

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

Table of Contents

Acknowledgement	3
Introduction.....	4
Report 01 Target Details	5
Target Reconnaissance.....	6
Vulnerabilities:.....	15
Report 02 Target Details	17
Target Reconnaissance.....	18
Vulnerabilities:.....	26
Report 03 Target Details	28
Target Reconnaissance.....	29
Vulnerabilities:.....	38
Report 04 Target Details	40
Target Reconnaissance.....	41
Vulnerabilities:.....	49
Report 05 Target Details	50
Target Reconnaissance.....	51
Vulnerabilities:.....	59
Report 06 Target Details	60
Target Reconnaissance.....	61
Vulnerabilities:.....	69
Report 07 Target Details	70
Target Reconnaissance.....	71
Vulnerabilities:.....	79
Report 08 Target Details	80
Target Reconnaissance.....	81
Vulnerabilities:.....	89
Report 09 Target Details	90
Target Reconnaissance.....	91
Vulnerabilities:.....	99
Report 10 Target Details	100
Target Reconnaissance.....	101
Vulnerabilities:.....	109

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 screenshot shows a Bug Bounty report interface. On the left is a sidebar with various icons and a list of links: Security page, Program guidelines (selected), Scope, Hacktivity, Thanks, Updates, Safe harbor, Help, and Notifications. The main content area has several sections: 'Program highlights' with icons for Closed Scope, Gold Standard, Platform Standards, and Top Response Efficiency; performance metrics for Average time to first response (7 hours), Average time to triage (2 days, 5 hours), Average time to bounty (N/A), and Average time to resolution (1 month, 3 weeks); 'Scope exclusions' noting Core Ineligible Findings; and an 'Overview' section last updated on July 15, 2024. On the right, there's a TransUnion logo, company details (http://transunion.com, @transunion), a brief description of their vulnerability disclosure program, and a 'Submit report' button. Below that is a 'Stats' section with metrics like Reports received (90 days: 44), Last report resolved (5 days ago), Reports resolved (43), Hackers thanked (45), and Assets in scope (726).

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.

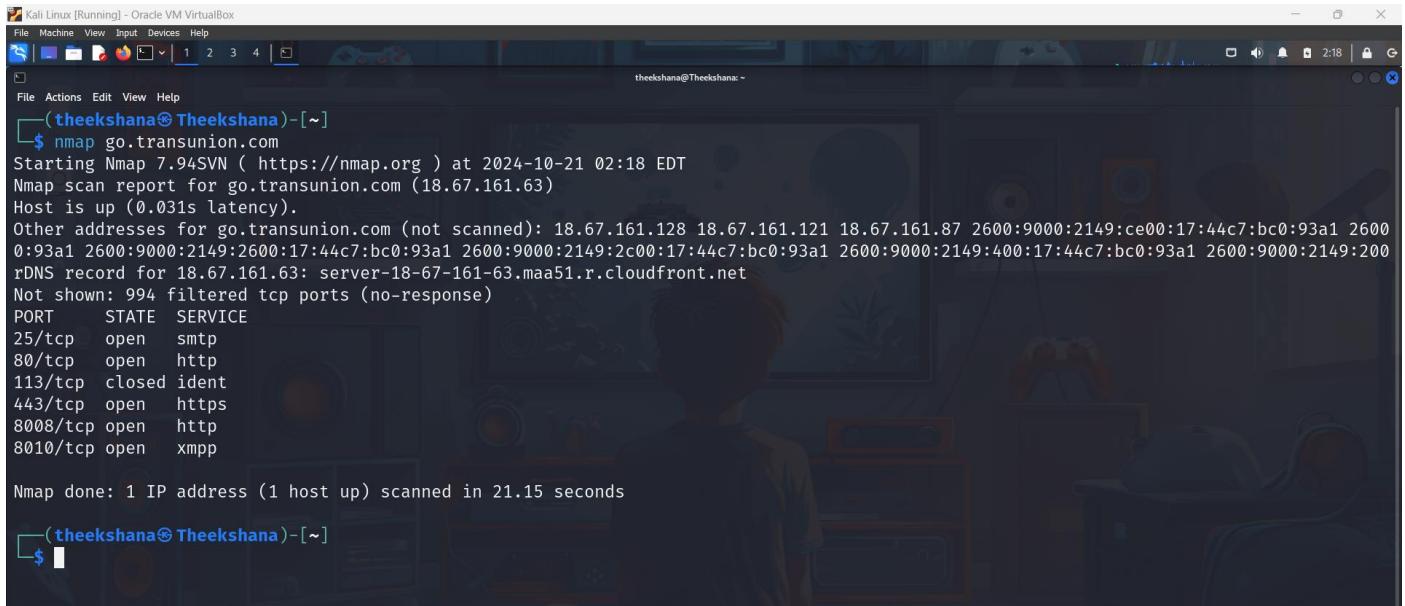
In this report, I have chosen to focus on 10 subdomains under the main domain transunion.com. Each subdomain may offer distinct functionalities or services, which can potentially introduce different security risks. The subdomains were selected based on their relevance and the likelihood of containing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

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

The screenshot shows the initial step of a sign-up process for TransUnion Credit Monitoring. It features a progress bar labeled 'STEP 1/6'. The main form asks for First Name, Last Name, and Email. To the right, there's a promotional section for Credit Monitoring, showing a magnifying glass icon over a credit score of 720. It explains that TransUnion® Credit Report & Score are available as part of a subscription service, costing \$29.95 per month. A 'View Benefits' dropdown is shown. Below it is a 'What You Need to Know' box stating that credit scores are based on the VantageScore® 3.0 model and vary by lender.

Target Reconnaissance

Nmap Scan



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
theekshana@Theekshana: ~
(theekshana@Theekshana)-[~]
$ nmap go.transunion.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-21 02:18 EDT
Nmap scan report for go.transunion.com (18.67.161.63)
Host is up (0.031s latency).
Other addresses for go.transunion.com (not scanned): 18.67.161.128 18.67.161.121 18.67.161.87 2600:9000:2149:ce00:17:44c7:bc0:93a1 2600:9000:2149:2600:17:44c7:bc0:93a1 2600:9000:2149:2c00:17:44c7:bc0:93a1 2600:9000:2149:400:17:44c7:bc0:93a1 2600:9000:2149:200:rDNS record for 18.67.161.63: server-18-67-161-63.maa51.r.cloudfront.net
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
113/tcp   closed ident
443/tcp   open  https
8080/tcp  open  http
8010/tcp  open  xmpp

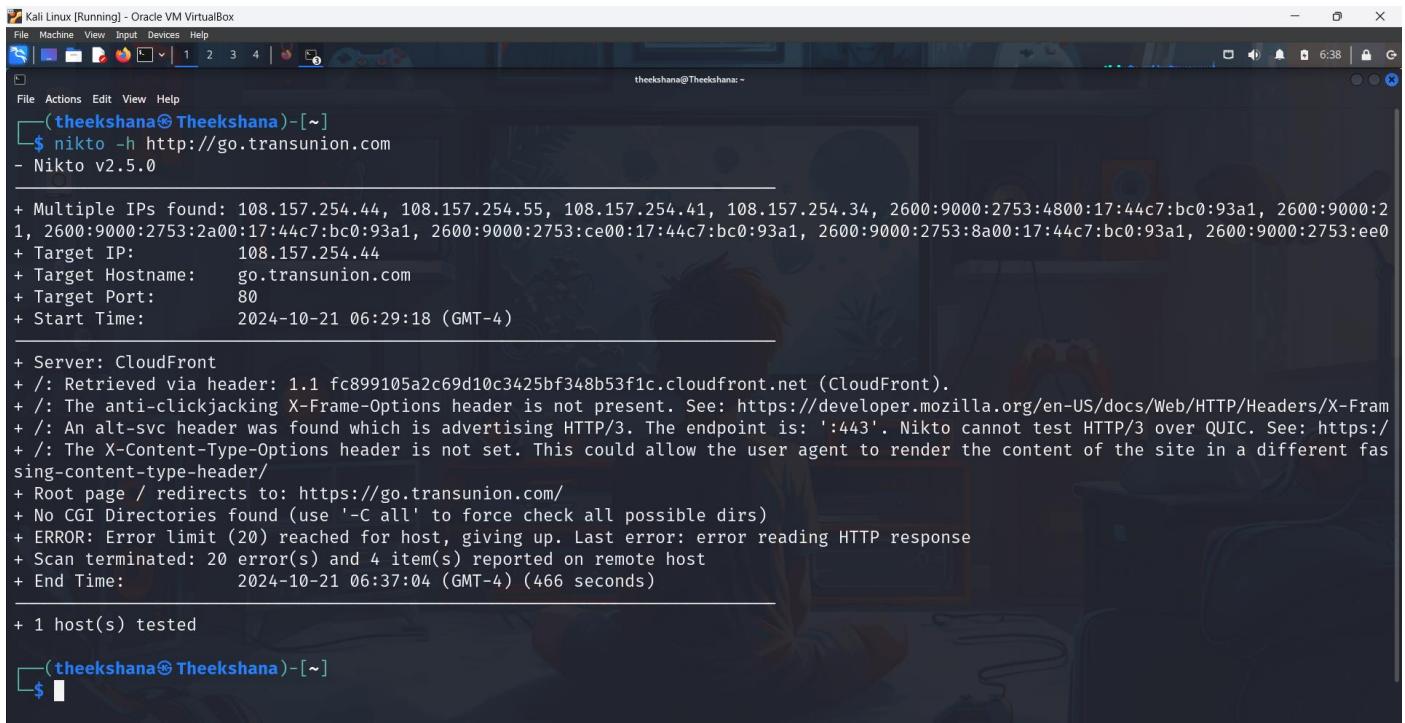
Nmap done: 1 IP address (1 host up) scanned in 21.15 seconds
(theekshana@Theekshana)-[~]
$
```

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



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
(theekshana@Theekshana)-[~]
$ nikto -h http://go.transunion.com
- Nikto v2.5.0

+ Multiple IPs found: 108.157.254.44, 108.157.254.55, 108.157.254.41, 108.157.254.34, 2600:9000:2753:4800:17:44c7:bc0:93a1, 2600:9000:2
1, 2600:9000:2753:2a00:17:44c7:bc0:93a1, 2600:9000:2753:ce00:17:44c7:bc0:93a1, 2600:9000:2753:8a00:17:44c7:bc0:93a1, 2600:9000:2753:ee0
+ Target IP:          108.157.254.44
+ Target Hostname:   go.transunion.com
+ Target Port:       80
+ Start Time:        2024-10-21 06:29:18 (GMT-4)

+ Server: CloudFront
+ /: Retrieved via header: 1.1 fc899105a2c69d10c3425bf348b53f1c.cloudfront.net (CloudFront).
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Fram
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 over QUIC. See: https:/
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fas
sing-content-type-header/
+ Root page / redirects to: https://go.transunion.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 4 item(s) reported on remote host
+ End Time:          2024-10-21 06:37:04 (GMT-4) (466 seconds)

+ 1 host(s) tested

(theekshana@Theekshana)-[~]
$
```

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 Scanner

```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
theekshana@Theekshana: ~
$ sqlmap -h

{1.7.11#stable}
https://sqlmap.org

Usage: python3 sqlmap [options]

Options:
-h, --help Show basic help message and exit
-hh Show advanced help message and exit
--version Show program's version number and exit
-v VERBOSE Verbosity level: 0-6 (default 1)

Target:
At least one of these options has to be provided to define the target(s)

-u URL, --url=URL Target URL (e.g. "http://www.site.com/vuln.php?id=1")
-g GOOGLEDORK Process Google dork results as target URLs

Request:
These options can be used to specify how to connect to the target URL

--data=DATA Data string to be sent through POST (e.g. "id=1")
--cookie=COOKIE HTTP Cookie header value (e.g. "PHPSESSID=a8d127e..")
--random-agent Use randomly selected HTTP User-Agent header value
--proxy=PROXY Use a proxy to connect to the target URL
--tor Use Tor anonymity network
--check-tor Check to see if Tor is used properly

Injection:
These options can be used to specify which parameters to test for,
provide custom injection payloads and optional tampering scripts
```

```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
theekshana@Theekshana: ~
$ sqlmap -u go.transunion.com --level 5 --risk 3 --batch

{1.7.11#stable}
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable laws. There are consequences to breaking and entering into most systems. The software is supplied as-is with no warranty of any kind. The user will defend Kali Linux Ltd. for any damages or damage caused by their actions.
[*] starting @ 07:04:19 /2024-10-21

[07:04:19] [INFO] testing connection to the target URL
got a 301 redirect to 'https://go.transunion.com/'. Do you want to follow? [y/n] y
[07:04:22] [INFO] testing if the target URL content is stable
[07:04:23] [WARNING] parameter 'User-Agent' does not appear to be dynamic
[07:04:24] [WARNING] heuristic (basic) test shows that parameter 'User-Agent' might not be injectable
[07:04:25] [INFO] testing for SQL injection on parameter 'User-Agent'
[07:04:25] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[07:05:11] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[07:06:21] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT)'
[07:07:03] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[07:07:34] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[07:08:17] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'
[07:08:25] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (comment)'
[07:08:40] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - comment)'
[07:08:49] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[07:09:08] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[07:09:41] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
[07:10:00] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'
[07:10:19] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'
```

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

```
[Kali Linux [Running] - Oracle VM VirtualBox]
File Machine View Input Devices Help
File Actions Edit View Help
$ nuclei -u go.transunion.com
projectdiscovery.io
v3.3.4
[INF] Current nuclei version: v3.3.4 (outdated)
[INF] Current nuclei-templates version: v10.0.2 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 68
[INF] Templates loaded for current scan: 8654
[INF] Executing 8455 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 199 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Running httpx on input host
[INF] Found 1 URL from httpx
[INF] Templates clustered: 1613 (Reduced 1517 Requests)
[INF] Using Interactsh Server: oast.site
[tls-version] [ssl] [info] go.transunion.com:443 ["tls12"]
[tls-version] [ssl] [info] go.transunion.com:443 ["tls13"]
[http-missing-security-headers:clear-site-data] [http] [info] https://go.transunion.com
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] https://go.transunion.com
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] https://go.transunion.com
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] https://go.transunion.com
[http-missing-security-headers:permissions-policy] [http] [info] https://go.transunion.com
[http-missing-security-headers:x-frame-options] [http] [info] https://go.transunion.com
[http-missing-security-headers:x-content-type-options] [http] [info] https://go.transunion.com
[http-missing-security-headers:referrer-policy] [http] [info] https://go.transunion.com
[http-missing-security-headers:strict-transport-security] [http] [info] https://go.transunion.com
[http-missing-security-headers:content-security-policy] [http] [info] https://go.transunion.com
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] https://go.transunion.com
[dns-saas-service-detection:amazon-cloudfront] [dns] [info] go.transunion.com ["dns-1096.awsdns-99.org.", "ns-1964.awsdns-53.co.uk.", "ns-241.awsdns-30.com.", "ns-672.awsdns-20.net."]
[nameserver-fingerprint] [dns] [info] go.transunion.com ["dig@njuw34kkv.cloudflare.net"]
[ssl-issue] [ssl] [info] go.transunion.com:443 [ Fortinet ]
[mismatched-ssl-certificate] [ssl] [low] go.transunion.com:443 [ "CN: Fortiguard SDNS Blocked Page" ]
[self-signed-ssl] [ssl] [low] go.transunion.com:443
[caa-fingerprint] [dns] [info] go.transunion.com

(theekshana@Theekshana)-~]
```

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

```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
theekshana@Theekshana: ~
$ dmtrly go.transunion.com
Deepmagic Information Gathering Tool
"Here be some deep magic going on"

HostIP:108.157.254.34
HostName:go.transunion.com
Gathered Inet-whois information for 108.157.254.34

inetnum: 108.60.32.0 - 108.179.63.255
netname: NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr: IPv4 address block not managed by the RIPE NCC
remarks:
remarks: For registration information,
remarks: you can consult the following sources:
remarks:
remarks: IANA
remarks: http://www.iana.org/assignments/ipv4-address-space
remarks: http://www.iana.org/assignments/iana-ipv4-special-registry
remarks: http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks: AFRINIC (Africa)
remarks: http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks: APNIC (Asia Pacific)
remarks: http://www.apnic.net/ whois.apnic.net
remarks:
remarks: ARIN (Northern America)
remarks: http://www.arin.net/ whois.arin.net
remarks:
remarks: LACNIC (Latin America and the Caribbean)
remarks: http://www.lacnic.net/ whois.lacnic.net
remarks:
remarks: EU # Country is really world wide
admin-c: IANA1-RIPE
tech-c: IANA1-RIPE
status: ALLOCATED UNSPECIFIED
mnt-by: RIPE-NCC-HM-MNT
created: 2024-03-05T15:08:33Z
last-modified: 2024-03-05T15:08:33Z
source: RIPE

role: Internet Assigned Numbers Authority
address: see http://www.iana.org.
admin-c: IANA1-RIPE
tech-c: IANA1-RIPE
nic-hdl: IANA1-RIPE

remarks: EU # Country is really world wide
country: IANA1-RIPE
tech-c: IANA1-RIPE
status: ALLOCATED UNSPECIFIED
mnt-by: RIPE-NCC-HM-MNT
created: 2024-03-05T15:08:33Z
last-modified: 2024-03-05T15:08:33Z
source: RIPE

role: Internet Assigned Numbers Authority
address: see http://www.iana.org.
admin-c: IANA1-RIPE
tech-c: IANA1-RIPE
nic-hdl: IANA1-RIPE

remarks: For more information on IANA services
remarks: go to IANA web site at http://www.iana.org.
mnt-by: RIPE-NCC-MNT
created: 1970-01-01T00:00:00Z
last-modified: 2001-09-22T09:31:27Z
source: RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.114 (SHETLAND)

Gathered Inic-whois information for go.transunion.com
ERROR: Unable to locate Name Whois data on go.transunion.com
Gathered Netcraft information for go.transunion.com
Retrieving Netcraft.com information for go.transunion.com
zsh: segmentation fault dmtrly go.transunion.com
theekshana@Theekshana: ~
```

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

Detailed Scan Report

http://go.transunion.com/ [🔗](#)
 Scan Time : 10/21/2024 6:03:11 PM (UTC+05:30)

Total Requests: 10,479
 Average Speed: 24.6/s

Risk Level: **MEDIUM**

14	5	0 !	0 !
IDENTIFIED	CONFIRMED	CRITICAL	HIGH

1 MEDIUM	3 LOW
4 BEST PRACTICE	6 INFORMATION

Identified Vulnerabilities

SERIAL	VULNERABILITY	Critical	High	Medium	Low	Best Practice	Information	TOTAL
1	HTTP Strict Transport Security (HSTS) Policy Not Enabled	0	0	1	3	4	6	14

Confirmed Vulnerabilities

SERIAL	VULNERABILITY	Critical	High	Medium	Low	Best Practice	Information	TOTAL
1	Cookie Not Marked as HttpOnly	0	0	0	3	0	2	5

Vulnerability Summary

SEVERITY FILTER : <input checked="" type="checkbox"/> CRITICAL <input checked="" type="checkbox"/> HIGH <input checked="" type="checkbox"/> MEDIUM <input checked="" type="checkbox"/> LOW <input checked="" type="checkbox"/> BEST PRACTICE <input checked="" type="checkbox"/> INFORMATION						PARAMETER	»
CONFIRM	VULNERABILITY	METHOD	URL				»
1	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://go.transunion.com/				0
1	Cookie Not Marked as HttpOnly	GET	https://go.transunion.com/				0
1	Cookie Not Marked as Secure	GET	https://go.transunion.com/				1
1	Insecure Frame (External)	GET	https://go.transunion.com/				3
1	Expect-CT Not Enabled	GET	https://go.transunion.com/well-known/				4
1	Missing X-XSS-Protection Header	GET	https://go.transunion.com/_next/static/chunks/main-app-73c201cc0b2119e4.js				5
1	SameSite Cookie Not Implemented	GET	https://go.transunion.com/				
1	Subresource Integrity (SRI) Not Implemented	GET	https://go.transunion.com/.svn/wc.db				
1	[Possible] Internal Path Disclosure (*nix)	GET	https://go.transunion.com/etc/static/				
1	[Possible] Internal Path Disclosure (Windows)	GET	https://go.transunion.com/c/static/				
1	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. https://go.transunion.com/ [🔗](#)

Certainty



Request

Response

OWASP ZAP

The screenshot shows the OWASP ZAP interface with an 'Automated Scan' configuration window open. The URL to attack is set to <http://go.transunion.com>. The 'Attack' button is highlighted. Below the configuration, the 'Alerts' section is expanded, showing 15 alerts, including several CSP-related issues. A red box highlights this section.

URL to attack: <http://go.transunion.com>

Attack: If Modern with Firefox Headless

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 (1)
- Server Leaks Version Information via "Server" HTTP Response Header (1)
- 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)

Detailed view of a selected alert: CSP: script-src unsafe-eval (5). The alert details include:

- URL: <http://go.transunion.com>
- Risk: Medium
- Confidence: High
- Parameter: content-security-policy
- Attack: content-security-policy
- Evidence: m.com/dpm.demdex.net/api/company-target.com.t.teads.tv/transunion.tt.omrtdc.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>

The screenshot shows the OWASP ZAP interface with an 'Alerts' section expanded, showing 15 alerts, including several CSP-related issues. A large code snippet is visible in the center of the screen, likely a captured response or payload.

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 (1)
- Server Leaks Version Information via "Server" HTTP Response Header (1)
- Strict-Transport-Security Header Not Set (47)
- Timestamp Disclosure - Unix (33)
- X-Content-Type-Options Header Missing (46)
- Information Disclosure - Suspicious Comments (25)
- Modern Web Application (5)

Burp Suite

Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahaan

Tasks

- 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 4 0
- 1. Live passive crawl from Proxy (all traffic)**
 - Add links. Add item itself, same domain and URLs in suite scope.
 - Capturing
 - Issues: 0

3. Crawl and audit of go.transunion.com

Most serious vulnerabilities found (live)

Issue type	Host	Time
Strict transport security not enforced	https://go.transunion...	18:54:41 21 Oct 202...
Cacheable HTTPS response	https://go.transunion...	18:54:42 21 Oct 202...
Cacheable HTTPS response	https://go.transunion...	18:54:41 21 Oct 202...
Content security policy: allowedlist script	https://go.transunion...	18:54:42 21 Oct 202...
Content security policy: allows untrusted	https://go.transunion...	18:54:42 21 Oct 202...
Content security policy: allows untrusted	https://go.transunion...	18:54:42 21 Oct 202...
Cross-domain script include	https://go.transunion...	18:57:28 21 Oct 202...
Input returned in response (reflected)	https://go.transunion...	18:59:08 21 Oct 202...
Input returned in response (reflected)	https://go.transunion...	18:56:16 21 Oct 202...
Input returned in response (reflected)	https://go.transunion...	18:56:40 21 Oct 202...
Robot.txt file	https://go.transunion...	18:54:40 21 Oct 202...
TLS certificate	https://go.transunion...	18:55:14 21 Oct 202...
DOM data manipulation (DOM-based)	https://go.transunion...	18:55:14 21 Oct 202...
DOM data manipulation (DOM-based)	https://go.transunion...	18:55:15 21 Oct 202...
DOM data manipulation (DOM-based)	https://go.transunion...	18:55:14 21 Oct 202...
HTML5 storage manipulation (DOM-based)	https://go.transunion...	18:55:14 21 Oct 202...
HTML5 storage manipulation (DOM-based)	https://go.transunion...	18:55:14 21 Oct 202...
HTML5 storage manipulation (DOM-based)	https://go.transunion...	18:55:14 21 Oct 202...

Task configuration

Task progress

Task log

Audit cookie of "https://go.transunion.com/_next/static/media/2077e37affc4dcb7-s.p...

woff for Open Redirection

Audit cookie of "https://go.transunion.com/_next/static/media/0af43e1791b11c85-s...

pwoff for Server Side JavaScript Injection

Audit cookie of "https://go.transunion.com/_next/static/media/2077e37affc4dcb7-s.p...

woff for OS Command Injection

Audit cookie of "https://go.transunion.com/_next/static/media/0af43e1791b11c85-s...

pwoff for XML Injection

Audit cookie of "https://go.transunion.com/_next/static/media/0af43e1791b11c85-s...

woff for HTTP Header Injection

Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahaan

Tasks

- 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
 - Issues: 0

3. Crawl and audit of go.transunion.com

Issues

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...	/		Info
18:55:14 21 Oct 2024	Task 3	DOM data manipulation (DOM-based)	https://go.transunion...	/		Info
18:55:14 21 Oct 2024	Task 3	HTML5 storage manipulation (DOM-based)	https://go.transunion...	/		Info
18:55:14 21 Oct 2024	Task 3	HTML5 storage manipulation (DOM-based)	https://go.transunion...	/		Info
18:55:14 21 Oct 2024	Task 3	HTML5 storage manipulation (DOM-based)	https://go.transunion...	/		Info
18:55:14 21 Oct 2024	Task 3	Content security policy: allowedlist script reso...	https://go.transunion...	/		Info
18:55:14 21 Oct 2024	Task 3	Content security policy: allows untrusted style...	https://go.transunion...	/		Info
18:55:14 21 Oct 2024	Task 3	Content security policy: allows untrusted scrip...	https://go.transunion...	/		Info
18:55:14 21 Oct 2024	Task 3	Content security policy: allows untrusted scrip...	https://go.transunion...	/		Info
18:55:14 21 Oct 2024	Task 3	Cacheable HTTPS response	https://go.transunion...	/robots.txt		Info
18:55:14 21 Oct 2024	Task 3	Cross-domain script include	https://go.transunion...	/		Info
18:55:14 21 Oct 2024	Task 3	Strict transport security not enforced	https://go.transunion...	/		Low
18:55:14 21 Oct 2024	Task 3	TLS certificate	https://go.transunion...	/		Info

Issue detail

This issue was found in multiple locations under the reported path.

Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahaan

Tasks

- 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
 - Issues: 0

3. Crawl and audit of go.transunion.com

Issues

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...	/		Info
18:55:14 21 Oct 2024	Task 3	DOM data manipulation (DOM-based)	https://go.transunion...	/		Info
18:55:14 21 Oct 2024	Task 3	HTML5 storage manipulation (DOM-based)	https://go.transunion...	/		Info
18:55:14 21 Oct 2024	Task 3	HTML5 storage manipulation (DOM-based)	https://go.transunion...	/		Info
18:55:14 21 Oct 2024	Task 3	HTML5 storage manipulation (DOM-based)	https://go.transunion...	/		Info
18:55:14 21 Oct 2024	Task 3	Content security policy: allowedlist script reso...	https://go.transunion...	/		Info
18:55:14 21 Oct 2024	Task 3	Content security policy: allows untrusted style...	https://go.transunion...	/		Info
18:55:14 21 Oct 2024	Task 3	Content security policy: allows untrusted scrip...	https://go.transunion...	/		Info
18:55:14 21 Oct 2024	Task 3	Content security policy: allows untrusted scrip...	https://go.transunion...	/		Info
18:55:14 21 Oct 2024	Task 3	Cacheable HTTPS response	https://go.transunion...	/robots.txt		Info
18:55:14 21 Oct 2024	Task 3	Cross-domain script include	https://go.transunion...	/		Info
18:55:14 21 Oct 2024	Task 3	Strict transport security not enforced	https://go.transunion...	/		Low
18:55:14 21 Oct 2024	Task 3	TLS certificate	https://go.transunion...	/		Info

Inspector

Response headers

```

HTTP/2 200 OK
Content-Type: text/javascript
Date: Thu, 17 Oct 2024 15:43:47 GMT
Etag: W/"923a602cb0243c307593b0d901ec460"
Last-Modified: Thu, 17 Oct 2024 15:43:26 GMT
Cache-Control: max-age=31536000, immutable
Vary: Accept-Encoding
X-Cache: Hit from cloudfront
Via: 1.1 203.113.144.5:8080, 1.1 128.112.117.7:80
X-Amz-Cf-Id: h3m-1447-nm=6400
X-Amz-Cf-Ttl: QoVadmB8RMQmR7yFC4-4_BE-1177d1e6Kw112HdwtVmOk&JatT-hQ==
Age: 337242
    
```

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	<p>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.</p> <p>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.</p> <p>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.</p>
Affected Components	<p>Web Application Configuration: Specifically, the Referrer-Policy setting within the HTTP response headers.</p> <p>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.</p> <p>Third-party Sites: Any external site linked from a vulnerable website can receive the referrer URL, which may include sensitive or confidential information.</p>
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	<ol style="list-style-type: none">1. Visit the http://go.transunion.com2. 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

h Security page

Program guidelines

Scope

Hacktivity

Thanks

Updates

Submit report

Moov

http://moov.io

Vulnerability Disclosure Program launched in Jul 2024

Response efficiency: 77%

Submit report

Stats

Reports received | 90 days 71

Last report resolved 2 years ago

Reports resolved 8

Hackers thanked 7

Assets In Scope 9

Program highlights

Managed by HackerOne

Average time to first response: 3 days, 12 hours

Average time to triage: 3 days, 12 hours

Average time to bounty: N/A

Average time to resolution: N/A

Scope exclusions

Core Ineligible Findings are out of scope and won't be rewarded. [Learn more](#)

Overview Last updated on July 25, 2024. [View changes](#)

Brand Promise

Moov looks forward to working with the security community to find vulnerabilities in order to keep our businesses and customers safe.

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](https://www.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



Join **moov** on Slack.

4760 users are registered so far.

you@yourdomain.com

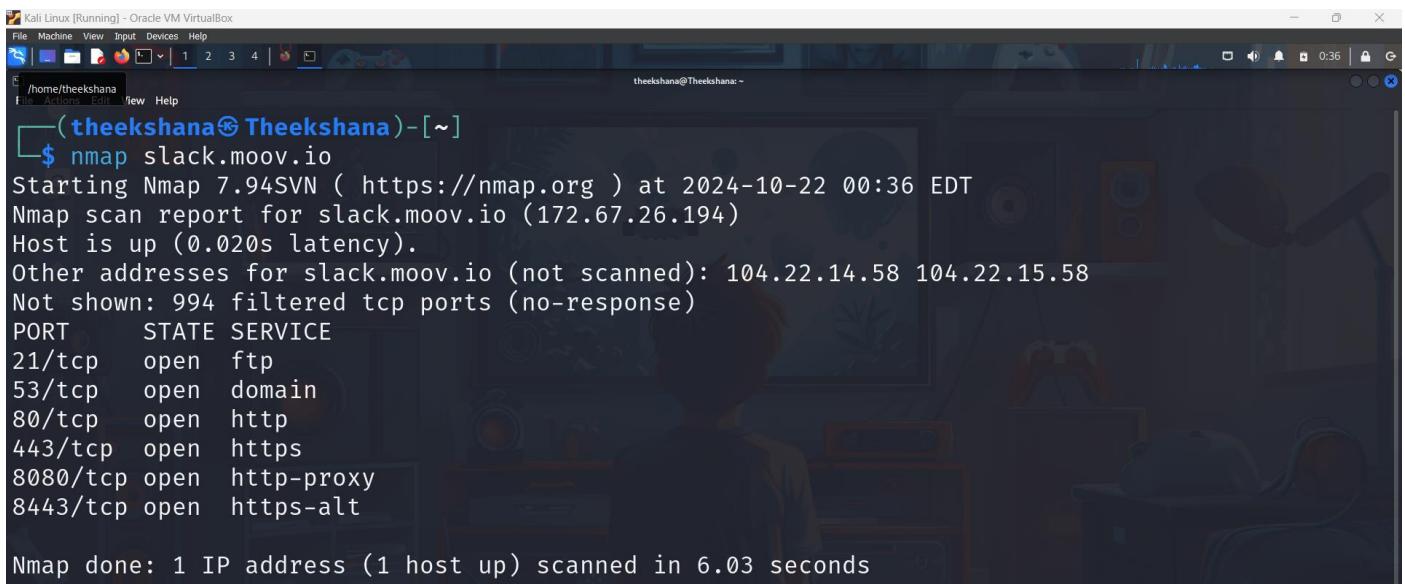
I agree to the [Code of Conduct](#).

GET MY INVITE

or sign in.

Target Reconnaissance

Nmap Scan



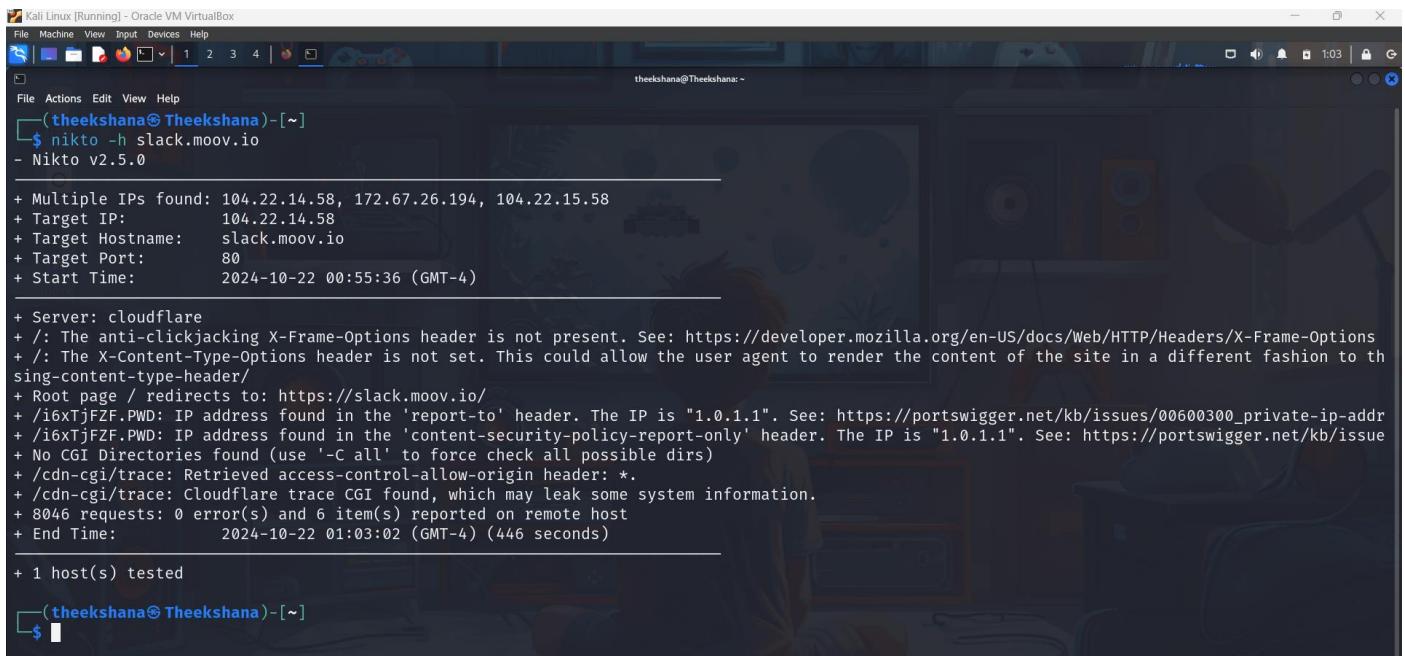
```
[Kali Linux (Running) - Oracle VM VirtualBox]
File Machine View Input Devices Help
/home/theekshana File Actions Edit New Help
[theekshana@Theekshana:~]
$ nmap slack.moov.io
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-22 00:36 EDT
Nmap scan report for slack.moov.io (172.67.26.194)
Host is up (0.020s latency).
Other addresses for slack.moov.io (not scanned): 104.22.14.58 104.22.15.58
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
8080/tcp  open  http-proxy
8443/tcp  open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 6.03 seconds
```

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



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
theekshana@Theekshana: ~
$ nikto -h slack.moov.io
- Nikto v2.5.0

+ Multiple IPs found: 104.22.14.58, 172.67.26.194, 104.22.15.58
+ Target IP: 104.22.14.58
+ Target Hostname: slack.moov.io
+ Target Port: 80
+ Start Time: 2024-10-22 00:55:36 (GMT-4)

+ Server: cloudflare
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the
+ sing-content-type-header/
+ Root page / redirects to: https://slack.moov.io/
+ /i6xTjFZF.PWD: IP address found in the 'report-to' header. The IP is "1.0.1.1". See: https://portswigger.net/kb/issues/00600300_private-ip-addr
+ /i6xTjFZF.PWD: IP address found in the 'content-security-policy-report-only' header. The IP is "1.0.1.1". See: https://portswigger.net/kb/issue
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /cdn-cgi/trace: Retrieved access-control-allow-origin header: *
+ /cdn-cgi/trace: Cloudflare trace CGI found, which may leak some system information.
+ 8046 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time: 2024-10-22 01:03:02 (GMT-4) (446 seconds)

+ 1 host(s) tested

theekshana@Theekshana: ~
$
```

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 Scanner

```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
theekshana@Theekshana: ~
$ sqlmap -h
{1.7.11#stable}
https://sqlmap.org

Usage: python3 sqlmap [options]

Options:
-h, --help Show basic help message and exit
-hh Show advanced help message and exit
--version Show program's version number and exit
-v VERBOSE Verbosity level: 0-6 (default 1)

Target:
At least one of these options has to be provided to define the target(s)

-u URL, --url=URL Target URL (e.g. "http://www.site.com/vuln.php?id=1")
-g GOOGLEDORK Process Google dork results as target URLs

Request:
These options can be used to specify how to connect to the target URL

--data=DATA Data string to be sent through POST (e.g. "id=1")
--cookie=COOKIE HTTP Cookie header value (e.g. "PHPSESSID=a8d127e..")
--random-agent Use randomly selected HTTP User-Agent header value
--proxy=PROXY Use a proxy to connect to the target URL
--tor Use Tor anonymity network
--check-tor Check to see if Tor is used properly

Injection:
These options can be used to specify which parameters to test for,
provide custom injection payloads and optional tampering scripts
```

```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
theekshana@Theekshana: ~
$ sqlmap -u slack.moov.io --level 5 --risk 3 --batch
{1.7.11#stable}
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws
esponsible for any misuse or damage caused by this program

[*] starting @ 01:10:39 /2024-10-22/

[01:10:40] [INFO] testing connection to the target URL
[01:10:40] [CRITICAL] WAF/IPS identified as 'Cloudflare'
[01:10:40] [WARNING] the web server responded with an HTTP error code (403) which could interfere with the results of the tests
[01:10:40] [INFO] checking if the target is protected by some kind of WAF/IPS
[01:10:40] [INFO] testing if the target URL content is stable
[01:10:41] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable parameters are detected
manual paragraph 'Page comparison'
how do you want to proceed? [(C)ontinue/(s)tring/(r)egeX/(q)uit] c
[01:10:41] [INFO] testing if parameter 'User-Agent' is dynamic
got a 301 redirect to 'https://slack.moov.io/'. Do you want to follow? [Y/n] Y
[01:10:42] [WARNING] potential CAPTCHA protection mechanism detected
[01:10:42] [INFO] parameter 'User-Agent' appears to be dynamic
[01:10:42] [WARNING] heuristic (basic) test shows that parameter 'User-Agent' might not be injectable
[01:10:42] [INFO] testing for SQL injection on parameter 'User-Agent'
[01:10:42] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[01:10:52] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[01:11:13] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT)'
[01:11:19] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[01:11:23] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[01:11:28] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'
[01:11:29] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (comment)'
[01:11:30] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - comment)'
[01:11:31] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[01:11:36] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
```

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

```

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
theekshana@Theekshana: ~
$ nuclei -u slack.moov.io
v3.3.4
projectdiscovery.io

[INF] Current nuclei version: v3.3.4 (outdated)
[INF] Current nuclei-templates version: v10.0.2 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 68
[INF] Templates loaded for current scan: 8654
[INF] Executing 8455 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 199 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Running httpx on input host
[INF] Found 1 URL from httpx
[INF] Templates clustered: 1613 (Reduced 1517 Requests)
[INF] Using Interactsh Server: oast.me
[missing-sri] [http] [info] https://slack.moov.io ["https://www.google.com/recaptcha/api.js", "https://cdnjs.cloudflare.com/ajax/libs/socket.io/1.7.4/socket.i
[waf-detect:cloudflare] [http] [info] https://slack.moov.io
[INF] Skipped slack.moov.io:443 from target list as found unresponsive 30 times
[tls-version] [ssl] [info] slack.moov.io:443 ["tls12"]
[tls-version] [ssl] [info] slack.moov.io:443 ["tls13"]
[caa-fingerprint] [dns] [info] slack.moov.io
[ssl-issuer] [ssl] [info] slack.moov.io:443 ["Let's Encrypt"]
[ssl-dns-names] [ssl] [info] slack.moov.io:443 ["*.cards.moov.io", "*.moov.io", "moov.io"]
[wildcard-tls] [ssl] [info] slack.moov.io:443 ["CN: moov.io", "SAN: [*.cards.moov.io *.moov.io moov.io]"]

theekshana@Theekshana: ~
$ 

```

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

```
(theekshana㉿Theekshana) ~
$ dmitry slack.moov.io
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:104.22.15.58
HostName:slack.moov.io

Gathered Inet-whois information for 104.22.15.58

inetnum: 103.255.78.0 - 104.37.31.255
netname: NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr: IPv4 address block not managed by the RIPE NCC
remarks:
remarks:
remarks: For registration information,
remarks: you can consult the following sources:
remarks: IANA
remarks: http://www.iana.org/assignments/ipv4-address-space
remarks: http://www.iana.org/assignments/iana-ipv4-special-registry
remarks: http://www.iana.org/assignments/ipv4-recovered-address-space
remarks: AFRINIC (Africa)
remarks: http://www.apnic.net/ whois.apnic.net
remarks: APNIC (Asia Pacific)
remarks: http://www.apnic.net/ whois.apnic.net
remarks: ARIN (Northern America)
remarks: http://www.arin.net/ whois.arin.net

(theekshana㉿Theekshana) ~
File Actions Edit View Help
address: see http://www.iana.org.
admin-c: IANAI-RIPE
tech-c: IANAI-RIPE
nic-hdlc: IANAI-RIPE
remarks: For more information on IANA services
remarks: Go to IANA web site at http://www.iana.org.
mnt-by: RIPE-NCC-MNT
created: 1970-01-01T00:00:00Z
last-modified: 2001-09-22T09:31:27Z
source: RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.114 (ABERDEEN)

Gathered Inic-whois information for slack.moov.io

Gathered Netcraft information for slack.moov.io

Retrieving Netcraft.com information for slack.moov.io
Netcraft.com Information gathered

Gathered Subdomain information for slack.moov.io

Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 possible subdomain(s) for host slack.moov.io, Searched 0 pages containing 0 results

Gathered E-Mail information for slack.moov.io

Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 e-mail(s) for host slack.moov.io, Searched 0 pages containing 0 results

Gathered TCP Port information for 104.22.15.58

Port      State
21/tcp    open
53/tcp    open
80/tcp    open

Ports scan Finished: Scanned 150 ports, 0 ports were in state closed

All scans completed, exiting
(theekshana㉿Theekshana) ~
```

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

Detailed Scan Report

http://slack.moov.io/ [🔗](#)
 Scan Time : 10/22/2024 11:17:19 AM (UTC+05:30)

Total Requests: 4,174
 Average Speed: 25.6r/s

Risk Level: **MEDIUM**

VULNERABILITIES

16 IDENTIFIED	3 CONFIRMED	0 ! CRITICAL	0 ! HIGH	1 ! MEDIUM	4 ! LOW
				5 ! BEST PRACTICE	6 ! INFORMATION

Identified Vulnerabilities

Critical	0
High	0
Medium	1
Low	4
Best Practice	5
Information	6
TOTAL	16

Confirmed Vulnerabilities

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

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

This screenshot shows the OWASP ZAP interface running on Kali Linux. The main window displays an 'Automated Scan' configuration screen with the URL <http://slack.moov.io> entered in the 'URL to attack:' field. Below the URL input is a note: 'Please be aware that you should only attack applications that you have been specifically been given permission to test.' The 'Attack' button is highlighted with a red rectangle. The bottom left pane shows a list of alerts found during the scan, including 'CSP: Wildcard Directive (2)', 'Content Security Policy (CSP) Header Not Set', 'Cross-Domain Misconfiguration (10)', and 'Hidden File Found (2)'. The 'Alerts' tab is selected.

This screenshot shows the 'Edit Alert' dialog for a 'Cross-Domain Misconfiguration' alert found on <http://slack.moov.io>. The dialog fields include URL, Risk (Medium), Confidence (Medium), Parameter (empty), Attack (empty), Evidence (access-control-allow-origin: *), CWE ID (264), and WASC ID (14). The 'Description' field contains the text: 'Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.' The 'Other Info' section provides context about CORS misconfigurations. The 'Solution' section offers guidance on how to mitigate the issue. The 'Alert Tags' section lists tags such as 'OWASP_2017_A05', 'CWE-264', and 'OWASP_2021_A01'. Reference URLs are provided for each tag.

This screenshot shows a detailed view of a 'Cross-Domain Misconfiguration' alert for the URL <http://slack.moov.io>. The alert details match those in the previous 'Edit Alert' dialog. The 'Header' and 'Body' panes show the raw HTTP response headers and body content, respectively. The response body includes a portion of the HTML page with styling rules like 'background-color: #000000;' applied to various elements. The bottom left pane shows the same list of alerts as the first screenshot, including the 'Cross-Domain Misconfiguration (10)' item.

Burp Suite

Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan

Tasks

- 3. Crawl and audit of slack.moov.io**
- 2. Live audit from Proxy (all traffic)**
- 1. Live passive crawl from Proxy (all traffic)**

Issues: 0 0 10 19

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

Issues: 0 0 0 0

3. Crawl and audit of slack.moov.io

Most serious vulnerabilities found (live)

Issue type	Host	Time
Strict transport security not enforced	https://slack.moov.io	11:34:33 22 Oct 20...
Strict transport security not enforced	https://slack.moov.io	11:34:33 22 Oct 20...
Strict transport security not enforced	https://slack.moov.io	11:34:33 22 Oct 20...
Strict transport security not enforced	https://slack.moov.io	11:34:33 22 Oct 20...
Strict transport security not enforced	https://slack.moov.io	11:34:34 22 Oct 20...
Strict transport security not enforced	https://slack.moov.io	11:34:34 22 Oct 20...
Strict transport security not enforced	https://slack.moov.io	11:34:34 22 Oct 20...
Strict transport security not enforced	https://slack.moov.io	11:34:34 22 Oct 20...
Strict transport security not enforced	https://slack.moov.io	11:34:34 22 Oct 20...
Open redirection (DOM-based)	https://slack.moov.io	11:34:41 22 Oct 20...
Open redirection (DOM-based)	https://slack.moov.io	11:34:41 22 Oct 20...
Cachable HTTPS response	https://slack.moov.io	11:34:34 22 Oct 20...
Cachable HTTPS response	https://slack.moov.io	11:34:34 22 Oct 20...
Content security policy: allows clickjacking	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	https://slack.moov.io	11:35:20 22 Oct 20...
Cross-origin resource sharing	https://slack.moov.io	11:35:20 22 Oct 20...
Cross-origin resource sharing: arbitrary	https://slack.moov.io	11:35:15 22 Oct 20...
Cross-origin resource sharing: arbitrary	https://slack.moov.io	11:35:20 22 Oct 20...
Cross-origin resource sharing: arbitrary	https://slack.moov.io	11:35:20 22 Oct 20...
Cross-origin resource sharing: arbitrary	https://slack.moov.io	11:35:20 22 Oct 20...
Cross-origin resource sharing: arbitrary	https://slack.moov.io	11:35:20 22 Oct 20...
Cross-origin resource sharing: arbitrary	https://slack.moov.io	11:34:34 22 Oct 20...

Task configuration

Task type: Crawl & audit

Scope: slack.moov.io

Configuration: Crawl and Audit - Fast

Task progress

Total audit items: 11 Unique locations: 6

Audit items pending: 0 Pending actions: 0

Audit items in progress: 11 Current link depth: 0

Audit items completed: 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
- > Auditing JSON parameter of "https://slack.moov.io/cdn-cgi/rum" for HTTP Header injection

Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan

Tasks

- 3. Crawl and audit of slack.moov.io**
- 2. Live audit from Proxy (all traffic)**
- 1. Live passive crawl from Proxy (all traffic)**

Issues: 0 0 10 19

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

Issues: 0 0 0 0

3. Crawl and audit of slack.moov.io

Issues

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	Information
11:35:20 22 Oct 2024	Task 3	Cross-origin resource sharing	https://slack.moov.io /assets/superagent.js		Information
11:35:20 22 Oct 2024	Task 3	Cross-origin resource sharing: arbitrary origin ..	https://slack.moov.io /assets/superagent.js		Information
11:35:15 22 Oct 2024	Task 3	Cross-origin resource sharing	https://slack.moov.io /		Information
11:35:15 22 Oct 2024	Task 3	Cross-origin resource sharing: arbitrary origin ..	https://slack.moov.io /assets/main.css		Information
11:35:20 22 Oct 2024	Task 3	Cross-origin resource sharing	https://slack.moov.io /assets/main.css		Information
11:35:20 22 Oct 2024	Task 3	Cross-origin resource sharing: arbitrary origin ..	https://slack.moov.io /assets/client.js		Information
11:35:20 22 Oct 2024	Task 3	Cross-origin resource sharing	https://slack.moov.io /assets/client.js		Information
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 /robots.txt		Information
11:34:34 22 Oct 2024	Task 3	Content security policy: allows clickjacking	https://slack.moov.io /robots.txt		Information

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 pb4en959onk92j3l415ocq44vaoyfm7hv916q@oastify.com was submitted in the email JSON parameter.

The application sent an email via SMTP to the specified address.

Issue background

Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan

Tasks

- 3. Crawl and audit of slack.moov.io**
- 2. Live audit from Proxy (all traffic)**
- 1. Live passive crawl from Proxy (all traffic)**

Issues: 0 0 10 19

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

Issues: 0 0 0 0

3. Crawl and audit of slack.moov.io

Issues

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	Information
11:35:20 22 Oct 2024	Task 3	Cross-origin resource sharing	https://slack.moov.io /assets/superagent.js		Information
11:35:20 22 Oct 2024	Task 3	Cross-origin resource sharing: arbitrary origin ..	https://slack.moov.io /assets/superagent.js		Information
11:35:15 22 Oct 2024	Task 3	Cross-origin resource sharing	https://slack.moov.io /		Information
11:35:15 22 Oct 2024	Task 3	Cross-origin resource sharing: arbitrary origin ..	https://slack.moov.io /assets/main.css		Information
11:35:20 22 Oct 2024	Task 3	Cross-origin resource sharing	https://slack.moov.io /assets/main.css		Information
11:35:20 22 Oct 2024	Task 3	Cross-origin resource sharing: arbitrary origin ..	https://slack.moov.io /assets/client.js		Information
11:35:20 22 Oct 2024	Task 3	Cross-origin resource sharing	https://slack.moov.io /assets/client.js		Information
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 /robots.txt		Information
11:34:34 22 Oct 2024	Task 3	Content security policy: allows clickjacking	https://slack.moov.io /robots.txt		Information

Advisory Request Response Path to issue

1. HTTP/2 200 OK
2. Date: Tue, 22 Oct 2024 06:05:00 GMT
3. Content-Type: application/javascript; charset=UTF-8
4. Access-Control-Allow-Origin: *
5. Cache-Control: public, max-age=14400
6. Etag: W/“d9-177eddbd4d0”

Inspector

Response headers

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. <code><iframe src="http://slack.moov.io" style="width:100%; height:100%; opacity:0;"></iframe></code>
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	<p>Web server configuration, specifically the response headers for slack.moov.io.</p> <p>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.</p>
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	<p>Open a browser and connect to http://slack.moov.io.</p> <p>Use the browser's developer tools to inspect the response headers for any static resource</p> <p>Confirm the absence of the X-Content-Type-Options header, which would normally prevent MIME-type sniffing.</p> <p>Simulate a file type change (for instance, renaming a .js file to .txt) and observe how the browser tries to guess the content type.</p>
Proof of Concept	<p>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.</p> <p>Use network analysis tools or browser developer tools to confirm that the resource is missing the X-Content-Type-Options: nosniff header.</p>
Proposed Mitigation or Fix	<p>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.</p> <p>Header set X-Content-Type-Options "nosniff"</p>

Report 03 Target Details

The screenshot shows a bug bounty report interface. On the left is a sidebar with various icons and a navigation menu. The main area has a header for 'Program highlights' and several sections: 'Rewards', 'Severity', 'Rewards', and a summary of average response times.

Program highlights:

- Open Scope: Rewards reports for all owned assets based on impact, even if not listed in scope.
- Fast Payment: Ensures payment within 1 month of receiving a vulnerability report.
- Gold Standard: Adheres to Gold Standard Safe Harbor.
- Platform Standards: Fully compliant with Platform Standards.
- Top Response Efficiency: This program's response efficiency is above 90%.

Managed by HackerOne | Collaboration Enabled | Includes Retesting

Rewards:

Severity	Rewards
Low	\$500 Avg. bounty \$840 43.59% submissions
Medium	\$500-\$5,000 Avg. bounty \$1,465 38.03% submissions
High	\$5,000-\$25,000

Average time to first response: 1 day, 8 hours (48 hours)

Average time to triage: 3 days, 2 hours (18 hours)

Average time to bounty: 3 days, 11 hours (77 hours)

Average time from submission to bounty: 6 days, 13 hours (155 hours)

Average time to resolution: 3 weeks, 3 days (210 hours)

Grammarly:

- Link: <https://www.grammarly.com>
- Description: Grammarly makes sure everything you type is clear, effective, and mistake-free.
- Bug Bounty Program launched in Dec 2018
- Response efficiency: 97%

Submit report

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

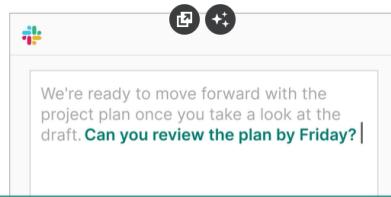
Responsible AI that ensures your writing and reputation shine

Work with an AI writing partner that helps you find the words you need—to write that tricky email, to get your point across, to keep your work moving.

[Sign up It's free →](#)

 Sign up with Google

By signing up, you agree to the [Terms and Conditions](#) and [Privacy Policy](#). California residents, see our [CA Privacy Notice](#).



Specify a deadline to review the plan.
[Show this change >](#)



Target Reconnaissance

Nmap Scan

```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(theekshana㉿Theekshana) - [~]
$ nmap app.grammarly.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-22 04:41 EDT
Nmap scan report for app.grammarly.com (18.208.28.153)
Host is up (0.026s latency).
Other addresses for app.grammarly.com (not scanned): 35.169.22.223 174.129.247.3
rDNS record for 18.208.28.153: ec2-18-208-28-153.compute-1.amazonaws.com
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 20.40 seconds
(theekshana㉿Theekshana) - [~]
$
```

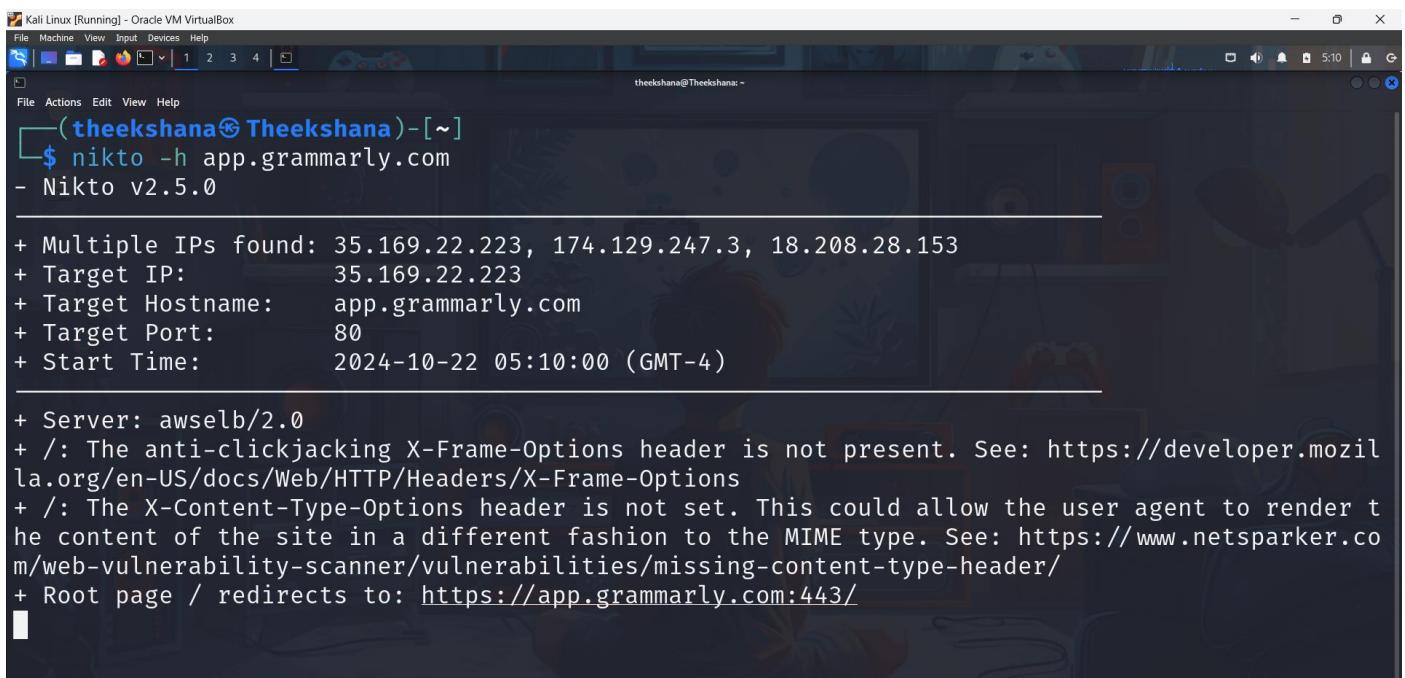
By scanning app.grammarly.com with Nmap I found out these information.

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

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



```

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
theekshana@Theekshana: ~
└─$ nikto -h app.grammarly.com
- Nikto v2.5.0

+ Multiple IPs found: 35.169.22.223, 174.129.247.3, 18.208.28.153
+ Target IP: 35.169.22.223
+ Target Hostname: app.grammarly.com
+ Target Port: 80
+ Start Time: 2024-10-22 05:10:00 (GMT-4)

+ Server: awselb/2.0
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: https://app.grammarly.com:443/

```

The screenshot shows the output of a Nikto scan against the target app.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.

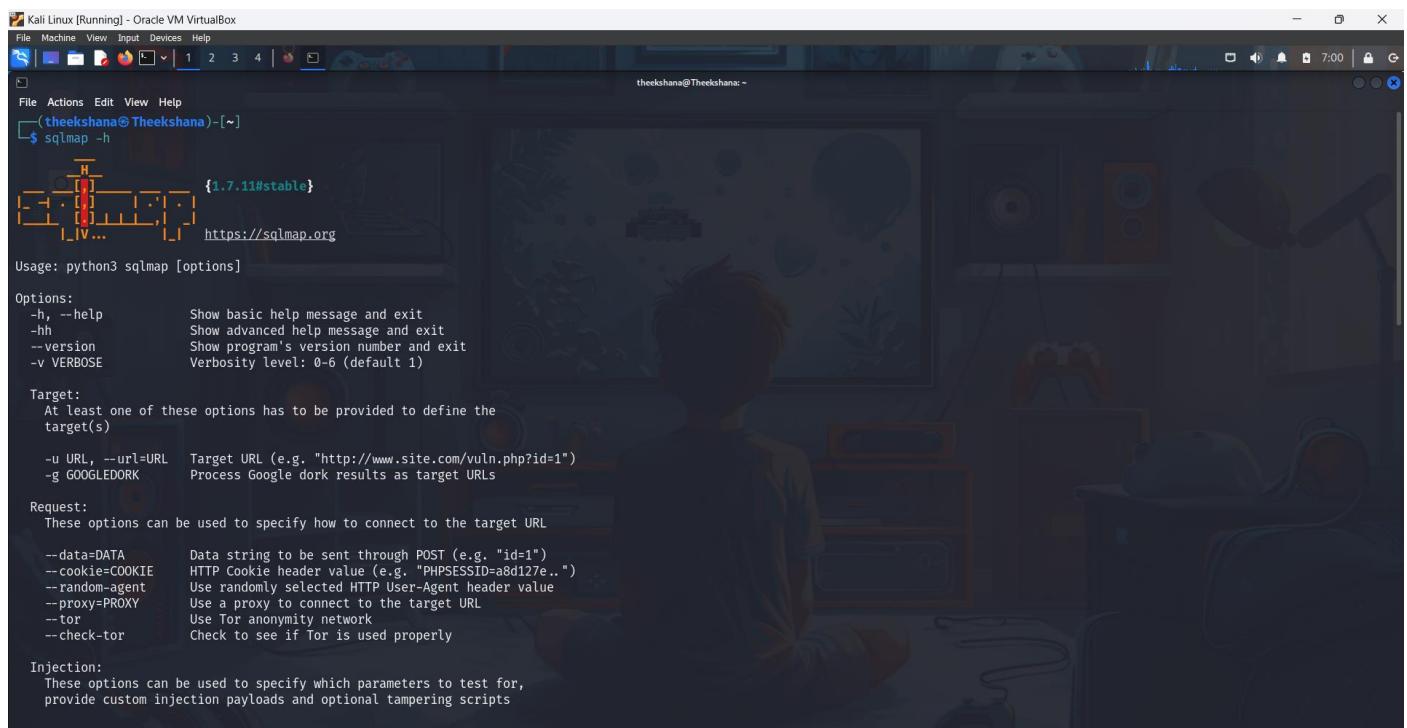
- **Missing X-Content-Type-Options Header:**

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 Scanner



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal is running the SQLmap command. The output is as follows:

```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
theekshana@Theekshana: ~
$ sqlmap -h
{ 1.7.11#stable }
https://sqlmap.org

Usage: python3 sqlmap [options]

Options:
-h, --help          Show basic help message and exit
--hh               Show advanced help message and exit
--version          Show program's version number and exit
-v VERBOSE         Verbosity level: 0-6 (default 1)

Target:
At least one of these options has to be provided to define the target(s)

-u URL, --url=URL  Target URL (e.g. "http://www.site.com/vuln.php?id=1")
-g GOOGLEDORK      Process Google dork results as target URLs

Request:
These options can be used to specify how to connect to the target URL

--data=DATA        Data string to be sent through POST (e.g. "id=1")
--cookie=COOKIE    HTTP Cookie header value (e.g. "PHPSESSID=a8d127e..")
--random-agent     Use randomly selected HTTP User-Agent header value
--proxy=PROXY      Use a proxy to connect to the target URL
--tor              Use Tor anonymity network
--check-tor        Check to see if Tor is used properly

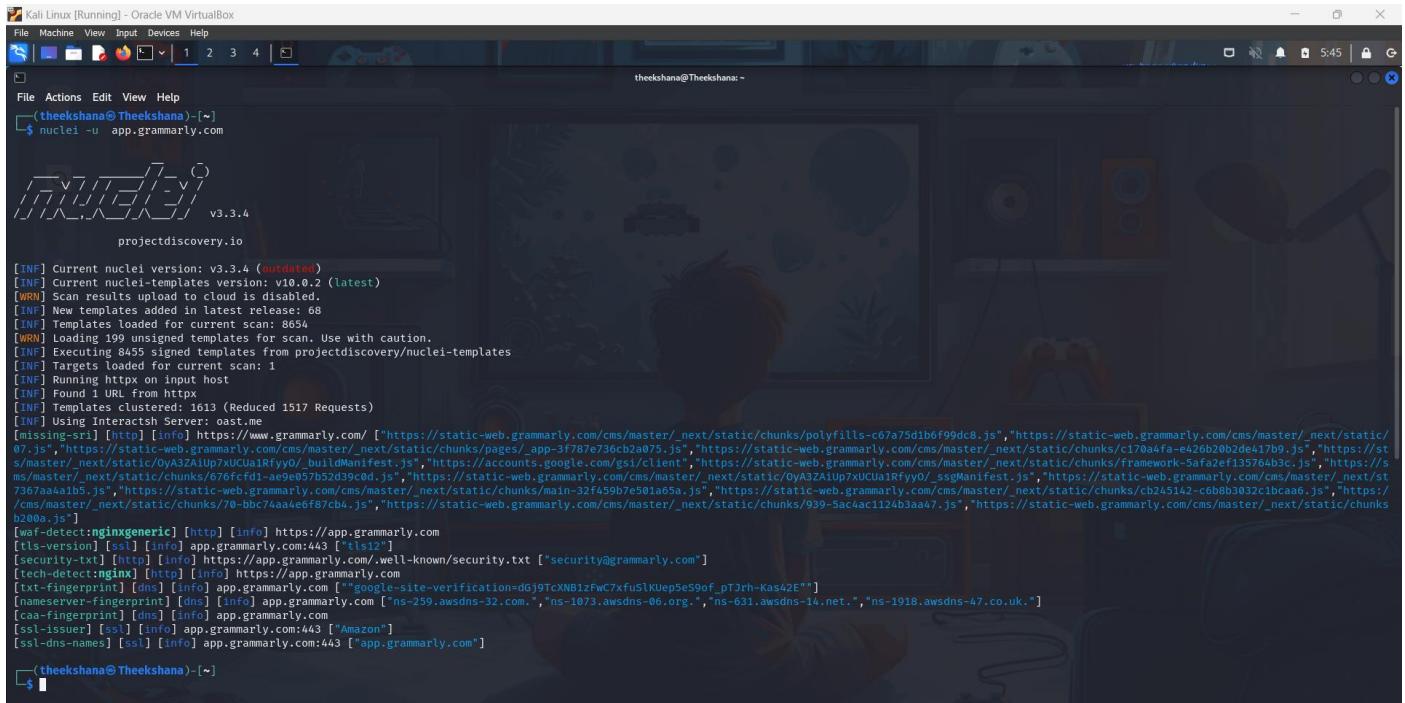
Injection:
These options can be used to specify which parameters to test for,
provide custom injection payloads and optional tampering scripts
```

```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
theekshana@Theekshana: ~
$ sqlmap -u app.grammarly.com --level 5 --risk 3 --batch
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility for any misuse or damage caused by this program
[*] starting @ 05:19:03 /2024-10-22/
[05:19:03] [INFO] testing connection to the target URL
got a 301 redirect to 'https://app.grammarly.com:443/'. Do you want to follow? [Y/n] Y
[05:19:06] [INFO] checking if the target is protected by some kind of WAF/IPS
[05:19:08] [INFO] testing if the target URL content is stable
[05:19:10] [WARNING] parameter 'User-Agent' does not appear to be dynamic
[05:19:12] [WARNING] heuristic (basic) test shows that parameter 'User-Agent' might not be injectable
[05:19:14] [INFO] testing for SQL injection on parameter 'User-Agent'
[05:19:14] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[05:23:00] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[05:24:58] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT)'
[05:29:00] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[05:32:00] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[05:33:21] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'
```

Vulnerabilities Detected:

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

Nuclei Scan



The screenshot shows a terminal window on a Kali Linux desktop. The terminal title is 'Nuclei Scan'. The command run is '\$ nuclei -u app.grammarly.com'. The output shows Nuclei version 3.3.4 and various scan logs, including template loading, target scanning, and specific findings like missing SRI on static resources.

```
[INFO] Current nuclei version: v3.3.4 (outdated)
[INFO] Current nuclei-templates version: v10.0.2 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 68
[INF] Templates loaded for current scan: 8654
[WRN] Loading 199 unsigned templates for scan. Use with caution.
[INF] Executing 8455 signed templates from projectdiscovery/nuclei-templates
[INF] Targets loaded for current scan: 1
[INF] Running https on input host
[INF] Found 1 URL from httpx
[INF] Templates clustered: 1613 (Reduced 1517 Requests)
[INF] Using Interactsh Server: oast.me
[missing-sri] [http] [info] https://www.grammarly.com/ [https://static-web.grammarly.com/cms/master/_next/static/chunks/polyfills-c67a75d1b6f99dc8.js,"https://static-web.grammarly.com/cms/master/_next/static/07.js","https://static-web.grammarly.com/cms/master/_next/static/chunks/pages/_app-3f787e736cb2a75.js","https://static-web.grammarly.com/cms/master/_next/static/chunks/c170a4fa-e426b20b2de417b9.js","https://static-web.grammarly.com/cms/master/_next/static/manifest-0y32A1Up7xUa1RfyO_buildManifest.js","https://accounts.google.com/gsi/client","https://static-web.grammarly.com/cms/master/_next/static/chunks/framework-5afa2ef1357643c.js","https://static-web.grammarly.com/cms/master/_next/static/chunks/676fcfd1-aee8e57b52d39c0d.js","https://static-web.grammarly.com/cms/master/_next/static/0yA3ZAIUp7xUa1RfyO_sgsmManifest.js","https://static-web.grammarly.com/cms/master/_next/static/7367a441b5.js","https://static-web.grammarly.com/cms/master/_next/static/chunks/main-32f459b7e501a65a.js","https://static-web.grammarly.com/cms/master/_next/static/chunks/cd245142-c6b8b3032c1bcaa6.js","https://static-web.grammarly.com/cms/master/_next/static/chunks/70-bbc7aaa4e6f87cb4.js","https://static-web.grammarly.com/cms/master/_next/static/chunks/939-5acac1124d3aa7.js","https://static-web.grammarly.com/cms/master/_next/static/chunks/b20a.js"]
[waf-detect:nginxgeneric] [http] [info] https://app.grammarly.com
[tls-version] [ssl] [info] app.grammarly.com:443 [tls12]
[security-txt] [http] [info] https://app.grammarly.com/.well-known/security.txt ["security@grammarly.com"]
[tech-detect:nginx] [http] [info] https://app.grammarly.com
[txt-fingerprint] [dns] [info] app.grammarly.com ["google-site-verification=d697cXNB1zFwC7xfuSlKuep5e59of_pTJrh-Kas42E**"]
[nameserver-fingerprint] [dns] [info] app.grammarly.com ["ns-259.awsdns-32.com.", "ns-1073.awsdns-06.org.", "ns-631.awsdns-14.net.", "ns-1918.awsdns-47.co.uk."]
[caa-fingerprint] [dns] [info] app.grammarly.com
[ssl-issue] [ssl] [info] app.grammarly.com:443 [Amazon]
[ssl-dns-names] [ssl] [info] app.grammarly.com:443 ['app.grammarly.com']

(theekshana@Theekshana)-~]
```

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

```
File Machine View Input Devices Help
theekshana@Theekshana: ~
[theekshana@Theekshana: ~]
dmitry app.grammarly.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:174.129.247.3
HostName:app.grammarly.com

Gathered Inet-whois Information for 174.129.247.3

inetnum: 173.255.152.0 - 174.139.255.255
netname: NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
desc: IPv4 address block not managed by the RIPE NCC
remarks:
remarks:
For registration information,
you can consult the following sources:
remarks: RIPE
remarks: IANA
remarks: http://www.iana.org/assignments/ipv4-address-space
remarks: http://www.iana.org/assignments/iana-ipv4-special-registry
remarks: http://www.iana.org/assignments/ipv4-recovered-address-space
remarks: AFRINIC (Africa)
remarks: http://www.afrinic.net/ whois.afrinic.net
remarks: APNIC (Asia Pacific)
remarks: http://www.apnic.net/ whois.apnic.net
remarks: ARIN (Northern America)
remarks: http://www.arin.net/ whois.arin.net
remarks: LACNIC (Latin America and the Caribbean)
remarks: http://www.lacnic.net/ whois.lacnic.net
remarks:
country: EU # Country is really world wide
admin-c: IANAI-RIPE
tech-c: IANAI-RIPE
status: ALLOCATED-UNSPECIFIED
mnt-by: RIPE-NCC-HM-MNT
created: 2019-01-07T10:50:40Z
last-modified: 2019-01-07T10:50:40Z
source: RIPE

File Actions Edit View Help
theekshana@Theekshana: ~
[theekshana@Theekshana: ~]
dmitry app.grammarly.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:174.129.247.3
HostName:app.grammarly.com

Gathered Inet-whois Information for 174.129.247.3

inetnum: 173.255.152.0 - 174.139.255.255
netname: NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
desc: IPv4 address block not managed by the RIPE NCC
remarks:
remarks:
For more information on IANA services
go to IANA web site at http://www.iana.org.
mnt-by: RIPE-NCC-HM-MNT
created: 1970-01-01T00:00:00Z
last-modified: 2001-09-22T09:31:27Z
source: RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.114 (ABERDEEN)

Gathered Inic-whois Information for app.grammarly.com
ERROR: Unable to locate Name Whois data on app.grammarly.com
Gathered Netcraft information for app.grammarly.com

Retrieving Netcraft.com information for app.grammarly.com
Netcraft.com Information gathered
Gathered Subdomain information for app.grammarly.com
Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 possible subdomain(s) for host app.grammarly.com, Searched 0 pages containing 0 results
Gathered E-Mail information for app.grammarly.com
Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 E-mail(s) for host app.grammarly.com, Searched 0 pages containing 0 results
Gathered TCP Port information for 174.129.247.3

Port      State
21/tcp    open
53/tcp    open
80/tcp    open
```

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.

<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
IDENTIFIED3
CONFIRMED0 !
CRITICAL0 !
HIGH2 MEDIUM
2 LOW
4 ?
4 i
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

- 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

The screenshot shows the OWASP ZAP interface with an "Automated Scan" dialog open. The URL to attack is set to `http://app.grammarly.com`. The "Use traditional spider:" checkbox is checked. The "Use ajax spider:" dropdown is set to "If Modern with Firefox Headless". The progress bar indicates "Actively scanning (attacking) the URLs discovered by the spider(s)". On the left, a sidebar shows a list of alerts under the "Alerts (17)" section, which is highlighted with a red box. The alerts include various security issues such as Cloud Metadata Potentially Exposed, CSP: Wildcard Directive, and Cookie No HttpOnly Flag.

This screenshot shows a detailed view of an alert titled "Cloud Metadata Potentially Exposed". The alert details include the URL (`http://app.grammarly.com/latest/meta-data/`), Risk (High), Confidence (Low), Attack IP (169.254.169.254), Evidence (empty), and CWE/WASC IDs (both 0). The "Description" section notes that the attack attempts to abuse a misconfigured NGINX server to access instance metadata from providers like AWS, GCP, and Azure. The "Solution" section advises not to trust user data in NGINX configs due to the use of the \$host variable. A reference link to the Nginx blog is provided. The "Alert Tags" section lists "OWASP_2021_A05" and "OWASP_2017_A06".

The screenshot displays a captured response in the Requester tab. The header shows standard HTTP headers like Content-Length, Connection, Date, and X-Xss-Protection. The body content is heavily redacted, showing only a few lines of the original HTML. Below the response, a sidebar shows a list of alerts, including "Cloud Metadata Potentially Exposed" and "CSP: Wildcard Directive", with the latter being the selected item. The "Description" for the selected alert states that Content Security Policy (CSP) helps detect XSS attacks and provides a set of approved content sources.

Burp Suite

Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahaan

Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Tasks

New scan New live task Filter Search

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 Issues: 0 0 0 0

Most serious vulnerabilities found (live)

Issue type	Host	Time
Strict transport security not enforced	https://app.grammarly...	15:43:59 22 Oct 202...
Cookie scoped to parent domain	https://app.grammarly...	15:43:59 22 Oct 202...
Cookie without HttpOnly flag set	https://app.grammarly...	15:43:59 22 Oct 202...
TLS certificate	https://app.grammarly...	15:44:00 22 Oct 202...
TLS cookie without secure flag set	https://app.grammarly...	15:43:59 22 Oct 202...

Task configuration

Task type: Crawl & audit
Scope: app.grammarly.com
Configuration: Crawl and Audit - Fast

Task progress

Total audit items: 2 Unique locations: 0
Audit items pending: 0 Pending actions: 0
Audit items in progress: 0 Current link depth: 0
Audit items completed: 2 Requests: 309
Network errors: 0

Task log

> Audit item "https://www.grammarly.com/info.txt" for RackUnit File Rename Extension

Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahaan

Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Tasks

New scan New live task Filter Search

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 Issues: 0 0 0 0

Issues

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 Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahaan

Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Tasks

New scan New live task Filter Search

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 Issues: 0 0 0 0

Issues

Advisory Request Response Path to issue

Pretty Raw Hex Render

```
1 HTTP/2 301 Moved Permanently
2 Date: Tue, 22 Oct 2024 10:13:17 GMT
3 Content-Type: text/html
4 Content-Length: 162
5 Location: https://www.grammarly.com/
6 Server: nginx
7 Cache-Control: no-cache
8 Set-Cookie: request_location=pg0x8ELj3L1i1uuhG5YXpb24iOJ0dHfPcozv1d3d5ncmFtbWfybHku29tLyj9;
9 Version=1;Domain=.grammarly.com;Path=/;Max-Age=3600;Secure;HttpOnly
10 Set-Cookie: funnelType=free;Version=1;Domain=.grammarly.com;Path=/;Max-Age=108000
11 Set-Cookie: browser_info=HOME;ID=6;COMPUTER=SUPTED;PREMIUM;WINDOWS_10;WINDOWS;
12 Version=1;Domain=.grammarly.com;Path=/;Max-Age=3600
13
14 <html>
15 <head>
```

Inspector

Response headers

Vulnerabilities:

1 Cloud Metadata Potentially Exposed

Vulnerability Title	Cloud Metadata Potentially Exposed
Vulnerability Description	<p>The vulnerability allows unauthorized access to cloud instance metadata, which may contain sensitive information such as credentials, API tokens, and service configurations.</p> <p>This can occur when access to metadata services is not properly restricted.</p>
Affected Components	<p>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.</p> <p>Example: "AWS EC2 Metadata Service, Google Cloud Compute Engine, Azure Virtual Machines."</p>
Impact Assessment	<p>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."</p>
Steps to Reproduce	<p>Spin up an EC2 instance on AWS.</p> <p>Access the instance metadata endpoint (http://169.254.169.254/latest/meta-data/) from within the instance.</p> <p>Observe the exposure of sensitive metadata without any authentication.</p>
Proof of Concept	<p>Provide a working example or a code snippet to demonstrate the vulnerability in action. This could be as simple as a curl command.</p> <pre>curl http://169.254.169.254/latest/meta-data/</pre>
Proposed Mitigation or Fix	<p>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.</p>

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	<p>Identify an HTML file that includes external JavaScript sources.</p> <p>Modify the external source to include a malicious JavaScript file.</p> <p>Access the web application and check the network requests to see the inclusion of the malicious script.</p> <p>Observe the execution of the malicious code within the application.</p>
Proof of Concept	<p>Provide a sample payload or code that demonstrates the issue in action.</p> <pre><script src="http://malicious-domain.com/malicious.js"></script></pre>
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 04 Target Details

The screenshot shows a detailed Bug Bounty report for Vendasta. On the left, there's a sidebar with various icons and a navigation menu. The main content area includes sections for 'Program highlights' (Managed by HackerOne), performance metrics (Average time to first response: 2 days, 14 hours; Average time to triage: 2 days, 22 hours; Average time to bounty: N/A; Average time to resolution: 1 month, 3 weeks), 'Scope exclusions' (Core Ineligible Findings), 'Overview' (Last updated on February 11, 2024), and an 'Introduction' section. On the right, there's a 'Stats' panel showing metrics like Reports received (90 days ago), Last report resolved (5 days ago), Reports resolved (219), Hackers thanked (123), and Assets In Scope (11). A 'Submit report' button is also present.

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.

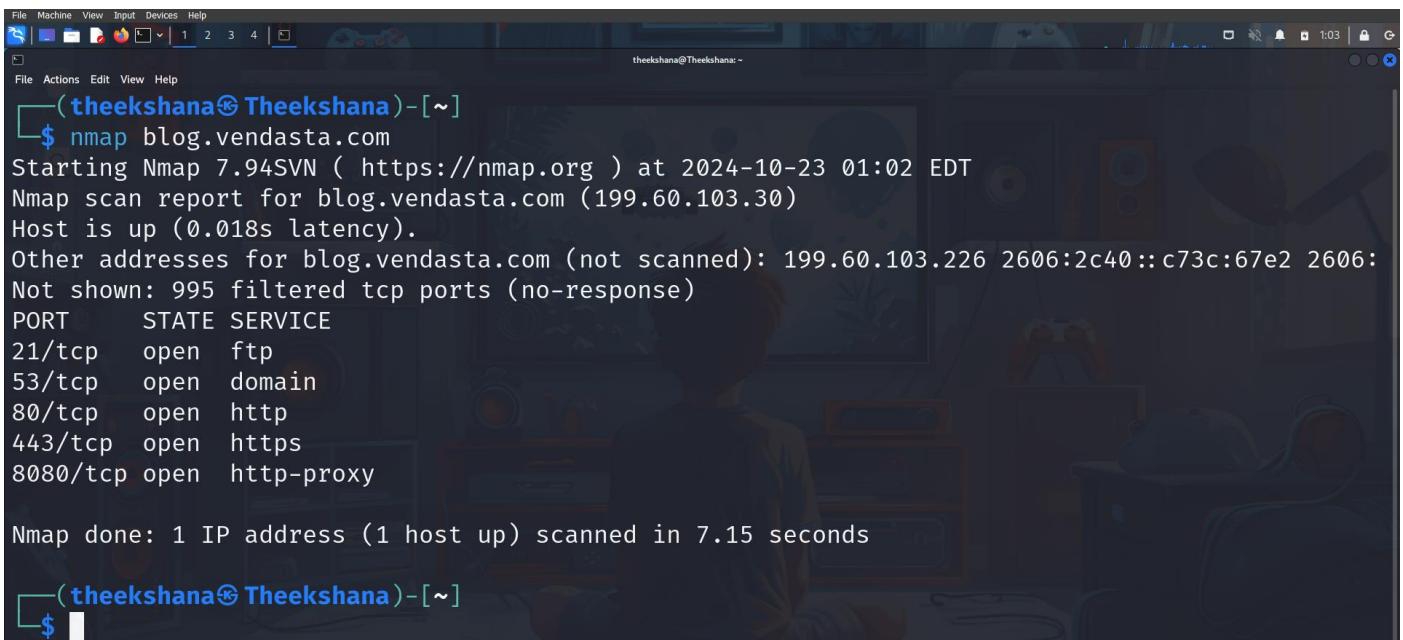
In this report, I have chosen to focus on 10 subdomains under the main domain vendasta.com. Each subdomain may serve different functionalities or services, potentially introducing distinct security risks, particularly in development or user-related areas. These subdomains were selected based on their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

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

The screenshot shows the Vendasta blog homepage. At the top, there's a dark header with the Vendasta logo, AI Tools (New), Products, Solutions, Resources, Pricing, and a 'Get free access' button. Below the header, there's a green navigation bar with 'BLOG' and 'Categories' dropdowns, along with a search bar and a 'SUBSCRIBE' button. The main content area features a large image of a hand holding a magnet over a globe, with silhouettes of people at the bottom. Below the image, the text reads: 'Agency Insights | May 17, 2024' and 'Why Lead Generation Outsourcing Is Key to Maximizing Your Growth Potential'. To the right, there are three blog card snippets: 'Marketing: 40 Awesome Review Sites to Fuel Your Business Growth' (published Sep 8, 2023), 'Marketing: The 120+ Best Online Business Directory Websites to Get Listed on (Updated 2022)' (published Aug 17, 2022), and 'Marketing: The Ultimate 10-Step Digital Marketing Strategy Playbook' (published Oct 30, 2023). A small green speech bubble icon is in the bottom right corner.

Target Reconnaissance

Nmap Scan



```
theekshana@Theekshana: ~
$ nmap blog.vendasta.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-23 01:02 EDT
Nmap scan report for blog.vendasta.com (199.60.103.30)
Host is up (0.018s latency).
Other addresses for blog.vendasta.com (not scanned): 199.60.103.226 2606:2c40::c73c:67e2 2606:
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
8080/tcp  open  http-proxy

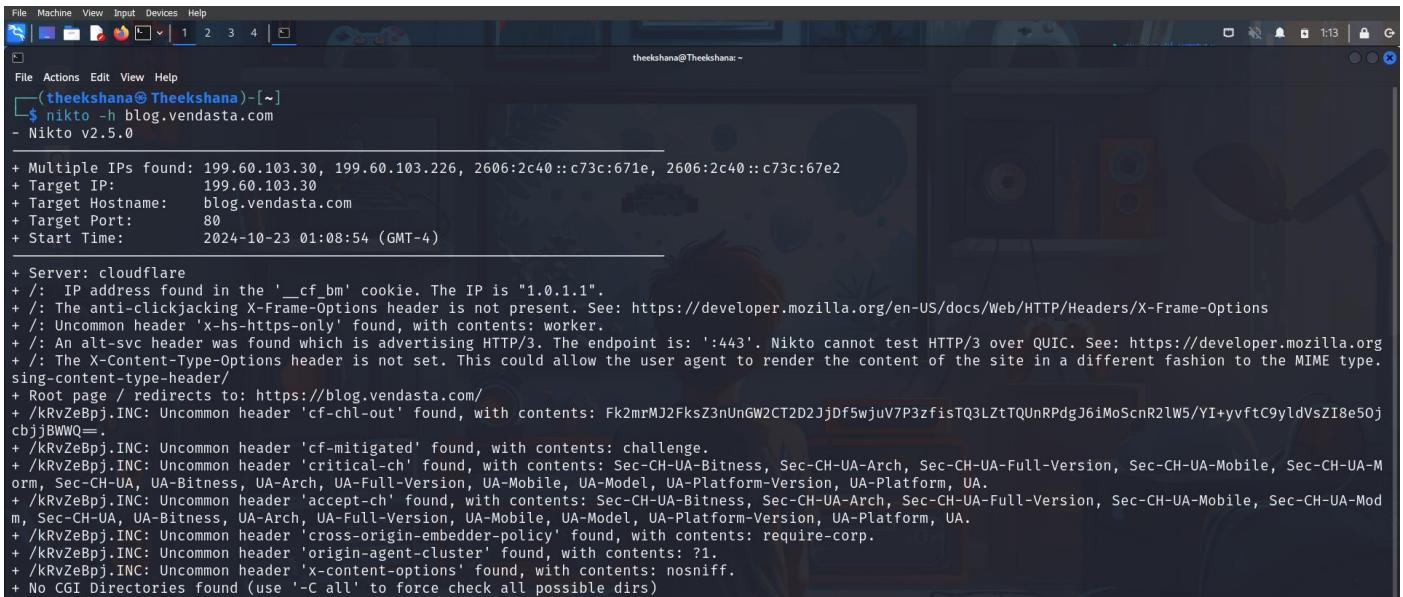
Nmap done: 1 IP address (1 host up) scanned in 7.15 seconds
```

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	HTTPS
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



```
File Machine View Input Devices Help
(theekshana@Theekshana)-[~]
$ nikto -h blog.vendasta.com
- Nikto v2.5.0

+ Multiple IPs found: 199.60.103.30, 199.60.103.226, 2606:2c40::c73c:671e, 2606:2c40::c73c:67e2
+ Target IP: 199.60.103.30
+ Target Hostname: blog.vendasta.com
+ Target Port: 80
+ Start Time: 2024-10-23 01:08:54 (GMT-4)

+ Server: cloudflare
+ /: IP address found in the '__cf_bm' cookie. The IP is "1.0.1.1".
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: An uncommon header 'x-hs-https-only' found, with contents: worker.
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.
sing-content-type-header/
+ Root page / redirects to: https://blog.vendasta.com/
+ /kRvZeBpj.INC: Uncommon header 'cf-chl-out' found, with contents: Fk2mrMJ2FksZ3nUnGW2CT2D2JjDf5wjuV7P3zfisTQ3LztTQuhRPdgJ6iMoScnR2lw5/YI+yvftC9yldVsZI8e50j
cbjjBWQ==.
+ /kRvZeBpj.INC: Uncommon header 'cf-mitigated' found, with contents: challenge.
+ /kRvZeBpj.INC: Uncommon header 'critical-ch' found, with contents: Sec-CH-UA-Bitness, Sec-CH-UA-Arch, Sec-CH-UA-Full-Version, Sec-CH-UA-Mobile, Sec-CH-UA-M
orm, Sec-CH-UA, UA-Bitness, UA-Arch, UA-Full-Version, UA-Mobile, UA-Model, UA-Platform-Version, UA-Platform, UA.
+ /kRvZeBpj.INC: Uncommon header 'accept-ch' found, with contents: Sec-CH-UA-Bitness, Sec-CH-UA-Arch, Sec-CH-UA-Full-Version, Sec-CH-UA-Mobile, Sec-CH-UA-Mod
m, Sec-CH-UA, UA-Bitness, UA-Arch, UA-Full-Version, UA-Mobile, UA-Model, UA-Platform-Version, UA-Platform, UA.
+ /kRvZeBpj.INC: Uncommon header 'cross-origin-embedder-policy' found, with contents: require-corp.
+ /kRvZeBpj.INC: Uncommon header 'origin-agent-cluster' found, with contents: ?1.
+ /kRvZeBpj.INC: Uncommon header 'x-content-options' found, with contents: nosniff.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

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.

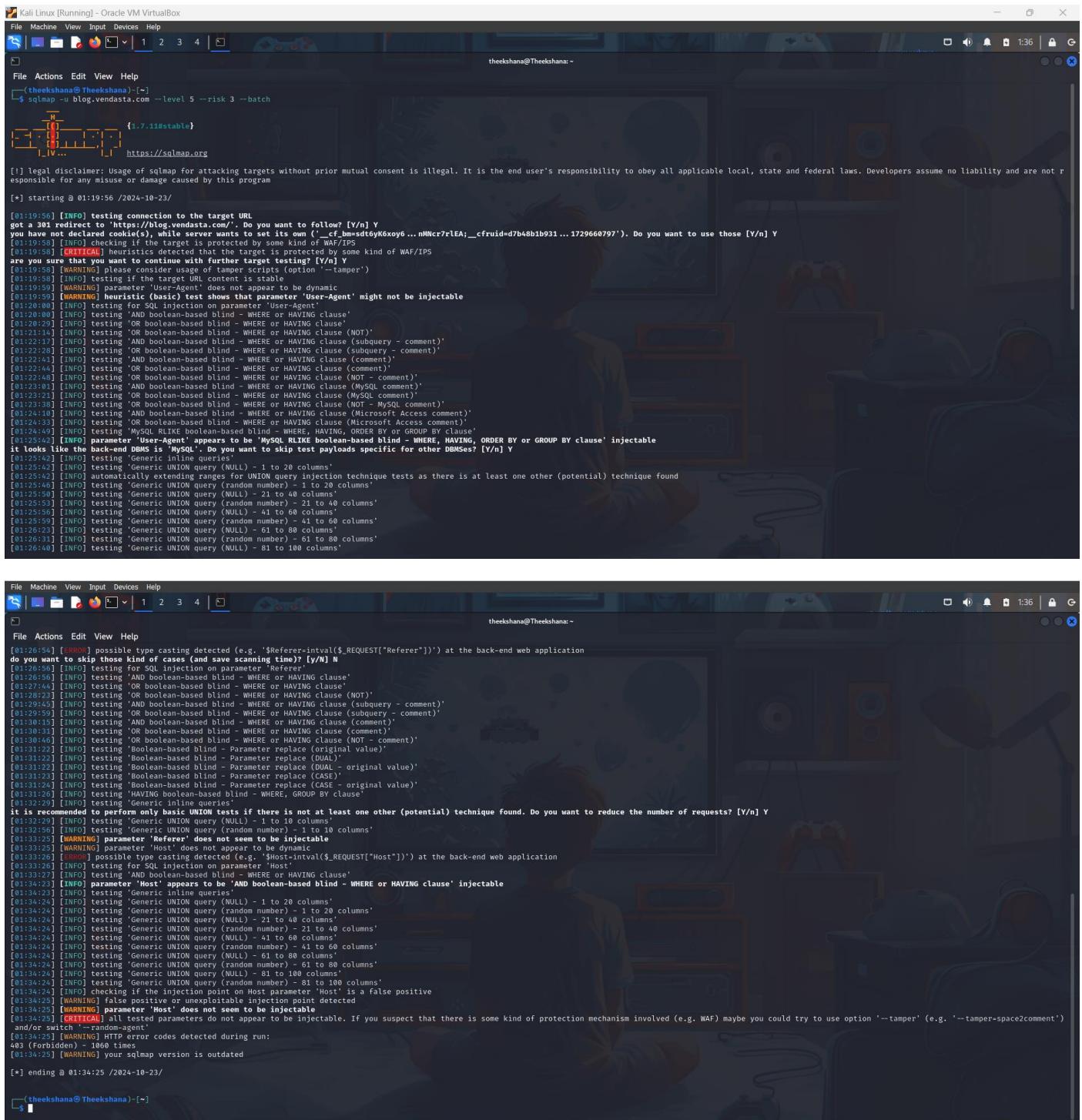
3. Uncommon Headers (Cross-Origin Resource Sharing)

- **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 Scanner



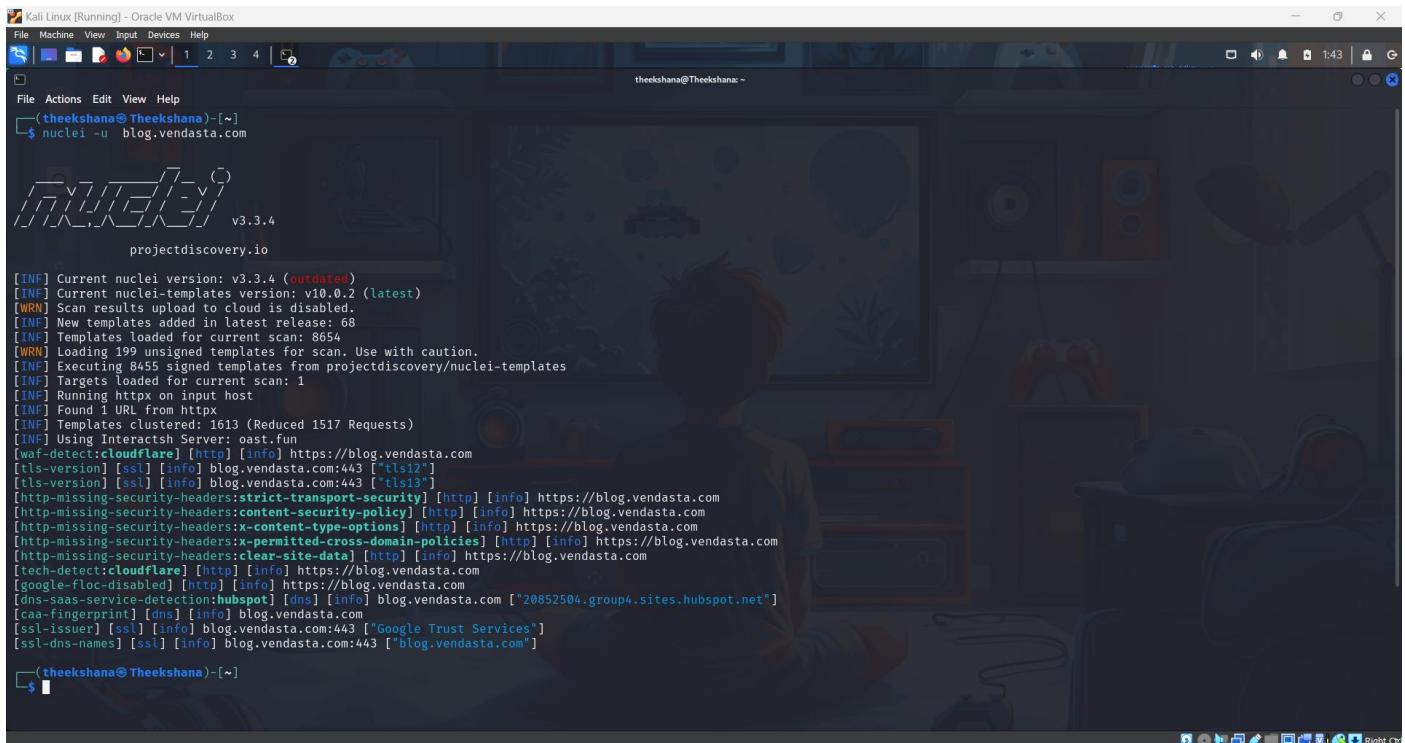
```
[+] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 01:19:56 /2024-10-23/
[01:19:56] [INFO] testing connection to the target URL
got a 301 redirect to 'https://blog.vendasta.com/'. Do you want to follow? [y/n] y
you have declared cookie(s), while server wants to set its own ('_cf_bmedtbyk6xoy6 ... nMNcr7rlEA; __cf_cuid=d7b48b1b931 ... 129660797'). Do you want to use those [y/n] y
[01:19:58] [INFO] checking if the target is protected by some kind of WAF/IPS
are you sure that you want to continue with further target testing? [Y/n] Y
[01:19:58] [WARNING] WAF/IPS detected, consider usage of tamper script (option '--tamper')
[01:19:59] [INFO] testing if the target is protected by a WAF/IPS
[01:19:59] [WARNING] parameter 'User-Agent' does not appear to be dynamic
[01:19:59] [WARNING] heuristic (basic) test shows that parameter 'User-Agent' might not be injectable
[01:20:00] [INFO] testing for SQL injection on parameter 'User-Agent'
[01:20:00] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[01:20:29] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[01:20:55] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (NOT)'
[01:22:17] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[01:22:28] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[01:22:41] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'
[01:22:44] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (comment)'
[01:22:47] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment - subquery)'
[01:22:51] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[01:23:21] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[01:23:38] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
[01:24:18] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'
[01:24:33] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'
[01:25:42] [INFO] parameter 'User-Agent' appears to be 'MySQL LIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause' injectable
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSs? [y/n] Y
[01:25:42] [INFO] testing 'Generic inline queries'
[01:25:42] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[01:25:42] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[01:25:42] [INFO] testing 'Generic UNION query (NULL) - 1 to 30 columns'
[01:25:50] [INFO] testing 'Generic UNION query (NULL) - 21 to 40 columns'
[01:25:53] [INFO] testing 'Generic UNION query (random number) - 21 to 40 columns'
[01:25:56] [INFO] testing 'Generic UNION query (NULL) - 41 to 60 columns'
[01:25:59] [INFO] testing 'Generic UNION query (random number) - 41 to 60 columns'
[01:26:23] [INFO] testing 'Generic UNION query (NULL) - 61 to 80 columns'
[01:26:31] [INFO] testing 'Generic UNION query (random number) - 61 to 80 columns'
[01:26:40] [INFO] testing 'Generic UNION query (NULL) - 81 to 100 columns'
[01:26:54] [ERROR] possible type casting detected (e.g. '$Referer=intval($_REQUEST["Referer"])') at the back-end web application
do you want to skip this kind of casting detection? [y/N] N
[01:26:54] [INFO] testing for SQL injection on parameter 'Referer'
[01:26:56] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[01:27:44] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[01:28:23] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (NOT)'
[01:29:45] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[01:29:58] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[01:30:01] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'
[01:30:31] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (comment)'
[01:30:46] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - comment)'
[01:31:22] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[01:31:22] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL)'
[01:31:22] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[01:31:22] [INFO] testing 'Boolean-based blind - Parameter replace (CASE)'
[01:31:24] [INFO] testing 'Boolean-based blind - Parameter replace (CASE - original value)'
[01:31:26] [INFO] testing 'HAVING boolean-based blind - WHERE, GROUP BY clause'
[01:32:29] [INFO] testing 'Generic inline queries'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [y/n] Y
[01:32:29] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[01:32:29] [INFO] testing 'Generic UNION query (NULL) - 11 to 20 columns'
[01:33:25] [WARNING] parameter 'Referer' does not seem to be injectable
[01:33:25] [WARNING] parameter 'Host' does not appear to be dynamic
[01:33:26] [INFO] possible type casting detected (e.g. '$host=intval($_REQUEST["Host"])') at the back-end web application
[01:33:26] [INFO] testing for SQL injection on parameter 'Host'
[01:33:27] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[01:34:23] [INFO] parameter 'Host' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable
[01:34:23] [INFO] testing 'Generic inline queries'
[01:34:24] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[01:34:24] [INFO] testing 'Generic UNION query (random number) - 1 to 20 columns'
[01:34:24] [INFO] testing 'Generic UNION query (NULL) - 21 to 40 columns'
[01:34:24] [INFO] testing 'Generic UNION query (random number) - 41 to 60 columns'
[01:34:24] [INFO] testing 'Generic UNION query (NULL) - 61 to 80 columns'
[01:34:24] [INFO] testing 'Generic UNION query (random number) - 61 to 80 columns'
[01:34:24] [INFO] testing 'Generic UNION query (random number) - 81 to 100 columns'
[01:34:25] [INFO] checking if the injection point on Host parameter 'Host' is a false positive
[01:34:25] [WARNING] False positive or unexploitable injection point detected
[01:34:25] [WARNING] parameter 'Host' does not seem to be injectable
[01:34:25] [CRITICAL] all tested parameters do not appear to be injectable. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper+space2comment') and/or switch --r=random-agent
[01:34:25] [WARNING] HTTP error codes detected during run:
403 (Forbidden) 100 times
[01:34:25] [WARNING] your sqlmap version is outdated
[*] ending @ 01:34:25 /2024-10-23/
```

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



The screenshot shows a terminal window on Kali Linux. The command run is \$ nuclei -u blog.vendasta.com. The output indicates the current nuclei version is v3.3.4 and the current nuclei-templates version is v10.0.2. It shows various findings across different protocols and ports, including TLS versions (tls12, tls13), Content-Security-Policy (Content-Security-Policy), and Strict-Transport-Security (strict-transport-security). It also detects Cloudflare and HubSpot services.

```
[INFO] Current nuclei version: v3.3.4 (outdated)
[INFO] Current nuclei-templates version: v10.0.2 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 68
[INF] Templates loaded for current scan: 8654
[WRN] Loading 199 unsigned templates for scan. Use with caution.
[INF] Executing 8455 signed templates from projectdiscovery/nuclei-templates
[INF] Targets loaded for current scan: 1
[INF] Running https:// on input host
[INF] Found 1 URL from https
[INF] Templates clustered: 1613 (Reduced 1517 Requests)
[INF] Using Interactsh Server: cast.fun
[waf-detect:cloudflare] [http] [info] https://blog.vendasta.com
[tls-version] [ssl] [info] blog.vendasta.com:443 ['tls12']
[tls-version] [ssl] [info] blog.vendasta.com:443 ['tls13']
[http-missing-security-headers:strict-transport-security] [http] [info] https://blog.vendasta.com
[http-missing-security-headers:content-security-policy] [http] [info] https://blog.vendasta.com
[http-missing-security-headers:x-content-type-options] [http] [info] https://blog.vendasta.com
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] https://blog.vendasta.com
[http-missing-security-headers:clear-site-data] [http] [info] https://blog.vendasta.com
[tech-detect:cloudflare] [http] [info] https://blog.vendasta.com
[google-floc-disabled] [http] [info] https://blog.vendasta.com
[dns-saas-service-detection:hubspot] [dns] [info] blog.vendasta.com ["20852504.group4.sites.hubspot.net"]
[caa-fingerprint] [dns] [info] blog.vendasta.com
[ssl-issuer] [ssl] [info] blog.vendasta.com:443 ["Google Trust Services"]
[ssl-dns-names] [ssl] [info] blog.vendasta.com:443 ["blog.vendasta.com"]

(theekshana@Theekshana)-~]
```

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

```
File Machine View Input Devices Help
(theekshana@Theekshana) ~]
$ dmitry blog.vendasta.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:199.60.103.30
HostName:blog.vendasta.com
Gathered Inet-whois information for 199.60.103.30

inetnum: 199.54.0.0 - 199.66.127.255
netname: NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr: IPv4 address block not managed by the RIPE NCC
remarks:
remarks:
remarks: For registration information,
remarks: you can consult the following sources:
remarks:
IANA
remarks: http://www.iana.org/assignments/ipv4-address-space
remarks: http://www.iana.org/assignments/iana-ipv4-special-registry
remarks: http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
AFRINIC (Africa)
remarks: http://www.afrinic.net/ whois.afrinic.net
remarks:
APNIC (Asia Pacific)
remarks: http://www.apnic.net/ whois.apnic.net
remarks:
ARIN (Northern America)
remarks: http://www.arin.net/ whois.arin.net
remarks:
LACNIC (Latin America and the Caribbean)
remarks: http://www.lacnic.net/ whois.lacnic.net
remarks:
EU # Country is really world wide
admin-c: IANA-RIPE
tech-c: IANA-RIPE
status: ALLOCATED UNSPECIFIED
mnt-by: RIPE-NCC-HM-MNT
created: 2022-04-14T12:57:42Z
last-modified: 2022-04-14T12:57:42Z
source: RIPE

role: Internet Assigned Numbers Authority
address: see http://www.iana.org.
admin-c: IANA-RIPE
tech-c: IANA-RIPE
nic-hdl: IANA-RIPE
```

```
File Machine View Input Devices Help
(theekshana@Theekshana) ~]
$ dmitry blog.vendasta.com
Deepmagic Information Gathering Tool
There be some deep magic going on

File Actions Edit View Help
admin-c: IANA-RIPE
tech-c: IANA-RIPE
nic-hdl: IANA-RIPE
remarks: For more information on IANA services
remarks: Go to IANA web site at http://www.iana.org.
mnt-by: RIPE-NCC-MNT
created: 1970-01-01T00:00:00Z
last-modified: 2001-09-22T09:31:27Z
source: RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.114 (DEXTER)

Gathered Inic-whois information for blog.vendasta.com
ERROR: Unable to locate Name Whois data on blog.vendasta.com
Gathered Netcraft information for blog.vendasta.com

Retrieving Netcraft.com information for blog.vendasta.com
Netcraft.com information gathered

Gathered Subdomain information for blog.vendasta.com
Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 possible subdomain(s) for host blog.vendasta.com, Searched 0 pages containing 0 results

Gathered E-Mail information for blog.vendasta.com
Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 E-mail(s) for host blog.vendasta.com, Searched 0 pages containing 0 results

Gathered TCP Port information for 199.60.103.30



| Port   | State |
|--------|-------|
| 21/tcp | open  |
| 53/tcp | open  |
| 80/tcp | open  |


Ports scan Finished: Scanned 150 ports, 0 ports were in state closed

All scans completed, exiting
(theekshana@Theekshana) ~]
```

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.

<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
IDENTIFIED**5**
CONFIRMED**0**

CRITICAL

0

HIGH

2

MEDIUM

3

LOW

6

BEST PRACTICE

5

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 SummarySEVERITY 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

- See the remedy for solution.
- 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

The screenshot shows the OWASP ZAP interface with an 'Automated Scan' dialog open. The URL to attack is set to `http://blog.vendasta.com`. The 'Attack' button is highlighted in red. The main window shows a list of alerts found during the scan.

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 Post
- 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 Content)
- Information Disclosure - Suspicious Comment
- Unsafe Session Cookies

The screenshot shows the OWASP ZAP interface with an 'Edit Alert' dialog open for a 'Hidden File Found' alert. The alert details are as follows:

Hidden File Found
URL: `http://blog.vendasta.com/._darc`
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-Snailygaster-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_Misconfig...
CWE-538	https://cwe.mitre.org/data/definitions/538.html

The screenshot shows the OWASP ZAP interface with a detailed view of an 'HTTP to HTTPS Insecure Transition in Form Post' alert. The alert details are as follows:

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/`

Header:

```
HTTP/1.1 200 OK
Connection: keep-alive
Content-Length: 649745
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
```

Body:

```
<div class="nav-col-5 nav-end-col nav-end-col-platform mob-none">
</div>
<h3 style="line-height:1.7em;">2023 Agency Insights<br />Report</h3>
<p style="color:#efefef; margin-bottom:10px; font-size:12px;">
  Data-driven insights and analysis to help you navigate the shifting landscape and level-set with
</p>
<a class="highlight" href="https://vendasta.com/content-library/insights/agency-benchmarks-report/">
```

Burp Suite

Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Saha

Tasks

- 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
 - Issues: 0 0 0 0

3. Crawl and audit of blog.vendasta.com

Task configuration

- Task type:** Crawl & audit
- Scope:** blog.vendasta.com
- Configuration:** Crawl and Audit - Fast

Task progress

- Total audit items: 16 Unique locations: 7
- Audit items pending: 0 Pending actions: 0
- Audit items in progress: 16 Current link depth: 0
- Audit items completed: 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 Redirectio
- > Auditing URL param of "https://blog.vendasta.com/_hcms/preview/" for OS Command Injec
- > Auditing URL param of "https://blog.vendasta.com/_hcms/preview/" for HTTP Header Injec

Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Saha

Tasks

- 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
 - Issues: 0 0 0 0

3. Crawl and audit of blog.vendasta.com

Issues

Time	Source	Issue type	Host	Path	Insertion point	Severity
11:40:56 23 Oct 2024	Task 3	Ajax request header manipulation (DOM-based)	https://blog.vendasta...	/hs/preferences-center/		Information
11:40:56 23 Oct 2024	Task 3	Ajax request header manipulation (DOM-based)	https://blog.vendasta...	/_hcms/preview/		Information
11:40:51 23 Oct 2024	Task 3	Content security policy: allows form hijacking	https://blog.vendasta...	/hs/manage-preferences/		Information
11:40:51 23 Oct 2024	Task 3	Content security policy: allows form hijacking	https://blog.vendasta...	/_hcms/perf/v2		Information
11:40:51 23 Oct 2024	Task 3	Content security policy: allows form hijacking	https://blog.vendasta...	/robots.txt		Information
11:40:51 23 Oct 2024	Task 3	Content security policy: allows clickjacking	https://blog.vendasta...	/_hcms/perf/v2		Information
11:40:51 23 Oct 2024	Task 3	Content security policy: allows clickjacking	https://blog.vendasta...	/robots.txt		Information
11:40:51 23 Oct 2024	Task 3	Content security policy: allows untrusted style...	https://blog.vendasta...	/hs/manage-preferences/		Information
11:40:51 23 Oct 2024	Task 3	Content security policy: allows untrusted style...	https://blog.vendasta...	/_hcms/perf/v2		Information
11:40:51 23 Oct 2024	Task 3	Content security policy: allows untrusted script...	https://blog.vendasta...	/robots.txt		Information
11:40:51 23 Oct 2024	Task 3	Cross-domain script include	https://blog.vendasta...	/hs/preferences-center/		Information

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.

Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Saha

Tasks

- 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
 - Issues: 0 0 0 0

3. Crawl and audit of blog.vendasta.com

Issues

Time	Source	Issue type	Host	Path	Insertion point	Severity
11:40:56 23 Oct 2024	Task 3	Ajax request header manipulation (DOM-based)	https://blog.vendasta...	/hs/preferences-center/		Information
11:40:56 23 Oct 2024	Task 3	Ajax request header manipulation (DOM-based)	https://blog.vendasta...	/_hcms/preview/		Information
11:40:51 23 Oct 2024	Task 3	Content security policy: allows form hijacking	https://blog.vendasta...	/hs/manage-preferences/		Information
11:40:51 23 Oct 2024	Task 3	Content security policy: allows clickjacking	https://blog.vendasta...	/_hcms/perf/v2		Information
11:40:51 23 Oct 2024	Task 3	Content security policy: allows clickjacking	https://blog.vendasta...	/robots.txt		Information
11:40:51 23 Oct 2024	Task 3	Content security policy: allows clickjacking	https://blog.vendasta...	/_hcms/perf/v2		Information
11:40:51 23 Oct 2024	Task 3	Content security policy: allows clickjacking	https://blog.vendasta...	/robots.txt		Information
11:40:51 23 Oct 2024	Task 3	Content security policy: allows untrusted style...	https://blog.vendasta...	/hs/manage-preferences/		Information
11:40:51 23 Oct 2024	Task 3	Content security policy: allows untrusted style...	https://blog.vendasta...	/_hcms/perf/v2		Information
11:40:51 23 Oct 2024	Task 3	Content security policy: allows untrusted script...	https://blog.vendasta...	/robots.txt		Information
11:40:51 23 Oct 2024	Task 3	Cross-domain script include	https://blog.vendasta...	/hs/preferences-center/		Information

Request

Pretty Raw Hex Render

```
1. 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/"73aa9f7ead5f2153de51db4e1d7e788"
Last-Modified: Wed, 16 Oct 2024 15:20:57 GMT
Strict-Transport-Security: max-age=31536000
Cache-Tag: P-2082504,SS-5735B,01368,P08-ADD,394-0
Content-Security-Policy: upgrade-insecure-Requests
```

Inspector

Response headers

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. <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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: <code>curl https://blog.vendasta.com/.env</code>
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 screenshot shows a bug bounty report page for Truist Financial. On the left, there's a sidebar with various icons and a navigation menu. The main content area includes sections for 'Program highlights', 'Scope exclusions', and 'Overview'. The 'Program highlights' section features four cards: 'Top Response Efficiency' (above 90%), 'Managed by HackerOne', and two time-related metrics ('17 hours' and '1 week, 7 hours'). The 'Scope exclusions' section notes that core ineligible findings are out of scope. The 'Overview' section last updated on October 14, 2023, states that Truist is committed to maintaining the security of its systems and customers' information.

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

The screenshot shows the Truist Developer Center homepage. It features a dark purple header with the Truist logo, a search bar, and a 'Sign in' button. Below the header, a large banner reads 'TRUIST DEVELOPER CENTER' and 'Developers are redefining the future of banking.' with a 'Register' button. A subtext below the banner says 'By transforming how our clients use our services, we can accelerate growth.'

Truist APIs

Tap into the power of the Truist network with our APIs.

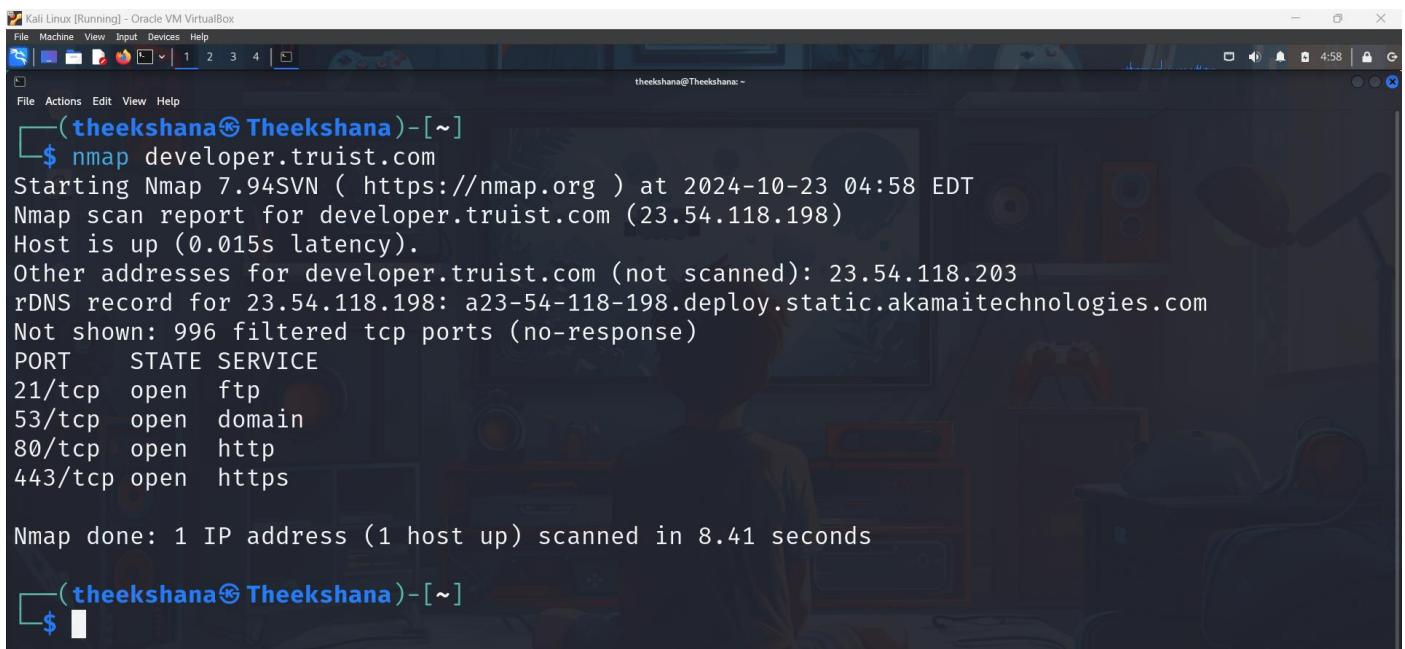
Commercial - Association Services >

Personal and small business >

Accounts and transactions >

Target Reconnaissance

Nmap Scan



```
(theekshana㉿Theekshana) [~]
$ nmap developer.truist.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-23 04:58 EDT
Nmap scan report for developer.truist.com (23.54.118.198)
Host is up (0.015s latency).
Other addresses for developer.truist.com (not scanned): 23.54.118.203
rDNS record for 23.54.118.198: a23-54-118-198.deploy.static.akamaitechnologies.com
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

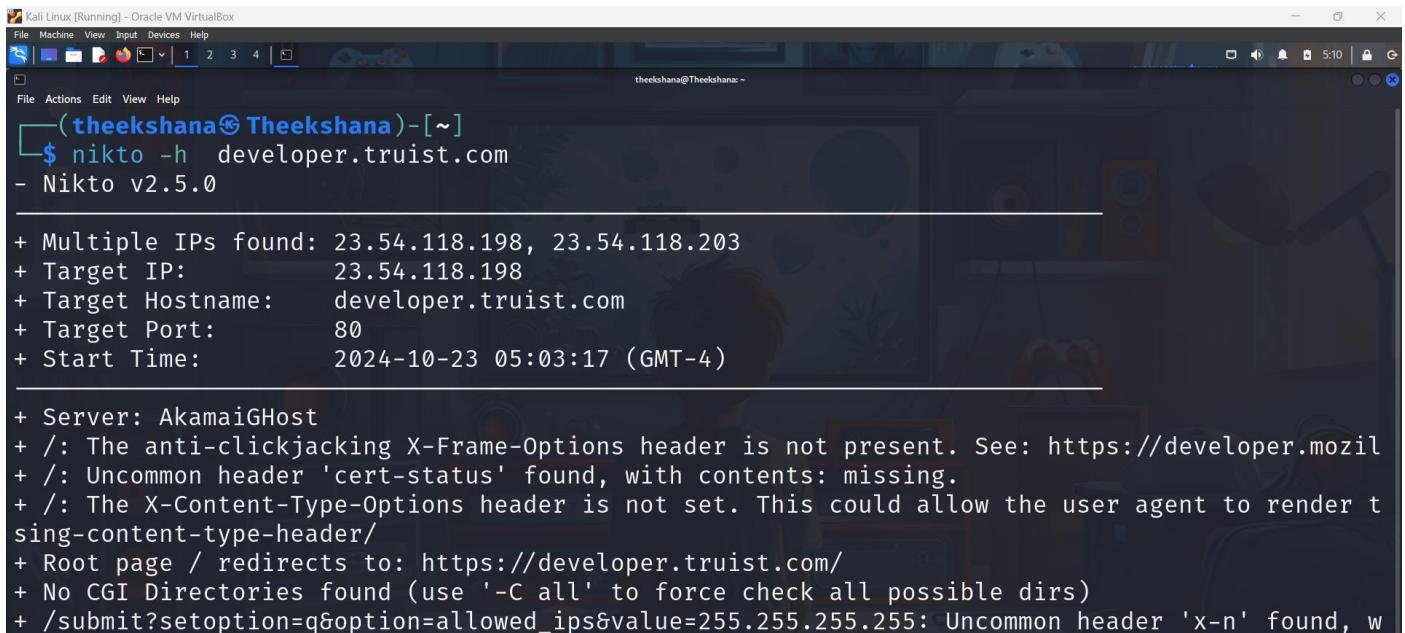
Nmap done: 1 IP address (1 host up) scanned in 8.41 seconds
```

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	HTTPS
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



```
(theekshana㉿Theekshana) [~]
$ nikto -h developer.truist.com
- Nikto v2.5.0

+ Multiple IPs found: 23.54.118.198, 23.54.118.203
+ Target IP: 23.54.118.198
+ Target Hostname: developer.truist.com
+ Target Port: 80
+ Start Time: 2024-10-23 05:03:17 (GMT-4)

+ Server: AkamaiGHost
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'cert-status' found, with contents: missing.
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render files as the wrong MIME type.
+ Root page / redirects to: https://developer.truist.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /submit?setoption=q&option=allowed_ips&value=255.255.255.255: Uncommon header 'x-n' found, with contents: missing.
```

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)

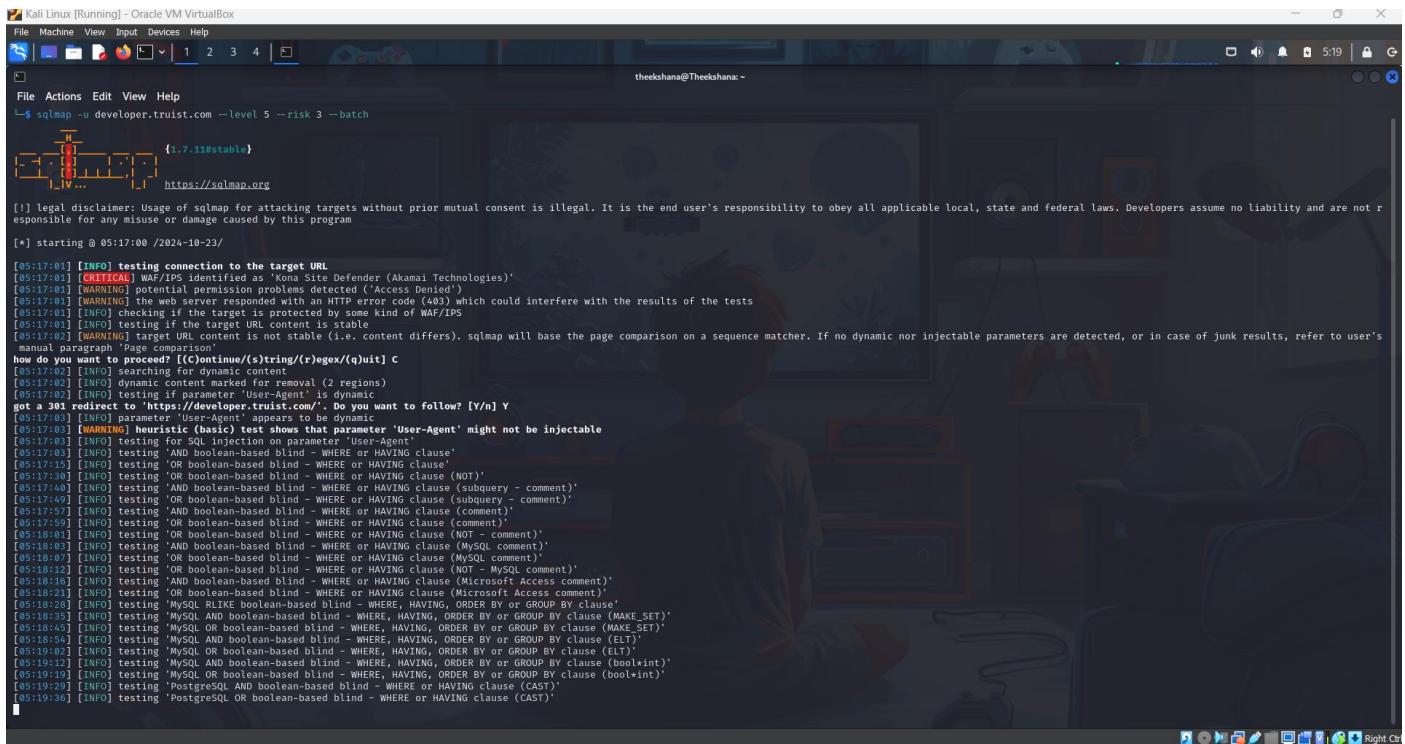
Security Headers:\

- **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:

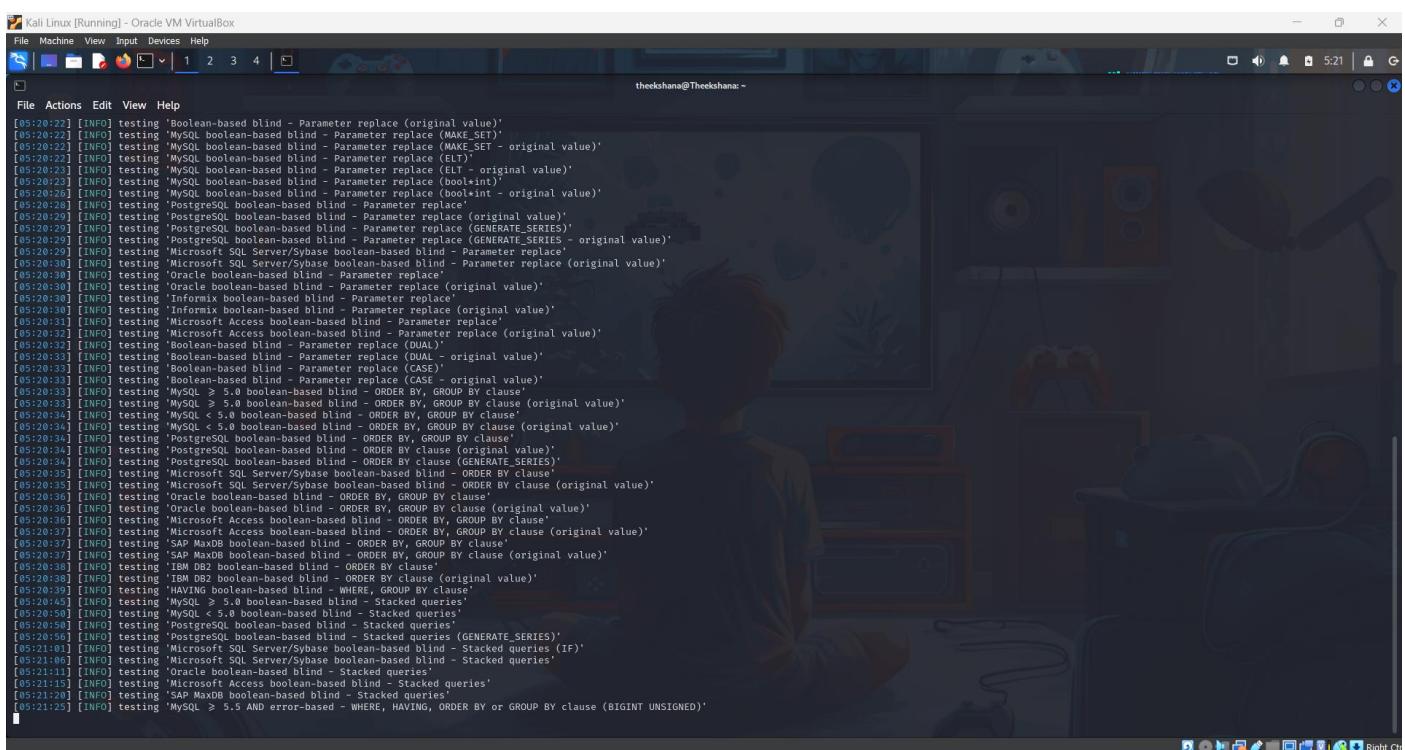
- The root page redirects to <https://developer.truist.com/>, indicating the website automatically redirects from HTTP to HTTPS.

SQLmap Scanner



```
[*] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 05:17:00 / 2024-10-23

[05:17:01] [INFO] testing connection to the target URL
[05:17:01] [CRITICAL] WAF/IPS identified as 'Kona Site Defender (Akamai Technologies)'
[05:17:01] [WARNING] potential permission problems detected ('Access Denied')
[05:17:01] [WARNING] the web server responded with an HTTP error code (403) which could interfere with the results of the tests
[05:17:01] [INFO] tracking if the target is protected by some kind of WAF/IPS
[05:17:01] [INFO] testing if the target URL content is stable
[05:17:01] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case of junk results, refer to user's manual paragraph "Page comparison"
how do you want to proceed? [(C)ontinue/(S)tring/(R)eject/(Q)uit] c
[05:17:02] [INFO] searching for dynamic content
[05:17:03] [INFO] dynamic content marked for removal (2 regions)
[05:17:03] [INFO] testing if parameter 'User-Agent' is dynamic
got a 301 redirect to 'https://developer.trust.com/'. Do you want to follow? [Y/n] Y
[05:17:03] [INFO] parameter 'User-Agent' appears to be dynamic
[05:17:03] [WARNING] heuristic (basic) test shows that parameter 'User-Agent' might not be injectable
[05:17:03] [INFO] testing for SQL injection on parameter 'User-Agent'
[05:17:03] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[05:17:03] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[05:17:03] [INFO] testing 'NOT boolean-based blind - WHERE or HAVING clause (NOT)'
[05:17:04] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[05:17:04] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[05:17:05] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'
[05:17:05] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (comment)'
[05:17:06] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[05:17:06] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[05:17:07] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
[05:17:08] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'
[05:17:09] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'
[05:17:09] [INFO] testing 'NOT LIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'
[05:17:09] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[05:17:09] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[05:17:09] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
[05:17:09] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
[05:17:09] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (bool+int)'
[05:17:09] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (bool+int)'
[05:17:09] [INFO] testing 'PostgreSQL AND boolean-based blind - WHERE or HAVING clause (CAST)'
[05:17:09] [INFO] testing 'PostgreSQL OR boolean-based blind - WHERE or HAVING clause (CAST)'
[05:17:09] [INFO] testing 'PostgreSQL AND boolean-based blind - WHERE or HAVING clause (CAST)'
```

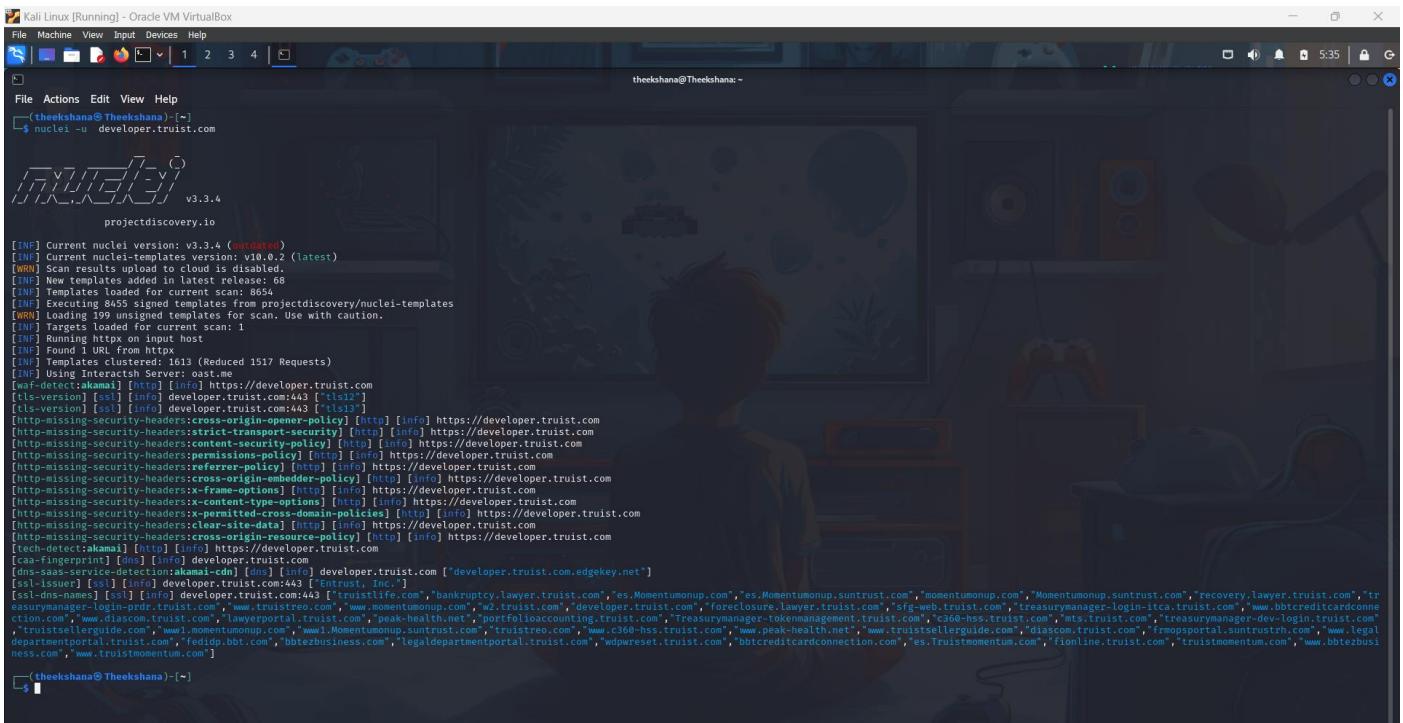


```
[05:20:22] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[05:20:22] [INFO] testing 'MySQL boolean-based blind - Parameter replace (MAKE_SET)'
[05:20:22] [INFO] testing 'MySQL boolean-based blind - Parameter replace (MAKE_SET - original value)'
[05:20:22] [INFO] testing 'MySQL boolean-based blind - Parameter replace (ELT)'
[05:20:23] [INFO] testing 'MySQL boolean-based blind - Parameter replace (ELT - original value)'
[05:20:23] [INFO] testing 'MySQL boolean-based blind - Parameter replace (bool+int)'
[05:20:23] [INFO] testing 'MySQL boolean-based blind - Parameter replace (bool+int - original value)'
[05:20:24] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace'
[05:20:24] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace (original value)'
[05:20:24] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace (GENERATE_SERIES)'
[05:20:24] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace (GENERATE_SERIES - original value)'
[05:20:24] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Parameter replace'
[05:20:24] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Parameter replace (original value)'
[05:20:24] [INFO] testing 'Oracle boolean-based blind - Parameter replace'
[05:20:24] [INFO] testing 'Oracle boolean-based blind - Parameter replace (original value)'
[05:20:24] [INFO] testing 'Informix boolean-based blind - Parameter replace'
[05:20:24] [INFO] testing 'Informix boolean-based blind - Parameter replace (original value)'
[05:20:31] [INFO] testing 'Microsoft Access boolean-based blind - Parameter replace'
[05:20:31] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[05:20:32] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL)'
[05:20:32] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL - original value)'
[05:20:33] [INFO] testing 'Boolean-based blind - Parameter replace (CASE)'
[05:20:33] [INFO] testing 'Boolean-based blind - Parameter replace (CASE - original value)'
[05:20:33] [INFO] testing 'MySQL > 5.5 boolean-based blind - ORDER BY, GROUP BY clause'
[05:20:33] [INFO] testing 'MySQL < 5.5 boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[05:20:34] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause'
[05:20:34] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[05:20:34] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY, GROUP BY clause'
[05:20:34] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[05:20:34] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY, GROUP BY clause (GENERATE_SERIES)'
[05:20:34] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY, GROUP BY clause (GENERATE_SERIES)'
[05:20:35] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - ORDER BY clause'
[05:20:35] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - ORDER BY clause (original value)'
[05:20:36] [INFO] testing 'Oracle boolean-based blind - ORDER BY, GROUP BY clause'
[05:20:36] [INFO] testing 'Oracle boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[05:20:36] [INFO] testing 'Microsoft Access boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[05:20:36] [INFO] testing 'Microsoft Access boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[05:20:37] [INFO] testing 'SAP MaxDB boolean-based blind - ORDER BY, GROUP BY clause'
[05:20:37] [INFO] testing 'SAP MaxDB boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[05:20:38] [INFO] testing 'IBM DB2 boolean-based blind - ORDER BY clause'
[05:20:38] [INFO] testing 'IBM DB2 boolean-based blind - ORDER BY clause (original value)'
[05:20:39] [INFO] testing 'HAVING boolean-based blind - WHERE, GROUP BY clause'
[05:20:39] [INFO] testing 'MySQL < 5.5 boolean-based blind - Stacked queries'
[05:20:40] [INFO] testing 'MySQL < 5.0 boolean-based blind - Stacked queries'
[05:20:40] [INFO] testing 'PostgreSQL boolean-based blind - Stacked queries'
[05:21:01] [INFO] testing 'PostgreSQL boolean-based blind - Stacked queries (GENERATE_SERIES)'
[05:21:01] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Stacked queries (IF)'
[05:21:01] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Stacked queries'
[05:21:13] [INFO] testing 'Oracle boolean-based blind - Stacked queries'
[05:21:13] [INFO] testing 'Microsoft Access boolean-based blind - Stacked queries'
[05:21:13] [INFO] testing 'SAP MaxDB boolean-based blind - Stacked queries'
[05:21:20] [INFO] testing 'MySQL > 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
```

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



```
[Kali Linux [Running] - Oracle VM VirtualBox]
File Machine View Input Devices Help
[theekshana@Theekshana: ~]
$ nuclei -u developer.trust.com
projectdiscovery.io
v3.3.4

[INF] Current nuclei version: v3.3.4 (unstable)
[INF] Current nuclei-templates version: v10.0.2 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 68
[INF] Total templates available for this version: 1555
[INF] Executing 8455 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 199 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Running httpx on input host
[INF] Found 1 target(s) for this scan
[INF] Templates Clustered: 1613 (Reduced 1517 Requests)
[INF] Using Intercept Server: ost:me
[waf-detect:akamai] [http] [info] https://developer.trust.com
[tsl-version] [ssl] [info] developer.trust.com:443 [tlsv12]
[http-missing-security-headers:cross-origin-open-policy] [http] [info] https://developer.trust.com
[http-missing-security-headers:strict-transports-security] [http] [info] https://developer.trust.com
[http-missing-security-headers:content-security-policy] [http] [info] https://developer.trust.com
[http-missing-security-headers:permissions-policy] [http] [info] https://developer.trust.com
[http-missing-security-headers:referrer-policy] [http] [info] https://developer.trust.com
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] https://developer.trust.com
[http-missing-security-headers:frame-options] [http] [info] https://developer.trust.com
[http-missing-security-headers:x-content-type-options] [http] [info] https://developer.trust.com
[http-missing-security-headers:permitted-cross-domain-policies] [http] [info] https://developer.trust.com
[http-missing-security-headers:clear-site-data] [http] [info] https://developer.trust.com
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] https://developer.trust.com
[tech-detect:akamai] [http] [info] https://developer.trust.com
[dns-dnssec-service-detection:akamai-cdn] [dns] [info] developer.trust.com ['developer.trust.com.edgekey.net']
[ssl-issuer] [ssl] [info] developer.trust.com:443 ['Entrust, Inc.']
[ssl-dns-names] [ssl] [info] developer.trust.com:443 ['trustlife.com', 'bankruptcy.lawyer.trust.com', 'es.Momentumup.suntrust.com', 'momentumup.com', 'momentumup.suntrust.com', 'recovery.lawyer.trust.com', 'treasurymanager-login-prd.trust.com', 'www.trusttree.com', 'www.momentumup.com', 'w2.trust.com', 'developer.trust.com', 'foreclosure.lawyer.trust.com', 'sfg-web.trust.com', 'treasurymanager-login-itca.trust.com', 'www.bbctruecarddcne.com', 'www.diagram.trust.com', 'lawportal.trust.com', 'peak-health.net', 'portfolioaccounting.trust.com', 'Treasurymanager-tokenmanagement.trust.com', 'mts.trust.com', 'treasurymanager-dev-login.trust.com', 'www.legaldepartmentportal.trust.com', 'fedidp.bbt.com', 'bbtebzbusiness.com', 'legaldepartmentportal.trust.com', 'wdpreset.trust.com', 'bbtcreditcardconnection.com', 'es.Trustmomentum.com', 'ionline.trust.com', 'trustmomentum.com', 'www.bbtebusi ness.com', 'www.trustmomentum.com']

[theekshana@Theekshana: ~]
```

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

The image shows a Kali Linux desktop environment with two terminal windows open. The top terminal window is titled 'File Machine View Input Devices Help' and displays the output of the 'dmitry developer.truist.com' command. It provides deep magic information gathering for the host IP 23.54.118.198, including Inet-whois information for the range 23.19.64.0 - 23.83.63.255, which is a non-RIPE-NCC-managed address block. It also lists various RIRs (IANA, APNIC, ARIN, LACNIC) and their respective WHOIS servers. The bottom terminal window is titled 'File Machine View Input Devices Help' and displays the output of 'dmitry developer.truist.com'. It includes sections for IANA WHOIS, Netcraft information, Subdomain information, E-Mail information, and TCP Port information. The port scan results show ports 21/tcp, 53/tcp, and 80/tcp as open. The entire interface is set against a dark background with a video game-themed wallpaper.

```
[theekshana@Theekshana: ~]
$ dmitry developer.truist.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:23.54.118.198
HostName:developer.truist.com

Gathered Inet-whois information for 23.54.118.198

inetnum: 23.19.64.0 - 23.83.63.255
netname: NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr: IPv4 address block not managed by the RIPE NCC
remarks:
remarks:
remarks:
remarks: For registration information,
remarks: you can consult the following sources:
remarks: IANA
remarks: http://www.iana.org/assignments/ipv4-address-space
remarks: http://www.iana.org/assignments/iana-ipv4-special-registry
remarks: http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks: AFRINIC (Africa)
remarks: http://www.afrinic.net/ whois.afrinic.net
remarks: APNIC (Asia Pacific)
remarks: http://www.apnic.net/ whois.apnic.net
remarks: ARIN (Northern America)
remarks: http://www.arin.net/ whois.arin.net
remarks: LACNIC (Latin America and the Caribbean)
remarks: http://www.lacnic.net/ whois.lacnic.net
remarks:
remarks: EU # Country is really world wide
country: IANA-RIPE
admin-c: IANA-RIPE
tech-c: IANA-RIPE
sys-c: ALLOCATED-UNSPECIFIED
mnt-by: RIPE-NCC-HM-MNT
created: 2019-01-07T10:48:01Z
last-modified: 2019-01-07T10:48:01Z
source: RIPE

role: Internet Assigned Numbers Authority
address: see http://www.iana.org/
admin-c: IANA-RIPE
tech-c: IANA-RIPE
nic-hdl: IANA-RIPE
remarks: For more information on IANA services

% This query was served by the RIPE Database Query Service version 1.114 (DEXTER)

Gathered Iinc-whois information for developer.truist.com
ERROR: Unable to locate Name Whois data on developer.truist.com

Gathered Netcraft information for developer.truist.com

Retrieving Netcraft.com information for developer.truist.com
Netcraft.com Information gathered

Gathered Subdomain information for developer.truist.com
Searching Google.com:80...
Searching Altavista.com:80...
Found 0 possible subdomain(s) for host developer.truist.com, Searched 0 pages containing 0 results

Gathered E-Mail information for developer.truist.com
Searching Google.com:80...
Searching Altavista.com:80...
Found 0 E-Mail(s) for host developer.truist.com, Searched 0 pages containing 0 results

Gathered TCP Port information for 23.54.118.198

Port      State
21/tcp    open
53/tcp    open
80/tcp    open

Portscan Finished: Scanned 150 ports, 0 ports were in state closed

All scans completed, exiting
[theekshana@Theekshana: ~]
```

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.

<http://developer.trusit.com/>

Scan Time

: 10/23/2024 3:12:32 PM (UTC+05:30)

Total Requests: 435
Average Speed: 6.07/sRisk Level:
MEDIUM

VULNERABILITIES

9
IDENTIFIED2
CONFIRMED0 !
CRITICAL0 !
HIGH3 !
MEDIUM
4 ?
BEST PRACTICE1 !
LOW
1 i
INFORMATION**Identified Vulnerabilities**

Critical	0
High	0
Medium	3
Low	1
Best Practice	4
Information	1
TOTAL	9

Confirmed Vulnerabilities

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

Vulnerability SummarySEVERITY 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 ! | 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.

Vulnerabilities2.1. <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

The screenshot shows the OWASP ZAP interface with an "Automated Scan" dialog open. The URL to attack is set to <http://developer.trust.com>. The "Attack" button is highlighted. The progress bar indicates "Using ajax spider to discover the content". On the left, the "Alerts" panel shows 15 alerts, including Content Security Policy (CSP) Header Not Set, Cross-Domain Misconfiguration, Missing Anti-clickjacking Header, and Cookie No HttpOnly Flag.

This screenshot shows a detailed view of an alert for "CSP: script-src unsafe-eval". The alert details include:

- URL: <http://go.transunion.com>
- Risk: Medium
- Confidence: High
- Parameter: content-security-policy
- Attack: Evidence: `im.com dpm.demdex.net api.company-target.com t.teads.tv transunion.tt.omrtdc.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.

The "Solution" section suggests ensuring the Content-Security-Policy header is properly configured. The "Reference" section links to <https://www.w3.org/TR/CSP/> and <https://caniuse.com/#search=content+security+policy>.

This screenshot shows another detailed view of an alert for "CSP: script-src unsafe-eval". The alert details are identical to the previous one. The "Header" tab shows the following headers:

```
x-frame-options: DENY  
x-xss-protection: 1; mode=block  
x-content-type-options: HIT  
x-powered-by: Next.js  
Cache-Control: s-maxage=31536000, stale-while-revalidate  
ETag: "smigyfse2599n"  
Vary: Accept-Encoding  
X-Cache: Hit from cloudfront
```

The "Body" tab displays a large block of JavaScript code, likely a preloading snippet for Adobe Target, which is part of the alert's payload.

The "Solution" section again advises setting the Content-Security-Policy header. The "Reference" section provides links to the W3C CSP specification and a CanIUse compatibility table.

The "Alert Tags" table lists the following:

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_A05	https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html

Burp Suite

Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Saha

Tasks

- 3. Crawl and audit of developer.trust.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
 - Issues: 0 0 0 0

3. Crawl and audit of developer.trust.com

Most serious vulnerabilities found (live)

Issue type	Host	Time
Strict transport security not enforced	https://developer.trust...	09:44:38 24 Oct 20...
Source code disclosure	https://developer.trust...	09:44:38 24 Oct 20...
Cacheable HTTPS response	https://developer.trust...	09:44:37 24 Oct 20...
Cacheable HTTPS response	https://developer.trust...	09:44:37 24 Oct 20...
Cookie scoped to parent domain	https://developer.trust...	09:44:40 24 Oct 20...
Cookie scoped to parent domain	https://developer.trust...	09:44:40 24 Oct 20...
Cookie without HttpOnly flag set	https://developer.trust...	09:44:40 24 Oct 20...
Cookie without HttpOnly flag set	https://developer.trust...	09:44:39 24 Oct 20...
Cross-origin resource sharing	https://developer.trust...	09:46:33 24 Oct 20...
Cross-origin resource sharing	https://developer.trust...	09:46:48 24 Oct 20...
Cross-origin resource sharing	https://developer.trust...	09:45:44 24 Oct 20...
Cross-origin resource sharing	https://developer.trust...	09:46:30 24 Oct 20...
Cross-origin resource sharing	https://developer.trust...	09:45:26 24 Oct 20...
Cross-origin resource sharing; arbitrary origin	https://developer.trust...	09:45:44 24 Oct 20...
Cross-origin resource sharing; arbitrary origin	https://developer.trust...	09:46:48 24 Oct 20...
Cross-origin resource sharing; arbitrary origin	https://developer.trust...	09:46:33 24 Oct 20...
Cross-origin resource sharing; arbitrary origin	https://developer.trust...	09:46:30 24 Oct 20...
Email addresses disclosed	https://developer.trust...	09:44:39 24 Oct 20...
Email addresses disclosed	https://developer.trust...	09:44:39 24 Oct 20...
Input returned in response (reflected)	https://developer.trust...	09:46:48 24 Oct 20...
Private IP addresses disclosed	https://developer.trust...	09:44:38 24 Oct 20...
Ref ID cookie	https://developer.trust.../api/v1/...	09:44:40 24 Oct 20...

Task configuration

Task type: Crawl & audit
Scope: developer.trust.com
Configuration: Crawl and Audit - Fast

Task progress

Total audit items: 24 Unique locations: 49
Audit items pending: 0 Pending actions: 0
Audit items in progress: 24 Current link depth: 0
Audit items completed: 0 Requests: 3187
Network errors: 5

Task log

- > Auditing cookie of "https://developer.trust.com/categories/commercial-association-services" for XSS and Template injection
- > Auditing "https://developer.trust.com/styles/48e0cce36cb68c74.css" for Web Cache Poisoning
- > Auditing "https://developer.trust.com/runtime.76e97e1696eb4b2e.js" for Backup Files & refix Filename
- > Auditing "https://developer.trust.com/runtime.76e97e1696eb4b2e.js" for Backup Files & replace Extension
- > Auditing "https://developer.trust.com/runtime.76e97e1696eb4b2e.js" for Backup Files & append Extension

Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Saha

Tasks

- 3. Crawl and audit of developer.trust.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
 - Issues: 0 0 0 0

3. Crawl and audit of developer.trust.com

Issues

Time	Source	Issue type	Host	Path	Insertion point	Severity
09:46:48 24 Oct 2024	Task 3	Input returned in response (reflected)	https://developer.trust.../categories/commercial-association-services		dtCookie cookie	Information
09:46:48 24 Oct 2024	Task 3	Cross-origin resource sharing	https://developer.trust.../_main.e02792e0b89f614.js			Information
09:46:48 24 Oct 2024	Task 3	Cross-origin resource sharing; arbitrary origin	https://developer.trust.../_main.e02792e0b89f614.js			Information
09:46:33 24 Oct 2024	Task 3	Cross-origin resource sharing	https://developer.trust.../_styles/48e0cce36cb68c74.css			Information
09:46:33 24 Oct 2024	Task 3	Cross-origin resource sharing; arbitrary origin	https://developer.trust.../_styles/48e0cce36cb68c74.css			Information
09:46:30 24 Oct 2024	Task 3	Cross-origin resource sharing	https://developer.trust.../_runtime.76e97e1696eb4b2e.js			Information
09:46:30 24 Oct 2024	Task 3	Cross-origin resource sharing; arbitrary origin	https://developer.trust.../_runtime.76e97e1696eb4b2e.js			Information
09:45:44 24 Oct 2024	Task 3	Cross-origin resource sharing	https://developer.trust.../_			Information
09:45:44 24 Oct 2024	Task 3	Cross-origin resource sharing; arbitrary origin	https://developer.trust.../_			Information
09:45:26 24 Oct 2024	Task 3	Cross-origin resource sharing	https://developer.trust.../_robots.txt			Information
09:45:26 24 Oct 2024	Task 3	Cross-origin resource sharing; arbitrary origin	https://developer.trust.../_robots.txt			Information
09:44:40 24 Oct 2024	Task 3	Framable resource (potential Clickjacking)	https://developer.trust.../_signup			Information
09:44:40 24 Oct 2024	Task 3	Cookie scoped to parent domain	https://developer.trust.../_			Information

Advisory Request Response Path to issue

Cross-origin resource sharing

Severity: Information Confidence: Certain URL: https://developer.trust.com/main.e02792e0b89f614.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 Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Saha

Tasks

- 3. Crawl and audit of developer.trust.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
 - Issues: 0 0 0 0

3. Crawl and audit of developer.trust.com

Issues

Time	Source	Issue type	Host	Path	Insertion point	Severity
09:46:48 24 Oct 2024	Task 3	Input returned in response (reflected)	https://developer.trust.../categories/commercial-association-services		dtCookie cookie	Information
09:46:48 24 Oct 2024	Task 3	Cross-origin resource sharing	https://developer.trust.../_main.e02792e0b89f614.js			Information
09:46:48 24 Oct 2024	Task 3	Cross-origin resource sharing; arbitrary origin	https://developer.trust.../_main.e02792e0b89f614.js			Information
09:46:33 24 Oct 2024	Task 3	Cross-origin resource sharing	https://developer.trust.../_styles/48e0cce36cb68c74.css			Information
09:46:33 24 Oct 2024	Task 3	Cross-origin resource sharing; arbitrary origin	https://developer.trust.../_styles/48e0cce36cb68c74.css			Information
09:46:30 24 Oct 2024	Task 3	Cross-origin resource sharing	https://developer.trust.../_runtime.76e97e1696eb4b2e.js			Information
09:46:30 24 Oct 2024	Task 3	Cross-origin resource sharing; arbitrary origin	https://developer.trust.../_runtime.76e97e1696eb4b2e.js			Information
09:45:44 24 Oct 2024	Task 3	Cross-origin resource sharing	https://developer.trust.../_			Information
09:45:44 24 Oct 2024	Task 3	Cross-origin resource sharing; arbitrary origin	https://developer.trust.../_			Information
09:45:26 24 Oct 2024	Task 3	Cross-origin resource sharing	https://developer.trust.../_robots.txt			Information
09:45:26 24 Oct 2024	Task 3	Cross-origin resource sharing; arbitrary origin	https://developer.trust.../_robots.txt			Information
09:44:40 24 Oct 2024	Task 3	Framable resource (potential Clickjacking)	https://developer.trust.../_signup			Information
09:44:40 24 Oct 2024	Task 3	Cookie scoped to parent domain	https://developer.trust.../_			Information

Advisory Request Response Path to issue

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Accept-Ranges: bytes
3 Content-Type: application/javascript
4 ETag: "66e4ed-427f2"
5 Last-Modified: Sat, 14 Sep 2024 01:28:50 GMT
6 P3P: CP="NON COM CONN NOV NOPI"
7 Access-Control-Allow-Origin: *
8 Access-Control-Allow-Credentials: false

```

Inspector

Response headers

Vulnerabilities:

1 Cross-Origin Resource Sharing:

Vulnerability Title	Cross-Origin Resource Sharing: Arbitrary Origin Trusted
Vulnerability Description	<p>The application implements an HTML5 cross-origin resource sharing (CORS) policy that allows access from any domain, effectively disabling the same-origin policy.</p> <p>This can lead to security risks, especially if sensitive data or privileged actions are involved.</p>
Affected Components	<p>CORS configuration for the web application.</p> <p>API endpoints and web pages that rely on CORS for cross-domain requests.</p> <p>Any components that handle sensitive data or user credentials.</p>
Impact Assessment	<p>Allows unauthorized cross-origin access to sensitive data or functionalities. Potential exposure of user sessions or sensitive information to malicious websites</p> <p>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.</p>
Steps to Reproduce	<p>Access the application at developer.truist.com</p> <p>Use browser developer tools to monitor network requests.</p> <p>Make a cross-origin request from a malicious site to see if it successfully retrieves data or performs actions that should be restricted.</p> <p>Check the Access-Control-Allow-Origin header in the response to confirm it allows arbitrary origins.</p>
Proof of Concept	<p>developer.truist.com in an unsecured network.</p> <p>Use network analysis tools (e.g., Wireshark) to observe traffic and confirm it's unencrypted.</p>
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

- h1
- Security page
- Program guidelines
- Scope
- Hacktivity
- Thanks
- Updates
- File
- ?
- !
- User

Program highlights

Platform Standards	Fully compliant with Platform Standards.
⚡ Top Response Efficiency	This program's response efficiency is above 90%.
Managed by HackerOne	

1 day, 7 hours	Average time to first response
1 day, 7 hours	Average time to triage
N/A	Average time to bounty
2 weeks, 4 days	Average time to resolution

Scope exclusions

Core Ineligible Findings are out of scope and won't be rewarded. [Learn more](#)

Overview

Last updated on August 8, 2024. [View changes](#)

APNIC (Asia Pacific Network Information Centre) is an open, membership-based, not-for-profit organization providing Internet addressing services to the Asia Pacific region.

APNIC

<http://apnic.net>
[@apnic](#)

APNIC is the regional Internet address registry for the Asia-Pacific region.

Vulnerability Disclosure Program launched in Mar 2023

- Response efficiency: 94%

[Submit report](#)

Stats

Reports received 90 days	17
Last report resolved	3 months ago
Reports resolved	68
Hackers thanked	52
Assets In Scope	18

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](https://www.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

LOG IN

WHOIS & WEBSITE [SEARCH](#) ADVANCED WHOIS MAKE A PAYMENT Your IP address: 43.250.242.124

APNIC

Get IP [▼](#) Manage IP [▼](#) Training [▼](#) Events [▼](#) Insights [▼](#) Community [▼](#) Blog Help Centre About [▼](#) Contact

Get your own IP Addresses

If your organization relies on the Internet, you may want to consider building your networks' infrastructure with your own IP addresses and AS numbers.

APNIC is the Regional Internet Registry for the Asia Pacific and delegates IP addresses to the region.

To get your own independent IP addresses and take control of your network, apply below.

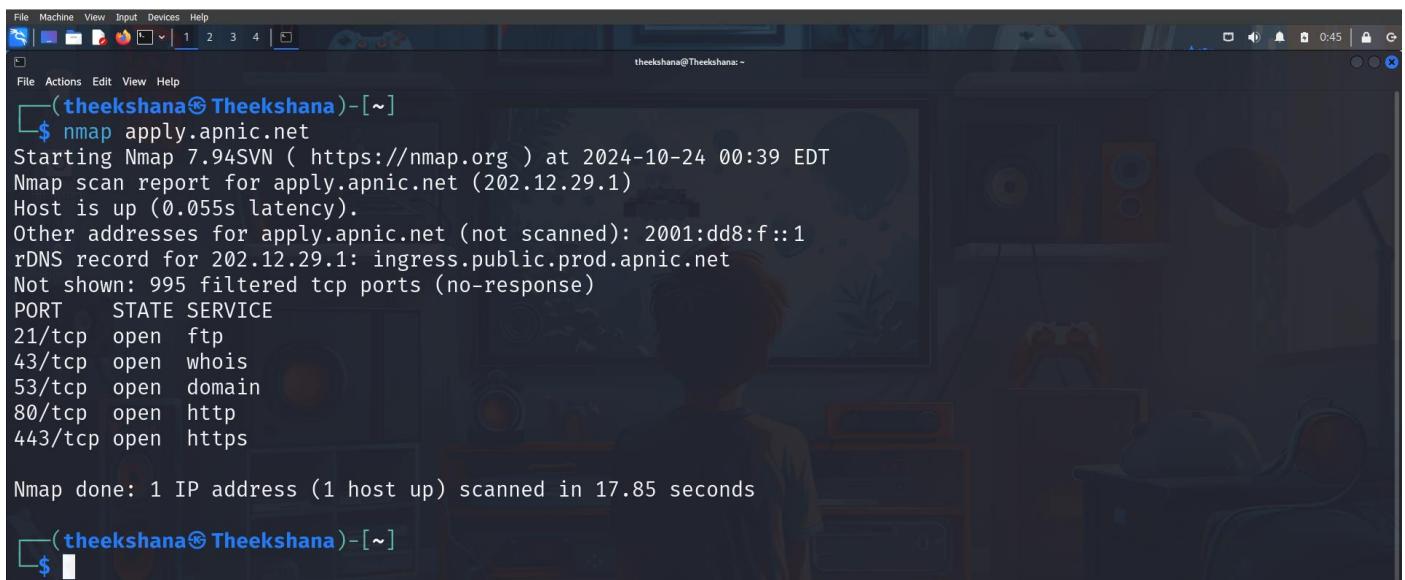
[Apply now](#) [I need more information first.](#)

Connect with us

APNIC

Target Reconnaissance

Nmap Scan



```
(theekshana@Theekshana)-[~]
$ nmap apply.apnic.net
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-24 00:39 EDT
Nmap scan report for apply.apnic.net (202.12.29.1)
Host is up (0.055s latency).
Other addresses for apply.apnic.net (not scanned): 2001:dd8:f::1
rDNS record for 202.12.29.1: ingress.public.prod.apnic.net
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
43/tcp    open  whois
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

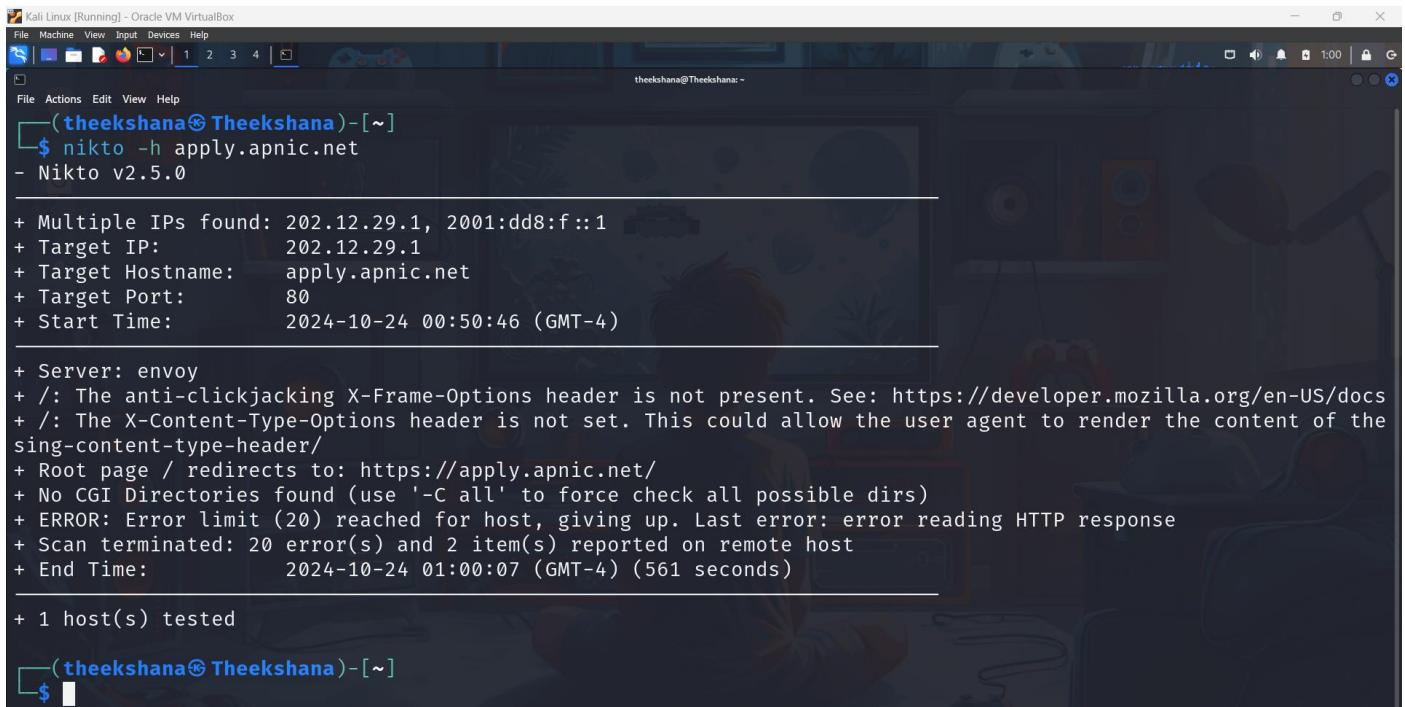
Nmap done: 1 IP address (1 host up) scanned in 17.85 seconds
```

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	HTTPS

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



```
[Kali Linux (Running) - Oracle VM VirtualBox]
File Machine View Input Devices Help
File Actions Edit View Help
(theekshana㉿Theekshana)-[~]
$ nikto -h apply.apnic.net
- Nikto v2.5.0
+ Multiple IPs found: 202.12.29.1, 2001:dd8:f::1
+ Target IP: 202.12.29.1
+ Target Hostname: apply.apnic.net
+ Target Port: 80
+ Start Time: 2024-10-24 00:50:46 (GMT-4)
+ Server: envoy
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the
sing-content-type-header/
+ Root page / redirects to: https://apply.apnic.net/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 2 item(s) reported on remote host
+ End Time: 2024-10-24 01:00:07 (GMT-4) (561 seconds)
+ 1 host(s) tested
(theekshana㉿Theekshana)-[~]
$
```

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.

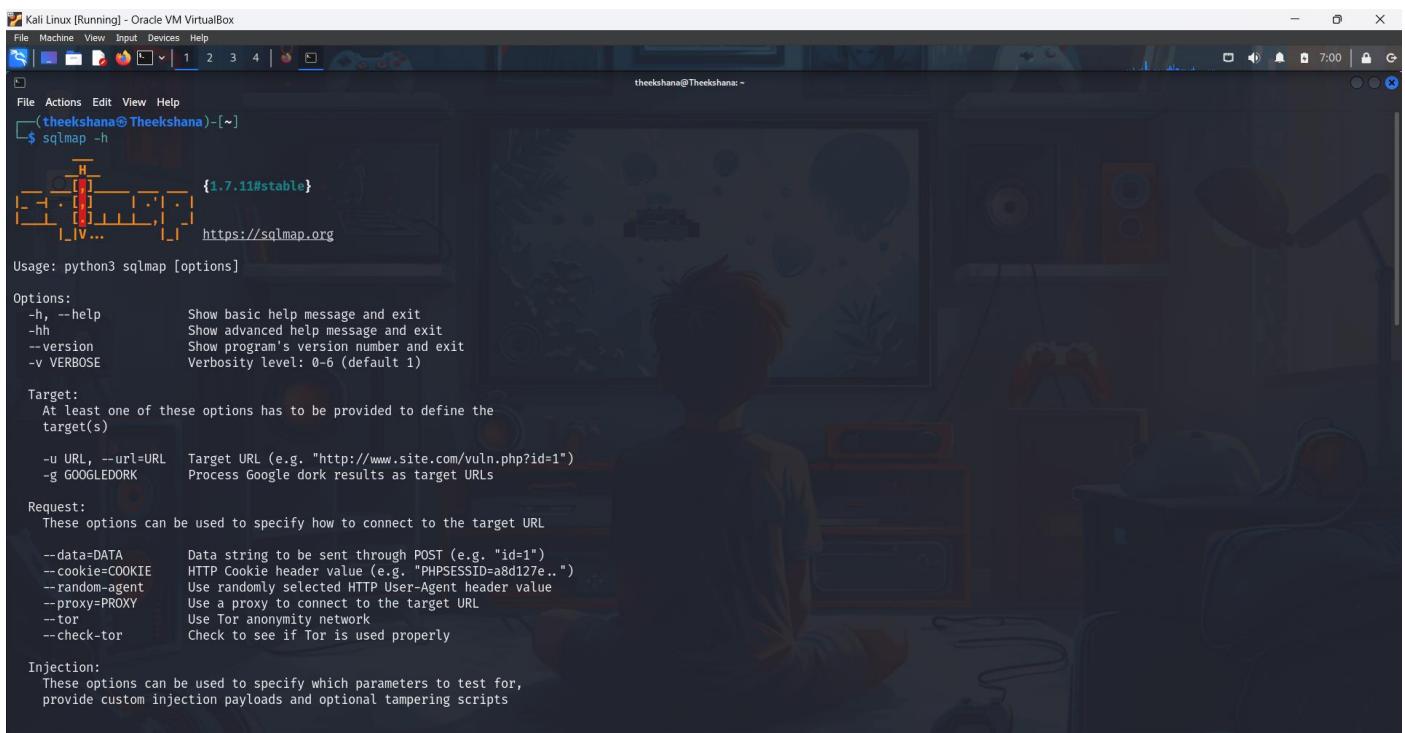
X-Frame-Options header missing: This header is not present, which could expose the site to **clickjacking attacks**. Without this, a malicious actor might embed the site in a hidden iframe on a malicious page and trick users into interacting with it.

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 Scanner



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
theekshana@Theekshana: ~
$ sqlmap -h

{ 1.7.11#stable }
https://sqlmap.org

Usage: python3 sqlmap [options]

Options:
-h, --help      Show basic help message and exit
-hh            Show advanced help message and exit
--version       Show program's version number and exit
-v VERBOSE     Verbosity level: 0-6 (default 1)

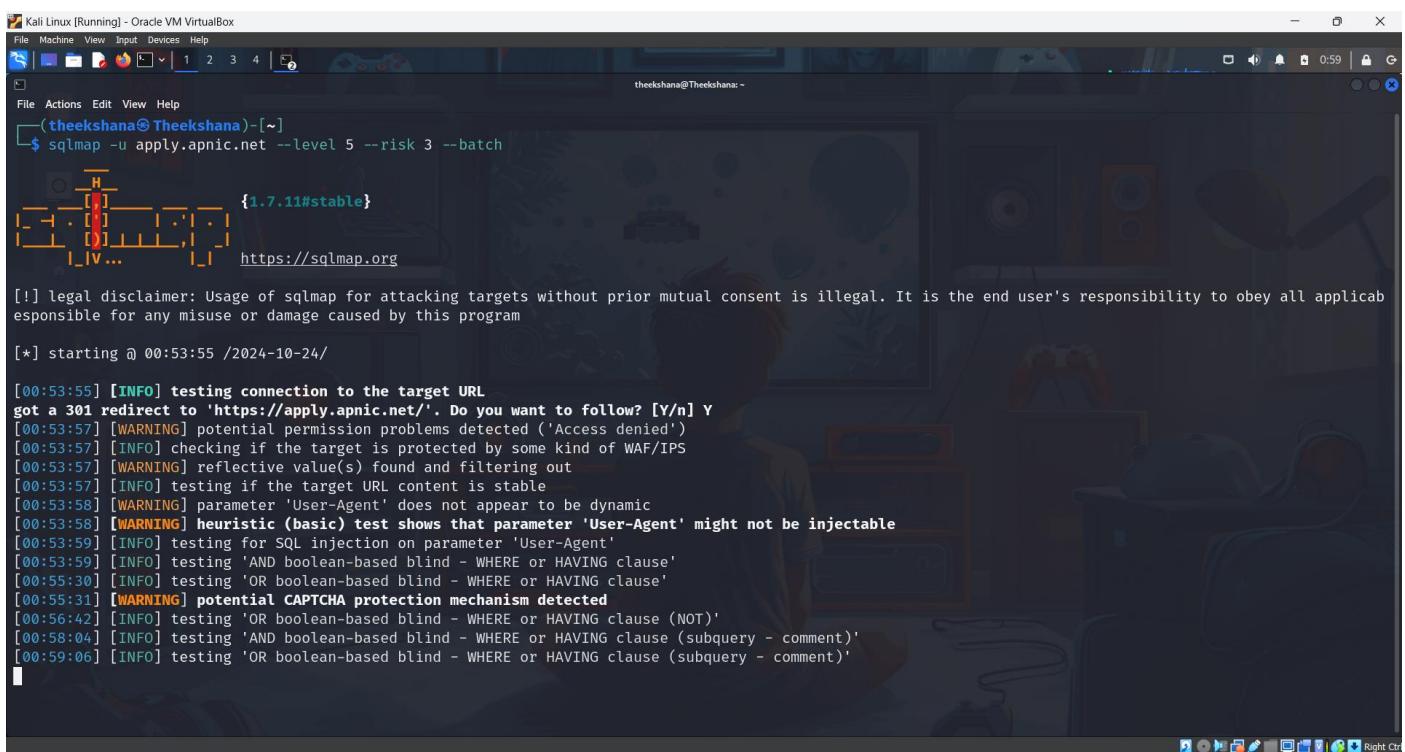
Target:
At least one of these options has to be provided to define the
target(s)

-u URL, --url=URL Target URL (e.g. "http://www.site.com/vuln.php?id=1")
-g GOOGLEDORK  Process Google dork results as target URLs

Request:
These options can be used to specify how to connect to the target URL

--data=DATA      Data string to be sent through POST (e.g. "id=1")
--cookie=COOKIE   HTTP Cookie header value (e.g. "PHPSESSID=a8d127e..")
--random-agent    Use randomly selected HTTP User-Agent header value
--proxy=PROXY     Use a proxy to connect to the target URL
--tor             Use Tor anonymity network
--check-tor       Check to see if Tor is used properly

Injection:
These options can be used to specify which parameters to test for,
provide custom injection payloads and optional tampering scripts
```



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
theekshana@Theekshana: ~
$ sqlmap -u apply.apnic.net --level 5 --risk 3 --batch

{ 1.7.11#stable }
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable laws
[*] starting @ 00:53:55 /2024-10-24

[00:53:55] [INFO] testing connection to the target URL
got a 301 redirect to 'https://apply.apnic.net/'. Do you want to follow? [Y/n] Y
[00:53:57] [WARNING] potential permission problems detected ('Access denied')
[00:53:57] [INFO] checking if the target is protected by some kind of WAF/IPS
[00:53:57] [WARNING] reflective value(s) found and filtering out
[00:53:57] [INFO] testing if the target URL content is stable
[00:53:58] [WARNING] parameter 'User-Agent' does not appear to be dynamic
[00:53:58] [WARNING] heuristic (basic) test shows that parameter 'User-Agent' might not be injectable
[00:53:59] [INFO] testing for SQL injection on parameter 'User-Agent'
[00:53:59] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[00:53:59] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[00:55:31] [WARNING] potential CAPTCHA protection mechanism detected
[00:56:42] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT)'
[00:58:04] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[00:59:06] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (subquery - comment)'
```

- **[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

```
File Machine View Input Devices Help
(theekshana@Theekshana)-[~]
$ nuclei -u apply.apnic.net

v3.3.4
projectdiscovery.io

[INF] Current nuclei version: v3.3.4 (outdated)
[INF] Current nuclei-templates version: v10.0.2 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 68
[INF] Templates loaded for current scan: 8654
[INF] Executing 8455 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 199 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Running httpx on input host
[INF] Found 1 URL from httpx
[INF] Templates clustered: 1613 (Reduced 1517 Requests)
[INF] Using Interactsh Server: cast.live
[INF] Skipped apply.apnic.net:443 from target list as found unresponsive 30 times
[missing-sri] [http] [info] https://www.apnic.net/landing ["https://www.apnic.net/wp-content/themes/apnic/assets/scripts/navigation.js?v=a1088181c5f05cc0f24b79463c7573a43409756c4238954d4427 /wp-content/themes/apnic/dist/index-vCpbzK5cd.js","https://www.recaptcha.net/recaptcha/api.js?onLoad=onLoadCallback&render=explicit","https://www.apnic.net/wp-includes/js/jquery/jquery.min.es/js/jquery/jquery-migrate.min.js?ver=3.4.1","https://www.apnic.net/wp-content/themes/apnic/js/bootstrap.min.js?v=651836407c1de5d122c2b394178950bd0508df3c7b5ff66607c5e740de09c27b16ver=6.2 K-theme/9.1.5/js/theme_min.js?ver=6.6.2","https://www.apnic.net/wp-content/themes/apnic/assets/scripts/main.js?v=5ad33bc6cb8cfcc5061be67ba45d0f692f78590ab558d62498eb8ad5fcada38c9ver=6.6.2"]
[tls-version] [ssl] [info] apply.apnic.net:443 [tls12]
[tls-version] [ssl] [info] apply.apnic.net:443 [tls13]
[ssl-issuer] [ssl] [info] apply.apnic.net:443 ["Let's Encrypt"]
[ssl-dns-names] [ssl] [info] apply.apnic.net:443 ["apnic.mobi","www.apnic.org","www.apnic.com","www.apnic.net.au","apnic.com.au","apnic.net.au","forms.apnic.net","www.apnic.academy","apnic.c.org.au","apnic.social","apnicfoundation.net","myapnic.net","www.apnic.com.au","apnic.academy","apnic.int","apnic.net","www.apnic.int","www.apnicfoundation.org","apnic.au","apnic.com","web.jc.au","www.apnicfoundation.com","www.apnicfoundation.net","apnic.blog","apply.apnic.net","www.apnic.mobi","apnicfoundation.com","www.apnic.org.au","www.myapnic.net"]
[caa-fingerprint] [dns] [info] apply.apnic.net [letsencrypt.org"]

(theekshana@Theekshana)-[~]
$
```

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

```
File Machine View Input Devices Help
theekshana@Theekshana: ~
File Actions Edit View Help
(theekshana@Theekshana) [~]
$ dmitry apply.apnic.net
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:202.12.29.1
HostName:apply.apnic.net

Gathered Inet-whois information for 202.12.29.1

inetnum: 202.112.0 - 202.22.159.255
netname: NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
desc: IPv4 address block not managed by the RIPE NCC
remarks:
remarks:
remarks: For registration information,
remarks: you can consult the following sources:
remarks:
remarks: IANA
remarks: http://www.iana.org/assignments/ipv4-address-space
remarks: http://www.iana.org/assignments/iana-ppn-special-registry
remarks: http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks: AFRINIC (Africa)
remarks: http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks: APNIC (Asia Pacific)
remarks: http://www.apnic.net/ whois.apnic.net
remarks:
remarks: ARIN (Northern America)
remarks: http://www.arin.net/ whois.arin.net
remarks:
remarks: LACNIC (Latin America and the Caribbean)
remarks: http://www.lacnic.net/ whois.lacnic.net
remarks:
remarks: EU # Country is really world wide
country: EU # Country is really world wide
admin-c: IANA-RIPE
tech-c: IANA-RIPE
status: ALLOCATED-UNSPECIFIED
mnt-by: RIPE-NCC-HM-MNT
created: 2021-11-15T16:06:25Z
last-modified: 2021-11-15T16:06:25Z
source: RIPE
role: Internet Assigned Numbers Authority
address: see http://www.iana.org/
admin-c: IANA-RIPE
tech-c: IANA-RIPE
nic-hdl: IANA-RIPE
remarks: For more information on IANA services
```

```
File Machine View Input Devices Help
theekshana@Theekshana: ~
File Actions Edit View Help
tech-c: IANA-RIPE
nic-hdl: IANA-RIPE
remarks: For more information on IANA services
remarks: Go to IANA web site at http://www.iana.org/
mnt-by: RIPE-NCC-MNT
created: 1970-01-01T00:00:00Z
last-modified: 2001-09-27T09:31:27Z
source: RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.114 (BUSA)

Gathered Inic-whois information for apply.apnic.net
ERROR: Unable to locate Name Whois data on apply.apnic.net
Gathered Netcraft information for apply.apnic.net

Retrieving Netcraft.com information for apply.apnic.net
Netcraft.com Information gathered

Gathering Subdomain information for apply.apnic.net
Searching Google.com:80...
Searching Altavista.com:80...
Found 0 possible subdomain(s) for host apply.apnic.net, Searched 0 pages containing 0 results

Gathered E-Mail information for apply.apnic.net
Searching Google.com:80...
Searching Altavista.com:80...
Found 0 E-Mail(s) for host apply.apnic.net, Searched 0 pages containing 0 results

Gathered TCP Port information for 202.12.29.1

Port      State
21/tcp    open
43/tcp    open
53/tcp    open
80/tcp    open

Portscan Finished: Scanned 150 ports, 0 ports were in state closed

All scans completed, exiting
(theekshana@Theekshana) [~]
```

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.

<http://apply.apnic.net/>

Scan Time

: 10/24/2024 10:57:41 AM (UTC+05:30)

Total Requests: 1,129

Average Speed: 8.3r/s

Risk Level:

INFORMATION

VULNERABILITIES

2

IDENTIFIED

0

CONFIRMED

0

CRITICAL

0

HIGH

0

MEDIUM

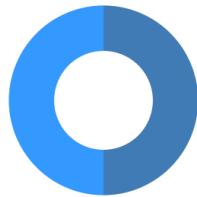
0

LOW

BEST PRACTICE

INFORMATION

Identified Vulnerabilities



Confirmed Vulnerabilities



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 misissued certificates to be used.

Vulnerabilities

<https://apply.apnic.net/>

Vulnerabilities

<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

[A14.1.2](#)

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 given permission to test.

URL to attack: Select...

Use traditional spider:

Use ajax spider: If Modern with Firefox Headless

Attack Stop

Progress: Manually stopped

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

Header: Text Body: Text

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

<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"/>

Raw Response: <html><head><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"/></head></html>

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:

Description:

Burp Suite

Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan

Tasks

- 4. Crawl and audit of apnic.net**
Crawl and Audit - Fast
Finished
Issues: 0 0 0 1
- 3. Crawl and audit of apply.apnic.net**
Crawl and Audit - Fast
Finished
Issues: 0 0 0 0

4. Crawl and audit of apnic.net

Summary Audit items Issues Event log Logger Audit log Live crawl view

Time	Source	Issue type	Host	Path	Insertion point	Severity
11:09:30 24 Oct 2024	Task 4	TLS certificate	https://apnic.net	/		Informational

Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan

Tasks

- 4. Crawl and audit of apnic.net**
Crawl and Audit - Fast
Finished
Issues: 0 0 0 1
- 3. Crawl and audit of apply.apnic.net**
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
Issues: 0 0 0 0

4. Crawl and audit of apnic.net

Summary Audit items Issues Event log Logger Audit log Live crawl view

Time	Source	Issue type	Host	Path	Insertion point	Severity
11:09:30 24 Oct 2024	Task 4	TLS certificate	https://apnic.net	/		Informational

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](#)

Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan

Tasks

- 4. Crawl and audit of apnic.net**
Crawl and Audit - Fast
Finished
Issues: 0 0 0 1
- 3. Crawl and audit of apply.apnic.net**
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
Issues: 0 0 0 0

4. Crawl and audit of apnic.net

Summary Audit items Issues Event log Logger Audit log Live crawl view

Time	Source	Issue type	Host	Path	Insertion point	Severity
11:09:30 24 Oct 2024	Task 4	TLS certificate	https://apnic.net	/		Informational

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

Vulnerabilities:

1 Link manipulation (DOM-based)

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

Report 07 Target Details

The screenshot shows a bug bounty report page for CBRE. On the left is a sidebar with various icons and links: Security page, Program guidelines (highlighted), Scope, Hacktivity, Thanks, Updates, and a user profile icon. The main content area has several sections: 'Program highlights' showing compliance with Platform Standards and response efficiency above 90%; performance metrics like average time to first response (21 hours), triage (1 day, 14 hours), bounty (N/A), and resolution (3 months, 1 week); 'Scope exclusions' noting Core Ineligible Findings; and an 'Overview' section last updated on May 3, 2024. A 'Stats' sidebar on the right tracks reports received (114), last report resolved (17 hours ago), reports resolved (1054), hackers thanked (311), and assets in scope (8553). A blue 'Submit report' button is also visible.

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.

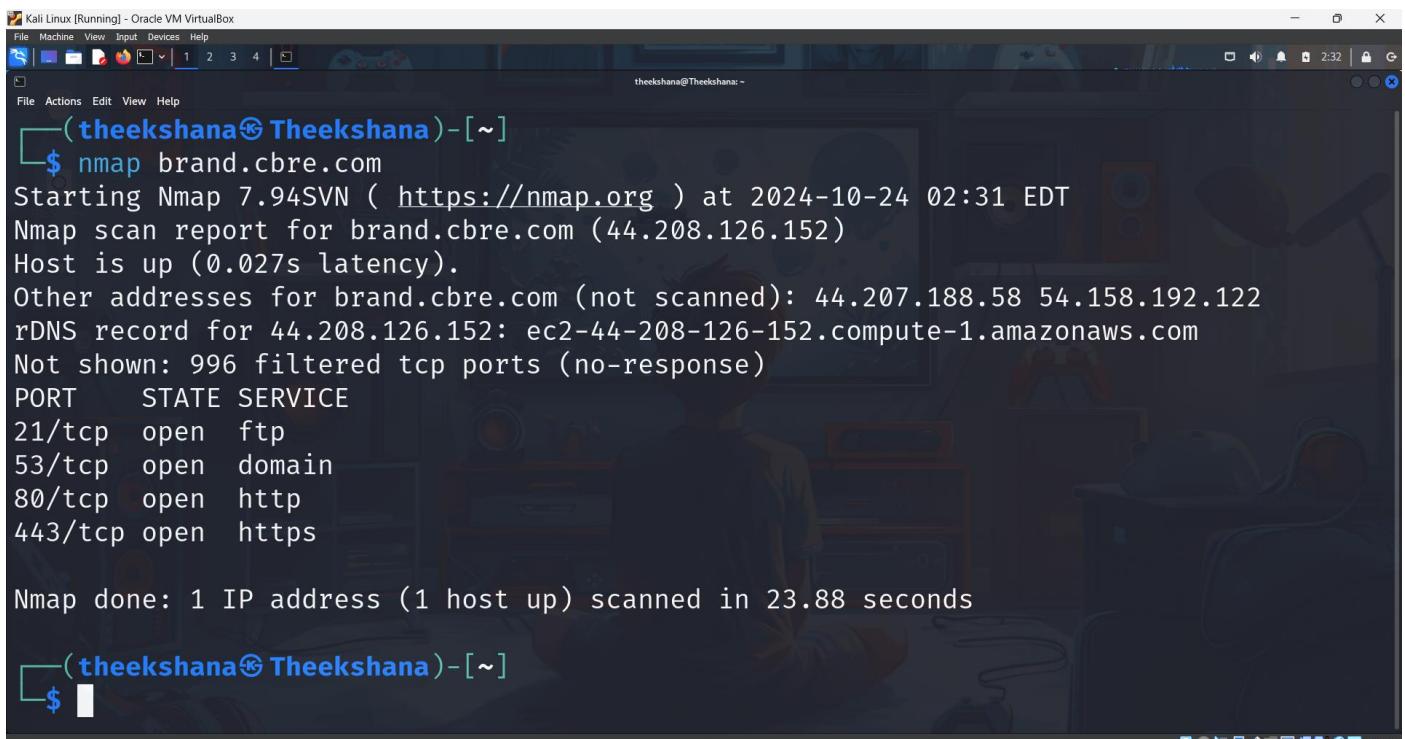
In this report, I have chosen to focus on 10 subdomains under the main domain cbre.com. Each subdomain may serve different functionalities or services, potentially introducing distinct security risks, particularly in development or user-related areas. These subdomains were selected based on their relevance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

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

The screenshot shows the CBRE Brand Experience Center website. It features a dark header with the CBRE logo and a dropdown menu set to 'English'. Below the header is a large image of the CBRE logo. The main content area has a teal background with the text 'Brand Experience Center'. A quote below it reads: 'Our brand helps us represent who we are, what we do, and what we stand for. It is a foundation that guides our visual and verbal expression both internally and externally.' There are two buttons at the bottom: a dark green 'Employee' button and a white 'External User Login' button.

Target Reconnaissance

Nmap Scan



```
(theekshana㉿Theekshana) [~]
$ nmap brand.cbre.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-24 02:31 EDT
Nmap scan report for brand.cbre.com (44.208.126.152)
Host is up (0.027s latency).
Other addresses for brand.cbre.com (not scanned): 44.207.188.58 54.158.192.122
rDNS record for 44.208.126.152: ec2-44-208-126-152.compute-1.amazonaws.com
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

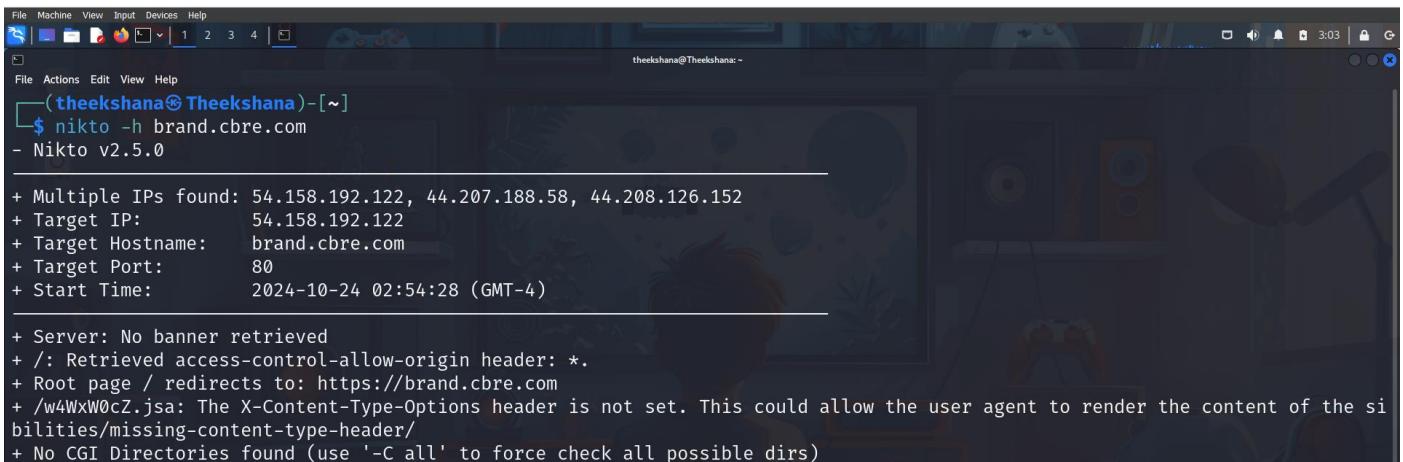
Nmap done: 1 IP address (1 host up) scanned in 23.88 seconds
```

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	HTTPS

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



```
File Machine View Input Devices Help
(theekshana@Theekshana)-[~]
$ nikto -h brand.cbre.com
- Nikto v2.5.0

+ Multiple IPs found: 54.158.192.122, 44.207.188.58, 44.208.126.152
+ Target IP: 54.158.192.122
+ Target Hostname: brand.cbre.com
+ Target Port: 80
+ Start Time: 2024-10-24 02:54:28 (GMT-4)

+ Server: No banner retrieved
+ /: Retrieved access-control-allow-origin header: *.
+ Root page / redirects to: https://brand.cbre.com
+ /w4WxW0cZ.jsa: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the sibilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

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 Scanner

```
File Machine View Input Devices Help
(theekshana@Theekshana) [-]
$ sqlmap -u brand.cbre.com --level 5 --risk 3 --batch
{1.7.11#stable}
https://sqlmap.org

[[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 02:34:28 /2024/10/24

[02:34:29] [INFO] testing connection to the target URL
[02:35:01] [INFO] checking if the target is protected by some kind of WAF/IPS
[02:35:02] [INFO] testing if the target URL content is stable
[02:35:03] [INFO] target URL content is stable
[02:35:04] [INFO] testing if parameter 'User-Agent' is dynamic
[02:35:05] [WARNING] parameter 'User-Agent' does not appear to be dynamic
[02:35:06] [INFO] heuristic (basic) test shows that parameter 'User-Agent' might not be injectable
[02:35:07] [INFO] testing for SQL injection on parameter 'User-Agent'
[02:35:08] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[02:35:09] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[02:35:10] [INFO] testing 'NOT AND boolean-based blind - WHERE or HAVING clause (NOT)'
[02:38:48] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[02:38:49] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (comment)'
[02:39:35] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (comment)'
[02:39:49] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT comment)'
[02:39:50] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[02:40:57] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[02:40:53] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
[02:41:14] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'
[02:41:34] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'
[02:42:18] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'
[02:42:20] [INFO] testing 'MySQL REGEXP boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[02:42:26] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[02:44:28] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
[02:45:05] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
[02:46:08] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (bool+int)'
[02:46:45] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (bool+int)'
[02:47:36] [INFO] testing 'PostgreSQL OR boolean-based blind - WHERE or HAVING clause (CAST)'
[02:48:36] [INFO] testing 'PostgreSQL OR boolean-based blind - WHERE or HAVING clause (CAST)'
[02:49:36] [INFO] testing 'Oracle AND boolean-based blind - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)'
[02:50:44] [INFO] testing 'Oracle OR boolean-based blind - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)'
[02:52:08] [INFO] testing 'SQLite AND boolean-based blind - WHERE, HAVING, GROUP BY or HAVING clause (JSON)'
[02:52:57] [INFO] testing 'SQLite OR boolean-based blind - WHERE, HAVING, GROUP BY or HAVING clause (JSON)'
[02:54:27] [INFO] testing 'MySQL boolean-based blind - Parameter replace (MAKE_SET)'
[02:54:28] [INFO] testing 'MySQL boolean-based blind - Parameter replace (MAKE_SET - original value)'
[02:54:30] [INFO] testing 'MySQL boolean-based blind - Parameter replace (ELT)'

File Machine View Input Devices Help
(theekshana@Theekshana) [-]
$ sqlmap -u brand.cbre.com --level 5 --risk 3 --batch
{1.7.11#stable}
https://sqlmap.org

[[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 02:54:27 /2024/10/24

[02:54:27] [INFO] testing 'MySQL boolean-based blind - Parameter replace (MAKE_SET)'
[02:54:28] [INFO] testing 'MySQL boolean-based blind - Parameter replace (MAKE_SET - original value)'
[02:54:30] [INFO] testing 'MySQL boolean-based blind - Parameter replace (ELT)'
[02:54:31] [INFO] testing 'MySQL boolean-based blind - Parameter replace (ELT - original value)'
[02:54:32] [INFO] testing 'MySQL boolean-based blind - Parameter replace (original value)'
[02:54:34] [INFO] testing 'MySQL boolean-based blind - Parameter replace (bool+int)'
[02:54:35] [INFO] testing 'MySQL boolean-based blind - Parameter replace (original value)'
[02:54:36] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace'
[02:54:37] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace (ELT)'
[02:54:39] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace (GENERATE_SERIES - original value)'
[02:54:40] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace (original value)'
[02:54:41] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Parameter replace'
[02:54:42] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Parameter replace (original value)'
[02:54:43] [INFO] testing 'Oracle boolean-based blind - Parameter replace'
[02:54:44] [INFO] testing 'Oracle boolean-based blind - Parameter replace (original value)'
[02:54:45] [INFO] testing 'Informix boolean-based blind - Parameter replace'
[02:54:47] [INFO] testing 'Informix boolean-based blind - Parameter replace (original value)'
[02:54:48] [INFO] testing 'Microsoft Access boolean-based blind - Parameter replace'
[02:54:49] [INFO] testing 'Microsoft Access boolean-based blind - Parameter replace (original value)'
[02:54:50] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL)'
[02:54:51] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL - original value)'
[02:54:52] [INFO] testing 'Boolean-based blind - Parameter replace (CASE)'
[02:54:54] [INFO] testing 'Boolean-based blind - Parameter replace (CASE - original value)'
[02:54:55] [INFO] testing 'MySQL > 5.0 boolean-based blind - ORDER BY, GROUP BY clause'
[02:55:06] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[02:55:08] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[02:55:09] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY, GROUP BY clause'
[02:55:09] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[02:55:09] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[02:55:09] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[02:55:09] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[02:55:09] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[02:55:12] [INFO] testing 'Oracle boolean-based blind - ORDER BY, GROUP BY clause'
[02:55:14] [INFO] testing 'Oracle boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[02:55:17] [INFO] testing 'Microsoft Access boolean-based blind - ORDER BY, GROUP BY clause'
[02:55:22] [INFO] testing 'SAP MaxDB boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[02:55:25] [INFO] testing 'SAP MaxDB boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[02:55:27] [INFO] testing 'IBM DB2 boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[02:55:29] [INFO] testing 'IBM DB2 boolean-based blind - ORDER BY clause'
[02:55:33] [INFO] testing 'HAVING boolean-based blind - WHERE, GROUP BY clause'
[02:55:33] [INFO] testing 'MySQL > 5.0 boolean-based blind - Stacked queries'
[02:56:01] [INFO] testing 'MySQL < 5.0 boolean-based blind - Stacked queries'
[02:56:51] [INFO] testing 'PostgreSQL boolean-based blind - Stacked queries'
[02:57:23] [INFO] testing 'PostgreSQL boolean-based blind - Stacked queries (GENERATE_SERIES)'
[02:57:51] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Stacked queries (IF)'
[02:58:23] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Stacked queries'
[02:59:23] [INFO] testing 'Oracle boolean-based blind - Stacked queries'
[02:59:26] [INFO] testing 'Microsoft Access boolean-based blind - Stacked queries'
[03:00:01] [INFO] testing 'SAP MaxDB boolean-based blind - Stacked queries'
[03:00:34] [INFO] testing 'MySQL > 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[03:01:42] [INFO] testing 'MySQL > 5.5 OR error-based - WHERE, HAVING clause (BIGINT UNSIGNED)'
```

- **[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

```
File Machine View Input Devices Help
(theekshana@Theekshana) ~
$ nuclei -u brand.cbre.com
v3.3.4
projectdiscovery.io

[INF] Current nuclei version: v3.3.4 (outdated)
[INF] Current nuclei-templates version: v10.0.2 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 68
[INF] Templates loaded for current scan: 8654
[WRN] Loading 199 unsigned templates for scan. Use with caution.
[INF] Executing 8455 signed templates from projectdiscovery/nuclei-templates
[INF] Targets loaded for current scan: 1
[INF] Running httpx on input host
[INF] Found 1 URL from httpx
[INF] Templates clustered: 1613 (Reduced 1517 Requests)
[INF] Using Interactsh Server: oast.me
[tls-version] [ssl] [info] brand.cbre.com:443 ["tls12"]
[tls-version] [ssl] [info] brand.cbre.com:443 ["tls13"]
[http-missing-security-headers:clear-site-data] [http] [info] https://brand.cbre.com
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] https://brand.cbre.com
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] https://brand.cbre.com
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] https://brand.cbre.com
[http-missing-security-headers:content-security-policy] [http] [info] https://brand.cbre.com
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] https://brand.cbre.com
[robots-txt-endpoint] [http] [info] https://brand.cbre.com/robots.txt
[xss-deprecated-header] [http] [info] https://brand.cbre.com ['1; mode=block']
[dns-saas-service-detection] [dns] [info] brand.cbre.com ['lbi.beam3.monigle.net']
[caa-fingerprint] [dns] [info] brand.cbre.com
[ssl-issuer] [ssl] [info] brand.cbre.com:443 ['Let's Encrypt']
[ssl-dns-names] [ssl] [info] brand.cbre.com:443 ['brand.cbre.com', 'cbre.beam3.monigle.net']

(theekshana@Theekshana) ~
$
```

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

```
File Machine View Input Devices Help
(theekshana@Theekshana) [~]
$ dmitry brand.cbre.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:44.208.126.152
HostName:brand.cbre.com

Gathered Inet-whois information for 44.208.126.152

inetnum: 43.255.112.0 - 45.3.31.255
netname: NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
desc: IPv4 address block not managed by the RIPE NCC
remarks:
remarks:
remarks: For registration information,
remarks: you can consult the following sources:
remarks: IANA
remarks: http://www.iana.org/assignments/ipv4-address-space
remarks: http://www.iana.org/assignments/iana-ipv4-special-registry
remarks: http://www.iana.org/assignments/ipv4-recovered-address-space
remarks: AFRINIC (Africa)
remarks: http://www.apnic.net/ whois.apnic.net
remarks: APNIC (Asia Pacific)
remarks: http://www.apnic.net/ whois.apnic.net
remarks: ARIN (Northern America)
remarks: http://www.arin.net/ whois.arin.net
remarks: LACNIC (Latin America and the Caribbean)
remarks: http://www.lacnic.net/ whois.lacnic.net
remarks: country: EU # Country is really world wide
admin-c: IANAI-RIPE
tech-c: IANAI-RIPE
status: ALLOCATED UNSPECIFIED
mnt-by: RIPE-NCC-HM-MNT
created: 2022-03-09T15:18:21Z
last-modified: 2022-03-09T15:18:21Z
source: RIPE
role: Internet Assigned Numbers Authority
address: see http://www.iana.org/
admin-c: IANAI-RIPE
tech-c: IANAI-RIPE
nic-hdl: IANAI-RIPE

File Machine View Input Devices Help
(theekshana@Theekshana) [~]
$ File Actions Edit View Help
admin-c: IANAI-RIPE
tech-c: IANAI-RIPE
nic-hdl: IANAI-RIPE
remarks: No Whois information on IANA services
remarks: go to IANA web site at http://www.iana.org.
mnt-by: RIPE-NCC-MNT
created: 1970-01-01T00:00:00Z
last-modified: 2001-09-22T09:31:27Z
source: RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.114 (SHETLAND)

Gathered Inic-whois information for brand.cbre.com
ERROR: Unable to locate Name Whois data on brand.cbre.com
Gathered Netcraft information for brand.cbre.com

Retrieving Netcraft.com information for brand.cbre.com
Netcraft.com Information gathered

Gathered Subdomain information for brand.cbre.com
Searching Google.com:80...
Searching Altavista.com:80...
Found 0 possible subdomain(s) for host brand.cbre.com, Searched 0 pages containing 0 results

Gathered E-Mail information for brand.cbre.com
Searching Google.com:80...
Searching Altavista.com:80...
Found 0 E-Mail(s) for host brand.cbre.com, Searched 0 pages containing 0 results

Gathered TCP Port information for 44.208.126.152

Port      State
21/tcp    open
53/tcp    open
80/tcp    open

Portscan Finished: Scanned 150 ports, 0 ports were in state closed

All scans completed, exiting
(theekshana@Theekshana) [~]
```

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

Detailed Scan Report

http://brand.cbre.com/ 🔗

Scan Time : 10/24/2024 12:20:49 PM (UTC+05:30)

Total Requests: 1,091
Average Speed: 13.7/s

Risk Level: **MEDIUM**

VULNERABILITIES

13
IDENTIFIED

3
CONFIRMED

0 !
CRITICAL

0 !
HIGH

1 !
MEDIUM

2 !
LOW

1 !
BEST PRACTICE

9 !
INFORMATION

Identified Vulnerabilities



Severity	Count
Critical	0
High	0
Medium	1
Low	2
Best Practice	1
Information	9
TOTAL	13

Confirmed Vulnerabilities



Severity	Count
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
!	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

The screenshot shows the OWASP ZAP interface during an automated scan. The main window displays the URL `http://brand.cbre.com` and the status "Actively scanning (attacking) the URLs discovered by the spider(s)". A detailed alert for a "CSP: Wildcard Directive" is highlighted in red, showing the following details:

- URL:** `http://brand.cbre.com`
- Risk:** Medium
- Confidence:** High
- Parameter:** content-security-policy
- Attack:** content-uri-self; object-src 'self'; script-src 'self' https: sentry.io googleapis.com googletagmanager.com google-analytics.com adobedtm.com 'nonce-sSmcDmsYV6AJUrv5cTeg=' 'nonce-1BoaJSfLzYDlpTs9hpCyA=' 'nonce-3s76EEbjkZZWnlZtSC600Q=' 'nonce-F1a74PVNmT0R0Uvr2JObg=' 'nonce-zmXO3pmKZfQDjzrQ75keIA=' 'nonce-gFuYlc3g4M4V+6/a0afw=' 'nonce-ridsUJllslN5yEwTv0w='; style-src 'self' https: typekit.net 'nonce-sSmcDmsYV6AJUrv5cTeg=' 'sha256-47DEOp8HBSa+/TlmW+5jCeUoRkm5NMjWZG3hsFuU=' 'sha256-yh0RarI3Zbst2lWTgVV3wpbY6KrnMKoBrodb98UNc=' 'nonce-U2/27gcR2Kgh2Ynr7ragg=' 'nonce-6uzC3g8Z96YEW5hHGSw=' 'nonce-1R2hQot0jWUMe9zmHSTA=' 'nonce-jZCkRHShw5Uig/8ehFBQ='; default-src 'self' https: font-src 'self' data: typekit.net use.typekit.net; form-action 'none'; frame-src 'self' https: img-src 'self' https: blob: data:; upgrade-insecure-requests
- Evidence:** `base-uri 'self'; object-src 'self'; script-src 'self' https: sentry.io googleapis.com googletagmanager.com google-analytics.com adobedtm.com 'nonce-sSmcDmsYV6AJUrv5cTeg=' 'nonce-1BoaJSfLzYDlpTs9hpCyA=' 'nonce-3s76EEbjkZZWnlZtSC600Q=' 'nonce-F1a74PVNmT0R0Uvr2JObg=' 'nonce-zmXO3pmKZfQDjzrQ75keIA=' 'nonce-gFuYlc3g4M4V+6/a0afw=' 'nonce-ridsUJllslN5yEwTv0w='; style-src 'self' https: typekit.net 'nonce-sSmcDmsYV6AJUrv5cTeg=' 'sha256-47DEOp8HBSa+/TlmW+5jCeUoRkm5NMjWZG3hsFuU=' 'sha256-yh0RarI3Zbst2lWTgVV3wpbY6KrnMKoBrodb98UNc=' 'nonce-U2/27gcR2Kgh2Ynr7ragg=' 'nonce-6uzC3g8Z96YEW5hHGSw=' 'nonce-1R2hQot0jWUMe9zmHSTA=' 'nonce-jZCkRHShw5Uig/8ehFBQ='; default-src 'self' https: font-src 'self' data: typekit.net use.typekit.net; form-action 'none'; frame-src 'self' https: img-src 'self' https: blob: data:; upgrade-insecure-requests`
- CWE ID:** 693
- WASC ID:** 15
- Source:** Passive (10055 - CSP)
- Alert Reference:** 10055-4

The alert description states: "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."

The screenshot shows the detailed view of the "CSP: Wildcard Directive" alert. The "Solution" section contains the following text:

Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.

The "Reference" section lists several URLs:

- <https://www.w3.org/TR/CSP/>
- <https://canuse.com/#search=content+security+policy>
- <https://content-security-policy.com/>
- <https://github.com/HtmlUnit/htmlunit-csp>

The "Alert Tags" section includes tags for "CWE-693", "OWASP_2021_A05", and "OWASP_2017_A06". The "Key" and "Value" table shows the following configuration:

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-top10/2017/A06-Security_Misconfiguration.html

The screenshot shows the ZAP interface with the "Response" tab selected. The response content is as follows:

```
HTTP/1.1 200 OK
Date: Thu, 24 Oct 2024 07:10:37 GMT
Content-Type: text/javascript
Content-Length: 355257
Connection: keep-alive
Last-Modified: Thu, 19 Sep 2024 00:22:24 GMT
ETag: "36352d-6226dea93000"
R:a.render,staticRenderFn:a.staticRenderFn,},function(t){function e(e,n){var a=Object.create(t),o=[],r=[];if(n)for(var i in n.modules){a[i].closed:[],endedAnimations:[],}props:{options:{type:Object,required:[],},escapeKeyClose:(type:Boolean,default:!1),registeredViews:(type:Obj
for(;3==t._state;t=_value||t=_state?{t:_handled:!0,r:_immediateFn:(function(){var n=1==t._state?e.onFullFilled:e.onRejected;if(!n){t._modules.getNamespace(n).if(a.namespaced66(t._modules.getNamespaceMap[1],t,_0)(return r=Math.round(100*L(this._r,255))+%,g:Math.round(100*L(this._g,255))+%,b:Math.round(100*L(this._b,255))+%,a:this._a),toPercentConstructor,o:t,a:ba.prototype|i,s:="constructor";for($t,r){e.contains(r)||e.push(r);n-=1;r=g[n]||t._modules.getNamespaceMap[1].push(t._apply(t,arguments)),Nn(this,t))}});var Pn=pt,Fn=En(a);Fn._=Fn;var Vn=Fn;64198:function(t){"use strict";t.exports=JSON.parse(`{"name":`}}
```

The detailed alert for a "Vulnerable JS Library" is shown in the bottom left:

- URL:** `https://brand.cbre.com/assets/j/s/1799_9b974f.js`
- Risk:** Medium
- Confidence:** Medium
- Parameter:**
- Attack:**
- Evidence:** "axios","version":"0.21.4"
- CWE ID:** 829
- WASC ID:**

Burp Suite

Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Saha

Tasks

- 3. Crawl and audit of brand.cbre.com** (Paused) Issues: 0 0 0 13
- 2. Live audit from Proxy (all traffic)** (Capturing) Issues: 0 0 0 0
- 1. Live passive crawl from Proxy (all traffic)** (Capturing) Issues: 0 0 0 0

3. Crawl and audit of brand.cbre.com

Most serious vulnerabilities found (live)

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 (DOM-ba...	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

Task type: Crawl & audit
Scope: brand.cbre.com
Configuration: Crawl and Audit - Fast

Task progress

Total audit items: 22 Unique locations: 16
Audit items pending: 0 Pending actions: 0
Audit items in progress: 22 Current link depth: 0
Audit items completed: 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 Dnsync
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 Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Saha

Tasks

- 3. Crawl and audit of brand.cbre.com** (Paused) Issues: 0 0 0 13
- 2. Live audit from Proxy (all traffic)** (Capturing) Issues: 0 0 0 0
- 1. Live passive crawl from Proxy (all traffic)** (Capturing) Issues: 0 0 0 0

3. Crawl and audit of brand.cbre.com

Issues

Time	Source	Issue type	Host	Path	Insertion point	Severity
12:17:31 24 Oct 2024	Task 3	Web cache deception	https://brand.cbre.com	/		Informative
12:17:31 24 Oct 2024	Task 3	Cross-origin resource sharing	https://brand.cbre.com	/		Informative
12:16:18 24 Oct 2024	Task 3	Cross-origin resource sharing: arbitrary origin	https://brand.cbre.com	/		Informative
12:16:07 24 Oct 2024	Task 3	Ajax request header manipulation (DOM-based)	https://brand.cbre.com	/login		Informative
12:16:07 24 Oct 2024	Task 3	Cross-origin resource sharing	http://brand.cbre.com	/robots.txt		Informative
12:16:04 24 Oct 2024	Task 3	Cross-origin resource sharing: arbitrary origin	http://brand.cbre.com	/robots.txt		Informative
12:16:04 24 Oct 2024	Task 3	Email addresses disclosed	https://brand.cbre.com	/assets/js/853_9b974fjs		Informative
12:16:03 24 Oct 2024	Task 3	Content security policy: allowlisted script reso...	https://brand.cbre.com	/		Informative
12:16:03 24 Oct 2024	Task 3	Content security policy: allowlisted script reso...	https://brand.cbre.com	/login		Informative
12:16:02 24 Oct 2024	Task 3	Content security policy: allowlisted script reso...	https://brand.cbre.com	/zh-cn/		Informative
12:16:02 24 Oct 2024	Task 3	TLS certificate	https://brand.cbre.com	/		Informative
12:16:02 24 Oct 2024	Task 3	Robots.txt file	https://brand.cbre.com	/robots.txt		Informative

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.

Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Saha

Tasks

- 3. Crawl and audit of brand.cbre.com** (Paused) Issues: 0 0 0 13
- 2. Live audit from Proxy (all traffic)** (Capturing) Issues: 0 0 0 0
- 1. Live passive crawl from Proxy (all traffic)** (Capturing) Issues: 0 0 0 0

3. Crawl and audit of brand.cbre.com

Issues

Time	Source	Issue type	Host	Path	Insertion point	Severity
12:17:31 24 Oct 2024	Task 3	Web cache deception	https://brand.cbre.com	/		Informative
12:17:11 24 Oct 2024	Task 3	Cross-origin resource sharing	https://brand.cbre.com	/		Informative
12:17:11 24 Oct 2024	Task 3	Cross-origin resource sharing: arbitrary origin	https://brand.cbre.com	/		Informative
12:16:18 24 Oct 2024	Task 3	Ajax request header manipulation (DOM-based)	https://brand.cbre.com	/login		Informative
12:16:07 24 Oct 2024	Task 3	Cross-origin resource sharing	http://brand.cbre.com	/robots.txt		Informative
12:16:07 24 Oct 2024	Task 3	Cross-origin resource sharing: arbitrary origin	http://brand.cbre.com	/robots.txt		Informative
12:16:04 24 Oct 2024	Task 3	Content security policy: allowlisted script reso...	https://brand.cbre.com	/en/		Informative
12:16:04 24 Oct 2024	Task 3	Email addresses disclosed	https://brand.cbre.com	/assets/js/853_9b974fjs		Informative
12:16:03 24 Oct 2024	Task 3	Content security policy: allowlisted script reso...	https://brand.cbre.com	/		Informative
12:16:03 24 Oct 2024	Task 3	Content security policy: allowlisted script reso...	https://brand.cbre.com	/login		Informative
12:16:02 24 Oct 2024	Task 3	Content security policy: allowlisted script reso...	https://brand.cbre.com	/zh-cn/		Informative
12:16:02 24 Oct 2024	Task 3	TLS certificate	https://brand.cbre.com	/		Informative
12:16:02 24 Oct 2024	Task 3	Robots.txt file	https://brand.cbre.com	/robots.txt		Informative

Response 1

```

HTTP/2 200 OK
Date: Thu, 24 Oct 2024 06:45:58 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 2449
Vary: Accept-Encoding
Strict-Transport-Security: max-age=15724800; includeSubDomains
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: PUT, GET, POST, OPTIONS, DELETE, PATCH
Access-Control-Allow-Headers: X-Auth-Token, X-Requested-With, Content-Type, Accept, Origin, Authorization, Cache-Control, Beam-Client-Name, Beam-Current-Entity
Access-Control-Max-Age: 1728000
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Cache-Control: max-age=0, no-cache, no-store, must-revalidate

```

Inspector

Response headers

Vulnerabilities:

1 Misconfigured Access-Control-Allow-Origin Header

Vulnerability Title	Misconfigured Access-Control-Allow-Origin Header
Vulnerability Description	<p>The Access-Control-Allow-Origin header is misconfigured, allowing resources to be accessed by unauthorized or malicious origins.</p> <p>This header is responsible for controlling which domains are allowed to access a website's resources via cross-origin resource sharing (CORS).</p> <p>If misconfigured, it can expose sensitive data to any website that makes a request, leading to data breaches.</p>
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	<p>Risk Level: High. It allows unauthorized origins to access sensitive resources.</p> <p>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.</p>
Steps to Reproduce	<ol style="list-style-type: none">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 JavaScript5. Check if the Access-Control-Allow-Origin header is set to or includes unwanted origins.
Proof of Concept	<p>Expected Result: The response should be blocked due to CORS restrictions.</p> <p>Observed Result: The response is successfully received despite originating from an unauthorized domain.</p>
Proposed Mitigation or Fix	<p>Restrict the Access-Control-Allow-Origin header to specific trusted domains instead of using the wildcard.</p> <p>Ensure that credentials (cookies, HTTP authentication) are only shared with trusted origins by adding Access-Control-Allow-Credentials:true.</p> <p>Implement a strict CORS policy and thoroughly test its implementation across different origins.</p>

Report 08 Target Details

The screenshot shows a bug bounty report page for 'Fastly VDP'. On the left is a sidebar with various icons and links: Security page, Program guidelines (highlighted), Scope, Hacktivity, Thanks, Updates, and Help. The main content area has a header 'Program highlights' with sections for Closed Scope, Platform Standards, and Top Response Efficiency, all marked as compliant. It also shows 'Managed by HackerOne'. Below this are four boxes showing average response times: 3 days for first response, 3 days, 4 hours for triage, N/A for bounty, and 1 year, 1 month for resolution. A 'Scope exclusions' section notes that Core Ineligible Findings are out of scope. At the bottom is an 'Overview' section updated on July 15, 2024. To the right is a 'Stats' panel with metrics like Reports received (90 days: 7), Last report resolved (11 days ago), Reports resolved (26), and Hackers thanked (29). A 'Submit report' button is at the top right of the stats panel.

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.

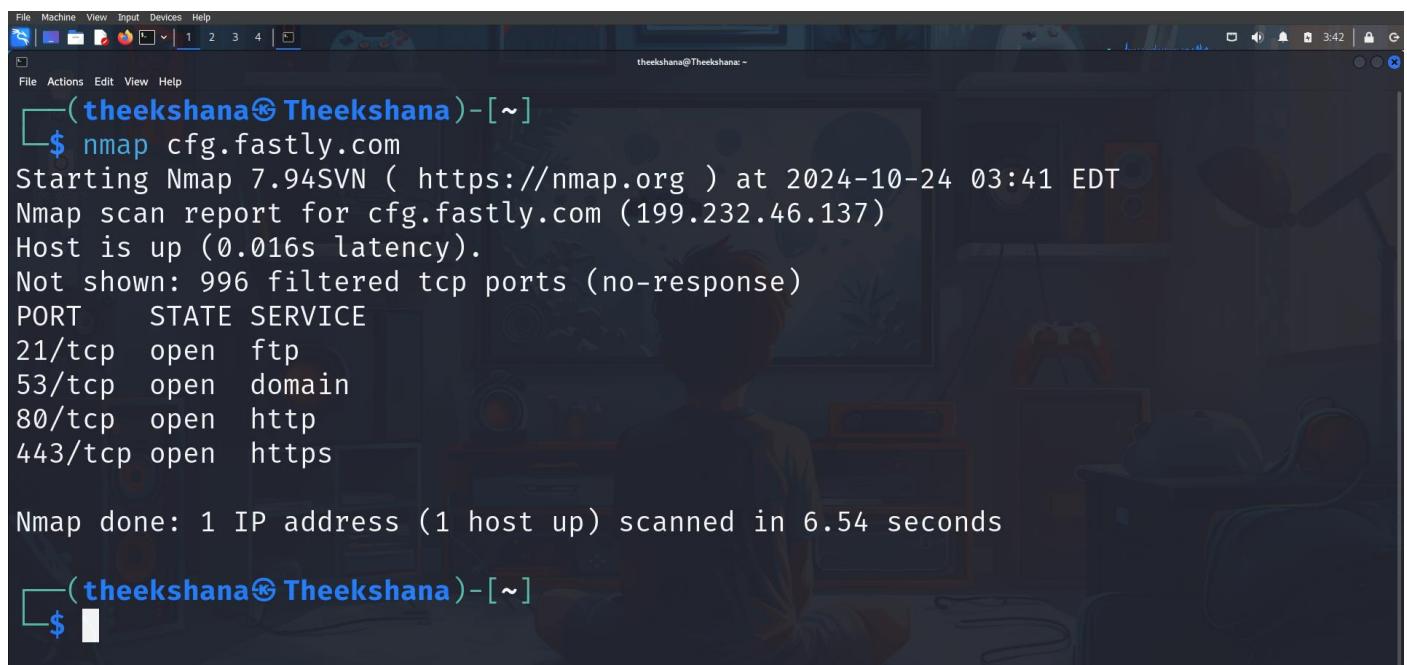
This report covers the findings for the subdomain: [cfg.faslty.com](#)

A screenshot of a sign-up or login form for 'faslty'. The form has a red 'faslty' logo at the top. It contains a 'Email *' field with a placeholder 'Email' and a 'Continue' button below it. Below the button is a 'Try another way' link. At the bottom, there is a note: 'By continuing, you agree to the [Terms of Service](#) and acknowledge our [Privacy Policy](#)'.

Don't have an account? [Sign up >](#)

Target Reconnaissance

Nmap Scan



```
(theekshana㉿Theekshana) - [~]
$ nmap cfg.fastly.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-24 03:41 EDT
Nmap scan report for cfg.fastly.com (199.232.46.137)
Host is up (0.016s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

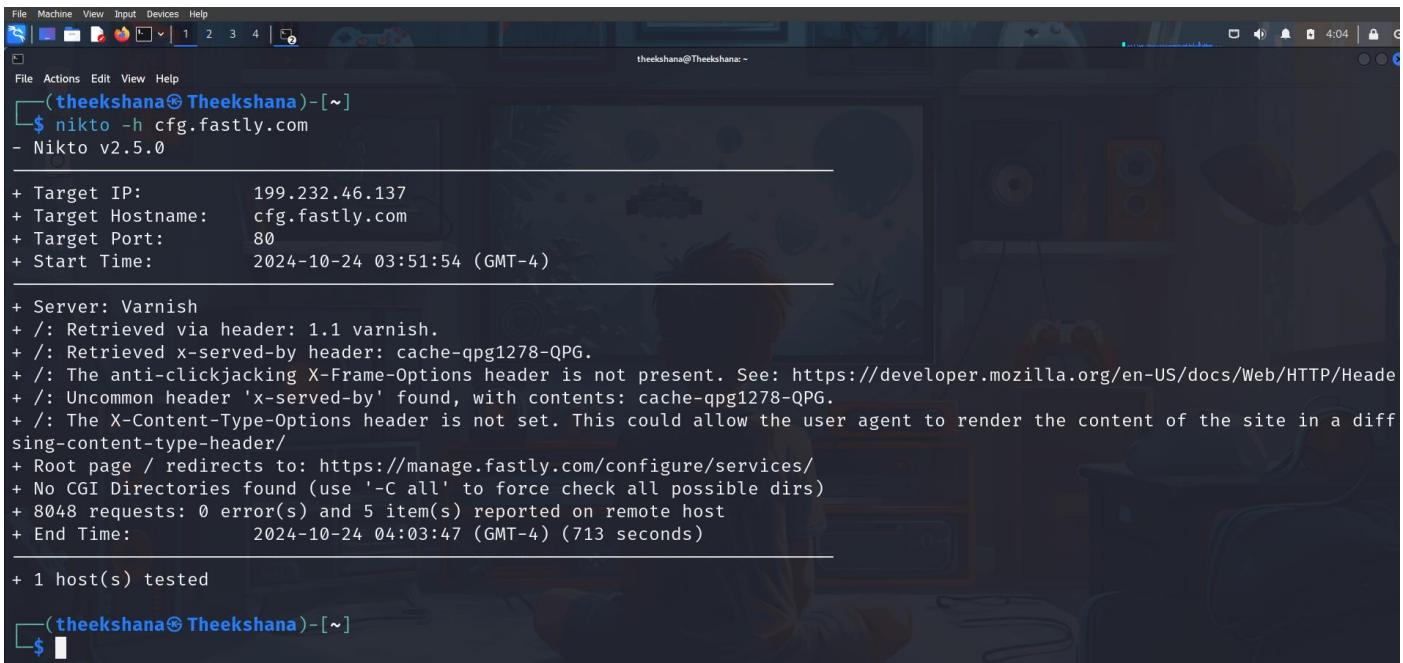
Nmap done: 1 IP address (1 host up) scanned in 6.54 seconds
```

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	HTTPS

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



```
File Machine View Input Devices Help
theekshana@Theekshana: ~
(theekshana@Theekshana)-[~]
$ nikto -h cfg.fastly.com
- Nikto v2.5.0

+ Target IP: 199.232.46.137
+ Target Hostname: cfg.fastly.com
+ Target Port: 80
+ Start Time: 2024-10-24 03:51:54 (GMT-4)

+ Server: Varnish
+ /: Retrieved via header: 1.1 varnish.
+ /: Retrieved x-served-by header: cache-qpg1278-QPG.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Heade
+ /: Uncommon header 'x-served-by' found, with contents: cache-qpg1278-QPG.
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a diff
sing-content-type-header/
+ Root page / redirects to: https://manage.fastly.com/configure/services/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 8048 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time: 2024-10-24 04:03:47 (GMT-4) (713 seconds)

+ 1 host(s) tested

(theekshana@Theekshana)-[~]
$
```

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)

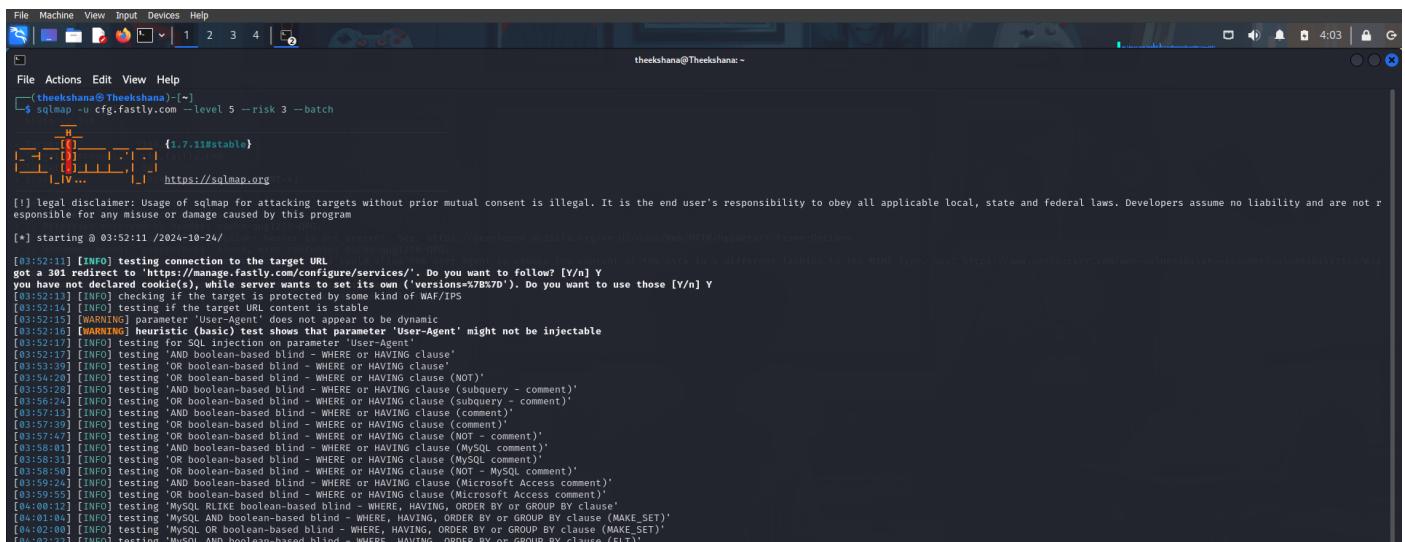
Findings:

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 Scanner

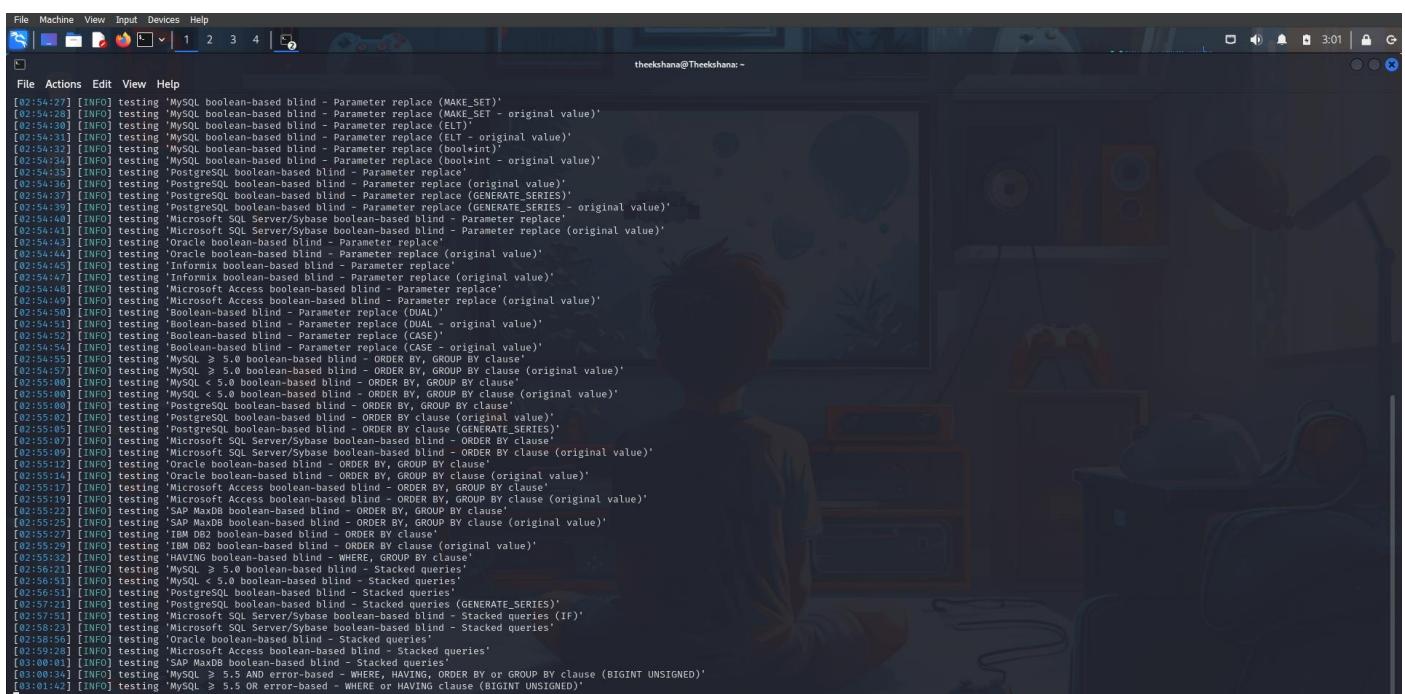


```
File Machine View Input Devices Help
(theekshana@Theekshana) [-]
$ sqlmap -u cfg.fastly.com --level 5 --risk 3 --batch
{1.7.11#stable}
https://sqlmap.org ...

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 03:52:11 /2024-10-24/

[03:52:11] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ({version=78%D}). Do you want to follow? [Y/n] Y
[03:52:14] [INFO] testing if the target URL content is stable
[03:52:15] [INFO] parameter 'User-Agent' does not appear to be dynamic
[03:52:16] [WARNING] heuristic (basic) test shows that parameter 'User-Agent' might not be injectable
[03:52:17] [INFO] testing for SQL injection on parameter 'User-Agent'
[03:52:17] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[03:52:18] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[03:52:19] [INFO] testing 'NOT boolean-based blind - WHERE or HAVING clause (NOT)'
[03:52:20] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[03:52:24] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (comment)'
[03:52:25] [INFO] testing 'NOT boolean-based blind - WHERE or HAVING clause (NOT - comment)'
[03:52:26] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[03:52:31] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[03:52:36] [INFO] testing 'NOT boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
[03:52:39] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'
[03:52:40] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'
[03:52:41] [INFO] testing 'NOT boolean-based blind - WHERE or HAVING clause (NOT - Microsoft Access comment)'
[03:52:42] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (PostgreSQL comment)'
[03:52:43] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (PostgreSQL comment)'
[03:52:44] [INFO] testing 'NOT boolean-based blind - WHERE or HAVING clause (NOT - PostgreSQL comment)'
[03:52:45] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQLi comment)'
[03:52:46] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQLi comment)'
[03:52:47] [INFO] testing 'NOT boolean-based blind - WHERE or HAVING clause (NOT - MySQLi comment)'
[03:52:48] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (Microsoft ODBC comment)'
[03:52:49] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (PostgreSQL ODBC comment)'
[03:52:50] [INFO] testing 'NOT boolean-based blind - WHERE or HAVING clause (NOT - PostgreSQL ODBC comment)'
[03:52:51] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (Microsoft ODBC comment)'
[03:52:52] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (PostgreSQL ODBC comment)'
[03:52:53] [INFO] testing 'NOT boolean-based blind - WHERE or HAVING clause (NOT - PostgreSQL ODBC comment)'
[03:52:54] [INFO] testing 'AND boolean-based blind - ORDER BY or GROUP BY clause (MAKE_SET)'
[03:52:55] [INFO] testing 'OR boolean-based blind - ORDER BY or GROUP BY clause (ELT)'
[03:52:56] [INFO] testing 'NOT boolean-based blind - ORDER BY or GROUP BY clause (NOT - ELT)'
```



```
File Machine View Input Devices Help
(theekshana@Theekshana) [-]
$ sqlmap -u cfg.fastly.com --level 5 --risk 3 --batch
{1.7.11#stable}
https://sqlmap.org ...

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 03:52:11 /2024-10-24/

[02:54:27] [INFO] testing 'MySQL boolean-based blind - Parameter replace (MAKE_SET)'
[02:54:28] [INFO] testing 'MySQL boolean-based blind - Parameter replace (MAKE_SET - original value)'
[02:54:30] [INFO] testing 'MySQL boolean-based blind - Parameter replace (ELT)'
[02:54:31] [INFO] testing 'MySQL boolean-based blind - Parameter replace (ELT - original value)'
[02:54:32] [INFO] testing 'MySQL boolean-based blind - Parameter replace (original int)'
[02:54:33] [INFO] testing 'MySQL boolean-based blind - Parameter replace (original float - original value)'
[02:54:35] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace'
[02:54:36] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace (original value)'
[02:54:37] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace (GENERATE_SERIES)'
[02:54:39] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace (GENERATE_SERIES - original value)'
[02:54:40] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Parameter replace'
[02:54:41] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Parameter replace (original value)'
[02:54:43] [INFO] testing 'Oracle boolean-based blind - Parameter replace'
[02:54:44] [INFO] testing 'Oracle boolean-based blind - Parameter replace (original value)'
[02:54:45] [INFO] testing 'Informix boolean-based blind - Parameter replace'
[02:54:47] [INFO] testing 'Informix boolean-based blind - Parameter replace (original value)'
[02:54:48] [INFO] testing 'Microsoft Access boolean-based blind - Parameter replace'
[02:54:49] [INFO] testing 'Microsoft Access boolean-based blind - Parameter replace (original value)'
[02:54:50] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL)'
[02:54:51] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL - original value)'
[02:54:52] [INFO] testing 'Boolean-based blind - Parameter replace (CASE)'
[02:54:54] [INFO] testing 'Boolean-based blind - Parameter replace (CASE - original value)'
[02:55:39] [INFO] testing 'MySQL > 5.0 boolean-based blind - ORDER BY, GROUP BY clause'
[02:55:40] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[02:55:48] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[02:55:49] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[02:55:50] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY, GROUP BY clause'
[02:55:52] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[02:55:53] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY, GROUP BY clause (GENERATE_SERIES)'
[02:55:54] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[02:55:55] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - ORDER BY, GROUP BY clause'
[02:55:56] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[02:55:57] [INFO] testing 'Microsoft Access boolean-based blind - ORDER BY, GROUP BY clause'
[02:55:58] [INFO] testing 'Microsoft Access boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[02:55:59] [INFO] testing 'SAP MaxDB boolean-based blind - ORDER BY, GROUP BY clause'
[02:55:25] [INFO] testing 'SAP MaxDB boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[02:55:27] [INFO] testing 'IBM DB2 boolean-based blind - ORDER BY clause'
[02:55:29] [INFO] testing 'IBM DB2 boolean-based blind - ORDER BY clause (original value)'
[02:55:32] [INFO] testing 'HAVING boolean-based blind - WHERE, GROUP BY clause'
[02:55:33] [INFO] testing 'MySQL > 5.5 boolean-based blind - Stacked queries'
[02:55:34] [INFO] testing 'MySQL < 5.5 boolean-based blind - Stacked queries'
[02:56:51] [INFO] testing 'PostgreSQL boolean-based blind - Stacked queries (GENERATE_SERIES)'
[02:57:51] [INFO] testing 'PostgreSQL boolean-based blind - Stacked queries (IF)'
[02:58:23] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Stacked queries'
[02:58:24] [INFO] testing 'Microsoft Access boolean-based blind - Stacked queries'
[02:59:28] [INFO] testing 'Microsoft Access boolean-based blind - Stacked queries'
[03:00:01] [INFO] testing 'SAP MaxDB boolean-based blind - Stacked queries'
[03:00:34] [INFO] testing 'MySQL > 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[03:01:42] [INFO] testing 'MySQL > 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
```

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

```
File Machine View Input Devices Help
theekshana@Theekshana:~$ nuclei -u cfg.fastly.com
______v_/_/_/_/_/_/_\(_)
____/_/_/_/_/_/_/_/_/_\ v3.3.4
projectdiscovery.io

[INF] Current nuclei version: v3.3.4 (outdated)
[INF] Current nuclei-templates version: v10.0.2 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 68
[INF] Templates loaded for current scan: 8654
[INF] Executing 8455 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 199 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Running httpx on input host
[INF] Found 1 URL from httpx
[INF] Templates clustered: 1613 (Reduced 1517 Requests)
[INF] Using Interactsh Server: oast.fun
[missing-sri] [http] [info] https://manage.fastly.com/configure/services/ ["https://www.googletagmanager.com/gtag/js?id=G-639WJK504N"]
[waf-detect:varnish] [http] [info] https://cfg.fastly.com
[tls-version] [ssl] [info] cfg.fastly.com:443 [*tls12*]
[tls-version] [ssl] [info] cfg.fastly.com:443 [*tls13*]
[dns-saas-service-detection:fastly-cdn] [dns] [info] cfg.fastly.com ["cfg.fastly.com.map.fastly.net"]
[caa-fingerprint] [dns] [info] cfg.fastly.com
[ssl-issuer] [ssl] [info] cfg.fastly.com:443 ["Certainly"]
[ssl-dns-names] [ssl] [info] cfg.fastly.com:443 ["cfg.fastly.com", "zd.fastly.com"]

(theekshana@Theekshana:~)$
```

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

```
File Machine View Input Devices Help
theekshana@Theekshana: ~
$ dmitry cfg.fastly.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:199.232.46.137
HostName:cfg.fastly.com
Gathered Inet-whois information for 199.232.46.137

inetnum: 199.231.236.0 - 199.244.99.255
netname: NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
desc: IPv4 address block not managed by the RIPE NCC
remarks:
remarks: For registration information,
remarks: you can consult the following sources:
remarks: IANA
remarks: http://www.iana.org/assignments/ipv4-address-space
remarks: http://www.iana.org/assignments/iana-ipv4-special-registry
remarks: http://www.iana.org/assignments/ipv4-recovered-address-space
remarks: AFRINIC (Africa)
remarks: http://www.apnic.net/ whois.apnic.net
remarks: APNIC (Asia Pacific)
remarks: http://www.apnic.net/ whois.apnic.net
remarks: ARIN (Northern America)
remarks: http://www.arin.net/ whois.arin.net
remarks: LACNIC (Latin America and the Caribbean)
remarks: http://www.lacnic.net/ whois.lacnic.net
remarks: EU # Country is really world wide
country: IANA-RIPE
tech-c: IANA-RIPE
status: ALLOCATED UNSPECIFIED
mnt-by: RIPE-NCC-HM-MNT
created: 2023-11-06T15:03:10Z
last-modified: 2023-11-06T15:03:10Z
source: RIPE

role: Internet Assigned Numbers Authority
address: see http://www.iana.org/
admin-c: IANA-RIPE
tech-c: IANA-RIPE
nic-hdl: IANA-RIPE
remarks: For more information on IANA services
remarks: go to IANA web site at http://www.iana.org.
mnt-by: RIPE-NCC-HM-MNT
changed: 1970-01-01T00:00:00Z
last-modified: 2001-09-22T09:31:27Z
source: RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.114 (DEXTER)

Gathered Inic-whois information for cfg.fastly.com
ERROR: Unable to locate Name Whois data on cfg.fastly.com
Gathered Netcraft information for cfg.fastly.com
Retrieving Netcraft.com information for cfg.fastly.com
Netcraft.com Information gathered
Gathered Subdomain information for cfg.fastly.com
Searching Google.com:80 ...
Searching Alta Vista.com:80 ...
Found 0 possible subdomain(s) for host cfg.fastly.com, Searched 0 pages containing 0 results
Gathered E-Mail information for cfg.fastly.com
Searching Google.com:80 ...
Searching Alta Vista.com:80 ...
Found 0 E-Mail(s) for host cfg.fastly.com, Searched 0 pages containing 0 results
Gathered TCP Port information for 199.232.46.137

Port      State
22/tcp    open
53/tcp    open
80/tcp    open
```

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.

http://fastly.com/ ↗

Scan Time

: 10/24/2024 1:53:59 PM (UTC+05:30)

Total Requests: 1,134
Average Speed: 15.21/sRisk Level:
MEDIUM

VULNERABILITIES

3
IDENTIFIED**1**
CONFIRMED**0** !
CRITICAL**0** ⚠️
HIGH2 MEDIUM
0 LOW
1 BEST PRACTICE
0 INFORMATION

Identified Vulnerabilities



Confirmed Vulnerabilities



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

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

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

- Lighttpd:

```
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "ECDH+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

The screenshot shows the OWASP ZAP interface in Standard Mode. The main window displays an 'Automated Scan' configuration screen. It includes fields for 'URL to attack' (set to <http://cfg.fastly.com>), 'Spider' type ('Use traditional spider' checked), 'Ajax Spider' type ('If Modern' selected with 'Firefox Headless'), and a 'Progress' bar indicating the scan is complete. On the left, a sidebar shows a tree view of 'Alerts' (12) with various findings like 'CSP: Wildcard Directive', 'CSP: script-src unsafe-inline', etc. The bottom navigation bar includes tabs for History, Search, Alerts, Output, Spider, AJAX Spider, and Active Scan.

This screenshot shows the 'Edit Alert' dialog for a 'CSP: script-src unsafe-inline' alert. The alert details include: URL (<http://cfg.fastly.com>), Risk (Medium), Confidence (High), Parameter (content-security-policy), Attack (script-src), Evidence (<https://app.pendo.io>), CWE ID (693), and WASC ID (15). The 'Description' section explains Content Security Policy (CSP) as a security feature. The 'Solution' section advises setting the Content-Security-Policy header. The 'Reference' section links to external resources like the W3C CSP specification and OWASP A05 and A06 documents. The 'Alert Tags' section lists 'OWASP_2021_A05' and 'OWASP_2017_A06'. The 'Key' and 'Value' columns show the CSP header configuration.

The screenshot shows the 'Requester' tool in the OWASP ZAP interface. It displays a modified HTTP request with several headers added or modified, including 'Content-Security-Policy', 'X-Content-Type-Options', 'X-XSS-Protection', 'X-Frame-Options', and 'X-Content-Security-Policy'. The 'Body: Text' tab shows the modified HTML content. A warning message at the bottom indicates 'Content Modified'.

Burp Suite

Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan

Tasks

- 4. Crawl and audit of fastly.com**
Crawl and Audit - Fast
Finished
Issues: 0 0 0 1
- 3. Crawl and audit of cfg.fastly.com**
Crawl and Audit - Fast
Finished
Issues: 0 0 1 1
- 2. Live audit from Proxy (all traffic)**
Audit checks - passive
Capturing
- 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 fastly.com

Most serious vulnerabilities found (live)

Issue type	Host	Time
TLS certificate	https://fastly.com	13:54:29 24 Oct 2024

Task configuration

Task type: Crawl & audit
Scope: fastly.com
Configuration: Crawl and Audit - Fast

Task progress

Total audit items: 2 Unique locations: 0
Audit items pending: 0 Pending actions: 0
Audit items in progress: 0 Current link depth: 0
Audit items completed: 2 Requests: 240
Network errors: 0

Task log

> Auditing "https://fastly.com/" for Web Cache Deception

Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan

Tasks

- 4. Crawl and audit of fastly.com**
Crawl and Audit - Fast
Finished
Issues: 0 0 0 1
- 3. Crawl and audit of cfg.fastly.com**
Crawl and Audit - Fast
Finished
Issues: 0 0 1 1
- 2. Live audit from Proxy (all traffic)**
Audit checks - passive
Capturing
- 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 fastly.com

Issues

Time	Source	Issue type	Host	Path	Insertion point	Severity
13:54:29 24 Oct 2024	Task 4	TLS certificate	https://fastly.com	/		Information

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

Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan

Tasks

- 4. Crawl and audit of fastly.com**
Crawl and Audit - Fast
Finished
Issues: 0 0 0 1
- 3. Crawl and audit of cfg.fastly.com**
Crawl and Audit - Fast

4. Crawl and audit of fastly.com

Issues

Time	Source	Issue type	Host	Path	Insertion point	Severity
13:54:29 24 Oct 2024	Task 4	TLS certificate	https://fastly.com	/		Information

All issues All issues found by the scanner

Issues

Time	Source	Issue type	Host
13:54:29 24 Oct 2024	Task 4	TLS certificate	https://fastly.com
13:52:43 24 Oct 2024	Task 3	TLS certificate	https://cfg.fastly.com
13:52:43 24 Oct 2024	Task 3	Strict transport security not enforced	https://cfg.fastly.com/robots.txt

1 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 ssstrip 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	<p>Web server applications that rely on User-Agent for filtering or access control.</p> <p>Logging systems that depend on User-Agent headers for tracking user activity.</p> <p>APIs or services that apply specific rules based on User-Agent information.</p>
Impact Assessment	<p>Circumvention of security policies based on User-Agent filtering.</p> <p>Possible exploitation of application vulnerabilities when coupled with other attack vectors.</p> <p>Inaccurate logging and monitoring of user activity, leading to incomplete forensic data.</p> <p>.</p>
Steps to Reproduce	<p>Use a tool like Burp Suite or an HTTP client.</p> <p>Modify the User-Agent header in the request to a custom string or inject malicious payloads .</p> <p>Send the modified request to the server.</p> <p>Observe if the server behaves differently .</p>
Proof of Concept	<pre>curl -A "Mozilla/5.0 (hackedUserAgent)" http://example.com</pre>
Proposed Mitigation or Fix	<p>Avoid reliance on User-Agent headers for access control or security decisions.</p> <p>Implement strict input validation and sanitization for all incoming data, including User-Agent headers.</p> <p>Employ Content Security Policy (CSP) and other protective mechanisms to reduce the impact of injected payloads.</p>

Report 09 Target Details

The screenshot shows the 'Program highlights' section of the report. It includes a summary of compliance (Fully compliant with Platform Standards) and response efficiency (above 90%), managed by HackerOne, with collaboration enabled and includes retesting. Below this are time-to-resolution metrics: 1 day, 16 hours (average time to first response), 4 days, 22 hours (average time to triage), 3 weeks, 2 days (average time to bounty), 3 weeks, 6 days (average time from submission to bounty), and 2 months, 3 weeks (average time to resolution). A 'Rewards summary' table shows rewards for low-severity (Avg. bounty \$146, 20.38% submissions) and medium-severity (Avg. bounty \$505, 20.38% submissions) reports. A 'Submit report' button is at the bottom right.

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](#)

The screenshot shows the homepage of the B.log subdomain on Medium. The header includes the Medium logo, the subdomain B.log, and a 'Join our teams' button. Below the header are category tabs: All Topics (184 posts), Data Science, Design, Development, Infrastructure, Writing, and Product. A section titled 'Newest posts from each category' displays three cards: 'The Engineering Behind Booking.com's Ranking Platform | A System Overview' (Development), 'Meta-experiments: Improving experimentation through experimentation' (Data Science), and 'Unifying Hybrid Clouds: A Journey Through Multi-Control Plane Service Mesh' (Infrastructure). Each card includes a brief description, a 'Read on Medium' link, and a timestamp.

Target Reconnaissance

Nmap Scan

```
theekshana@Theekshana: ~
$ nmap blog.booking.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-24 05:09 EDT
Nmap scan report for blog.booking.com (108.157.254.103)
Host is up (0.017s latency).
Other addresses for blog.booking.com (not scanned): 108.157.254.88 108.157.254.71 108.
rDNS record for 108.157.254.103: server-108-157-254-103.sin2.r.cloudfront.net
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 6.51 seconds
```

(theekshana@Theekshana)-[~]

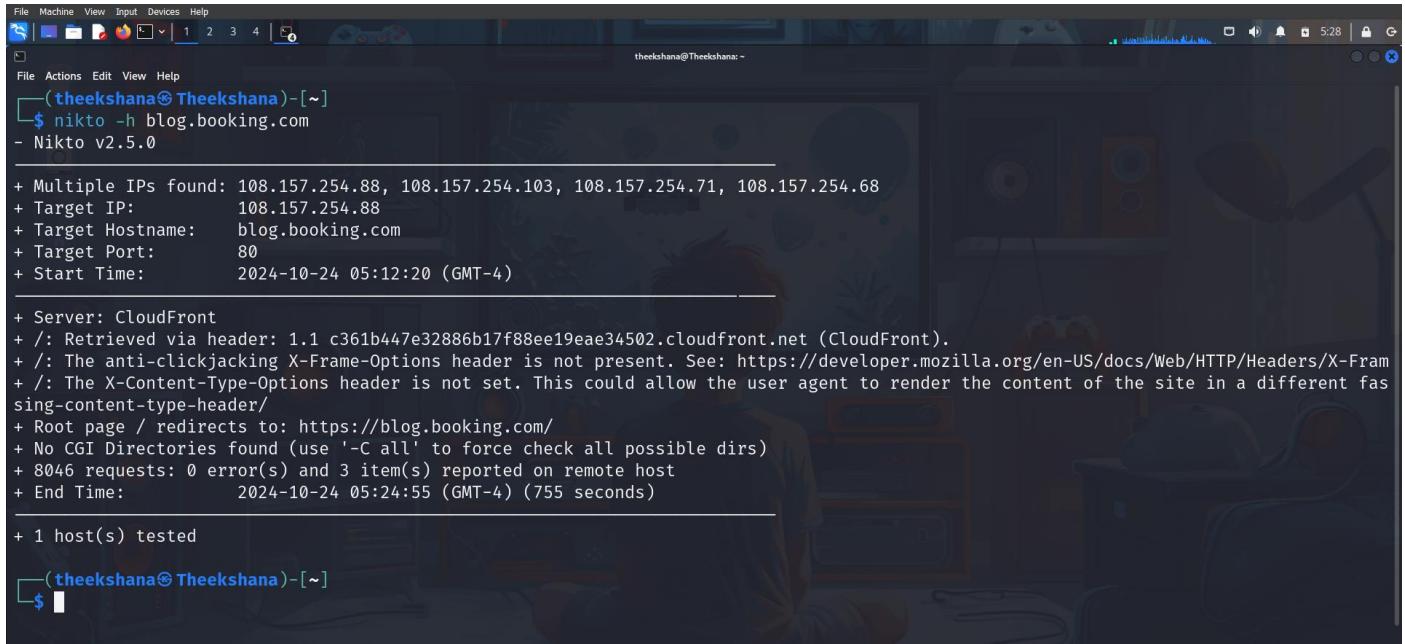
\$

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	HTTPS

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



```
File Machine View Input Devices Help
theekshana@Theekshana: ~
File Actions Edit View Help
(theekshana@Theekshana)-[~]
$ nikto -h blog.booking.com
- Nikto v2.5.0

+ Multiple IPs found: 108.157.254.88, 108.157.254.103, 108.157.254.71, 108.157.254.68
+ Target IP: 108.157.254.88
+ Target Hostname: blog.booking.com
+ Target Port: 80
+ Start Time: 2024-10-24 05:12:20 (GMT-4)

+ Server: CloudFront
+ /: Retrieved via header: 1.1 c361b447e32886b17f88ee19eae34502.cloudfront.net (CloudFront).
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion-content-type-header/
+ Root page / redirects to: https://blog.booking.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 8046 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time: 2024-10-24 05:24:55 (GMT-4) (755 seconds)

+ 1 host(s) tested
(theekshana@Theekshana)-[~]
$
```

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

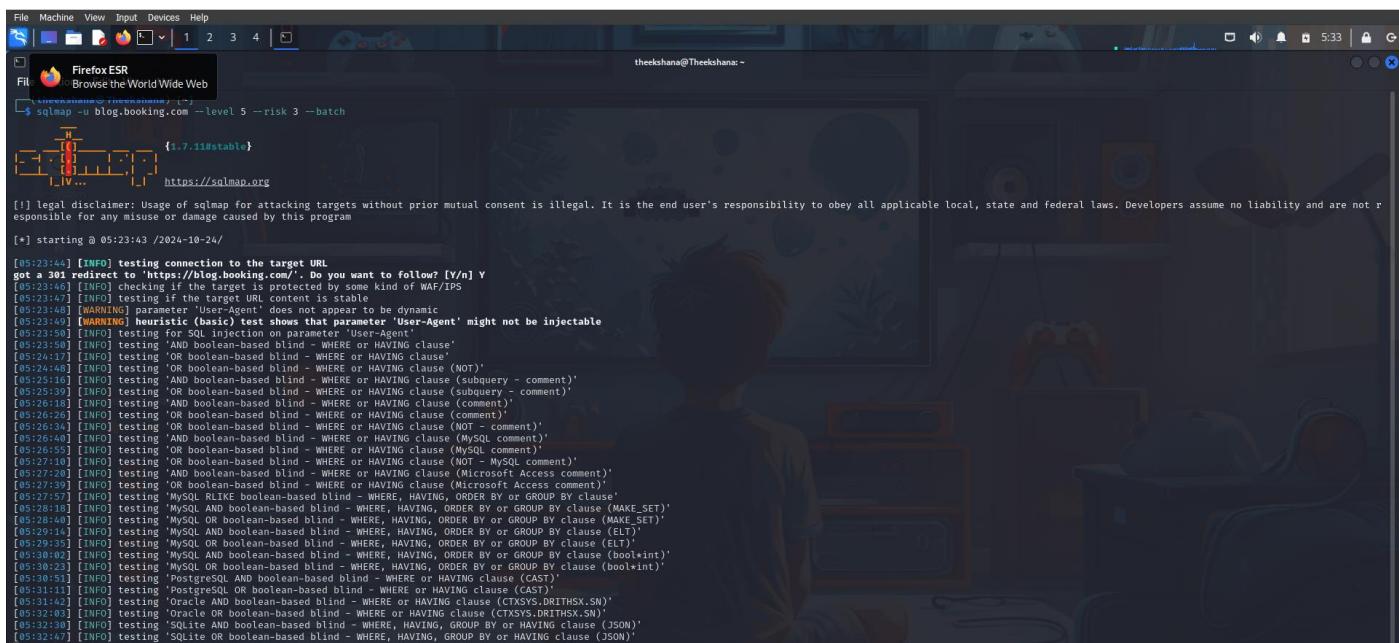
Target Information:

- **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 Scanner



```
File Machine View Input Devices Help
Firefox ESR Browse the World Wide Web
sqlmap -u blog.booking.com --level 5 --risk 3 --batch
{7.11#stable}
https://sqlmap.org

[[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[+] starting @ 05:23:43 /2024-10-24/
[05:23:44] [INFO] testing connection to the target URL
got a 301 redirect to 'https://blog.booking.com/'. Do you want to follow? [y/n] Y
[05:23:46] [INFO] checking if the target is protected by some kind of WAF/IPS
[05:23:47] [INFO] testing if target is protected by static WAF
[05:23:49] [WARNING] parameter 'User-Agent' does not appear to be dynamic
[05:23:50] [INFO] heuristic (basic) test shows that parameter 'User-Agent' might not be injectable
[05:23:50] [INFO] testing for SQL injection on parameter 'User-Agent'
[05:23:50] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[05:24:17] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[05:24:48] [INFO] testing 'NOT AND boolean-based blind - WHERE or HAVING clause (NOT)'
[05:25:13] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[05:25:39] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[05:26:18] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'
[05:26:26] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (comment)'
[05:26:34] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - comment)'
[05:26:42] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[05:26:45] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[05:27:18] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
[05:27:20] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'
[05:27:39] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'
[05:27:57] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'
[05:28:18] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clauses (MAKE_SET)'
[05:29:16] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[05:29:35] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
[05:30:02] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (bool+int)'
[05:30:23] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (bool+int)'
[05:30:31] [INFO] testing 'PostgreSQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (CAST)'
[05:31:42] [INFO] testing 'Oracle AND boolean-based blind - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)'
[05:32:03] [INFO] testing 'Oracle AND boolean-based blind - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)'
[05:32:38] [INFO] testing 'SQLite AND boolean-based blind - WHERE, HAVING, GROUP BY or HAVING clause (JSON)'
[05:32:47] [INFO] testing 'SQLite OR boolean-based blind - WHERE, HAVING, GROUP BY or HAVING clause (JSON)'

[05:31:42] [INFO] testing Oracle AND boolean-based blind - WHERE, HAVING clause (CTXSYS.DRITHSX.SN)
[05:32:03] [INFO] testing Oracle AND boolean-based blind - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)
[05:32:47] [INFO] testing SQLite AND boolean-based blind - WHERE, HAVING, GROUP BY or HAVING clause (JSON)
[05:33:16] [INFO] testing Boolean-based blind - Parameter replace (original value)
[05:33:16] [INFO] testing MySQL boolean-based blind - Parameter replace (MAKE_SET)
[05:33:17] [INFO] testing MySQL boolean-based blind - Parameter replace (MAKE_SET - original value)
[05:33:17] [INFO] testing MySQL boolean-based blind - Parameter replace (ELT)
[05:33:17] [INFO] testing MySQL boolean-based blind - Parameter replace (ELT - original value)
[05:33:18] [INFO] testing MySQL boolean-based blind - Parameter replace (bool+int)
[05:33:18] [INFO] testing MySQL boolean-based blind - Parameter replace (bool+int - original value)
[05:33:19] [INFO] testing PostgreSQL boolean-based blind - Parameter replace
[05:33:19] [INFO] testing PostgreSQL boolean-based blind - Parameter replace (GENERATE_SERIES)
[05:33:20] [INFO] testing PostgreSQL boolean-based blind - Parameter replace (GENERATE_SERIES - original value)
[05:33:21] [INFO] testing Microsoft SQL Server/Sybase boolean-based blind - Parameter replace
[05:33:22] [INFO] testing Oracle boolean-based blind - Parameter replace (original value)
[05:33:22] [INFO] testing Oracle boolean-based blind - Parameter replace (original value)
[05:33:23] [INFO] testing Informix boolean-based blind - Parameter replace (original value)
[05:33:24] [INFO] testing Microsoft Access boolean-based blind - Parameter replace
[05:33:24] [INFO] testing Boolean-based blind - Parameter replace (DUAL)
[05:33:25] [INFO] testing Boolean-based blind - Parameter replace (NULL - original value)
[05:33:26] [INFO] testing Boolean-based blind - Parameter replace (CASE)
[05:33:26] [INFO] testing Boolean-based blind - Parameter replace (CASE - original value)
[05:33:27] [INFO] testing MySQL > 5.0 boolean-based blind - ORDER BY, GROUP BY clause
[05:33:28] [INFO] testing MySQL > 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)
[05:33:29] [INFO] testing MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause
[05:33:29] [INFO] testing MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)
[05:33:30] [INFO] testing PostgreSQL boolean-based blind - ORDER BY, GROUP BY clause
[05:33:31] [INFO] testing PostgreSQL boolean-based blind - ORDER BY clause (original value)
[05:33:32] [INFO] testing Microsoft SQL Server/Sybase boolean-based blind - ORDER BY clause
[05:33:33] [INFO] testing Microsoft SQL Server/Sybase boolean-based blind - ORDER BY clause (original value)
[05:33:33] [INFO] testing Oracle boolean-based blind - ORDER BY, GROUP BY clause
[05:33:33] [INFO] testing Microsoft Access boolean-based blind - ORDER BY, GROUP BY clause
[05:33:37] [INFO] testing SAP MaxDB boolean-based blind - ORDER BY, GROUP BY clause (original value)
[05:33:38] [INFO] testing SAP MaxDB boolean-based blind - ORDER BY, GROUP BY clause (original value)
[05:33:40] [INFO] testing IBM DB2 boolean-based blind - ORDER BY, GROUP BY clause (original value)
[05:33:43] [INFO] testing HAVING boolean-based blind - WHERE, GROUP BY clause
[05:33:59] [INFO] testing MySQL > 5.0 boolean-based blind - Stacked queries
[05:34:12] [INFO] testing MySQL < 5.0 boolean-based blind - Stacked queries
[05:34:13] [INFO] testing PostgreSQL boolean-based blind - Stacked queries
[05:34:25] [INFO] testing PostgreSQL boolean-based blind - Stacked queries (GENERATE_SERIES)
[05:34:37] [INFO] testing Microsoft SQL Server/Sybase boolean-based blind - Stacked queries (IF)
[05:34:55] [INFO] testing Microsoft SQL Server/Sybase boolean-based blind - Stacked queries
```

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

```
File Machine View Input Devices Help
theekshana@Theekshana: ~
$ nuclei -u blog.booking.com
[INFO] Current nuclei version: v3.3.4 (unreleased)
[INFO] Current nuclei-templates version: v10.0.2 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 68
[INF] Templates loaded for current scan: 8654
[INF] Executing 53 assigned templates from projectdiscovery/nuclei-templates
[WRN] Providing 399 assigned templates for scan. Use with caution.
[LIN] Targets loaded for current scan: 1
[LIN] Running httpx on input host
[LIN] Found 1 URIs from httpx
[LIN] Templates clustered: 1613 (Reduced 1517 Requests)
[LIN] Using scanner: Server: oast.pro
[DISCOVER] [http] [info] https://blog.booking.com ["https://www.googletagmanager.com/gtag/js?id=G-B50GQ2SBDL","https://cdn.cookielaw.org/consent/c1551684-cfc2-4b13-90e9-9c2d27a4aa7a/0tAutoBlock.js","https://cdn.cookielaw.org/scriptt
emplate/ox5D0Stub.js"]
[waf-detect:cloudfront] [http] [info] https://blog.booking.com
[waf-detect:ngingeneric] [http] [info] https://blog.booking.com
[HTTP-VIEWER] [http] [info] https://blog.booking.com:443 [title]
[allow-redirect] [call] [info] https://blog.booking.com:443 [title]
[fp-fingerprint] [http] [info] https://blog.booking.com
[http-missing-security-headers:referrer-policy] [http] [info] https://blog.booking.com
[http-missing-security-headers:clear-site-data] [http] [info] https://blog.booking.com
[http-missing-security-headers:permissions-policy] [http] [info] https://blog.booking.com
[http-missing-security-headers:frame-options] [http] [info] https://blog.booking.com
[http-missing-security-headers:cross-site-cookies-domain-policy] [http] [info] https://blog.booking.com
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] https://blog.booking.com
[http-missing-security-headers:cross-origin-openner-policy] [http] [info] https://blog.booking.com
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] https://blog.booking.com
[http-missing-security-headers:content-security-policy] [http] [info] https://blog.booking.com
[http-missing-security-headers:x-content-type-options] [http] [info] https://blog.booking.com
[aws-detected:aws-cloudfront] [http] [info] https://blog.booking.com
[xss-deprecated-header] [http] [info] https://blog.booking.com ["1; mode-block"]
[aws-cloudfront] [http] [info] https://blog.booking.com
[nameserver-fingerprint] [dns] [info] blog.booking.com ["ns-107.awsdns-13.com.", "ns-1192.awsdns-21.org.", "ns-658.awsdns-18.net.", "ns-1912.awsdns-47.co.uk."]
[dns-saas-service-detection:amazon-cloudfront] [dns] [info] blog.booking.com ["d5alhxfppqeb.cloudfront.net"]
[caa-fingerprint] [dns] [info] blog.booking.com
[ssl-dns-name] [ssl] [info] blog.booking.com:443 ["*.booking.com","booking.com"]
[wildcard-tls] [ssl] [info] blog.booking.com:443 ["SAN": ["*.booking.com booking.com"], "CN": *.booking.com"]

theekshana@Theekshana: ~
```

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

```
File Machine View Input Devices Help
(theekshana@Theekshana) [~]
dmitry blog.booking.com
Deepmagic Information Gathering Tool
"There are some deep magic going on"

HostIP:108.157.254.71
HostName:blog.booking.com
Gathered Inet-whois information for 108.157.254.71

inetnum: 108.60.32.0 - 108.179.63.255
netname: NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
desc: IPv4 address block not managed by the RIPE NCC
remarks:
remarks:
For registration information,
you can consult the following sources:
remarks: IANA
http://www.iana.org/assignments/ipv4-address-space
http://www.iana.org/assignments/iana-ipv4-special-registry
http://www.iana.org/assignments/ipv4-recovered-address-space
remarks: AFRINIC (Africa)
http://www.afrinic.net/ whois.afrinic.net
remarks: APNIC (Asia Pacific)
http://www.apnic.net/ whois.apnic.net
remarks: ARIN (Northern America)
http://www.arin.net/ whois.arin.net
remarks: LACNIC (Latin America and the Caribbean)
http://www.lacnic.net/ whois.lacnic.net
remarks:
remarks: EU # Country is really world wide
country: IANA-RIPE
admin-c: IANA-RIPE
tech-c: IANA-RIPE
nic-hdl: IANA-RIPE
status: ALLOCATED UNSPECIFIED
mnt-by: RIPE-NCC-HM-MNT
created: 2024-03-05T15:08:33Z
last-modified: 2024-03-05T15:08:33Z
source: RIPE

role: Internet Assigned Numbers Authority
address: see http://www.iana.org/
admin-c: IANA-RIPE
tech-c: IANA-RIPE
nic-hdl: IANA-RIPE

File Machine View Input Devices Help
(theekshana@Theekshana) [~]
File Actions Edit View Help
admin-c: IANA-RIPE
tech-c: IANA-RIPE
nic-hdl: IANA-RIPE
Port: 80
For more information on IANA services
remarks: go to IANA web site at http://www.iana.org.
mnt-by: RIPE-NCC-MNT
created: 1970-01-01T00:00:00Z
last-modified: 2001-09-22T09:31:27Z
source: RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.114 (ABERDEEN)

Gathered Inic-whois information for blog.booking.com
ERROR: Unable to locate Name Whois data on blog.booking.com
Gathered Netcraft information for blog.booking.com

Retrieving Netcraft.com information for blog.booking.com
Netcraft.com Information gathered

Gathered Subdomain information for blog.booking.com
Searching Google.com:80...
Searching Altavista.com:80...
Found 0 possible subdomain(s) for host blog.booking.com, Searched 0 pages containing 0 results

Gathered E-Mail information for blog.booking.com
Searching Google.com:80...
Searching Altavista.com:80...
Found 0 E-Mail(s) for host blog.booking.com, Searched 0 pages containing 0 results

Gathered TCP Port information for 108.157.254.71

Port      State
21/tcp    open
53/tcp    open
80/tcp    open

Portscan Finished: Scanned 150 ports, 0 ports were in state closed

All scans completed, exiting
(theekshana@Theekshana) [~]
```

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

Detailed Scan Report

http://blog.booking.com/ | Scan Time : 10/24/2024 3:12:42 PM (UTC+05:30)

Total Requests: 1,530 Average Speed: 6.0/s

Risk Level: **MEDIUM**

VULNERABILITIES	IDENTIFIED	CONFIRMED	CRITICAL	HIGH	MEDIUM	LOW
	6	1	0 !	0	1	1
	IDENTIFIED	CONFIRMED	CRITICAL	HIGH	MEDIUM	LOW

BEST PRACTICE	INFORMATION
4	0

Identified Vulnerabilities

Critical	High	Medium	Low	Best Practice	Information	TOTAL
0	0	1	1	4	0	6

Confirmed Vulnerabilities

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

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 ! | 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. https://blog.booking.com/ | CONFIRMED

Hide Remediation

Actions to Take

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

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

- 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

The screenshot shows the OWASP ZAP interface with an 'Automated Scan' configuration window open. The URL 'http://blog.booking.com' is entered in the 'URL to attack:' field. The 'Attack' button is highlighted. Below the main window, the 'Alerts' tab is selected in the bottom navigation bar, showing a list of 5 detected issues:

- Content Security Policy (CSP) Header Not Set (5 occurrences)
- Missing Anti-clickjacking Header (2)
- Cross-Domain JavaScript Source File Inclusion (1)
- X-Content-Type-Options Header Missing (4)
- Re-examine Cache-control Directives (1)

The screenshot shows the 'Edit Alert' dialog for the 'Re-examine Cache-control Directives' alert. The alert details are as follows:

- 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.

The 'Solution' section suggests setting the cache-control HTTP header to "no-cache, no-store, must-revalidate". The 'Reference' section links to various resources on CSP and cache-control headers.

The screenshot shows the 'Requester' tab with a captured response from https://blog.booking.com. The response body is displayed in a monospaced text area:

```
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: "6692d2e9-392d0"
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>
</head>
```

The 'Alerts' tab is selected at the bottom, showing the same 5 alerts as the previous screenshots.

Burp Suite

Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan

Tasks

- 3. Crawl and audit of blog.booking.com**
Crawl and Audit - Fast
Paused
Issues: 0 0 0 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

Most serious vulnerabilities found (live)

Issue type	Host	Time
Cookie manipulation (DOM-based)	https://blog.booking...	15:16:23 24 Oct 202...
Cachable 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 Clickjacking)	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

Task type: Crawl & audit
Scope: blog.booking.com
Configuration: Crawl and Audit - Fast

Task progress

Total audit items: 7 Unique locations: 5
Audit items pending: 0 Pending actions: 0
Audit items in progress: 7 Current link depth: 0
Audit items completed: 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 Description
- Auditing "https://blog.booking.com/robots.txt" for Backup File Append Extension
- Auditing "https://blog.booking.com/robots.txt" for Backup File Prefix Filename
- Auditing "https://blog.booking.com/robots.txt" for Backup File Append Filename
- Auditing "https://blog.booking.com/robots.txt" for Backup File 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 Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan

Tasks

- 3. Crawl and audit of blog.booking.com**
Crawl and Audit - Fast
Paused
Issues: 0 0 0 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

Issues

Time	Source	Issue type	Host	Path	Insertion point	Severity
15:16:26 24 Oct 2024	Task 3	User agent-dependent response	https://blog.booking...	/robots.txt		Informational
15:16:23 24 Oct 2024	Task 3	Cookie manipulation (DOM-based)	https://blog.booking...	/		Low
15:16:21 24 Oct 2024	Task 3	Path-relative style sheet import	https://blog.booking...	/		Informational
15:16:23 24 Oct 2024	Task 3	Cross-domain script include	https://blog.booking...	/		Informational
15:15:44 24 Oct 2024	Task 3	HTML does not specify charset	https://blog.booking...	/robots.txt		Informational
15:15:44 24 Oct 2024	Task 3	Cachable HTTPS response	https://blog.booking...	/		Informational
15:15:43 24 Oct 2024	Task 3	Frameable response (potential Clickjacking)	https://blog.booking...	/		Informational
15:15:36 24 Oct 2024	Task 3	TLS certificate	https://blog.booking...	/		Informational

Advisory Request Response Dynamic analysis Path to issue

Cookie manipulation (DOM-based)

Severity: Low Confidence: Firm URL: https://blog.booking.com/

Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahan

Tasks

- 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

Issues

Time	Source	Issue type	Host	Path	Insertion point	Severity
15:16:26 24 Oct 2024	Task 3	User agent-dependent response	https://blog.booking...	/robots.txt		Informational
15:16:23 24 Oct 2024	Task 3	Cookie manipulation (DOM-based)	https://blog.booking...	/		Low
15:16:21 24 Oct 2024	Task 3	Path-relative style sheet import	https://blog.booking...	/		Informational
15:15:44 24 Oct 2024	Task 3	Cross-domain script include	https://blog.booking...	/		Informational
15:15:44 24 Oct 2024	Task 3	HTML does not specify charset	https://blog.booking...	/robots.txt		Informational
15:15:44 24 Oct 2024	Task 3	Cachable HTTPS response	https://blog.booking...	/		Informational
15:15:43 24 Oct 2024	Task 3	Frameable response (potential Clickjacking)	https://blog.booking...	/		Informational
15:15:36 24 Oct 2024	Task 3	TLS certificate	https://blog.booking...	/		Informational

Advisory Request Response Path to issue

Pretty Raw Hex Render

```
35: }</script>
36:
37: <link rel="stylesheet" href="main.css">
38: <meta name="viewport" content="width=device-width, initial-scale=1" />
39: <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 scale." />
40: <meta property="og:title" content="Booking.com Blog" />
41: <meta property="og:type" content="blob" />
42: <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 designers and writers, developers, database engineers and Sysadmins are solving complicated problems at huge scale." />
```

Inspector

Response headers 14

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	<p>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.</p> <p>Web servers : If configured to allow weak ciphers, these servers could expose HTTPS traffic to attacks .</p> <p>VPN servers: Encryption between clients and the VPN server may be weak, risking exposure of sensitive corporate data.</p> <p>Email servers: Email communications protected by weak ciphers can be intercepted and decrypted.</p> <p>Client-server applications: Any custom or commercial application that uses weak ciphers for encryption in transit.</p>
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	<p>Disable weak ciphers in the system's configuration files .</p> <p>Implement stronger ciphers such as AES or GCM-based ciphers.</p> <p>Regularly review and update SSL/TLS configurations to adhere to the latest security best practices.</p>

Report 10 Target Details

The screenshot shows a bug bounty report for the domain render.com. On the left, there's a sidebar with various icons and a navigation menu. The main content area includes sections for 'Program highlights' (listing 'Gold Standard' and 'Platform Standards'), performance metrics (response time, triage time, bounty time, resolution time), 'Scope exclusions' (mentioning Core Ineligible Findings), and an 'Overview' section. A 'Stats' panel on the right tracks reports received, last report resolved, reports resolved, hackers thanked, and assets in scope. A 'Submit report' button is also visible.

The target for this Bug Bounty report is [render.com](https://www.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](#)

The screenshot shows the homepage of the Render website. It features a top navigation bar with links for Product, Pricing, Blog, Docs, Changelog, Careers, About, Contact, Sign In, and Get Started. A green banner at the top announces 'New: Flexible Plans for Render PostgreSQL' with a 'Learn more >' link. The main visual is a large, abstract graphic composed of a grid of purple and black squares. To the left of the graphic, the text 'Your fastest path to production' is displayed in a large, white, sans-serif font. Below this, a smaller text block reads: 'Build, deploy, and scale your apps with unparalleled ease – from your first user to your billionth.'

Target Reconnaissance

Nmap Scan

```
theekshana@Theekshana: ~
$ nmap onrender.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-24 06:19 EDT
Nmap scan report for onrender.com (34.83.64.96)
Host is up (0.021s latency).
rDNS record for 34.83.64.96: 96.64.83.34.bc.googleusercontent.com
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

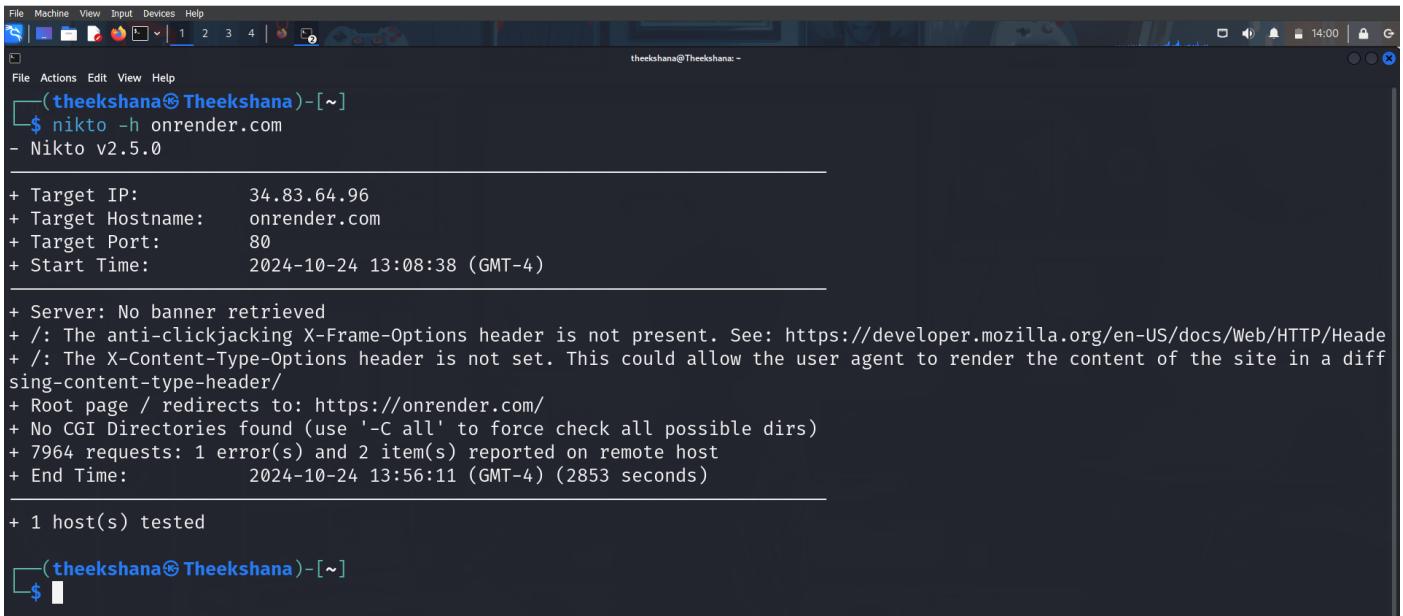
Nmap done: 1 IP address (1 host up) scanned in 31.51 seconds
```

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	HTTPS

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



```
(theekshana@Theekshana)-[~]
$ nikto -h onrender.com
- Nikto v2.5.0

+ Target IP:      34.83.64.96
+ Target Hostname: onrender.com
+ Target Port:     80
+ Start Time:    2024-10-24 13:08:38 (GMT-4)

+ Server: No banner retrieved
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different content-type-header/
+ Root page / redirects to: https://onrender.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7964 requests: 1 error(s) and 2 item(s) reported on remote host
+ End Time:       2024-10-24 13:56:11 (GMT-4) (2853 seconds)

+ 1 host(s) tested

(theekshana@Theekshana)-[~]
$
```

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 Scanner

```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
theekshana@Theekshana: ~
$ sqlmap -h
{ 1.7.11#stable }
https://sqlmap.org

Usage: python3 sqlmap [options]

Options:
-h, --help Show basic help message and exit
-hh Show advanced help message and exit
--version Show program's version number and exit
-v VERBOSE Verbosity level: 0-6 (default 1)

Target:
At least one of these options has to be provided to define the target(s)

-u URL, --url=URL Target URL (e.g. "http://www.site.com/vuln.php?id=1")
-g GOOGLEDORK Process Google dork results as target URLs

Request:
These options can be used to specify how to connect to the target URL

--data=DATA Data string to be sent through POST (e.g. "id=1")
--cookie=COOKIE HTTP Cookie header value (e.g. "PHPSESSID=a8d127e..")
--random-agent Use randomly selected HTTP User-Agent header value
--proxy=PROXY Use a proxy to connect to the target URL
--tor Use Tor anonymity network
--check-tor Check to see if Tor is used properly

Injection:
These options can be used to specify which parameters to test for,
provide custom injection payloads and optional tampering scripts
```

```
File Machine View Input Devices Help
theekshana@Theekshana: ~
$ sqlmap -u onrender.com --level 5 --risk 3 --batch
{ 1.7.11#stable }
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 14:12:54 /2024-10-24

[14:12:55] [INFO] testing connection to the target URL
got a 301 redirect to 'https://onrender.com/'. Do you want to follow? [Y/n] Y
[14:12:58] [INFO] checking if the target is protected by some kind of WAF/IPS
[14:13:00] [INFO] testing if the target URL content is stable
[14:13:02] [WARNING] parameter 'User-Agent' does not appear to be dynamic
[14:13:03] [WARNING] heuristic (basic) test shows that parameter 'User-Agent' might not be injectable
[14:13:06] [INFO] testing if the target supports 'User-Agent'
[14:13:07] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[14:13:07] [CRITICAL] WAF/IPS identified as 'CloudFlare'
[14:14:33] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[14:16:03] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT)'
[14:16:53] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[14:17:00] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[14:18:16] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'
[14:18:33] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (comment)'
[14:18:56] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - comment)'
[14:19:07] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[14:19:48] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[14:20:34] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'
[14:21:27] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'
[14:22:04] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'
[14:22:54] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[14:23:56] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[14:26:08] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
[14:26:09] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[14:26:09] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[14:26:13] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
[14:26:30] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[14:27:47] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (bool+int)'
[14:28:20] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (bool+int)'
[14:29:16] [INFO] testing 'PostgreSQL AND boolean-based blind - WHERE or HAVING clause (CAST)'
[14:30:39] [INFO] testing 'PostgreSQL OR boolean-based blind - WHERE or HAVING clause (CAST)'
[14:32:06] [INFO] testing 'Oracle AND boolean-based blind - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)'
[14:32:57] [INFO] testing 'Oracle AND boolean-based blind - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)'
[14:34:26] [INFO] testing 'SQLite AND boolean-based blind - WHERE, HAVING, GROUP BY or HAVING clause (JSON)'
[14:35:09] [INFO] testing 'SQLite OR boolean-based blind - WHERE, HAVING, GROUP BY or HAVING clause (JSON)'
[14:36:27] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
```

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

```
File Machine View Input Devices Help
(theekshana@Theekshana)-[~]
$ nuclei -u onredner.com
v3.3.4
projectdiscovery.io

[INF] Current nuclei version: v3.3.4 (outdated)
[INF] Current nuclei-templates version: v10.0.2 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 68
[INF] Templates loaded for current scan: 8654
[INF] Executing 8455 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 199 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Running httpx on input host
[INF] Found 1 URL from httpx
[INF] Templates clustered: 1613 (Reduced 1517 Requests)
[INF] Using Interactsh Server: oast.live
[INF] Skipped onredner.com:443 from target list as found unresponsive 30 times
[nameserver-fingerprint] [dns] [info] onredner.com ["ns11.abovedomains.com.", "ns12.abovedomains.com."]
[mx-fingerprint] [dns] [info] onredner.com ["10 park-mx.above.com."]
[caa-fingerprint] [dns] [info] onredner.com
[spf-record-detect] [dns] [info] onredner.com ["v=spf1 ip6:fdcf:abda:4154::/48 -all"]
[txt-fingerprint] [dns] [info] onredner.com ["v=spf1 ip6:fdcf:abda:4154::/48 -all"]

(theekshana@Theekshana)-[~]
$
```

Scan Status:

- **Targets Loaded:** 1 target (onredner.com) is being scanned.
- **Running httpx on input host:** The scan is running a tool that processes the target URL(s).
- **Found 1 URL from httpx:** 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

```
File Machine View Input Devices Help
theekshana@Theekshana: ~
Deepmagic Information Gathering Tool
"There be some deep magic going on"
HostIP:34.83.64.96
HostName:onrender.com
Gathered Inet-whois information for 34.83.64.96

inetnum: 32.0.0.0 - 36.255.91.255
netname: NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
desc: IPv4 address block not managed by the RIPE NCC
remarks:
remarks:
remarks: For registration information,
remarks: you can consult the following sources:
remarks: IANA
remarks: http://www.iana.org/assignments/ipv4-address-space
remarks: http://www.iana.org/assignments/iana-ipv4-special-registry
remarks: http://www.iana.org/assignments/ipv4-recovered-address-space
remarks: APNIC
remarks: AFRINIC (Africa)
remarks: http://www.apnic.net/ whois.apnic.net
remarks: ARIN (Asia Pacific)
remarks: http://www.arin.net/ whois.arin.net
remarks: ARIN (Northern America)
remarks: http://www.lacnic.net/ whois.lacnic.net
remarks: LACNIC (Latin America and the Caribbean)
remarks: http://www.ripe.net/ whois.ripe.net
remarks:
country: EU # Country is really world wide
admin-c: IANAI-RIPE
tech-c: IANAI-RIPE
status: ALLOCATED-UNSPECIFIED
mnt-by: RIPE-DB-EM-MNT
created: 2019-04-16T15:48:11Z
last-modified: 2019-04-16T15:48:11Z
source: RIPE

Role: Internet Assigned Numbers Authority
address: see http://www.iana.org.
admin-c: IANAI-RIPE
tech-c: IANAI-RIPE
nic-hdl: IANAI-RIPE
```

```
File Machine View Input Devices Help
theekshana@Theekshana: ~
File Actions Edit View Help
Gathered Netcraft information for onrender.com

Retrieving Netcraft.com information for onrender.com
Netcraft.com Information gathered

Gathered Subdomain information for onrender.com

Searching Google.com:80 ...
HostName:render-web.onrender.com
HostIP:216.24.57.252
HostName:render-onrender.com
HostIP:216.24.57.4
HostName:www.whosonrender.com
HostIP:216.24.57.252
HostName:certificadosapp.onrender.com
HostIP:216.24.57.252
HostName:awards.onrender.com
HostIP:216.24.57.252
HostName:geobits.onrender.com
HostIP:216.24.57.252
HostName:wp-content.onrender.com (1517 Requests)
HostName:vsp-app.onrender.com
HostIP:216.24.57.252
HostName:api.onrender.com
HostIP:216.24.57.4
HostName:hp-ap1.onrender.com
HostIP:216.24.57.4
HostName:cono.onrender.com
HostIP:216.24.57.252
HostName:scrapetutorial-doc.onrender.com
HostIP:216.24.57.252
HostName:gold-bl.onrender.com
HostIP:216.24.57.4
Searching Altavista.com:80...
Found 12 possible subdomain(s) for host onrender.com, Searched 0 pages containing 0 results

Gathered E-Mail information for onrender.com

Searching Google.com:80 ...
Searching Altavista.com:80...
Found 0 E-Mail(s) for host onrender.com, Searched 0 pages containing 0 results

Gathered TCP Port information for 34.83.64.96

Port      State
21/tcp    open
53/tcp    open
80/tcp    open
```

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.

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

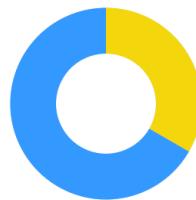
VULNERABILITIES

9
IDENTIFIED3
CONFIRMED0 !
CRITICAL0 !
HIGH0 !
MEDIUM
1 !
LOW3 !
BEST PRACTICE
5 !
INFORMATION

Identified Vulnerabilities



Confirmed Vulnerabilities



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-eval 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

The screenshot shows the OWASP ZAP interface during an automated scan of <http://onrender.com>. The 'Alerts' section (highlighted with a red box) contains four entries:

- Content Security Policy (CSP) Header Not Set
- Strict-Transport-Security Header Not Set (3)
- Information Disclosure - Suspicious Comments
- Modern Web Application

The main panel displays the 'Automated Scan' configuration, including the URL, spider type, and attack options.

The screenshot shows the 'Edit Alert' dialog for the 'Content Security Policy (CSP) Header Not Set' alert. The alert details are as follows:

- 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 video.
- Other Info:

The 'Solution' section suggests ensuring the web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

The screenshot shows the 'Requester' tab displaying a captured HTTP response. The response header includes:

- HTTP/1.1 200 OK
- Date: Thu, 24 Oct 2024 10:59:25 GMT
- Content-Type: text/html; charset=utf-8
- Connection: keep-alive
- CF-Ray: 8d97513e8c392f9-CMB
- CF-Cache-Status: DYNAMIC
- Cache-Control: public, max-age=0, s-maxage=300
- ETag: W/"5f89e9a45766fb22296ca141bdde99"

The response body contains a JSON object with fields like 'key', 'type', 'text', and 'children'. A note at the bottom of the body states: "We may share your personal information in the instances described below. For further information, please refer to our privacy policy." The 'Alerts' section at the bottom shows two additional alerts related to CSP and Strict-Transport-Security headers.

Burp Suite

Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Theekshana Sahaan

Task configuration

Task progress

Task log

Issue type

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 Referrer leakage	https://render.com	16/21/35 24 Oct 202...
Cross-domain Referrer 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...
TLS certificate	https://render.com	16/21/34 24 Oct 202...

Issues

Issue type

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		Information
16/21/35 24 Oct 2024	Task 4	Email addresses disclosed	https://render.com	/_next/data/GRUjoZS6Yfd9Tu95aQNP9/trust.json		Information
16/21/35 24 Oct 2024	Task 4	Email addresses disclosed	https://render.com	/		Information
16/21/35 24 Oct 2024	Task 4	Cross-domain Referrer leakage	https://render.com	/_next/data/GRUjoZS6Yfd9Tu95aQNP9/blog/fee...		Information
16/21/35 24 Oct 2024	Task 4	Email addresses disclosed	https://render.com	/		Information
16/21/35 24 Oct 2024	Task 4	Email addresses disclosed	https://render.com	/		Information
16/21/35 24 Oct 2024	Task 4	Email addresses disclosed	https://render.com	/		Information
16/21/35 24 Oct 2024	Task 4	Cross-domain Referrer leakage	https://render.com	/_next/data/GRUjoZS6Yfd9Tu95aQNP9/changelo...		Information
16/21/35 24 Oct 2024	Task 4	Cacheable HTTPS response	https://render.com	/		Information
16/21/34 24 Oct 2024	Task 4	TLS certificate	https://render.com	/		Information

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 content in the response body.

Response Headers

Header	Value
HTTP/2 200 OK	
Date	Thu, 24 Oct 2024 10:48:00 GMT
Content-Type	application/json
CF-Ray	8d79645cc83eb2b4f2-CMB
CF-Cache-Status	DYNAMIC
Cache-Control	public, max-age=0, s-maxage=300
ETag	"5ac33a8a5c53ebe82b4b98da774657"
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	<p>HSTS is a security feature that forces web browsers to communicate with servers only via secure HTTPS connections.</p> <p>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.</p>
Affected Components	<p>Web server configuration, specifically the response headers for go.transunion.com</p> <p>Any external site linked from a vulnerable website can receive the referrer URL, which may include sensitive or confidential information.</p>
Impact Assessment	<p>Without HSTS, users may accidentally connect over HTTP, exposing sensitive data to interception.</p> <p>Attackers could exploit this to steal session cookies, login credentials, or other confidential information through downgrading attacks.</p>
Steps to Reproduce	<ol style="list-style-type: none">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	<p>http://go.transunion.com in an unsecured network.</p> <p>Use network analysis tools (e.g., Wireshark) to observe traffic and confirm it's unencrypted.</p>
Proposed Mitigation or Fix	<p>Enable the HSTS policy on the server by adding the Strict-Transport-Security header.</p> <p>This header enforces HTTPS, prevents downgrade attacks, and sets a max age to enforce the policy.</p> <p>Ensure the site supports HTTPS properly before enabling this policy.</p>