerabilities, particularly in development or user-related functionalities.

This report covers the findings for the subdomain: slack.moov.io



Target Reconnaissance

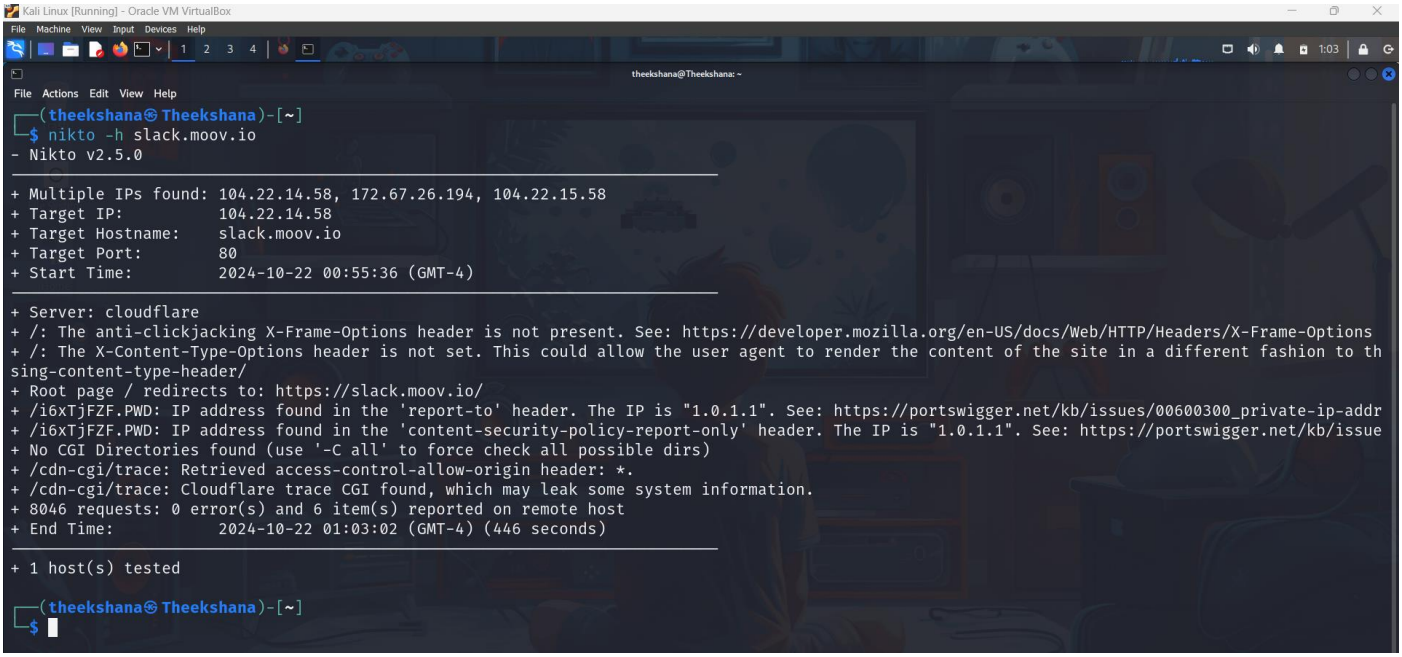
Nmap Scan



By scanning slack.moov.io with Nmap I found out these information.

Port	State	Service	Potential Vulnerabilities
21/tcp	Open	FTP	Data is not encrypted, so sensitive information can be stolen. Hackers can guess passwords (brute force attacks) Misconfigurations might allow unauthorized access
53/tcp	Open	DNS	Attackers can redirect users to fake sites (DNS poisoning) Hackers might flood the system (amplification attacks) Sensitive DNS info could be exposed (zone transfer)
80/tcp	Open	HTTP	Data is not secure (no encryption) Hackers can inject harmful scripts (XSS) Vulnerabilities in web applications might allow unauthorized access
443/tcp	Open	HTTPS	If not properly secured, attackers can intercept data Older encryption protocols may be weak
8080/tcp	Open	HTTP PROXY	If not secured, anyone can use the proxy for illegal activity Hackers could manipulate traffic through the proxy (HTTP smuggling)
8443/tcp	Open	HTTPS Alt	Same as HTTPS (443) risks if misconfigured Additional risks depending on how the alternate service is set up

Nikto Scan



The screenshot shows the output of a Nikto scan against the target slack.moov.io, which reveals several potential security issues and misconfigurations.

1. Missing X-Frame-Options Header:

The site lacks protection against clickjacking attacks. This allows attackers to embed the site in an iframe and trick users into interacting with it.

2. Missing X-Content-Type-Options Header:

The absence of this header allows browsers to interpret files as a different MIME type, making the site vulnerable to content-sniffing attacks.

3. Exposed Private IP Addresses:

Private IP addresses (1.0.1.1) were found in the report-to and content-security-policy-report-only headers. Exposing internal network information can assist attackers in planning further attacks.

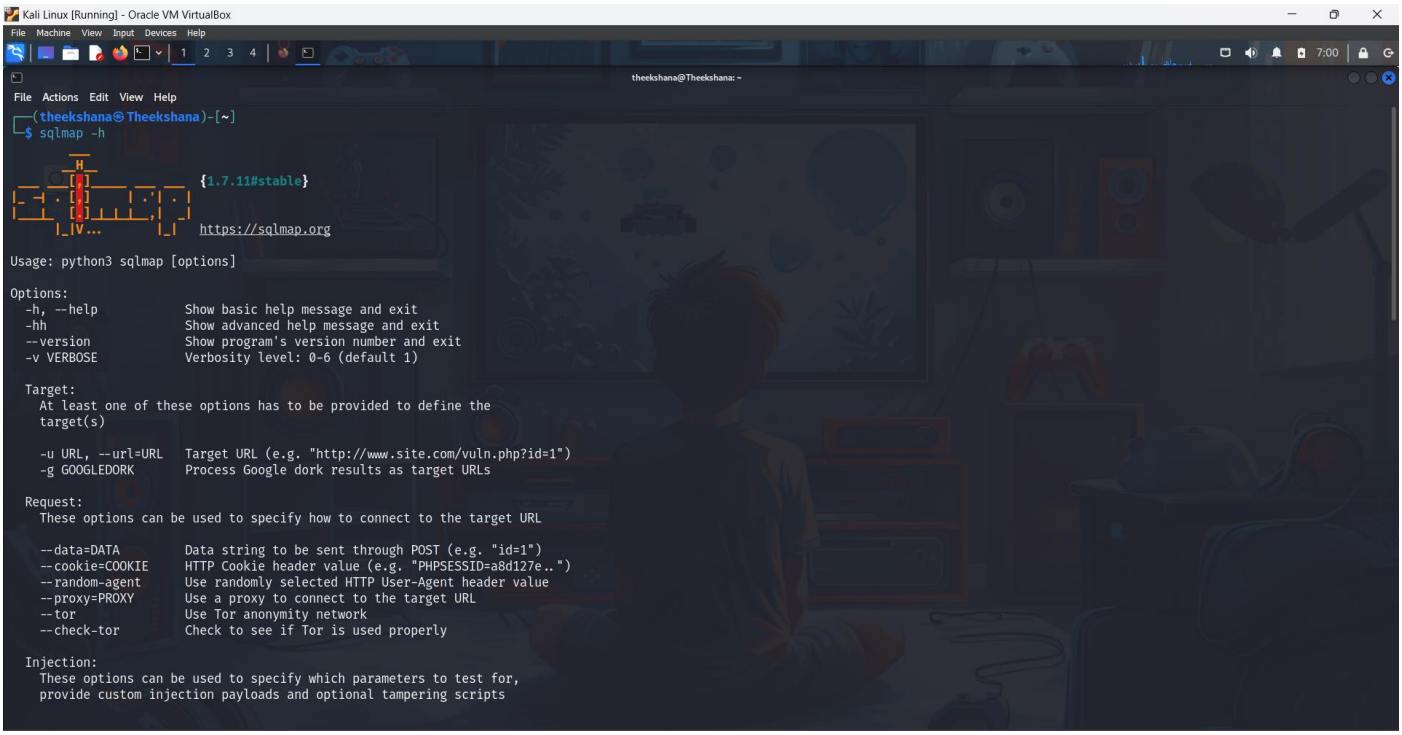
4. Overly Permissive Access-Control-Allow-Origin Header:

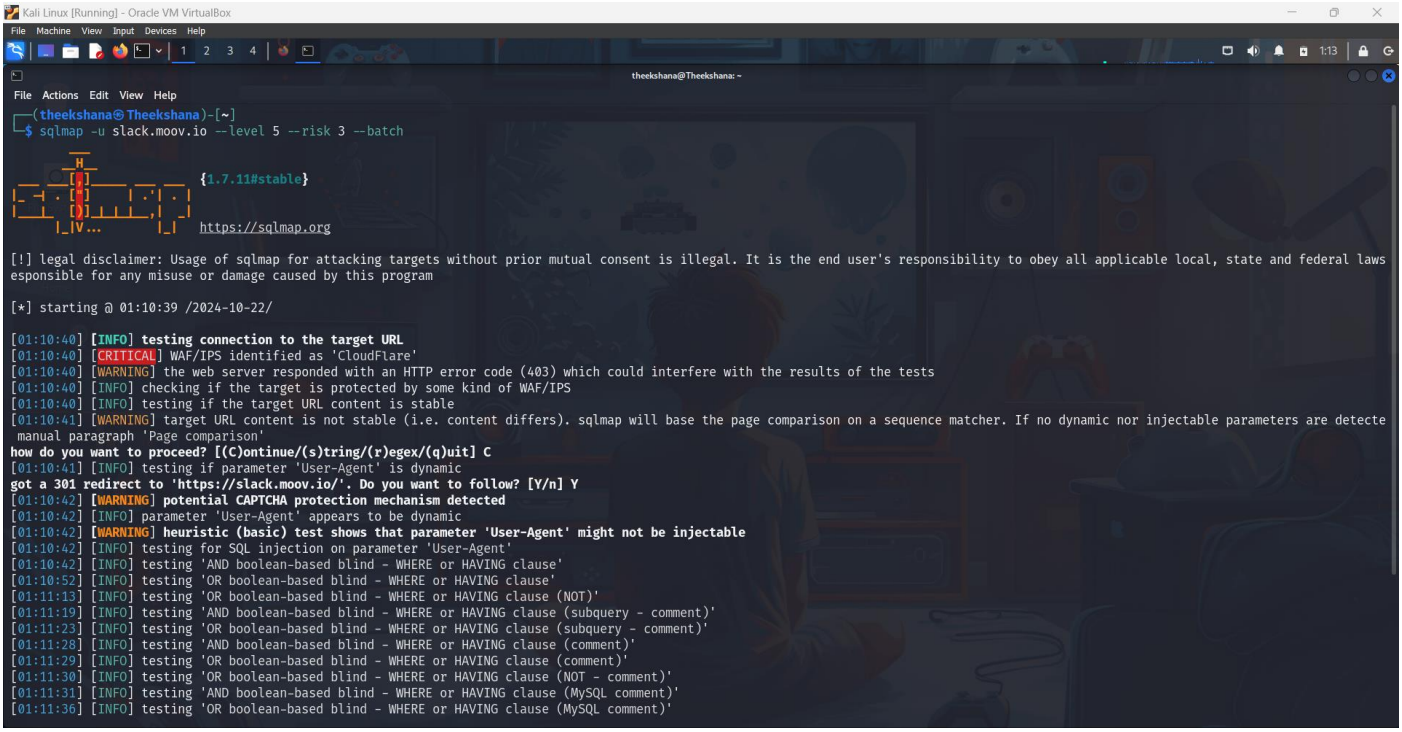
The CORS policy allows requests from any origin (Access-Control-Allow-Origin:). This could lead to a Cross-Origin Resource Sharing (CORS) vulnerability if sensitive data is accessible to unauthorized origins.

5. Potential Information Leakage via Cloudflare Trace:

The /cdn-cgi/trace`endpoint may leak system information that could be useful to attackers during reconnaissance.

SQLmap Scaner





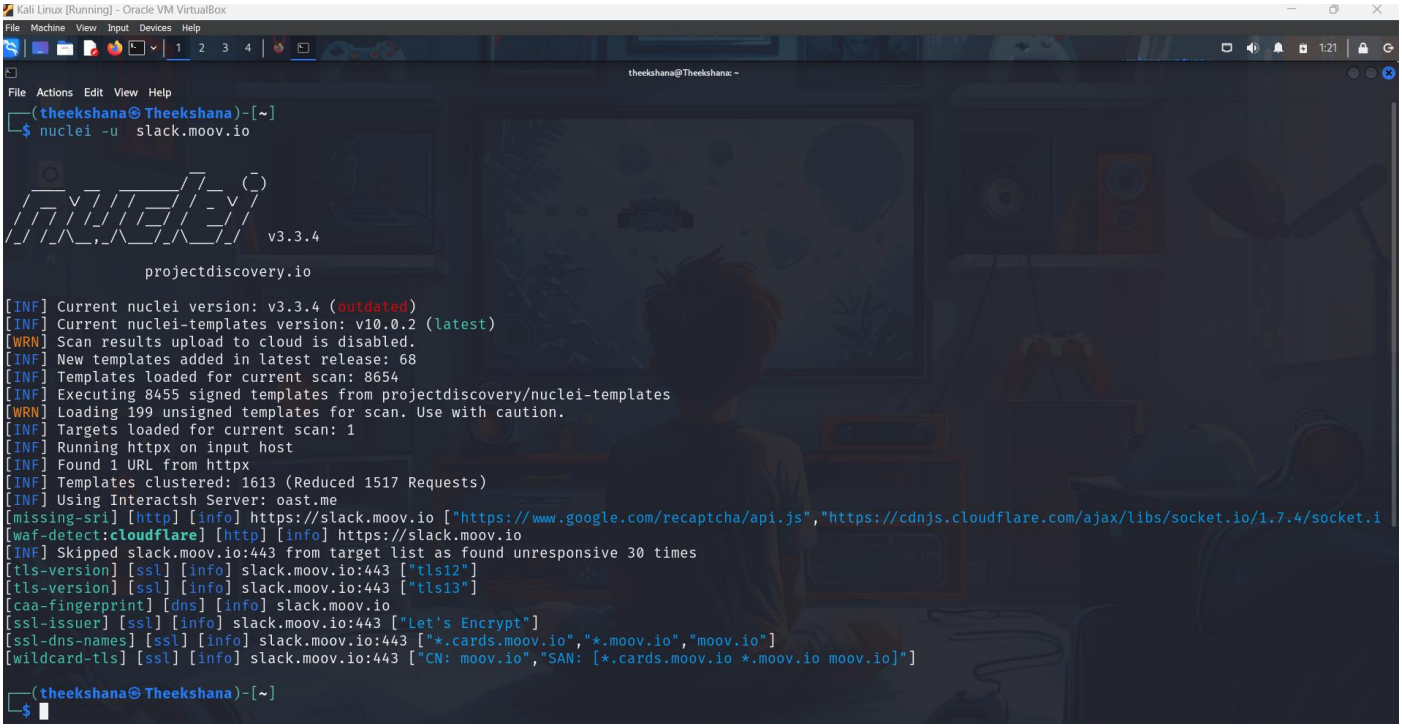
Vulnerabilities Detected:

WAF/IPS Detected (Cloudflare): The target URL has a Web Application Firewall (WAF), specifically Cloudflare, which is actively protecting the site.

403 Error & CAPTCHA: The web server returned an HTTP 403 error (forbidden), indicating some protective measures. CAPTCHA mechanisms might be in place to thwart automated scripts.

Testing Dynamic Parameters: Sqlmap is checking if the User-Agent parameter is injectable. However, basic heuristic tests suggest it might not be injectable.

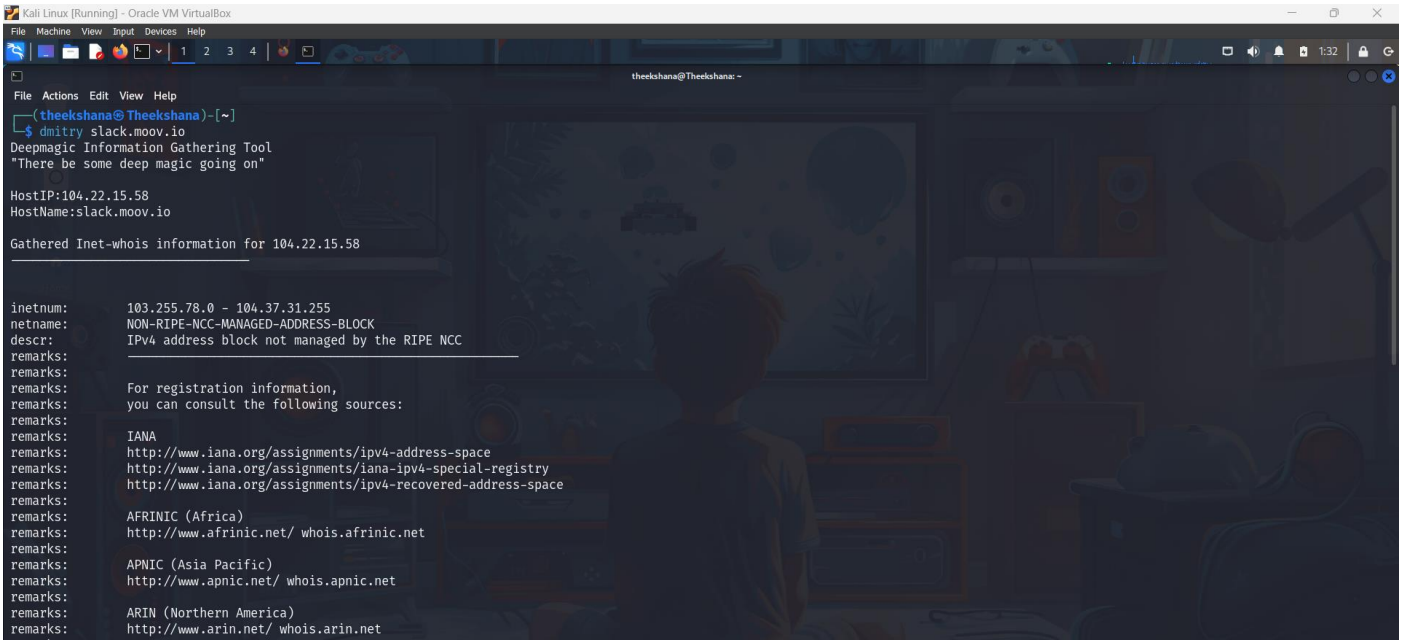
Nuclei Scan

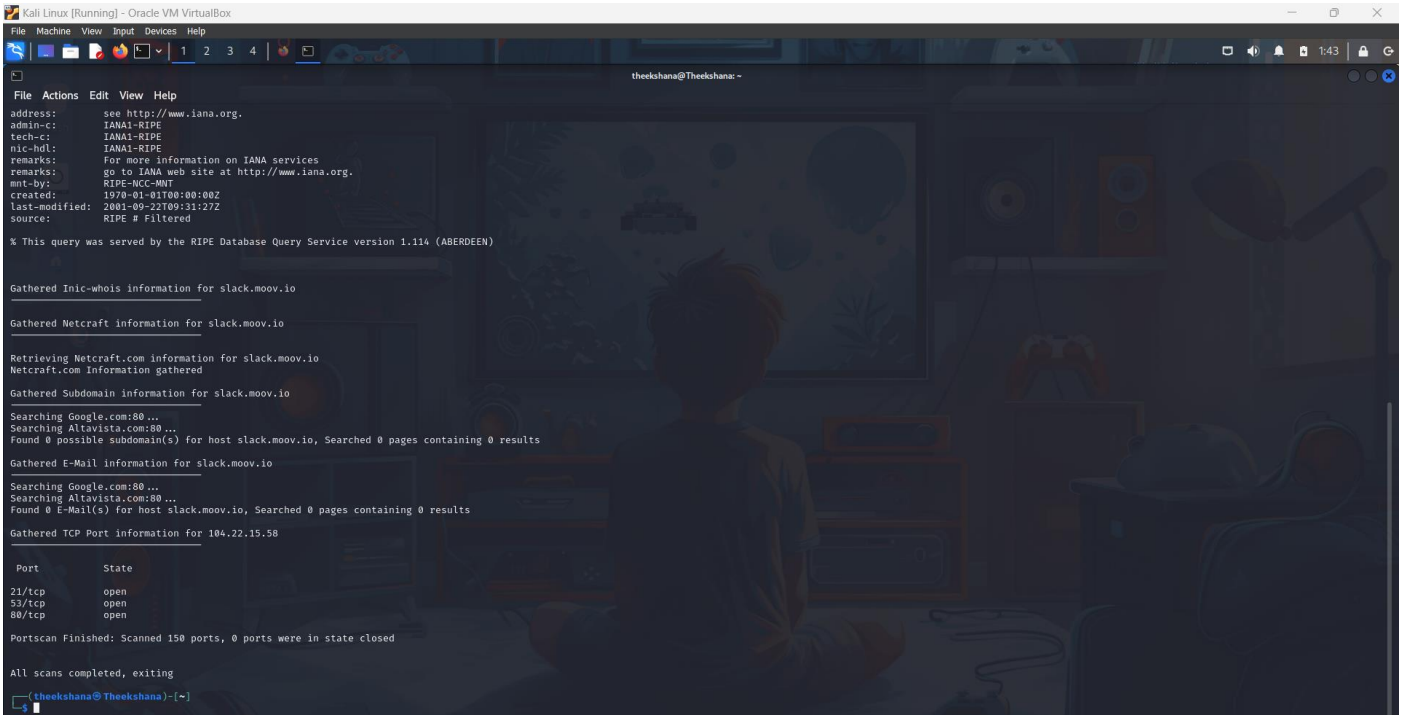


Important Findings:

Vulnerability Type	Description	Risk
missing-sri [http]	The URL https://slack.moov.io is missing Subresource Integrity (SRI) checks. SRI is a security feature that ensures that external resources (like scripts or stylesheets) haven't been altered by an attacker.	High
waf-detect [Cloudflare]	The target URL slack.moov.io is protected by a Web Application Firewall (WAF), specifically Cloudflare. This means that the server has an additional layer of security that filters and blocks malicious traffic, such as SQL injections or cross-site scripting attempts.	Low
tls-version [ssl]	The site slack.moov.io is using TLS 1.3, which is the latest version of the Transport Layer Security (TLS) protocol. TLS provides secure communication over a network (encryption) to protect data integrity and confidentiality.	Low
ssl-issuer [ssl]	The SSL certificate for slack.moov.io is issued by Let's Encrypt, a free, automated, and open Certificate Authority (CA) that issues SSL certificates. The SSL certificate ensures that the connection between users and the site is encrypted.	Low
ssl-dns-names [ssl]	The Subject Alternative Names (SAN) for this SSL certificate include .cards.moov.io, .moov.io, and moov.io. This means that the SSL certificate covers these subdomains and the base domain.	Low
wildcard-tls [ssl]	The SSL certificate includes a wildcard for cards.moov.io and .moov.io. A wildcard certificate covers all subdomains under the specified domains. While wildcard certificates are convenient, they can pose a risk if any subdomain is vulnerable because it could potentially affect the security of the entire domain.	Medium

Dmitry Scan



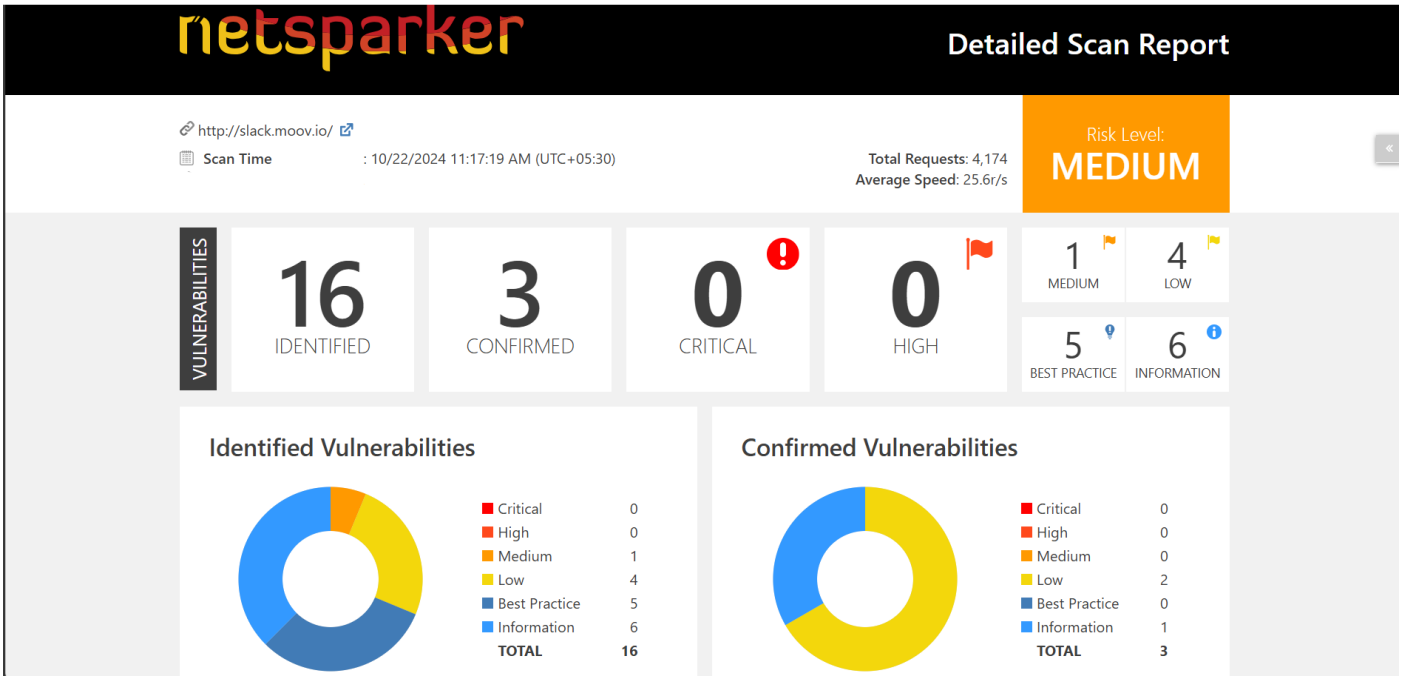


Port 21 (FTP - File Transfer Protocol): This port is typically used for file transfer services. Having FTP open can be risky if not properly secured, as it often transmits data in plain text (though secure variants like SFTP exist).

Port 53 (DNS - Domain Name System): This port is used for DNS services, which translate domain names into IP addresses. While DNS services need to be accessible, misconfigurations or vulnerabilities (like DNS amplification attacks) can expose the server to risks.

Port 80 (HTTP - Hypertext Transfer Protocol): This port is used for unencrypted web traffic. Port 80 being open suggests that the website is accessible via HTTP, but this should be redirected to HTTPS (Port 443) for encrypted communication. If not, it leaves the site vulnerable to man-in-the-middle (MITM) attacks.

Netsparker



Vulnerability Summary

SEVERITY FILTER : CRITICAL HIGH MEDIUM LOW BEST PRACTICE INFORMATION

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://slack.moov.io/	
	Misconfigured Access-Control-Allow-Origin Header	GET	https://slack.moov.io/assets/	
	Missing X-Frame-Options Header	GET	https://slack.moov.io/.well-known/	
	Cookie Not Marked as Secure	GET	https://slack.moov.io/socket.io/?EIO=3&t=PAon3aA&transport=polling	
	Insecure Frame (External)	GET	https://slack.moov.io/	
	Content Security Policy (CSP) Not Implemented	GET	https://slack.moov.io/	
	Expect-CT Not Enabled	GET	https://slack.moov.io/assets/main.css	
	Missing X-XSS-Protection Header	GET	https://slack.moov.io/.well-known/	
	Referrer-Policy Not Implemented	GET	https://slack.moov.io/.well-known/	
	Subresource Integrity (SRI) Not Implemented	GET	https://slack.moov.io/?nsextt=%0d%0ans%3anetsparker056650%3dvuln	nsextt

Misconfigured Access-Control-Allow-Origin Header

LOW 1

Netsparker detected a possibly misconfigured Access-Control-Allow-Origin header in resource's HTTP response.

Cross-origin resource sharing (CORS) is a mechanism that allows resources on a web page to be requested outside the domain through XMLHttpRequest.

Unless this HTTP header is present, such "cross-domain" requests are forbidden by web browsers, per the same-origin security policy.

Impact

This is generally not appropriate when using the same-origin security policy. The only case where this is appropriate when using the same-origin policy is when a page or API response is considered completely public content and it is intended to be accessible to everyone.

Vulnerabilities

4.1. https://slack.moov.io/assets/

Hide Remediation

Remedy

If this page is intended to be accessible to everyone, you don't need to take any action. Otherwise please follow the guidelines for different architectures below in order to set this header and permit outside domain.

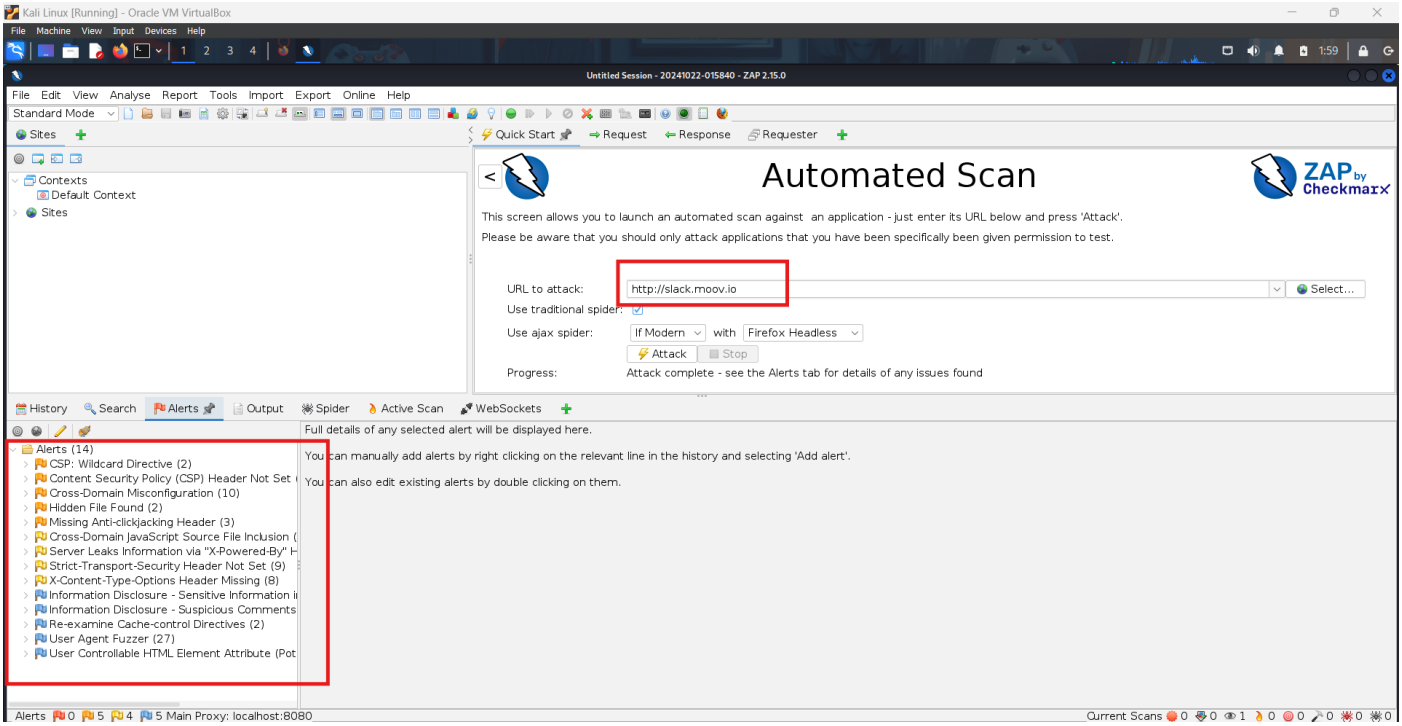
Apache

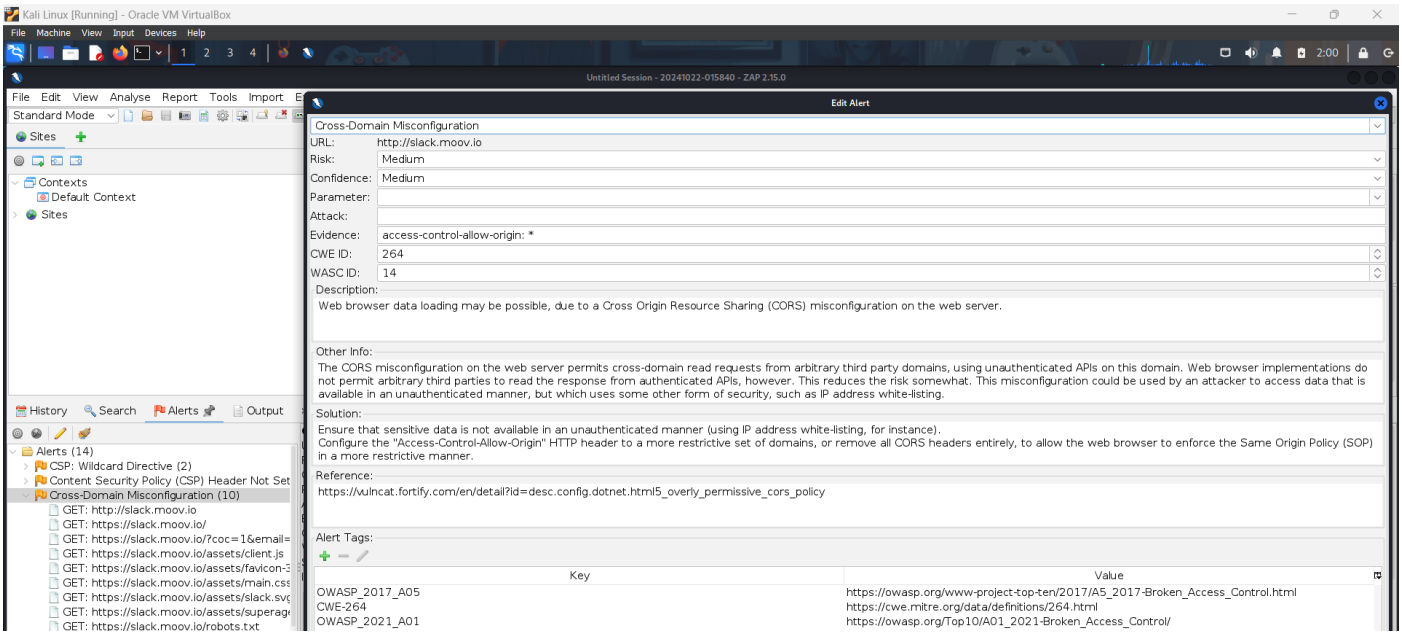
- Add the following line inside either the <directory>, <location>, <files> or <virtualhost> sections of your server config (usually located in `httpd.conf` or `apache.conf`), or within a `.htaccess` file.

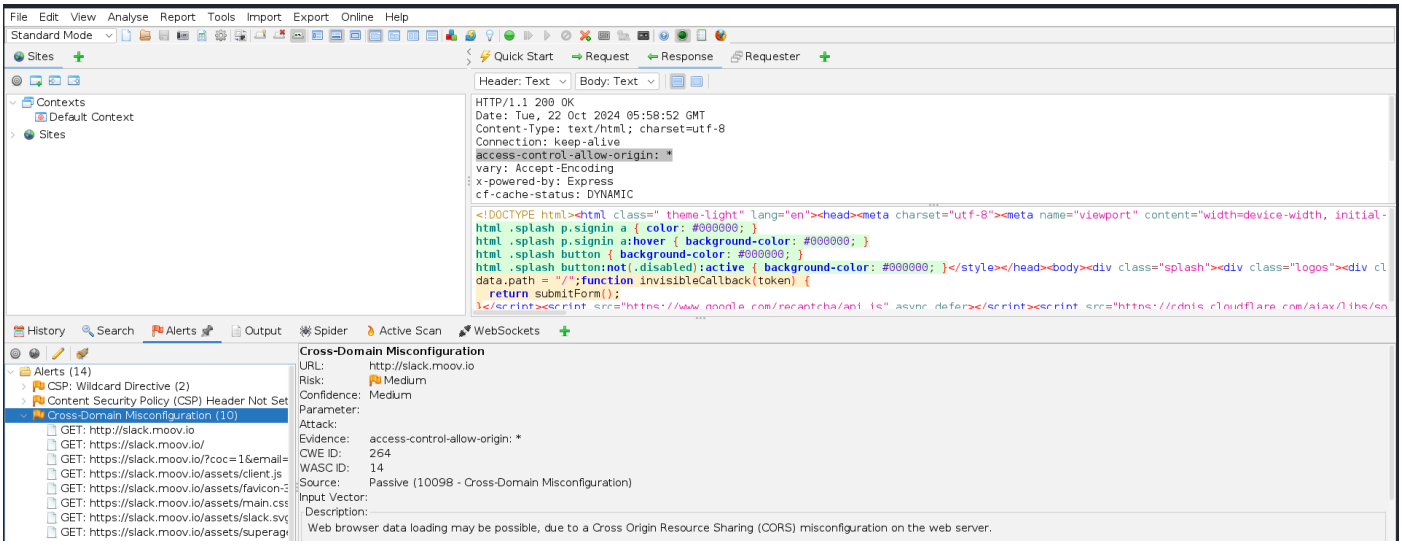
CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
SANS Top 25	16

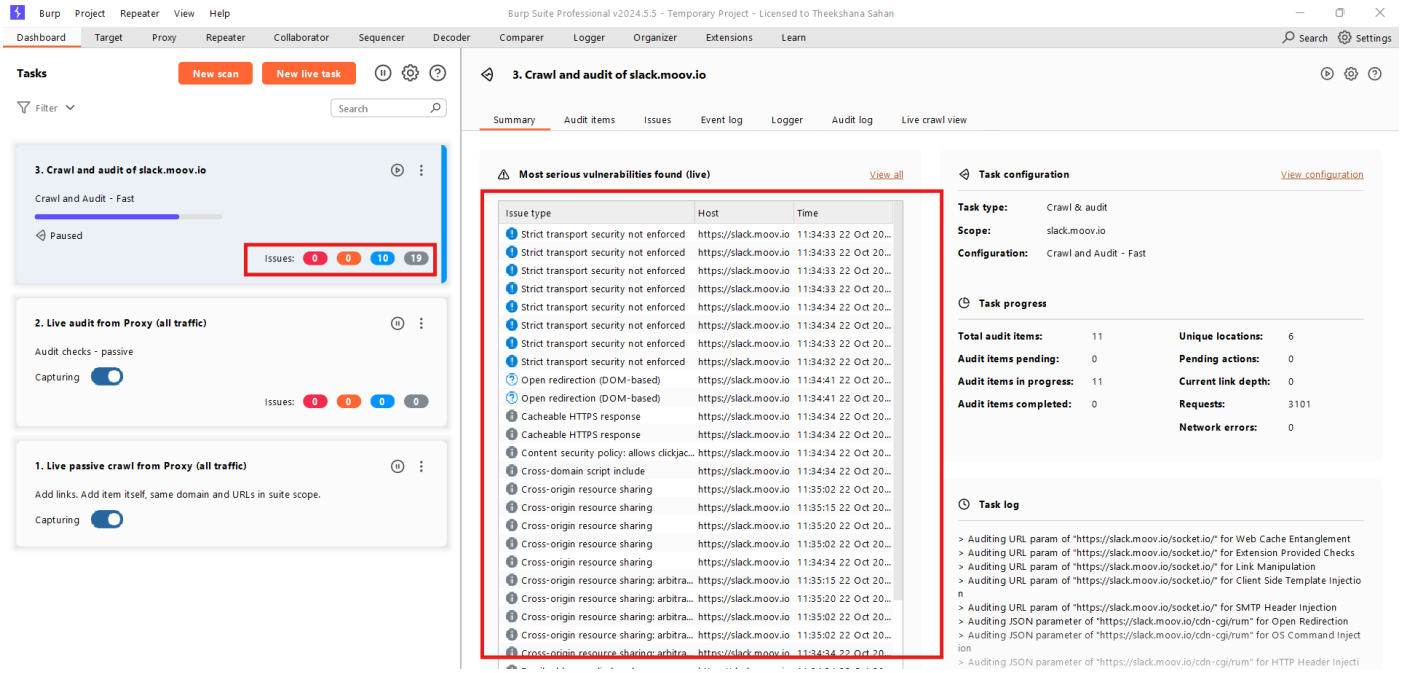
OWASP ZAP

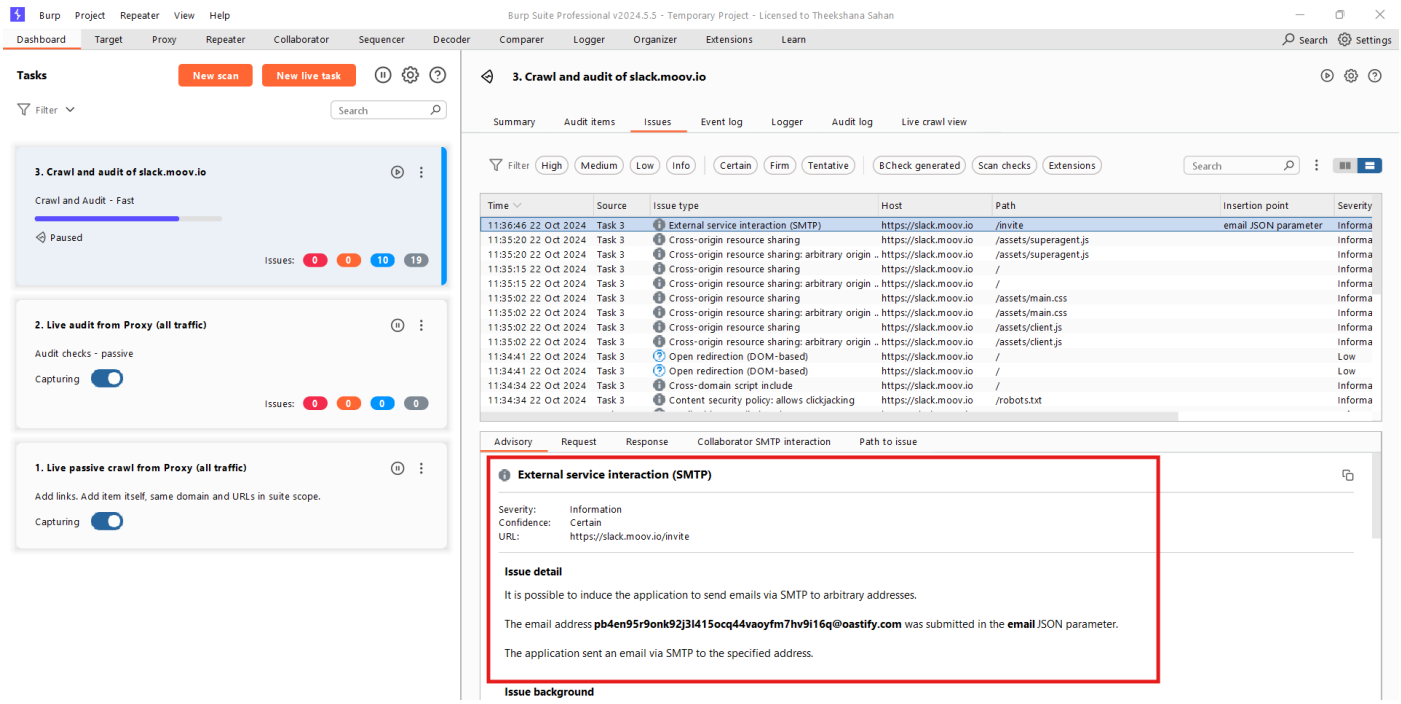

Kali Linux [Running] - Oracle VM VirtualBox
Untitled Session - 20241022-015840 - ZAP 2.15.0
Automated Scan
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack: http://slack.moov.io
Use traditional spider:
Use ajax spider: If Modern with Firefox Headless
Attack
Stop
Progress: Attack complete - see the Alerts tab for details of any issues found
Alerts (14)
CSP: Wildcard Directive (2)
Content Security Policy (CSP) Header Not Set
Cross-Domain Misconfiguration (10)
Hidden File Found (2)
Missing Anti-clickjacking Header (3)
Strict-Transport-Security Header Not Set (9)
X-Content-Type-Options Header Missing (8)
Information Disclosure - Suspicious Comments
Re-examine Cache-control Directives (2)
User Agent Fuzzer (27)
User Controllable HTML Element Attribute (Pot
Full details of any selected alert will be displayed here.
You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.
You can also edit existing alerts by double clicking on them.

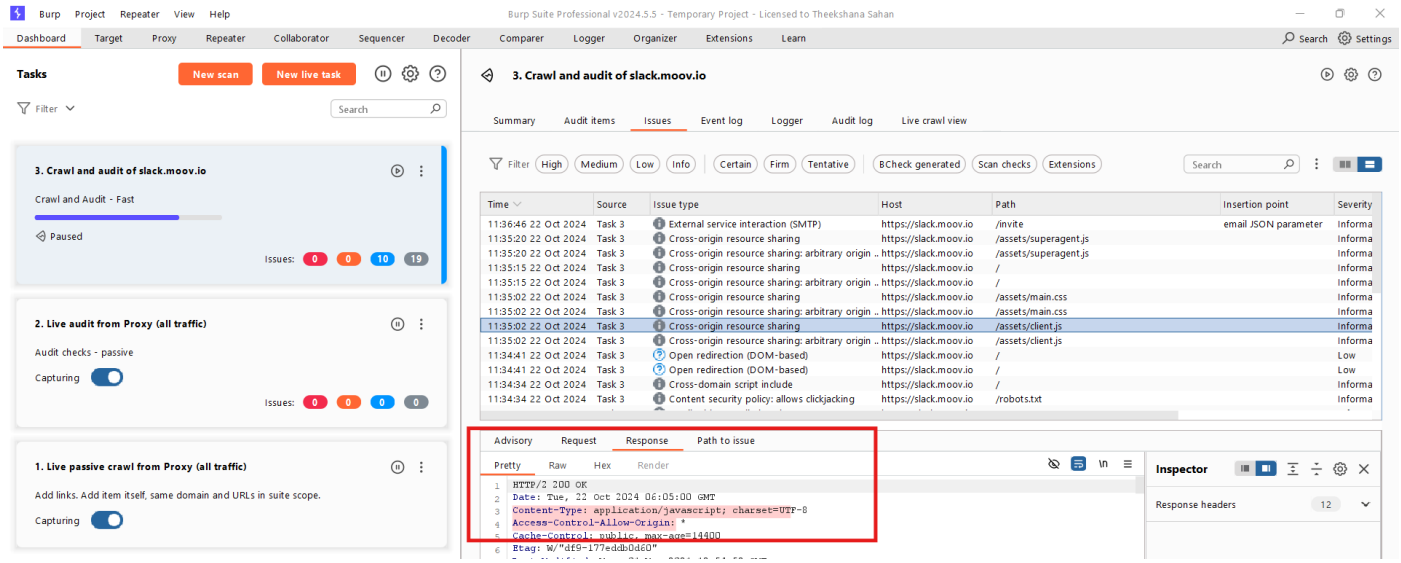

Edit Alert
Cross-Domain Misconfiguration
URL: http://slack.moov.io
Risk: Medium
Confidence: Medium
Parameter:
Attack:
Evidence: access-control-allow-origin: *
CWE ID: 264
WASC ID: 14
Description:
Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration 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).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Reference:
https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
Alert Tags:
Key
Value
OWASP_2017_A05
https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html
CWE-264
https://cwe.mitre.org/data/definitions/264.html
OWASP_2021_A01
https://owasp.org/Top10/A01_2021-Broken_Access_Control/


HTTP/1.1 200 OK
Date: Tue, 22 Oct 2024 05:58:52 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
access-control-allow-origin: *
vary: Accept-Encoding
x-powered-by: Express
cf-cache-status: DYNAMIC
Cross-Domain Misconfiguration
URL: http://slack.moov.io
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.

Burp Suite


Burp Project Repeater View Help
Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan
Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Tasks
New scan
New live task
Filter
Search
3. Crawl and audit of slack.moov.io
Crawl and Audit - Fast
Paused
Issues: 0 0 10 19
2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing
Issues: 0 0 0 0
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing
3. Crawl and audit of slack.moov.io
Summary Audit items Issues Event log Logger Audit log Live crawl view
Most serious vulnerabilities found (live)
View all
Issue type Host Time
Strict transport security not enforced https://slack.moov.io 11:34:33 22 Oct 20...
Open redirection (DOM-based) https://slack.moov.io 11:34:41 22 Oct 20...
Cacheable HTTPS response https://slack.moov.io 11:34:34 22 Oct 20...
Content security policy: allows clickjac... https://slack.moov.io 11:34:34 22 Oct 20...
Cross-domain script include https://slack.moov.io 11:34:34 22 Oct 20...
Cross-origin resource sharing https://slack.moov.io 11:35:02 22 Oct 20...
Cross-origin resource sharing https://slack.moov.io 11:35:15 22 Oct 20...
Cross-origin resource sharing: arbitra... https://slack.moov.io 11:35:15 22 Oct 20...
Task configuration
View configuration
Task type: Crawl & audit
Scope: slack.moov.io
Configuration: Crawl and Audit - Fast
Task progress
Total audit items: 11
Audit items pending: 0
Audit items in progress: 11
Audit items completed: 0
Unique locations: 6
Pending actions: 0
Current link depth: 0
Requests: 3101
Network errors: 0
Task log
> Auditing URL param of "https://slack.moov.io/socket.io/" for Web Cache Entanglement
> Auditing URL param of "https://slack.moov.io/socket.io/" for Extension Provided Checks
> Auditing URL param of "https://slack.moov.io/socket.io/" for Link Manipulation
> Auditing URL param of "https://slack.moov.io/socket.io/" for Client Side Template Injection
> Auditing URL param of "https://slack.moov.io/socket.io/" for SMTP Header Injection
> Auditing JSON parameter of "https://slack.moov.io/cdn-cgi/rum" for Open Redirection
> Auditing JSON parameter of "https://slack.moov.io/cdn-cgi/rum" for OS Command Injection


Burp Project Repeater View Help
Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan
Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Tasks
New scan
New live task
3. Crawl and audit of slack.moov.io
Summary Audit items Issues Event log Logger Audit log Live crawl view
Filter High Medium Low Info Certain Firm Tentative BCheck generated Scan checks Extensions
Time Source Issue type Host Path Insertion point Severity
11:36:46 22 Oct 2024 Task 3 External service interaction (SMTP) https://slack.moov.io /invite email JSON parameter Informa
11:35:20 22 Oct 2024 Task 3 Cross-origin resource sharing https://slack.moov.io /assets/superagent.js Informa
11:35:20 22 Oct 2024 Task 3 Cross-origin resource sharing: arbitrary origin ... https://slack.moov.io /assets/superagent.js Informa
11:35:15 22 Oct 2024 Task 3 Cross-origin resource sharing https://slack.moov.io / Informa
11:35:15 22 Oct 2024 Task 3 Cross-origin resource sharing: arbitrary origin ... https://slack.moov.io / Informa
11:35:02 22 Oct 2024 Task 3 Cross-origin resource sharing https://slack.moov.io /assets/main.css Informa
11:35:02 22 Oct 2024 Task 3 Cross-origin resource sharing: arbitrary origin ... https://slack.moov.io /assets/main.css Informa
11:35:02 22 Oct 2024 Task 3 Cross-origin resource sharing https://slack.moov.io /assets/client.js Informa
11:35:02 22 Oct 2024 Task 3 Cross-origin resource sharing: arbitrary origin ... https://slack.moov.io /assets/client.js Informa
11:34:41 22 Oct 2024 Task 3 Open redirection (DOM-based) https://slack.moov.io / Low
11:34:41 22 Oct 2024 Task 3 Open redirection (DOM-based) https://slack.moov.io / Low
11:34:34 22 Oct 2024 Task 3 Cross-domain script include https://slack.moov.io / Informa
11:34:34 22 Oct 2024 Task 3 Content security policy: allows clickjacking https://slack.moov.io /robots.txt Informa
Advisory Request Response Collaborator SMTP interaction Path to issue
External service interaction (SMTP)
Severity: Information
Confidence: Certain
URL: https://slack.moov.io/invite
Issue detail
It is possible to induce the application to send emails via SMTP to arbitrary addresses.
The email address pb4en95r9onk92j3l415ocq44vaoyfm7hv9i16q@oastify.com was submitted in the email JSON parameter.
The application sent an email via SMTP to the specified address.
Issue background


Burp Project Repeater View Help
Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan
Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Tasks
New scan
New live task
3. Crawl and audit of slack.moov.io
Summary Audit items Issues Event log Logger Audit log Live crawl view
Filter High Medium Low Info Certain Firm Tentative BCheck generated Scan checks Extensions
Time Source Issue type Host Path Insertion point Severity
11:36:46 22 Oct 2024 Task 3 External service interaction (SMTP) https://slack.moov.io /invite email JSON parameter Informa
11:35:20 22 Oct 2024 Task 3 Cross-origin resource sharing https://slack.moov.io /assets/superagent.js Informa
11:35:20 22 Oct 2024 Task 3 Cross-origin resource sharing: arbitrary origin ... https://slack.moov.io /assets/superagent.js Informa
11:35:15 22 Oct 2024 Task 3 Cross-origin resource sharing https://slack.moov.io / Informa
11:35:15 22 Oct 2024 Task 3 Cross-origin resource sharing: arbitrary origin ... https://slack.moov.io / Informa
11:35:02 22 Oct 2024 Task 3 Cross-origin resource sharing https://slack.moov.io /assets/main.css Informa
11:35:02 22 Oct 2024 Task 3 Cross-origin resource sharing: arbitrary origin ... https://slack.moov.io /assets/main.css Informa
11:35:02 22 Oct 2024 Task 3 Cross-origin resource sharing https://slack.moov.io /assets/client.js Informa
11:35:02 22 Oct 2024 Task 3 Cross-origin resource sharing: arbitrary origin ... https://slack.moov.io /assets/client.js Informa
11:34:41 22 Oct 2024 Task 3 Open redirection (DOM-based) https://slack.moov.io / Low
11:34:41 22 Oct 2024 Task 3 Open redirection (DOM-based) https://slack.moov.io / Low
11:34:34 22 Oct 2024 Task 3 Cross-domain script include https://slack.moov.io / Informa
11:34:34 22 Oct 2024 Task 3 Content security policy: allows clickjacking https://slack.moov.io /robots.txt Informa
Advisory Request Response Path to issue
Pretty Raw Hex Render
HTTP/2 200 OK
Date: Tue, 22 Oct 2024 06:05:00 GMT
Content-Type: application/javascript; charset=UTF-8
Access-Control-Allow-Origin: *
Cache-Control: public, max-age=14400
Etag: W/"df9-177eddb0d60"
Inspector
Response headers 12

Vulnerabilities:

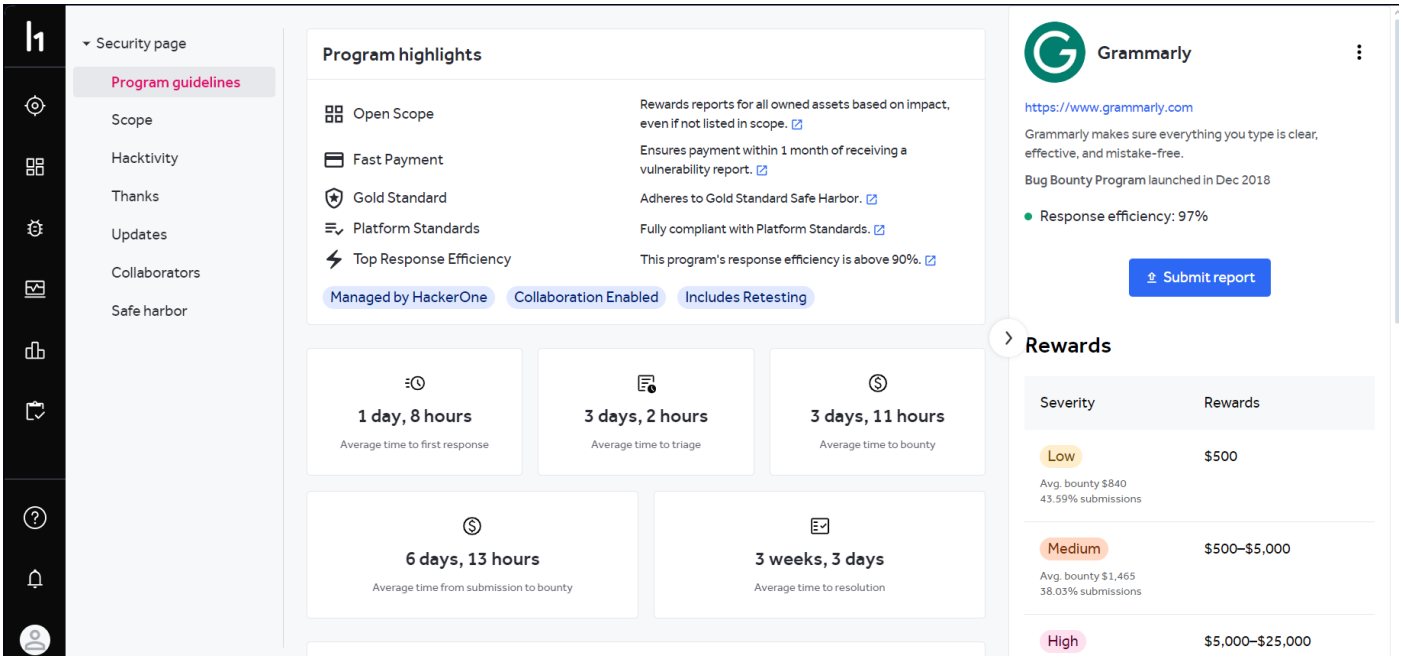
1 Anti-Clickjacking Header Missing

Vulnerability Title	**Anti-Clickjacking Header Missing**
Vulnerability Description	slack.moov.io, does not include headers that prevent it from being embedded in an iframe. Attackers can create a malicious page that embeds the website in an invisible frame (an HTML element that displays another webpage inside it). Since users don't see the malicious frame, they might unknowingly perform sensitive actions, such as clicking buttons, submitting forms, or approving transactions.
Affected Components	**slack.moov.io** is the affected domain, and the issue lies in the server's HTTP response headers. The server is not sending the X-Frame-Options or Content-Security-Policy headers, which are responsible for dictating how (or if) a site can be embedded into an iframe.
Impact Assessment	Without the appropriate anti-clickjacking headers, users could unknowingly interact with a malicious version of the site. This could lead to actions being performed without the user's consent, which is especially dangerous if those actions involve sensitive data, such as financial transactions, login credentials, or administrative tasks.
Steps to Reproduce	Inspect the HTTP response headers: Most browsers and developer tools (such as Chrome's DevTools) allow you to view response headers from a server. Here, you would see that the X-Frame-Options or Content-Security-Policy headers are missing, which would normally prevent the page from being embedded. Attempt an iframe attack: Create a simple HTML page that embeds slack.moov.io inside an iframe and see if the site loads within the frame. If it does, this demonstrates that the site is vulnerable to clickjacking.
Proof of Concept	create an HTML file that embeds **slack.moov.io** within an iframe on an external site. When the embedded page loads, an attacker could place transparent buttons or overlay sensitive page elements, tricking users into performing unintended actions. <iframe src="http://slack.moov.io" style="width:100%; height:100%; opacity:0;"></iframe>
Proposed Mitigation or Fix	Add this header with the value DENY to completely block all iframes. Or use SAMEORIGIN to allow framing only from the same domain Header always set X-Frame-Options "DENY"

2 X-Content-Type-Options Header Missing

Vulnerability Title	X-Content-Type-Options Header Missing
Vulnerability Description	The X-Content-Type-Options header is a security feature that prevents browsers from interpreting files as a different MIME type than what is declared by the server. This helps protect against MIME-based attacks, where an attacker could trick the browser into executing potentially harmful content (such as a script) when it is interpreted as a different file type.
Affected Components	Web server configuration, specifically the response headers for slack.moov.io. Without this header, various resources (like JavaScript or CSS files) served by slack.moov.io may be interpreted as the wrong content type by browsers, potentially leading to security vulnerabilities.
Impact Assessment	Without the X-Content-Type-Options header, attackers could exploit the browser's MIME-type sniffing capabilities to launch cross-site scripting (XSS) or other attacks. For example, a file served as a text/plain MIME type might be interpreted by the browser as executable script code, leading to unintended execution and possible compromise.
Steps to Reproduce	Open a browser and connect to **http://slack.moov.io**. Use the browser's developer tools to inspect the response headers for any static resource Confirm the absence of the X-Content-Type-Options header, which would normally prevent MIME-type sniffing. Simulate a file type change (for instance, renaming a .js file to .txt) and observe how the browser tries to guess the content type.
Proof of Concept	Attempt to load a static resource (such as a CSS or JS file) from **http://slack.moov.io** without the X-Content-Type-Options header. Use network analysis tools or browser developer tools to confirm that the resource is missing the X-Content-Type-Options: nosniff header.
Proposed Mitigation or Fix	This prevents the browser from attempting to infer (or "sniff") the MIME type of a resource. By specifying this header, the server ensures that the browser will only handle resources according to their declared type, mitigating the risk of MIME-based attacks. Header set X-Content-Type-Options "nosniff"

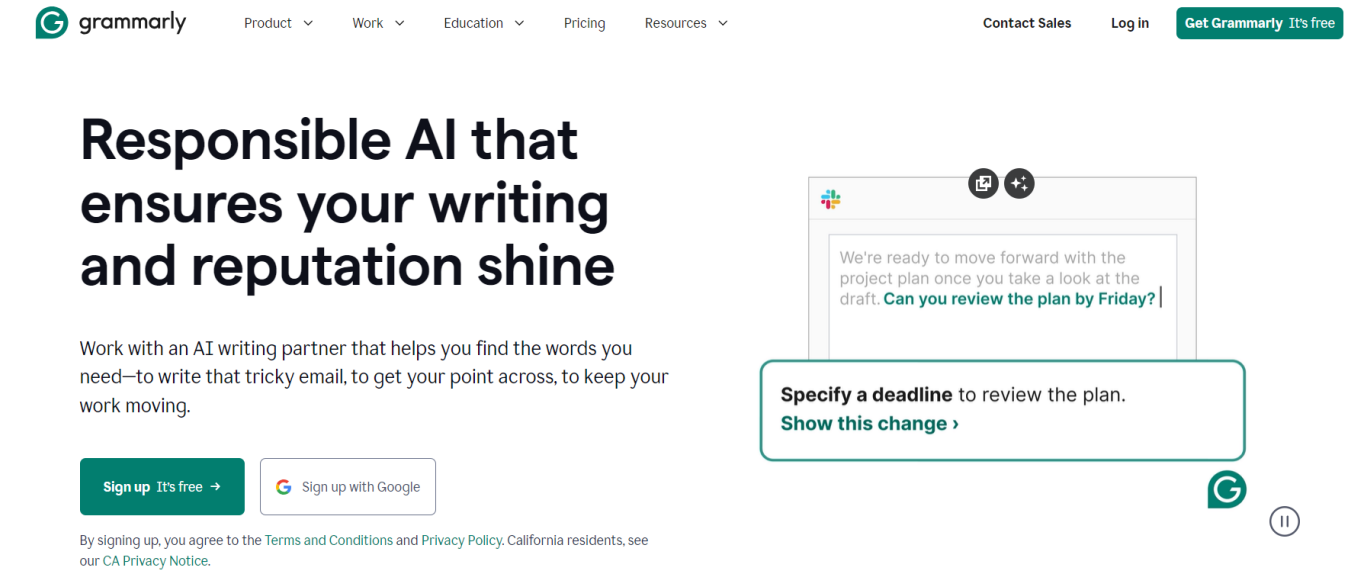
Report 03Target Details



The target for this Bug Bounty report is Grammarly (https://www.grammarly.com), a platform providing modern writing assistance and grammar-checking solutions.The company offers various digital services, including grammar checking, writing enhancement, and APIs for language integrations. The platform is designed to make writing services more efficient, user-friendly, and scalable by leveraging advanced technology.

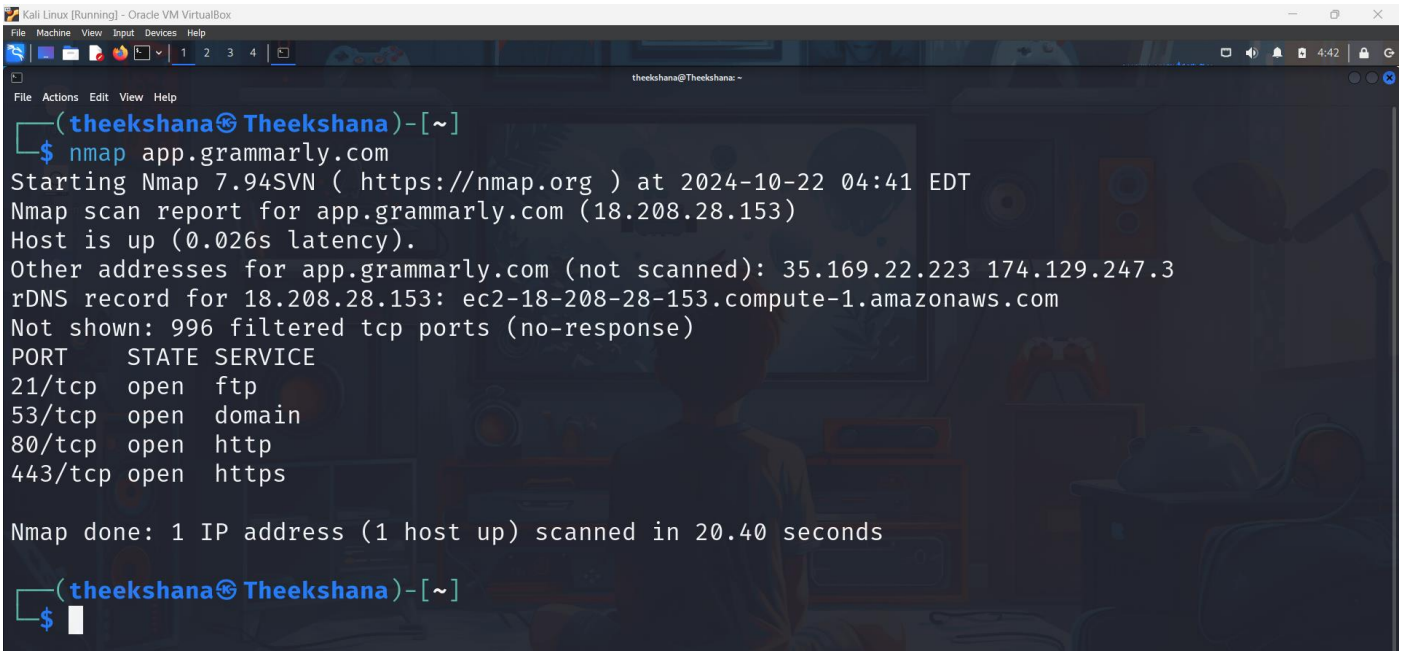
In this report, I have chosen to focus on 10 subdomains under the main domain grammarly.com. Each subdomain may offer distinct functionalities or services, which can potentially introduce different security risks. The subdomains were selected based on their relevance and the likelihood of containing vulnerabilities, particularly in development or user-related functionalities.

This report covers the findings for the subdomain: app.grammarly.com



Target Reconnaissance

Nmap Scan



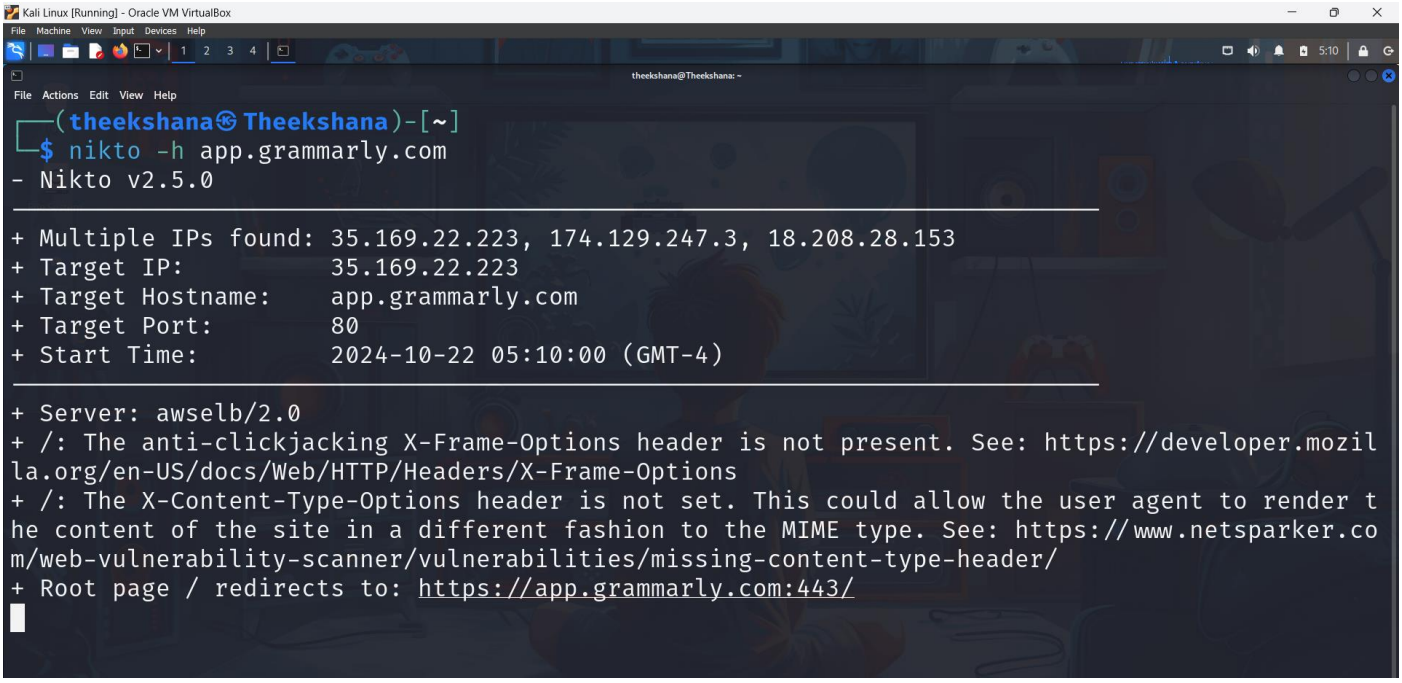
By scanning app.grammarly.com with Nmap I found out these information.

Port	State	Service
21/tcp	Open	FTP
53/tcp	Open	DOMAIN
80/tcp	Open	HTTP
443/tcp	Open	HTPPS

Port	State	Service	Potential Vulnerabilities

21/tcp	Open	FTP	Data is not encrypted, so sensitive information can be stolen. Hackers can guess passwords (brute force attacks) Misconfigurations might allow unauthorized access
53/tcp	Open	DNS	Attackers can redirect users to fake sites (DNS poisoning) Hackers might flood the system (amplification attacks) Sensitive DNS info could be exposed (zone transfer)
80/tcp	Open	HTTP	Data is not secure (no encryption) Hackers can inject harmful scripts (XSS)
443/tcp	Open	HTTPS	If not properly secured, attackers can intercept data Older encryption protocols may be weak

Nikto Scan



The screenshot shows the output of a Nikto scan against the targetapp.grammarly.com, which reveals several potential security issues and misconfigurations.

Vulnerabilities Identified:

- **Missing X-Frame-Options Header**:

  What is X-Frame-Options?: This HTTP header is used to control whether a browser should be allowed to render a page inside an <iframe>. If it's missing, a site is vulnerable to **clickjacking attacks**.

Clickjacking is a type of attack where an attacker tricks a user into clicking on something different from what the user perceives, essentially hijacking the click to perform actions without the user's consent.

How it works: An attacker might embed app.grammarly.com in a hidden <iframe> on their own website. The user would unknowingly interact with the legitimate site, performing actions such as liking or purchasing without realizing it.

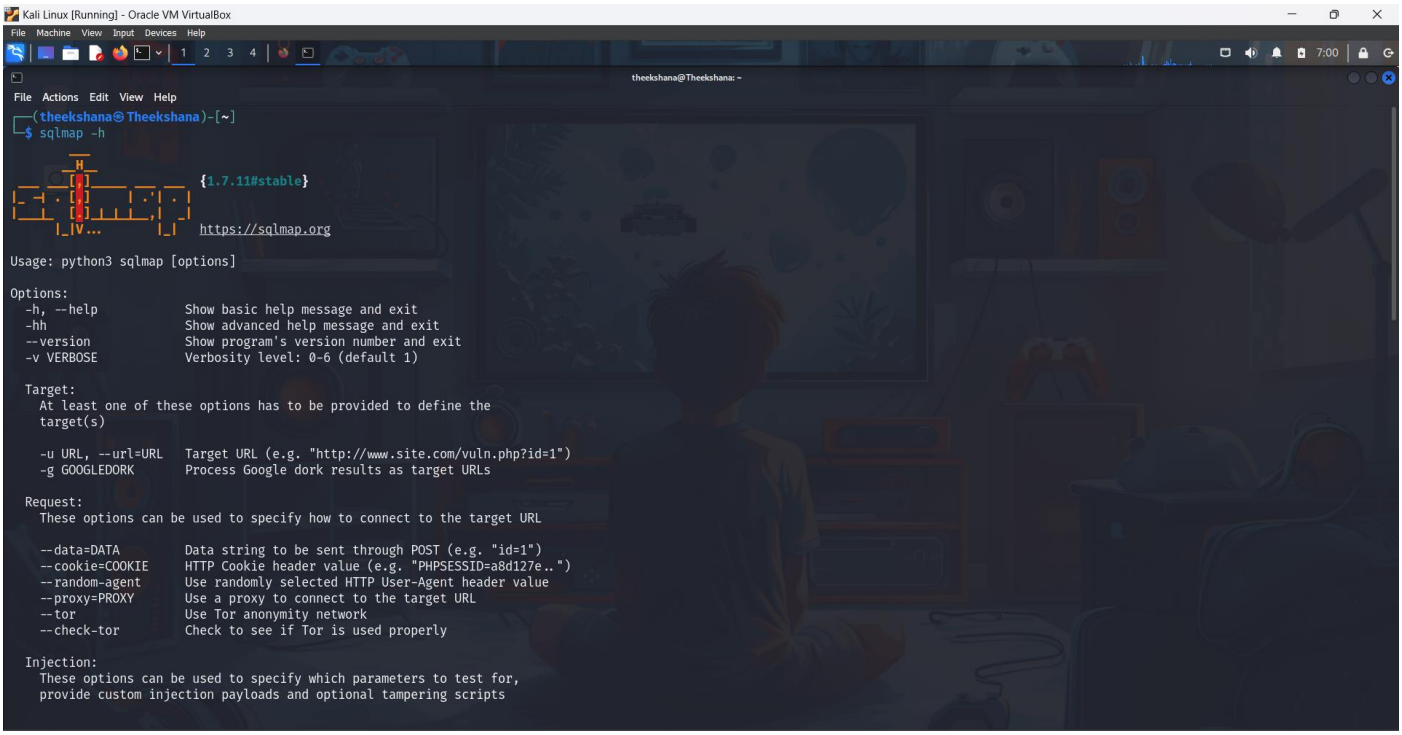
- **Missing X-Content-Type-Options Header**:

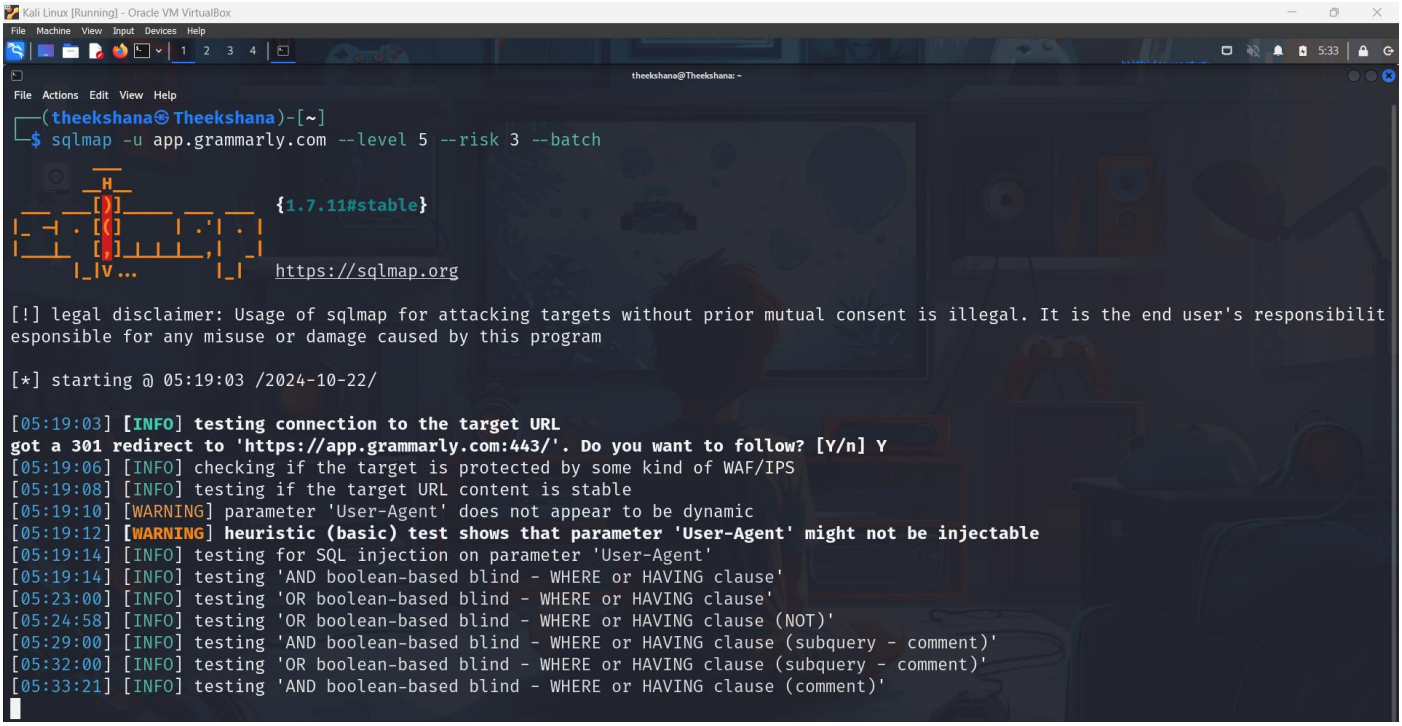
  What is X-Content-Type-Options?: This header prevents browsers from interpreting files as a different MIME type than what is specified. It stops browsers from attempting to "guess" the content type, preventing MIME-type confusion attacks.

  Why is it important?: If an attacker can upload or trick the server into serving a file with a manipulated MIME type, it could be executed as a script or interpreted differently than intended.

  Example attack: An uploaded file like an image could be misinterpreted as executable JavaScript by the browser. This might allow the attacker to execute a cross-site scripting (XSS) attack.

SQLmap Scaner

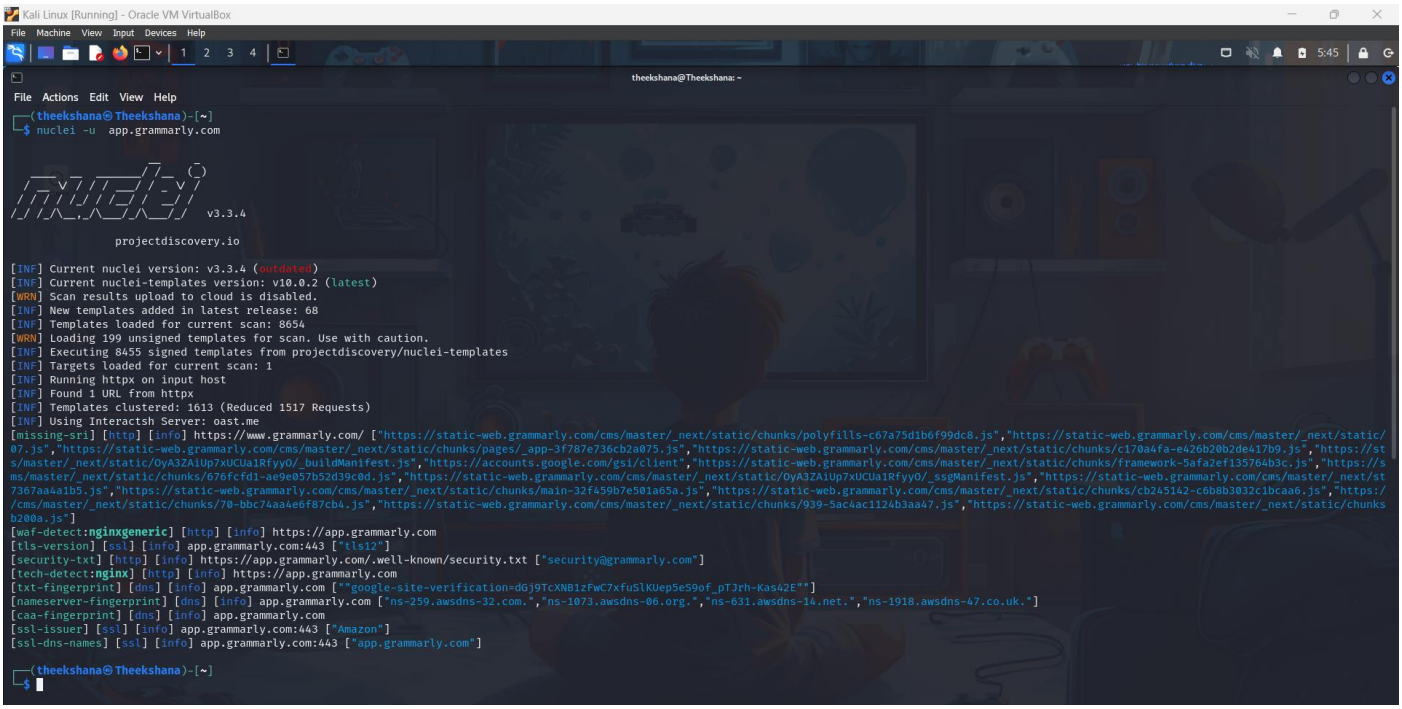




Vulnerabilities Detected:

1. Boolean-based Blind SQL Injection
2. WHERE or HAVING Clause SQL Injection
3. Subquery-based Injection

Nuclei Scan



Missing SRI on Static Resources:

This can allow attackers to inject malicious scripts into the JavaScript files if the integrity of these files is compromised. Adding SRI hashes would mitigate this risk.

TLS Version Issues:

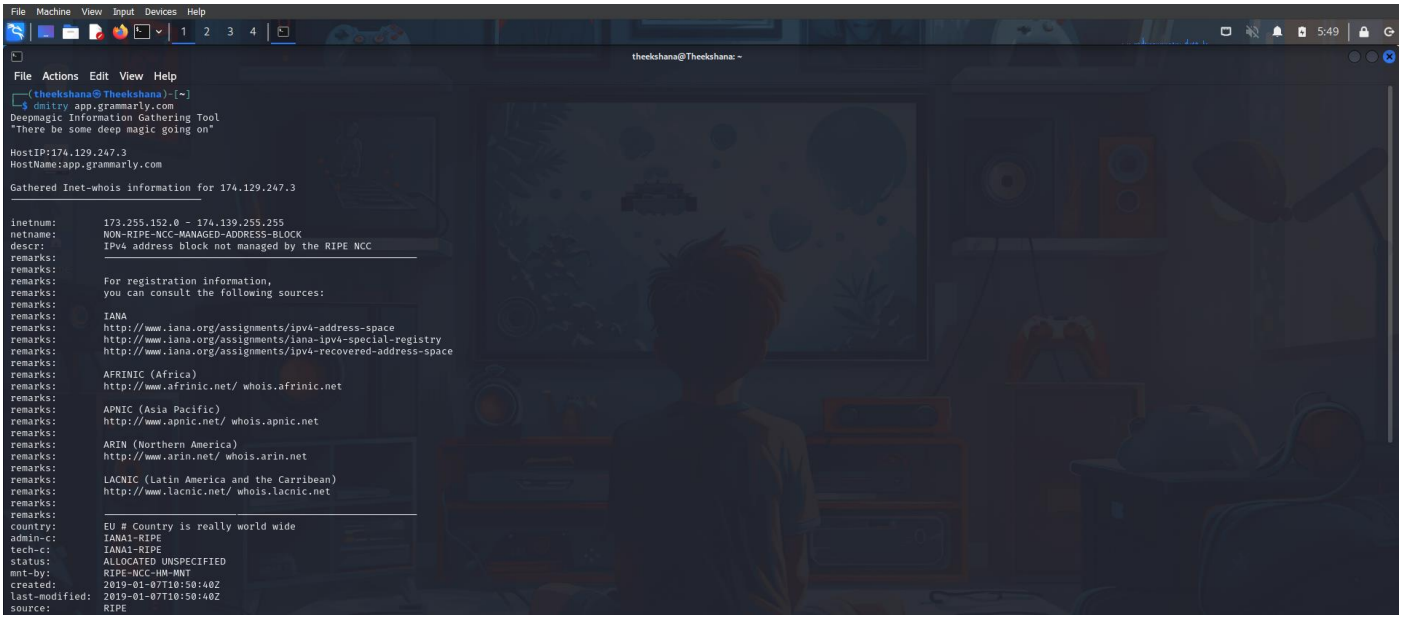
A specific TLS version might be flagged as outdated or insecure, indicating the need for updating to a more secure version.

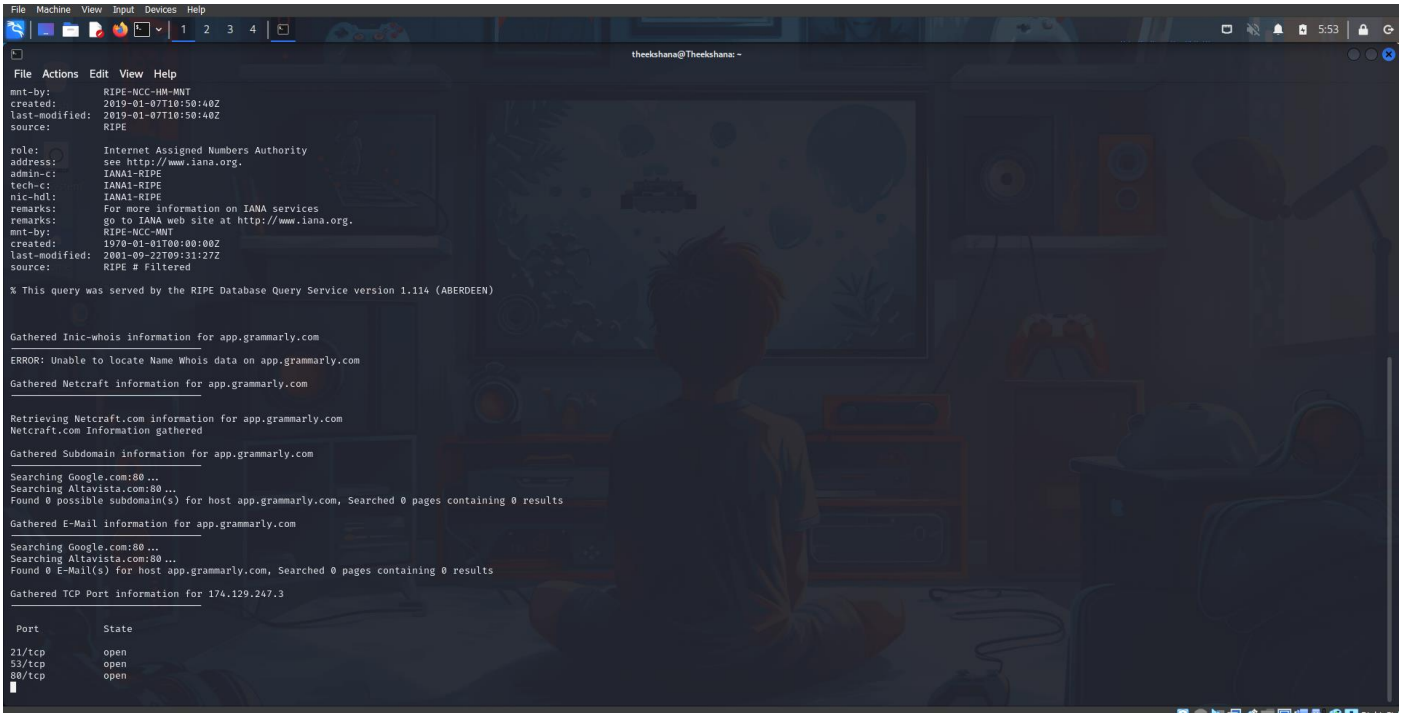
Server and SSL Information:

The scan identifies the technologies used (Nginx server and Amazon-issued SSL certificates), which is useful for mapping the infrastructure.

- **[tls-version]**: The TLS version used by app.grammarly.com:443 is flagged. It could indicate that an outdated or insecure TLS version is being used.
- **[security-txt]**: This refers to the security.txt file, a standard for websites to provide security contact information. Here, the security contact is security@grammarly.com.
- **[tech-detect: nginx]**: Nginx was detected as the web server technology for app.grammarly.com.
- **[ssl-fingerprint]**: Shows that a particular SSL fingerprint was detected for the domain.
- **[nameserver-fingerprint]**: Displays fingerprint data related to the domain's nameservers. It shows that app.grammarly.com uses AWS nameservers (awsdns), specifically from various geographical locations like the US and UK.

Dmitry Scan





Port 21 (FTP - File Transfer Protocol): This port is typically used for file transfer services. Having FTP open can be risky if not properly secured, as it often transmits data in plain text (though secure variants like SFTP exist).

Port 53 (DNS - Domain Name System): This port is used for DNS services, which translate domain names into IP addresses. While DNS services need to be accessible, misconfigurations or vulnerabilities (like DNS amplification attacks) can expose the server to risks.

Port 80 (HTTP - Hypertext Transfer Protocol): This port is used for unencrypted web traffic. Port 80 being open suggests that the website is accessible via HTTP, but this should be redirected to HTTPS (Port 443) for encrypted communication. If not, it leaves the site vulnerable to man-in-the middle (MITM) attacks.

Netsparker

netsparker — Detailed Scan Report

http://app.grammarly.com/

Scan Time : 10/22/2024 3:25:13 PM (UTC+05:30)

Total Requests: 562
Average Speed: 7.8r/s

Risk Level: MEDIUM

VULNERABILITIES

12	3	0	0	2	2	4	4
IDENTIFIED	CONFIRMED	CRITICAL	HIGH	MEDIUM	LOW	BEST PRACTICE	INFORMATION

Identified Vulnerabilities

Critical	0
High	0
Medium	2
Low	2
Best Practice	4
Information	4
TOTAL	12

Confirmed Vulnerabilities

Critical	0
High	0
Medium	1
Low	2
Best Practice	0
Information	0
TOTAL	3

Vulnerability Summary

SEVERITY FILTER : CRITICAL HIGH MEDIUM LOW BEST PRACTICE INFORMATION

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://app.grammarly.com/	
	Weak Ciphers Enabled	GET	https://app.grammarly.com/	
	Cookie Not Marked as HttpOnly	GET	https://app.grammarly.com/	
	Cookie Not Marked as Secure	GET	https://app.grammarly.com/	
	Expect-CT Not Enabled	GET	https://app.grammarly.com/	
	Missing X-XSS-Protection Header	GET	https://app.grammarly.com/.well-known/apple-app-site-association	
	SameSite Cookie Not Implemented	GET	https://app.grammarly.com/	
	Subresource Integrity (SRI) Not Implemented	GET	https://app.grammarly.com/not-found	
	Apple's App-Site Association (AASA) Detected	GET	https://app.grammarly.com/.well-known/apple-app-site-association	
	Email Address Disclosure	GET	https://app.grammarly.com/not-found	
	Generic Email Address Disclosure	GET	https://app.grammarly.com/not-found	
	Nginx Web Server Identified	GET	https://app.grammarly.com/	

Weak Ciphers Enabled

MEDIUM 1 CONFIRMED 1

Netsparker detected that weak ciphers are enabled during secure communication (SSL).

You should allow only strong ciphers on your web server to protect secure communication with your visitors.

Impact

Attackers might decrypt SSL traffic between your server and your visitors.

Vulnerabilities

2.1. https://app.grammarly.com/ CONFIRMED

Hide Remediation

Actions to Take

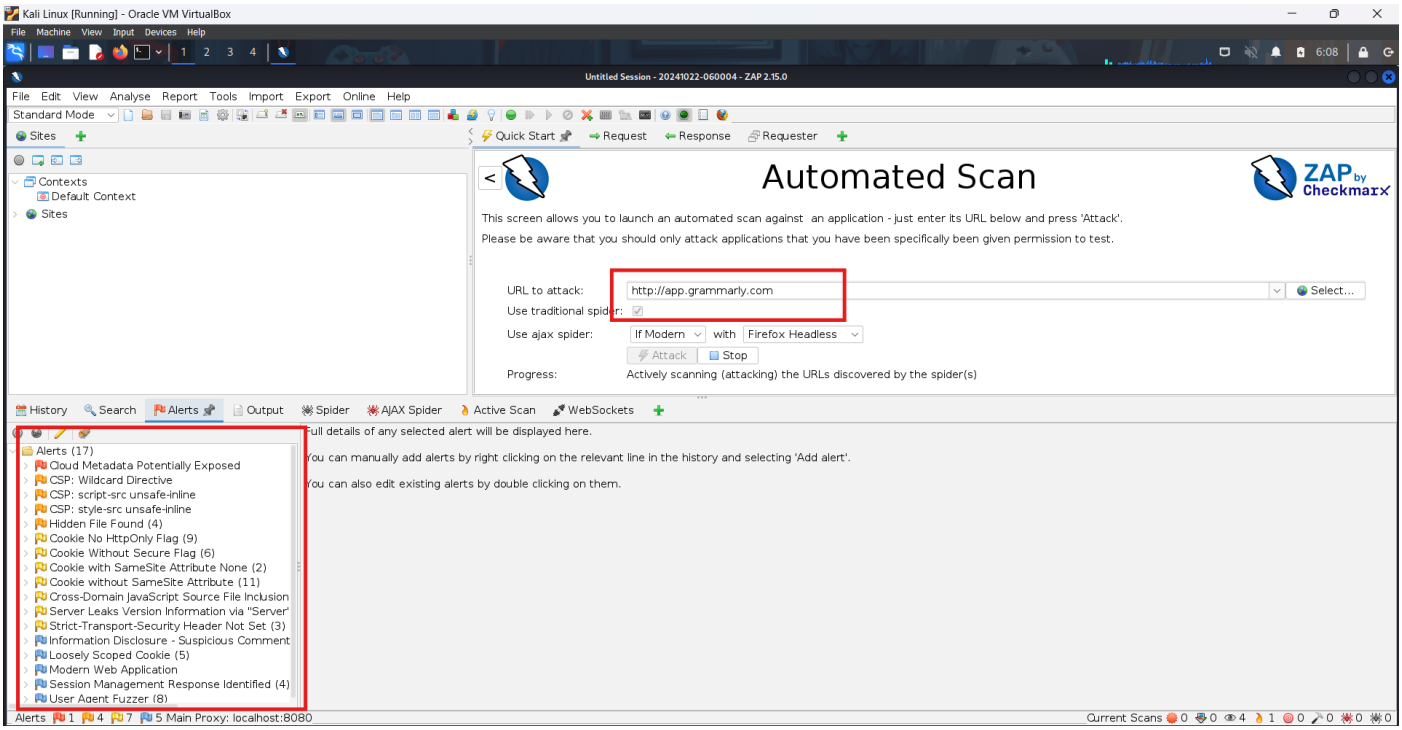
1. For Apache, you should modify the SSLCipherSuite directive in the `httpd.conf`.

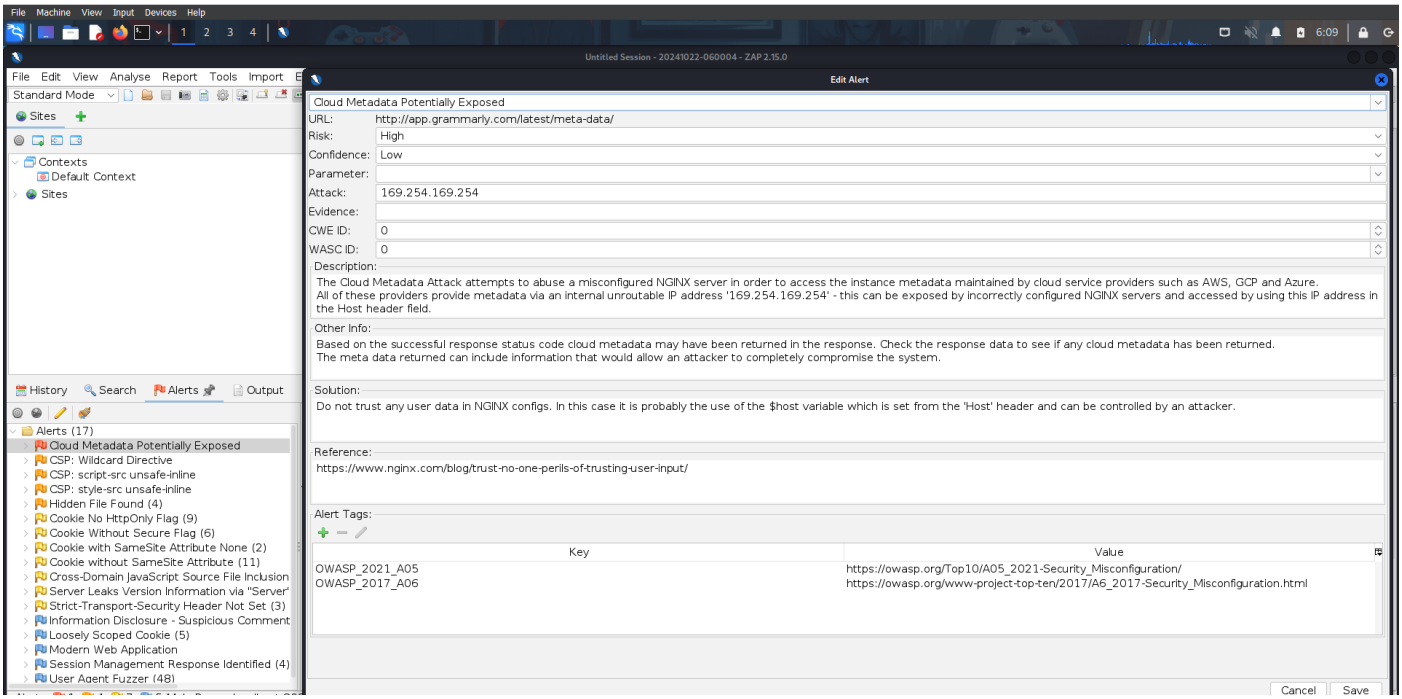
```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

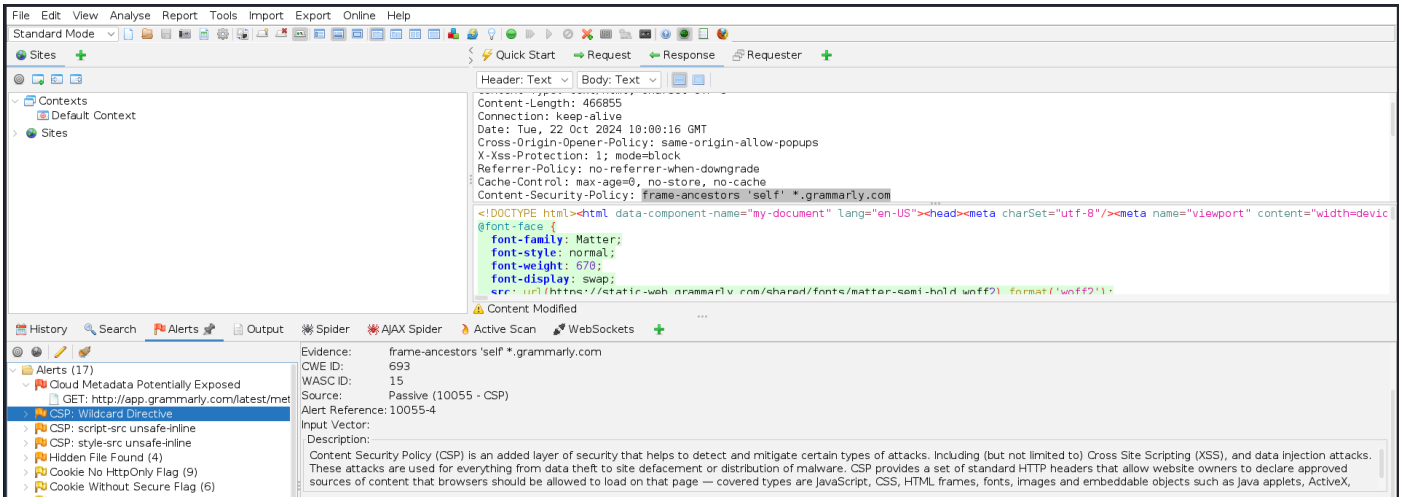
CLASSIFICATION

PCI DSS v3.2	6.5.4
OWASP 2013	A6

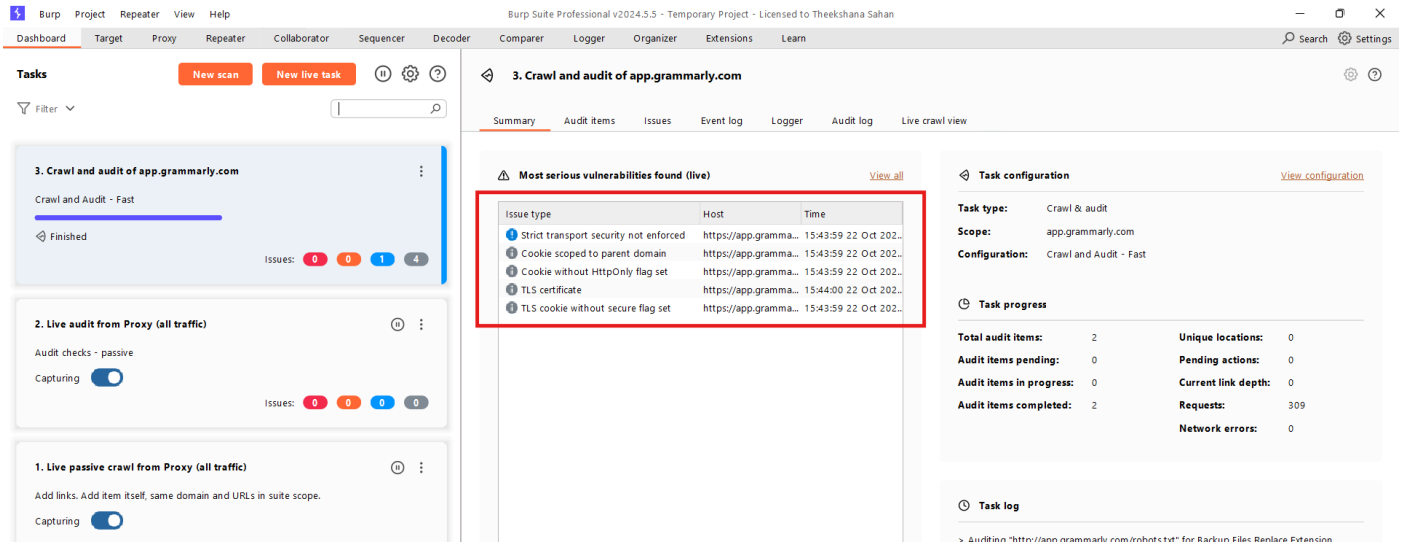
OWASP ZAP

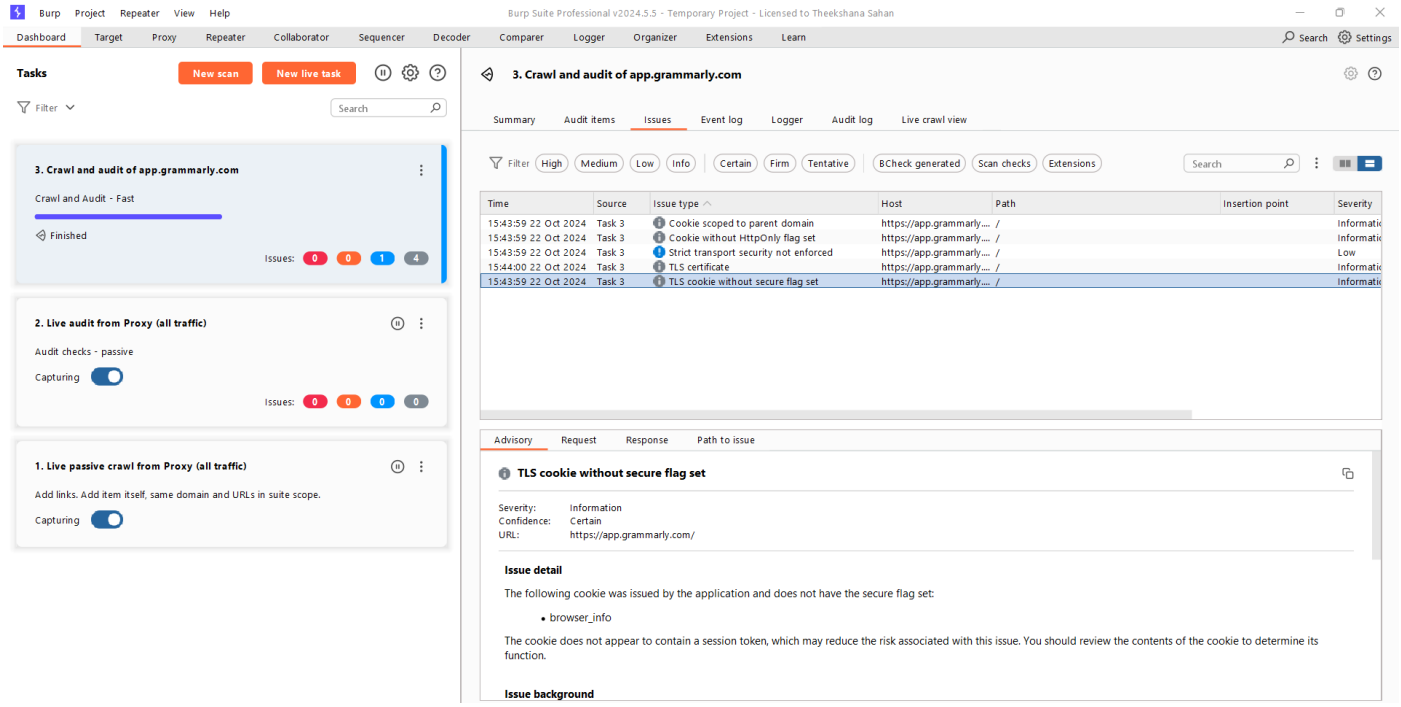

Kali Linux [Running] - Oracle VM VirtualBox
Untitled Session - 20241022-060004 - ZAP 2.15.0
Automated Scan
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack: http://app.grammarly.com
Use traditional spider:
Use ajax spider: If Modern with Firefox Headless
Attack
Stop
Progress: Actively scanning (attacking) the URLs discovered by the spider(s)
Alerts (17)
Cloud Metadata Potentially Exposed
CSP: Wildcard Directive
CSP: script-src unsafe-inline
CSP: style-src unsafe-inline
Hidden File Found (4)
Cookie No HttpOnly Flag (9)
Cookie Without Secure Flag (6)
Cookie with SameSite Attribute None (2)
Cookie without SameSite Attribute (11)
Cross-Domain JavaScript Source File Inclusion
Server Leaks Version Information via "Server"
Strict-Transport-Security Header Not Set (3)
Information Disclosure - Suspicious Comment
Loosely Scoped Cookie (5)
Modern Web Application
Session Management Response Identified (4)
User Agent Fuzzer (8)

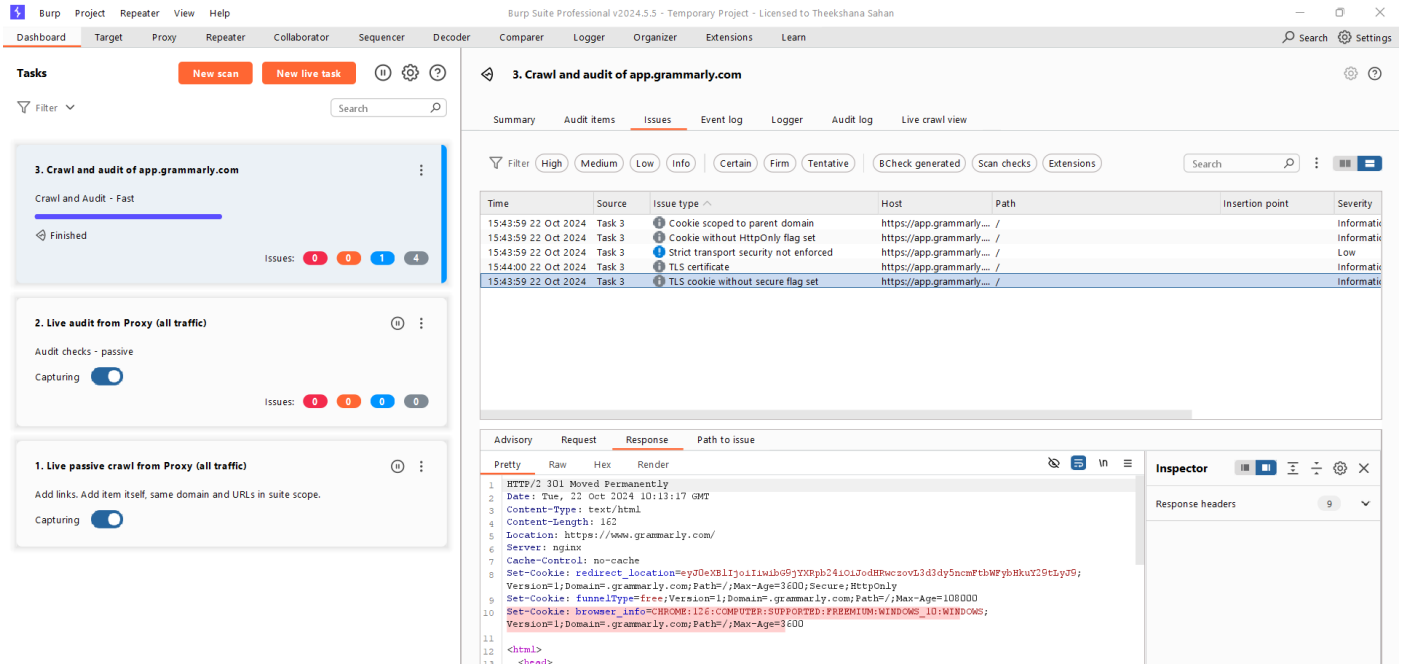

Edit Alert
Cloud Metadata Potentially Exposed
URL: http://app.grammarly.com/latest/meta-data/
Risk: High
Confidence: Low
Parameter:
Attack: 169.254.169.254
Evidence:
CWE ID: 0
WASC ID: 0
Description:
The Cloud Metadata Attack attempts to abuse a misconfigured NGINX server in order to access the instance metadata maintained by cloud service providers such as AWS, GCP and Azure.
All of these providers provide metadata via an internal unroutable IP address '169.254.169.254' - this can be exposed by incorrectly configured NGINX servers and accessed by using this IP address in the Host header field.
Other Info:
Based on the successful response status code cloud metadata may have been returned in the response. Check the response data to see if any cloud metadata has been returned.
The meta data returned can include information that would allow an attacker to completely compromise the system.
Solution:
Do not trust any user data in NGINX configs. In this case it is probably the use of the $host variable which is set from the 'Host' header and can be controlled by an attacker.
Reference:
https://www.nginx.com/blog/trust-no-one-perils-of-trusting-user-input/
Alert Tags:
Key
Value
OWASP_2021_A05
https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
OWASP_2017_A06
https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html
Cancel
Save


Content-Length: 466855
Connection: keep-alive
Date: Tue, 22 Oct 2024 10:00:16 GMT
Cross-Origin-Opener-Policy: same-origin-allow-popups
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade
Cache-Control: max-age=0, no-store, no-cache
Content-Security-Policy: frame-ancestors 'self' *.grammarly.com
Content Modified
Evidence: frame-ancestors 'self' *.grammarly.com
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, ActiveX,

Burp Suite


Burp Project Repeater View Help
Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan
Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Tasks
New scan
New live task
3. Crawl and audit of app.grammarly.com
Crawl and Audit - Fast
Finished
Issues: 0 0 1 4
2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing
Issues: 0 0 0 0
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing
3. Crawl and audit of app.grammarly.com
Summary Audit items Issues Event log Logger Audit log Live crawl view
Most serious vulnerabilities found (live)
View all
Issue type Host Time
Strict transport security not enforced https://app.gramma... 15:43:59 22 Oct 202...
Cookie scoped to parent domain https://app.gramma... 15:43:59 22 Oct 202...
Cookie without HttpOnly flag set https://app.gramma... 15:43:59 22 Oct 202...
TLS certificate https://app.gramma... 15:44:00 22 Oct 202...
TLS cookie without secure flag set https://app.gramma... 15:43:59 22 Oct 202...
Task configuration
View configuration
Task type: Crawl & audit
Scope: app.grammarly.com
Configuration: Crawl and Audit - Fast
Task progress
Total audit items: 2
Audit items pending: 0
Audit items in progress: 0
Audit items completed: 2
Unique locations: 0
Pending actions: 0
Current link depth: 0
Requests: 309
Network errors: 0
Task log


Burp Project Repeater View Help
Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan
Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Tasks
New scan
New live task
3. Crawl and audit of app.grammarly.com
Crawl and Audit - Fast
Finished
Issues: 0 0 1 4
2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing
Issues: 0 0 0 0
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing
3. Crawl and audit of app.grammarly.com
Summary Audit items Issues Event log Logger Audit log Live crawl view
Filter High Medium Low Info Certain Firm Tentative BCheck generated Scan checks Extensions
Search
Time Source Issue type Host Path Insertion point Severity
15:43:59 22 Oct 2024 Task 3 Cookie scoped to parent domain https://app.grammarly.... / Informatio
15:43:59 22 Oct 2024 Task 3 Cookie without HttpOnly flag set https://app.grammarly.... / Informatio
15:43:59 22 Oct 2024 Task 3 Strict transport security not enforced https://app.grammarly.... / Low
15:44:00 22 Oct 2024 Task 3 TLS certificate https://app.grammarly.... / Informatio
15:43:59 22 Oct 2024 Task 3 TLS cookie without secure flag set https://app.grammarly.... / Informatio
Advisory Request Response Path to issue
TLS cookie without secure flag set
Severity: Information
Confidence: Certain
URL: https://app.grammarly.com/
Issue detail
The following cookie was issued by the application and does not have the secure flag set:
browser_info
The cookie does not appear to contain a session token, which may reduce the risk associated with this issue. You should review the contents of the cookie to determine its function.
Issue background


Burp Project Repeater View Help
Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan
Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Tasks
New scan
New live task
3. Crawl and audit of app.grammarly.com
Crawl and Audit - Fast
Finished
Issues: 0 0 1 4
2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing
Issues: 0 0 0 0
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing
3. Crawl and audit of app.grammarly.com
Summary Audit items Issues Event log Logger Audit log Live crawl view
Filter High Medium Low Info Certain Firm Tentative BCheck generated Scan checks Extensions
Search
Time Source Issue type Host Path Insertion point Severity
15:43:59 22 Oct 2024 Task 3 Cookie scoped to parent domain https://app.grammarly.... / Informatio
15:43:59 22 Oct 2024 Task 3 Cookie without HttpOnly flag set https://app.grammarly.... / Informatio
15:43:59 22 Oct 2024 Task 3 Strict transport security not enforced https://app.grammarly.... / Low
15:44:00 22 Oct 2024 Task 3 TLS certificate https://app.grammarly.... / Informatio
15:43:59 22 Oct 2024 Task 3 TLS cookie without secure flag set https://app.grammarly.... / Informatio
Advisory Request Response Path to issue
Pretty Raw Hex Render
HTTP/2 301 Moved Permanently
Date: Tue, 22 Oct 2024 10:13:17 GMT
Content-Type: text/html
Content-Length: 162
Location: https://www.grammarly.com/
Server: nginx
Cache-Control: no-cache
Set-Cookie: redirect_location=eyJ0eXBlIjoiIiwibG9jYXRpb24iOiJodHRwczovL3d3dy5ncmFtbWFybHkuY29tLyJ9;
Version=1;Domain=.grammarly.com;Path=/;Max-Age=3600;Secure;HttpOnly
Set-Cookie: funnelType=free;Version=1;Domain=.grammarly.com;Path=/;Max-Age=108000
Set-Cookie: browser_info=CHROME:126:COMPUTER:SUPPORTED:FREEMIUM:WINDOWS_10:WINDOWS;
Version=1;Domain=.grammarly.com;Path=/;Max-Age=3600
<html>
Inspector
Response headers 9

Vulnerabilities:

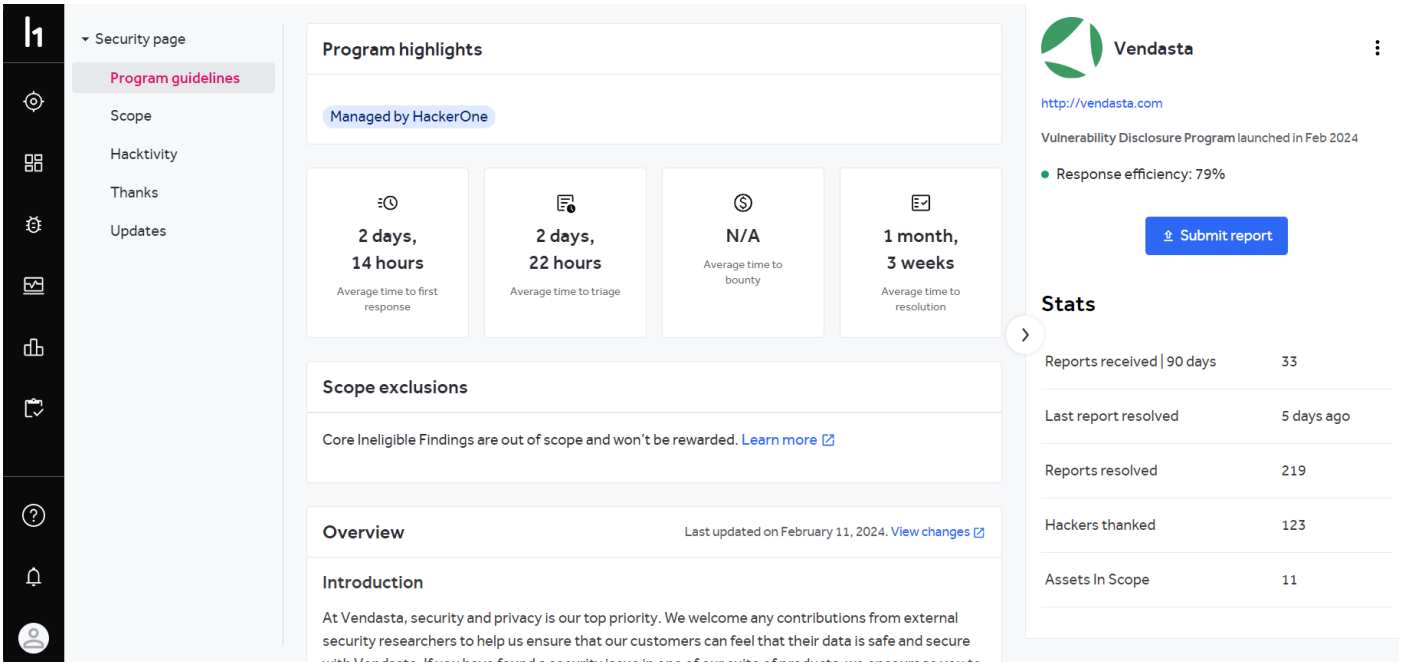
1 Cloud Metadata Potentially Exposed

Vulnerability Title	**Cloud Metadata Potentially Exposed**
Vulnerability Description	The vulnerability allows unauthorized access to cloud instance metadata, which may contain sensitive information such as credentials, API tokens, and service configurations. This can occur when access to metadata services is not properly restricted.
Affected Components	List the specific cloud components or services that are impacted. For instance, it could be specific cloud platforms (AWS, GCP, Azure) or services like EC2 or VM instances. Example: "AWS EC2 Metadata Service, Google Cloud Compute Engine, Azure Virtual Machines."
Impact Assessment	Exploitation of this vulnerability could lead to unauthorized access to cloud instance credentials, allowing attackers to assume privileged roles, escalate privileges, and exfiltrate sensitive data."
Steps to Reproduce	Spin up an EC2 instance on AWS. Access the instance metadata endpoint (http://169.254.169.254/latest/meta-data/) from within the instance. Observe the exposure of sensitive metadata without any authentication.
Proof of Concept	Provide a working example or a code snippet to demonstrate the vulnerability in action. This could be as simple as a curl command. curl http://169.254.169.254/latest/meta-data/
Proposed Mitigation or Fix	Restrict access to the metadata service by implementing IMDSv2 on AWS or using equivalent features in GCP and Azure. Additionally, limit network access to internal metadata services using firewall rules.

2 Cross domain JavaScript source file

Vulnerability Title	Cross domain JavaScript source file
Vulnerability Description	This vulnerability allows external JavaScript files to be included in the application from untrusted or unsafe domains. This can lead to the execution of malicious scripts within the context of the user's browser, potentially leading to data theft, session hijacking, or unauthorized actions.
Affected Components	Frontend web application components, web browsers, and any externally included JavaScript libraries.
Impact Assessment	Exploiting this vulnerability can lead to malicious code execution in users' browsers, data leakage, session hijacking, or potential compromise of user accounts.
Steps to Reproduce	Identify an HTML file that includes external JavaScript sources. Modify the external source to include a malicious JavaScript file. Access the web application and check the network requests to see the inclusion of the malicious script. Observe the execution of the malicious code within the application.
Proof of Concept	Provide a sample payload or code that demonstrates the issue in action. <script src="http://malicious-domain.com/malicious.js"></script>
Proposed Mitigation or Fix	Implement a Content Security Policy (CSP) that restricts external JavaScript files to trusted domains. Consider using Subresource Integrity (SRI) to ensure that externally included JavaScript files have not been tampered with.

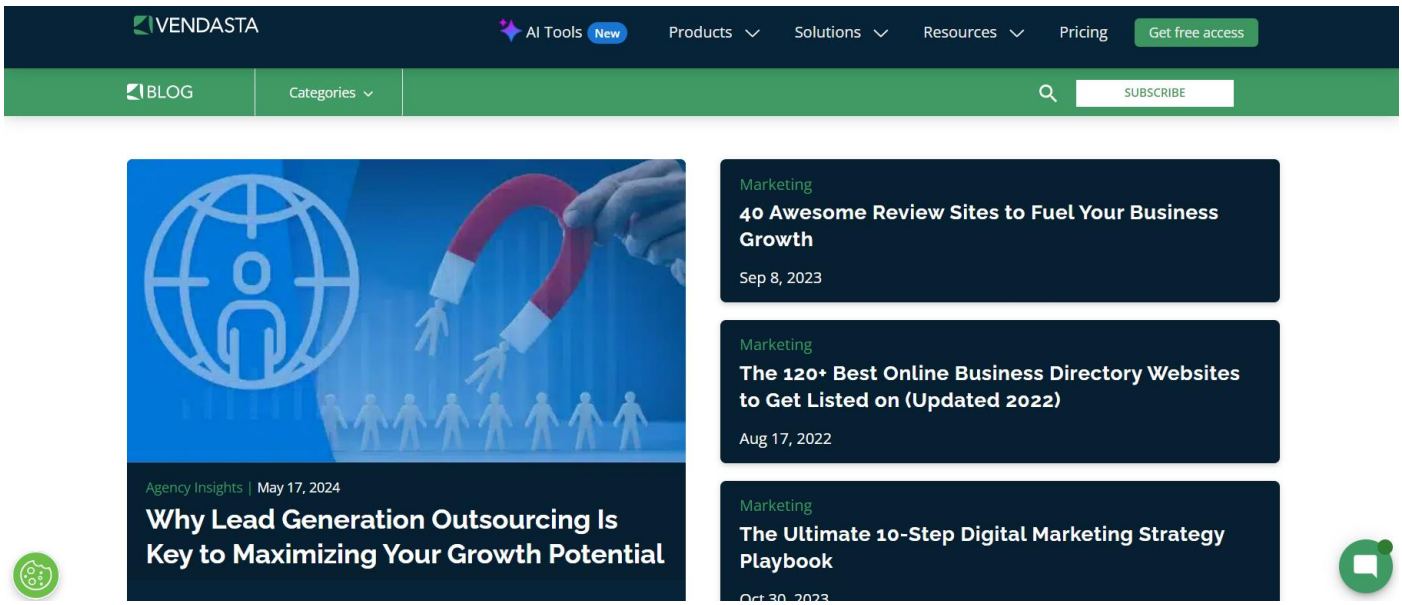
Report 04Target Details



The target for this Bug Bounty report is Vendasta (https://www.vendasta.com), a platform providing digital solutions for businesses, including tools for marketing, sales, and customer management. The company offers a range of services such as digital advertising, reputation management, and APIs for integrating various business functions. Vendasta's platform is designed to help businesses grow by offering scalable and efficient solutions, leveraging modern technologies.

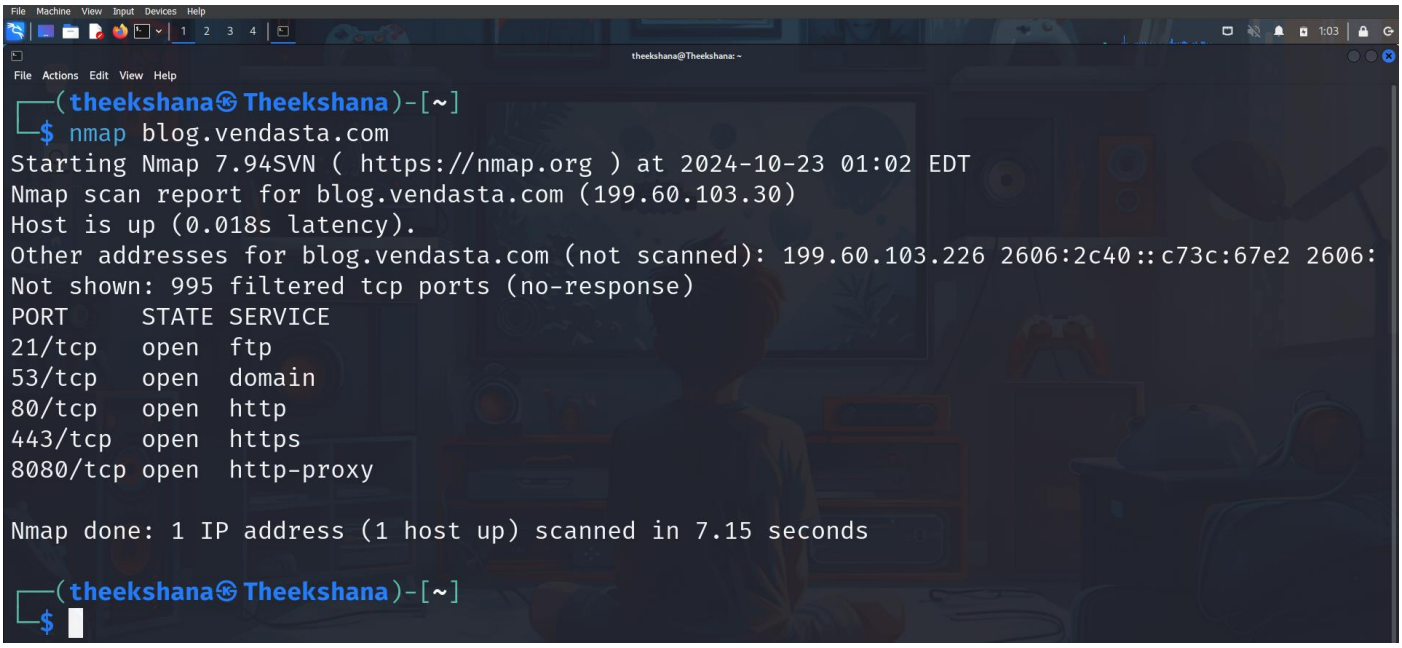
In this report, I have chosen to focus on 10 subdomains under the main domain vendasta.com. Each subdomain may serve different functionalities or services, potentially introducing distinct security risks, particularly in development or user-related areas. These subdomains were selected based on their relevance and the likelihood of containing vulnerabilities.

This report covers the findings for the subdomain: blog.vendasta.com.



Target Reconnaissance

Nmap Scan

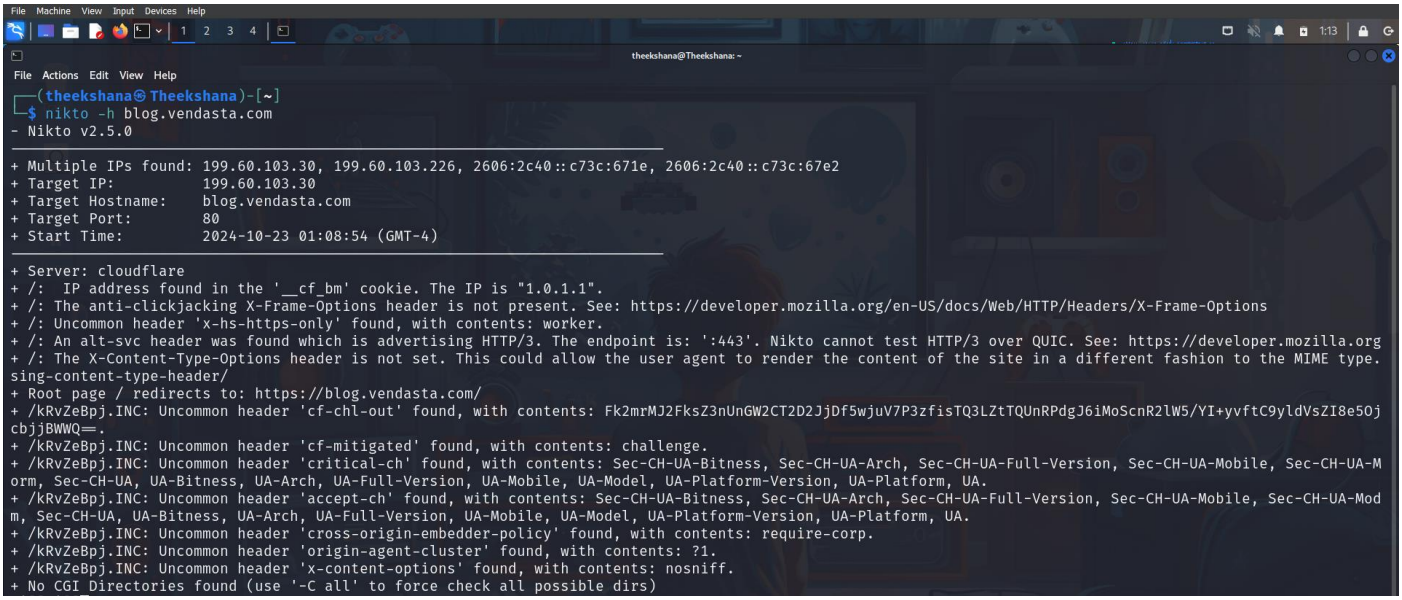


By scanning blog.vendasta.com. with Nmap I found out these information.

Port	State	Service
21/tcp	Open	FTP
53/tcp	Open	DOMAIN
80/tcp	Open	HTTP
443/tcp	Open	HTPPS
8080/tcp	Open	HTTP-PROXY

Port	State	Service	Potential Vulnerabilities
21/tcp	Open	FTP	Data is not encrypted, so sensitive information can be stolen. Hackers can guess passwords (brute force attacks) Misconfigurations might allow unauthorized access
53/tcp	Open	DNS	Attackers can redirect users to fake sites (DNS poisoning) Hackers might flood the system (amplification attacks) Sensitive DNS info could be exposed (zone transfer)
80/tcp	Open	HTTP	Data is not secure (no encryption) Hackers can inject harmful scripts (XSS)
443/tcp	Open	HTTPS	If not properly secured, attackers can intercept data Older encryption protocols may be weak

Nikto Scan



The screenshot shows the output of a Nikto scan against the target blog.vendasta.com., which reveals several potential security issues and misconfigurations.

1. Missing X-Frame-Options Header

- **Issue**: The X-Frame-Options header is not present.
- **Risk**: This header helps prevent clickjacking attacks, where an attacker could trick users into interacting with a page in a way they didn't intend. Without it, the site is vulnerable to being embedded in iframes from malicious sites.

2. Missing X-Content-Type-Options Header

- **Issue**: The X-Content-Type-Options header is missing.
- **Risk**: This can lead to MIME-type sniffing vulnerabilities, where browsers may incorrectly detect the type of content being served, which could expose users to attacks, especially if malicious content is injected.

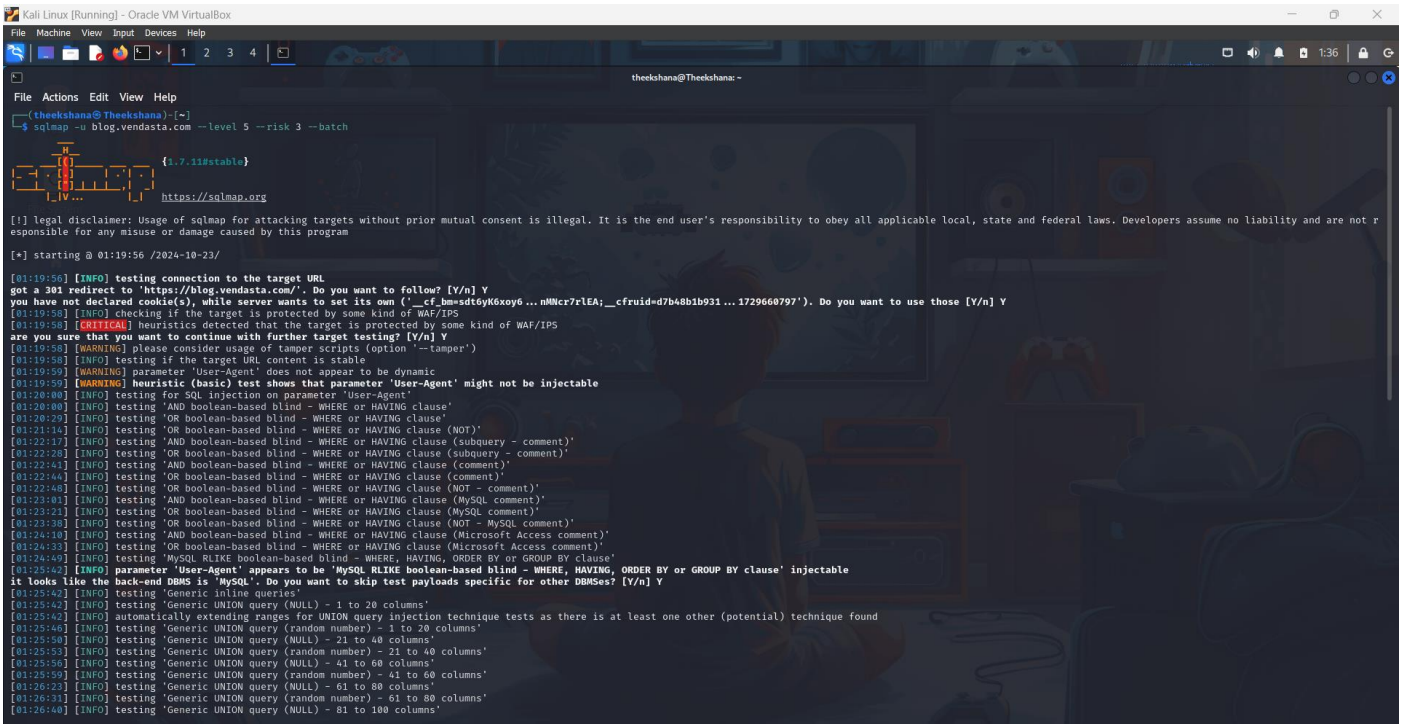
3. Uncommon Headers (Cross-Origin Resource Sharing)

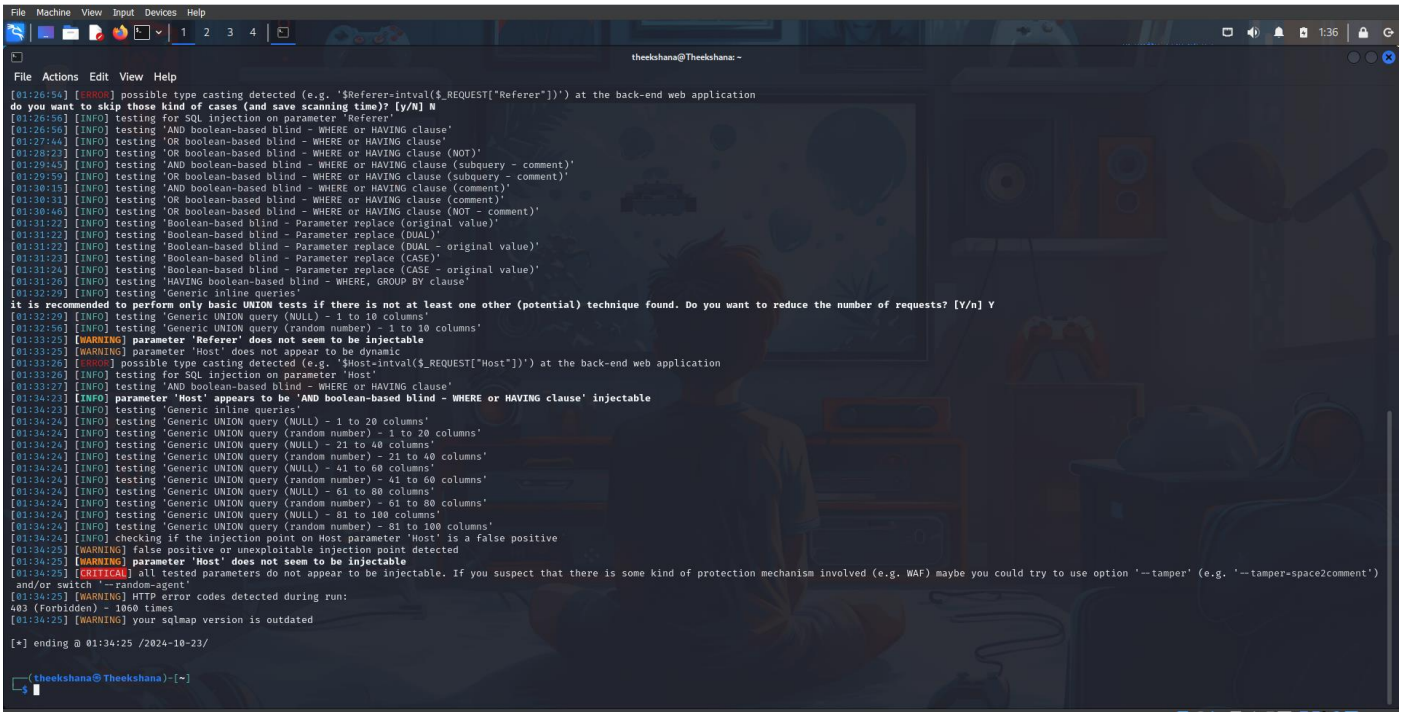
- **Issue**: Uncommon headers such as cross-origin-embedder-policy and origin-agent-cluster were found.
- **Risk**: These headers are typically related to **cross-origin** policies and security mechanisms, but their misconfiguration could expose the site to **cross-origin attacks**.

4. HTTP/3 and QUIC Protocol Testing

- **Issue**: The site advertises support for HTTP/3 via the Alt-Svc header, but Nikto cannot fully test HTTP/3 over QUIC.
- **Risk**: If not properly configured, newer protocols like HTTP/3 may introduce vulnerabilities, especially if there are weaknesses in the implementation or security measures are overlooked.

SQLmap Scaner



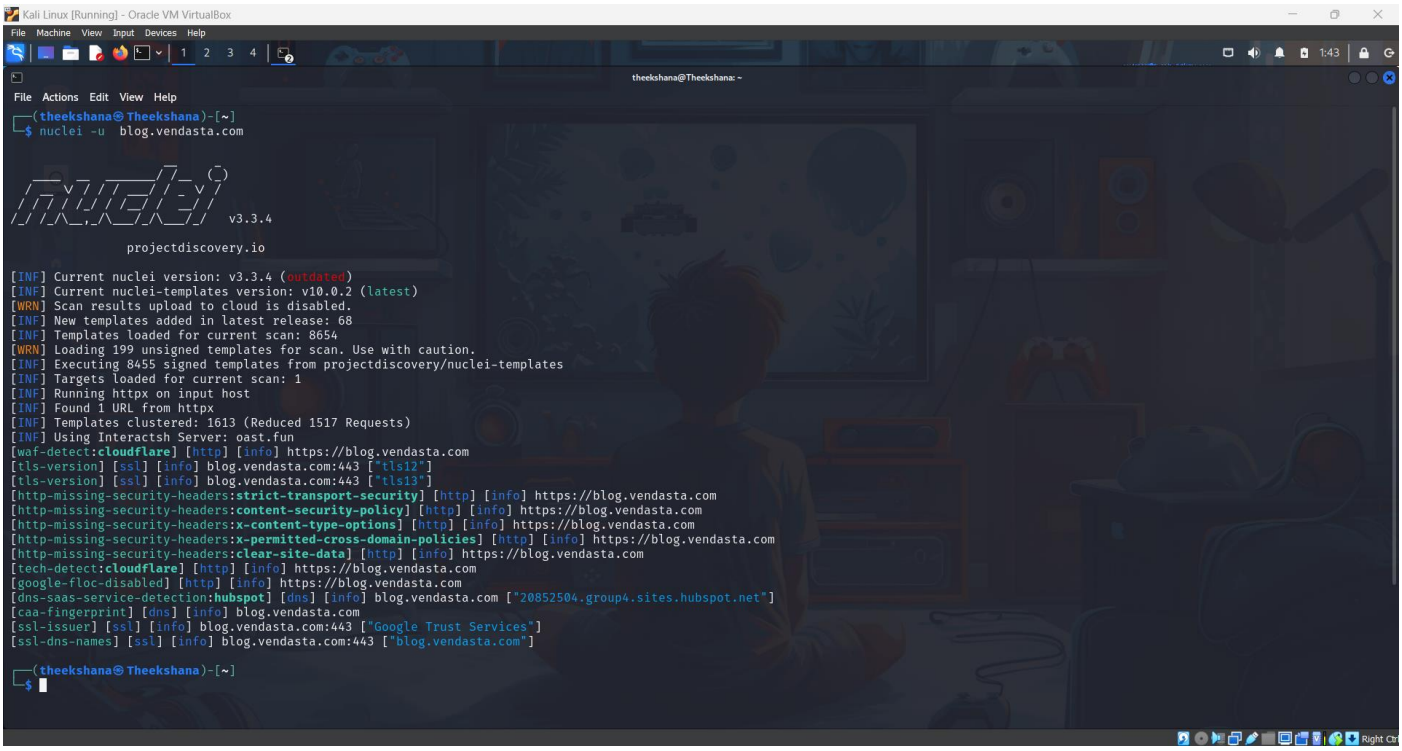


Vulnerabilities Detected:

The scan indicates possible blind SQL injection vulnerabilities in some SQL queries (WHERE, HAVING, ORDER BY). While protections like WAF/IPS are present, these vulnerabilities may still be exploitable with advanced techniques. You should further explore these blind SQL injection vectors to confirm their exploitability.

- WAF/IPS Detection
- Parameter Testing
- SQL Injection

Nuclei Scan



1. Missing Security Headers:

- Strict-Transport-Security (HSTS): This header ensures that browsers only interact with the site using HTTPS. Its absence can make the site vulnerable to SSL stripping attacks.

- Content-Security-Policy (CSP): A CSP header helps mitigate a wide range of attacks such as XSS by specifying which content sources are trusted. Its absence may increase exposure to content injection attacks.

- X-Content-Type-Options: Without this header, browsers may attempt to guess the MIME type, potentially leading to MIME-type confusion attacks.

- X-Permitted-Cross-Domain-Policies: This header governs how cross-domain content is handled. Its absence may allow unrestricted sharing of sensitive content.

- Clear-Site-Data: Missing this header could allow persistent data to remain in the browser, increasing the risk of data leakage.

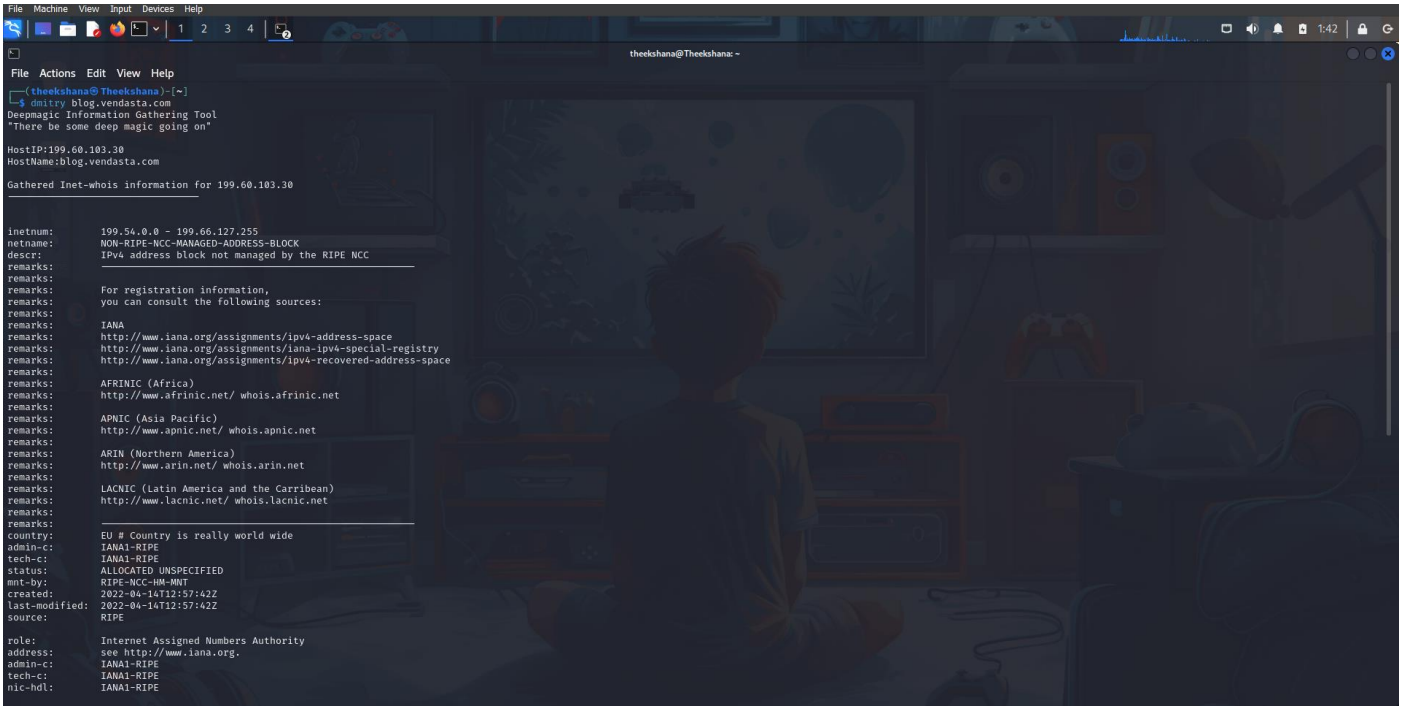
- Cross-Origin Resource Sharing (CORS): Missing or misconfigured CORS headers may allow unauthorized access to resources from different origins.

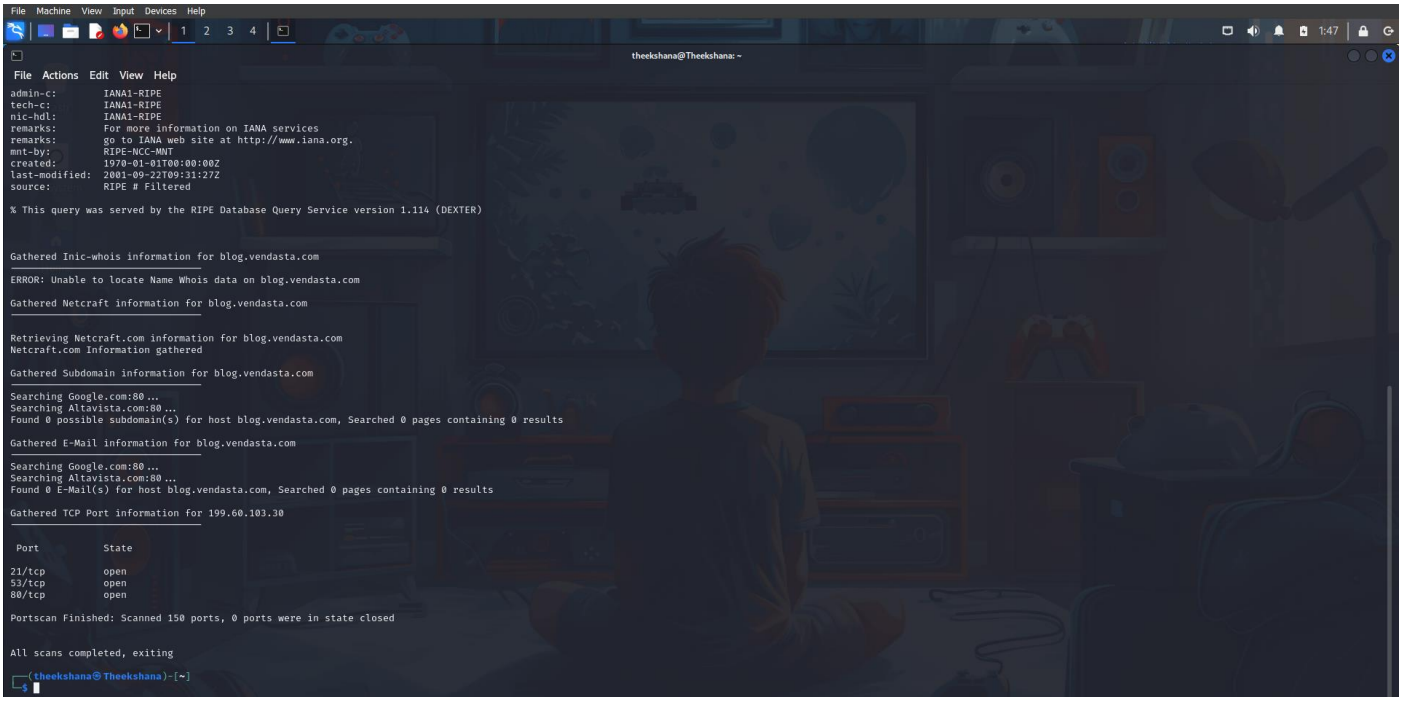
2. Detection of SaaS/Third-Party Service:

- HubSpot :The site appears to be using HubSpot, which may introduce potential risks related to third-party services.

- TLS Versions: The scan lists the supported TLS versions (`tls12`, `tls13`), which are modern and generally secure, indicating good SSL/TLS configuration.

Dmitry Scan





Port 21 (FTP - File Transfer Protocol): This port is typically used for file transfer services. Having FTP open can be risky if not properly secured, as it often transmits data in plain text (though secure variants like SFTP exist).

Port 53 (DNS - Domain Name System): This port is used for DNS services, which translate domain names into IP addresses. While DNS services need to be accessible, misconfigurations or vulnerabilities (like DNS amplification attacks) can expose the server to risks.

Port 80 (HTTP - Hypertext Transfer Protocol): This port is used for unencrypted web traffic. Port 80 being open suggests that the website is accessible via HTTP, but this should be redirected to HTTPS (Port 443) for encrypted communication. If not, it leaves the site vulnerable to man-in-the middle (MITM) attacks.

Netsparker

netsparker — Detailed Scan Report

http://blog.vendasta.com/

Scan Time : 10/23/2024 11:20:53 AM (UTC+05:30)

Total Requests: 1,774
Average Speed: 23.6r/s

Risk Level: MEDIUM

VULNERABILITIES

16	5	0	0	2	3	6	5
IDENTIFIED	CONFIRMED	CRITICAL	HIGH	MEDIUM	LOW	BEST PRACTICE	INFORMATION

Identified Vulnerabilities

Critical	0
High	0
Medium	2
Low	3
Best Practice	6
Information	5
TOTAL	16

Confirmed Vulnerabilities

Critical	0
High	0
Medium	1
Low	2
Best Practice	0
Information	2
TOTAL	5

Vulnerability Summary

SEVERITY FILTER : ☑ CRITICAL ☑ HIGH ☑ MEDIUM ☑ LOW ☑ BEST PRACTICE ☑ INFORMATION

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://blog.vendasta.com/	
	Weak Ciphers Enabled	GET	https://blog.vendasta.com/	
	Missing X-Frame-Options Header	GET	https://blog.vendasta.com/.well-known/	
	Cookie Not Marked as HttpOnly	GET	https://blog.vendasta.com/.well-known/	
	Cookie Not Marked as Secure	GET	https://blog.vendasta.com/.well-known/	
	Content Security Policy (CSP) Not Implemented	GET	http://blog.vendasta.com/%3Cscript%3Ealert(0)%3C/script%3E	
	Expect-CT Not Enabled	GET	https://blog.vendasta.com/	
	Missing X-XSS-Protection Header	GET	https://blog.vendasta.com/sitemap.xml	
	Referrer-Policy Not Implemented	GET	https://blog.vendasta.com/.well-known/	
	SameSite Cookie Not Implemented	GET	http://blog.vendasta.com/	
	Subresource Integrity (SRI) Not Implemented	GET	https://blog.vendasta.com/opensearch.xml?nsextt=%0d%0ans%3anetsparker056650%3dvuln	nsextt
	Missing object-src in CSP Declaration	GET	https://blog.vendasta.com/.well-known/	
	Sitemap Detected	GET	https://blog.vendasta.com/sitemap.xml	

Cookie Not Marked as HttpOnly

LOW 1 CONFIRMED 1

Netsparker identified a cookie not marked as HTTPOnly.

HTTPOnly cookies cannot be read by client-side scripts, therefore marking a cookie as HTTPOnly can provide an additional layer of protection against cross-site scripting attacks.

Impact

During a cross-site scripting attack, an attacker might easily access cookies and hijack the victim's session.

Vulnerabilities

3.1. https://blog.vendasta.com/.well-known/ CONFIRMED

Hide Remediation

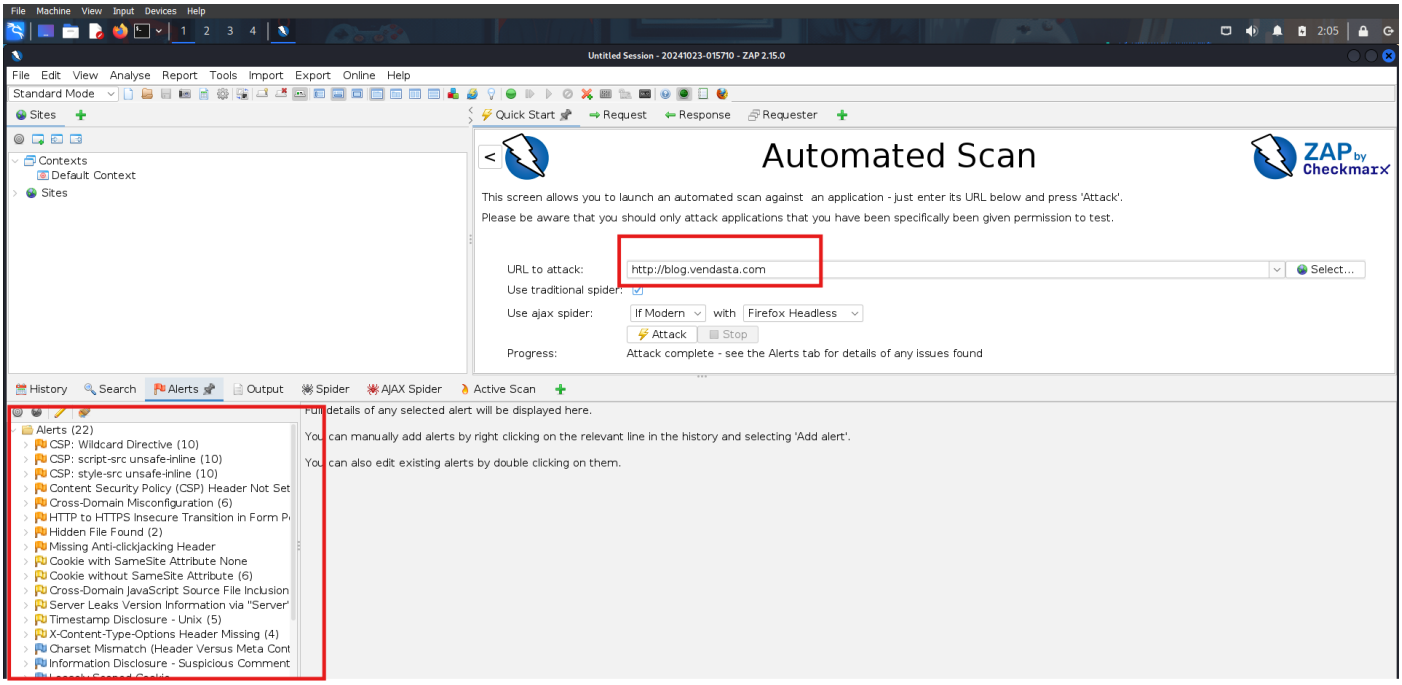
Actions to Take

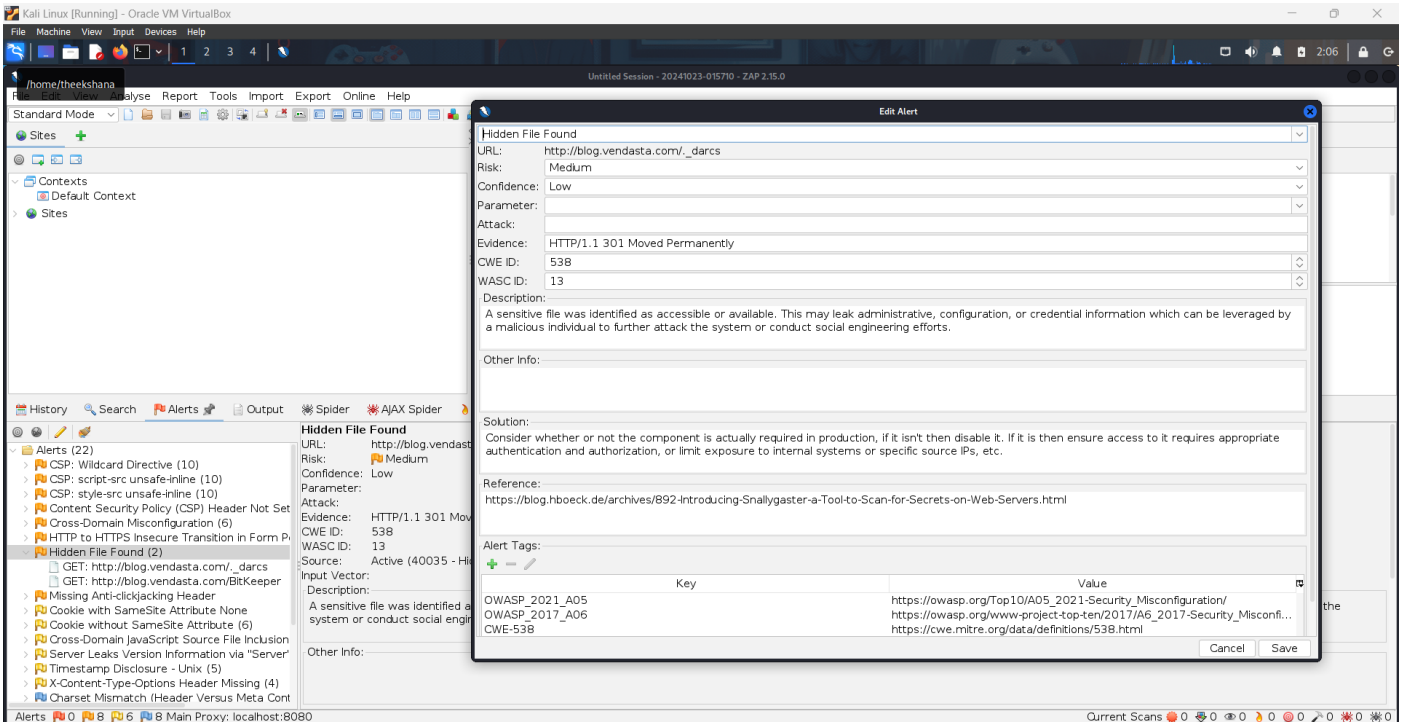
1. See the remedy for solution.
2. Consider marking all of the cookies used by the application as HTTPOnly. (*After these changes javascript code will not be able to read cookies.*)

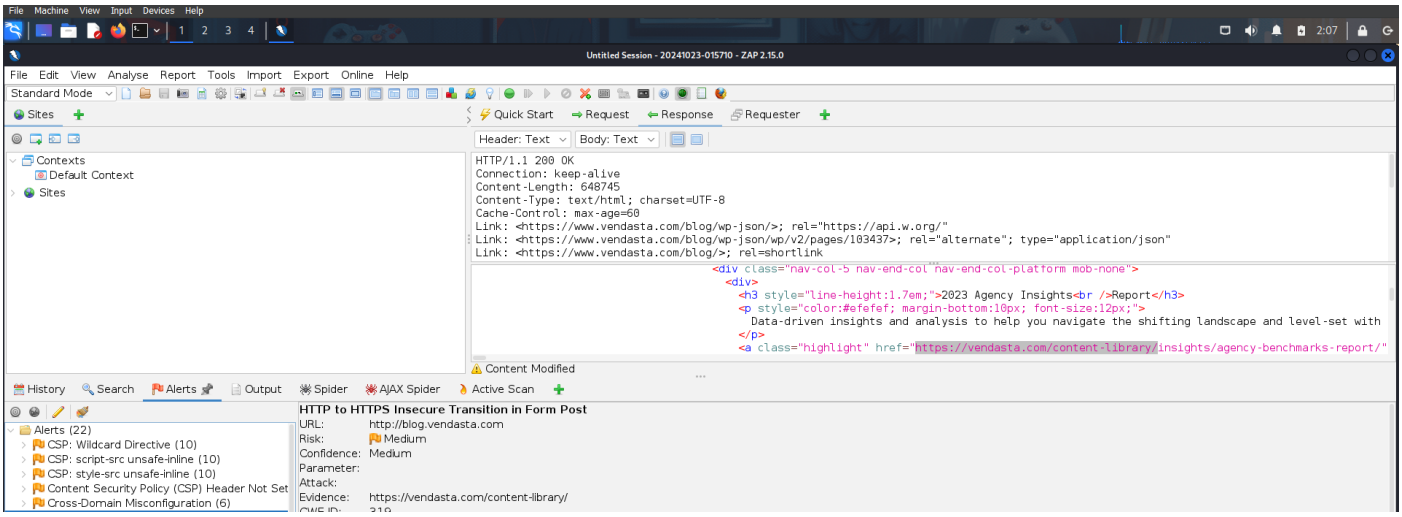
CLASSIFICATION

OWASP 2013	A5

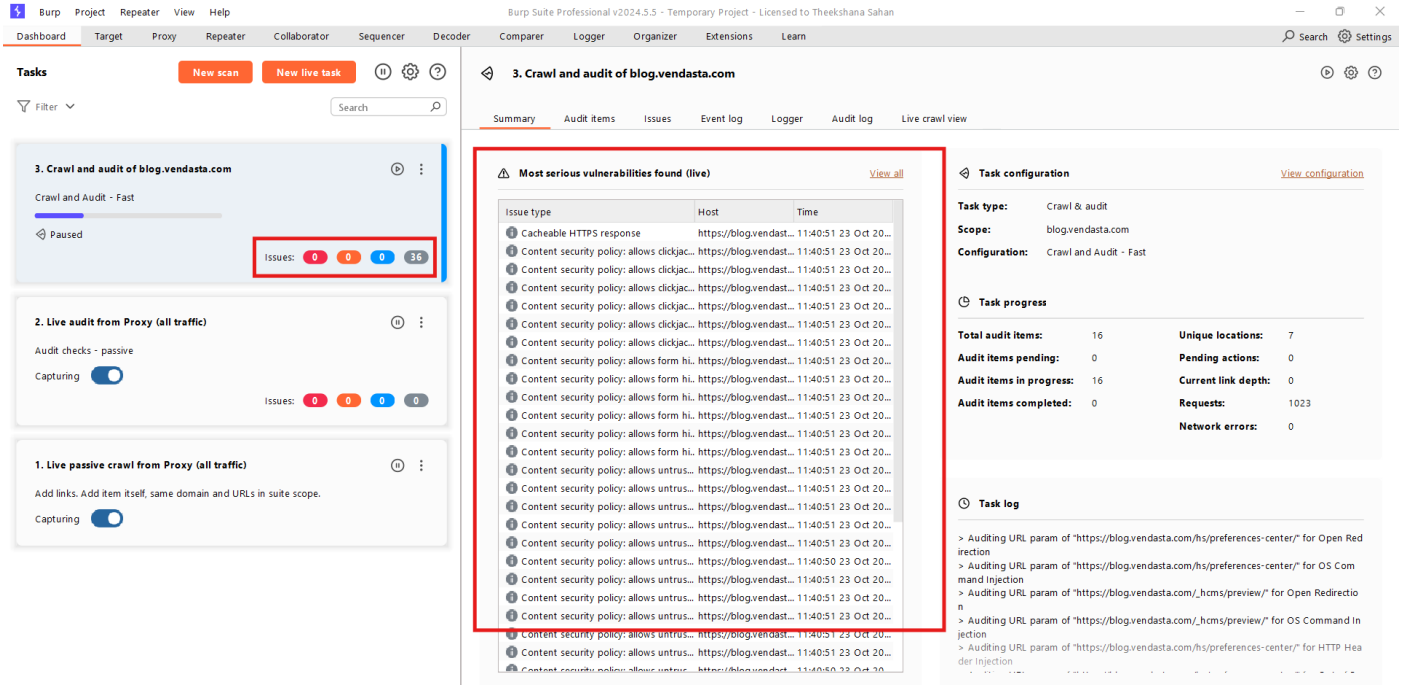
OWASP ZAP

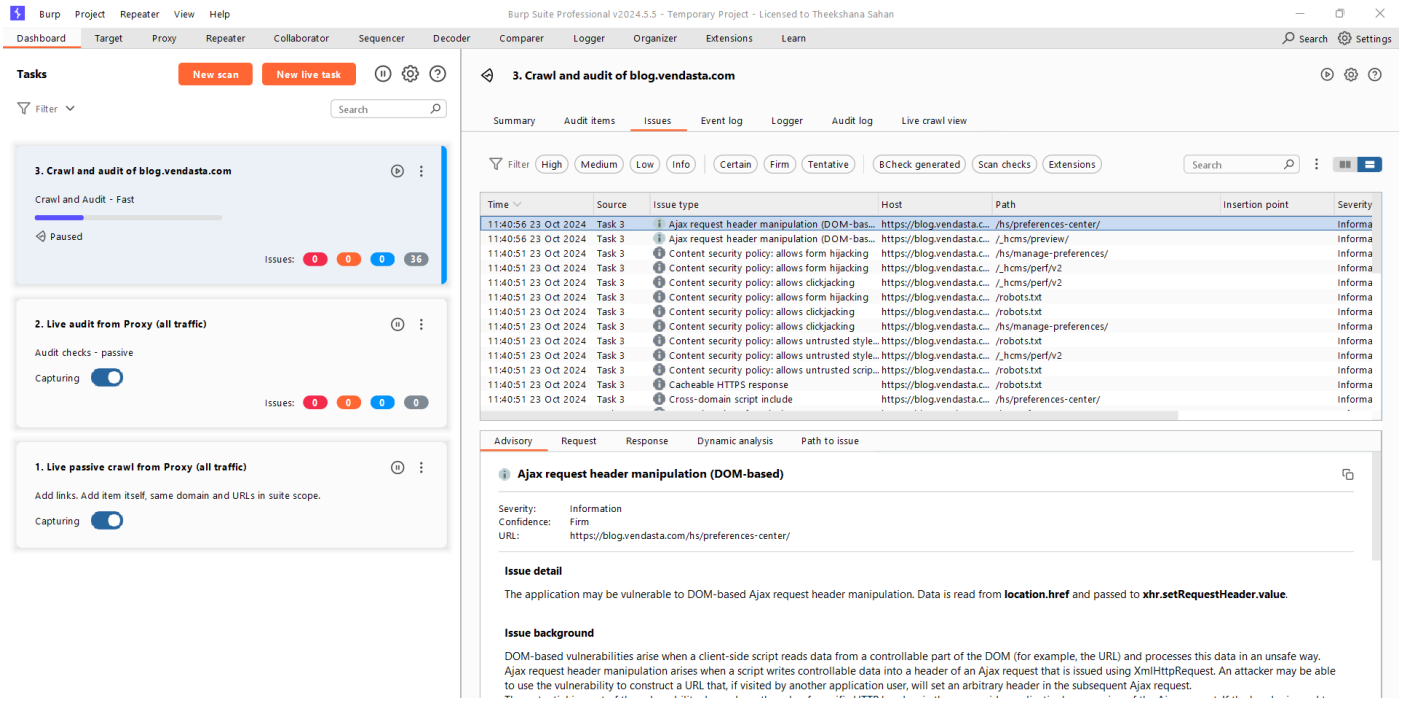

Untitled Session - 20241023-015710 - ZAP 2.15.0
Automated Scan
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack: http://blog.vendasta.com
Use traditional spider:
Use ajax spider: If Modern with Firefox Headless
Attack Stop
Progress: Attack complete - see the Alerts tab for details of any issues found
Alerts (22)
CSP: Wildcard Directive (10)
CSP: script-src unsafe-inline (10)
CSP: style-src unsafe-inline (10)
Content Security Policy (CSP) Header Not Set
Cross-Domain Misconfiguration (6)
HTTP to HTTPS Insecure Transition in Form P
Hidden File Found (2)
Missing Anti-clickjacking Header
Cookie with SameSite Attribute None
Cookie without SameSite Attribute (6)
Cross-Domain JavaScript Source File Inclusion
Server Leaks Version Information via "Server"
Timestamp Disclosure - Unix (5)
X-Content-Type-Options Header Missing (4)
Charset Mismatch (Header Versus Meta Cont
Information Disclosure - Suspicious Comment

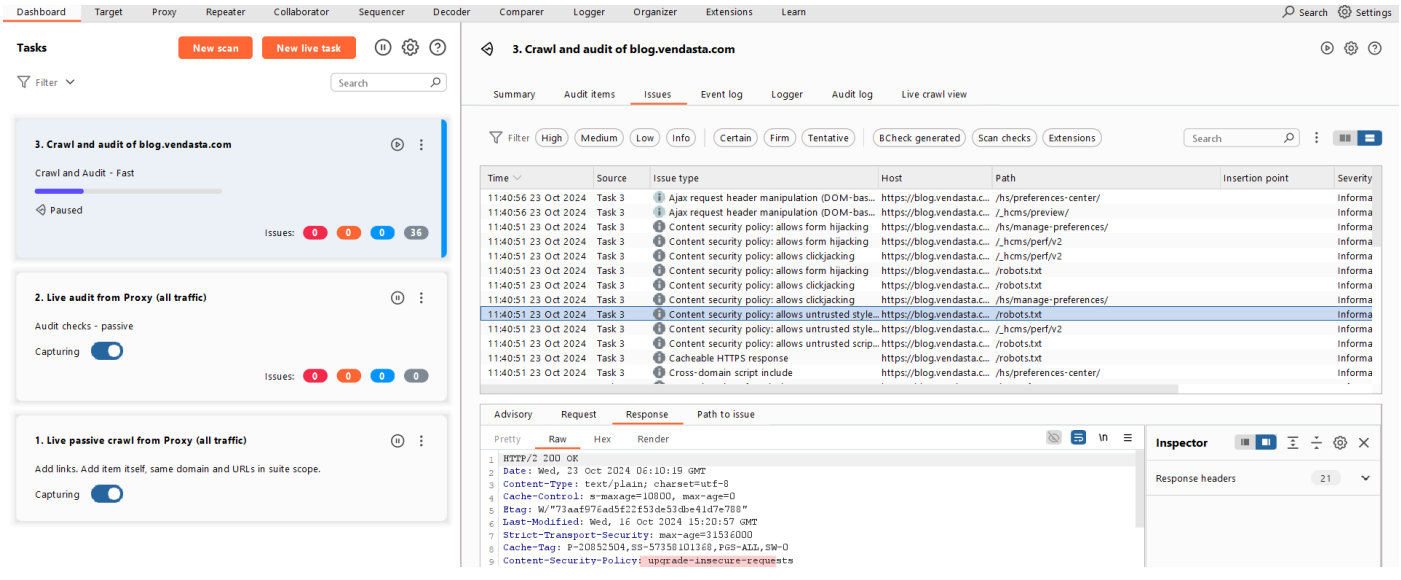

Edit Alert
Hidden File Found
URL: http://blog.vendasta.com/._darcs
Risk: Medium
Confidence: Low
Parameter:
Attack:
Evidence: HTTP/1.1 301 Moved Permanently
CWE ID: 538
WASC ID: 13
Description:
A sensitive file was identified as accessible or available. This may leak administrative, configuration, or 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 exposure to internal systems or specific source IPs, etc.
Reference:
https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html
Alert Tags:
Key
Value
OWASP_2021_A05
https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
OWASP_2017_A06
https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfi...
CWE-538
https://cwe.mitre.org/data/definitions/538.html
Cancel
Save


HTTP/1.1 200 OK
Connection: keep-alive
Content-Length: 648745
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=60
Link: <https://www.vendasta.com/blog/wp-json/>; rel="https://api.w.org/"
Link: <https://www.vendasta.com/blog/wp-json/wp/v2/pages/103437>; rel="alternate"; type="application/json"
Link: <https://www.vendasta.com/blog/>; rel=shortlink
2023 Agency Insights
Report
Data-driven insights and analysis to help you navigate the shifting landscape and level-set with
Content Modified
HTTP to HTTPS Insecure Transition in Form Post
URL: http://blog.vendasta.com
Risk: Medium
Confidence: Medium
Parameter:
Attack:
Evidence: https://vendasta.com/content-library/

Burp Suite


Burp Project Repeater View Help
Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan
Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Tasks
New scan
New live task
Filter
Search
3. Crawl and audit of blog.vendasta.com
Crawl and Audit - Fast
Paused
Issues: 0 0 0 36
2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing
Issues: 0 0 0 0
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing
3. Crawl and audit of blog.vendasta.com
Summary Audit items Issues Event log Logger Audit log Live crawl view
Most serious vulnerabilities found (live)
View all
Issue type Host Time
Cacheable HTTPS response https://blog.vendast... 11:40:51 23 Oct 20...
Content security policy: allows clickjac... https://blog.vendast... 11:40:51 23 Oct 20...
Content security policy: allows form hi... https://blog.vendast... 11:40:51 23 Oct 20...
Content security policy: allows untrus... https://blog.vendast... 11:40:51 23 Oct 20...
Task configuration
View configuration
Task type: Crawl & audit
Scope: blog.vendasta.com
Configuration: Crawl and Audit - Fast
Task progress
Total audit items: 16
Audit items pending: 0
Audit items in progress: 16
Audit items completed: 0
Unique locations: 7
Pending actions: 0
Current link depth: 0
Requests: 1023
Network errors: 0
Task log
> Auditing URL param of "https://blog.vendasta.com/hs/preferences-center/" for Open Redirection
> Auditing URL param of "https://blog.vendasta.com/hs/preferences-center/" for OS Command Injection
> Auditing URL param of "https://blog.vendasta.com/_hcms/preview/" for Open Redirection
> Auditing URL param of "https://blog.vendasta.com/_hcms/preview/" for OS Command Injection
> Auditing URL param of "https://blog.vendasta.com/hs/preferences-center/" for HTTP Header Injection


Burp Project Repeater View Help
Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan
Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Tasks
New scan
New live task
3. Crawl and audit of blog.vendasta.com
Summary Audit items Issues Event log Logger Audit log Live crawl view
Filter High Medium Low Info Certain Firm Tentative BCheck generated Scan checks Extensions
Time Source Issue type Host Path Insertion point Severity
Advisory Request Response Dynamic analysis Path to issue
Ajax request header manipulation (DOM-based)
Severity: Information
Confidence: Firm
URL: https://blog.vendasta.com/hs/preferences-center/
Issue detail
The application may be vulnerable to DOM-based Ajax request header manipulation. Data is read from location.href and passed to xhr.setRequestHeader.value.
Issue background
DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way. Ajax request header manipulation arises when a script writes controllable data into a header of an Ajax request that is issued using XmlHttpRequest. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will set an arbitrary header in the subsequent Ajax request.

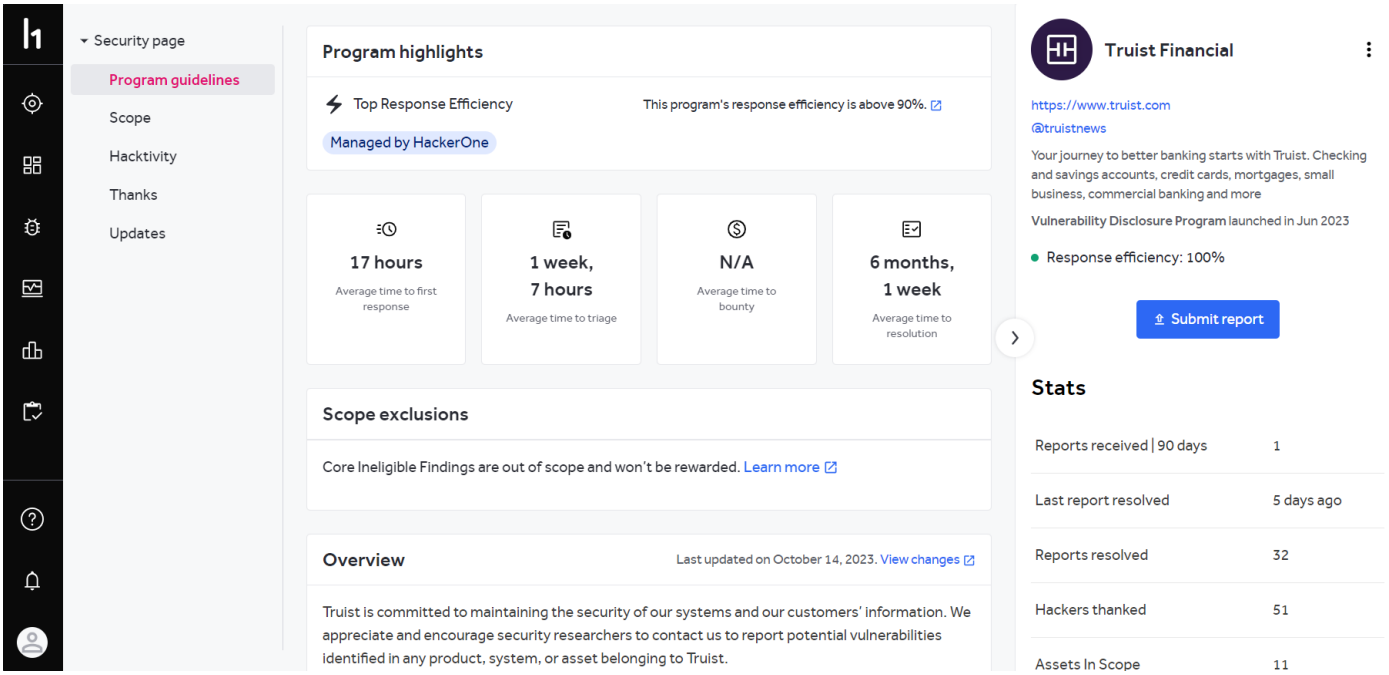

Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Tasks
New scan
New live task
3. Crawl and audit of blog.vendasta.com
Summary Audit items Issues Event log Logger Audit log Live crawl view
Filter High Medium Low Info Certain Firm Tentative BCheck generated Scan checks Extensions
Time Source Issue type Host Path Insertion point Severity
Advisory Request Response Path to issue
Pretty Raw Hex Render
Inspector
Response headers 21
HTTP/2 200 OK
Date: Wed, 23 Oct 2024 06:10:19 GMT
Content-Type: text/plain; charset=utf-8
Cache-Control: s-maxage=10800, max-age=0
Etag: W/"73aaf976ad5f22f53de53dbe41d7e788"
Last-Modified: Wed, 16 Oct 2024 15:20:57 GMT
Strict-Transport-Security: max-age=31536000
Cache-Tag: P-20852504,SS-573581013 68,PGS-ALL,SW-0
Content-Security-Policy: upgrade-insecure-requests

Vulnerabilities:

1 Hidden Data Found

Vulnerability Title	Hidden Data Found
Vulnerability Description	Sensitive data such as configuration files, credentials, API keys, or internal application data is exposed due to inadequate access controls. This data might be accessible to unauthorized users via URL endpoints, improperly configured APIs, or files that are unintentionally made public.
Affected Components	Components such as exposed API endpoints, configuration files,sensitive URL directories, or database files may be affected. • Specific file paths that are publicly accessible. • API endpoints returning sensitive information. • Misconfigured cloud resources exposing metadata.
Impact Assessment	**Credential Exposure**: Attackers could use the exposed data to log into privileged services. **Information Leakage**: Internal logic, API secrets, and environment details might be leaked, aiding in future attacks (like SQL injection or server-side request forgery (SSRF)).
Steps to Reproduce	**Access publicly exposed data**: Navigate to specific URL paths where sensitive data might be accessible. For instance: • https://blog.vendasta.com/robots.txt • https://blog.vendasta.com/.env **Observe the output**: Check the contents of the files or responses to see if any sensitive information like API keys, database credentials, or internal metadata is exposed.
Proof of Concept	Perform a simple curl request to the robots.txt file to extract hidden or disallowed URLs. Access sensitive metadata by querying an exposed API endpoint without authentication: curl https://blog.vendasta.com/.env
Proposed Mitigation or Fix	**Restrict Access**: Use proper server configurations to deny public access to sensitive files. **Encrypt Sensitive Data**: If exposure occurs, ensure that any sensitive data stored is encrypted. **Use Firewalls**: Apply firewalls and access rules to limit exposure to sensitive metadata and configuration files. **Regular Audits**: Continuously scan for exposed files or sensitive data on public-facing servers.

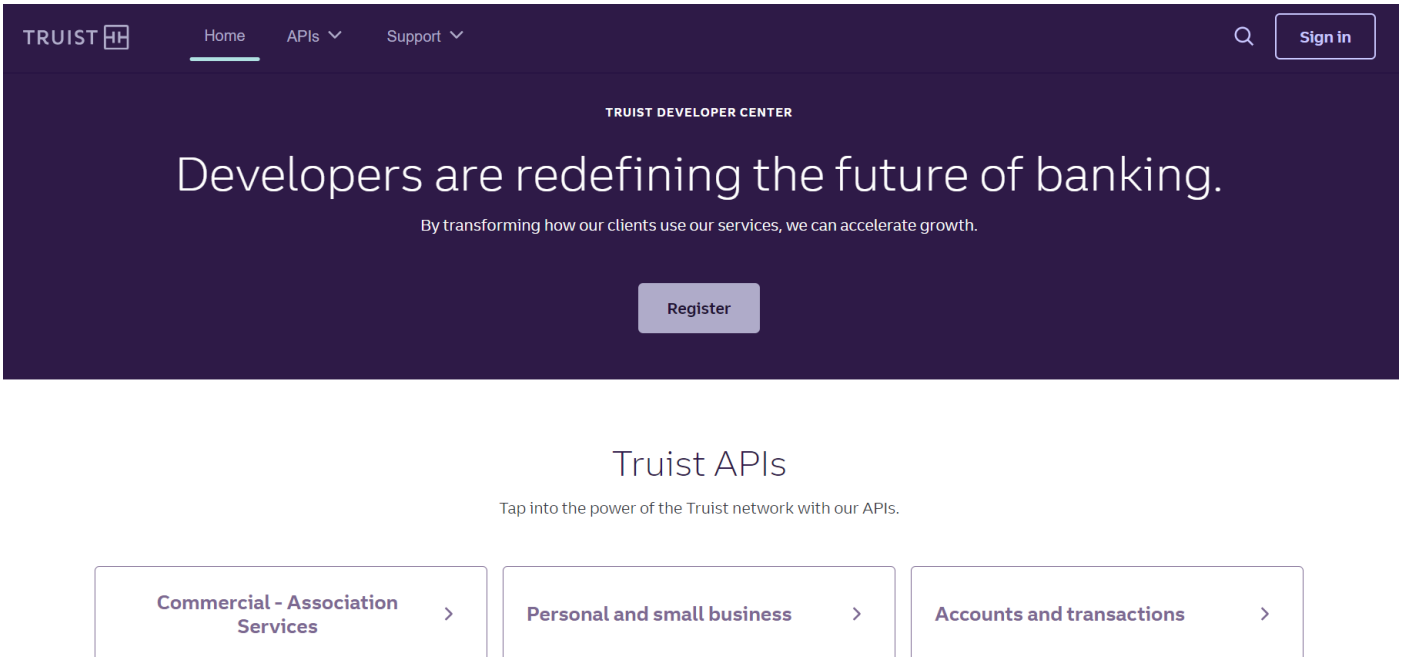
Report 05 Target Details



The target for this Bug Bounty report is Truist (https://www.truist.com), a platform providing digital solutions for businesses, including tools for marketing, sales, and customer management. The company offers a range of services such as digital advertising, reputation management, and APIs for integrating various business functions. Truist's platform is designed to help businesses grow by offering scalable and efficient solutions, leveraging modern technologies.

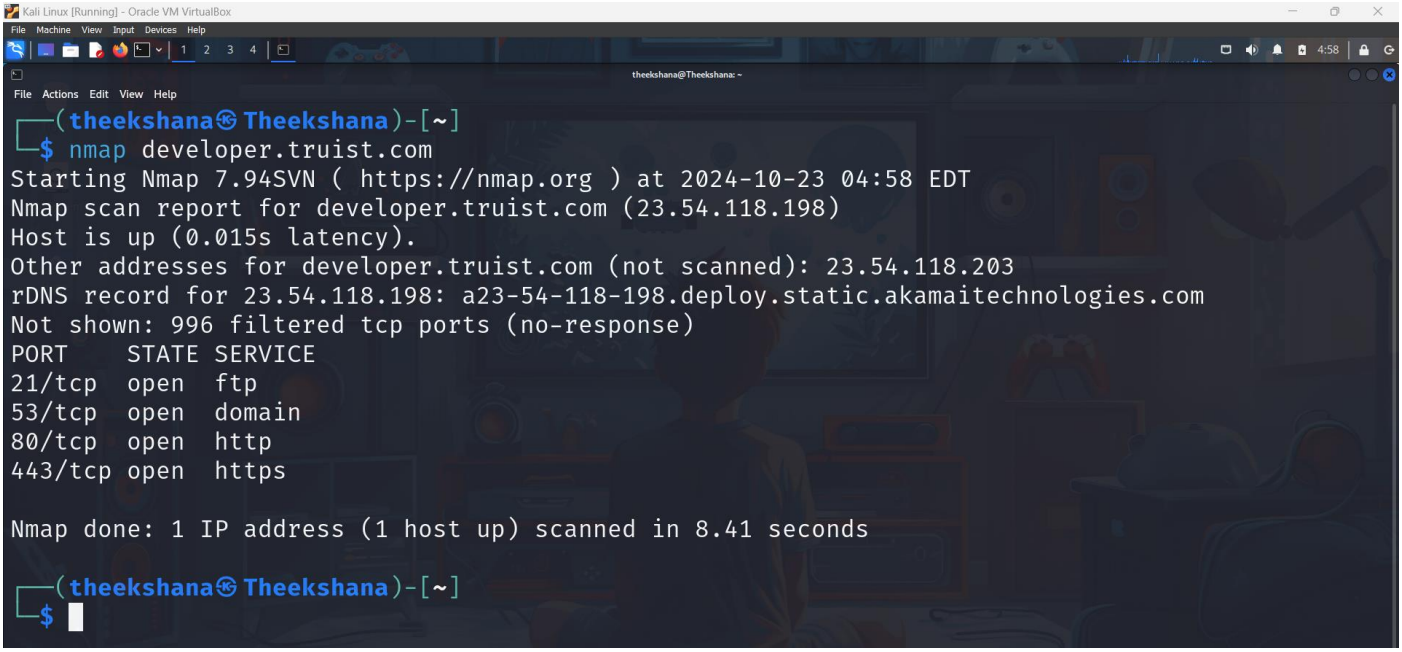
In this report, I have chosen to focus on 10 subdomains under the main domain truist.com. Each subdomain may serve different functionalities or services, potentially introducing distinct security risks, particularly in development or user-related areas. These subdomains were selected based on their relevance and the likelihood of containing vulnerabilities.

This report covers the findings for the subdomain: developer.truist.com



Target Reconnaissance

Nmap Scan

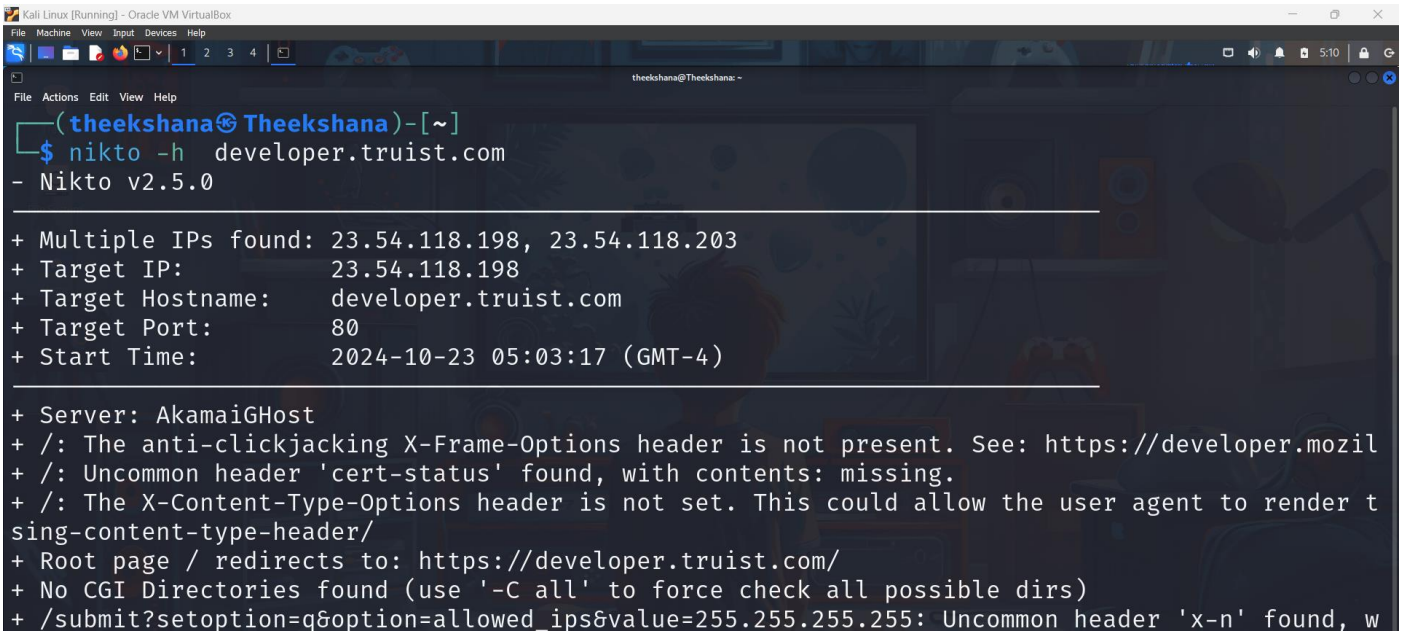


By scanning developer.truist.com with Nmap I found out these information.

Port	State	Service
21/tcp	Open	FTP
53/tcp	Open	DOMAIN
80/tcp	Open	HTTP
443/tcp	Open	HTPPS
8080/tcp	Open	HTTP-PROXY

Port	State	Service	Potential Vulnerabilities
21/tcp	Open	FTP	Data is not encrypted, so sensitive information can be stolen. Hackers can guess passwords (brute force attacks) Misconfigurations might allow unauthorized access
53/tcp	Open	DNS	Attackers can redirect users to fake sites (DNS poisoning) Hackers might flood the system (amplification attacks) Sensitive DNS info could be exposed (zone transfer)
80/tcp	Open	HTTP	Data is not secure (no encryption) Hackers can inject harmful scripts (XSS)
443/tcp	Open	HTTPS	If not properly secured, attackers can intercept data Older encryption protocols may be weak

Nikto Scan



The screenshot shows the output of a Nikto scan against the target developer.truist.com which reveals several potential security issues and misconfigurations.

Target Information:

- **Target IP**: 23.54.118.198
- **Target Hostname**: developer.truist.com
- **Target Port**: 80 (HTTP port)

Security Headers:\

- **X-Frame-Options header**: Missing. This header prevents clickjacking attacks, and its absence can be a vulnerability.

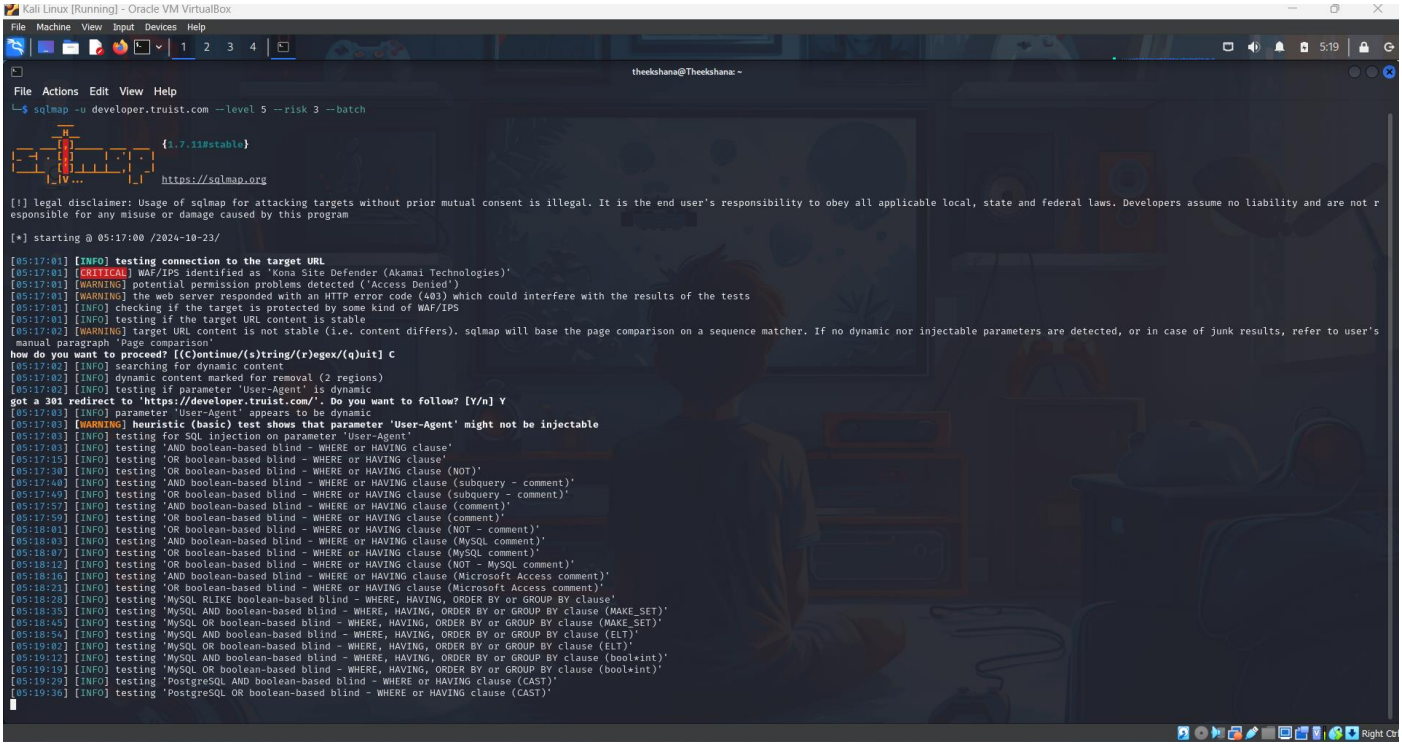
- **cert-status header**: Found but empty or missing contents.

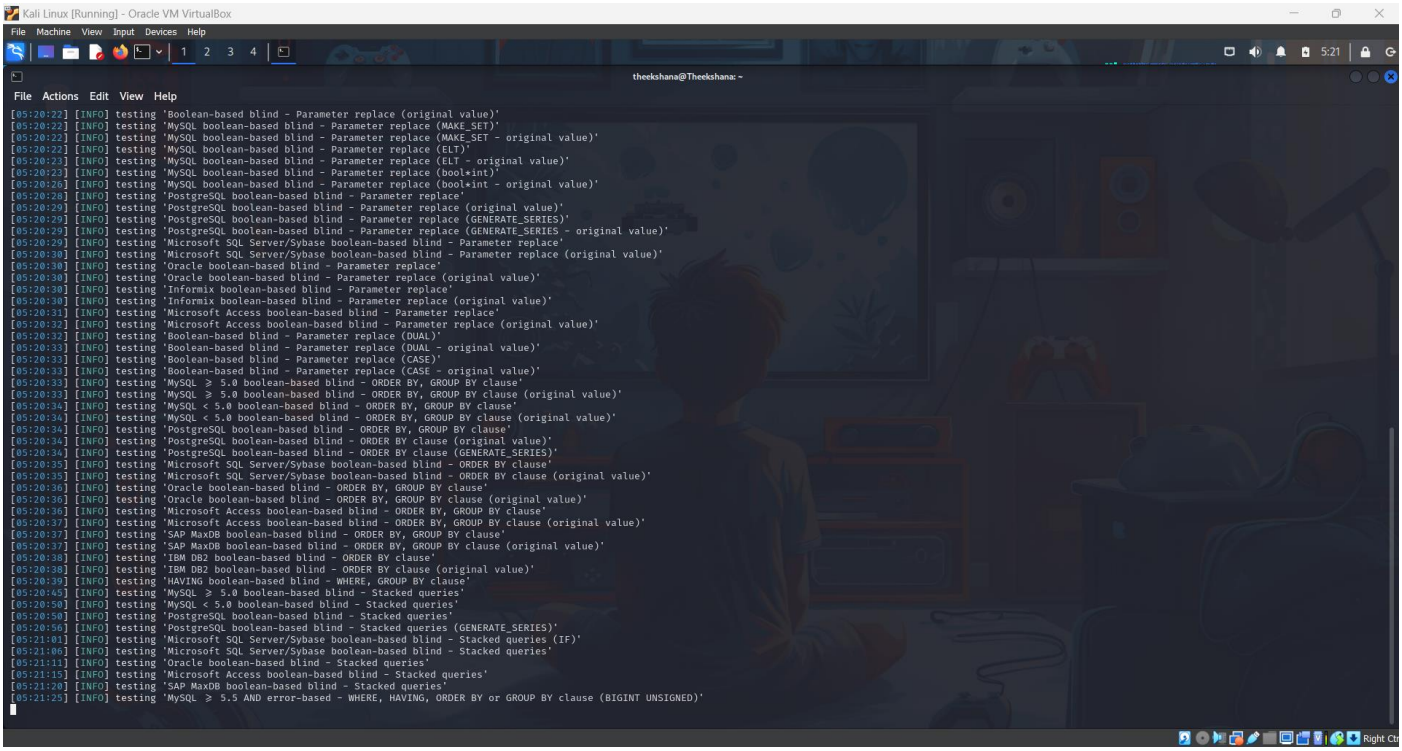
- **X-Content-Type-Options header**: Missing. This could allow browsers to misinterpret files as the wrong MIME type, potentially leading to security risks.

Root Page/Redirect:

- The root page redirects to https://developer.truist.com/, indicating the website automatically redirects from HTTP to HTTPS.

SQLmap Scaner

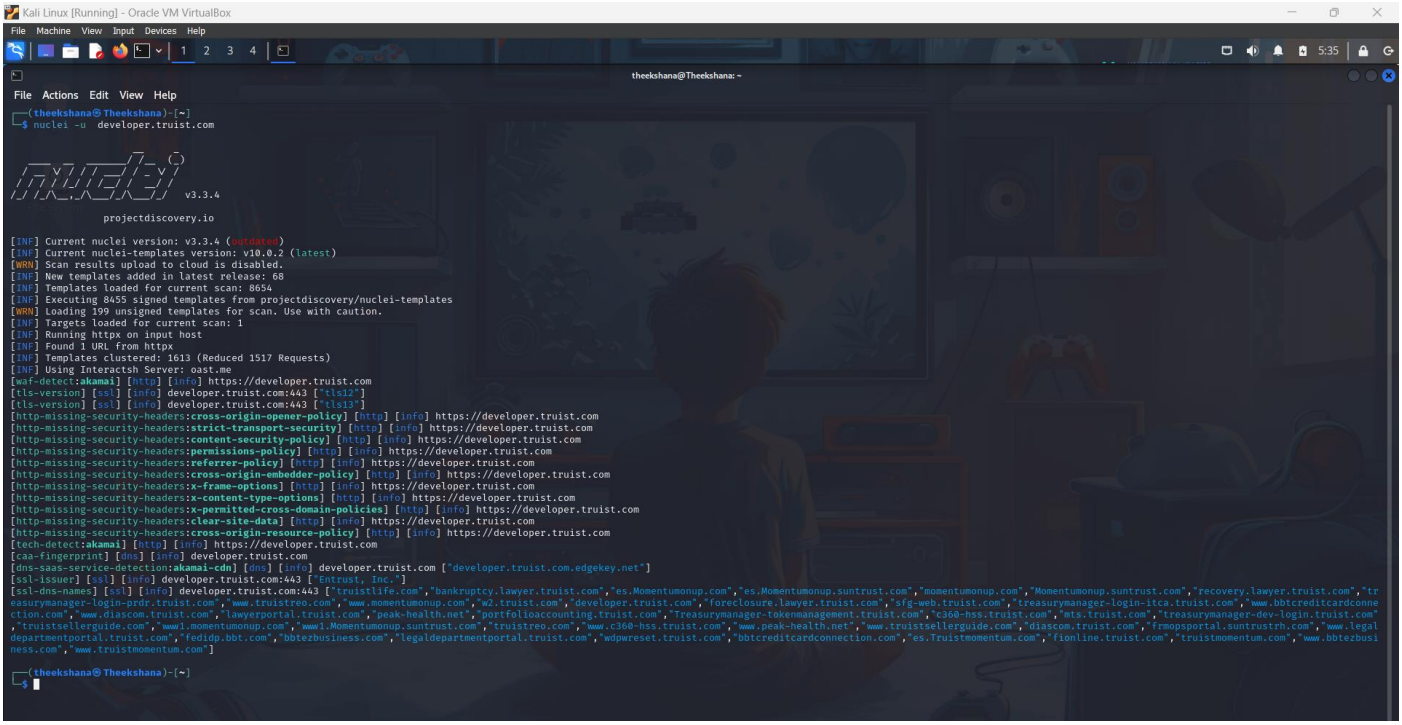




WAF (Web Application Firewall) Detected:

- A **CRITICAL** warning indicates that a Web Application Firewall (WAF) is active on the site, specifically identified as **Kona Site Defender** by **Akamai Technologies**. This WAF could interfere with sqlmap's scanning attempts, making it harder to detect vulnerabilities.
- **403 Forbidden HTTP error**: The server responded with an HTTP code 403, which suggests that access is restricted, possibly by the WAF or other server-side protections.

Nuclei Scan

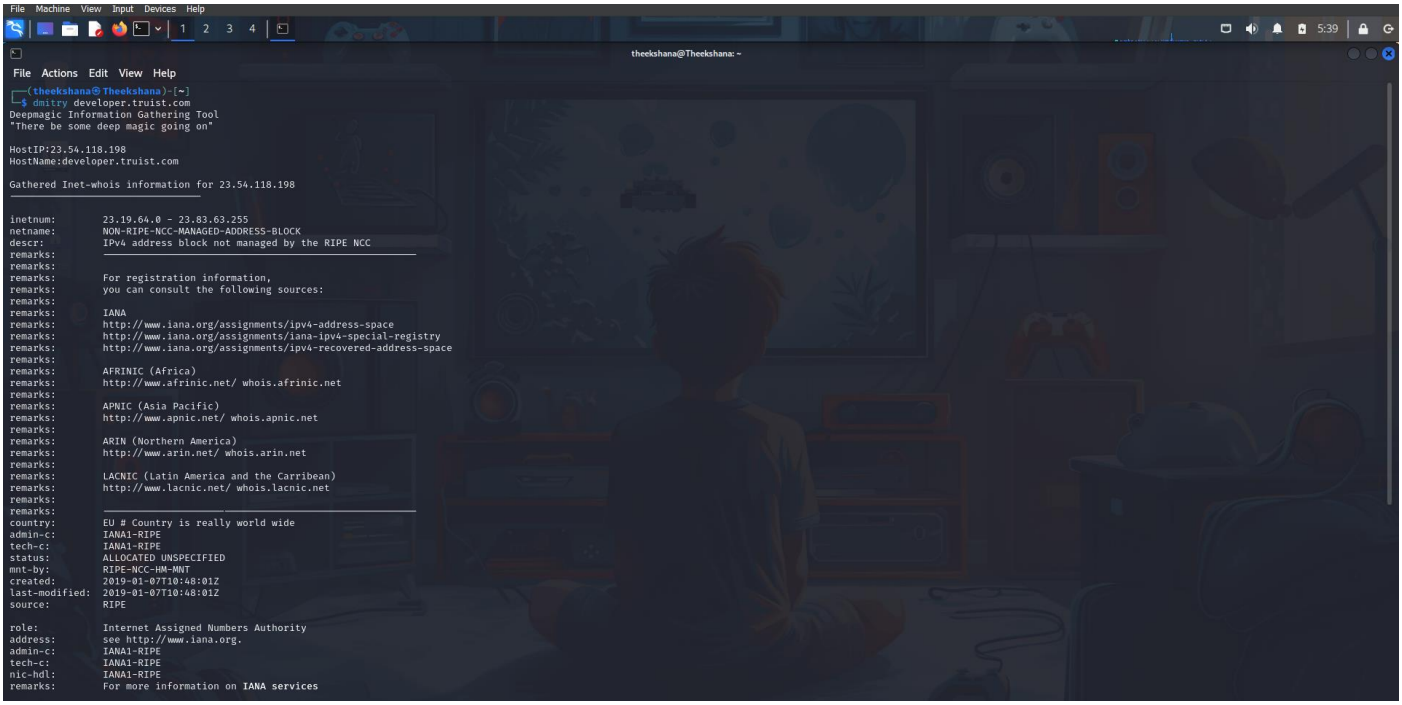


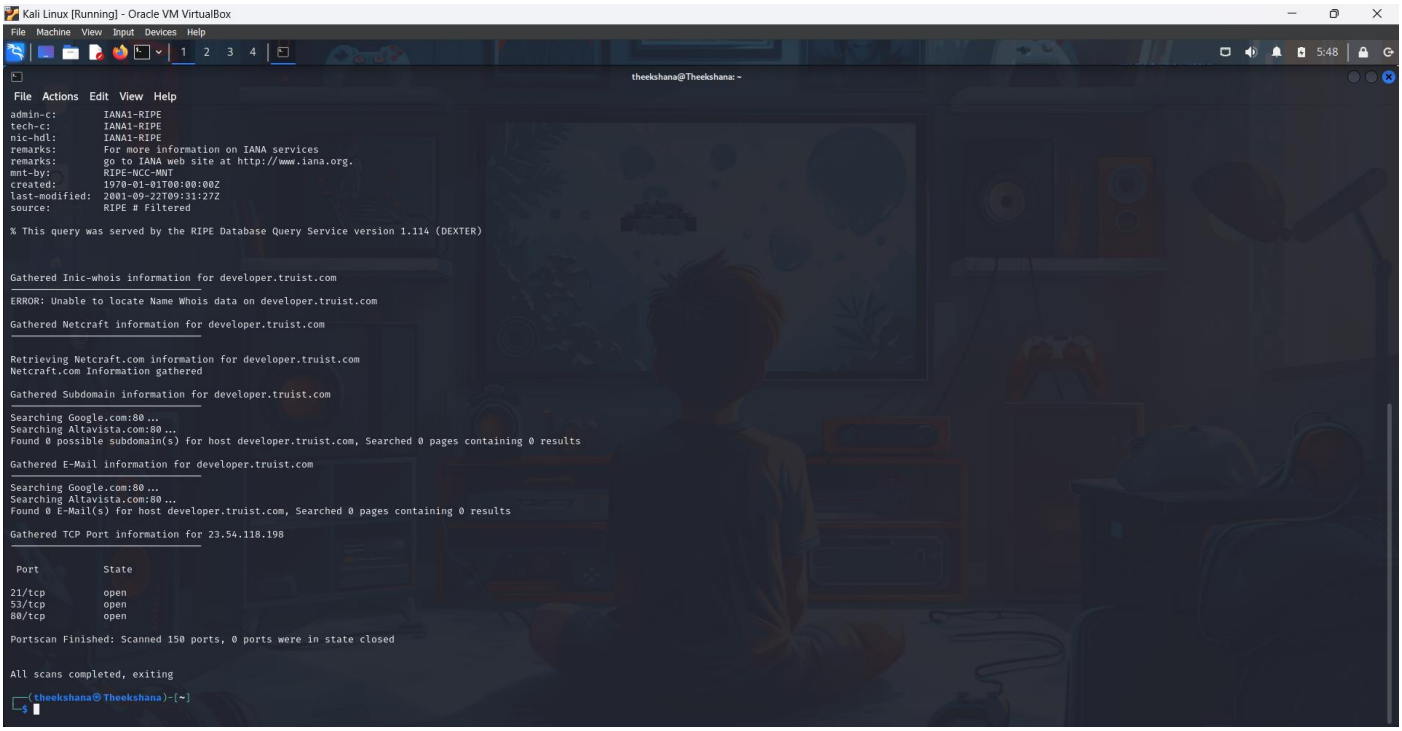
Scan Results:

- Several security headers are missing or misconfigured, which are important for securing web applications. These include:

    - Strict-Transport-Security
    - Content-Security-Policy
    - X-Frame-Options
    - Permissions-Policy
    - Referrer-Policy
    - X-Content-Type-Options
    - Cross-Origin-Embedder-Policy
    - Cross-Origin-Opener-Policy
    - Cross-Origin-Resource-Policy
    - Clear-Site-Data

Dmitry Scan



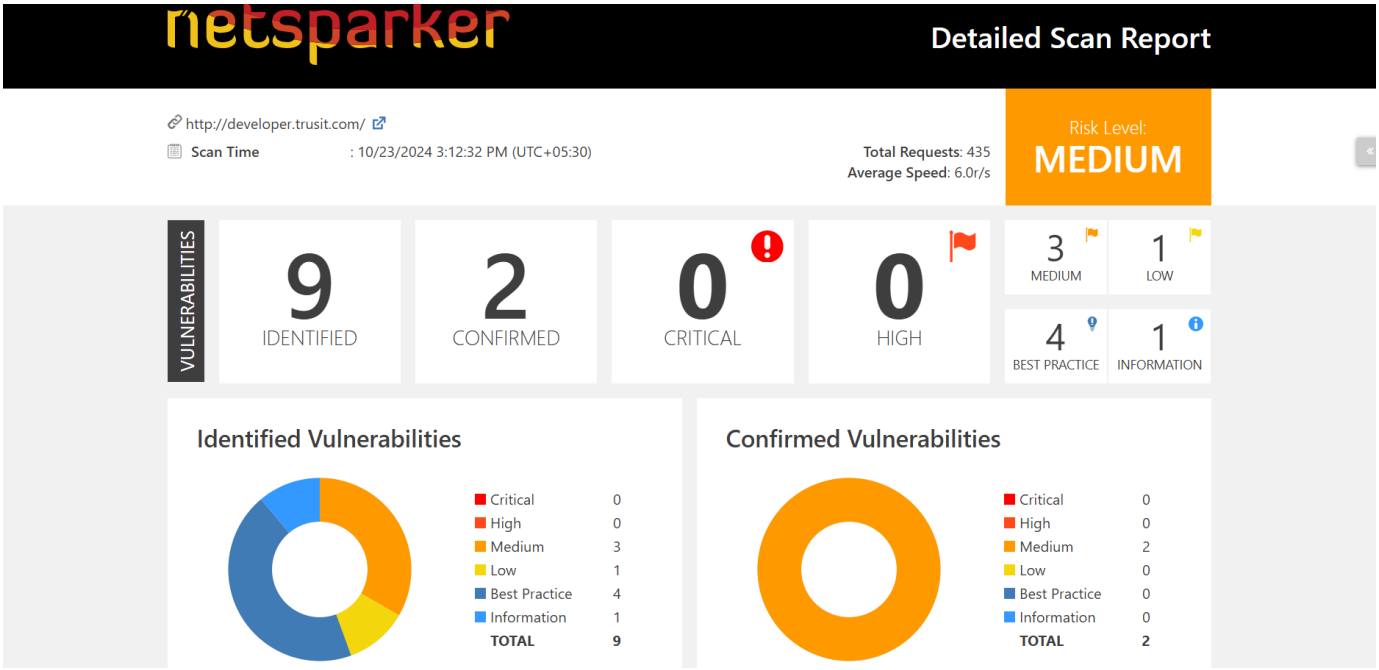


Port 21 (FTP - File Transfer Protocol): This port is typically used for file transfer services. Having FTP open can be risky if not properly secured, as it often transmits data in plain text (though secure variants like SFTP exist).

Port 53 (DNS - Domain Name System): This port is used for DNS services, which translate domain names into IP addresses. While DNS services need to be accessible, misconfigurations or vulnerabilities (like DNS amplification attacks) can expose the server to risks.

Port 80 (HTTP - Hypertext Transfer Protocol): This port is used for unencrypted web traffic. Port 80 being open suggests that the website is accessible via HTTP, but this should be redirected to HTTPS (Port 443) for encrypted communication. If not, it leaves the site vulnerable to man-in-the middle (MITM) attacks.

Netsparker



Vulnerability Summary

SEVERITY FILTER : CRITICAL HIGH MEDIUM LOW BEST PRACTICE INFORMATION

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://developer.trusit.com/	
	Invalid SSL Certificate	GET	https://developer.trusit.com/	
	Weak Ciphers Enabled	GET	https://developer.trusit.com/	
	Missing X-Frame-Options Header	GET	http://developer.trusit.com/	
	Content Security Policy (CSP) Not Implemented	GET	http://developer.trusit.com/	
	Expect-CT Not Enabled	GET	https://developer.trusit.com/	
	Missing X-XSS-Protection Header	GET	http://developer.trusit.com/	
	Referrer-Policy Not Implemented	GET	http://developer.trusit.com/	
	Apache Web Server Identified	GET	http://developer.trusit.com/	

Invalid SSL Certificate

MEDIUM 1 CONFIRMED 1

Netsparker identified an invalid SSL certificate.

An SSL certificate can be created and signed by anyone. You should have a valid SSL certificate to make your visitors sure about the secure communication between your website and them. If you have an invalid certificate, your visitors will have trouble distinguishing between your certificate and those of attackers.

Impact

Attackers can perform man-in-the-middle attacks and observe the encryption traffic between your website and its visitors.

Vulnerabilities

2.1. https://developer.trusit.com/ CONFIRMED

Hide Remediation

Remedy

Fix the problem with your SSL certificate to provide secure communication between your website and its visitors.

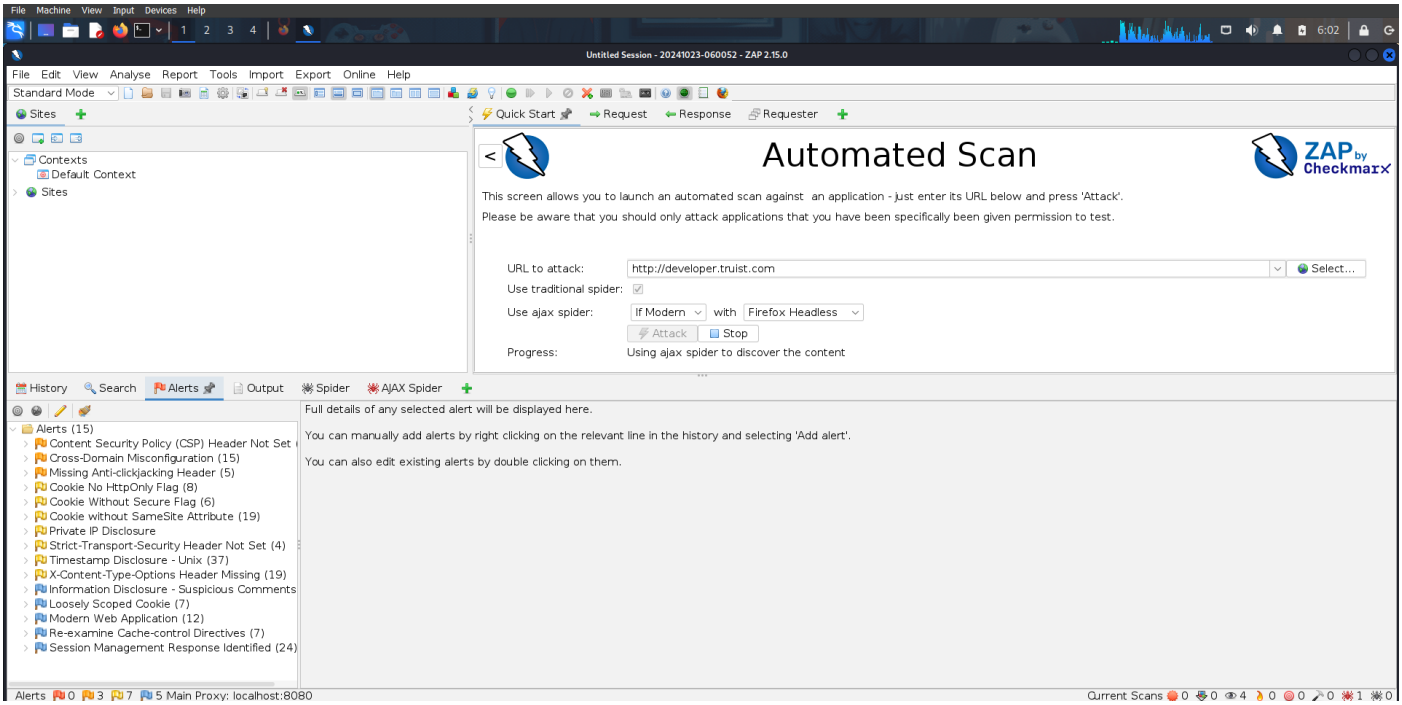
External References

- OWASP - Insecure Configuration Management
- OWASP Top 10-2017 A3-Sensitive Data Exposure

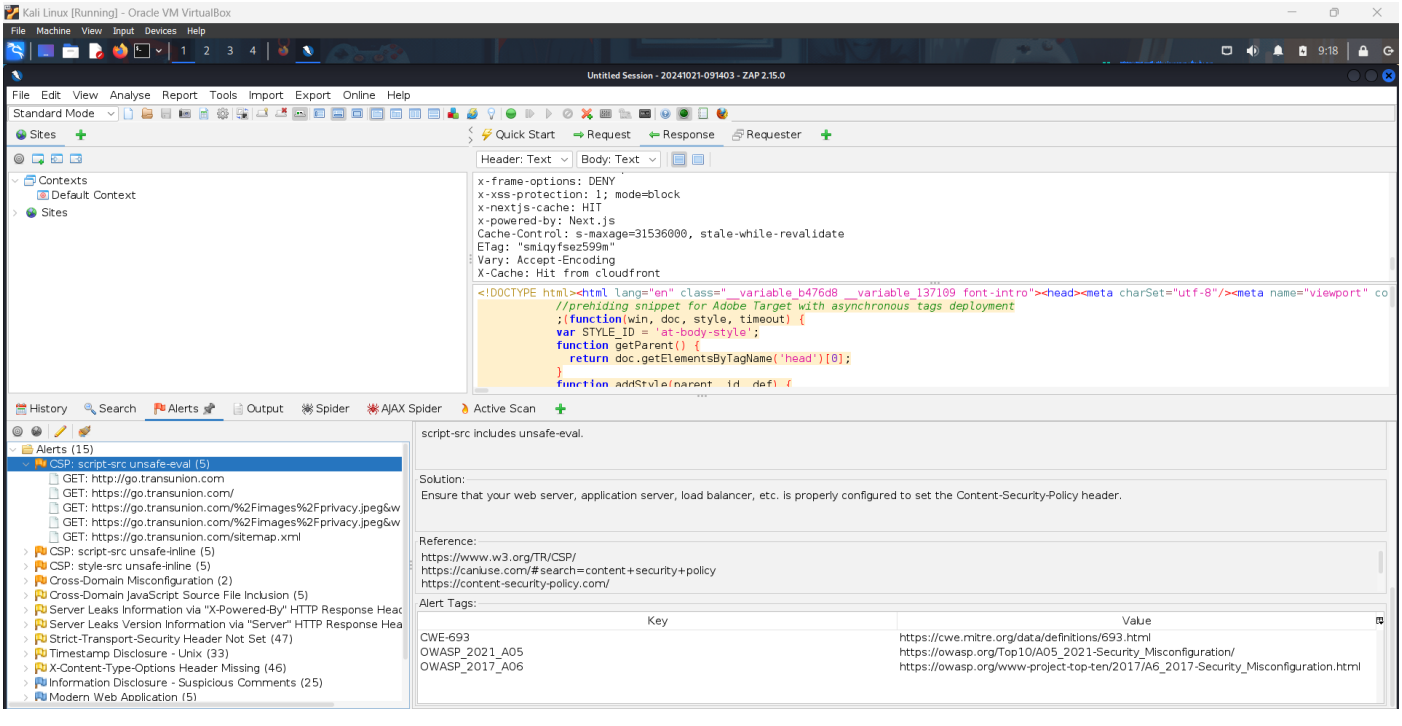
CLASSIFICATION

PCI DSS v3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	5
CAPEC	459

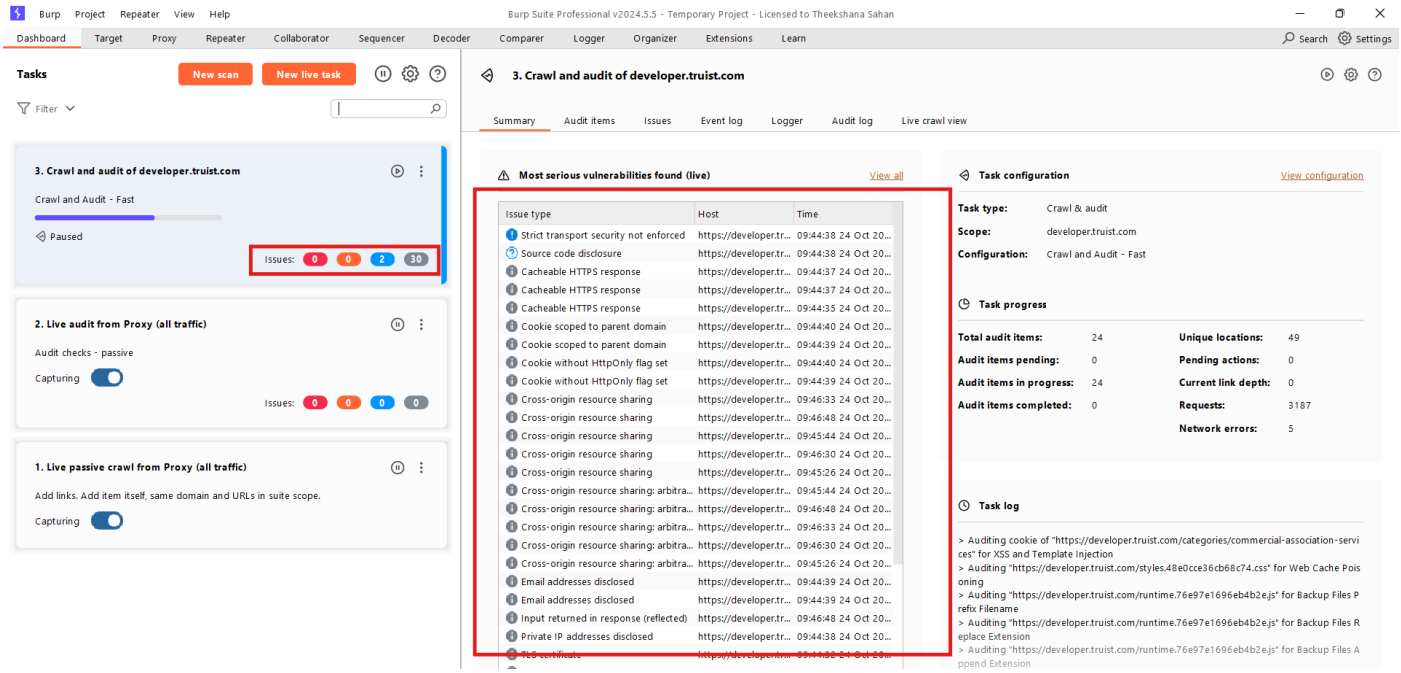
OWASP ZAP

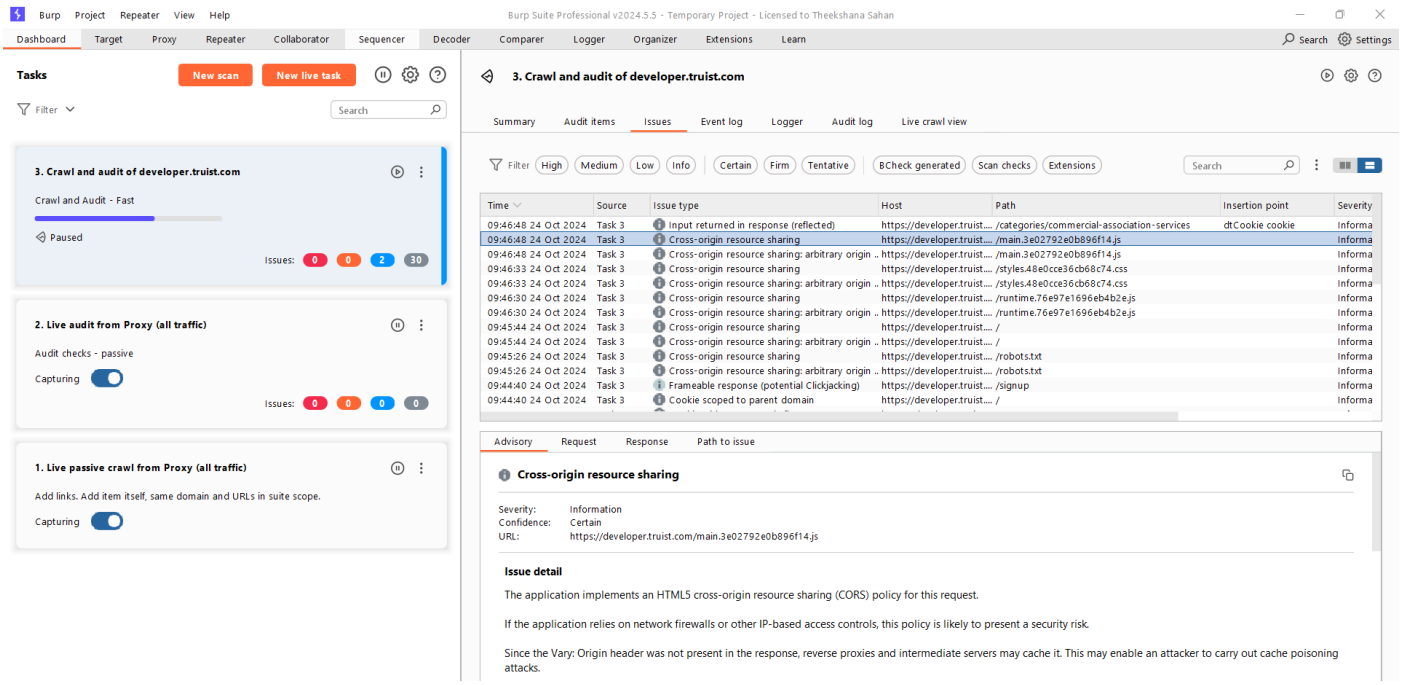

Automated Scan
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack: http://developer.truist.com
Use traditional spider:
Use ajax spider: If Modern with Firefox Headless
Attack
Stop
Progress: Using ajax spider to discover the content
Alerts (15)
Content Security Policy (CSP) Header Not Set
Cross-Domain Misconfiguration (15)
Missing Anti-clickjacking Header (5)
Cookie No HttpOnly Flag (8)
Cookie Without Secure Flag (6)
Cookie without SameSite Attribute (19)
Private IP Disclosure
Strict-Transport-Security Header Not Set (4)
Timestamp Disclosure - Unix (37)
X-Content-Type-Options Header Missing (19)
Information Disclosure - Suspicious Comments
Loosely Scoped Cookie (7)
Modern Web Application (12)
Re-examine Cache-control Directives (7)
Session Management Response Identified (24)
Full details of any selected alert will be displayed here.
You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.
You can also edit existing alerts by double clicking on them.

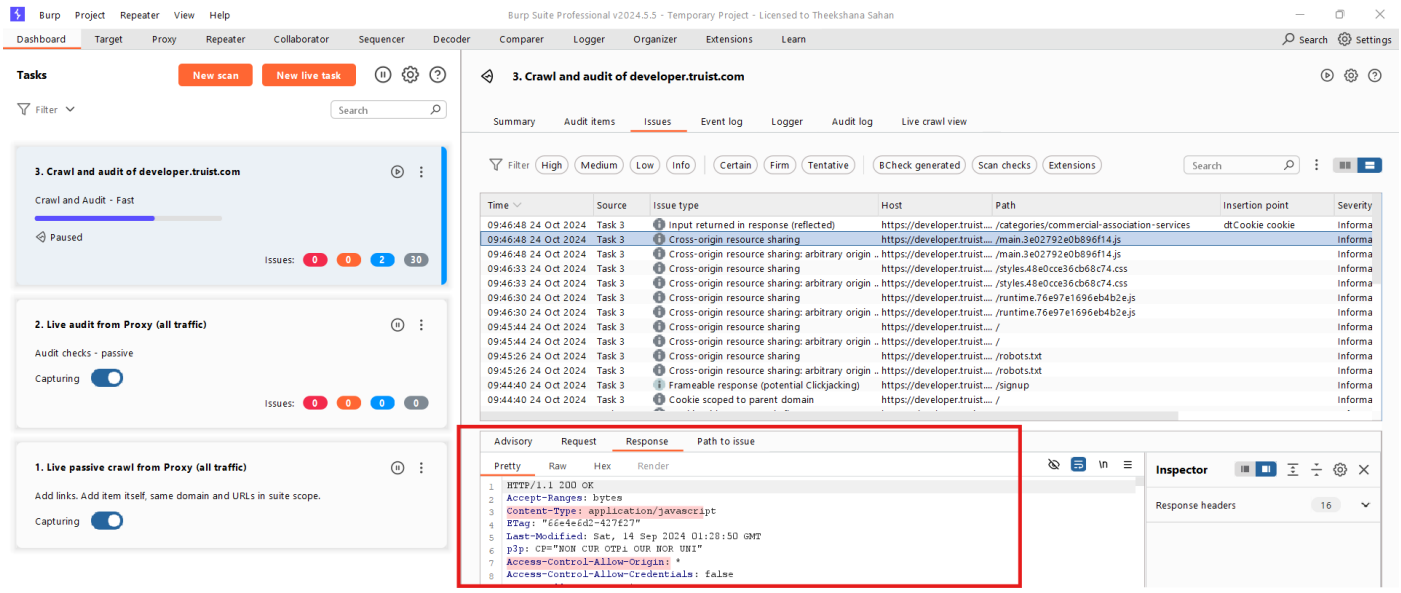

CSP: script-src unsafe-eval
URL: http://go.transunion.com
Risk: Medium
Confidence: High
Parameter: content-security-policy
Attack:
Evidence: :m.com dpm.demdex.net api.company-target.com t.teads.tv transunion.tt.omtrdc.net googleads.g.doubleclick.net ; block-all-mixed-content; upgrade-insecure-requests;
CWE ID: 693
WASC ID: 15
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, ActiveX, audio and video files.
Other Info:
script-src includes unsafe-eval.
Solution:
Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference:
https://www.w3.org/TR/CSP/
https://caniuse.com/#search=content+security+policy
Cancel
Save


Untitled Session - 20241021-091403 - ZAP 2.15.0
x-frame-options: DENY
x-xss-protection: 1; mode=block
x-nextjs-cache: HIT
x-powered-by: Next.js
Cache-Control: s-maxage=31536000, stale-while-revalidate
ETag: "smiqyfsez599m"
Vary: Accept-Encoding
X-Cache: Hit from cloudfront
script-src includes unsafe-eval.
Solution:
Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference:
https://www.w3.org/TR/CSP/
https://caniuse.com/#search=content+security+policy
https://content-security-policy.com/
Alert Tags:
Key
Value
CWE-693
https://cwe.mitre.org/data/definitions/693.html
OWASP_2021_A05
https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
OWASP_2017_A06
https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html

Burp Suite


Burp Project Repeater View Help
Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan
Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Tasks
New scan
New live task
3. Crawl and audit of developer.truist.com
Crawl and Audit - Fast
Paused
Issues: 0 0 2 30
2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing
Issues: 0 0 0 0
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing
3. Crawl and audit of developer.truist.com
Summary Audit items Issues Event log Logger Audit log Live crawl view
Most serious vulnerabilities found (live)
View all
Issue type Host Time
Strict transport security not enforced https://developer.tr... 09:44:38 24 Oct 20...
Source code disclosure https://developer.tr... 09:44:38 24 Oct 20...
Cacheable HTTPS response https://developer.tr... 09:44:37 24 Oct 20...
Cacheable HTTPS response https://developer.tr... 09:44:37 24 Oct 20...
Cacheable HTTPS response https://developer.tr... 09:44:35 24 Oct 20...
Cookie scoped to parent domain https://developer.tr... 09:44:40 24 Oct 20...
Cookie scoped to parent domain https://developer.tr... 09:44:39 24 Oct 20...
Cookie without HttpOnly flag set https://developer.tr... 09:44:40 24 Oct 20...
Cookie without HttpOnly flag set https://developer.tr... 09:44:39 24 Oct 20...
Cross-origin resource sharing https://developer.tr... 09:46:33 24 Oct 20...
Cross-origin resource sharing https://developer.tr... 09:46:48 24 Oct 20...
Cross-origin resource sharing https://developer.tr... 09:45:44 24 Oct 20...
Cross-origin resource sharing https://developer.tr... 09:46:30 24 Oct 20...
Cross-origin resource sharing https://developer.tr... 09:45:26 24 Oct 20...
Cross-origin resource sharing: arbitra... https://developer.tr... 09:45:44 24 Oct 20...
Cross-origin resource sharing: arbitra... https://developer.tr... 09:46:48 24 Oct 20...
Cross-origin resource sharing: arbitra... https://developer.tr... 09:46:33 24 Oct 20...
Cross-origin resource sharing: arbitra... https://developer.tr... 09:46:30 24 Oct 20...
Cross-origin resource sharing: arbitra... https://developer.tr... 09:45:26 24 Oct 20...
Email addresses disclosed https://developer.tr... 09:44:39 24 Oct 20...
Email addresses disclosed https://developer.tr... 09:44:39 24 Oct 20...
Input returned in response (reflected) https://developer.tr... 09:46:48 24 Oct 20...
Private IP addresses disclosed https://developer.tr... 09:44:38 24 Oct 20...
Task configuration
View configuration
Task type: Crawl & audit
Scope: developer.truist.com
Configuration: Crawl and Audit - Fast
Task progress
Total audit items: 24
Audit items pending: 0
Audit items in progress: 24
Audit items completed: 0
Unique locations: 49
Pending actions: 0
Current link depth: 0
Requests: 3187
Network errors: 5
Task log
> Auditing cookie of "https://developer.truist.com/categories/commercial-association-services" for XSS and Template Injection
> Auditing "https://developer.truist.com/styles.48e0cce36cb68c74.css" for Web Cache Poisoning
> Auditing "https://developer.truist.com/runtime.76e97e1696eb4b2e.js" for Backup Files Prefix Filename
> Auditing "https://developer.truist.com/runtime.76e97e1696eb4b2e.js" for Backup Files Replace Extension
> Auditing "https://developer.truist.com/runtime.76e97e1696eb4b2e.js" for Backup Files Append Extension


Burp Project Repeater View Help
Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan
Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Tasks
New scan
New live task
3. Crawl and audit of developer.truist.com
Crawl and Audit - Fast
Paused
Issues: 0 0 2 30
2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing
Issues: 0 0 0 0
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing
3. Crawl and audit of developer.truist.com
Summary Audit items Issues Event log Logger Audit log Live crawl view
Filter High Medium Low Info Certain Firm Tentative BCheck generated Scan checks Extensions
Search
Time Source Issue type Host Path Insertion point Severity
09:46:48 24 Oct 2024 Task 3 Input returned in response (reflected) https://developer.truist.... /categories/commercial-association-services dtCookie cookie Informa
09:46:48 24 Oct 2024 Task 3 Cross-origin resource sharing https://developer.truist.... /main.3e02792e0b896f14.js Informa
09:46:48 24 Oct 2024 Task 3 Cross-origin resource sharing: arbitrary origin .. https://developer.truist.... /main.3e02792e0b896f14.js Informa
09:46:33 24 Oct 2024 Task 3 Cross-origin resource sharing https://developer.truist.... /styles.48e0cce36cb68c74.css Informa
09:46:33 24 Oct 2024 Task 3 Cross-origin resource sharing: arbitrary origin .. https://developer.truist.... /styles.48e0cce36cb68c74.css Informa
09:46:30 24 Oct 2024 Task 3 Cross-origin resource sharing https://developer.truist.... /runtime.76e97e1696eb4b2e.js Informa
09:46:30 24 Oct 2024 Task 3 Cross-origin resource sharing: arbitrary origin .. https://developer.truist.... /runtime.76e97e1696eb4b2e.js Informa
09:45:44 24 Oct 2024 Task 3 Cross-origin resource sharing https://developer.truist.... / Informa
09:45:44 24 Oct 2024 Task 3 Cross-origin resource sharing: arbitrary origin .. https://developer.truist.... / Informa
09:45:26 24 Oct 2024 Task 3 Cross-origin resource sharing https://developer.truist.... /robots.txt Informa
09:45:26 24 Oct 2024 Task 3 Cross-origin resource sharing: arbitrary origin .. https://developer.truist.... /robots.txt Informa
09:44:40 24 Oct 2024 Task 3 Frameable response (potential Clickjacking) https://developer.truist.... /signup Informa
09:44:40 24 Oct 2024 Task 3 Cookie scoped to parent domain https://developer.truist.... / Informa
Advisory Request Response Path to issue
Cross-origin resource sharing
Severity: Information
Confidence: Certain
URL: https://developer.truist.com/main.3e02792e0b896f14.js
Issue detail
The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.
If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.
Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

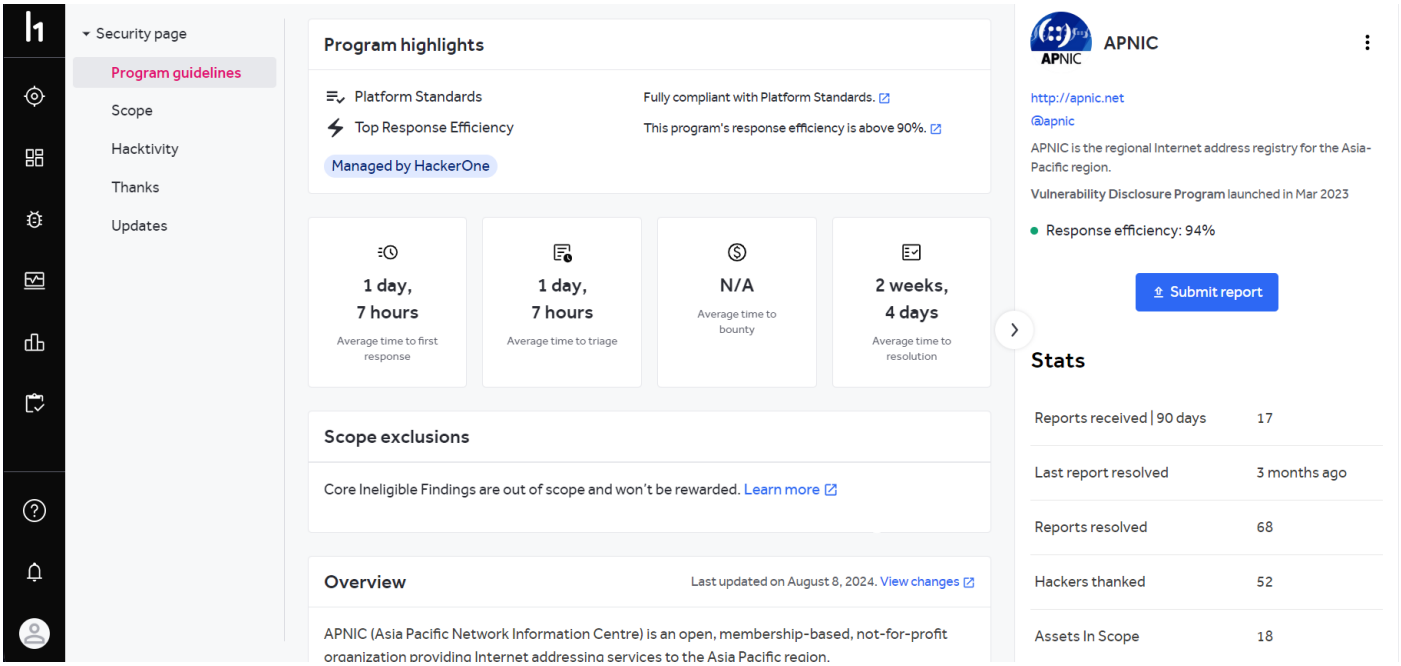

Burp Project Repeater View Help
Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan
Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Tasks
New scan
New live task
3. Crawl and audit of developer.truist.com
Crawl and Audit - Fast
Paused
Issues: 0 0 2 30
2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing
Issues: 0 0 0 0
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing
3. Crawl and audit of developer.truist.com
Summary Audit items Issues Event log Logger Audit log Live crawl view
Filter High Medium Low Info Certain Firm Tentative BCheck generated Scan checks Extensions
Search
Time Source Issue type Host Path Insertion point Severity
09:46:48 24 Oct 2024 Task 3 Input returned in response (reflected) https://developer.truist.... /categories/commercial-association-services dtCookie cookie Informa
09:46:48 24 Oct 2024 Task 3 Cross-origin resource sharing https://developer.truist.... /main.3e02792e0b896f14.js Informa
09:46:48 24 Oct 2024 Task 3 Cross-origin resource sharing: arbitrary origin .. https://developer.truist.... /main.3e02792e0b896f14.js Informa
09:46:33 24 Oct 2024 Task 3 Cross-origin resource sharing https://developer.truist.... /styles.48e0cce36cb68c74.css Informa
09:46:33 24 Oct 2024 Task 3 Cross-origin resource sharing: arbitrary origin .. https://developer.truist.... /styles.48e0cce36cb68c74.css Informa
09:46:30 24 Oct 2024 Task 3 Cross-origin resource sharing https://developer.truist.... /runtime.76e97e1696eb4b2e.js Informa
09:46:30 24 Oct 2024 Task 3 Cross-origin resource sharing: arbitrary origin .. https://developer.truist.... /runtime.76e97e1696eb4b2e.js Informa
09:45:44 24 Oct 2024 Task 3 Cross-origin resource sharing https://developer.truist.... / Informa
09:45:44 24 Oct 2024 Task 3 Cross-origin resource sharing: arbitrary origin .. https://developer.truist.... / Informa
09:45:26 24 Oct 2024 Task 3 Cross-origin resource sharing https://developer.truist.... /robots.txt Informa
09:45:26 24 Oct 2024 Task 3 Cross-origin resource sharing: arbitrary origin .. https://developer.truist.... /robots.txt Informa
09:44:40 24 Oct 2024 Task 3 Frameable response (potential Clickjacking) https://developer.truist.... /signup Informa
09:44:40 24 Oct 2024 Task 3 Cookie scoped to parent domain https://developer.truist.... / Informa
Advisory Request Response Path to issue
Pretty Raw Hex Render
HTTP/1.1 200 OK
Accept-Ranges: bytes
Content-Type: application/javascript
ETag: "£6e4e6d2-427£27"
Last-Modified: Sat, 14 Sep 2024 01:28:50 GMT
p3p: CP="NON CUR OTPi OUR NOR UNI"
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: false
Inspector
Response headers 16

Vulnerabilities:

1Cross-Origin Resource Sharing:

Vulnerability Title	**Cross-Origin Resource Sharing: Arbitrary Origin Trusted**
Vulnerability Description	The application implements an HTML5 cross-origin resource sharing (CORS) policy that allows access from any domain, effectively disabling the same-origin policy. This can lead to security risks, especially if sensitive data or privileged actions are involved.
Affected Components	CORS configuration for the web application. API endpoints and web pages that rely on CORS for cross-domain requests. Any components that handle sensitive data or user credentials.
Impact Assessment	Allows unauthorized cross-origin access to sensitive data or functionalities.Potential exposure of user sessions or sensitive information to malicious websites May allow attackers to bypass IP-based or origin-based access controls. If Access-Control-Allow-Credentials: true is set, it could enable attackers to carry out privileged actions by exploiting authenticated user sessions.
Steps to Reproduce	Access the application at developer.truist.com Use browser developer tools to monitor network requests. Make a cross-origin request from a malicious site to see if it successfully retrieves data or performs actions that should be restricted. Check the Access-Control-Allow-Origin header in the response to confirm it allows arbitrary origins.
Proof of Concept	developer.truist.com in an unsecured network. Use network analysis tools (e.g., Wireshark) to observe traffic and confirm it's unencrypted.
Proposed Mitigation or Fix	Implement a strict CORS policy that uses a whitelist of trusted domains instead of allowing all origins. Remove the wildcard from the Access-Control-Allow-Origin header and only specify domains that should be trusted. Additionally, if Access-Control-Allow-Credentials: true is set, ensure that only secure, trusted origins are allowed.

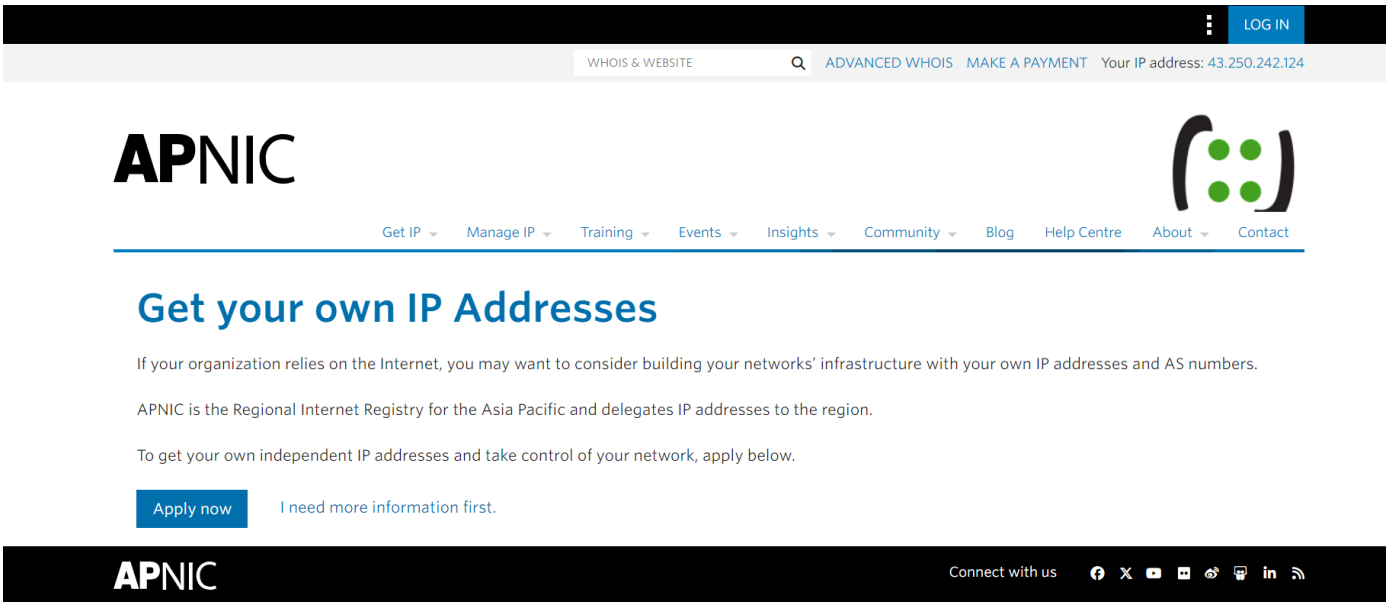
Report 06 Target Details



The target for this Bug Bounty report is **APNIC** (https://www.apnic.net), a platform providing digital solutions for businesses, including tools for marketing, sales, and customer management. The company offers a range of services such as digital advertising, reputation management, and APIs for integrating various business functions. APNIC's platform is designed to help businesses grow by offering scalable and efficient solutions, leveraging modern technologies.

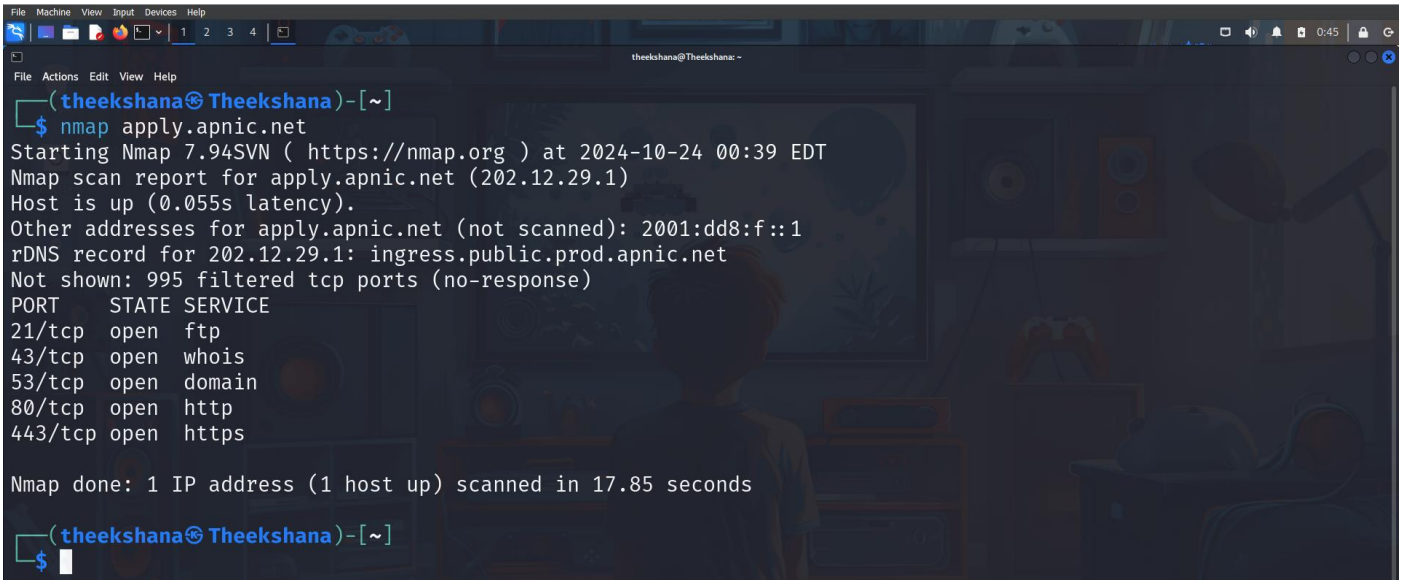
In this report, I have chosen to focus on 10 subdomains under the main domain **apnic.net** Each subdomain may serve different functionalities or services, potentially introducing distinct security risks, particularly in development or user-related areas. These subdomains were selected based on their relevance and the likelihood of containing vulnerabilities.

This report covers the findings for the subdomain: **apply.apnic.net**



Target Reconnaissance

Nmap Scan

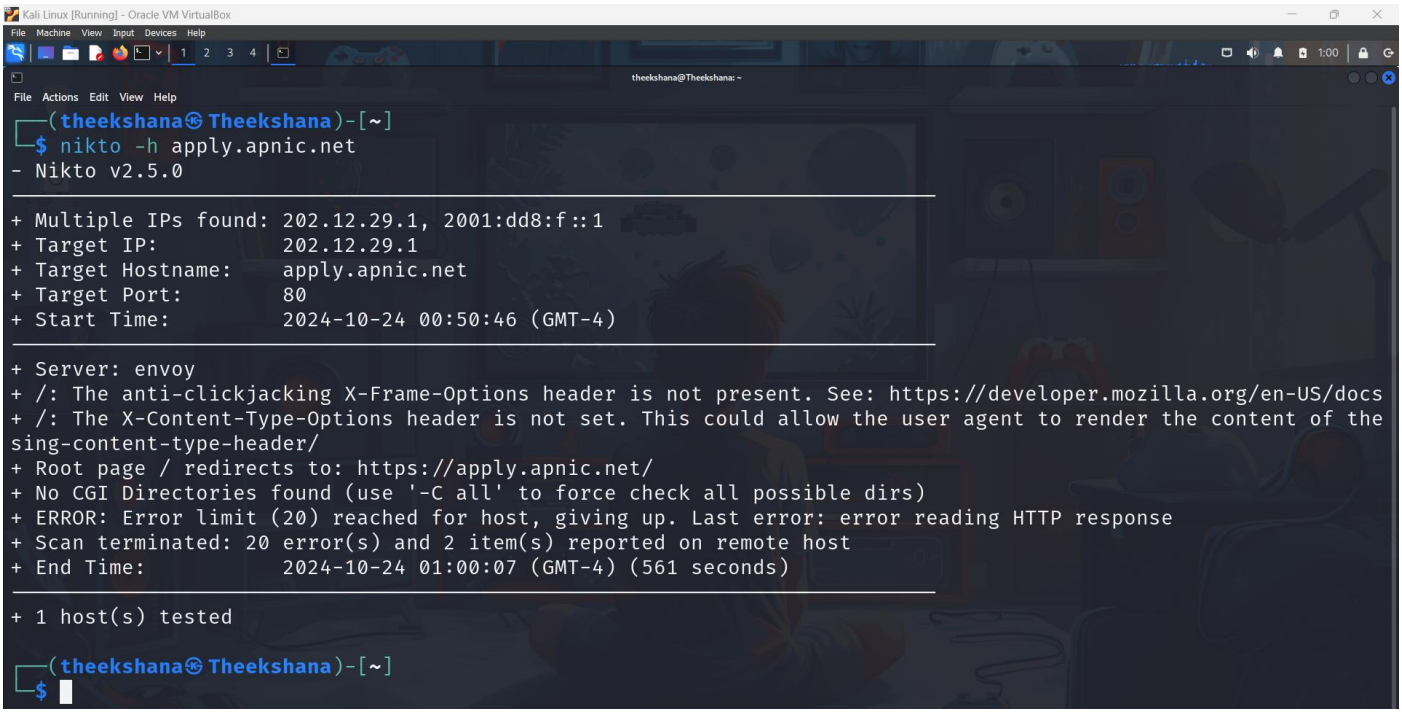


By scanning **apply.apnic.net** with Nmap I found out these information.

Port	State	Service
21/tcp	Open	FTP
43-tcp	Open	Whois
53/tcp	Open	DOMAIN
80/tcp	Open	HTTP
443/tcp	Open	HTPPS

Port	State	Service	Potential Vulnerabilities
21/tcp	Open	FTP	Data is not encrypted, so sensitive information can be stolen. Hackers can guess passwords (brute force attacks) Misconfigurations might allow unauthorized access
53/tcp	Open	DNS	Attackers can redirect users to fake sites (DNS poisoning) Hackers might flood the system (amplification attacks) Sensitive DNS info could be exposed (zone transfer)
80/tcp	Open	HTTP	Data is not secure (no encryption) Hackers can inject harmful scripts (XSS)
443/tcp	Open	HTTPS	If not properly secured, attackers can intercept data Older encryption protocols may be weak

Nikto Scan



The screenshot shows the output of a Nikto scan against the target **apply.apnic.net** which reveals several potential security issues and misconfigurations.

Initial Information:

- **Multiple IPs found**: The tool identifies two IP addresses (one IPv4 202.12.29.1 and one IPv6 2001:dd8:f::1) associated with the domain.
- **Target Hostname**: apply.apnic.net is confirmed as the target.
- **Target Port**: Port 80 (the default for HTTP) is being scanned.
- **Start Time**: The scan began at 00:50:46 GMT-4 on 2024-10-24.

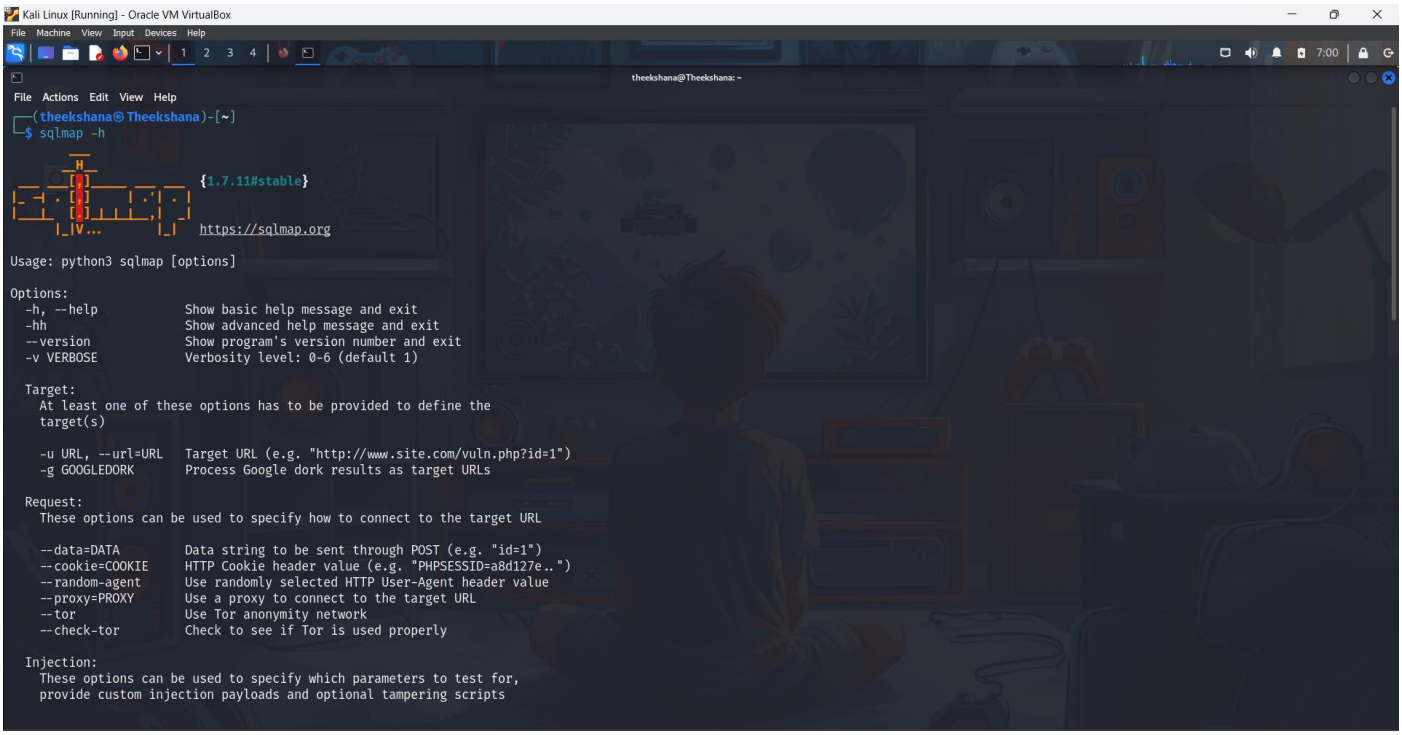
X-Frame-Options header missing: This header is not present, which could expose the site to **clickjacking attacks**. Without this, a malicious actor might embed the site in a hidden iframe on a malicious page and trick users into interacting with it.

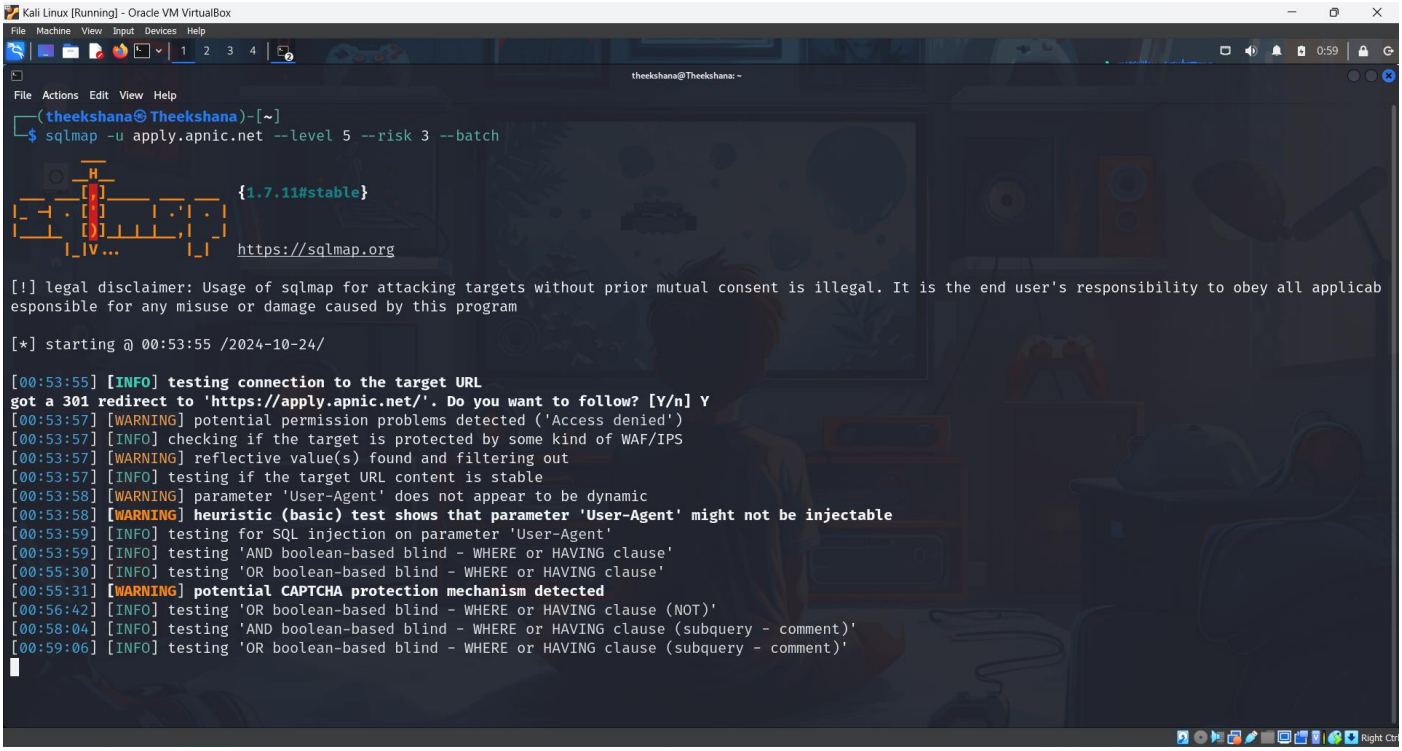
X-Content-Type-Options header missing: This could allow the browser to interpret files as the wrong MIME type, potentially causing security risks. The X-Content-Type-Options header helps prevent MIME type confusion attacks.

Errors:

- **Error limit reached**: The scan encountered an error limit after 20 errors, and the last error seems to have been related to reading an HTTP response.
- **Scan terminated**: The scan was stopped after reaching the error limit with a total of **20 errors** and **2 items** reported on the remote host.

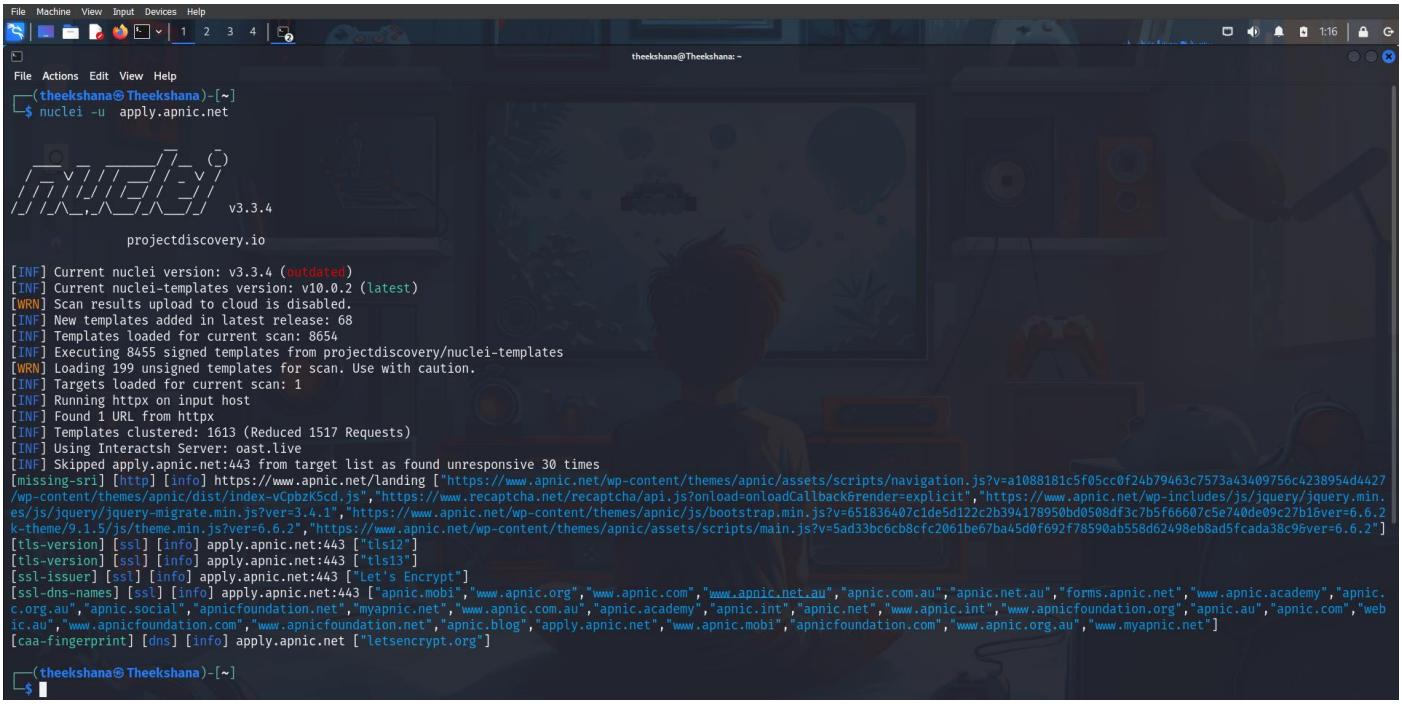
SQLmap Scaner





- **[WARNING] Potential permission problems**: The tool detects access restrictions, possibly caused by an application firewall (WAF) or intrusion prevention system (IPS).
- **[WARNING] Reflective value(s) found**: Indicates potential reflective vulnerabilities where input values are echoed back in the HTTP response.
- **[INFO] Testing for SQL injection on 'User-Agent'**: The tool tries to test if the User-Agent parameter (a typical HTTP header) is vulnerable to SQL injection.
- **[WARNING] Heuristic test shows that 'User-Agent' might not be injectable**: Early tests suggest that this parameter is not injectable.

Nuclei Scan



Scan Results:

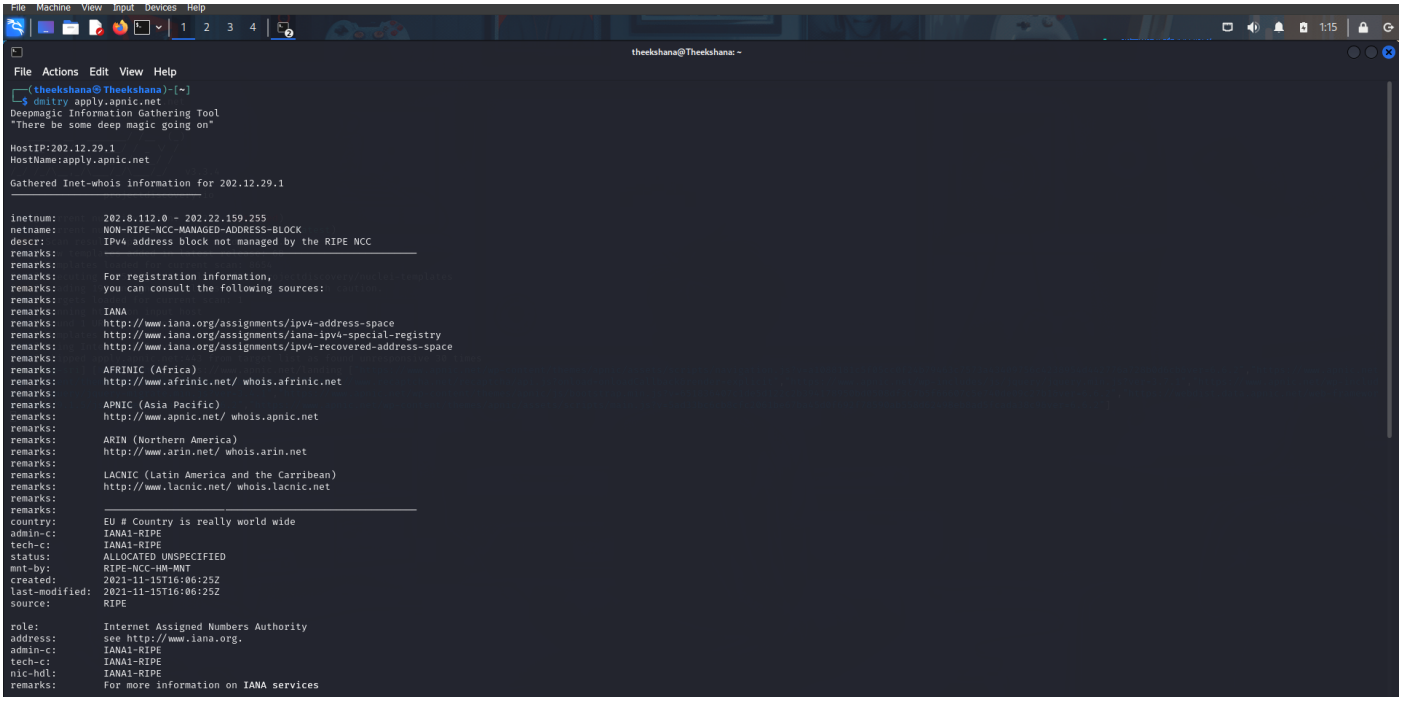
Missing Subresource Integrity (SRI): This might indicate that external JavaScript files loaded on the website (such as jQuery or Recaptcha) are not protected by an integrity hash. Without SRI, attackers could potentially inject malicious scripts.

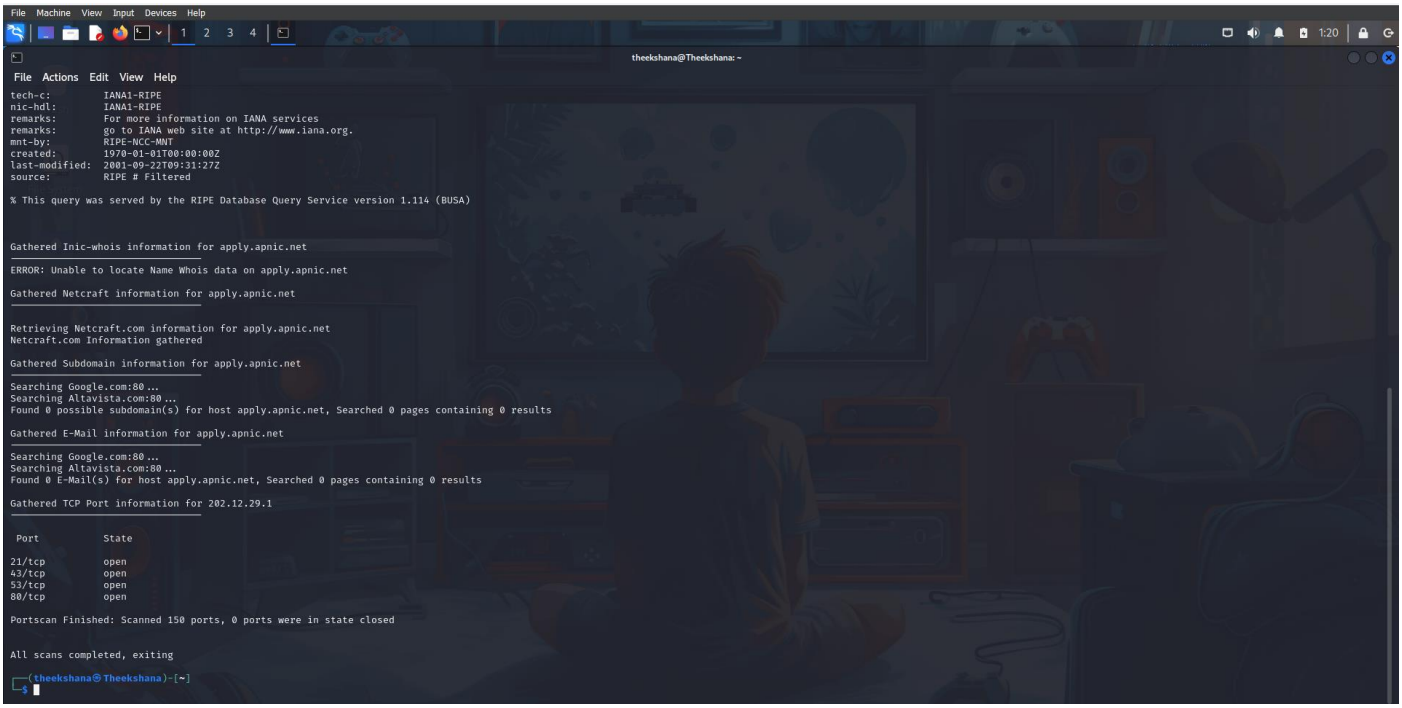
Unresponsive Target: The fact that the target is unresponsive several times might suggest a denial of service (DoS) issue or that the server is deliberately blocking scan attempts.

SSL/TLS Issues: If older versions of SSL/TLS were present, it could pose security risks. However, TLS 1.2 and 1.3 are considered secure

- Several security headers are missing or misconfigured, which are important for securing web applications. These include:
    - X-Frame-Options
    - Permissions-Policy
    - Referrer-Policy
    - X-Content-Type-Options
    - Cross-Origin-Embedder-Policy
    - Cross-Origin-Opener-Policy
    - Cross-Origin-Resource-Policy
    - Clear-Site-Data

Dmitry Scan



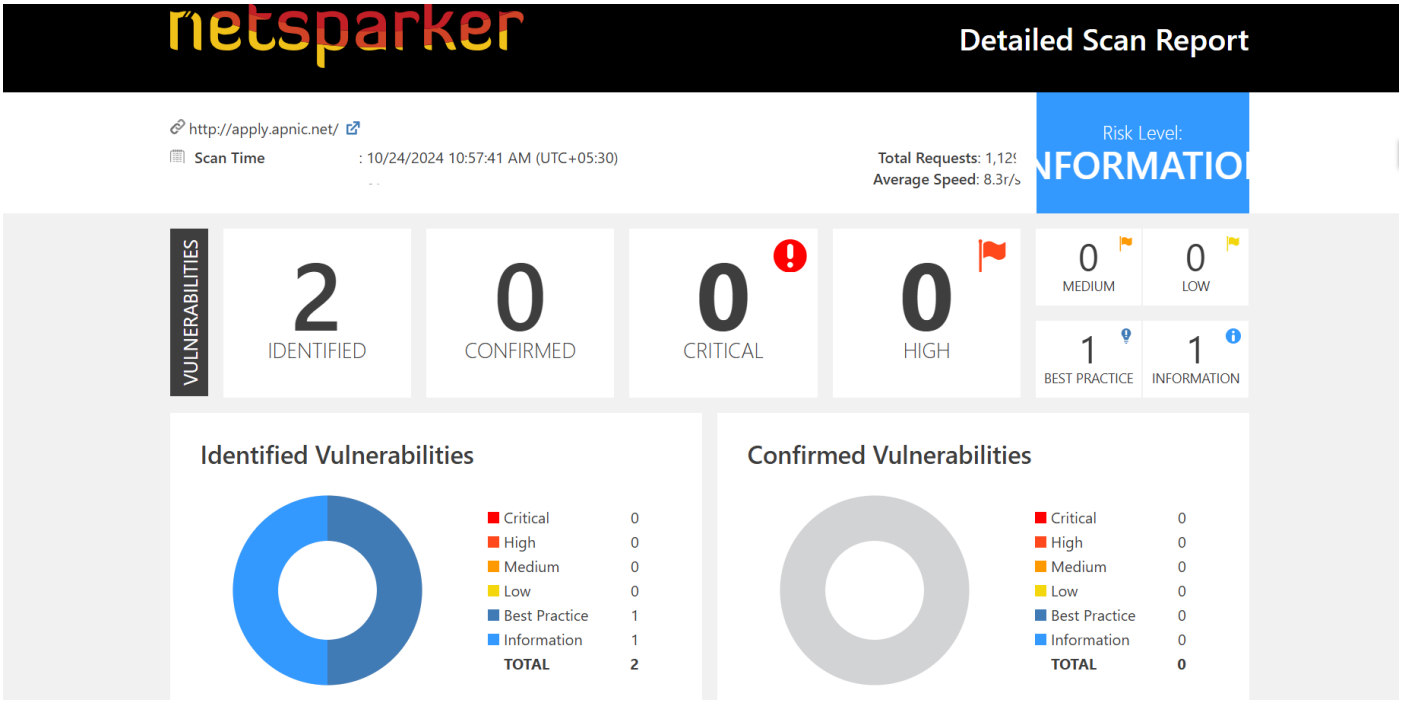


Port 21 (FTP - File Transfer Protocol): This port is typically used for file transfer services. Having FTP open can be risky if not properly secured, as it often transmits data in plain text (though secure variants like SFTP exist).

Port 53 (DNS - Domain Name System): This port is used for DNS services, which translate domain names into IP addresses. While DNS services need to be accessible, misconfigurations or vulnerabilities (like DNS amplification attacks) can expose the server to risks.

Port 80 (HTTP - Hypertext Transfer Protocol): This port is used for unencrypted web traffic. Port 80 being open suggests that the website is accessible via HTTP, but this should be redirected to HTTPS (Port 443) for encrypted communication. If not, it leaves the site vulnerable to man-in-the middle (MITM) attacks.

Netsparker



Vulnerability Summary

SEVERITY FILTER : CRITICAL HIGH MEDIUM LOW BEST PRACTICE INFORMATION

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Expect-CT Not Enabled	GET	https://apply.apnic.net/	
	HTTP Strict Transport Security (HSTS) Max-Age Value Too Low	GET	https://apply.apnic.net/	

1. Expect-CT Not Enabled

BEST PRACTICE 1

Netsparker identified that Expect-CT is not enabled.

Certificate Transparency is a technology that makes impossible (or at least very difficult) for a CA to issue an SSL certificate for a domain without the certificate being visible to the owner of that domain.

Google announced that, starting with April 2018, if it runs into a certificate that is not seen in Certificate Transparency (CT) Log, it will consider that certificate invalid and reject the connection. Thus sites should serve certificate that takes place in CT Logs. While handshaking, sites should serve a valid Signed Certificate Timestamp (SCT) along with the certificate itself.

Expect-CT can also be used for detecting the compatibility of the certificates that are issued before the April 2018 deadline. For instance, a certificate that was signed before April 2018, for 10 years it will be still posing a risk and can be ignored by the certificate transparency policy of the browser. By setting Expect-CT header, you can prevent misissused certificates to be used.

Vulnerabilities

1.1. https://apply.apnic.net/

Vulnerabilities

1.1. https://apply.apnic.net/

Hide Remediation

Remedy

Configure your web server to respond with Expect-CT header.

```
Expect-CT: enforce, max-age=7776000, report-uri="https://ABSOLUTE_REPORT_URL"
```

Note: We strongly suggest you to use Expect-CT header in **report-only mode**first. If everything goes well and your certificate is ready, go with the Expect-CT enforcemode. To use **report-only mode**first, omit **enforce**flag and see the browser's behavior with your deployed certificate.

```
Expect-CT: max-age=7776000, report-uri="https://ABSOLUTE_REPORT_URL"
```

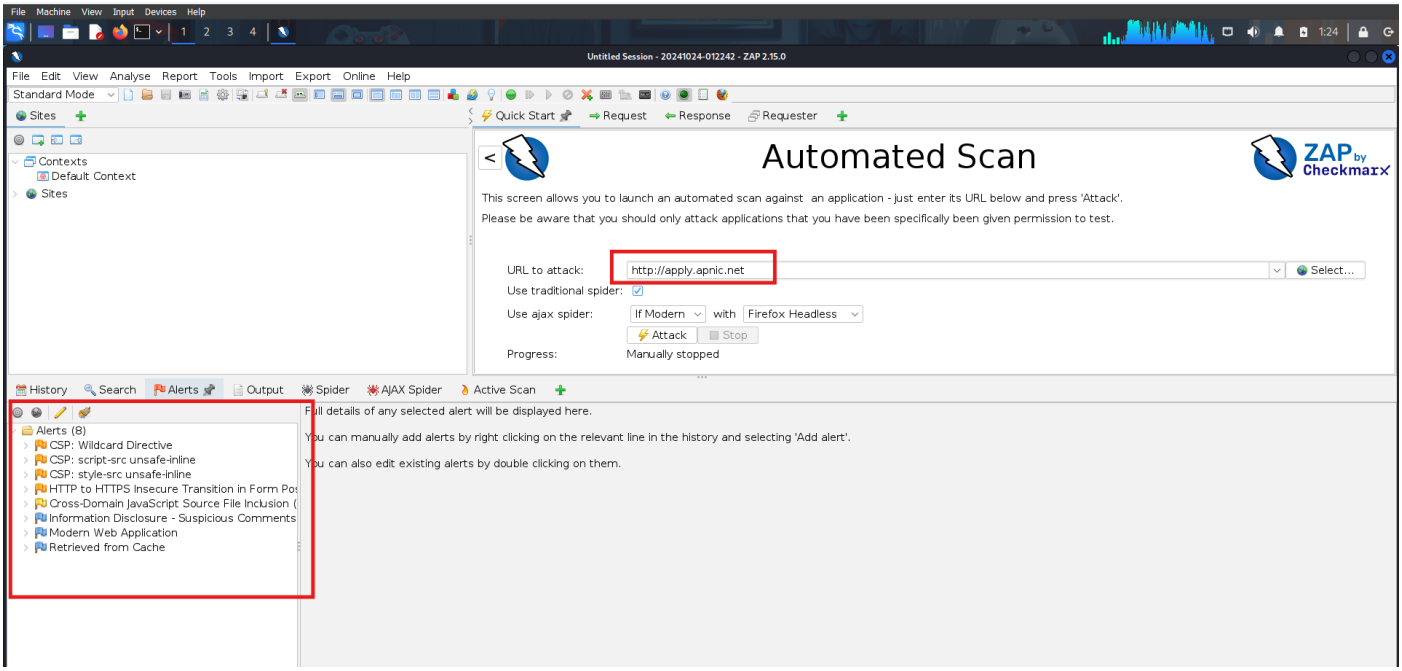
External References

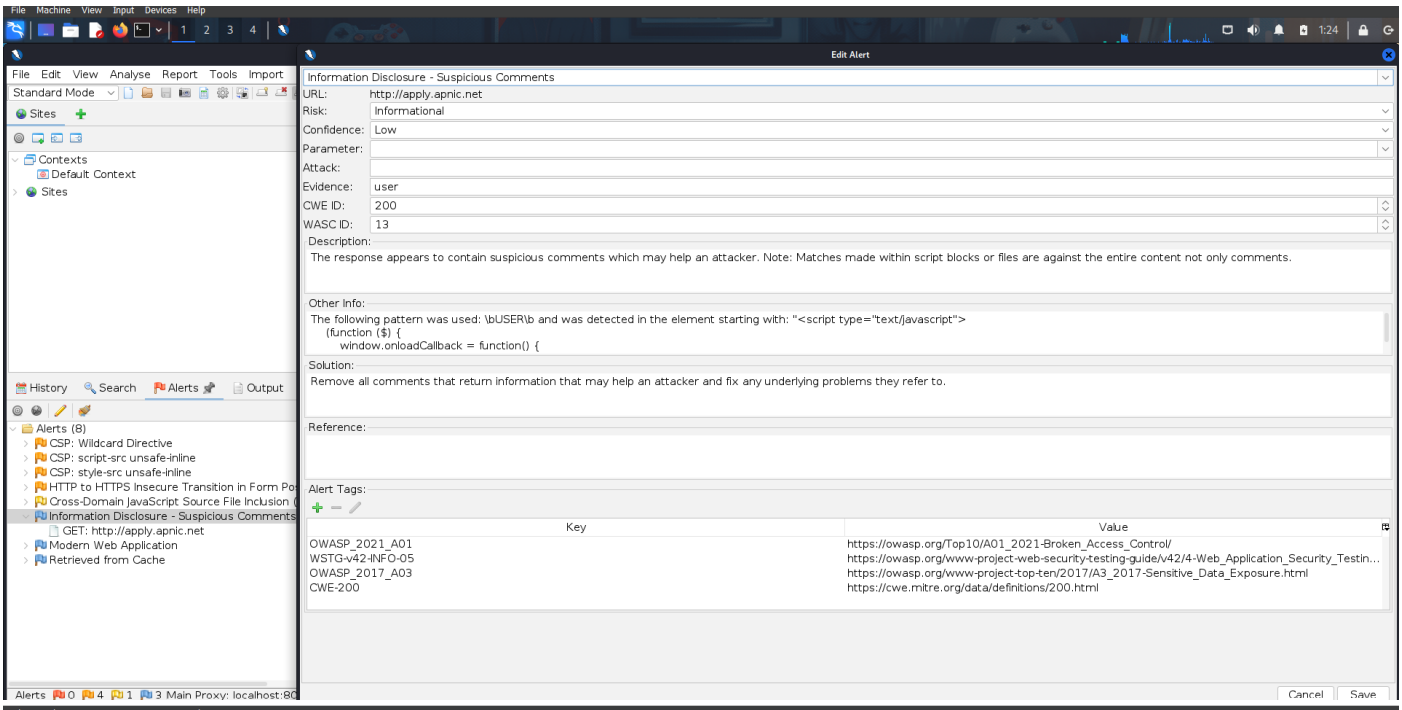
- Expect-CT Extension for HTTP
- Expect-CT HTTP Header
- Expect-CT Header

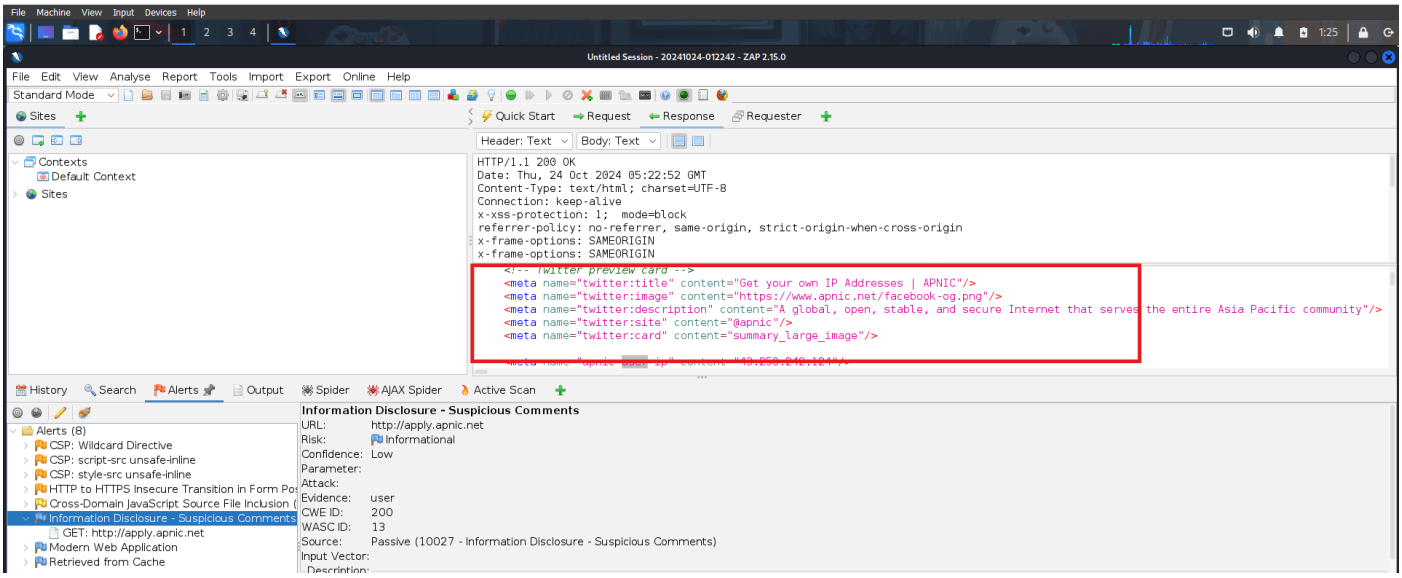
CLASSIFICATION

SANS Top 25	16
WASC	15
ISO27001	A.14.1.2

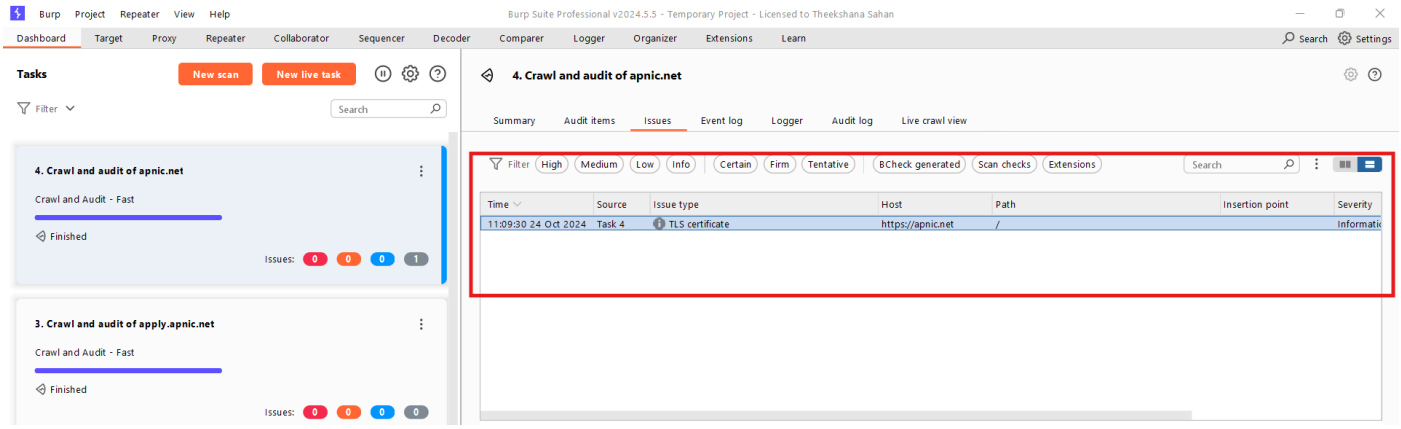
OWASP ZAP

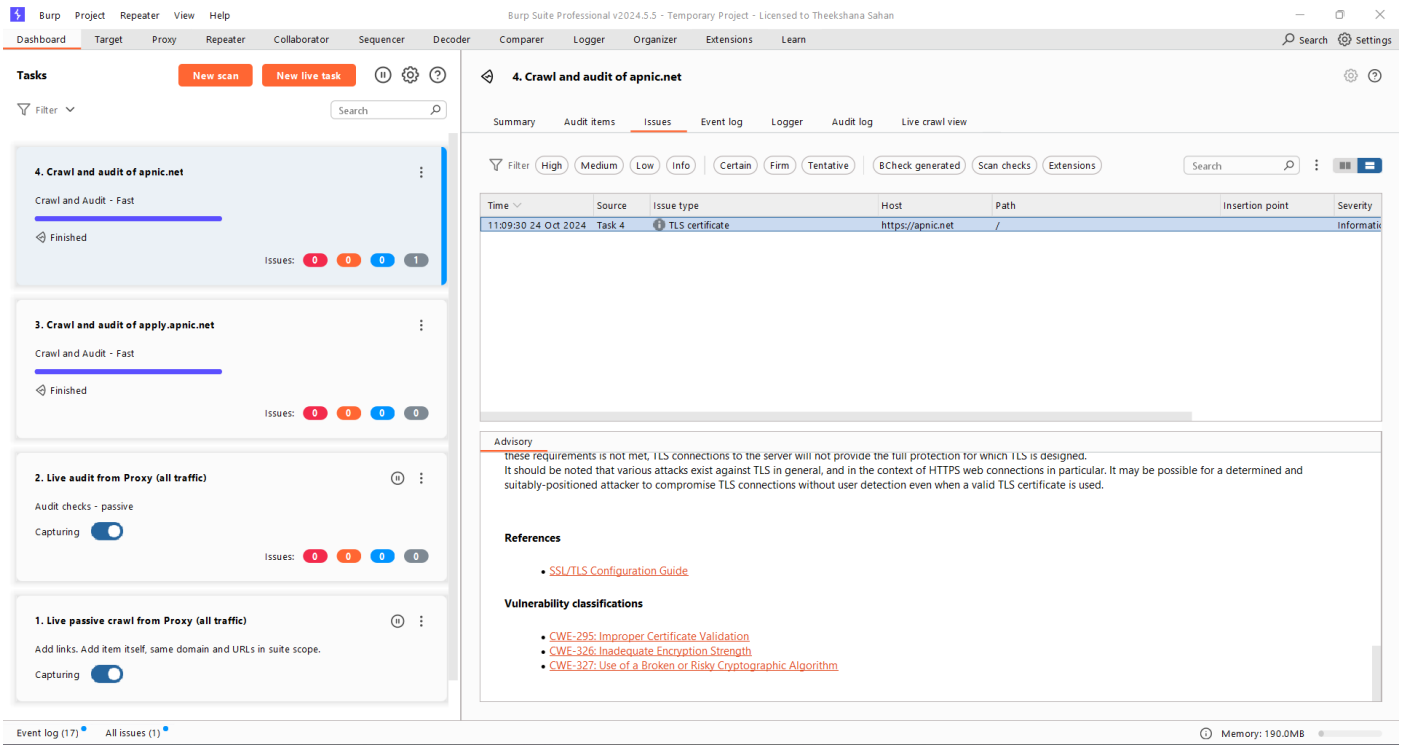

Untitled Session - 20241024-012242 - ZAP 2.15.0
Automated Scan
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack: http://apply.apnic.net
Use traditional spider:
Use ajax spider: If Modern with Firefox Headless
Attack
Stop
Progress: Manually stopped
Alerts (8)
CSP: Wildcard Directive
CSP: script-src unsafe-inline
CSP: style-src unsafe-inline
HTTP to HTTPS Insecure Transition in Form Post
Cross-Domain JavaScript Source File Inclusion
Information Disclosure - Suspicious Comments
Modern Web Application
Retrieved from Cache

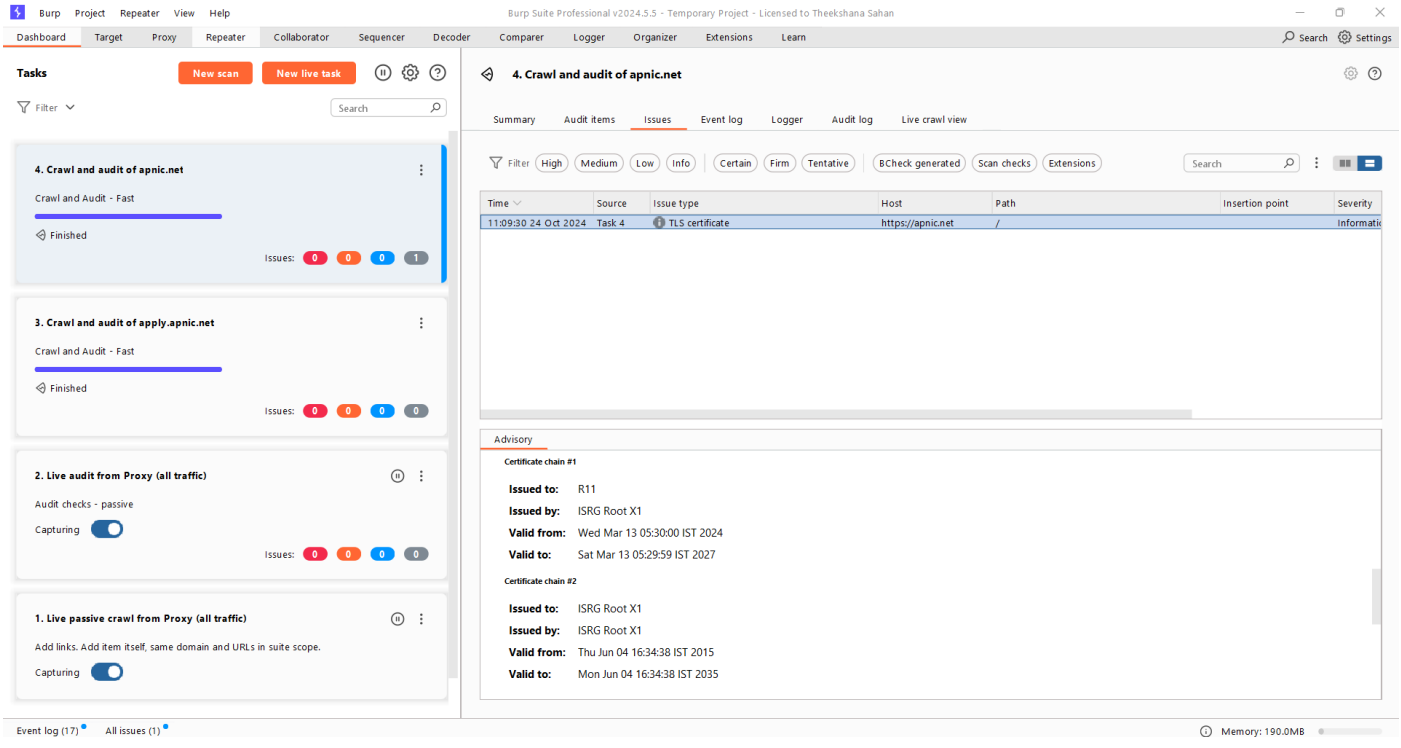

Edit Alert
Information Disclosure - Suspicious Comments
URL: http://apply.apnic.net
Risk: Informational
Confidence: Low
Parameter:
Attack:
Evidence: user
CWE ID: 200
WASC ID: 13
Description:
The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Other Info:
The following pattern was used: \bUSER\b and was detected in the element starting with: "<script type="text/javascript">
(function ($) {
window.onloadCallback = function() {
Solution:
Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference:
Alert Tags:
Key
Value
OWASP_2021_A01
https://owasp.org/Top10/A01_2021-Broken_Access_Control/
WSTG-v42-INFO-05
https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testin...
OWASP_2017_A03
https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html
CWE-200
https://cwe.mitre.org/data/definitions/200.html
Cancel
Save


Untitled Session - 20241024-012242 - ZAP 2.15.0
HTTP/1.1 200 OK
Date: Thu, 24 Oct 2024 05:22:52 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
x-xss-protection: 1; mode=block
referrer-policy: no-referrer, same-origin, strict-origin-when-cross-origin
x-frame-options: SAMEORIGIN
x-frame-options: SAMEORIGIN
<!-- Twitter preview card -->
<meta name="twitter:title" content="Get your own IP Addresses | APNIC"/>
<meta name="twitter:image" content="https://www.apnic.net/facebook-og.png"/>
<meta name="twitter:description" content="A global, open, stable, and secure Internet that serves the entire Asia Pacific community"/>
<meta name="twitter:site" content="@apnic"/>
<meta name="twitter:card" content="summary_large_image"/>
Information Disclosure - Suspicious Comments
URL: http://apply.apnic.net
Risk: Informational
Confidence: Low
Parameter:
Attack:
Evidence: user
CWE ID: 200
WASC ID: 13
Source: Passive (10027 - Information Disclosure - Suspicious Comments)
Input Vector:

Burp Suite


Burp Project Repeater View Help
Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan
Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Tasks
New scan
New live task
4. Crawl and audit of apnic.net
Crawl and Audit - Fast
Finished
Issues:
3. Crawl and audit of apply.apnic.net
Crawl and Audit - Fast
Finished
Issues:
4. Crawl and audit of apnic.net
Summary Audit items Issues Event log Logger Audit log Live crawl view
Filter High Medium Low Info Certain Firm Tentative BCheck generated Scan checks Extensions
Search
Time Source Issue type Host Path Insertion point Severity
11:09:30 24 Oct 2024 Task 4 TLS certificate https://apnic.net /


Burp Project Repeater View Help
Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan
Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Tasks
New scan
New live task
4. Crawl and audit of apnic.net
Crawl and Audit - Fast
Finished
Issues:
3. Crawl and audit of apply.apnic.net
Crawl and Audit - Fast
Finished
Issues:
2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing
Issues:
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing
4. Crawl and audit of apnic.net
Summary Audit items Issues Event log Logger Audit log Live crawl view
Filter High Medium Low Info Certain Firm Tentative BCheck generated Scan checks Extensions
Search
Time Source Issue type Host Path Insertion point Severity
11:09:30 24 Oct 2024 Task 4 TLS certificate https://apnic.net /
Advisory
these requirements is not met, TLS connections to the server will not provide the full protection for which TLS is designed.
It should be noted that various attacks exist against TLS in general, and in the context of HTTPS web connections in particular. It may be possible for a determined and suitably-positioned attacker to compromise TLS connections without user detection even when a valid TLS certificate is used.
References
SSL/TLS Configuration Guide
Vulnerability classifications
CWE-295: Improper Certificate Validation
CWE-326: Inadequate Encryption Strength
CWE-327: Use of a Broken or Risky Cryptographic Algorithm
Event log (17)
All issues (1)
Memory: 190.0MB

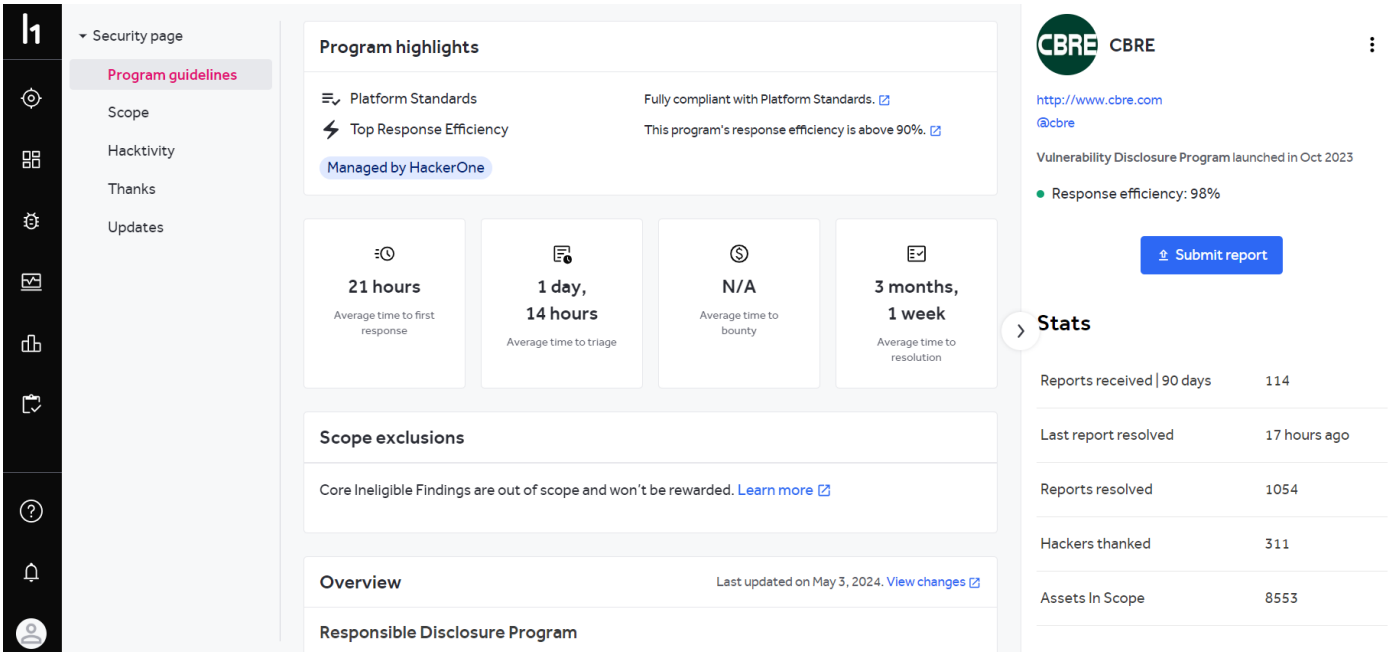

Burp Project Repeater View Help
Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan
Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Tasks
New scan
New live task
4. Crawl and audit of apnic.net
Crawl and Audit - Fast
Finished
Issues:
3. Crawl and audit of apply.apnic.net
Crawl and Audit - Fast
Finished
Issues:
2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing
Issues:
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing
4. Crawl and audit of apnic.net
Summary Audit items Issues Event log Logger Audit log Live crawl view
Filter High Medium Low Info Certain Firm Tentative BCheck generated Scan checks Extensions
Search
Time Source Issue type Host Path Insertion point Severity
11:09:30 24 Oct 2024 Task 4 TLS certificate https://apnic.net /
Advisory
Certificate chain #1
Issued to: R11
Issued by: ISRG Root X1
Valid from: Wed Mar 13 05:30:00 IST 2024
Valid to: Sat Mar 13 05:29:59 IST 2027
Certificate chain #2
Issued to: ISRG Root X1
Issued by: ISRG Root X1
Valid from: Thu Jun 04 16:34:38 IST 2015
Valid to: Mon Jun 04 16:34:38 IST 2035
Event log (17)
All issues (1)
Memory: 190.0MB

Vulnerabilities:

1 Link manipulation (DOM-based)

Vulnerability Title	Link manipulation (DOM-based)
Vulnerability Description	The application is vulnerable to DOM-based link manipulation. Data is read from location.href and passed to element.setAttribute.href, potentially allowing attackers to manipulate navigation targets. This can lead to phishing, unintended actions, or bypassing anti-XSS defenses if a user visits a crafted URL.
Affected Components	Client-side JavaScript code manipulating links and form submission URLs using data from location.href. DOM elements where the link target or form submission URL is set dynamically. Navigation functionalities within the application that use dynamic URL setting based on user input or URL parameters.
Impact Assessment	May allow attackers to manipulate the target URLs of links within the application. Users could be redirected to phishing sites, enabling attackers to steal credentials or sensitive information. Sensitive form data might be sent to an attacker's server.
Steps to Reproduce	Access a page in the application where link targets or form submission URLs are set based on the URL. Modify the URL to include malicious values (?redirectUrl=https://malicious site.com) Observe if the application updates the link target to the attacker-controlled URL.
Proof of Concept	**apply.apnic.net** in an unsecured network. Use network analysis tools to observe traffic and confirm it's unencrypted.
Proposed Mitigation or Fix	Avoid dynamically setting link targets or form submission URLs using untrusted data. Implement a whitelist of permitted URLs and validate the target URL against this list before setting it dynamically. Sanitize and validate user input to prevent malicious data from influencing the URL.

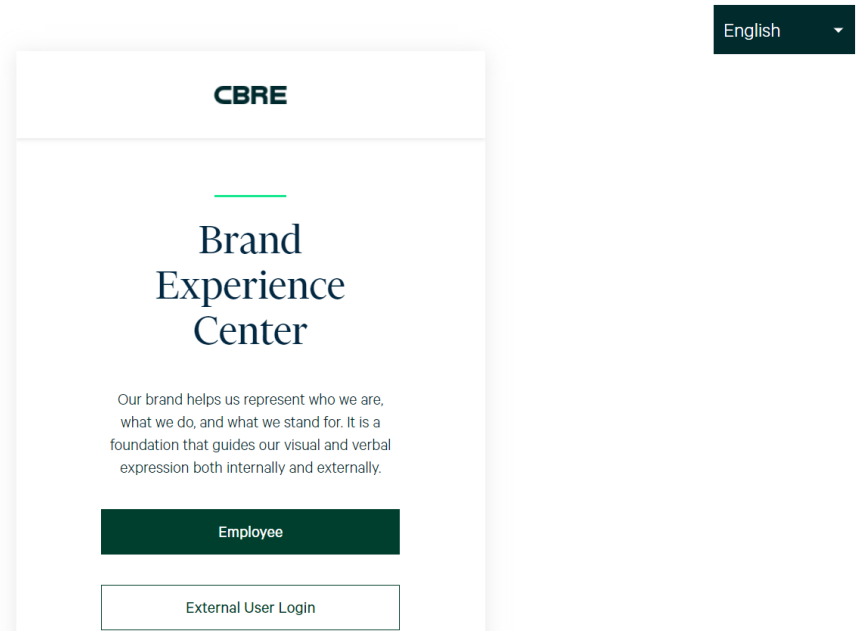
Report 07 Target Details



The target for this Bug Bounty report is CBRE (https://www.cbre.com), a platform providing digital solutions for businesses, including tools for marketing, sales, and customer management. The company offers a range of services such as digital advertising, reputation management, and APIs for integrating various business functions. CBRE's platform is designed to help businesses grow by offering scalable and efficient solutions, leveraging modern technologies.

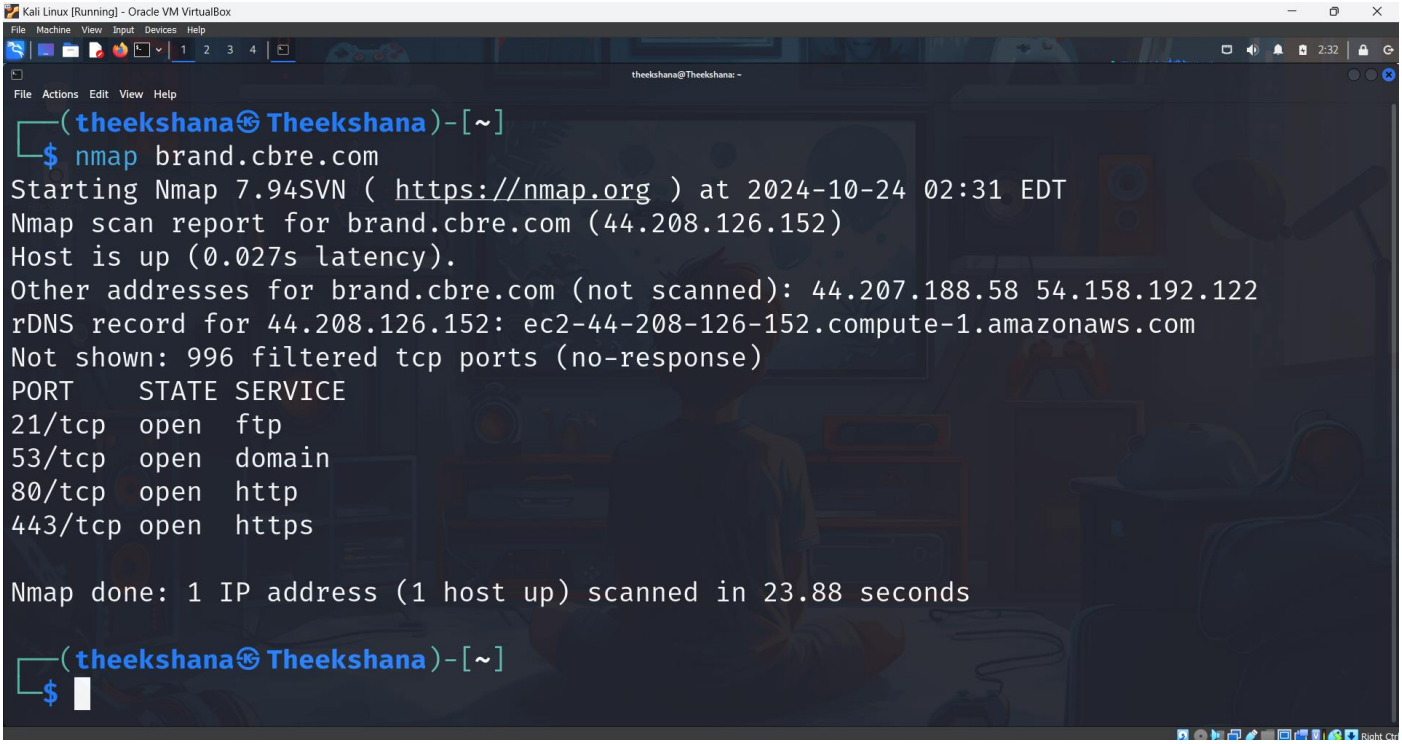
In this report, I have chosen to focus on 10 subdomains under the main domain cbre.com. Each subdomain may serve different functionalities or services, potentially introducing distinct security risks, particularly in development or user-related areas. These subdomains were selected based on their relevance and the likelihood of containing vulnerabilities.

This report covers the findings for the subdomain: brand.cbre.com



Target Reconnaissance

Nmap Scan



By scanning brand.cbre.com with Nmap I found out these information.

Port	State	Service
21/tcp	Open	FTP
53/tcp	Open	DOMAIN
80/tcp	Open	HTTP
443/tcp	Open	HTPPS

Port	State	Service	Potential Vulnerabilities
21/tcp	Open	FTP	Data is not encrypted, so sensitive information can be stolen. Hackers can guess passwords (brute force attacks) Misconfigurations might allow unauthorized access
53/tcp	Open	DNS	Attackers can redirect users to fake sites (DNS poisoning) Hackers might flood the system (amplification attacks) Sensitive DNS info could be exposed (zone transfer)
80/tcp	Open	HTTP	Data is not secure (no encryption) Hackers can inject harmful scripts (XSS)
443/tcp	Open	HTTPS	If not properly secured, attackers can intercept data Older encryption protocols may be weak

Nikto Scan

The screenshot shows the output of a Nikto scan against the target brand.cbre.com which reveals several potential security issues and misconfigurations.

Target Information:

- **Target IP**: 54.158.192.122 (the chosen IP for the scan)
- **Target Hostname**: brand.cbre.com
- **Target Port**: 80 (indicating an HTTP connection)

Server Information:

- **Server**: No banner was retrieved, meaning the server did not reveal what software (like Apache or Nginx) it's running.

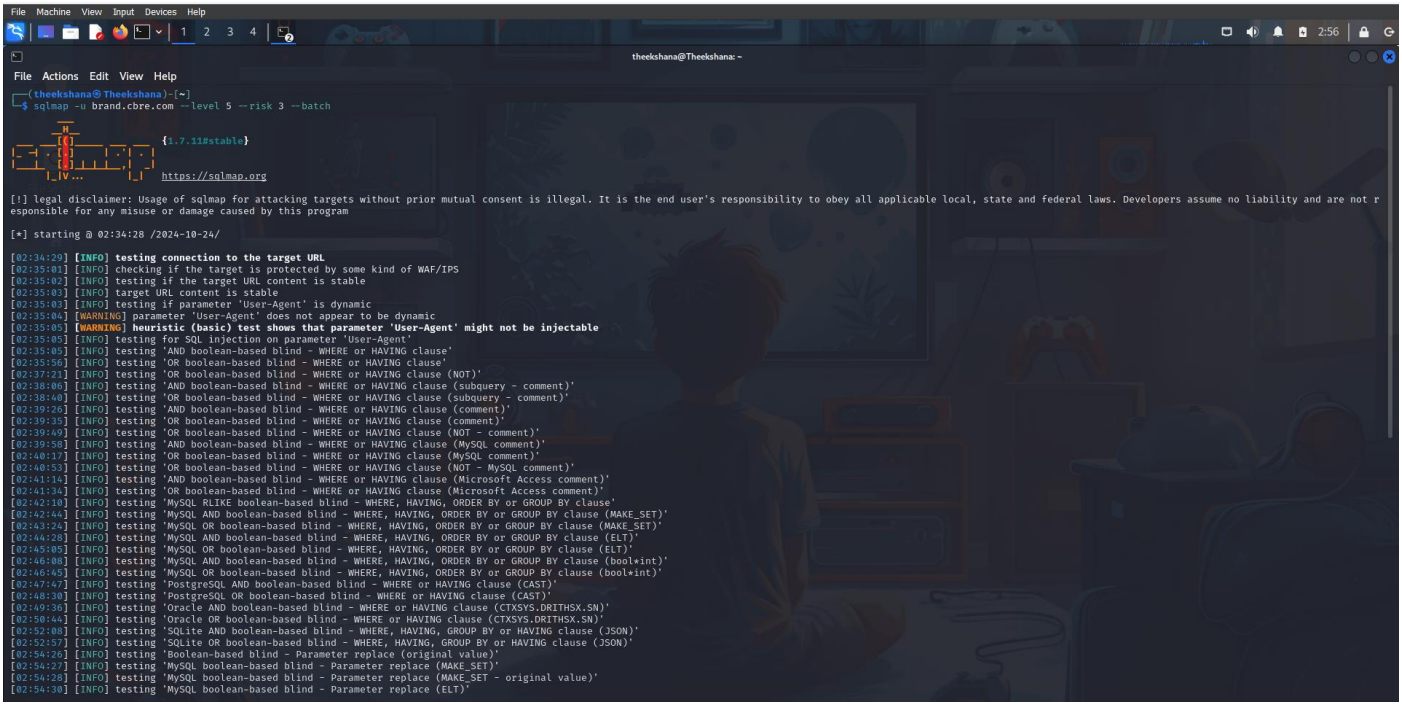
Findings:

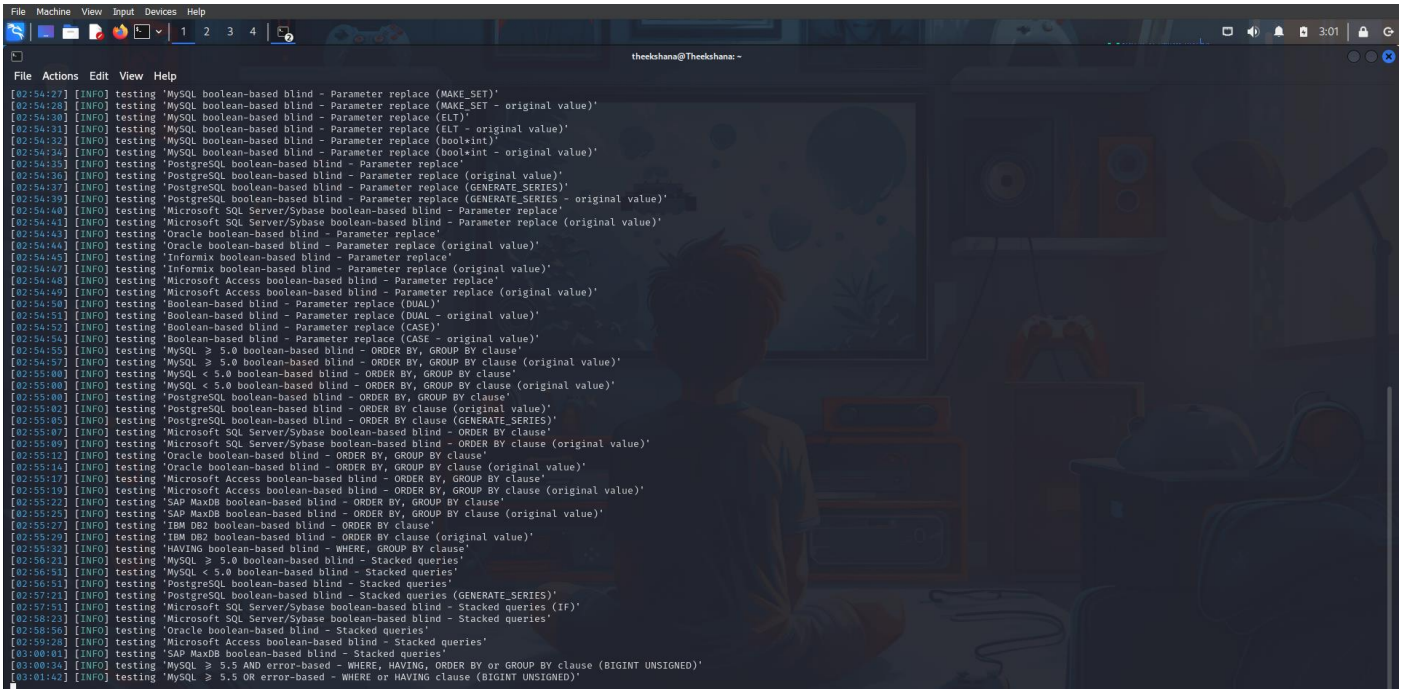
- The server has an Access-Control-Allow-Origin header set to . This means the server allows resources to be accessed by any domain, which could be risky depending on the context.

- The root page redirects to https://brand.cbre.com (HTTP to HTTPS redirection).

- **X-Content-Type-Options** header is not set. This could allow the browser to interpret files in ways that could introduce security vulnerabilities (e.g., MIME type confusion).

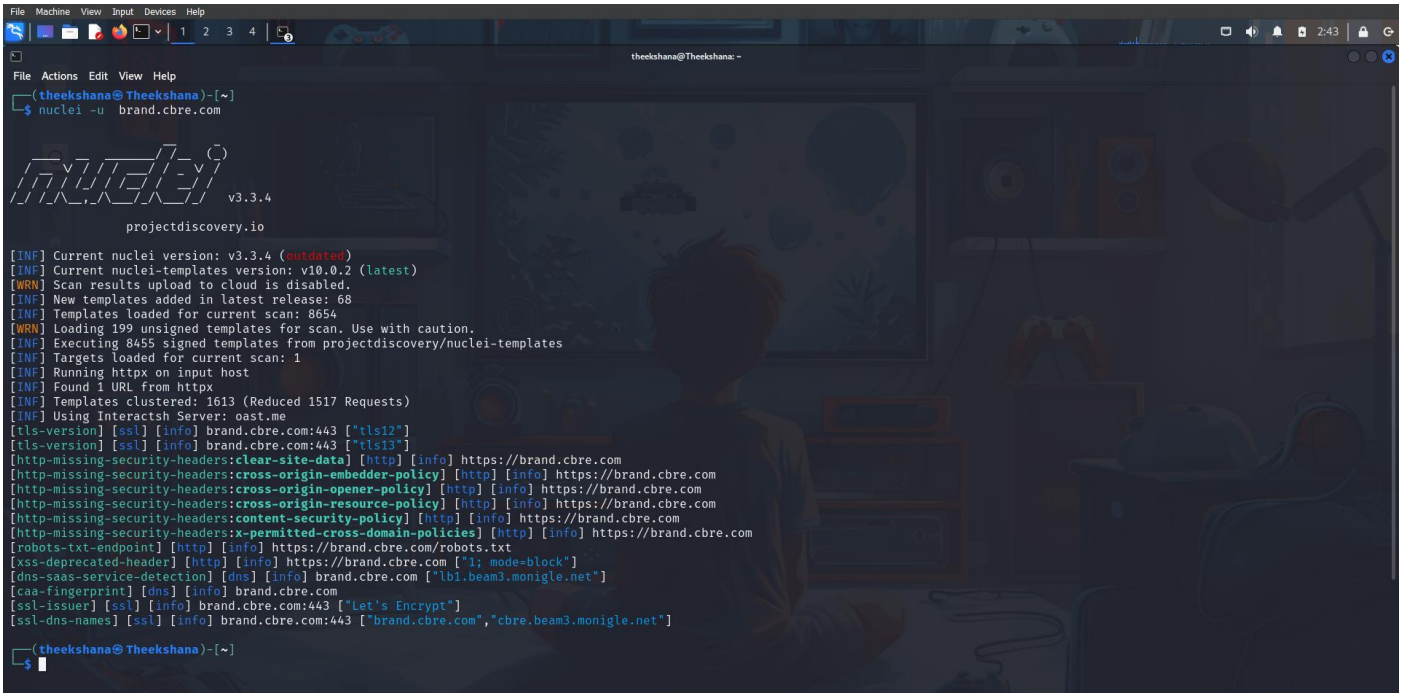
SQLmap Scaner





- **[WARNING] Potential permission problems**: The tool detects access restrictions, possibly caused by an application firewall (WAF) or intrusion prevention system (IPS).
- **[WARNING] Reflective value(s) found**: Indicates potential reflective vulnerabilities where input values are echoed back in the HTTP response.
- **[INFO] Testing for SQL injection on 'User-Agent'**: The tool tries to test if the User-Agent parameter (a typical HTTP header) is vulnerable to SQL injection.
- **[WARNING] Heuristic test shows that 'User-Agent' might not be injectable**: Early tests suggest that this parameter is not injectable.

Nuclei Scan



Missing Security Headers:

- **Clear Site Data**: Not implemented. This can help in clearing cookies, cache, and storage data, enhancing privacy and preventing cache-related attacks.
- **Cross-Origin-Embedder-Policy**: Not implemented. This can prevent embedding malicious content by controlling resources loaded by the page.
- **Cross-Origin-Opener-Policy**: Not implemented. This helps isolate browsing contexts to prevent cross-origin attacks.
- **Cross-Origin-Resource-Policy**: Not implemented. This can block cross-origin resource loads that may be unnecessary.
- **Content-Security-Policy**: Not implemented. This is crucial for preventing various types of attacks such as XSS (Cross-Site Scripting) by restricting resources the page can load.
- **X-Permitted-Cross-Domain-Policies**: Not implemented. This limits or allows Adobe Flash and other plugins to handle data across domains.

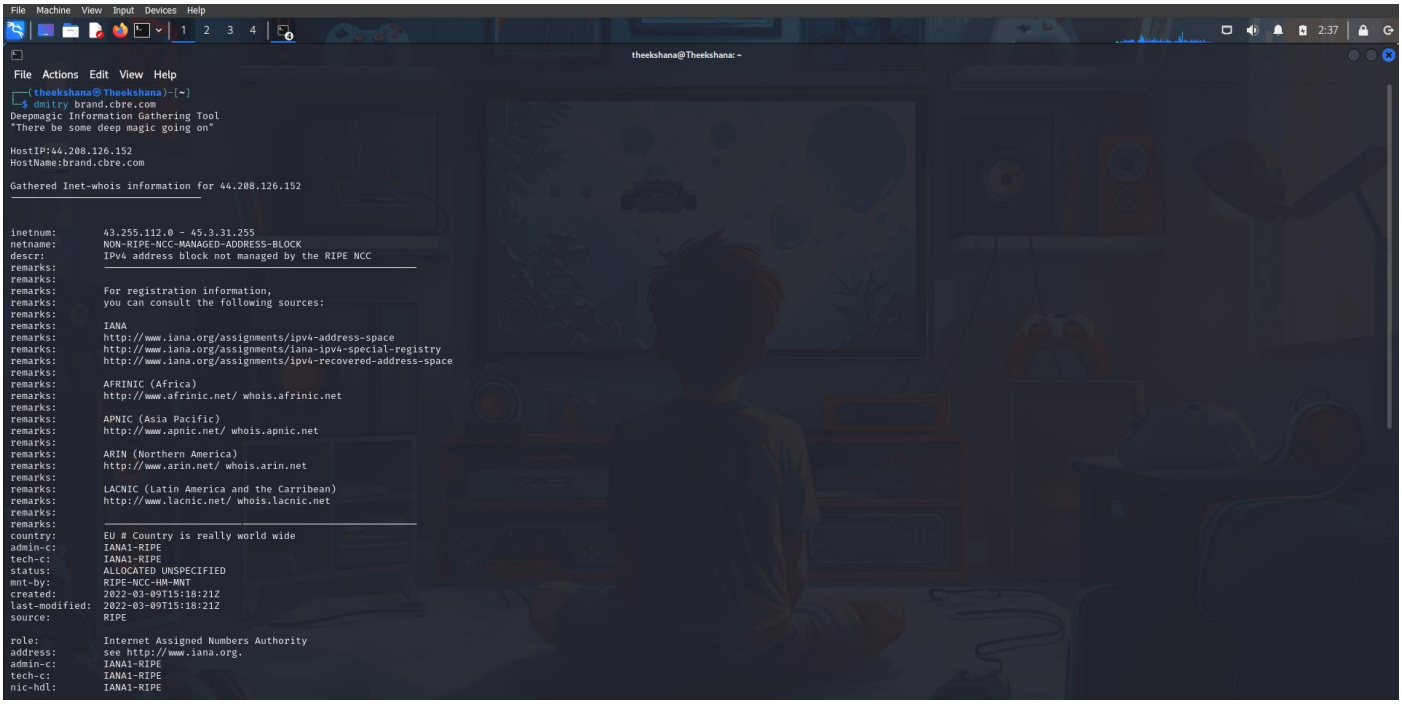
Robots.txt File Missing:

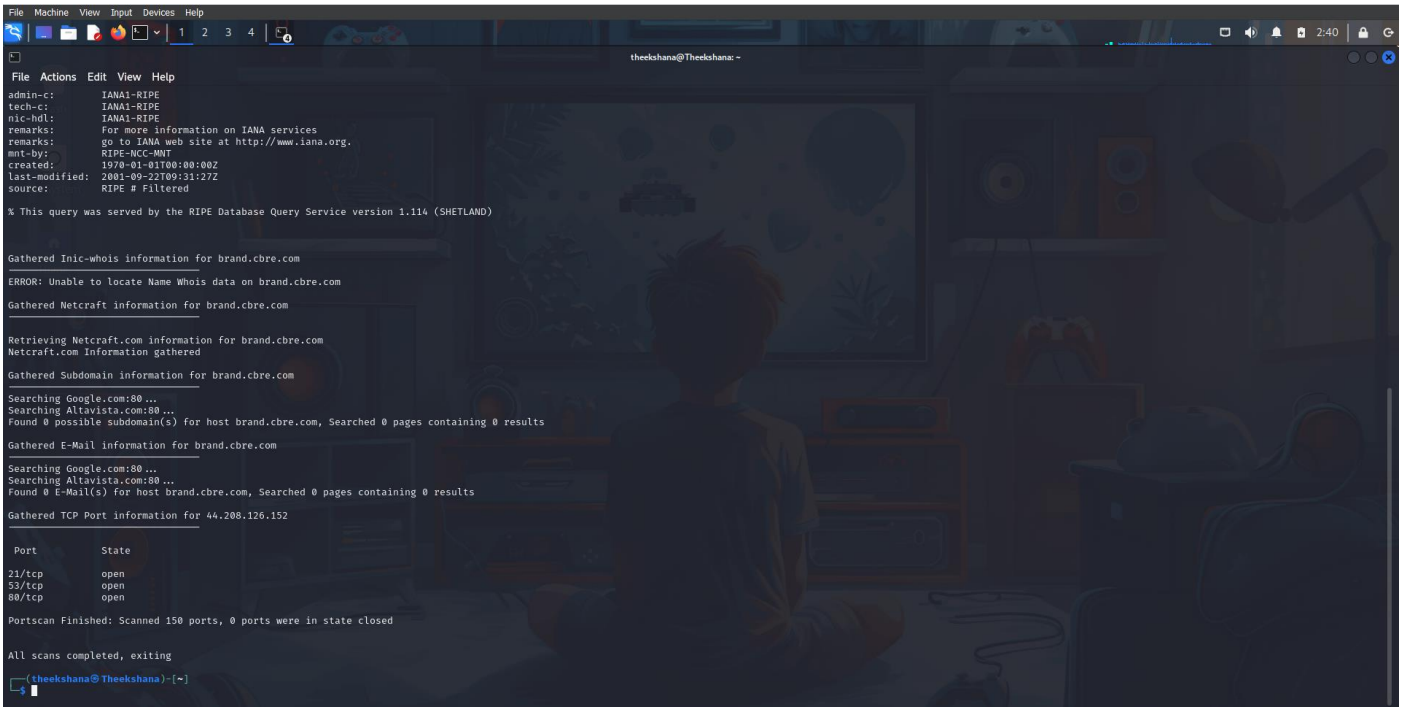
- The scan also reveals the lack of a robots.txt file at https://brand.cbre.com/robots.txt. While not a critical issue, this file is typically used to manage search engine indexing and can sometimes expose sensitive directories if misconfigured.

XSS-Deprecated Header:

- There seems to be an old header related to cross-site scripting. It might be worth investigating or updating to ensure compatibility and security

Dmitry Scan



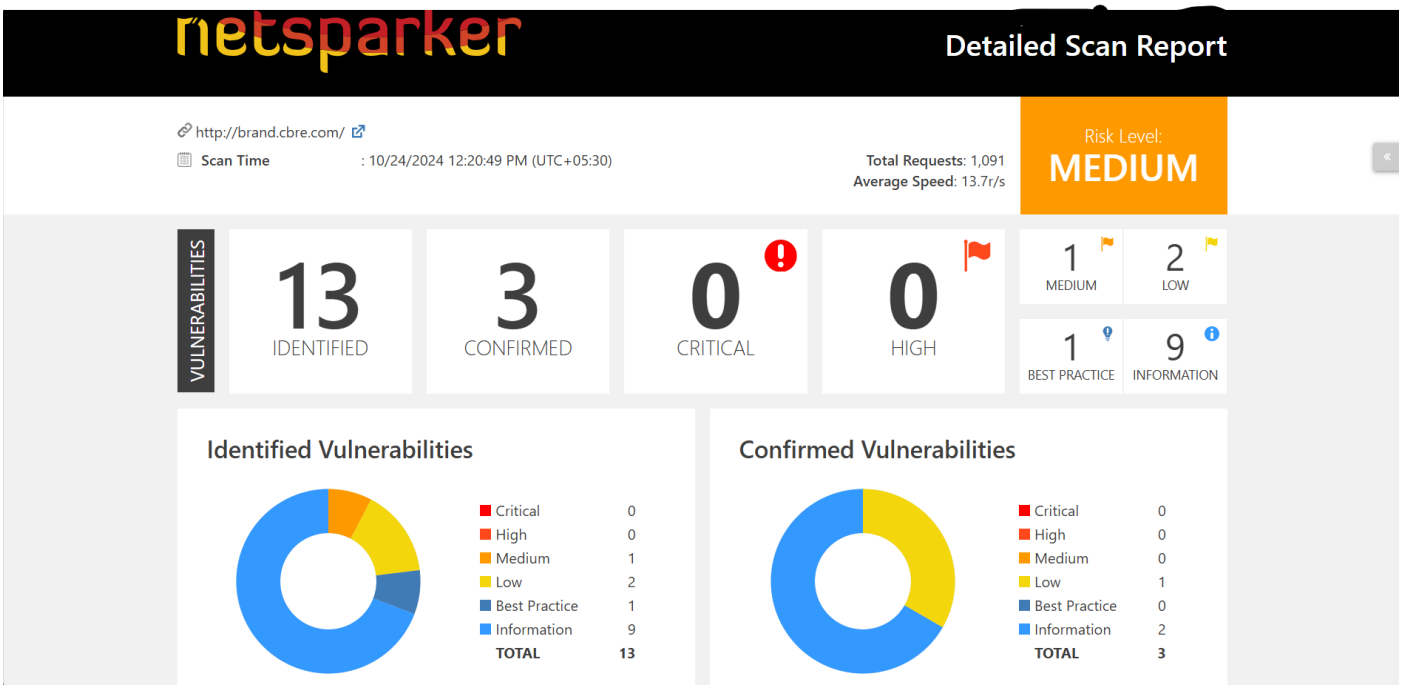


Port 21 (FTP - File Transfer Protocol): This port is typically used for file transfer services. Having FTP open can be risky if not properly secured, as it often transmits data in plain text (though secure variants like SFTP exist).

Port 53 (DNS - Domain Name System): This port is used for DNS services, which translate domain names into IP addresses. While DNS services need to be accessible, misconfigurations or vulnerabilities (like DNS amplification attacks) can expose the server to risks.

Port 80 (HTTP - Hypertext Transfer Protocol): This port is used for unencrypted web traffic. Port 80 being open suggests that the website is accessible via HTTP, but this should be redirected to HTTPS (Port 443) for encrypted communication. If not, it leaves the site vulnerable to man-in-the middle (MITM) attacks.

Netsparker



Vulnerability Summary

SEVERITY FILTER : CRITICAL HIGH MEDIUM LOW BEST PRACTICE INFORMATION

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://brand.cbre.com/	
	Misconfigured Access-Control-Allow-Origin Header	GET	http://brand.cbre.com/	
	Cookie Not Marked as HttpOnly	GET	https://brand.cbre.com/	
	Expect-CT Not Enabled	GET	https://brand.cbre.com/	
	Content Security Policy (CSP) Nonce Without Matching Script Block	GET	https://brand.cbre.com/	
	data: Used in a Content Security Policy (CSP) Directive	GET	https://brand.cbre.com/	
	HTTP Strict Transport Security (HSTS) Max-Age Value Too Low	GET	https://brand.cbre.com/	
	HTTP Strict Transport Security (HSTS) via HTTP	GET	http://brand.cbre.com/	
	Nonce Usage Detected in Content Security Policy (CSP) Directive	GET	https://brand.cbre.com/	
	Scheme URI Detected in Content Security Policy (CSP) Directive	GET	https://brand.cbre.com/	
	Weak Nonce Detected in Content Security Policy (CSP) Declaration	GET	https://brand.cbre.com/	
	Cross-site Referrer Leakage through Referrer-Policy	GET	https://brand.cbre.com/	
	Forbidden Resource	GET	https://brand.cbre.com/assets/?hTTp://r87.com/n	

Misconfigured Access-Control-Allow-Origin Header

LOW 1

Netsparker detected a possibly misconfigured Access-Control-Allow-Origin header in resource's HTTP response.

Cross-origin resource sharing (CORS) is a mechanism that allows resources on a web page to be requested outside the domain through XMLHttpRequest.

Unless this HTTP header is present, such "cross-domain" requests are forbidden by web browsers, per the same-origin security policy.

Impact

This is generally not appropriate when using the same-origin security policy. The only case where this is appropriate when using the same-origin policy is when a page or API response is considered completely public content and it is intended to be accessible to everyone.

Vulnerabilities

3.1. http://brand.cbre.com/

Hide Remediation

Remedy

If this page is intended to be accessible to everyone, you don't need to take any action. Otherwise please follow the guidelines for different architectures below in order to set this header and permit outside domain.

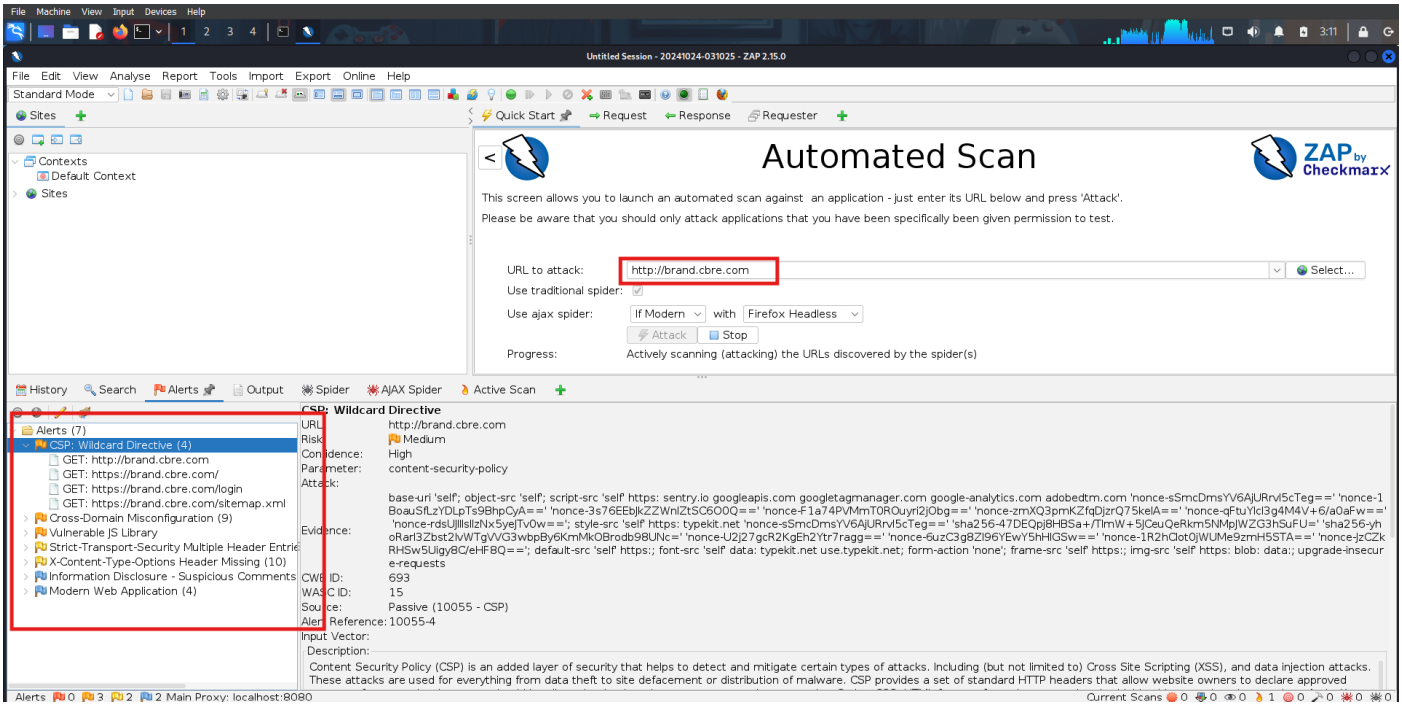
Apache

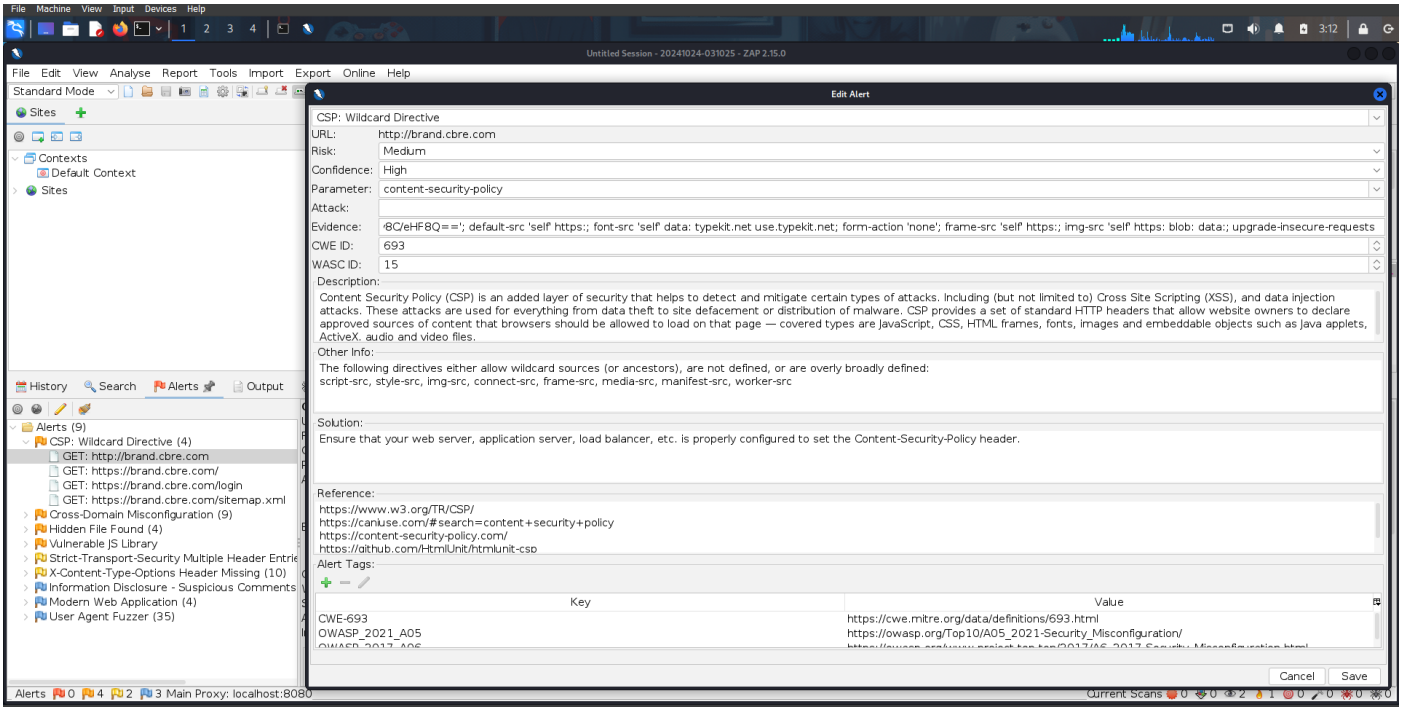
- Add the following line inside either the <directory>, <location>, <files> or <virtualhost> sections of your server config (usually located in `httpd.conf` or `apache.conf`), or within a `.htaccess` file.

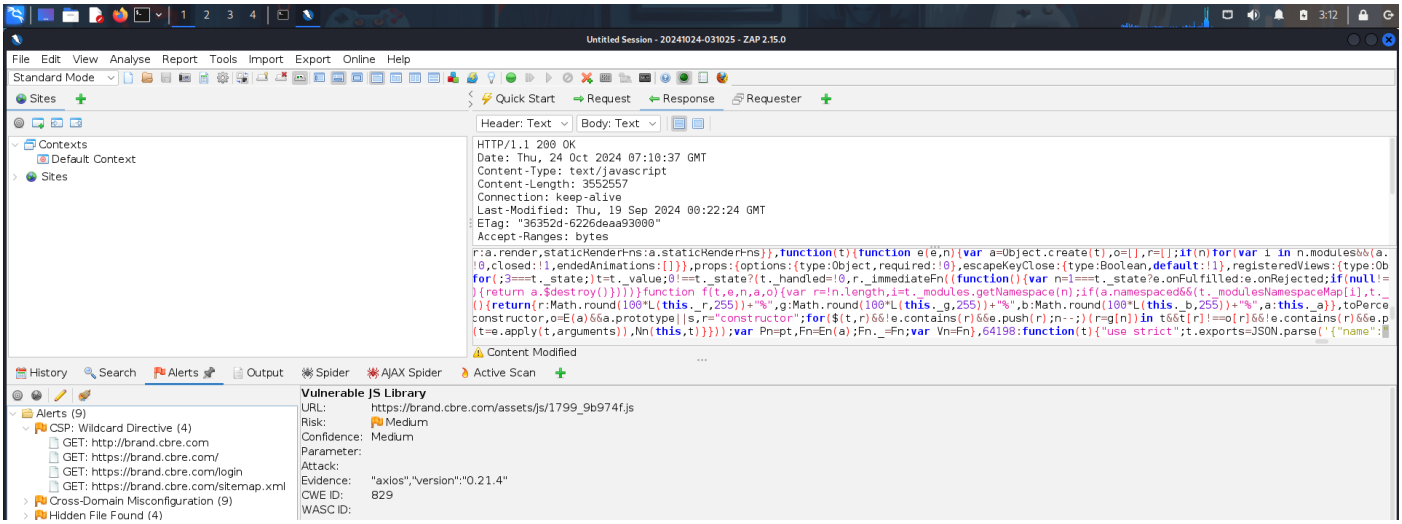
CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6

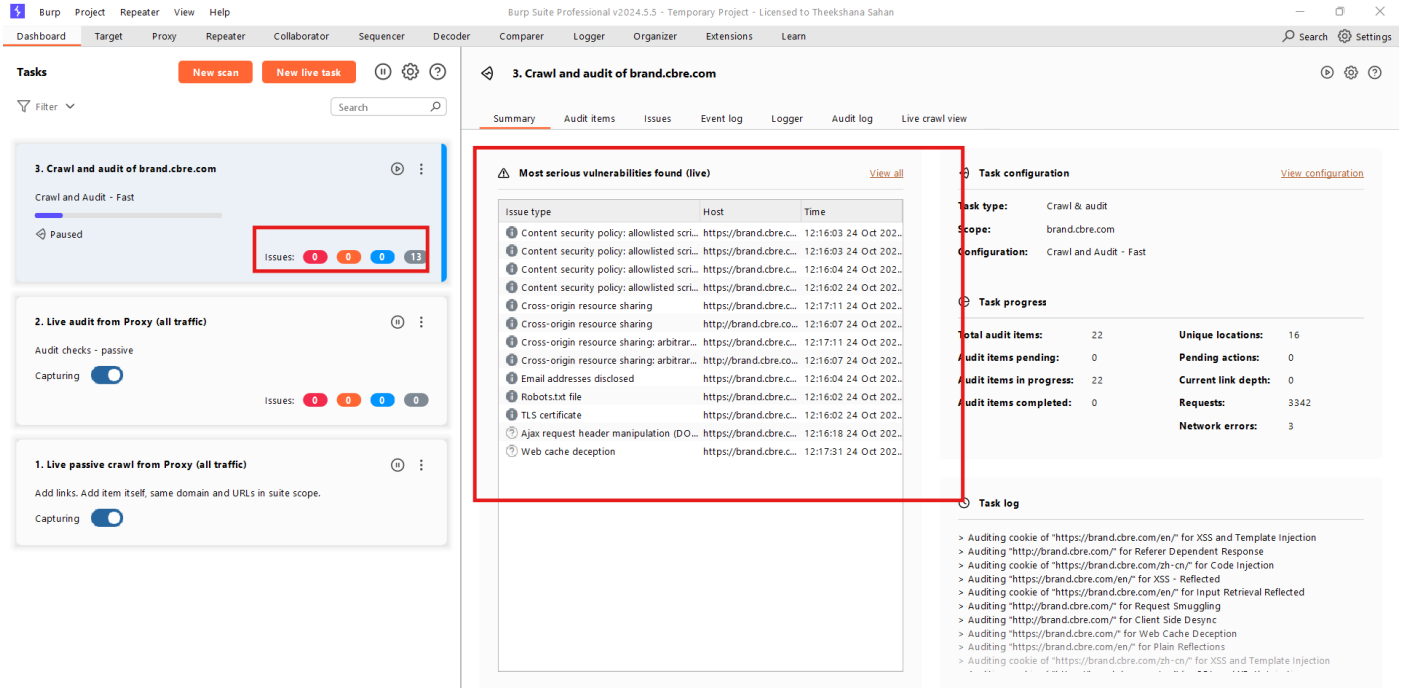
OWASP ZAP

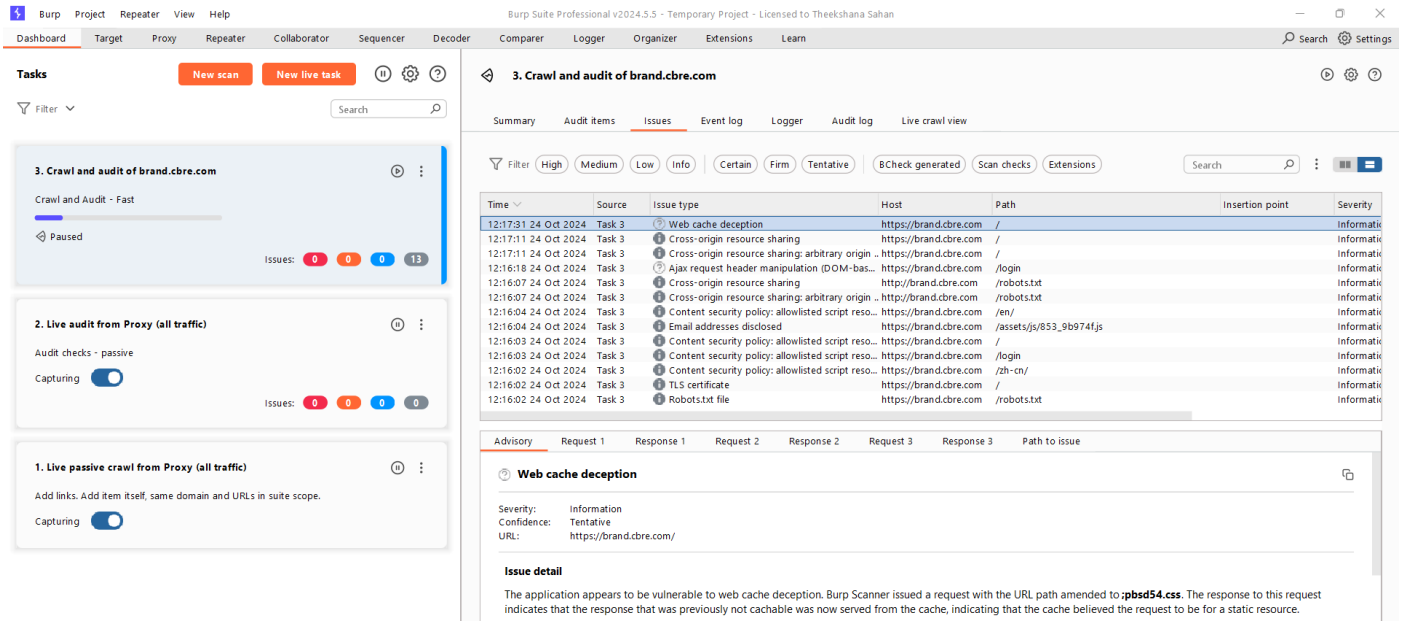

Untitled Session - 20241024-031025 - ZAP 2.15.0
Automated Scan
ZAP by Checkmarx
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack: http://brand.cbre.com
Use traditional spider:
Use ajax spider: If Modern with Firefox Headless
Attack
Stop
Progress: Actively scanning (attacking) the URLs discovered by the spider(s)
CSP: Wildcard Directive
URL: http://brand.cbre.com
Risk: Medium
Confidence: High
Parameter: content-security-policy
Attack:
Evidence:
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

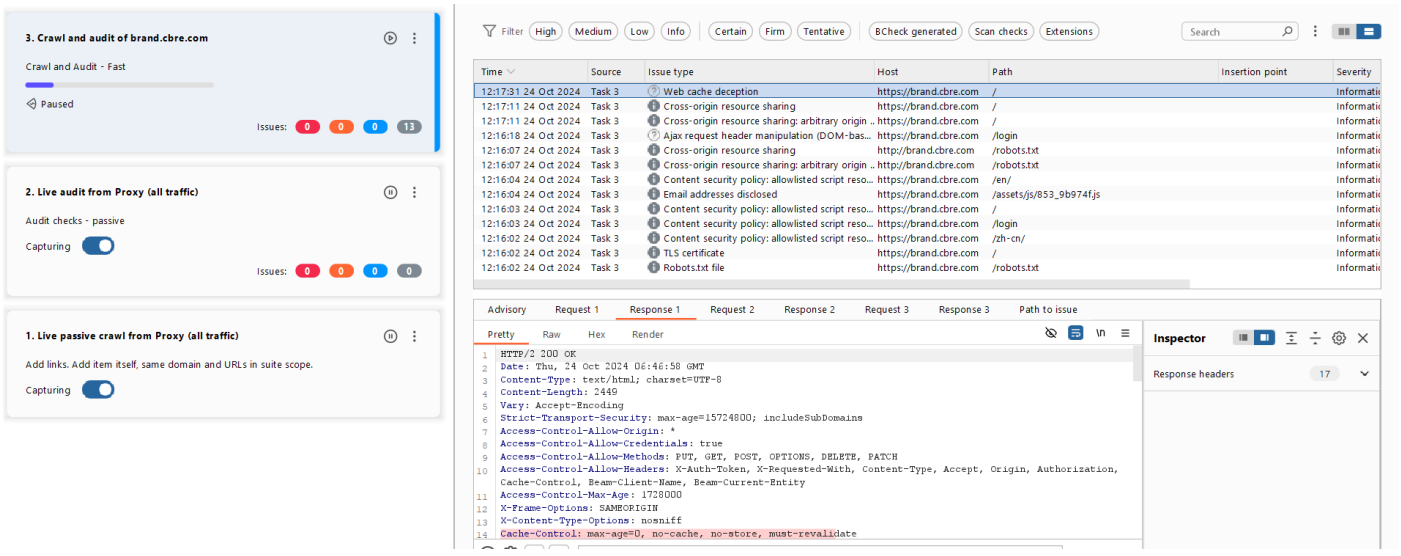

Edit Alert
CSP: Wildcard Directive
URL: http://brand.cbre.com
Risk: Medium
Confidence: High
Parameter: content-security-policy
Attack:
Evidence: 'sha256-47DEQpj8HBSa+/TImW+5JCeuQeRkm5NMpJWZG3hSuFU=' 'sha256-yhORaI3Zbst2lvWTgVVG3wbpBy6KmMkOBrodb98UNc=' 'nonce-U2j27gcR2KgEh2Ytr7ragg==' 'nonce-6uzC3g8ZI96YEwY5hHlGSw==' 'nonce-1R2hCIot0jWUMe9zmH5STA==' 'nonce-JzCZkRHSw5Uigy8/eHF8Q==';
CWE ID: 693
WASC ID: 15
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, ActiveX, audio and video files.
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, media-src, manifest-src, worker-src
Solution:
Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference:
https://www.w3.org/TR/CSP/
https://caniuse.com/#search=content+security+policy
https://content-security-policy.com/
https://github.com/HtmlUnit/htmlunit-csp
Alert Tags:
Key
Value
CWE-693
https://cwe.mitre.org/data/definitions/693.html
OWASP_2021_A05
https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
Cancel
Save


Untitled Session - 20241024-031025 - ZAP 2.15.0
HTTP/1.1 200 OK
Date: Thu, 24 Oct 2024 07:10:37 GMT
Content-Type: text/javascript
Content-Length: 3552557
Connection: keep-alive
Last-Modified: Thu, 19 Sep 2024 00:22:24 GMT
ETag: "36352d-6226deaa93000"
Accept-Ranges: bytes
Content Modified
Vulnerable JS Library
URL: https://brand.cbre.com/assets/js/1799_9b974f.js
Risk: Medium
Confidence: Medium
Parameter:
Attack:
Evidence: "axios","version":"0.21.4"
CWE ID: 829
WASC ID:

Burp Suite


Burp Project Repeater View Help
Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan
Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Tasks
New scan
New live task
3. Crawl and audit of brand.cbre.com
Crawl and Audit - Fast
Paused
Issues: 0 0 0 13
2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing
Issues: 0 0 0 0
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing
3. Crawl and audit of brand.cbre.com
Summary Audit items Issues Event log Logger Audit log Live crawl view
Most serious vulnerabilities found (live)
View all
Issue type Host Time
Content security policy: allowlisted scri... https://brand.cbre.c... 12:16:03 24 Oct 202...
Content security policy: allowlisted scri... https://brand.cbre.c... 12:16:03 24 Oct 202...
Content security policy: allowlisted scri... https://brand.cbre.c... 12:16:04 24 Oct 202...
Content security policy: allowlisted scri... https://brand.cbre.c... 12:16:02 24 Oct 202...
Cross-origin resource sharing https://brand.cbre.c... 12:17:11 24 Oct 202...
Cross-origin resource sharing http://brand.cbre.co... 12:16:07 24 Oct 202...
Cross-origin resource sharing: arbitrar... https://brand.cbre.c... 12:17:11 24 Oct 202...
Cross-origin resource sharing: arbitrar... http://brand.cbre.co... 12:16:07 24 Oct 202...
Email addresses disclosed https://brand.cbre.c... 12:16:04 24 Oct 202...
Robots.txt file https://brand.cbre.c... 12:16:02 24 Oct 202...
TLS certificate https://brand.cbre.c... 12:16:02 24 Oct 202...
Ajax request header manipulation (DO... https://brand.cbre.c... 12:16:18 24 Oct 202...
Web cache deception https://brand.cbre.c... 12:17:31 24 Oct 202...
Task configuration
View configuration
Task type: Crawl & audit
Scope: brand.cbre.com
Configuration: Crawl and Audit - Fast
Task progress
Total audit items: 22
Audit items pending: 0
Audit items in progress: 22
Audit items completed: 0
Unique locations: 16
Pending actions: 0
Current link depth: 0
Requests: 3342
Network errors: 3
Task log
> Auditing cookie of "https://brand.cbre.com/en/" for XSS and Template Injection
> Auditing "http://brand.cbre.com/" for Referer Dependent Response
> Auditing cookie of "https://brand.cbre.com/zh-cn/" for Code Injection
> Auditing "https://brand.cbre.com/en/" for XSS - Reflected
> Auditing cookie of "https://brand.cbre.com/en/" for Input Retrieval Reflected
> Auditing "http://brand.cbre.com/" for Request Smuggling
> Auditing "http://brand.cbre.com/" for Client Side Desync
> Auditing "https://brand.cbre.com/" for Web Cache Deception
> Auditing "https://brand.cbre.com/en/" for Plain Reflections
> Auditing cookie of "https://brand.cbre.com/zh-cn/" for XSS and Template Injection


Burp Project Repeater View Help
Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan
Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Tasks
New scan
New live task
3. Crawl and audit of brand.cbre.com
Crawl and Audit - Fast
Paused
Issues: 0 0 0 13
2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing
Issues: 0 0 0 0
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing
3. Crawl and audit of brand.cbre.com
Summary Audit items Issues Event log Logger Audit log Live crawl view
Filter High Medium Low Info Certain Firm Tentative BCheck generated Scan checks Extensions
Search
Time Source Issue type Host Path Insertion point Severity
12:17:31 24 Oct 2024 Task 3 Web cache deception https://brand.cbre.com /
12:17:11 24 Oct 2024 Task 3 Cross-origin resource sharing https://brand.cbre.com /
12:17:11 24 Oct 2024 Task 3 Cross-origin resource sharing: arbitrary origin ... https://brand.cbre.com /
12:16:18 24 Oct 2024 Task 3 Ajax request header manipulation (DOM-bas... https://brand.cbre.com /login
12:16:07 24 Oct 2024 Task 3 Cross-origin resource sharing http://brand.cbre.com /robots.txt
12:16:07 24 Oct 2024 Task 3 Cross-origin resource sharing: arbitrary origin ... http://brand.cbre.com /robots.txt
12:16:04 24 Oct 2024 Task 3 Content security policy: allowlisted script reso... https://brand.cbre.com /en/
12:16:04 24 Oct 2024 Task 3 Email addresses disclosed https://brand.cbre.com /assets/js/853_9b974f.js
12:16:03 24 Oct 2024 Task 3 Content security policy: allowlisted script reso... https://brand.cbre.com /
12:16:03 24 Oct 2024 Task 3 Content security policy: allowlisted script reso... https://brand.cbre.com /login
12:16:02 24 Oct 2024 Task 3 Content security policy: allowlisted script reso... https://brand.cbre.com /zh-cn/
12:16:02 24 Oct 2024 Task 3 TLS certificate https://brand.cbre.com /
12:16:02 24 Oct 2024 Task 3 Robots.txt file https://brand.cbre.com /robots.txt
Advisory Request 1 Response 1 Request 2 Response 2 Request 3 Response 3 Path to issue
Web cache deception
Severity: Information
Confidence: Tentative
URL: https://brand.cbre.com/
Issue detail
The application appears to be vulnerable to web cache deception. Burp Scanner issued a request with the URL path amended to ;pbsd54.css. The response to this request indicates that the response that was previously not cachable was now served from the cache, indicating that the cache believed the request to be for a static resource.

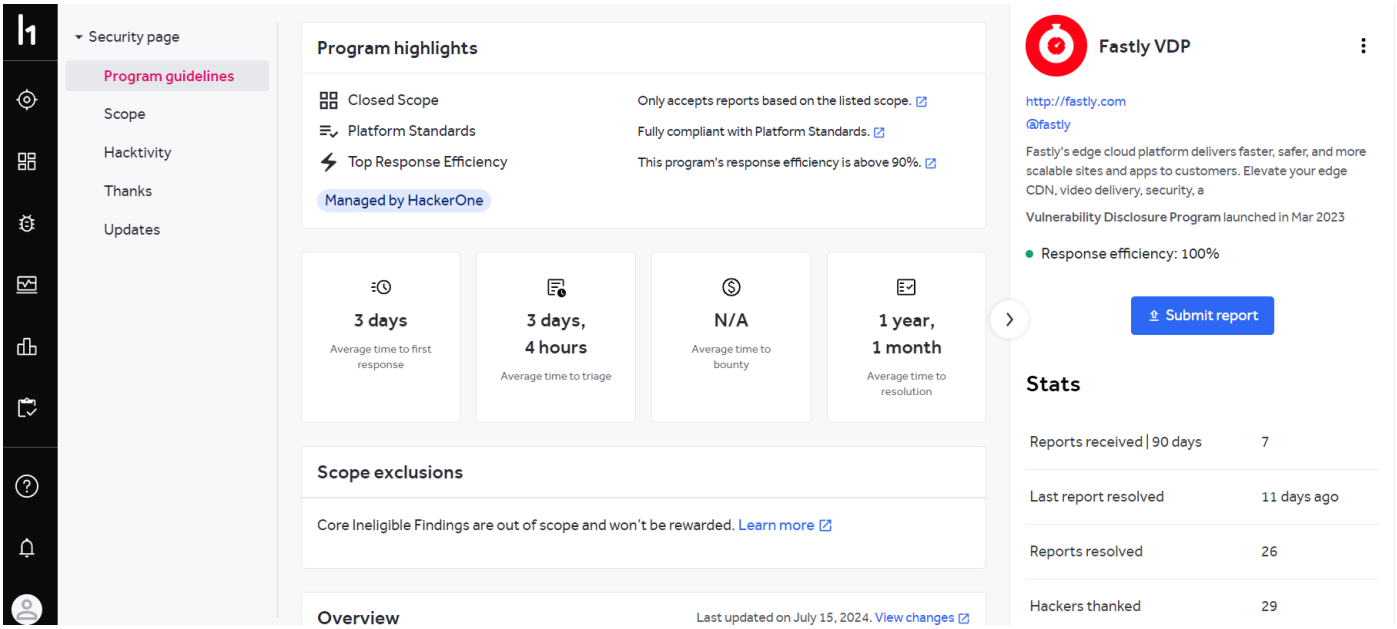

3. Crawl and audit of brand.cbre.com
Crawl and Audit - Fast
Paused
Issues: 0 0 0 13
2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing
Issues: 0 0 0 0
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing
Filter High Medium Low Info Certain Firm Tentative BCheck generated Scan checks Extensions
Search
Time Source Issue type Host Path Insertion point Severity
12:17:31 24 Oct 2024 Task 3 Web cache deception https://brand.cbre.com /
12:17:11 24 Oct 2024 Task 3 Cross-origin resource sharing https://brand.cbre.com /
12:17:11 24 Oct 2024 Task 3 Cross-origin resource sharing: arbitrary origin ... https://brand.cbre.com /
12:16:18 24 Oct 2024 Task 3 Ajax request header manipulation (DOM-bas... https://brand.cbre.com /login
12:16:07 24 Oct 2024 Task 3 Cross-origin resource sharing http://brand.cbre.com /robots.txt
12:16:07 24 Oct 2024 Task 3 Cross-origin resource sharing: arbitrary origin ... http://brand.cbre.com /robots.txt
12:16:04 24 Oct 2024 Task 3 Content security policy: allowlisted script reso... https://brand.cbre.com /en/
12:16:04 24 Oct 2024 Task 3 Email addresses disclosed https://brand.cbre.com /assets/js/853_9b974f.js
12:16:03 24 Oct 2024 Task 3 Content security policy: allowlisted script reso... https://brand.cbre.com /
12:16:03 24 Oct 2024 Task 3 Content security policy: allowlisted script reso... https://brand.cbre.com /login
12:16:02 24 Oct 2024 Task 3 Content security policy: allowlisted script reso... https://brand.cbre.com /zh-cn/
12:16:02 24 Oct 2024 Task 3 TLS certificate https://brand.cbre.com /
12:16:02 24 Oct 2024 Task 3 Robots.txt file https://brand.cbre.com /robots.txt
Advisory Request 1 Response 1 Request 2 Response 2 Request 3 Response 3 Path to issue
Pretty Raw Hex Render
Inspector
Response headers 17
1 HTTP/2 200 OK
2 Date: Thu, 24 Oct 2024 06:46:58 GMT
3 Content-Type: text/html; charset=UTF-8
4 Content-Length: 2449
5 Vary: Accept-Encoding
6 Strict-Transport-Security: max-age=15724800; includeSubDomains
7 Access-Control-Allow-Origin: *
8 Access-Control-Allow-Credentials: true
9 Access-Control-Allow-Methods: PUT, GET, POST, OPTIONS, DELETE, PATCH
10 Access-Control-Allow-Headers: X-Auth-Token, X-Requested-With, Content-Type, Accept, Origin, Authorization, Cache-Control, Beam-Client-Name, Beam-Current-Entity
11 Access-Control-Max-Age: 1728000
12 X-Frame-Options: SAMEORIGIN
13 X-Content-Type-Options: nosniff
14 Cache-Control: max-age=0, no-cache, no-store, must-revalidate

Vulnerabilities:

1 Misconfigured Access-Control-Allow-Origin Header

Vulnerability Title	Misconfigured Access-Control-Allow-Origin Header
Vulnerability Description	The Access-Control-Allow-Origin header is misconfigured, allowing resources to be accessed by unauthorized or malicious origins. This header is responsible for controlling which domains are allowed to access a website's resources via cross-origin resource sharing (CORS). If misconfigured, it can expose sensitive data to any website that makes a request, leading to data breaches.
Affected Components	Web server configuration, particularly in handling cross-origin resource sharing (CORS) requests. It can affect APIs, sensitive data endpoints, and resources such as scripts or media files.
Impact Assessment	**Risk Level**: High. It allows unauthorized origins to access sensitive resources. **Potential Exploits**: Attackers can craft malicious websites that make unauthorized API calls or retrieve sensitive user data from your domain. This can lead to data theft or unauthorized actions being performed on behalf of users.
Steps to Reproduce	1. Open the browser developer tools. 2. Navigate to the Network tab. 3. Visit the affected website. 4. Make a cross-origin request from a different domain using JavaScript 5. Check if the Access-Control-Allow-Origin header is set to or includes unwanted origins.
Proof of Concept	**Expected Result**: The response should be blocked due to CORS restrictions. **Observed Result**: The response is successfully received despite originating from an unauthorized domain.
Proposed Mitigation or Fix	Restrict the Access-Control-Allow-Origin header to specific trusted domains instead of using the wildcard. Ensure that credentials (cookies, HTTP authentication) are only shared with trusted origins by adding Access-Control-Allow-Credentials:true. Implement a strict CORS policy and thoroughly test its implementation across different origins.

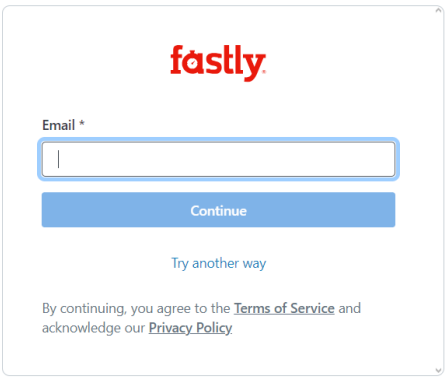
Report 08 Target Details



The target for this Bug Bounty report is **faslty.com** (https://www.domain-faslty.com), a platform providing digital solutions for businesses, including tools for marketing, sales, and customer management. The company offers a range of services such as digital advertising, reputation management, and APIs for integrating various business functions. **faslty.com**'s platform is designed to help businesses grow by offering scalable and efficient solutions, leveraging modern technologies.

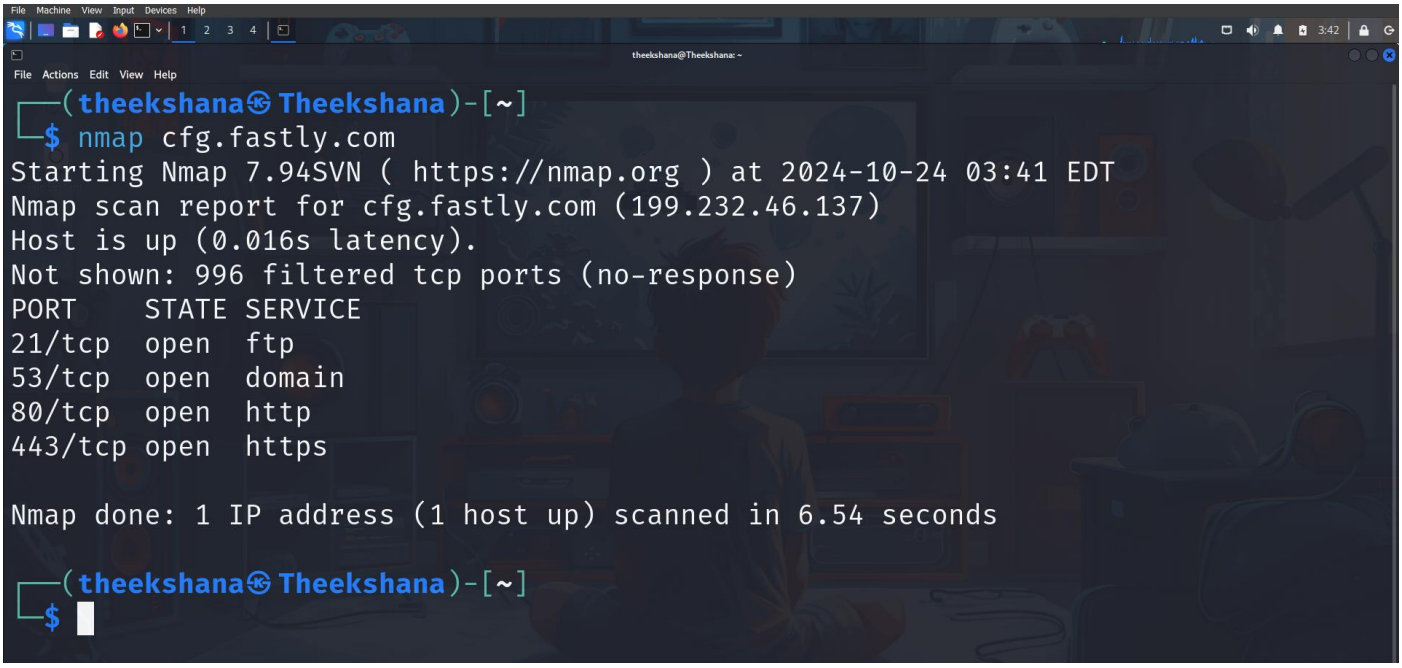
In this report, I have chosen to focus on 10 subdomains under the main domain **faslty.com**. Each subdomain may serve different functionalities or services, potentially introducing distinct security risks, particularly in development or user-related areas. These subdomains were selected based on their relevance and the likelihood of containing vulnerabilities.

This report covers the findings for the subdomain: **cfg.fastly.com**



Target Reconnaissance

Nmap Scan

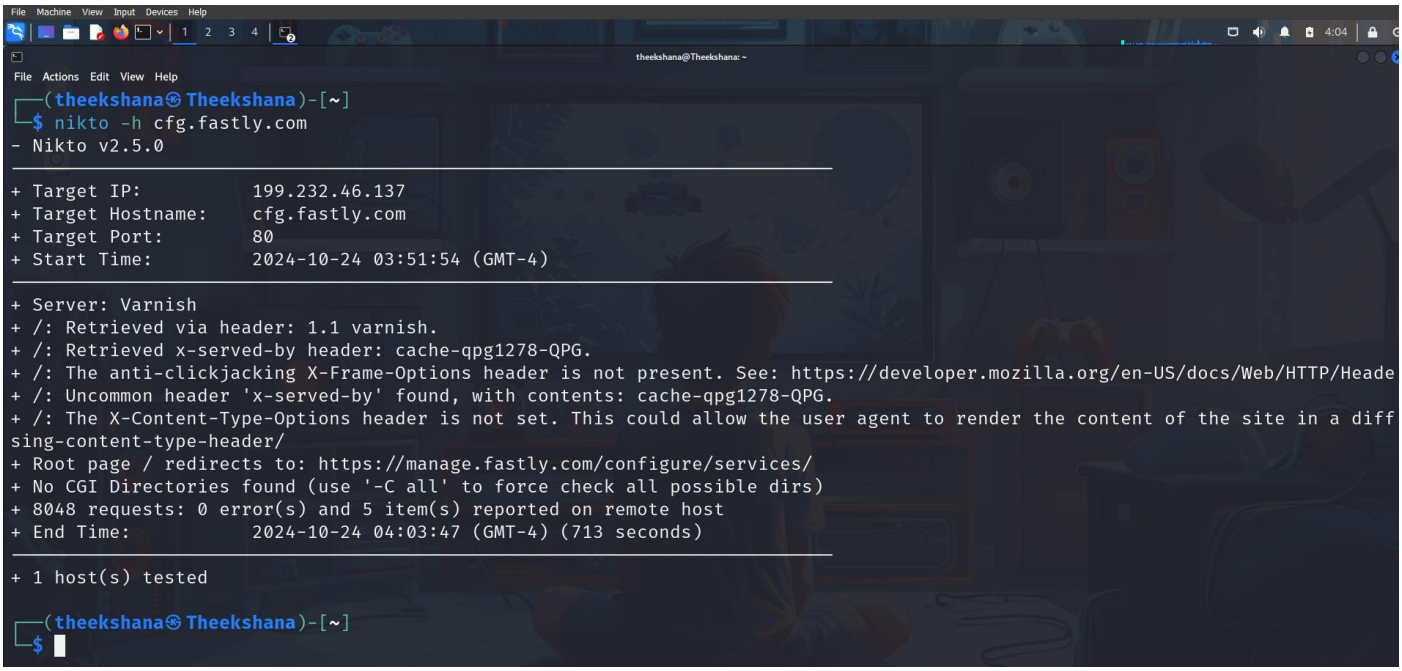


By scanning cfg.fastly.com with Nmap I found out these information.

Port	State	Service
21/tcp	Open	FTP
53/tcp	Open	DOMAIN
80/tcp	Open	HTTP
443/tcp	Open	HTPPS

Port	State	Service	Potential Vulnerabilities
21/tcp	Open	FTP	Data is not encrypted, so sensitive information can be stolen. Hackers can guess passwords (brute force attacks) Misconfigurations might allow unauthorized access
53/tcp	Open	DNS	Attackers can redirect users to fake sites (DNS poisoning) Hackers might flood the system (amplification attacks) Sensitive DNS info could be exposed (zone transfer)
80/tcp	Open	HTTP	Data is not secure (no encryption) Hackers can inject harmful scripts (XSS)
443/tcp	Open	HTTPS	If not properly secured, attackers can intercept data Older encryption protocols may be weak

Nikto Scan



The screenshot shows the output of a Nikto scan against the target cfg.fastly.com which reveals several potential security issues and misconfigurations.

Target Information:

- **Target IP**: 199.232.46.137
- **Target Hostname**: cfg.fastly.com
- **Target Port**: 80 (HTTP)

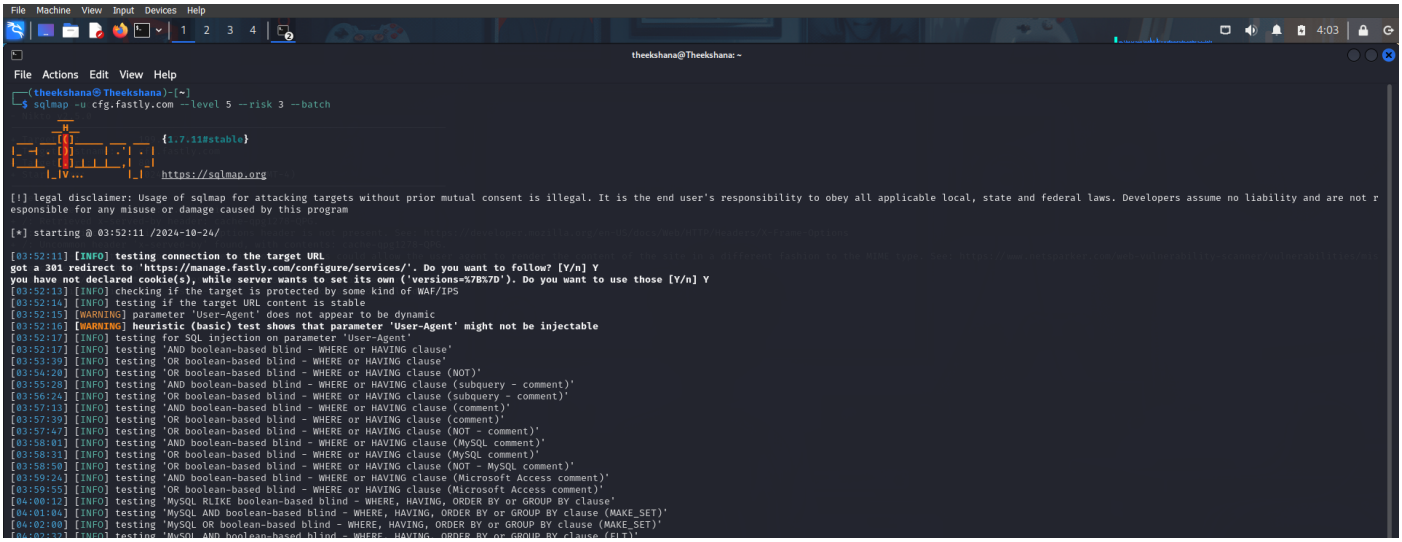
Findings:

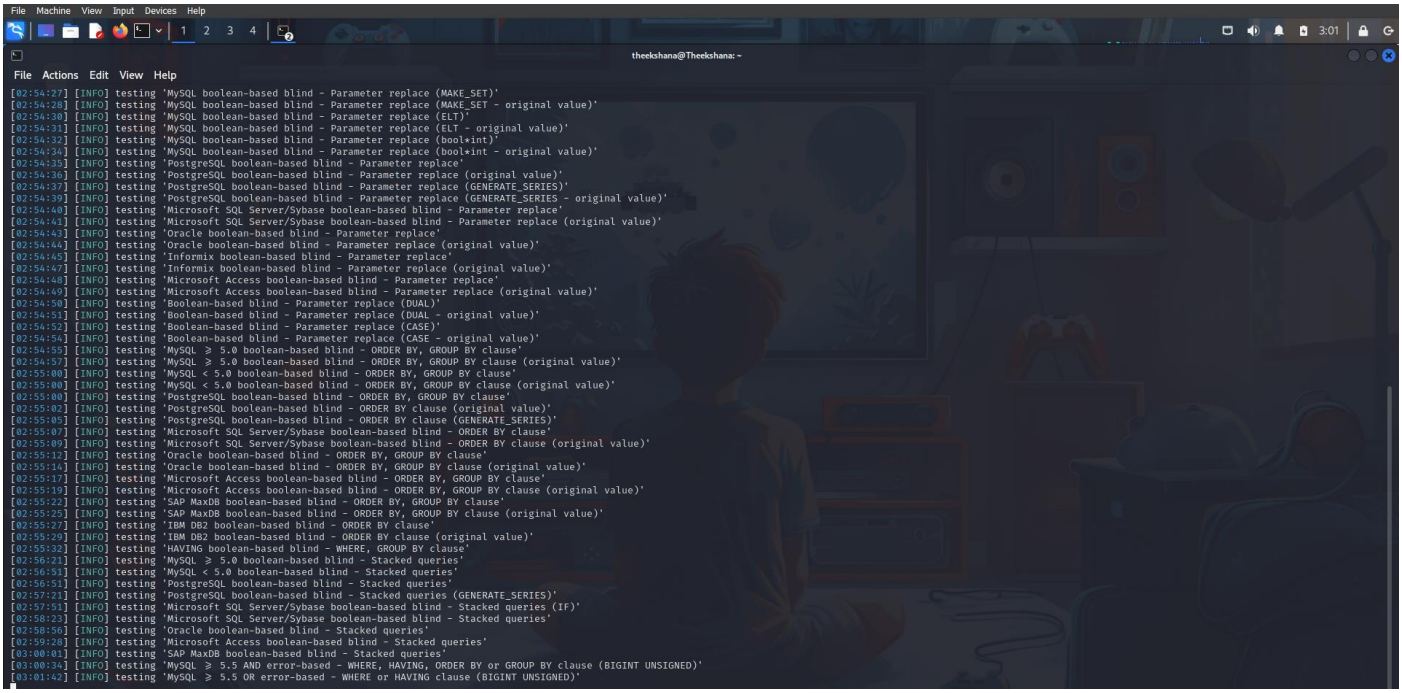
X-Frame-Options header is not present: This could allow clickjacking attacks where a website is embedded in a malicious website using iframes. It suggests adding the X-Frame-Options header to prevent this.

Uncommon header 'x-served-by' found: This reveals internal information about how the site is served, specifically showing the content is served by cache-qpg1278-QPG. Revealing internal headers may expose the server's internal infrastructure, which could potentially help an attacker map the environment.

X-Content-Type-Options header is not set: This can lead to MIME-type sniffing issues, where the browser tries to guess the content type of files. It recommends setting this header to nosniff to prevent the browser from interpreting files as a different MIME type, which can mitigate certain attacks

SQLmap Scaner

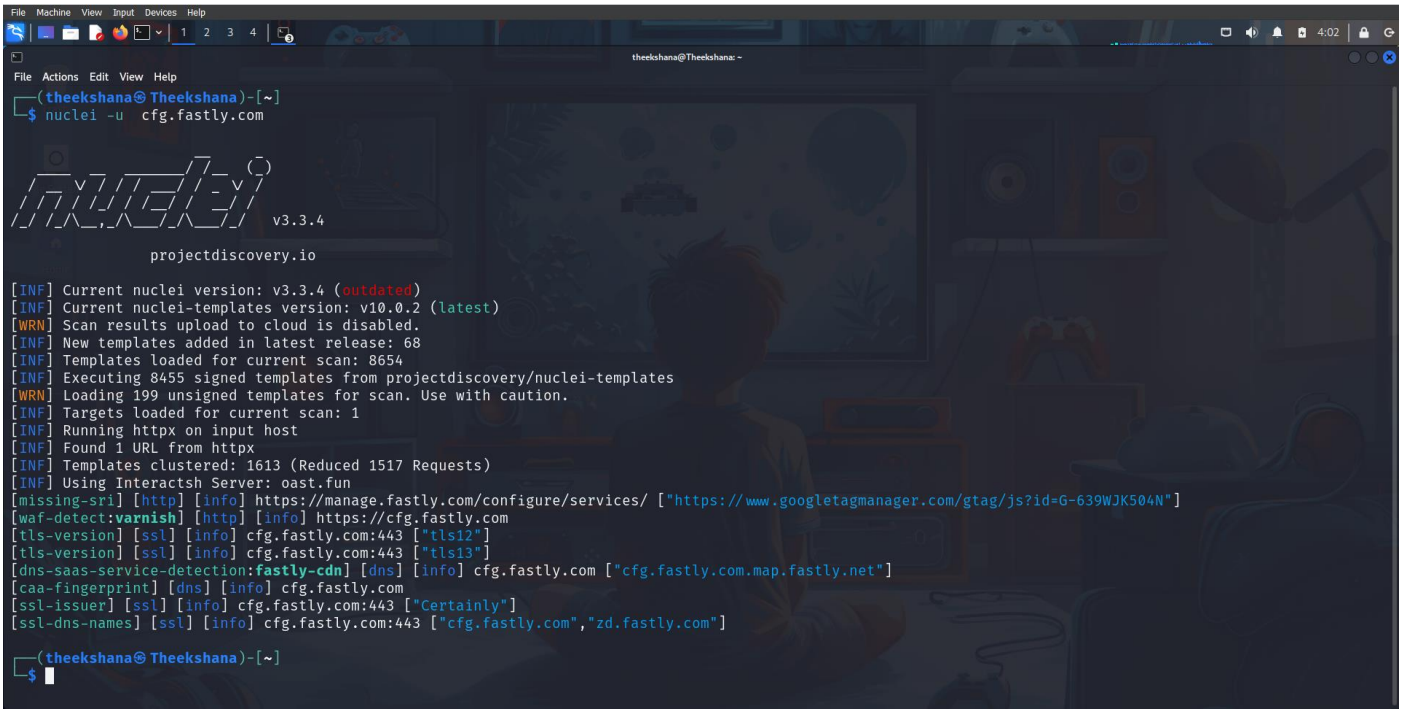




Techniques Tested:

- The tool tried several SQL injection techniques, including:
    - **Boolean-based blind SQL injection**: It tests queries that rely on conditions to confirm if injection is possible.
    - **AND/OR blind**: Uses AND and OR clauses to manipulate SQL statements and determine vulnerability.
    - **HAVING, ORDER BY, GROUP BY clauses**: These are SQL statements used to filter and sort query results, and they were tested for potential injection points.

Nuclei Scan



Missing SRI on Static Resources:

This can allow attackers to inject malicious scripts into the JavaScript files if the integrity of these files is compromised. Adding SRI hashes would mitigate this risk.

TLS Version Issues:

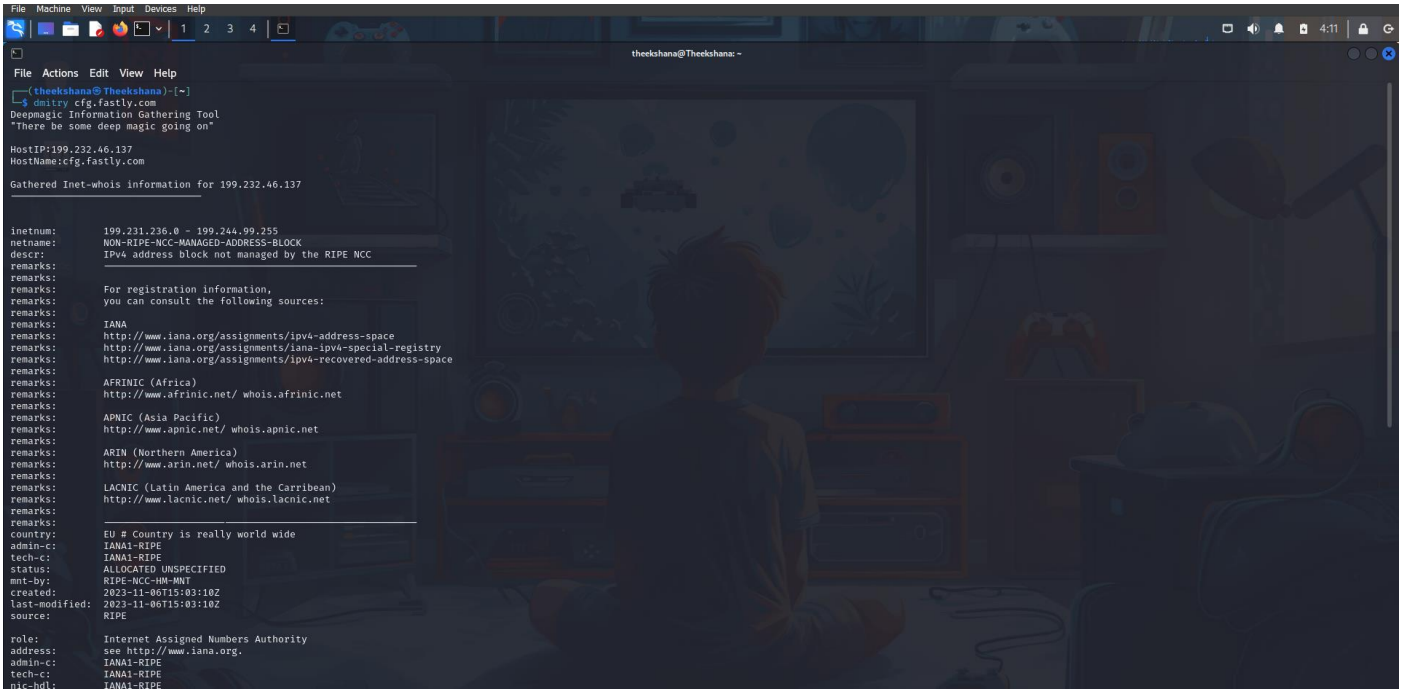
A specific TLS version might be flagged as outdated or insecure, indicating the need for updating to a more secure version.

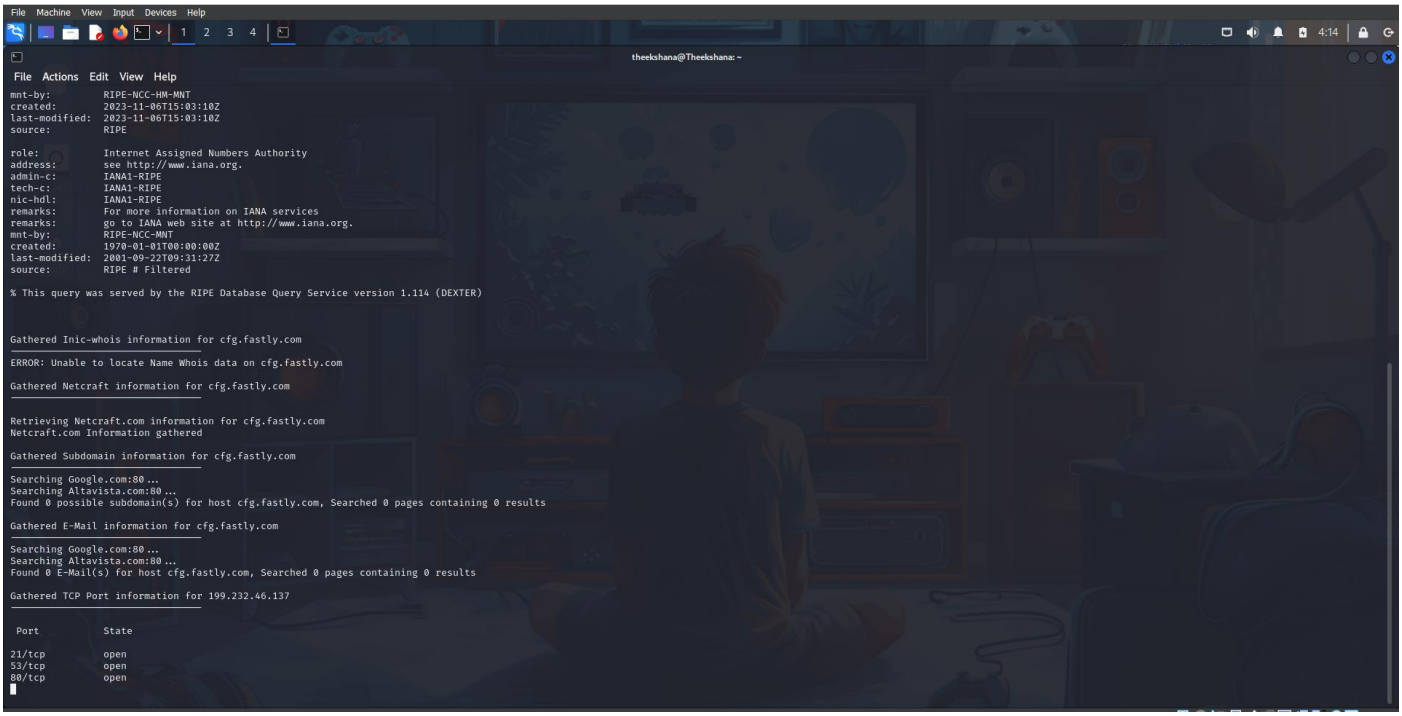
Server and SSL Information:

The scan identifies the technologies used (Nginx server and Amazon-issued SSL certificates), which is useful for mapping the infrastructure.

- **[tls-version]**: The TLS version used by app.grammarly.com:443 is flagged. It could indicate that an outdated or insecure TLS version is being used.
- **[security-txt]**: This refers to the security.txt file, a standard for websites to provide security contact information. Here, the security contact is security@grammarly.com.
- **[tech-detect: nginx]**: Nginx was detected as the web server technology for app.grammarly.com.
- **[ssl-fingerprint]**: Shows that a particular SSL fingerprint was detected for the domain.
- **[nameserver-fingerprint]**: Displays fingerprint data related to the domain's nameservers. It shows that app.grammarly.com uses AWS nameservers (awsdns), specifically from various geographical locations like the US and UK.

Dmitry Scan



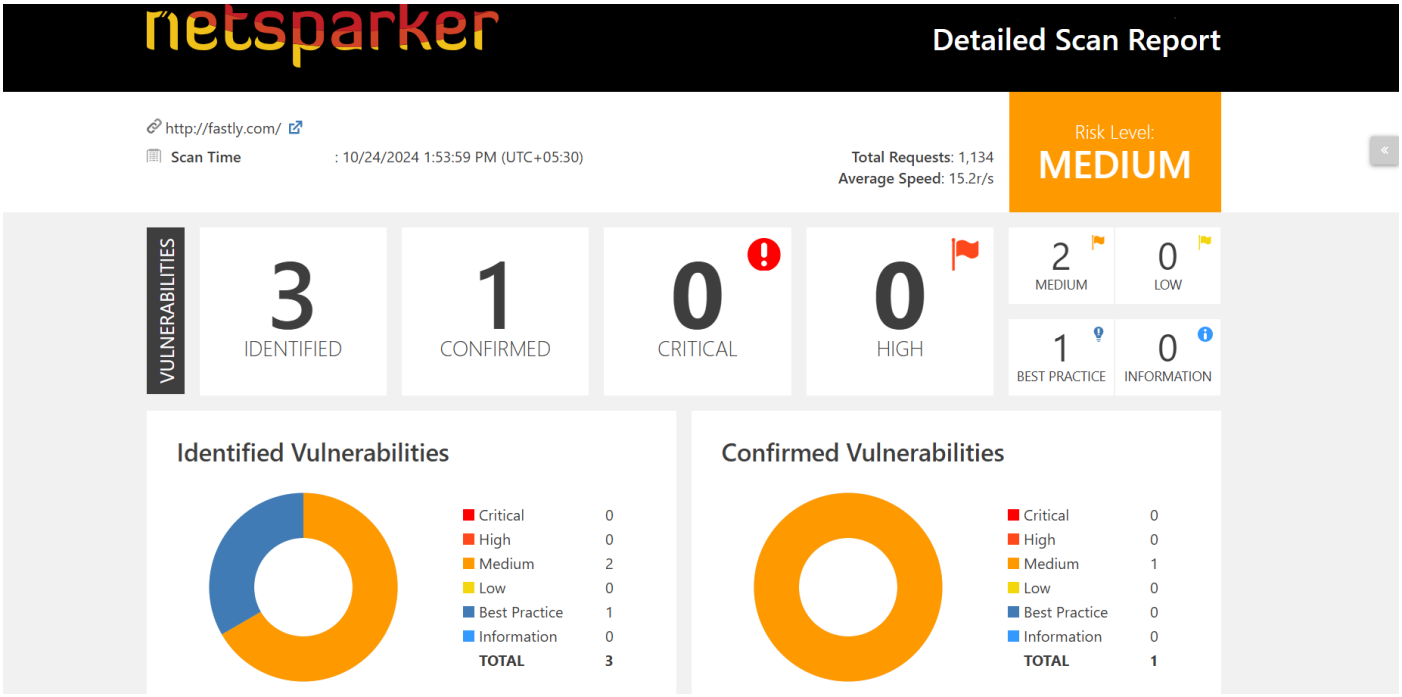


Port 21 (FTP - File Transfer Protocol): This port is typically used for file transfer services. Having FTP open can be risky if not properly secured, as it often transmits data in plain text (though secure variants like SFTP exist).

Port 53 (DNS - Domain Name System): This port is used for DNS services, which translate domain names into IP addresses. While DNS services need to be accessible, misconfigurations or vulnerabilities (like DNS amplification attacks) can expose the server to risks.

Port 80 (HTTP - Hypertext Transfer Protocol): This port is used for unencrypted web traffic. Port 80 being open suggests that the website is accessible via HTTP, but this should be redirected to HTTPS (Port 443) for encrypted communication. If not, it leaves the site vulnerable to man-in-the middle (MITM) attacks.

Netsparker



Vulnerability Summary

SEVERITY FILTER : CRITICAL HIGH MEDIUM LOW BEST PRACTICE INFORMATION

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://fastly.com/	
	Weak Ciphers Enabled	GET	https://fastly.com/	
	Expect-CT Not Enabled	GET	https://fastly.com/	

Weak Ciphers Enabled

MEDIUM 1 CONFIRMED 1

Netsparker detected that weak ciphers are enabled during secure communication (SSL).

You should allow only strong ciphers on your web server to protect secure communication with your visitors.

Impact

Attackers might decrypt SSL traffic between your server and your visitors.

Vulnerabilities

2.1. https://fastly.com/ CONFIRMED

Hide Remediation

Actions to Take

1. For Apache, you should modify the SSLCipherSuite directive in the `httpd.conf`.

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

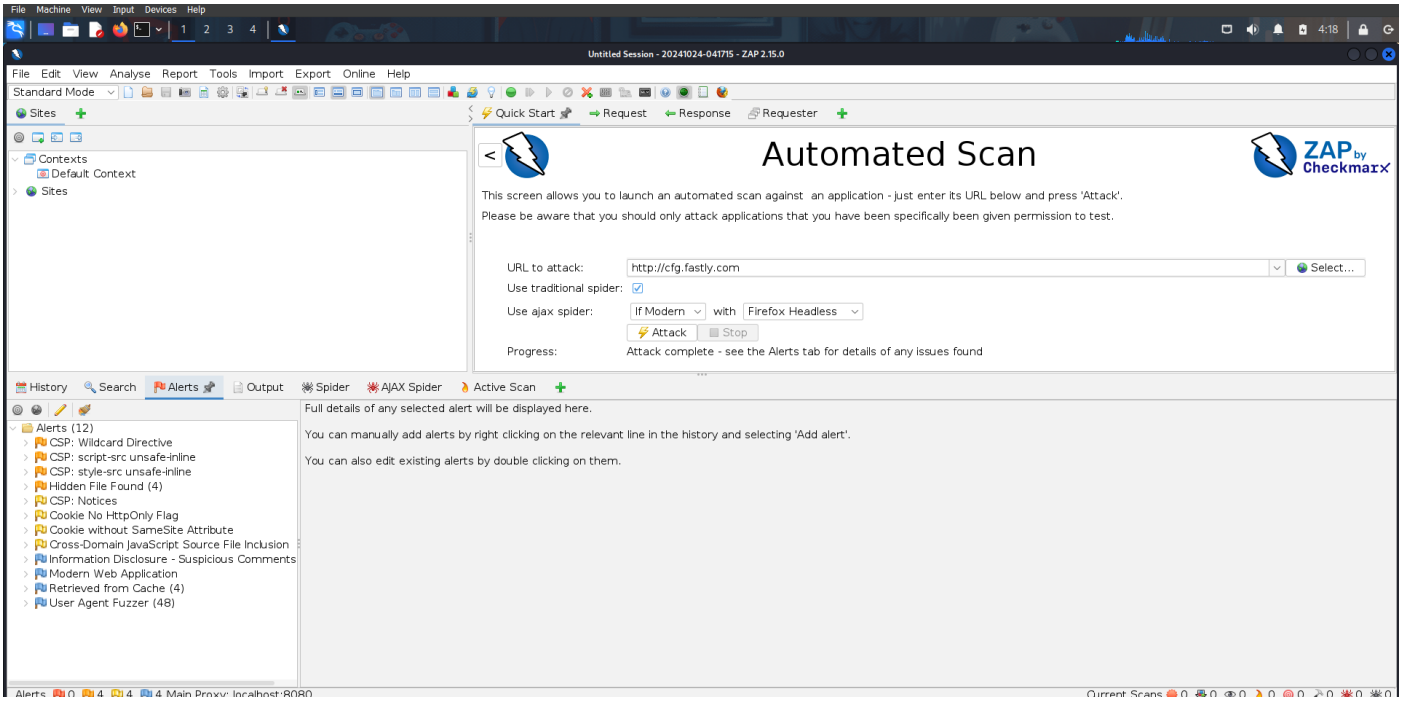
2. Lighttpd:

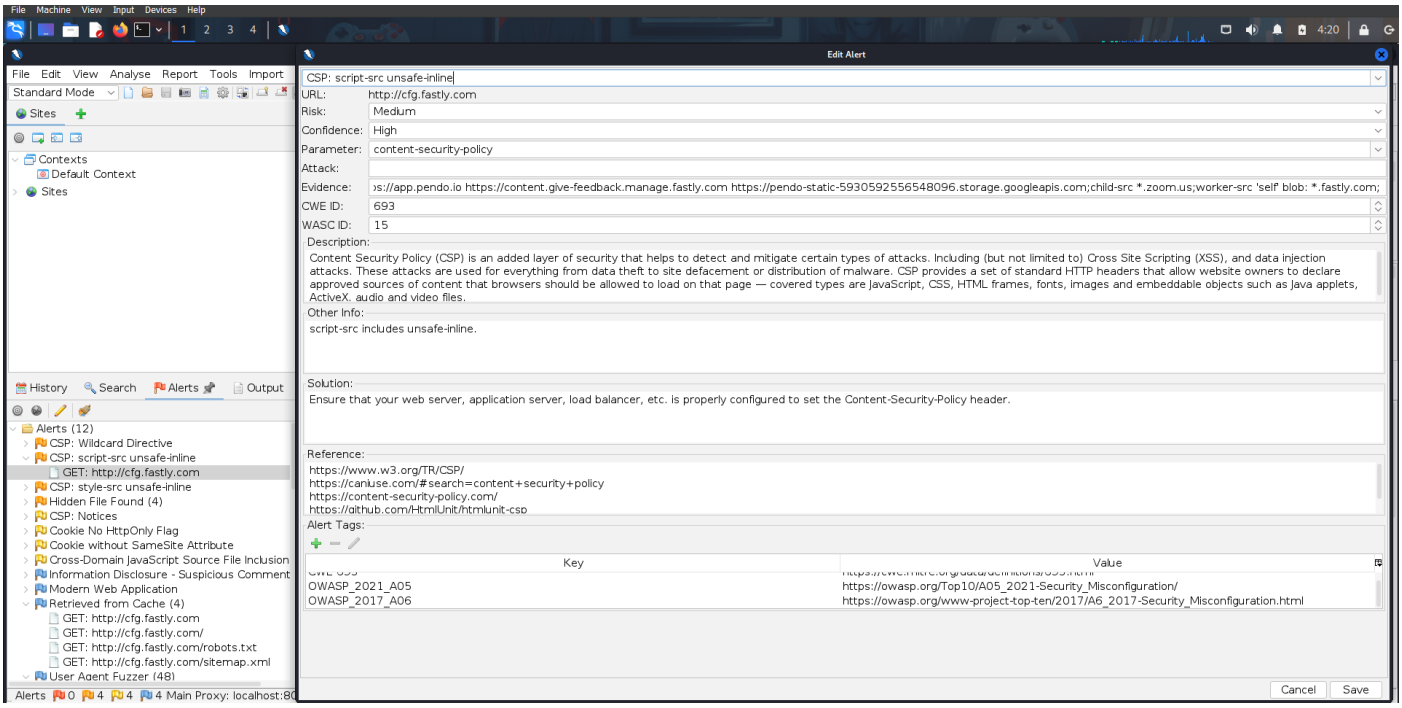
```
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

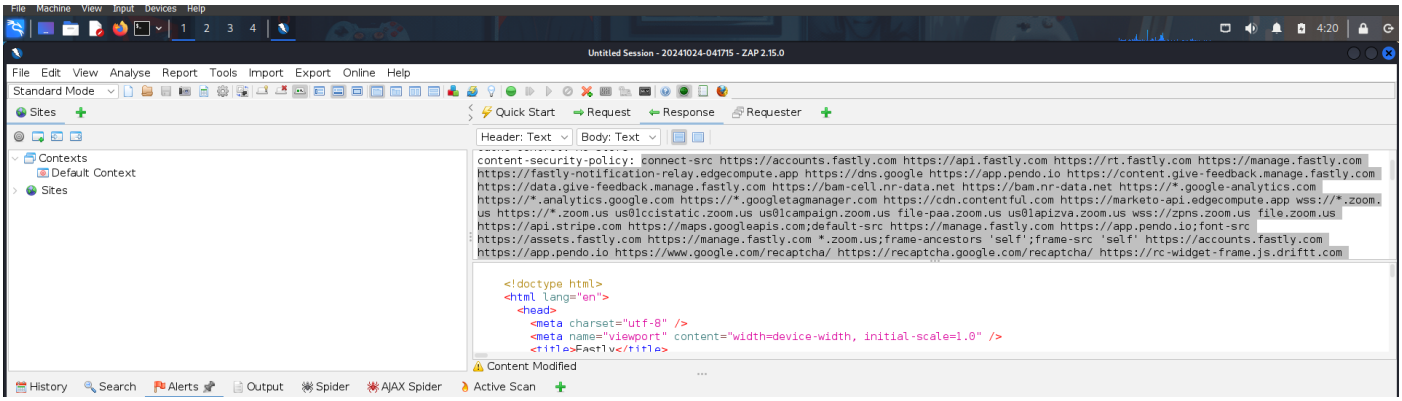
CLASSIFICATION

PCI DSS v3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	327
CAPEC	217

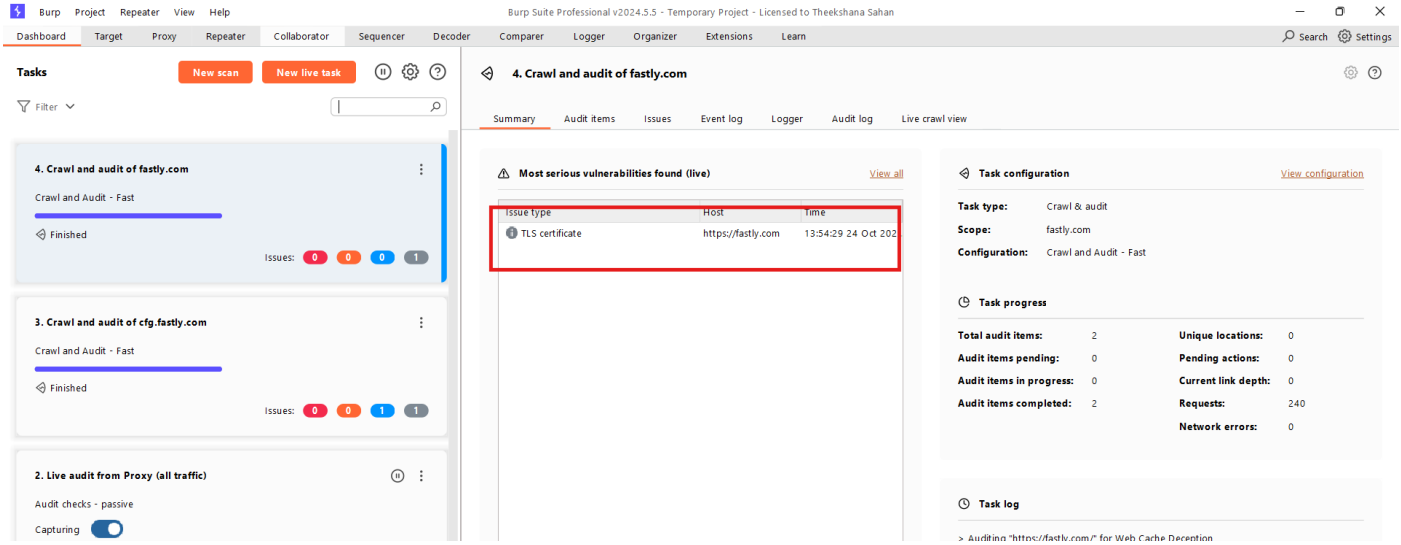
OWASP ZAP

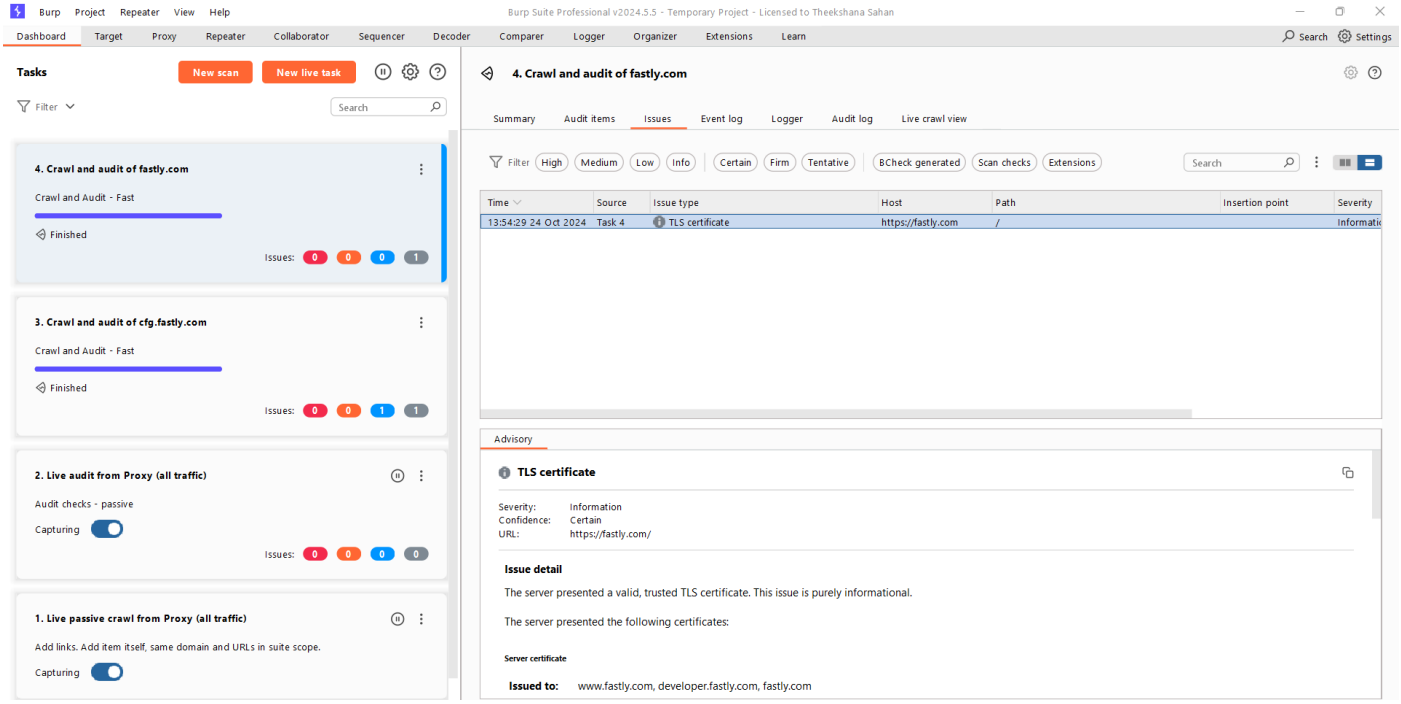

Automated Scan
ZAP by Checkmarx
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack: http://cfg.fastly.com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

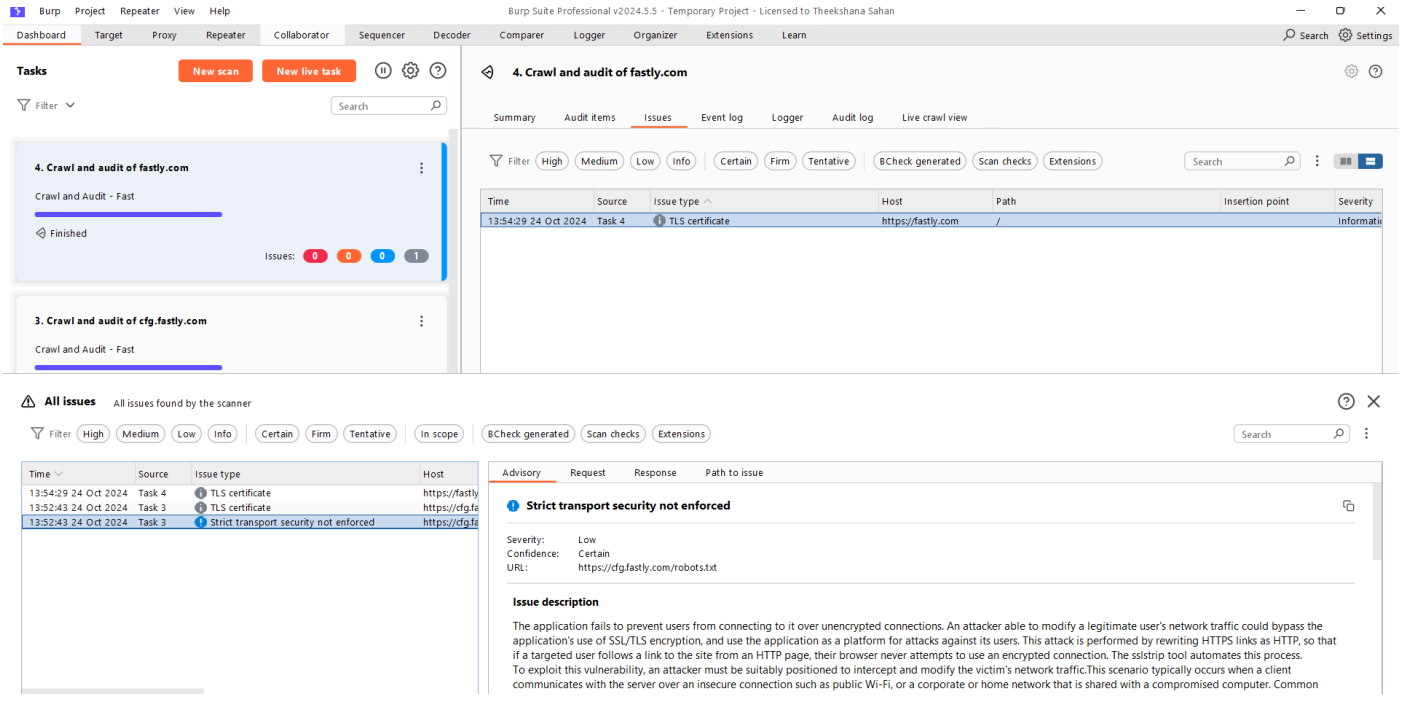

Edit Alert
CSP: script-src unsafe-inline
URL: http://cfg.fastly.com
Risk: Medium
Confidence: High
Parameter: content-security-policy
Attack:
CWE ID: 693
WASC ID: 15
Description:
Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (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, ActiveX, audio and video files.
Other Info:
script-src includes unsafe-inline.
Solution:
Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference:
https://www.w3.org/TR/CSP/
https://caniuse.com/#search=content+security+policy
https://content-security-policy.com/
https://github.com/HtmlUnit/htmlunit-csp
Alert Tags:
Key
Value
OWASP_2021_A05
https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
OWASP_2017_A06
https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html
Cancel
Save


Content Modified

Burp Suite


Burp Project Repeater View Help
Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan
Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Tasks
New scan
New live task
4. Crawl and audit of fastly.com
Summary Audit items Issues Event log Logger Audit log Live crawl view
Most serious vulnerabilities found (live)
View all
Issue type Host Time
TLS certificate https://fastly.com 13:54:29 24 Oct 202
Task configuration
View configuration
Task type: Crawl & audit
Scope: fastly.com
Configuration: Crawl and Audit - Fast
Task progress
Total audit items: 2
Audit items pending: 0
Audit items in progress: 0
Audit items completed: 2
Unique locations: 0
Pending actions: 0
Current link depth: 0
Requests: 240
Network errors: 0
Task log
4. Crawl and audit of fastly.com
Crawl and Audit - Fast
Finished
Issues:
3. Crawl and audit of cfg.fastly.com
Crawl and Audit - Fast
Finished
Issues:
2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing


Burp Project Repeater View Help
Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan
Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Tasks
New scan
New live task
4. Crawl and audit of fastly.com
Summary Audit items Issues Event log Logger Audit log Live crawl view
Filter High Medium Low Info Certain Firm Tentative BCheck generated Scan checks Extensions
Search
Time Source Issue type Host Path Insertion point Severity
13:54:29 24 Oct 2024 Task 4 TLS certificate https://fastly.com /
Advisory
TLS certificate
Severity: Information
Confidence: Certain
URL: https://fastly.com/
Issue detail
The server presented a valid, trusted TLS certificate. This issue is purely informational.
The server presented the following certificates:
Server certificate
Issued to: www.fastly.com, developer.fastly.com, fastly.com
4. Crawl and audit of fastly.com
Crawl and Audit - Fast
Finished
Issues:
3. Crawl and audit of cfg.fastly.com
Crawl and Audit - Fast
Finished
Issues:
2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing
Issues:
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing

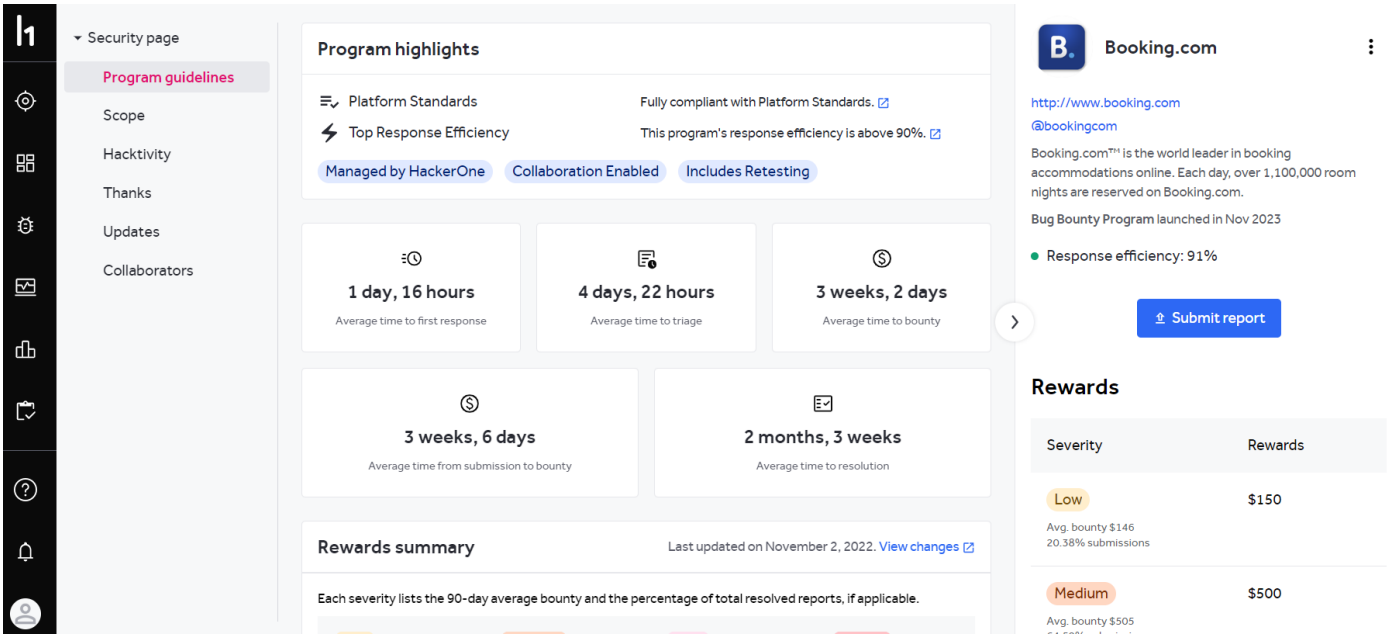

Burp Project Repeater View Help
Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan
Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Tasks
New scan
New live task
4. Crawl and audit of fastly.com
Summary Audit items Issues Event log Logger Audit log Live crawl view
Filter High Medium Low Info Certain Firm Tentative BCheck generated Scan checks Extensions
Search
Time Source Issue type Host Path Insertion point Severity
13:54:29 24 Oct 2024 Task 4 TLS certificate https://fastly.com /
4. Crawl and audit of fastly.com
Crawl and Audit - Fast
Finished
Issues:
3. Crawl and audit of cfg.fastly.com
Crawl and Audit - Fast
All issues
All issues found by the scanner
Filter High Medium Low Info Certain Firm Tentative In scope BCheck generated Scan checks Extensions
Search
Time Source Issue type Host
13:54:29 24 Oct 2024 Task 4 TLS certificate https://fastly
13:52:43 24 Oct 2024 Task 3 TLS certificate https://cfg.fa
13:52:43 24 Oct 2024 Task 3 Strict transport security not enforced https://cfg.fa
Advisory Request Response Path to issue
Strict transport security not enforced
Severity: Low
Confidence: Certain
URL: https://cfg.fastly.com/robots.txt
Issue description
The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption, and use the application as a platform for attacks against its users. This attack is performed by rewriting HTTPS links as HTTP, so that if a targeted user follows a link to the site from an HTTP page, their browser never attempts to use an encrypted connection. The sslstrip tool automates this process.
To exploit this vulnerability, an attacker must be suitably positioned to intercept and modify the victim's network traffic.This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common

Vulnerabilities:

1 User Agent Header Manipulation

Vulnerability Title	User Agent Header Manipulation
Vulnerability Description	User-Agent Header Manipulation refers to altering the "User-Agent" field in HTTP requests. This field typically contains information about the browser or device making the request. By manipulating this value, attackers can bypass security filters, initiate attacks like Cross-Site Scripting (XSS), or access parts of the application that are restricted based on User-Agent.
Affected Components	Web server applications that rely on User-Agent for filtering or access control. Logging systems that depend on User-Agent headers for tracking user activity. APIs or services that apply specific rules based on User-Agent information.
Impact Assessment	Circumvention of security policies based on User-Agent filtering. Possible exploitation of application vulnerabilities when coupled with other attack vectors. Inaccurate logging and monitoring of user activity, leading to incomplete forensic data. .
Steps to Reproduce	Use a tool like Burp Suite or an HTTP client. Modify the User-Agent header in the request to a custom string or inject malicious payloads . Send the modified request to the server. Observe if the server behaves differently .
Proof of Concept	curl -A "Mozilla/5.0 (hackedUserAgent)" http://example.com
Proposed Mitigation or Fix	Avoid reliance on User-Agent headers for access control or security decisions. Implement strict input validation and sanitization for all incoming data, including User-Agent headers. Employ Content Security Policy (CSP) and other protective mechanisms to reduce the impact of injected payloads.

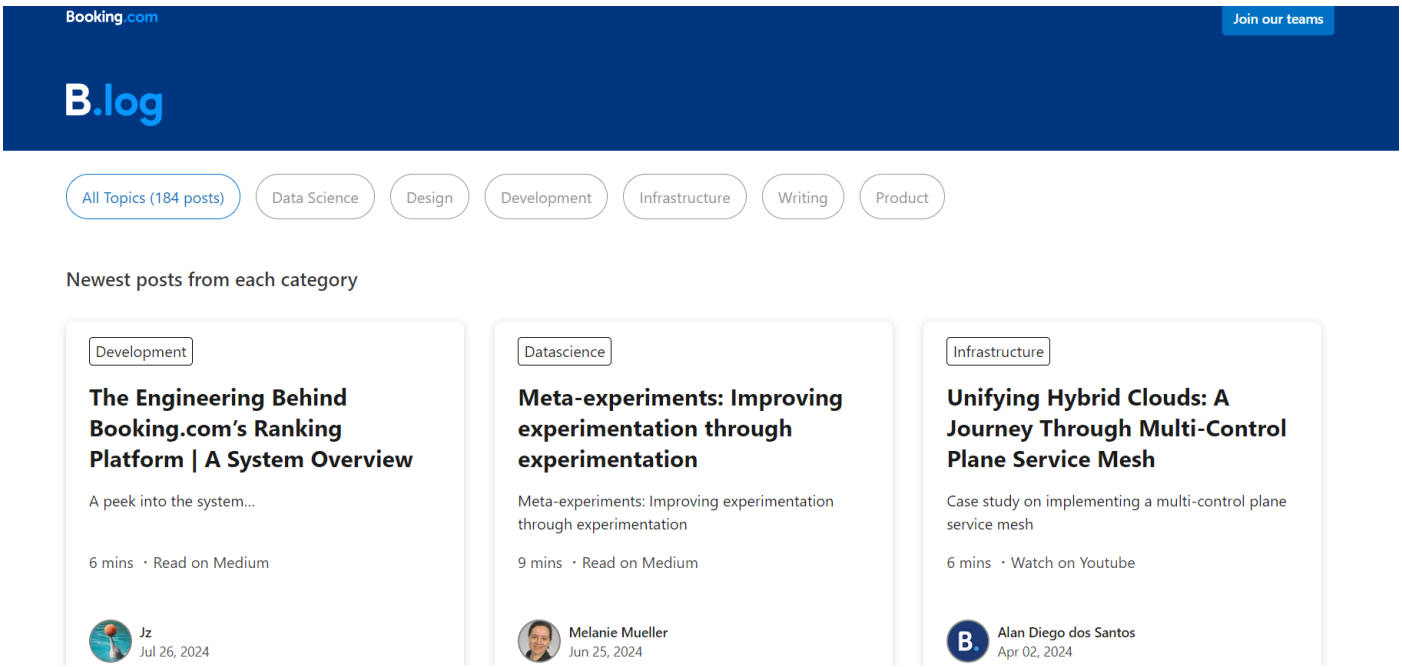
Report 09 Target Details



The target for this Bug Bounty report is domain-booking.com (https://www.booking.com), a platform providing travel and accommodation booking services for consumers worldwide. The company offers a comprehensive range of services including hotel reservations, flight bookings, rental car services, and vacation packages. domain-booking.com's platform is designed to help travelers find and book accommodations and travel services easily, leveraging modern booking technologies and user-friendly interfaces.

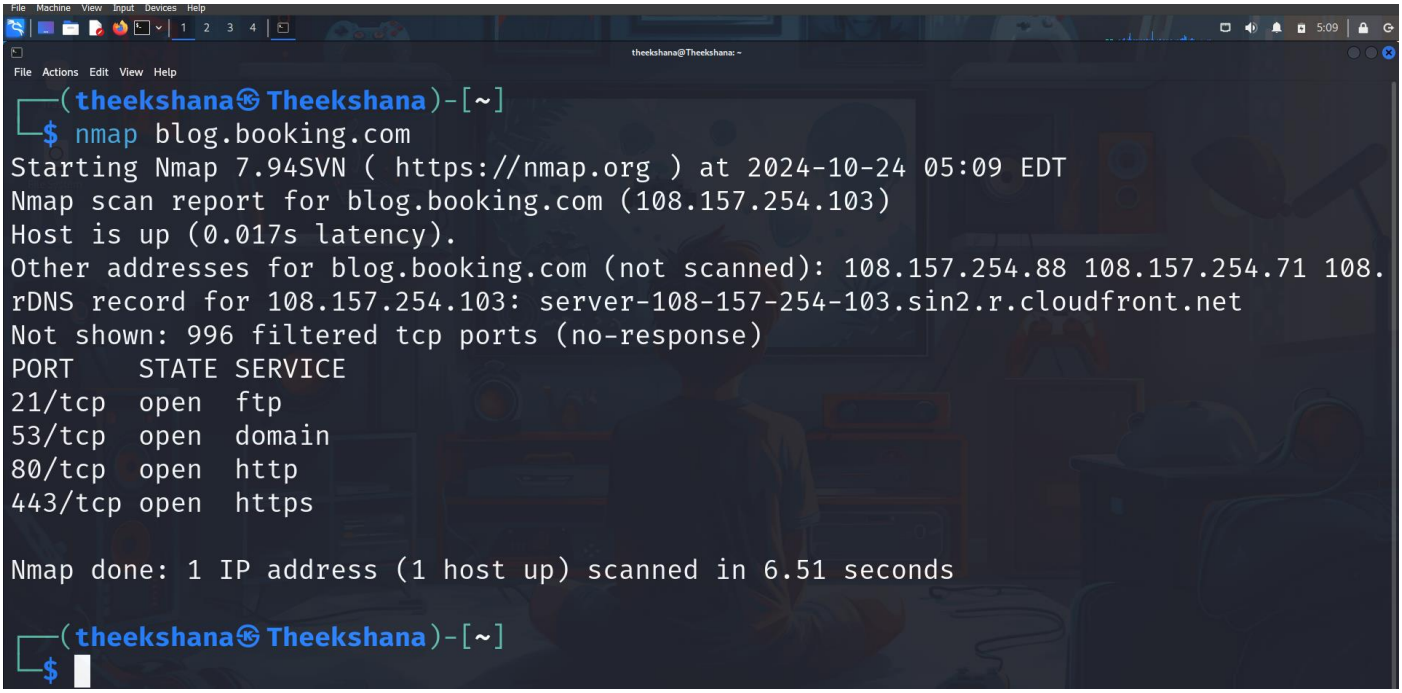
In this report, I have chosen to focus on 10 subdomains under the main domain domain-booking.com. Each subdomain serves different functionalities or services, potentially introducing distinct security risks, particularly in areas related to user data, payment processing, and booking systems. These subdomains were selected based on their relevance and the likelihood of containing vulnerabilities.

This report covers the findings for the subdomain: blog.booking.com



Target Reconnaissance

Nmap Scan

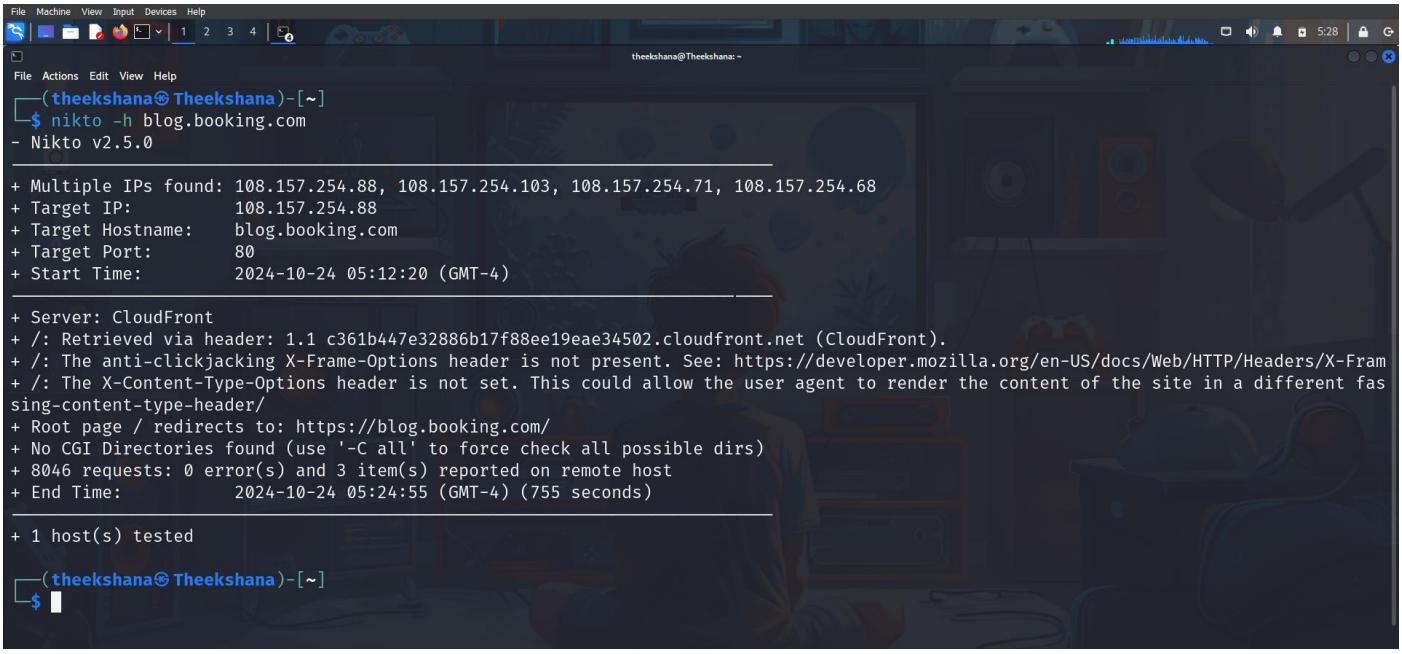


By scanning blog.booking.com with Nmap I found out these information.

Port	State	Service
21/tcp	Open	FTP
53/tcp	Open	DOMAIN
80/tcp	Open	HTTP
443/tcp	Open	HTPPS

Port	State	Service	Potential Vulnerabilities
21/tcp	Open	FTP	Data is not encrypted, so sensitive information can be stolen. Hackers can guess passwords (brute force attacks) Misconfigurations might allow unauthorized access
53/tcp	Open	DNS	Attackers can redirect users to fake sites (DNS poisoning) Hackers might flood the system (amplification attacks) Sensitive DNS info could be exposed (zone transfer)
80/tcp	Open	HTTP	Data is not secure (no encryption) Hackers can inject harmful scripts (XSS)
443/tcp	Open	HTTPS	If not properly secured, attackers can intercept data Older encryption protocols may be weak

Nikto Scan



The screenshot shows the output of a Nikto scan against the target blog.booking.com which reveals several potential security issues and misconfigurations.

Target Information:

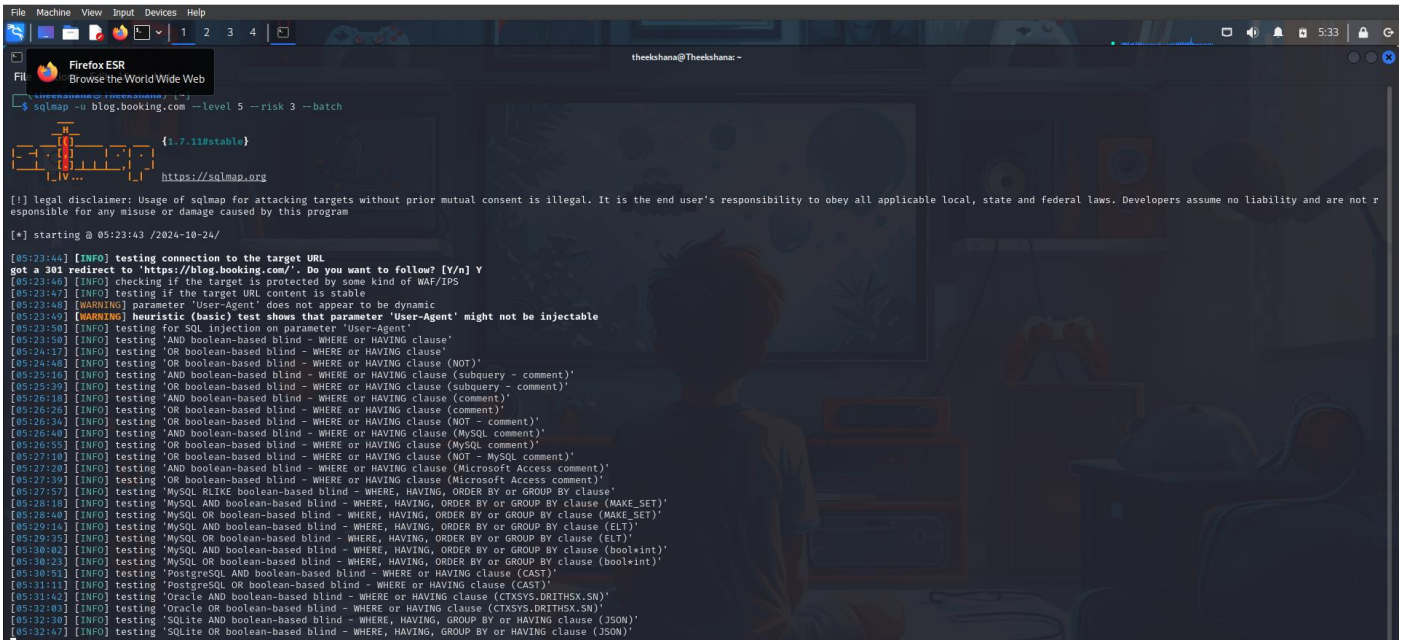
- **Target IP**: 108.157.254.88 (one of the IPs resolved for the domain).
- **Target Hostname**: blog.booking.com
- **Target Port**: 80 (HTTP traffic).

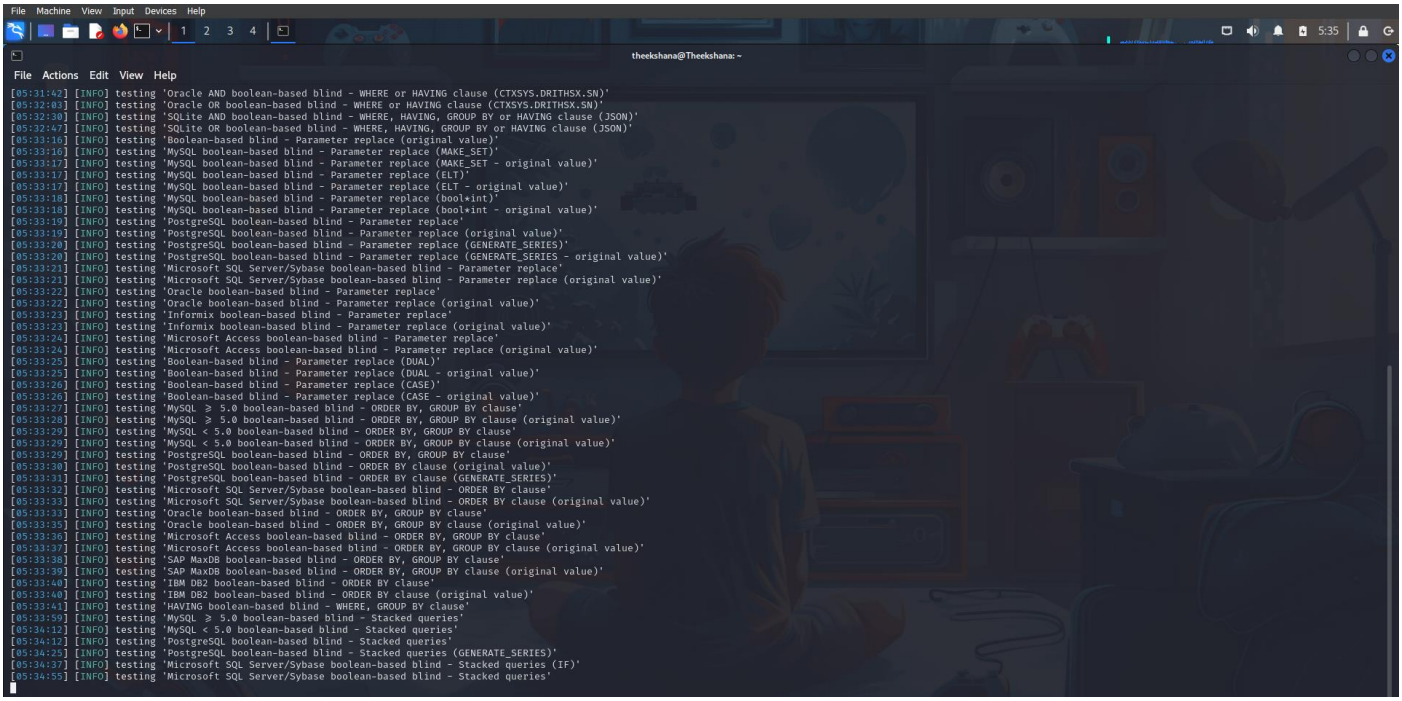
Issues Found:

- **X-Frame-Options Header Not Present**: This means the site does not use the X-Frame-Options header, which can lead to clickjacking attacks. The header is used to prevent the site from being embedded in an iframe on another page.

- **X-Content-Type-Options Header Not Set**: This means the server does not send the X-Content-Type-Options header. Without it, some browsers might allow MIME-type sniffing, potentially leading to security vulnerabilities like cross-site scripting (XSS).

SQLmap Scaner

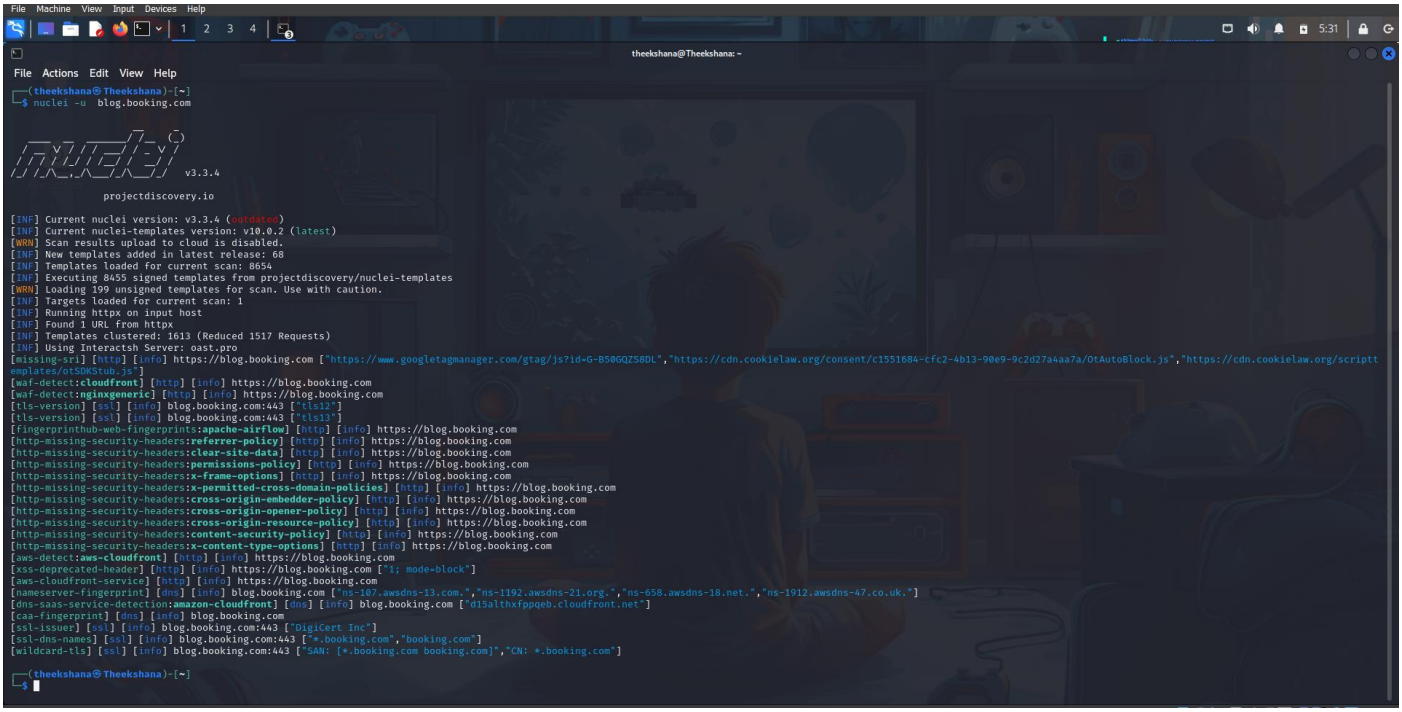




Techniques Tested:

- The tool tried several SQL injection techniques, including:
  - **Boolean-based blind SQL injection**: It tests queries that rely on conditions to confirm if injection is possible.
  - **AND/OR blind**: Uses AND and OR clauses to manipulate SQL statements and determine vulnerability.
  - **HAVING, ORDER BY, GROUP BY clauses**: These are SQL statements used to filter and sort query results, and they were tested for potential injection points.

Nuclei Scan



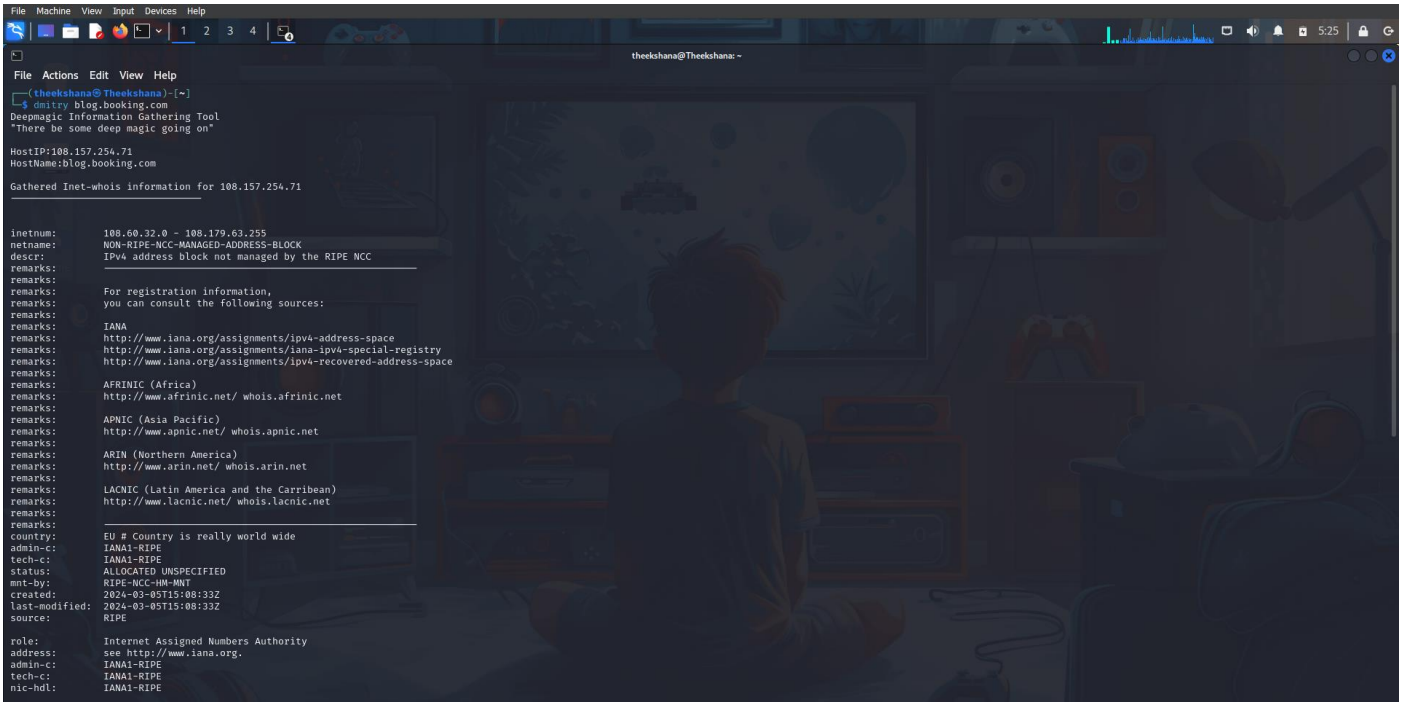
Missing Security Headers:

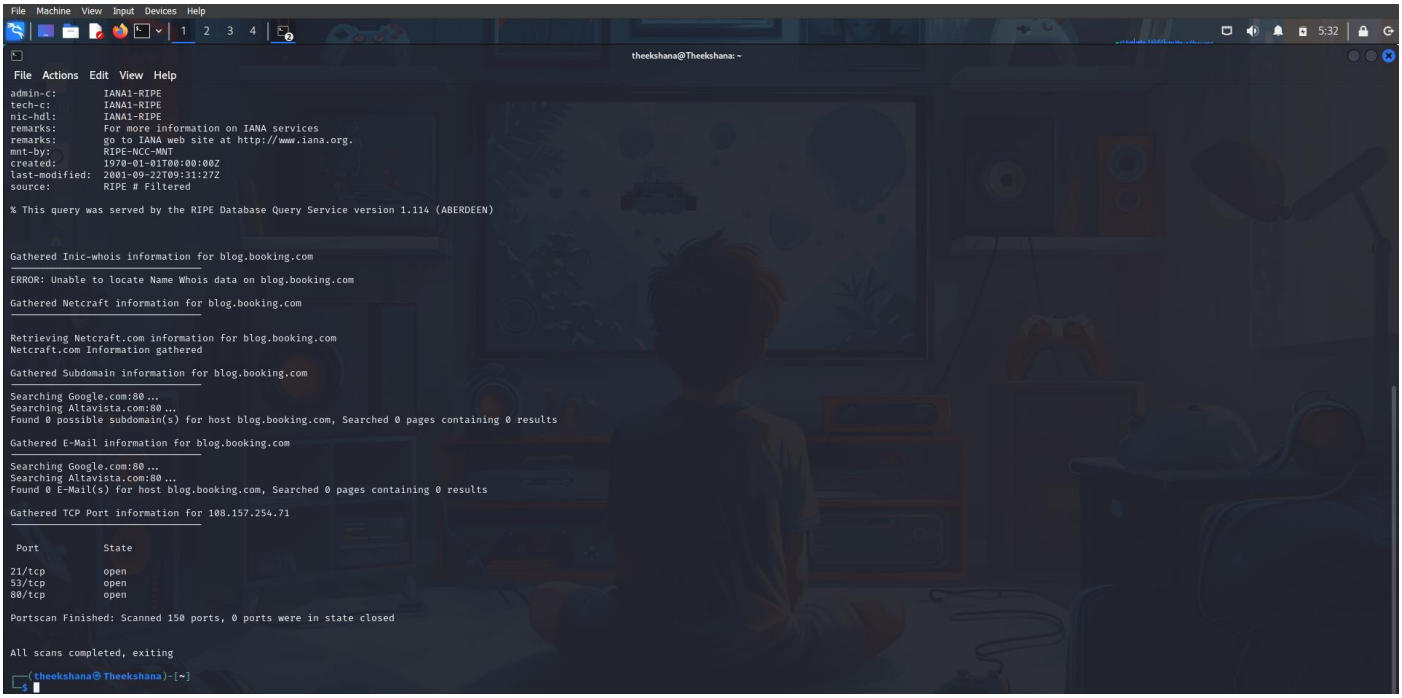
- **X-Content-Type-Options**: Not set, which could lead to content-type sniffing vulnerabilities.
- **X-Frame-Options**: Missing, allowing clickjacking attacks.
- **X-XSS-Protection**: Missing, which prevents XSS (cross-site scripting) attack protection.
- **Cross-Origin Resource Sharing (CORS) Issues**: Several CORS-related headers are missing or misconfigured, which could expose sensitive resources to untrusted origins.
- **Permissions Policy**: Not set, which defines which browser features can be used.
- **Strict Transport Security**: Not set, which could allow downgrade attacks.

Multiple missing security headers related to:

- Content-Type options,
- XSS protection,
- Frame options,
- CORS policy,
- Permissions policy,
- HSTS (HTTP Strict Transport Security).

Dmitry Scan



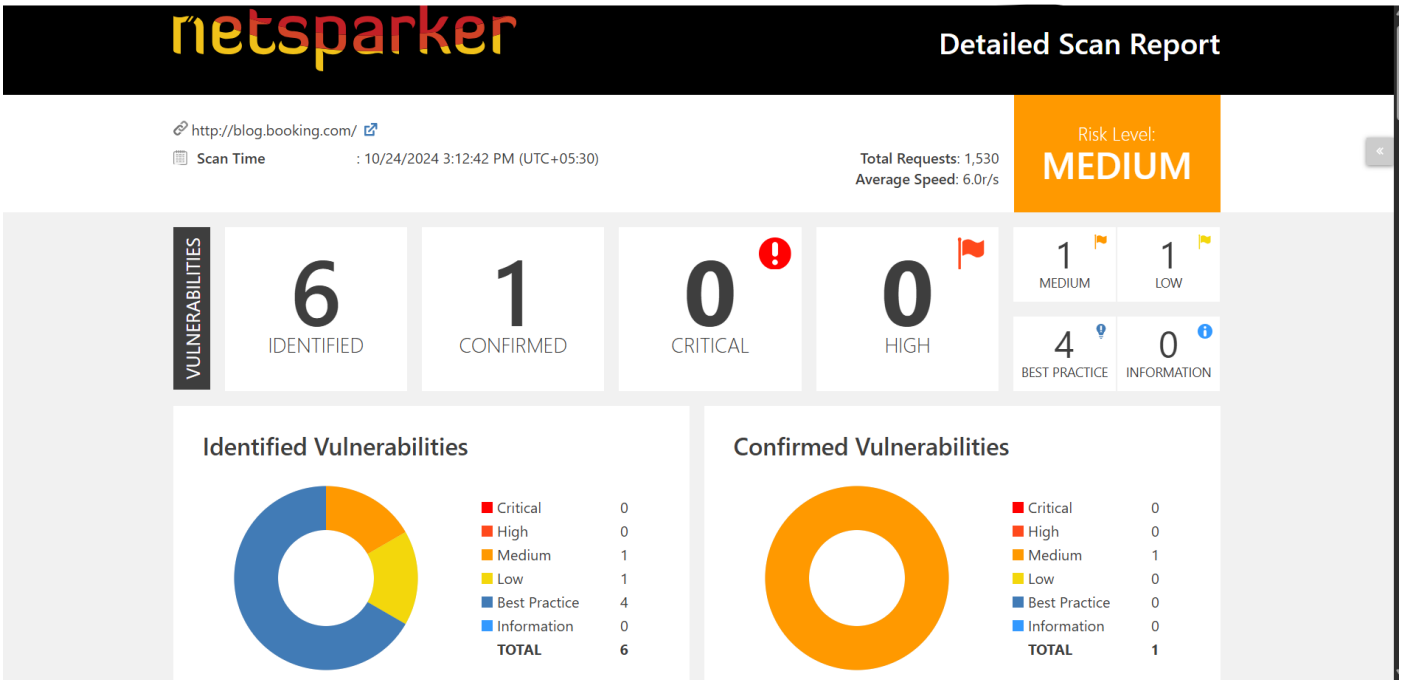


Port 21 (FTP - File Transfer Protocol): This port is typically used for file transfer services. Having FTP open can be risky if not properly secured, as it often transmits data in plain text (though secure variants like SFTP exist).

Port 53 (DNS - Domain Name System): This port is used for DNS services, which translate domain names into IP addresses. While DNS services need to be accessible, misconfigurations or vulnerabilities (like DNS amplification attacks) can expose the server to risks.

Port 80 (HTTP - Hypertext Transfer Protocol): This port is used for unencrypted web traffic. Port 80 being open suggests that the website is accessible via HTTP, but this should be redirected to HTTPS (Port 443) for encrypted communication. If not, it leaves the site vulnerable to man-in-the middle (MITM) attacks.

Netsparker



Vulnerability Summary

SEVERITY FILTER : CRITICAL HIGH MEDIUM LOW BEST PRACTICE INFORMATION

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Weak Ciphers Enabled	GET	https://blog.booking.com/	
	Missing X-Frame-Options Header	GET	https://blog.booking.com/.well-known/	
	Content Security Policy (CSP) Not Implemented	GET	https://blog.booking.com/.well-known/	
	Expect-CT Not Enabled	GET	https://blog.booking.com/main.js	
	Referrer-Policy Not Implemented	GET	https://blog.booking.com/.well-known/	
	Subresource Integrity (SRI) Not Implemented	GET	http://blog.booking.com/	

Weak Ciphers Enabled

MEDIUM 1 CONFIRMED 1

Netsparker detected that weak ciphers are enabled during secure communication (SSL).

You should allow only strong ciphers on your web server to protect secure communication with your visitors.

Impact

Attackers might decrypt SSL traffic between your server and your visitors.

Vulnerabilities

1.1. https://blog.booking.com/ CONFIRMED

Hide Remediation

Actions to Take

1. For Apache, you should modify the SSLCipherSuite directive in the `httpd.conf`.

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

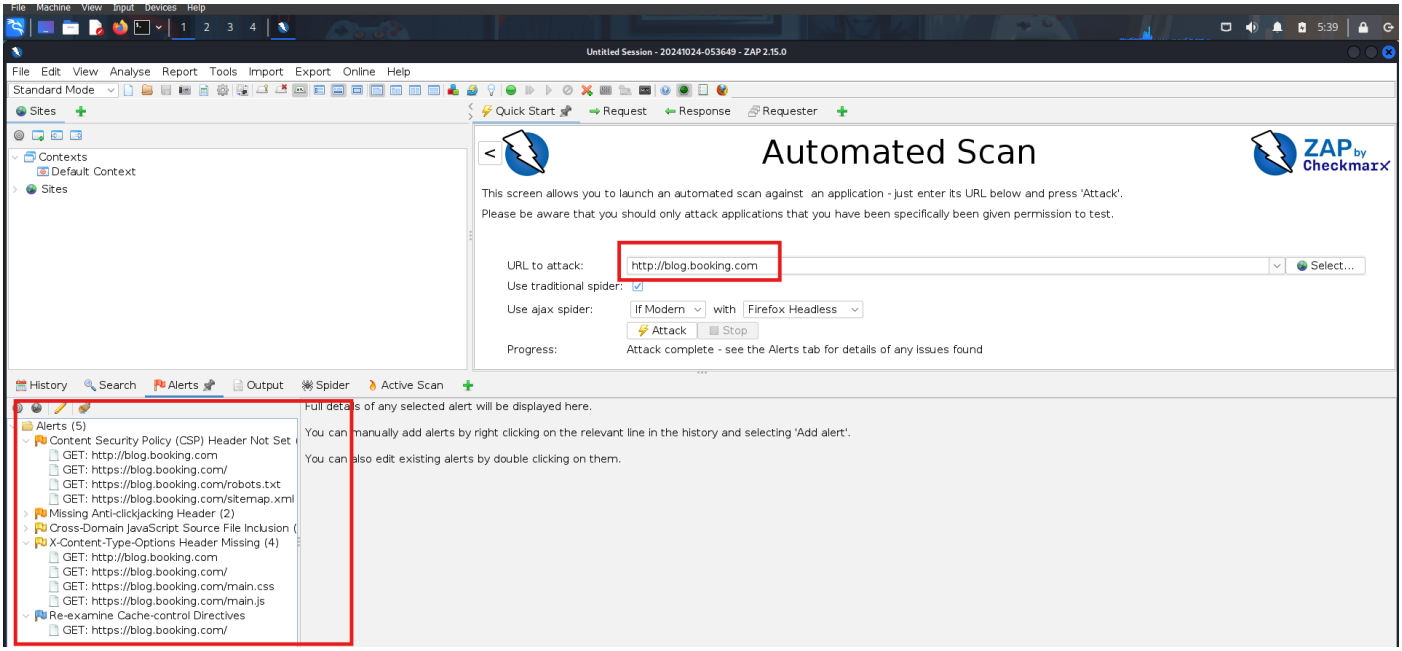
2. Lighttpd:

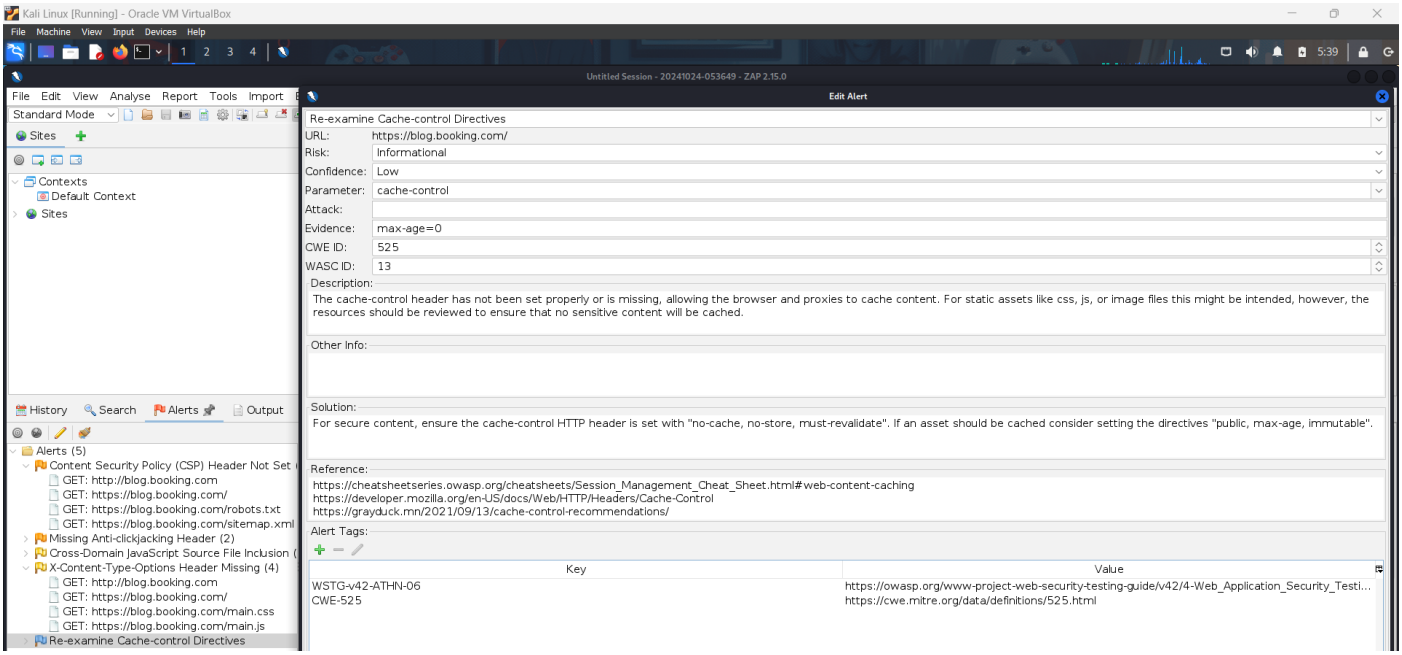
```
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

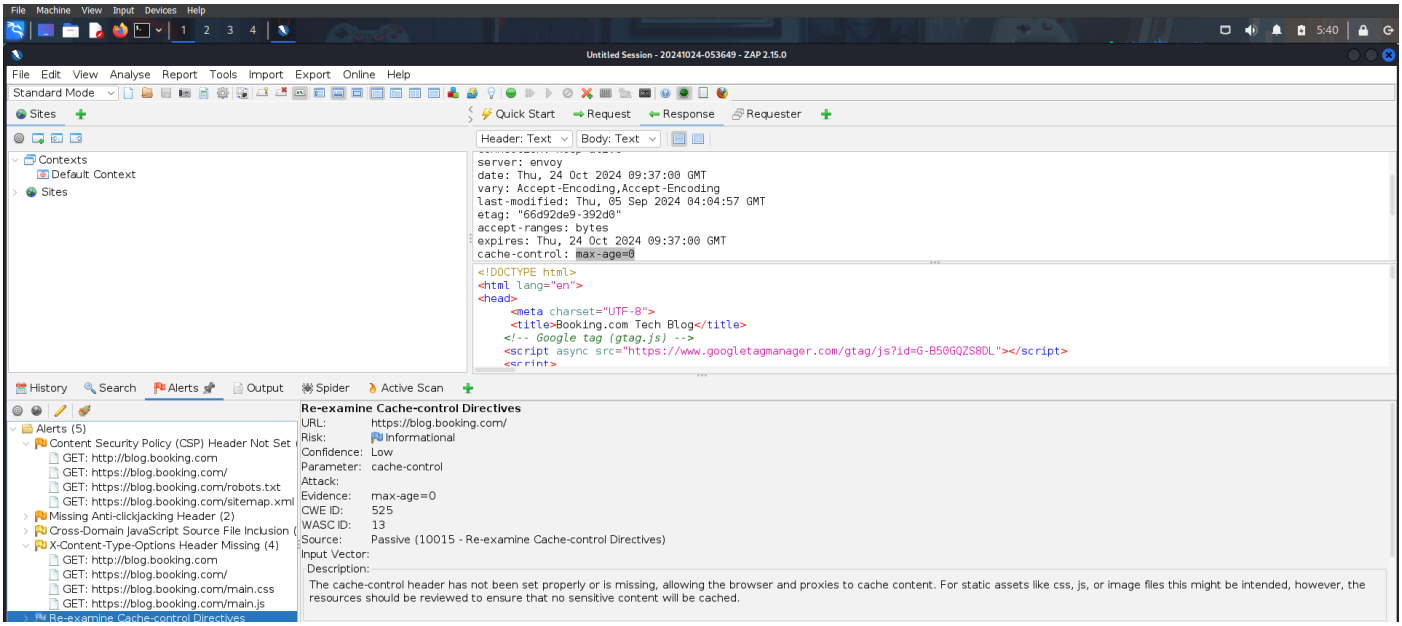
CLASSIFICATION

PCI DSS v3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	327
CAPEC	7
WASC	4

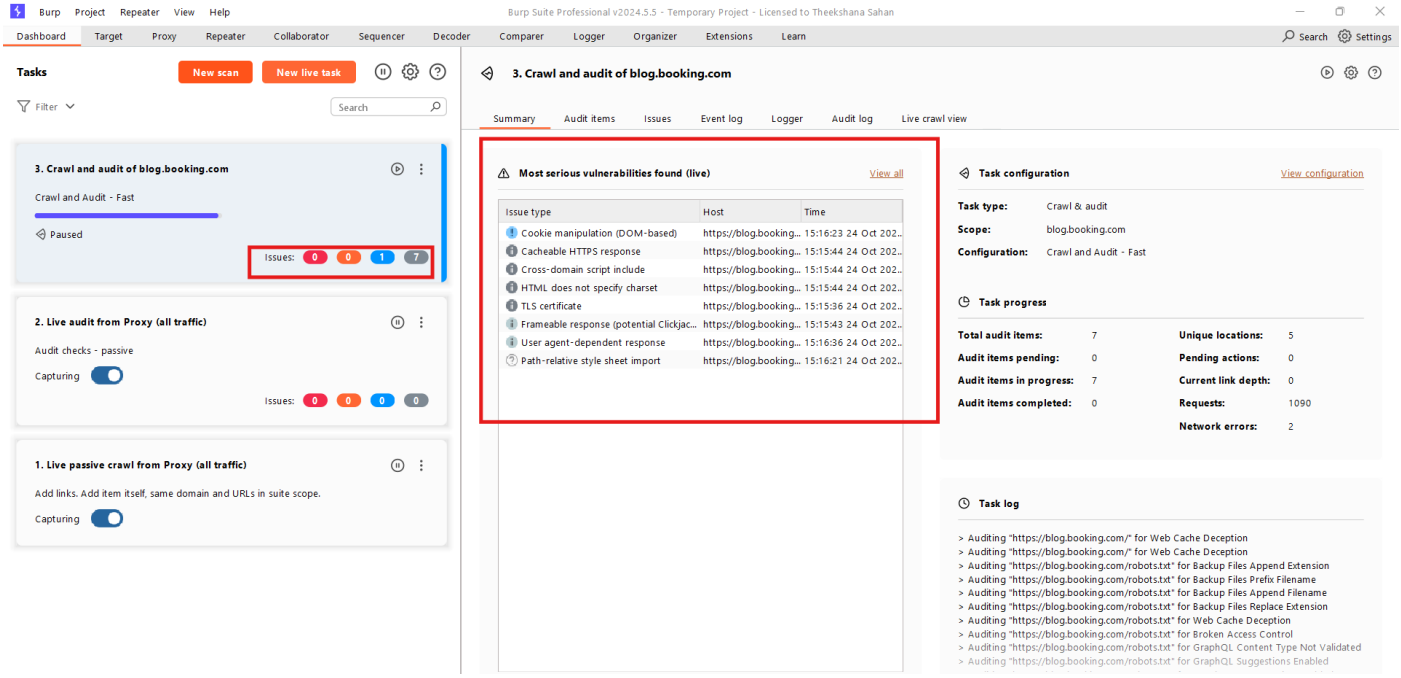
OWASP ZAP

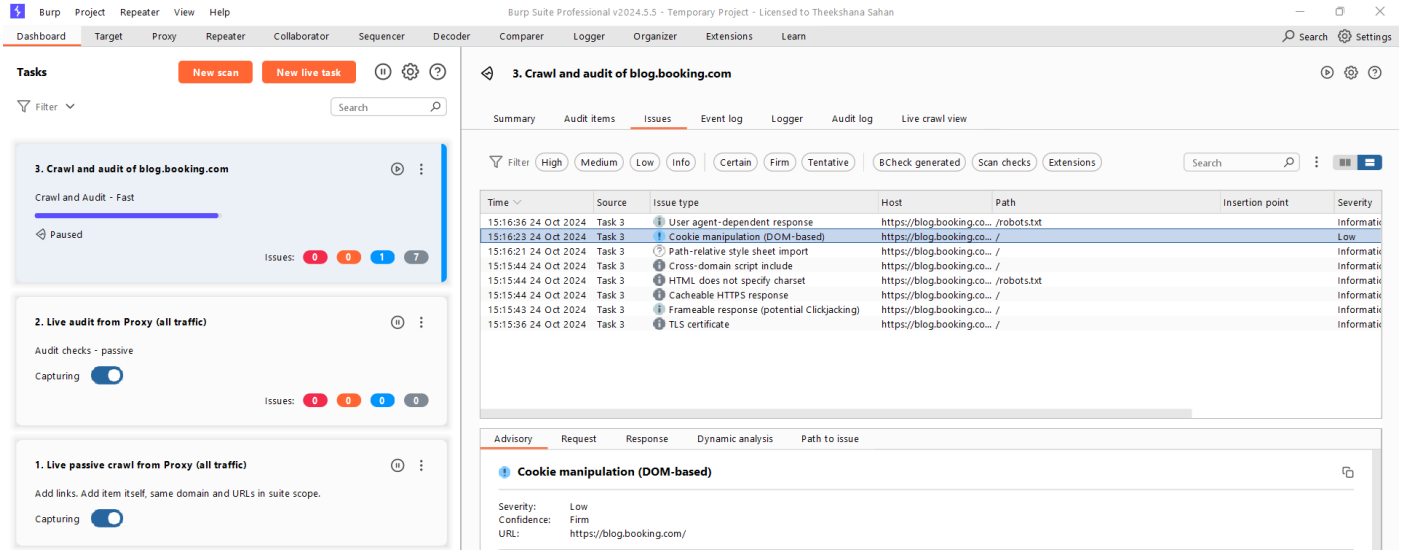

Untitled Session - 20241024-053649 - ZAP 2.15.0
Automated Scan
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack: http://blog.booking.com
Use traditional spider:
Use ajax spider: If Modern with Firefox Headless
Attack Stop
Progress: Attack complete - see the Alerts tab for details of any issues found
Alerts (5)
Content Security Policy (CSP) Header Not Set
GET: http://blog.booking.com
GET: https://blog.booking.com/
GET: https://blog.booking.com/robots.txt
GET: https://blog.booking.com/sitemap.xml
Missing Anti-clickjacking Header (2)
Cross-Domain JavaScript Source File Inclusion
X-Content-Type-Options Header Missing (4)
GET: http://blog.booking.com
GET: https://blog.booking.com/
GET: https://blog.booking.com/main.css
GET: https://blog.booking.com/main.js
Re-examine Cache-control Directives
GET: https://blog.booking.com/
Full details of any selected alert will be displayed here.
You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.
You can also edit existing alerts by double clicking on them.

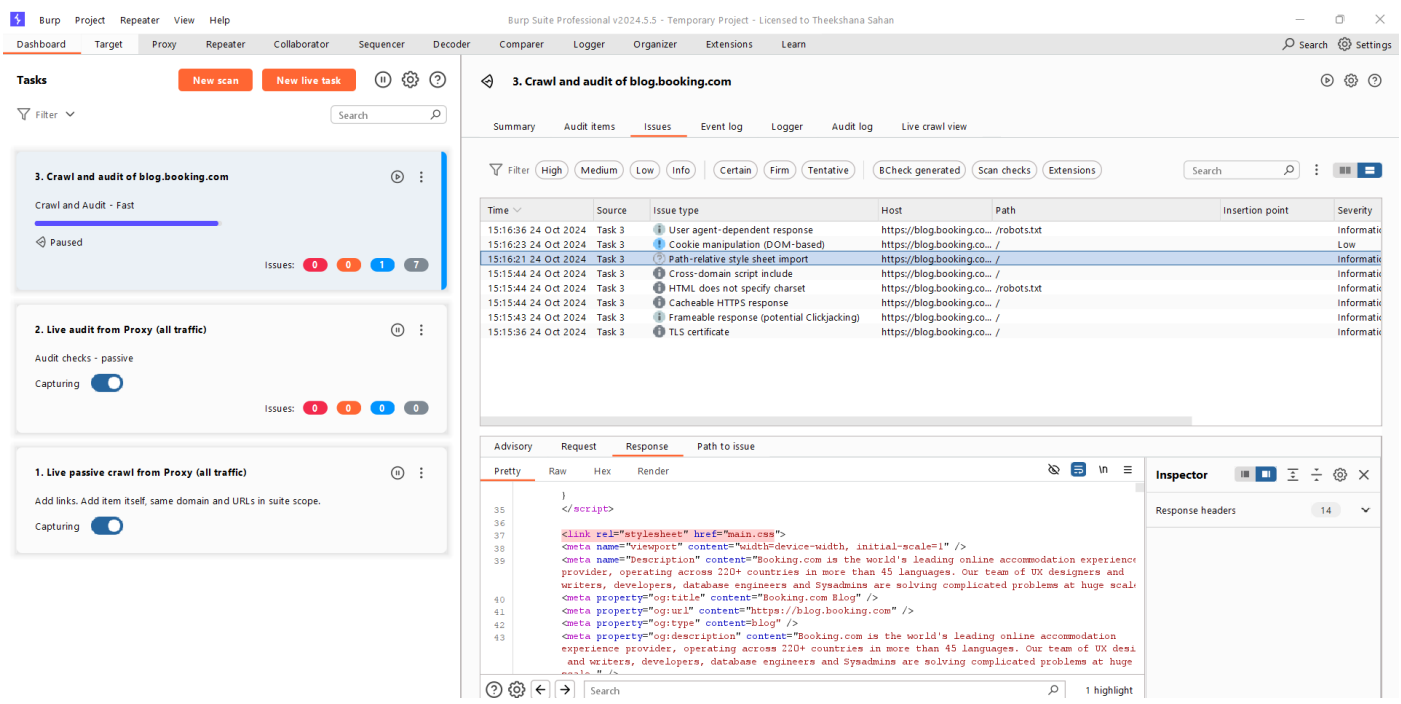

Kali Linux [Running] - Oracle VM VirtualBox
Edit Alert
Re-examine Cache-control Directives
URL: https://blog.booking.com/
Risk: Informational
Confidence: Low
Parameter: cache-control
Attack:
Evidence: max-age=0
CWE ID: 525
WASC ID: 13
Description:
The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Other Info:
Solution:
For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Reference:
https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control
https://grayduck.mn/2021/09/13/cache-control-recommendations/
Alert Tags:
Key
Value
WSTG-v42-ATHN-06
https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testi...
CWE-525
https://cwe.mitre.org/data/definitions/525.html


Quick Start
Request
Response
Requester
server: envoy
date: Thu, 24 Oct 2024 09:37:00 GMT
vary: Accept-Encoding,Accept-Encoding
last-modified: Thu, 05 Sep 2024 04:04:57 GMT
etag: "66d92de9-392d0"
accept-ranges: bytes
expires: Thu, 24 Oct 2024 09:37:00 GMT
cache-control: max-age=0
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<title>Booking.com Tech Blog</title>
<!-- Google tag (gtag.js) -->
<script async src="https://www.googletagmanager.com/gtag/js?id=G-B50GQZS8DL"></script>
Re-examine Cache-control Directives
URL: https://blog.booking.com/
Risk: Informational
Confidence: Low
Parameter: cache-control
Attack:
Evidence: max-age=0
CWE ID: 525
WASC ID: 13
Source: Passive (10015 - Re-examine Cache-control Directives)
Input Vector:
Description:
The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

Burp Suite


Burp Project Repeater View Help
Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan
Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Tasks
New scan
New live task
3. Crawl and audit of blog.booking.com
Crawl and Audit - Fast
Paused
Issues: 0 0 1 7
2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing
Issues: 0 0 0 0
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing
3. Crawl and audit of blog.booking.com
Summary Audit items Issues Event log Logger Audit log Live crawl view
Most serious vulnerabilities found (live)
View all
Issue type Host Time
Cookie manipulation (DOM-based) https://blog.booking... 15:16:23 24 Oct 202...
Cacheable HTTPS response https://blog.booking... 15:15:44 24 Oct 202...
Cross-domain script include https://blog.booking... 15:15:44 24 Oct 202...
HTML does not specify charset https://blog.booking... 15:15:44 24 Oct 202...
TLS certificate https://blog.booking... 15:15:36 24 Oct 202...
Frameable response (potential Clickjac... https://blog.booking... 15:15:43 24 Oct 202...
User agent-dependent response https://blog.booking... 15:16:36 24 Oct 202...
Path-relative style sheet import https://blog.booking... 15:16:21 24 Oct 202...
Task configuration
View configuration
Task type: Crawl & audit
Scope: blog.booking.com
Configuration: Crawl and Audit - Fast
Task progress
Total audit items: 7
Audit items pending: 0
Audit items in progress: 7
Audit items completed: 0
Unique locations: 5
Pending actions: 0
Current link depth: 0
Requests: 1090
Network errors: 2
Task log
> Auditing "https://blog.booking.com/" for Web Cache Deception
> Auditing "https://blog.booking.com/" for Web Cache Deception
> Auditing "https://blog.booking.com/robots.txt" for Backup Files Append Extension
> Auditing "https://blog.booking.com/robots.txt" for Backup Files Prefix Filename
> Auditing "https://blog.booking.com/robots.txt" for Backup Files Append Filename
> Auditing "https://blog.booking.com/robots.txt" for Backup Files Replace Extension
> Auditing "https://blog.booking.com/robots.txt" for Web Cache Deception
> Auditing "https://blog.booking.com/robots.txt" for Broken Access Control
> Auditing "https://blog.booking.com/robots.txt" for GraphQL Content Type Not Validated
> Auditing "https://blog.booking.com/robots.txt" for GraphQL Suggestions Enabled


Burp Project Repeater View Help
Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan
Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Tasks
New scan
New live task
3. Crawl and audit of blog.booking.com
Crawl and Audit - Fast
Paused
Issues: 0 0 1 7
2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing
Issues: 0 0 0 0
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing
3. Crawl and audit of blog.booking.com
Summary Audit items Issues Event log Logger Audit log Live crawl view
Filter High Medium Low Info Certain Firm Tentative BCheck generated Scan checks Extensions
Search
Time Source Issue type Host Path Insertion point Severity
15:16:36 24 Oct 2024 Task 3 User agent-dependent response https://blog.booking.co... /robots.txt Informati
15:16:23 24 Oct 2024 Task 3 Cookie manipulation (DOM-based) https://blog.booking.co... / Low
15:16:21 24 Oct 2024 Task 3 Path-relative style sheet import https://blog.booking.co... / Informati
15:15:44 24 Oct 2024 Task 3 Cross-domain script include https://blog.booking.co... / Informati
15:15:44 24 Oct 2024 Task 3 HTML does not specify charset https://blog.booking.co... /robots.txt Informati
15:15:44 24 Oct 2024 Task 3 Cacheable HTTPS response https://blog.booking.co... / Informati
15:15:43 24 Oct 2024 Task 3 Frameable response (potential Clickjacking) https://blog.booking.co... / Informati
15:15:36 24 Oct 2024 Task 3 TLS certificate https://blog.booking.co... / Informati
Advisory Request Response Dynamic analysis Path to issue
Cookie manipulation (DOM-based)
Severity: Low
Confidence: Firm
URL: https://blog.booking.com/

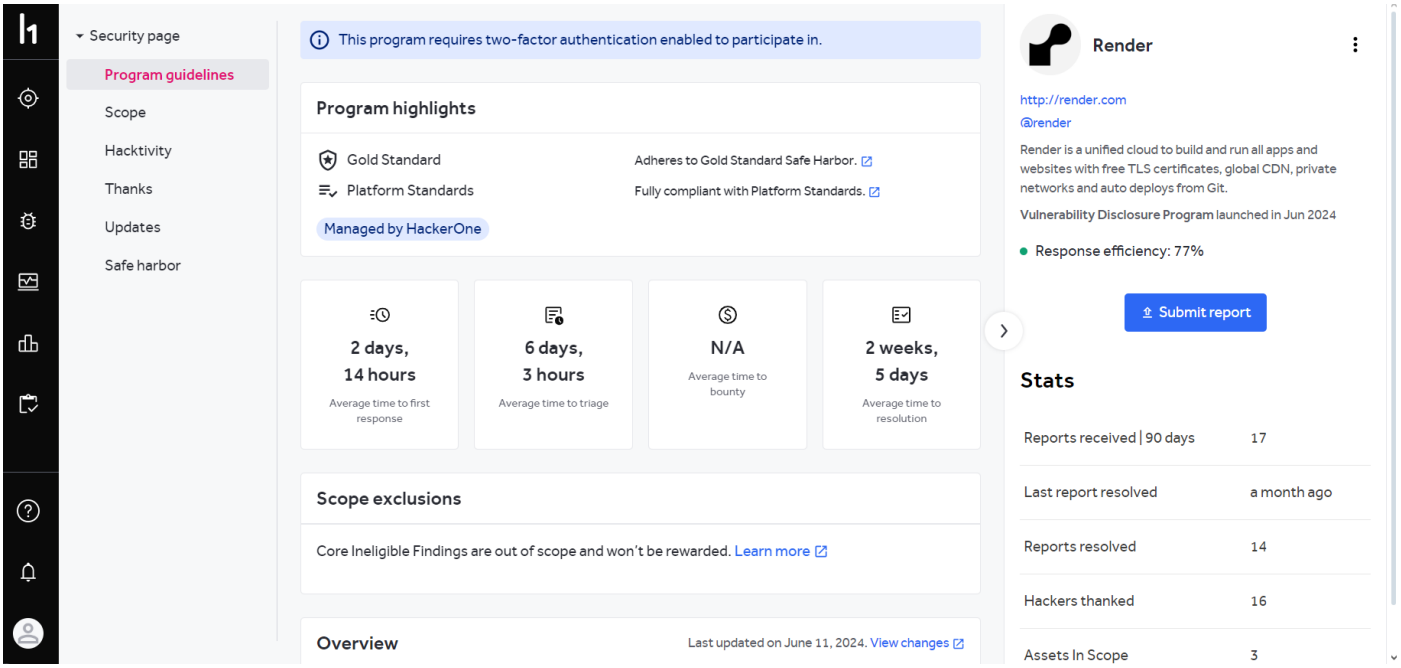

Burp Project Repeater View Help
Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan
Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Tasks
New scan
New live task
3. Crawl and audit of blog.booking.com
Crawl and Audit - Fast
Paused
Issues: 0 0 1 7
2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing
Issues: 0 0 0 0
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing
3. Crawl and audit of blog.booking.com
Summary Audit items Issues Event log Logger Audit log Live crawl view
Filter High Medium Low Info Certain Firm Tentative BCheck generated Scan checks Extensions
Search
Time Source Issue type Host Path Insertion point Severity
15:16:36 24 Oct 2024 Task 3 User agent-dependent response https://blog.booking.co... /robots.txt Informati
15:16:23 24 Oct 2024 Task 3 Cookie manipulation (DOM-based) https://blog.booking.co... / Low
15:16:21 24 Oct 2024 Task 3 Path-relative style sheet import https://blog.booking.co... / Informati
15:15:44 24 Oct 2024 Task 3 Cross-domain script include https://blog.booking.co... / Informati
15:15:44 24 Oct 2024 Task 3 HTML does not specify charset https://blog.booking.co... /robots.txt Informati
15:15:44 24 Oct 2024 Task 3 Cacheable HTTPS response https://blog.booking.co... / Informati
15:15:43 24 Oct 2024 Task 3 Frameable response (potential Clickjacking) https://blog.booking.co... / Informati
15:15:36 24 Oct 2024 Task 3 TLS certificate https://blog.booking.co... / Informati
Advisory Request Response Path to issue
Pretty Raw Hex Render
Inspector
Response headers 14
<link rel="stylesheet" href="main.css">
<meta name="viewport" content="width=device-width, initial-scale=1" />
<meta name="description" content="Booking.com is the world's leading online accommodation experience provider, operating across 220+ countries in more than 45 languages. Our team of UX designers and writers, developers, database engineers and Sysadmins are solving complicated problems at huge scal
<meta property="og:title" content="Booking.com Blog" />
<meta property="og:url" content="https://blog.booking.com" />
<meta property="og:type" content="blog" />
<meta property="og:description" content="Booking.com is the world's leading online accommodation experience provider, operating across 220+ countries in more than 45 languages. Our team of UX desi and writers, developers, database engineers and Sysadmins are solving complicated problems at huge
Search
1 highlight

Vulnerabilities:

1 Weak Ciphers Enabled

Vulnerability Title	Weak Ciphers Enabled
Vulnerability Description	The system or application is configured to support weak cryptographic ciphers, which are known to have vulnerabilities that can be exploited by attackers. This can lead to compromised communication channels, allowing attackers to decrypt or tamper with the data being transferred.
Affected Components	Any component that uses Secure Sockets Layer (SSL) or Transport Layer Security (TLS) for communication is vulnerable. This includes web servers, email servers, VPN services, or other services relying on encrypted data transmission. **Web servers :**If configured to allow weak ciphers, these servers could expose HTTPS traffic to attacks . **VPN servers**: Encryption between clients and the VPN server may be weak, risking exposure of sensitive corporate data. **Email servers**: Email communications protected by weak ciphers can be intercepted and decrypted. **Client-server applications**: Any custom or commercial application that uses weak ciphers for encryption in transit.
Impact Assessment	The use of weak ciphers can allow attackers to intercept and decrypt sensitive information, leading to data breaches, man-in-the-middle attacks, and unauthorized access. Depending on the sensitivity of the data, this can result in significant security risks for the organization.
Steps to Reproduce	Run an SSL/TLS scan on the affected server using tools like nmap with the ssl-enum-ciphers script, sslyze, or **SSL Labs** (a popular online tool).
Proof of Concept	Run an SSL/TLS scan on the system and provide a screenshot or log showing the weak ciphers being used. Tools like sslyze, OpenSSL, or Qualys SSL Test can generate the necessary output.
Proposed Mitigation or Fix	Disable weak ciphers in the system's configuration files . Implement stronger ciphers such as AES or GCM-based ciphers. Regularly review and update SSL/TLS configurations to adhere to the latest security best practices.

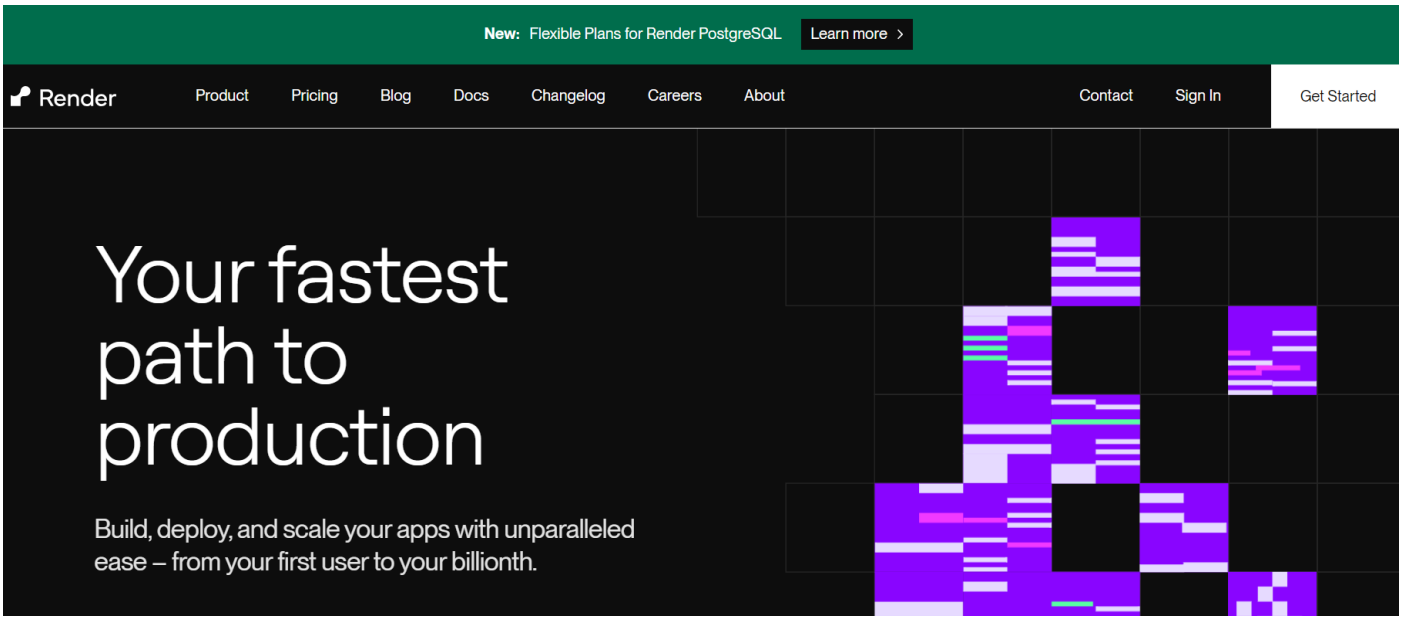
Report 10 Target Details



The target for this Bug Bounty report is render.com (https://www.render.com), a platform providing cloud hosting and deployment services for developers worldwide. The company offers a comprehensive range of services including web services hosting, static site deployment, database management, and containerized application deployment. render.com's platform is designed to help developers deploy and scale applications easily, leveraging modern cloud technologies and user-friendly interfaces.

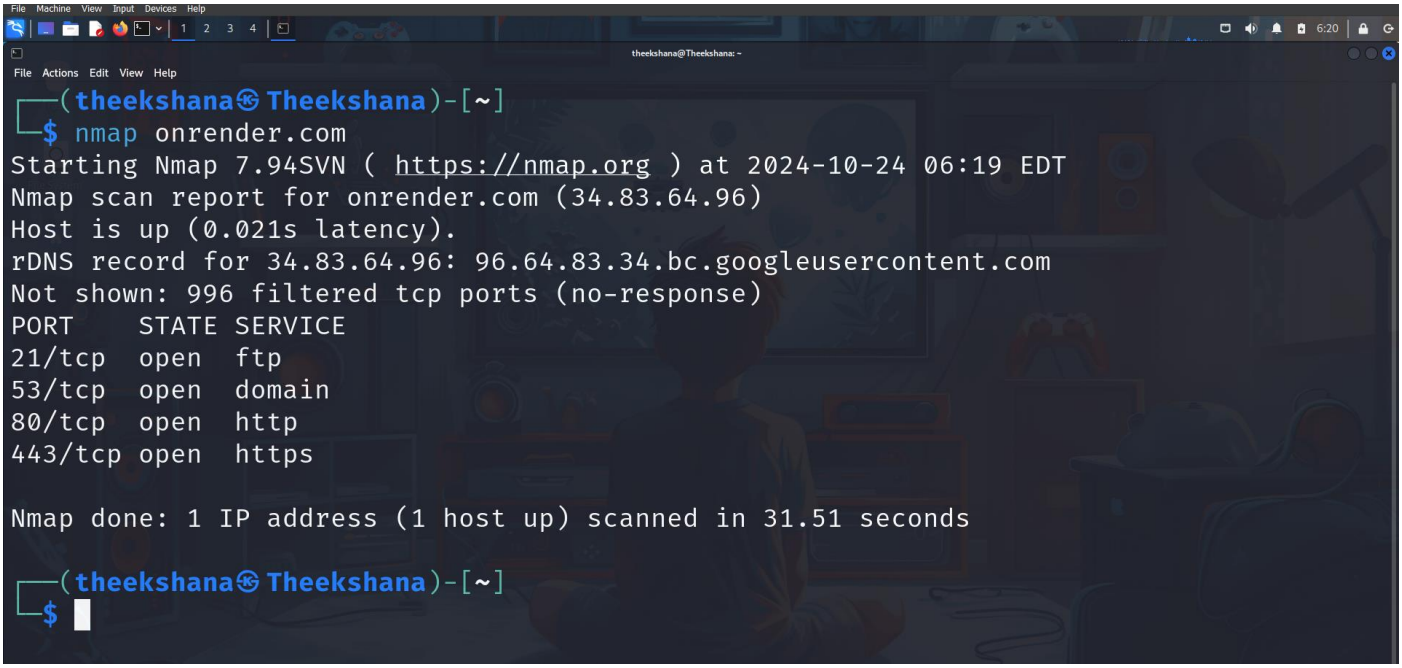
In this report, I have chosen to focus on 10 subdomains under the main domain render.com. Each subdomain serves different functionalities or services, potentially introducing distinct security risks, particularly in areas related to user data, application deployment, and infrastructure management. These subdomains were selected based on their relevance and the likelihood of containing vulnerabilities.

This report covers the findings for the subdomain: onrender.com



Target Reconnaissance

Nmap Scan

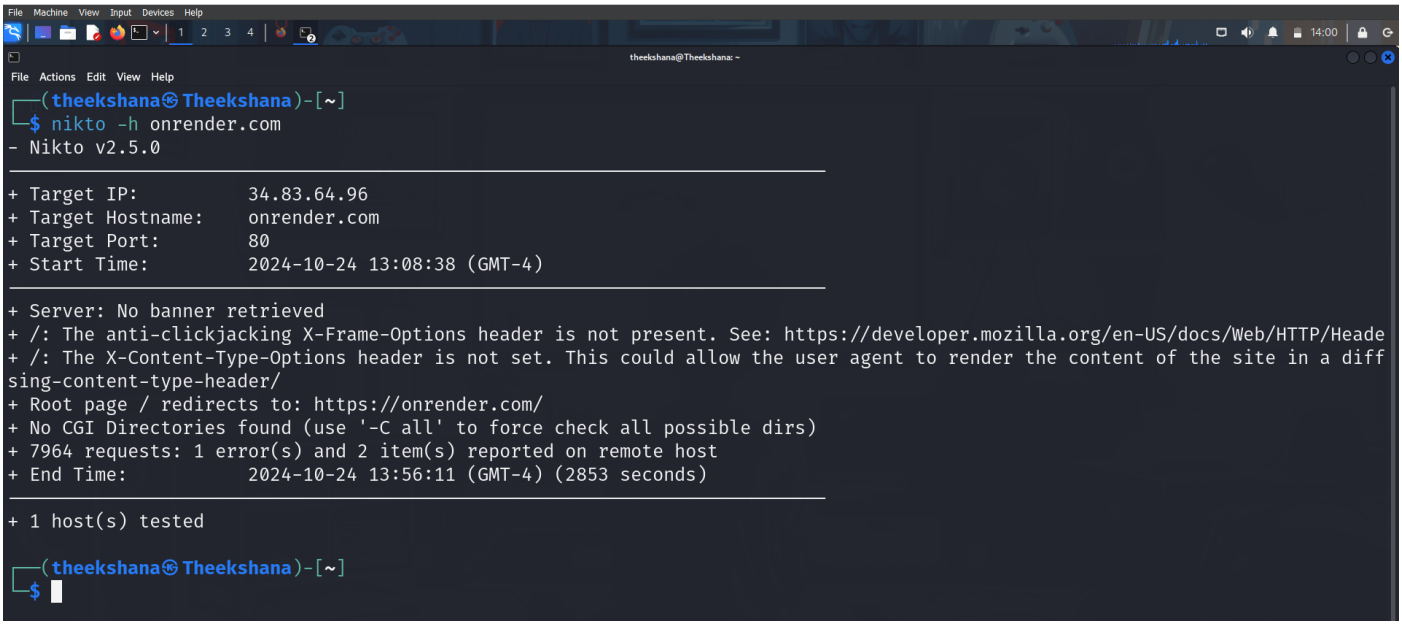


By onrender.com with Nmap I found out these information.

Port	State	Service
21/tcp	Open	FTP
53/tcp	Open	DOMAIN
80/tcp	Open	HTTP
443/tcp	Open	HTPPS

Port	State	Service	Potential Vulnerabilities
21/tcp	Open	FTP	Data is not encrypted, so sensitive information can be stolen. Hackers can guess passwords (brute force attacks) Misconfigurations might allow unauthorized access
53/tcp	Open	DNS	Attackers can redirect users to fake sites (DNS poisoning) Hackers might flood the system (amplification attacks) Sensitive DNS info could be exposed (zone transfer)
80/tcp	Open	HTTP	Data is not secure (no encryption) Hackers can inject harmful scripts (XSS)
443/tcp	Open	HTTPS	If not properly secured, attackers can intercept data Older encryption protocols may be weak

Nikto Scan



The screenshot shows the output of a Nikto scan against the target onrender.com which reveals several potential security issues and misconfigurations.

Target IP: 34.83.64.96 – This is the IP address of the target server.

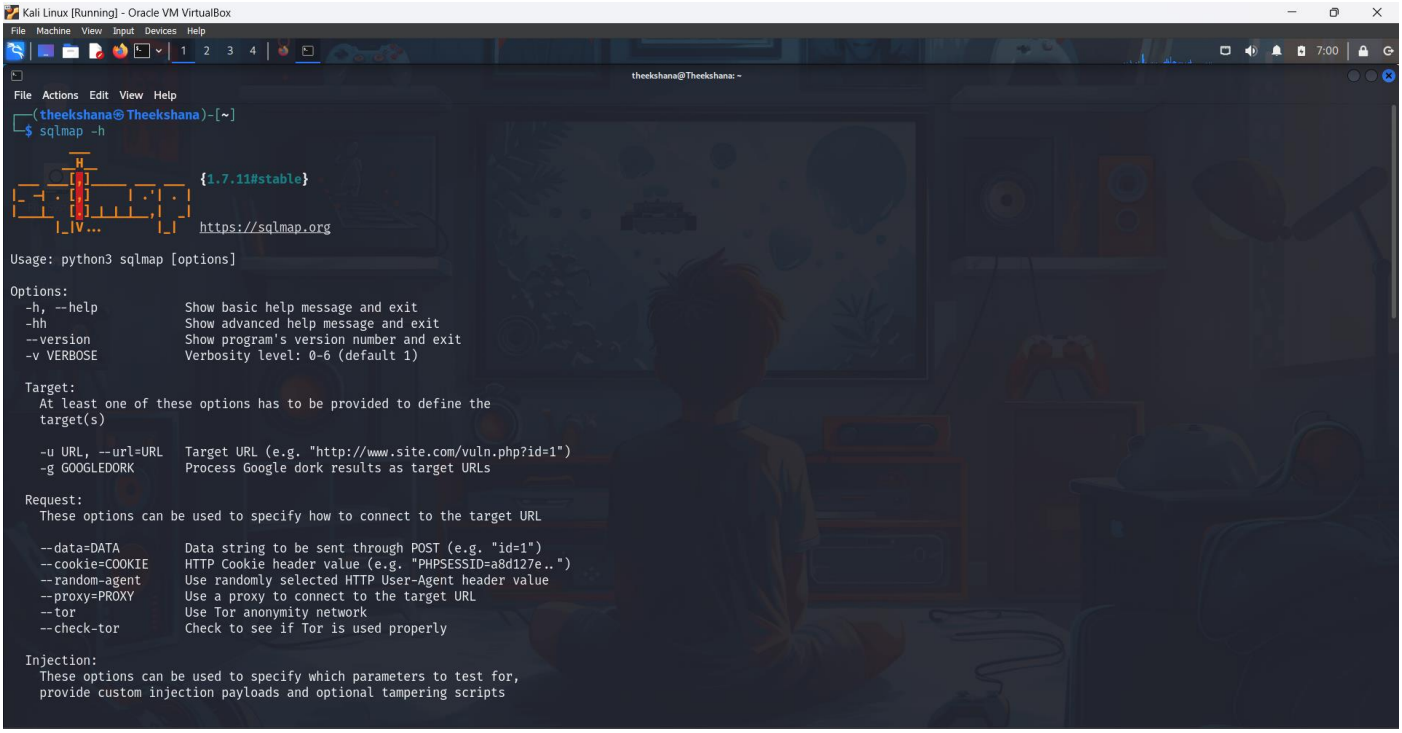
Target Hostname: onrender.com – The domain name of the server you are scanning.

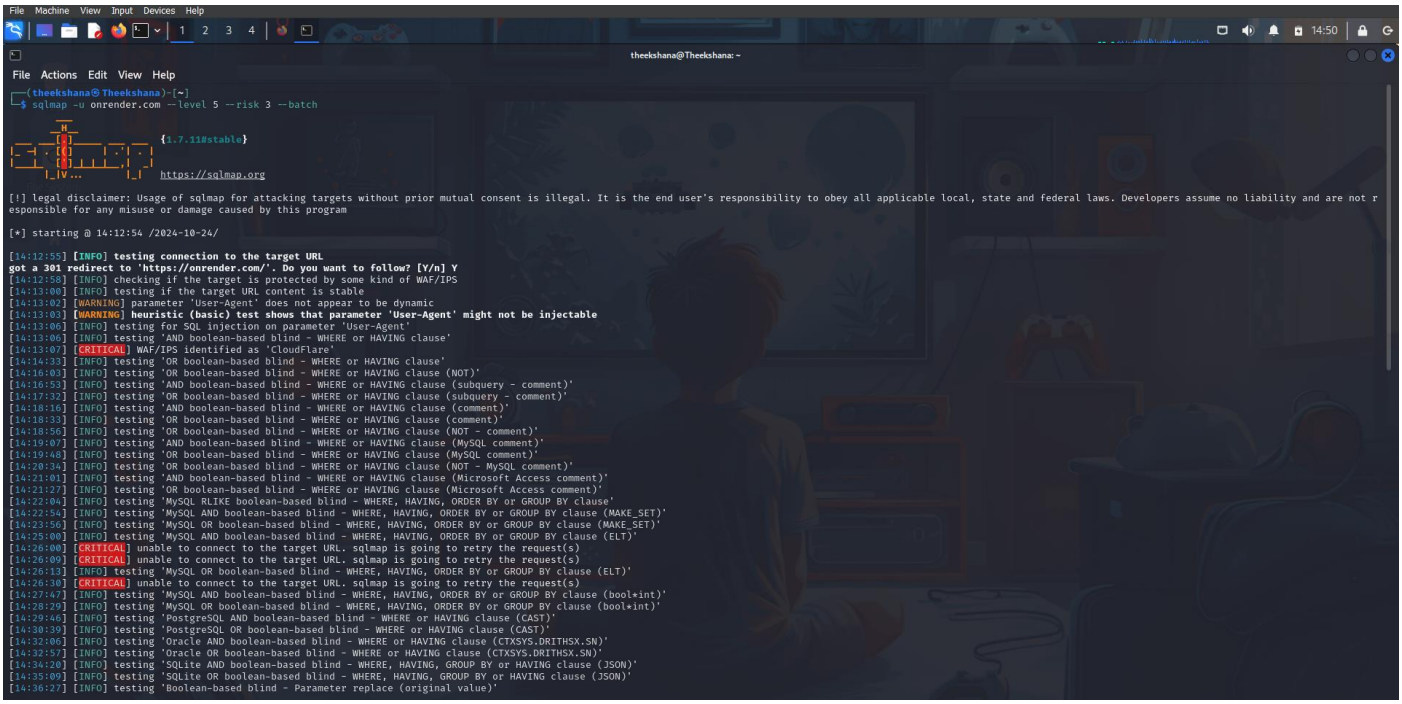
Target Port: 80 – The scan is targeting port 80, which is typically used for HTTP traffic

Security Headers:

- **X-Frame-Options header not present**: This header is used to protect against clickjacking attacks, but it is not set, which could make the site vulnerable.
- **X-Content-Type-Options header not set**: This header prevents browsers from interpreting files as a different MIME type (which can help prevent certain attacks). Its absence could pose a risk.

SQLmap Scaner

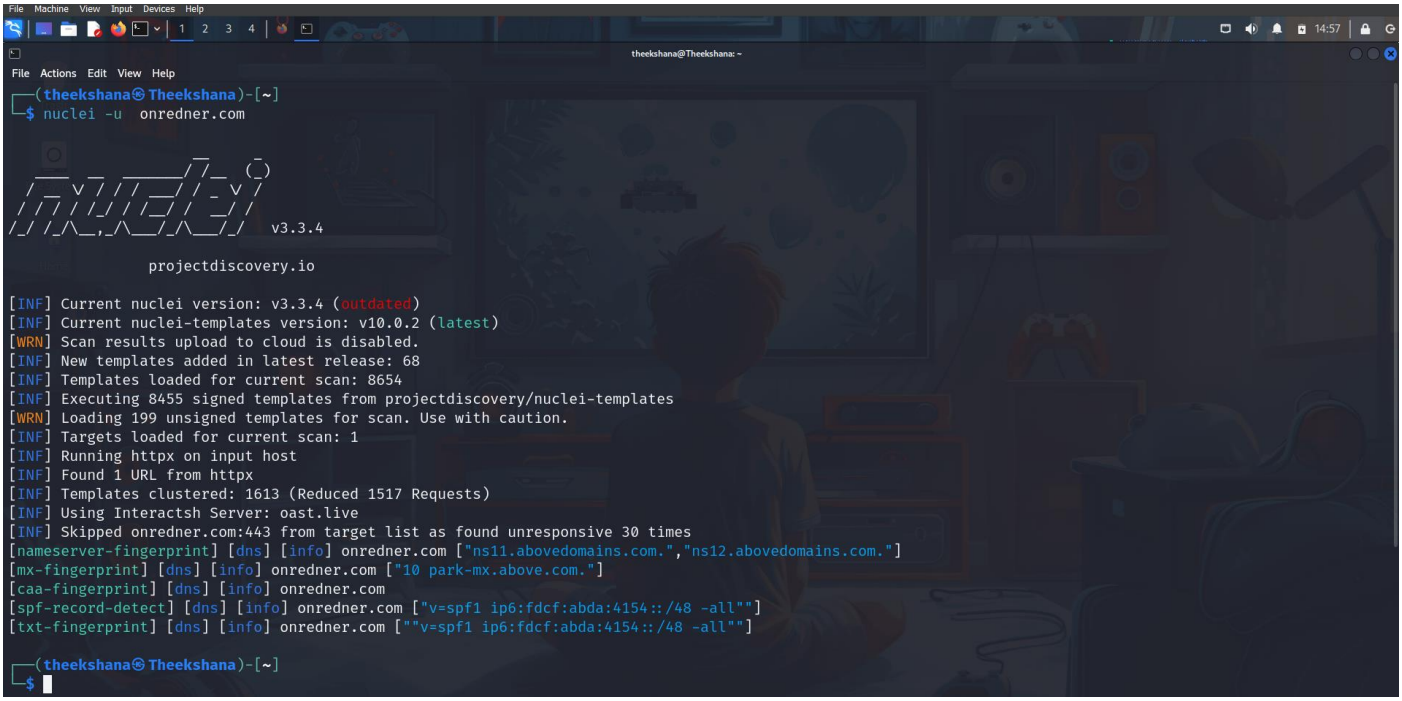




Techniques Tested:

- The tool tried several SQL injection techniques, including:
  - **Boolean-based blind SQL injection**: It tests queries that rely on conditions to confirm if injection is possible.
  - **AND/OR blind**: Uses AND and OR clauses to manipulate SQL statements and determine vulnerability.
  - **HAVING, ORDER BY, GROUP BY clauses**: These are SQL statements used to filter and sort query results, and they were tested for potential injection points.

Nuclei Scan



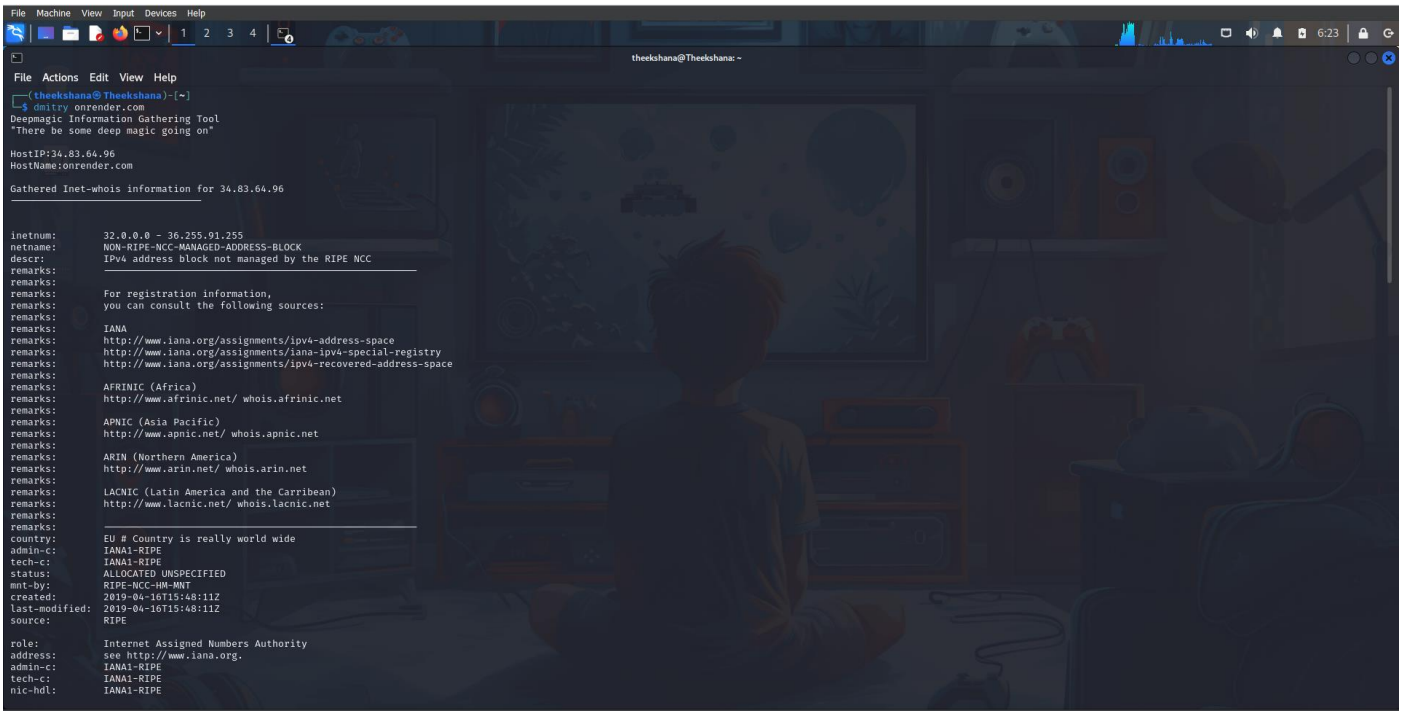
Scan Status:

- **Targets Loaded**: 1 target (onredner.com) is being scanned.
- **Running httx on input host**: The scan is running a tool that processes the target URL(s).
- **Found 1 URL from httx**: It found a URL to check on the target (onredner.com).
- **Templates Clustered**: The templates are reduced (from 1613 to 1517) to optimize the scan and remove redundancy.

DNS Information: The scan is reporting DNS-related information about the target domain:

- **Nameserver Fingerprint**: The nameservers for onredner.com are ns11.abovedomains.com and ns12.abovedomains.com.
- **MX Fingerprint**: The mail exchange (MX) record for onredner.com is 10 park-mx.above.com, which means that the domain is configured to handle emails through this server.
- **SPF Record Detect**: The domain has an SPF record configured for IP fdcf:abda:4154::/48, which helps in preventing email spoofing.
- **CAA Record**: The domain has a CAA record, which specifies which certificate authorities are allowed to issue SSL/TLS certificates for the domain.

Dmitry Scan



Port 21 (FTP - File Transfer Protocol): This port is typically used for file transfer services. Having FTP open can be risky if not properly secured, as it often transmits data in plain text (though secure variants like SFTP exist).

Port 53 (DNS - Domain Name System): This port is used for DNS services, which translate domain names into IP addresses. While DNS services need to be accessible, misconfigurations or vulnerabilities (like DNS amplification attacks) can expose the server to risks.

Port 80 (HTTP - Hypertext Transfer Protocol): This port is used for unencrypted web traffic. Port 80 being open suggests that the website is accessible via HTTP, but this should be redirected to HTTPS (Port 443) for encrypted communication. If not, it leaves the site vulnerable to man-in-the middle (MITM) attacks.

Netsparker

netsparker — Detailed Scan Report

http://render.com/

Scan Time : 10/24/2024 4:18:32 PM (UTC+05:30)

Total Requests: 1,401
Average Speed: 14.1r/s

Risk Level: LOW

VULNERABILITIES

9	3	0	0	0	1	3	5
IDENTIFIED	CONFIRMED	CRITICAL	HIGH	MEDIUM	LOW	BEST PRACTICE	INFORMATION

Identified Vulnerabilities

Critical	0
High	0
Medium	0
Low	1
Best Practice	3
Information	5
TOTAL	**9**

Confirmed Vulnerabilities

Critical	0
High	0
Medium	0
Low	1
Best Practice	0
Information	2
TOTAL	**3**

Vulnerability Summary

SEVERITY FILTER : ☑ CRITICAL ☑ HIGH ☑ MEDIUM ☑ LOW ☑ BEST PRACTICE ☑ INFORMATION

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Insecure Frame (External)	GET	https://render.com/	
	Content Security Policy (CSP) Not Implemented	GET	https://render.com/.well-known/	
	Expect-CT Not Enabled	GET	https://render.com/pan/script.js	
	Missing X-XSS-Protection Header	GET	https://render.com/pan/script.js	
	Email Address Disclosure	GET	https://render.com/?hTTp://r87.com/n	
	Generic Email Address Disclosure	GET	https://render.com/?hTTp://r87.com/n	
	Security.txt Detected	GET	https://render.com/.well-known/security.txt	
	Forbidden Resource	POST	http://render.com/	
	Robots.txt Detected	GET	https://render.com/robots.txt	

Content Security Policy (CSP) Not Implemented

BEST PRACTICE 1

CSP is an added layer of security that helps to mitigate mainly Cross-site Scripting attacks.

CSP can be enabled instructing the browser with a Content-Security-Policy directive in a response header;

```
Content-Security-Policy: script-src 'self';
```

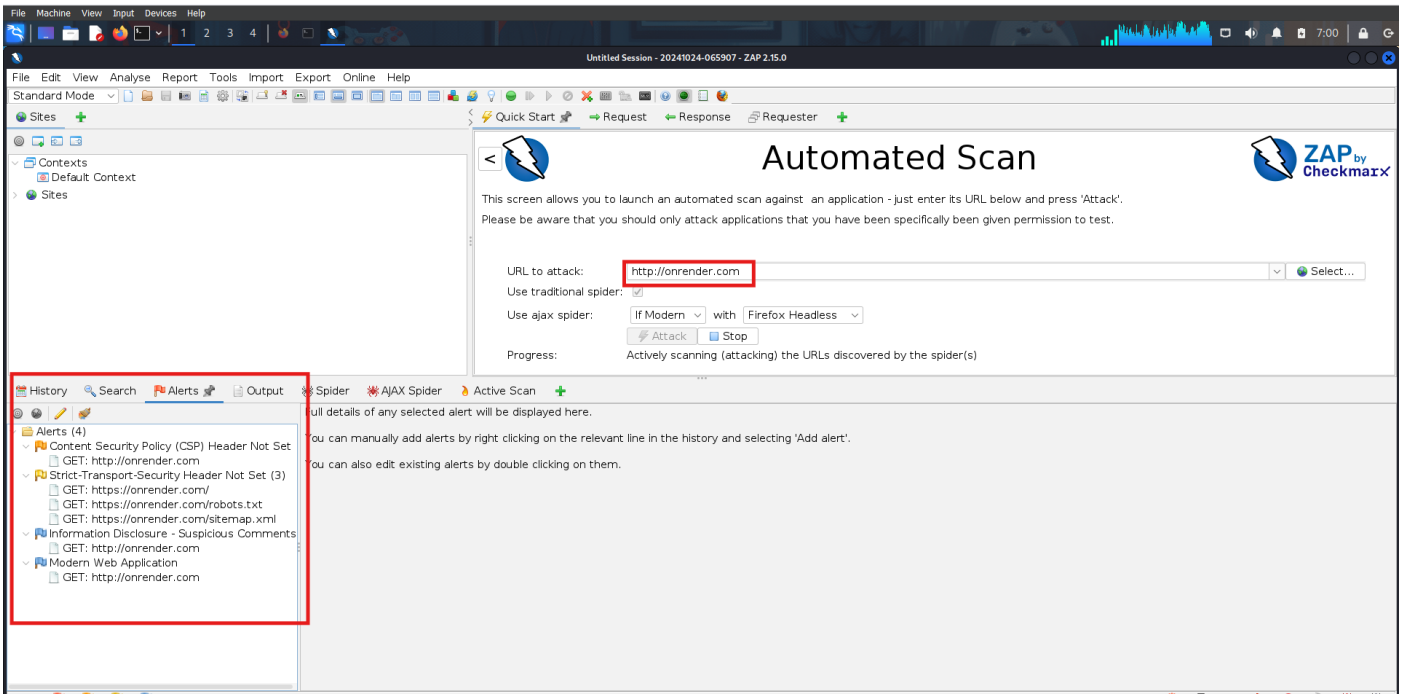
or in a meta tag;

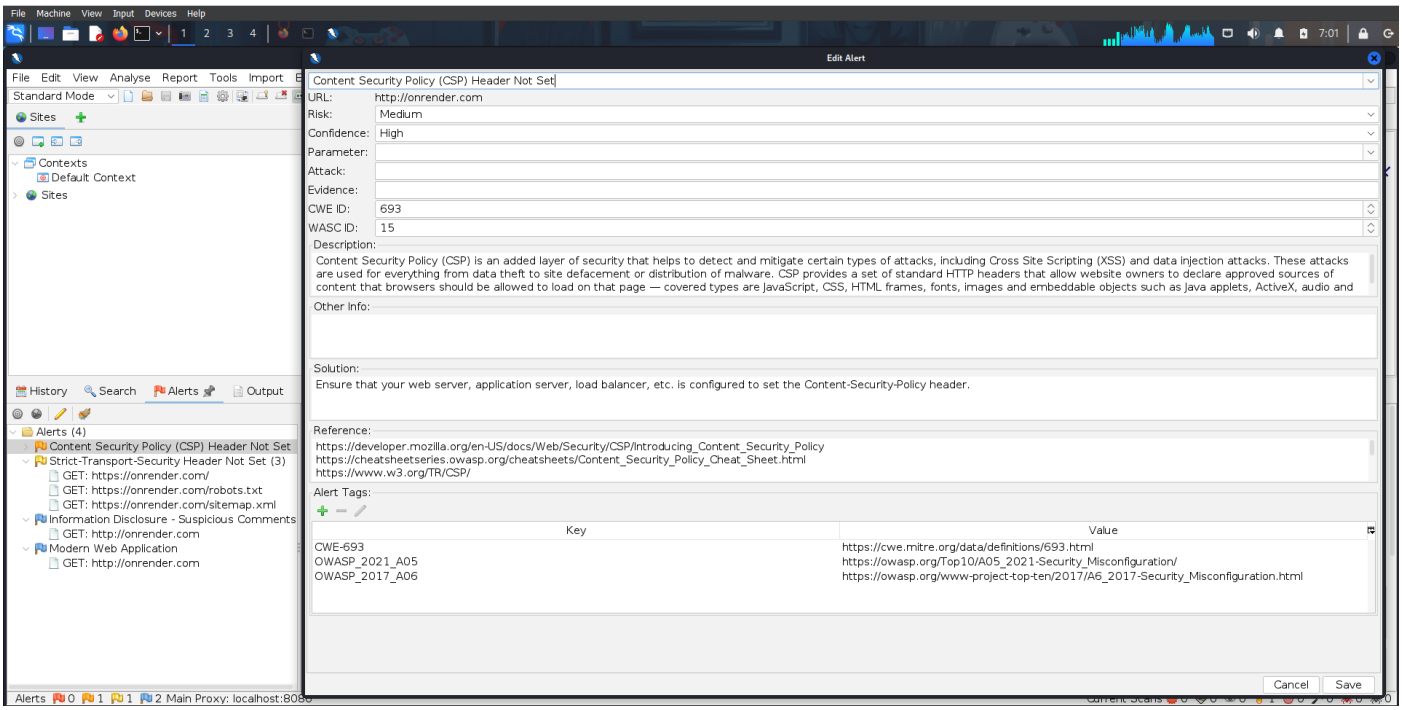
```
<meta http-equiv="Content-Security-Policy" content="script-src 'self';">
```

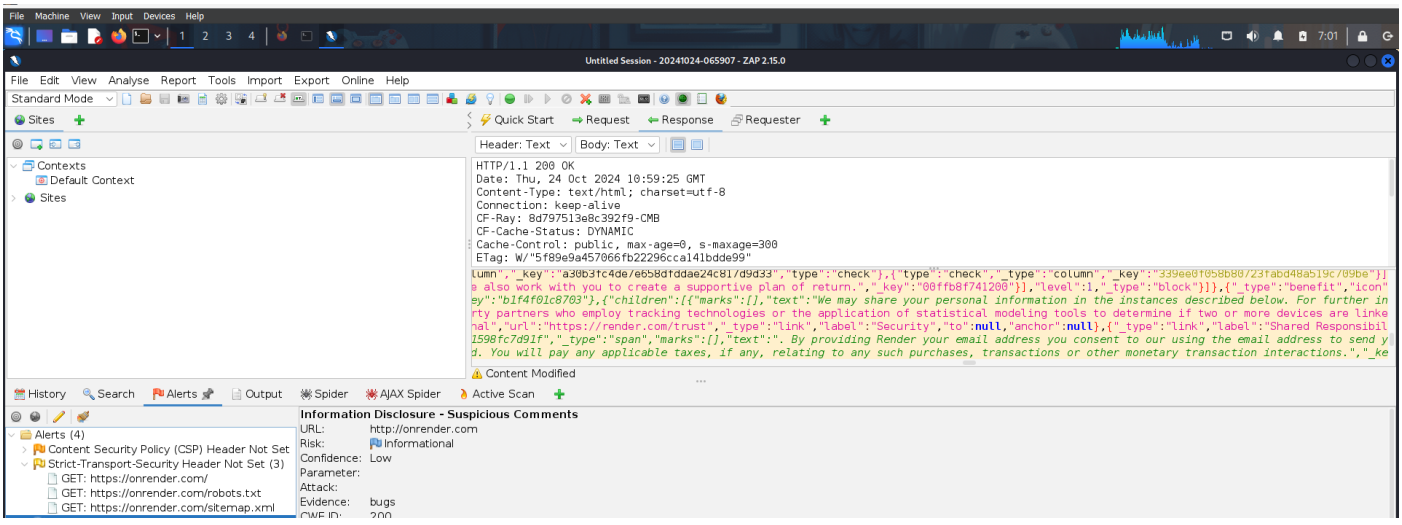
In the above example, you can restrict script loading only to the same domain. It will also restrict inline script executions both in the element attributes and the event handlers. There are various directives which you can use by declaring CSP:

- **script-src:**Restricts the script loading resources to the ones you declared. By default, it disables inline script executions unless you permit to the evaluation functions and inline scripts by the unsafe-ev and unsafe-inline keywords.
- **base-uri:**Base element is used to resolve relative URL to absolute one. By using this CSP directive, you can define all possible URLs which could be assigned to base-href attribute of the document.
- **frame-ancestors**: It is very similar to X-Frame-Options HTTP header. It defines the URLs by which the page can be loaded in an iframe.
- **frame-src / child-src**: frame-src is the deprecated version of child-src. Both define the sources that can be loaded by iframe in the page. (Please note that frame-src was brought back in CSP 3)
- **object-src**: Defines the resources that can be loaded by embedding such as Flash files, Java Applets.
- **img-src**: As its name implies, it defines the resources where the images can be loaded from.
- **connect-src**: Defines the whitelisted targets for XMLHttpRequest and WebSocket objects.
- **default-src**: It is a fallback for the directives that mostly ends with -src suffix. When the directives below are not defined, the value set to default-src will be used instead:
  - child-src
  - connect-src
  - font-src
  - img-src
  - manifest-src
  - media-src
  - object-src
  - script-src
  - style-src

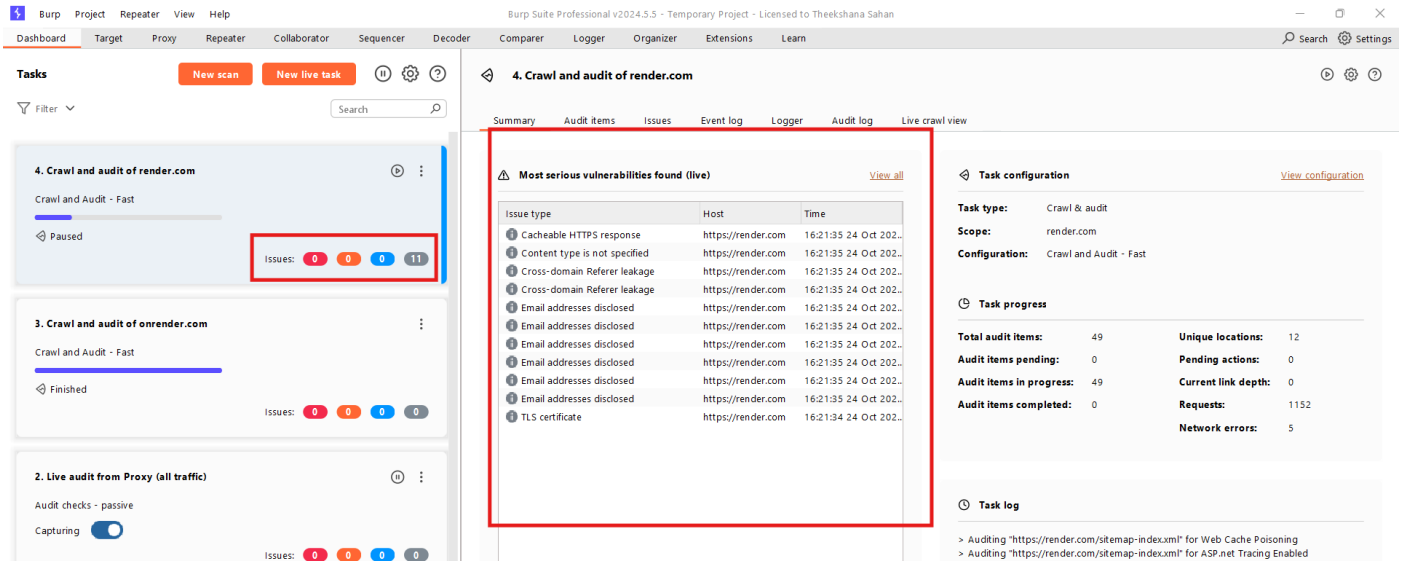
OWASP ZAP

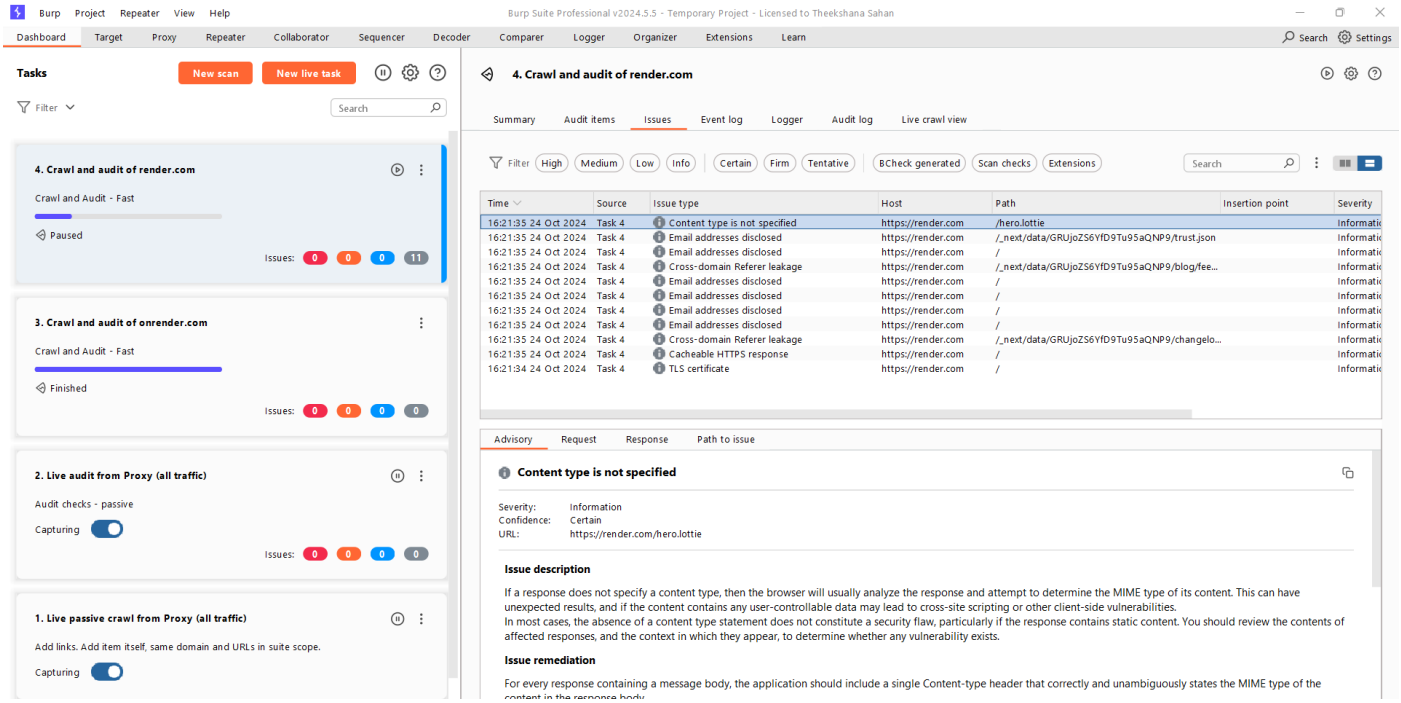

Untitled Session - 20241024-065907 - ZAP 2.15.0
Automated Scan
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack: http://onrender.com
Use traditional spider:
Use ajax spider: If Modern with Firefox Headless
Attack
Stop
Progress: Actively scanning (attacking) the URLs discovered by the spider(s)
Alerts (4)
Content Security Policy (CSP) Header Not Set
GET: http://onrender.com
Strict-Transport-Security Header Not Set (3)
GET: https://onrender.com/
GET: https://onrender.com/robots.txt
GET: https://onrender.com/sitemap.xml
Information Disclosure - Suspicious Comments
GET: http://onrender.com
Modern Web Application
GET: http://onrender.com

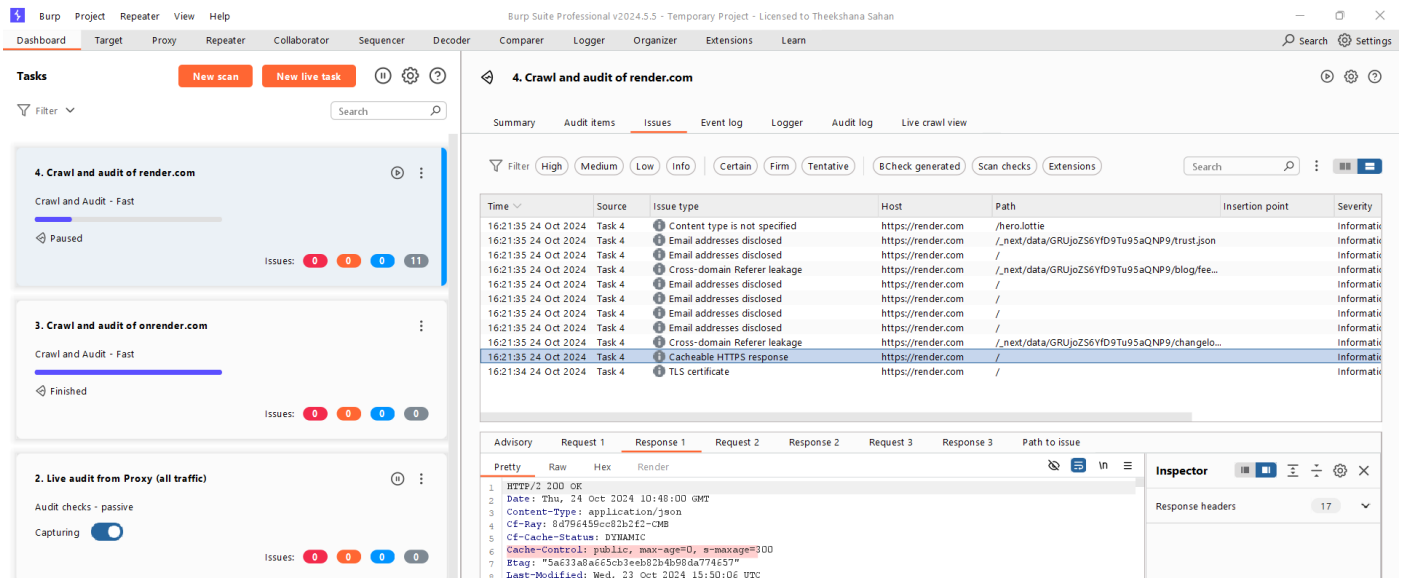

Edit Alert
Content Security Policy (CSP) Header Not Set
URL: http://onrender.com
Risk: Medium
Confidence: High
Parameter:
Attack:
Evidence:
CWE ID: 693
WASC ID: 15
Description:
Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including 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
Other Info:
Solution:
Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference:
https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
Alert Tags:
Key
Value
CWE-693
https://cwe.mitre.org/data/definitions/693.html
OWASP_2021_A05
https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
OWASP_2017_A06
https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html
Cancel
Save


Untitled Session - 20241024-065907 - ZAP 2.15.0
Content Modified
Information Disclosure - Suspicious Comments
URL: http://onrender.com
Risk: Informational
Confidence: Low
Parameter:
Attack:
Evidence: bugs

Burp Suite


Burp Project Repeater View Help
Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan
Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Tasks
New scan
New live task
Filter
Search
4. Crawl and audit of render.com
Crawl and Audit - Fast
Paused
Issues: 0 0 0 11
3. Crawl and audit of onrender.com
Crawl and Audit - Fast
Finished
Issues: 0 0 0 0
2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing
Issues: 0 0 0 0
4. Crawl and audit of render.com
Summary Audit items Issues Event log Logger Audit log Live crawl view
Most serious vulnerabilities found (live)
View all
Issue type Host Time
Cacheable HTTPS response https://render.com 16:21:35 24 Oct 202...
Content type is not specified https://render.com 16:21:35 24 Oct 202...
Cross-domain Referer leakage https://render.com 16:21:35 24 Oct 202...
Cross-domain Referer leakage https://render.com 16:21:35 24 Oct 202...
Email addresses disclosed https://render.com 16:21:35 24 Oct 202...
Email addresses disclosed https://render.com 16:21:35 24 Oct 202...
Email addresses disclosed https://render.com 16:21:35 24 Oct 202...
Email addresses disclosed https://render.com 16:21:35 24 Oct 202...
Email addresses disclosed https://render.com 16:21:35 24 Oct 202...
Email addresses disclosed https://render.com 16:21:35 24 Oct 202...
TLS certificate https://render.com 16:21:34 24 Oct 202...
Task configuration
View configuration
Task type: Crawl & audit
Scope: render.com
Configuration: Crawl and Audit - Fast
Task progress
Total audit items: 49
Audit items pending: 0
Audit items in progress: 49
Audit items completed: 0
Unique locations: 12
Pending actions: 0
Current link depth: 0
Requests: 1152
Network errors: 5
Task log
> Auditing "https://render.com/sitemap-index.xml" for Web Cache Poisoning
> Auditing "https://render.com/sitemap-index.xml" for ASP.net Tracing Enabled


Burp Project Repeater View Help
Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan
Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Tasks
New scan
New live task
Filter
Search
4. Crawl and audit of render.com
Crawl and Audit - Fast
Paused
Issues: 0 0 0 11
3. Crawl and audit of onrender.com
Crawl and Audit - Fast
Finished
Issues: 0 0 0 0
2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing
Issues: 0 0 0 0
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing
4. Crawl and audit of render.com
Summary Audit items Issues Event log Logger Audit log Live crawl view
Filter High Medium Low Info Certain Firm Tentative BCheck generated Scan checks Extensions
Search
Time Source Issue type Host Path Insertion point Severity
16:21:35 24 Oct 2024 Task 4 Content type is not specified https://render.com /hero.lottie Informatic
16:21:35 24 Oct 2024 Task 4 Email addresses disclosed https://render.com /_next/data/GRUjoZS6YfD9Tu95aQNP9/trust.json Informatic
16:21:35 24 Oct 2024 Task 4 Email addresses disclosed https://render.com / Informatic
16:21:35 24 Oct 2024 Task 4 Cross-domain Referer leakage https://render.com /_next/data/GRUjoZS6YfD9Tu95aQNP9/blog/fee... Informatic
16:21:35 24 Oct 2024 Task 4 Email addresses disclosed https://render.com / Informatic
16:21:35 24 Oct 2024 Task 4 Email addresses disclosed https://render.com / Informatic
16:21:35 24 Oct 2024 Task 4 Email addresses disclosed https://render.com / Informatic
16:21:35 24 Oct 2024 Task 4 Email addresses disclosed https://render.com / Informatic
16:21:35 24 Oct 2024 Task 4 Cross-domain Referer leakage https://render.com /_next/data/GRUjoZS6YfD9Tu95aQNP9/changelo... Informatic
16:21:35 24 Oct 2024 Task 4 Cacheable HTTPS response https://render.com / Informatic
16:21:34 24 Oct 2024 Task 4 TLS certificate https://render.com / Informatic
Advisory Request Response Path to issue
Content type is not specified
Severity: Information
Confidence: Certain
URL: https://render.com/hero.lottie
Issue description
If a response does not specify a content type, then the browser will usually analyze the response and attempt to determine the MIME type of its content. This can have unexpected results, and if the content contains any user-controllable data may lead to cross-site scripting or other client-side vulnerabilities.
In most cases, the absence of a content type statement does not constitute a security flaw, particularly if the response contains static content. You should review the contents of affected responses, and the context in which they appear, to determine whether any vulnerability exists.
Issue remediation
For every response containing a message body, the application should include a single Content-type header that correctly and unambiguously states the MIME type of the


Burp Project Repeater View Help
Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan
Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Tasks
New scan
New live task
Filter
Search
4. Crawl and audit of render.com
Crawl and Audit - Fast
Paused
Issues: 0 0 0 11
3. Crawl and audit of onrender.com
Crawl and Audit - Fast
Finished
Issues: 0 0 0 0
2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing
Issues: 0 0 0 0
4. Crawl and audit of render.com
Summary Audit items Issues Event log Logger Audit log Live crawl view
Filter High Medium Low Info Certain Firm Tentative BCheck generated Scan checks Extensions
Search
Time Source Issue type Host Path Insertion point Severity
16:21:35 24 Oct 2024 Task 4 Content type is not specified https://render.com /hero.lottie Informatic
16:21:35 24 Oct 2024 Task 4 Email addresses disclosed https://render.com /_next/data/GRUjoZS6YfD9Tu95aQNP9/trust.json Informatic
16:21:35 24 Oct 2024 Task 4 Email addresses disclosed https://render.com / Informatic
16:21:35 24 Oct 2024 Task 4 Cross-domain Referer leakage https://render.com /_next/data/GRUjoZS6YfD9Tu95aQNP9/blog/fee... Informatic
16:21:35 24 Oct 2024 Task 4 Email addresses disclosed https://render.com / Informatic
16:21:35 24 Oct 2024 Task 4 Email addresses disclosed https://render.com / Informatic
16:21:35 24 Oct 2024 Task 4 Email addresses disclosed https://render.com / Informatic
16:21:35 24 Oct 2024 Task 4 Email addresses disclosed https://render.com / Informatic
16:21:35 24 Oct 2024 Task 4 Cross-domain Referer leakage https://render.com /_next/data/GRUjoZS6YfD9Tu95aQNP9/changelo... Informatic
16:21:35 24 Oct 2024 Task 4 Cacheable HTTPS response https://render.com / Informatic
16:21:34 24 Oct 2024 Task 4 TLS certificate https://render.com / Informatic
Advisory Request 1 Response 1 Request 2 Response 2 Request 3 Response 3 Path to issue
Pretty Raw Hex Render
Inspector
Response headers 17
HTTP/2 200 OK
Date: Thu, 24 Oct 2024 10:48:00 GMT
Content-Type: application/json
Cf-Ray: 8d796459cc82b2f2-CMB
Cf-Cache-Status: DYNAMIC
Cache-Control: public, max-age=0, s-maxage=300
Etag: "5a633a8a665cb3eeb82b4b98da774e57"
Last-Modified: Wed, 23 Oct 2024 15:50:06 UTC

Vulnerabilities:

1 Absence of Anti-CSRF Tokens

Vulnerability Title	Absence of Anti-CSRF Tokens
Vulnerability Description	Cross-Site Request Forgery (CSRF) is a type of attack where an attacker tricks a user into unknowingly submitting a malicious request to a different website where the user is authenticated. The attacker exploits the fact that web browsers automatically include session cookies for authenticated users when making requests.
Affected Components	Forms Submitting Sensitive Data - Any form on the site that performs a state-changing action. Session Management - When CSRF tokens are absent, attackers can exploit the authenticated user's session to perform actions without their consent, leveraging session cookies.
Impact Assessment	**User Impact**: Attackers can perform unintended actions on behalf of users, such as transferring funds, changing account details, or altering permissions. **Security Risk**: This can lead to unauthorized transactions, theft of funds, data breaches, and loss of control over user accounts. CSRF can also be exploited to escalate privileges or gain access to sensitive resources.
Steps to Reproduce	**Step 1**: Log in to a web application where CSRF protection is absent. **Step 2**: Open the developer tools to observe the session cookies for authenticated requests. **Step 3**: Craft an HTML form or a malicious website that submits a state-changing to the target web application without user interaction. **Step 4**: Have the victim visit the malicious site. The forged request will be automatically submitted using the victim’s session.
Proof of Concept	(CSRF) attack can be demonstrated by exploiting the absence of anti-CSRF tokens. Here’s a simple proof of concept (PoC) that shows how an attacker can craft a malicious HTML form that sends an unwanted request on behalf of an authenticated user.
Proposed Mitigation or Fix	**Implement CSRF Tokens**: Ensure that all state-changing forms include a unique CSRF token that is validated on the server side. **SameSite Cookies**: Set cookies with the SameSite attribute to Strict or Lax to prevent cookies from being sent with cross-origin requests.

2 Strict Transport Security Policy Not Enabled

Vulnerability Title	**Strict Transport Security (HSTS) Policy Not Enabled**
Vulnerability Description	HSTS is a security feature that forces web browsers to communicate with servers only via secure HTTPS connections. The lack of HSTS increases the risk of Man-in-the-Middle (MITM) attacks, as users could be tricked into accessing the site over an insecure HTTP connection.
Affected Components	Web server configuration, specifically the response headers for **go.transunion.com** Any external site linked from a vulnerable website can receive the referrer URL, which may include sensitive or confidential information.
Impact Assessment	Without HSTS, users may accidentally connect over HTTP, exposing sensitive data to interception. Attackers could exploit this to steal session cookies, login credentials, or other confidential information through downgrading attacks.
Steps to Reproduce	1.Open a browser and attempt to connect to **http://go.transunion.com** (without HTTPS). 2. Observe that the connection is not automatically upgraded to HTTPS. 3. Inspect the HTTP response headers and note the absence of the **Strict-Transport-Security** header.
Proof of Concept	**http://go.transunion.com** in an unsecured network. Use network analysis tools (e.g., Wireshark) to observe traffic and confirm it's unencrypted.
Proposed Mitigation or Fix	Enable the HSTS policy on the server by adding the **Strict-Transport-Security** header. This header enforces HTTPS, prevents downgrade attacks, and sets a max age to enforce the policy. Ensure the site supports HTTPS properly before enabling this policy.