

Sri Lanka Institute of Information Technology




WEB SECURITY (IE2062)

BUG BOUNTY REPORT 9

Thilakarathna S.T.D- IT22578914

B.Sc. (Hons) in Information Technology Specializing in cyber
security

Overview of the website



Chime

We're a financial technology company building products that help our members manage money easily. It's your money. It's your life. Chime in.

<https://www.chime.com/> · [@chime](#)

[Submit report](#)

Bug Bounty Program

Launched in Feb 2021

Managed by HackerOne

Includes retesting

Collaboration enabled

[★ Bookmarked](#) [🔔 Subscribe](#)

Reports resolved
84

Assets in scope
24

Average bounty
\$100

[Give feedback](#)

Overview

Scope

Hacktivity

Thanks

Updates (3)

Collaborators

Rewards

Last updated on November 3, 2023. [View changes](#)

Low	Medium	High	Critical
Avg. bounty \$114 64.86% submissions	Avg. bounty \$432 20.27% submissions	Avg. bounty \$1,775 5.41% submissions	Avg. bounty \$7,329 9.46% submissions
\$100	\$500	\$5,000	\$10,000–\$20,000

Our rewards are based on severity per CVSS (the Common Vulnerability Scoring Standard). Please note these are general guidelines, and reward decisions are up to the discretion of Chime Financial, Inc.

Response Efficiency

1 day, 18 hours
Average time to first response

1 week, 2 days
Average time to triage





















3 weeks, 21 hours
Average time from triage to bounty

Leading provider of financial technology, Chime gives people the tools they need to take charge of their finances with cutting-edge banking options. Chime offers fee-free banking services, such as checking and savings accounts, early direct deposit, and a debit card with no additional costs, through its mobile app and web platform. Chime sets itself apart by emphasizing financial inclusion and the customer experience, serving people who might not receive enough attention from traditional banks. With features like real-time transaction alerts and automated savings tools, Chime is dedicated to assisting consumers in developing better financial practices. Furthermore, Chime's dedication to openness and simplicity is well-received by its user base, giving it a dependable and well-liked option for people looking for a contemporary banking experience.







Scope

• InScope

http://member-qa.chime.com/users/sign_in	URL	In scope	Critical	Eligible	Sep 19, 2023	3 (4%)
*.chimecard.com	Wildcard	In scope	Critical	Eligible	Sep 19, 2023	4 (5%)
Chime Android App (Beta) https://app.bitrise.io/app/5bec038cb1e318cd/build/53f4371a-2944-4724-a550-fe28ce12b310/artifact/febf8365737c2830/p/e0d7a0d7d6d1d28d13ae19e6df4bd563	Other	In scope	Critical	Eligible	Sep 12, 2023	0 (0%)
com.onedebit.chime Production Environment Android Chime App: https://play.google.com/store/apps/details?id=com.onedebit.chime	Android: Play Store	In scope	Critical	Eligible	Feb 5, 2021	1 (1%)
PayFriends/PayAnyone Features Pay Friends is a fast and safe way to send money to any of your friends and family through the existing Chime app at the bottom of the app screen. We are open to all findings that show impact but encourage researchers to test for any transactions inconsistencies such as: <ul style="list-style-type: none"> A person sent the money but the money stayed in their account A person sent the money but the recipient didn't receive it and they money was actually moved from the initial account Receive or less money more than is sent 						
*.chmfin.com	Wildcard	In scope	Critical	Eligible	May 15, 2023	0 (0%)
*.chimepayments.com	Wildcard	In scope	Critical	Eligible	May 15, 2023	1 (1%)
https://app.chime.com/	URL	In scope	Critical	Eligible	Oct 10, 2023	0 (0%)
app.chime.com	Domain	In scope	Critical	Eligible	Oct 10, 2023	0 (0%)
Chime iOS App (Beta) https://app.bitrise.io/app/5bec038cb1e318cd/build/164dfc03-f653-49aa-bfa6-f38d1fc449d7/artifact/c7c7c6f5eff4b8ae/p/c615268f8be4ae89f2c07a0a2afc1ae99	Other	In scope	Critical	Eligible	Sep 12, 2023	0 (0%)
*.chimebank.com	Wildcard	In scope	Critical	Eligible	Sep 19, 2023	7 (8%)
*.1debit.com	Wildcard	In scope	Critical	Eligible	Sep 19, 2023	7 (8%)
com.1debit.ChimeProdApp Production Environment iOS Chime App: https://apps.apple.com/us/app/chime-mobile-banking/id836215269	iOS: App Store	In scope	Critical	Eligible	Feb 5, 2021	0 (0%)
*.chime.com	Wildcard	In scope	Critical	Eligible	Sep 19, 2023	27 (32%)

http://member-qa.chime.com/enroll/#/account	URL	In scope	 Critical	 Eligible	Sep 19, 2023	2 (2%)
wp-ci.chime.com	Domain	In scope	 Low	 Eligible	Jul 25, 2023	1 (1%)
wp-dev1.chime.com	Domain	In scope	 Low	 Eligible	Jul 25, 2023	1 (1%)
wp-dev2.chime.com	Domain	In scope	 Low	 Eligible	Jul 25, 2023	1 (1%)
wp-dev3.chime.com	Domain	In scope	 Low	 Eligible	Jul 25, 2023	0 (0%)
wp-dev4.chime.com	Domain	In scope	 Low	 Eligible	Jul 25, 2023	0 (0%)
wp-dev5.chime.com	Domain	In scope	 Low	 Eligible	Jul 25, 2023	0 (0%)
wp-integ.chime.com	Domain	In scope	 Low	 Eligible	Jul 25, 2023	0 (0%)
www.chime.com	Domain	In scope	 Low	 Eligible	Jul 25, 2023	3 (4%)
wp-qa.chime.com	Domain	In scope	 Low	 Eligible	Jul 25, 2023	0 (0%)

• OutScope

careers.chime.com 3rd-party vendor	Domain	Out of scope	 None	 Ineligible	Feb 7, 2022	0 (0%)
*.pantheonsite.io	Wildcard	Out of scope	 None	 Ineligible	Sep 21, 2023	0 (0%)
nd.chime.com 3rd-party vendor	Domain	Out of scope	 None	 Ineligible	Nov 27, 2023	0 (0%)

Information Gathering

Security researchers and ethical hackers must first gather data through bug bounty programs in order to identify vulnerabilities in a target system or application. This step's objective is to learn as much as you can about the target, including its technologies, architecture, known vulnerabilities, and potential weak points. Open-source intelligence gathering (OSINT), network scanning, fingerprinting, and asset enumeration are typically required to give a complete view of the target's attack surface.

Since it enables ethical hackers to identify potential points of entry and focus their search for system security flaws, efficient information gathering is the cornerstone of a successful bug hunting operation.

Subdomains for Hunting

The process of listing sub-domains for one or more domains is called sub-domain enumeration. This is a critical stage in the reconnaissance process. Finding vulnerabilities is made more likely by sub-domain enumeration, which can identify several domains and sub-domains that are part of a security assessment.

Seen through cryptic, abandoned sub-domains, programs may have dangerous bugs.

The same weaknesses are frequently found throughout numerous domains and applications within a single organization.

- **Sublist3r**

Sublist3r is an open-source program used for efficient subdomain enumeration. Penetration testers, security experts, and ethical hackers utilize Sublist3r to locate subdomains linked to a target website. It accomplishes this by using methods like search engine scraping and DNS requests. Sublist3r only needs to know the target domain to begin searching for relevant subdomains. It then provides useful information that can be utilized for vulnerability discovery and security assessments.

```
(tharusha@kali)-[~]  
$ sublist3r -d chime.com
```

SUBLIST3R

Coded By Ahmed Aboul-Ela - @aboul3la

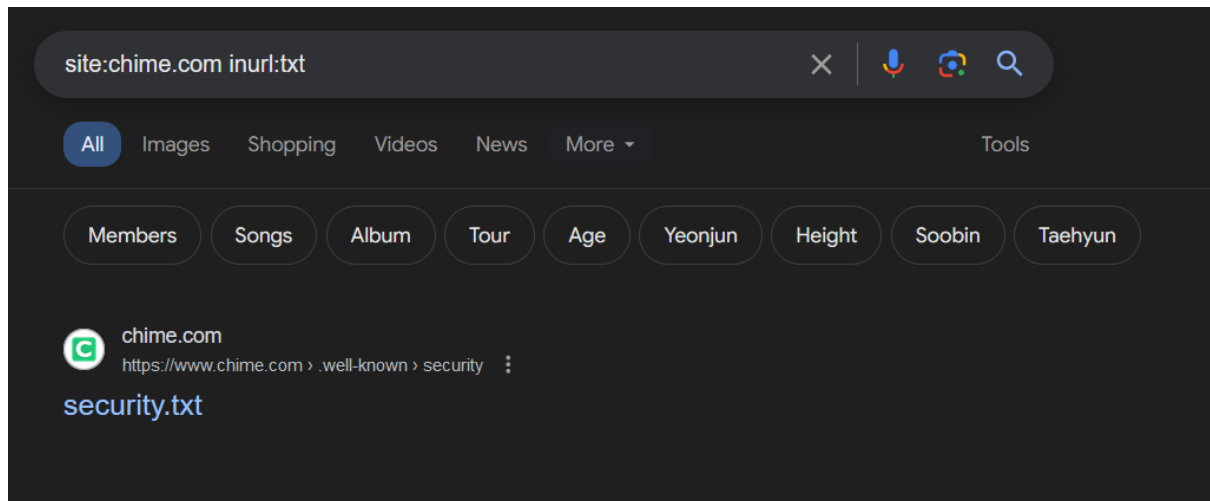
```
[~] Enumerating subdomains now for chime.com  
[~] Searching now in Baidu..  
[~] Searching now in Yahoo..  
[~] Searching now in Google..  
[~] Searching now in Bing..  
[~] Searching now in Ask..  
[~] Searching now in Netcraft..  
[~] Searching now in DNSdumpster..  
[~] Searching now in Virustotal..  
[~] Searching now in ThreatCrowd..  
[~] Searching now in SSL Certificates..  
[~] Searching now in PassiveDNS..  
[!] Error: Virustotal probably now is blocking our requests  
[~] Total Unique Subdomains Found: 43
```

```
www.chime.com  
16002407.account.chime.com  
links.account.chime.com  
affiliates.chime.com  
apply.chime.com  
attachments.chime.com  
careers.chime.com  
datadog-forwarder.chime.com  
datadog-forwarder-nonprod.chime.com  
dev.chime.com  
developer.chime.com  
element.chime.com  
error-pages.chime.com  
email.ethnio.chime.com  
email.gh-mail.ext.chime.com  
flows.chime.com  
email.gh-mail.chime.com  
handbooks.chime.com  
help.chime.com  
help-test.chime.com  
interchange.chime.com  
join.chime.com  
email.mg.chime.com  
migration.chime.com  
mobile-state.chime.com  
nd.chime.com
```

```
16002407.notify.chime.com  
links.notify.chime.com  
office.chime.com  
qa-wp.chime.com  
secure.chime.com  
stage-wp.chime.com  
static-attachments.chime.com  
email.talent.chime.com  
email.teamable.chime.com  
wp-ci.chime.com  
wp-dev1.chime.com  
wp-dev2.chime.com  
wp-dev3.chime.com  
wp-dev4.chime.com  
wp-dev5.chime.com  
wp-integ.chime.com  
wp-qa.chime.com
```

- **Google dorking**

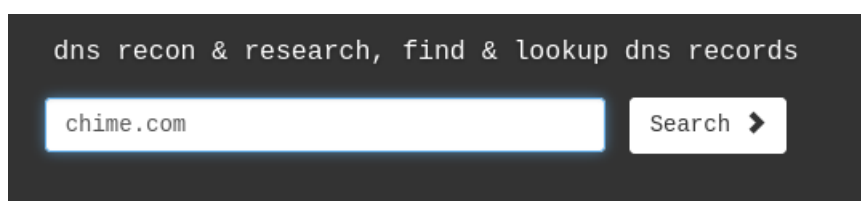
The practice of using specific queries and sophisticated search operators on the Google search engine to locate confidential information, configuration flaws, or publicly accessible resources that are not often indexed in ordinary search results is known as "Google Dorking," sometimes known as "Google Hacking."













































- **Dnsdumpster**

Block addresses, emails, domain names, and other kinds of DNS-related data can be gathered using an online passive scanning tool called DNSdumpster.

Result of chime.com



DNS Servers		
leah.ns.cloudflare.com.      	173.245.58.129	CLOUDFLARENET unknown
marty.ns.cloudflare.com.      	173.245.59.204	CLOUDFLARENET unknown
MX Records ** This is where email for the domain goes...		
10 aspmx.l.google.com.      	172.253.122.27	GOOGLE United States
20 alt1.aspmx.l.google.com.      	209.85.202.26	GOOGLE United States
20 alt2.aspmx.l.google.com.      	64.233.184.27	GOOGLE United States
30 aspmx2.googlemail.com.      	209.85.202.26	GOOGLE United States
30 aspmx3.googlemail.com.      	64.233.184.27	GOOGLE United States

TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations		
"1password-site-verification=IAJ2wLF63FES7LT2IFVWKBFRPQ"		
"_globalsign-domain-verification=2u717_L-vZH0Woo4vjzWv33RxFYl03VYGr9bHE2bww"		
"adobe-idp-site-verification=9255a2d47490b315770bef750c785f470d84ef57dba196d59d15245fd4b2482d"		
"amazon-business-verification=54346d23876622b8dc0ee76404b7774073d5029319eceb7ab98a0101c0383291"		
"apple-domain-verification=F2Eq0gD9eq2McJNX"		
"atlassian-domain-verification=aFWXHNMoLj3p53b1Gj4sS0BfBr16ELPnoMswv7YGw9/4qrc5IwIr9jodRZ5l9YR0"		
"docker-verification=627aeb62-9719-4dcc-98b0-76cc6f2a7373"		
"docusign=7124456e-4284-44f4-988a-ac42a1077e81"		
"facebook-domain-verification=daada16ss2kqrxkswt7khzkovvaite"		
"google-site-verification=-NThK4DnJRDNonjA-vcHEzRIETVqaPYDUDTLkzNyr0c"		
"google-site-verification=1ZQb6WwgsJjTIkNydYiy7InUKnzphb_kLmDRrNDU-sM"		
"google-site-verification=ocRmn5hh014JpsL0kozv9EIjzmGXoTnLJru5dgDrPtM"		
"h1-domain-verification=tyvT4Kxn189c94gaSomk6T8cUVj6pb469hTA9G16Ly32bXTh"		
"infoblox-domain-mastery=433f3ff08e4ef93508f1f3a4b90dc6903f8d4a2a6a21018ecbb93b6886ea353eeb"		
"jamf-site-verification=0-kEI1Q0TacRj8oiz6is_g"		
"loom-site-verification=24596622b5d54cfffabc078dfdd31525c"		
"miro-verification=d095c4615f086c0a9d658eff26c098a580ae39a7"		
"notion-domain-verification=wSDeTFh0JpCDkdb2G2zQcFfg2MgDPSbGZ2uYAzQgcd"		
"onetrust-domain-verification=8b8b52bd2e3a45a99f4807df66a6a9e0"		
"openai-domain-verification=dv-0hs9ErmjBtq6ltcnxPaoyBG8"		
"segment-site-verification=rNjTv8Kz5RIQ2Hef8pLIYgFJDLc2WxR2"		
"v=spf1 include:chime.com._nspf.vali.email include:%{i}._ip.%{h}._ehlo.%{d}._spf.vali.email ~all"		

- **DNSrecon**

For DNS enumeration and reconnaissance, an open-source tool named DNSRecon is utilized. The purpose of gathering information is to assist with penetration testing and security evaluations by providing details on DNS servers, domains, subdomains, and DNS records.


```

(root@kali)-[/home/tharusha]
# dnsrecon -d chime.com
[*] std: Performing General Enumeration against: chime.com...
[-] DNSSEC is not configured for chime.com
[*] SOA leah.ns.cloudflare.com 173.245.58.129
[*] SOA leah.ns.cloudflare.com 172.64.32.129
[*] SOA leah.ns.cloudflare.com 108.162.192.129
[*] SOA leah.ns.cloudflare.com 2a06:98c1:50::ac40:2081
[*] SOA leah.ns.cloudflare.com 2606:4700:50::adf5:3a81
[*] SOA leah.ns.cloudflare.com 2803:f800:50::6ca2:c081
[*] NS leah.ns.cloudflare.com 173.245.58.129
[*] Bind Version for 173.245.58.129 "2024.5.2"
[*] NS leah.ns.cloudflare.com 172.64.32.129
[*] Bind Version for 172.64.32.129 "2024.5.2"
[*] NS leah.ns.cloudflare.com 108.162.192.129
[*] Bind Version for 108.162.192.129 "2024.5.2"
[*] NS leah.ns.cloudflare.com 2a06:98c1:50::ac40:2081
[*] NS leah.ns.cloudflare.com 2606:4700:50::adf5:3a81
[*] NS leah.ns.cloudflare.com 2803:f800:50::6ca2:c081
[*] NS marty.ns.cloudflare.com 173.245.59.204
[*] Bind Version for 173.245.59.204 "2024.5.2"
[*] NS marty.ns.cloudflare.com 172.64.33.204
[*] Bind Version for 172.64.33.204 "2024.5.2"
[*] NS marty.ns.cloudflare.com 108.162.193.204
[*] Bind Version for 108.162.193.204 "2024.5.2"
[*] NS marty.ns.cloudflare.com 2a06:98c1:50::ac40:21cc
[*] NS marty.ns.cloudflare.com 2606:4700:58::adf5:3bcc
[*] NS marty.ns.cloudflare.com 2803:f800:50::6ca2:c1cc
[*] MX alt1.aspmx.l.google.com 173.194.202.27
[*] MX alt2.aspmx.l.google.com 142.250.141.27
[*] MX aspmx2.googlemail.com 173.194.202.27
[*] MX aspmx.l.google.com 64.233.170.27
[*] MX aspmx3.googlemail.com 142.250.141.27
[*] MX alt1.aspmx.l.google.com 2607:f8b0:400e:c00::1b
[*] MX alt2.aspmx.l.google.com 2607:f8b0:4023:c0b::1a
[*] MX aspmx2.googlemail.com 2607:f8b0:400e:c00::1a
[*] MX aspmx.l.google.com 2404:6800:4003:c00::1a
[*] MX aspmx3.googlemail.com 2607:f8b0:4023:c0b::1a
[*] A chime.com 172.64.152.131
[*] A chime.com 104.18.35.125
[*] TXT _dmarc.chime.com v=DMARC1; p=reject; rua=mailto:dmarc_agg@vali.email
[*] Enumerating SRV Records
[-] No SRV Records Found for chime.com

```

- WHOIS

Domain names, IP addresses, and autonomous system numbers (ASNs) can all be found via a database system or a protocol, respectively. It provides information, such as contact details, about the owner of a block of IP addresses or the person who registered a domain name.

```

(root@kali)-[/home/tharusha]
# whois chime.com
Domain Name: CHIME.COM
Registry Domain ID: 1233850_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: http://cscdns.com
Updated Date: 2021-02-08T17:38:01Z
Creation Date: 1997-07-17T04:00:00Z
Registry Expiry Date: 2024-07-16T04:00:00Z
Registrar: CSC Corporate Domains, Inc.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: 8887802723
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: LEAH.NS.CLOUDFLARE.COM
Name Server: MARTY.NS.CLOUDFLARE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-05-10T17:07:07Z <<<

```

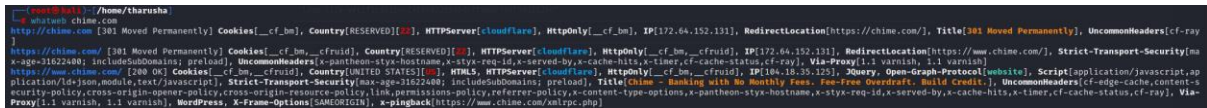
```

Domain Name: chime.com
Registry Domain ID: 1233850_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2021-01-22T00:31:30Z
Creation Date: 1997-07-17T00:00:00Z
Registrar Registration Expiration Date: 2024-07-16T04:00:00Z
Registrar: CSC CORPORATE DOMAINS, INC.
Sponsoring Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: +1.8887802723
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: CSC Corporate Domains, Inc.
Registrant Street: 251 Little Falls Drive
Registrant City: Wilmington
Registrant State/Province: DE
Registrant Postal Code: 19808
Registrant Country: US
Registrant Phone: +1.3026365400
Registrant Phone Ext:
Registrant Fax: +1.3026365454
Registrant Fax Ext:
Registrant Email: admin@internationaladmin.com
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: CSC Corporate Domains, Inc.
Admin Street: 251 Little Falls Drive
Admin City: Wilmington
Admin State/Province: DE
Admin Postal Code: 19808
Admin Country: US
Admin Phone: +1.3026365400
Admin Phone Ext:
Admin Fax: +1.3026365454
Admin Fax Ext:
Admin Email: admin@internationaladmin.com
Registry Tech ID:
Tech Name: DNS Administrator
Tech Organization: CSC Corporate Domains, Inc.
Tech Street: 251 Little Falls Drive
Tech City: Wilmington
Tech State/Province: DE
Tech Postal Code: 19808
Tech Country: US
Tech Phone: +1.3026365400
Tech Phone Ext:
Tech Fax: +1.3026365454
Tech Fax Ext:
Tech Email: dns-admin@cscglobal.com
Name Server: leah.ns.cloudflare.com

```

- **Whatweb**

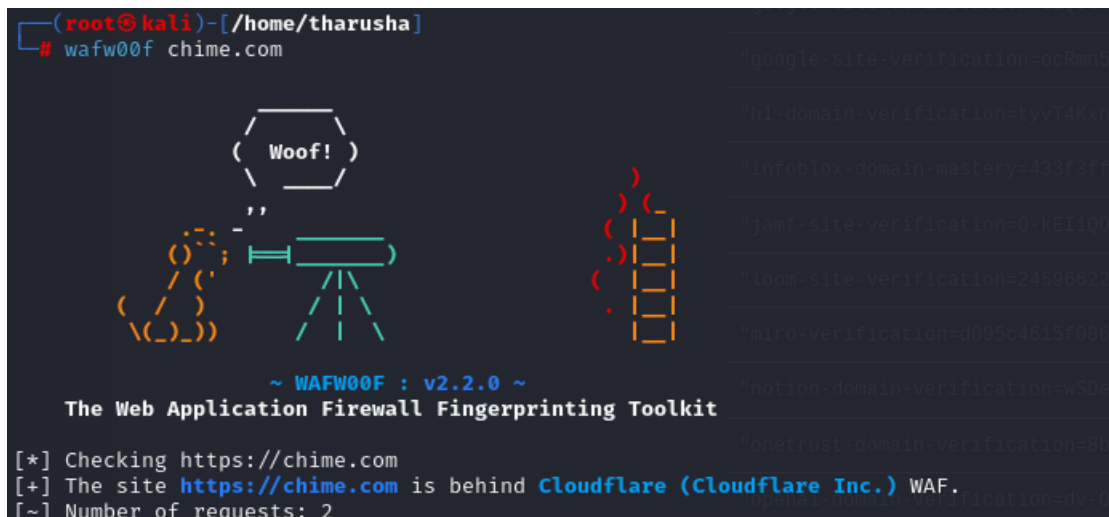
A web application's technology stack can be discovered with this open-source research tool. It analyzes HTTP answers from a target web server to collect further information about the web server, web framework, programming language, content management system (CMS), JavaScript libraries, and other technologies that the target site may be utilizing.



- **Wafw00f**

An open-source program called Wafw00f is used to identify and fingerprint Web application firewalls (WAFs). Web application firewalls (WAFs), security solutions, defend against SQL injection, cross-site scripting (XSS), and other attacks.

We can see that Cloudflare WAF is protecting chime.com.



- **Nslookup**

The command-line tool NSLOOKUP (Name Server Lookup) can be used to query the Domain Name System (DNS) using an IP address or domain name.

```
(root@kali)-[/home/tharusha]
# nslookup chime.com
Server:      192.168.1.1
Address:     192.168.1.1#53
```

```
Non-authoritative answer:
Name:   chime.com
Address: 172.64.152.131
Name:   chime.com
Address: 104.18.35.125
```

```
"loom-site-ve
"miro-verifio
"notion-domai
"onetrust-dow
"openai-doma
```

- **Using nmap, open port enumeration**

Open port enumeration is a method for locating and classifying the open network ports on a target machine or network using the Nmap (Network Mapper) program. Nmap is an effective open-source tool for network scanning and host discovery that provides extensive information on the services and statuses that are running on various ports. This process involves sending specially made packets to a target system and analyzing the responses in order to determine which ports are open and what services are using them.

Nmap is a popular tool for network administrators and security specialists to assess system security, identify potential security flaws, and enhance network configurations due to its abundance of features and versatility. It's a helpful tool for enhancing security and computer network administration in general.

```
(root@kali)-[/home/tharusha]research
# nmap -sS chime.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 13:12 EDT : nmap_resources is deprecated
Nmap scan report for chime.com (104.18.35.125)
Host is up (0.013s latency).
Other addresses for chime.com (not scanned): 172.64.152.131
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https
8080/tcp   open  http-proxy
8443/tcp   open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 4.58 seconds

(root@kali)-[/home/tharusha]research
# nmap --script vuln chime.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 13:12 EDT
Stats: 0:01:35 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.70% done; ETC: 13:14 (0:00:02 remaining)
Nmap scan report for chime.com (104.18.35.125)
Host is up (0.0043s latency).
Other addresses for chime.com (not scanned): 172.64.152.131
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
443/tcp    open  https
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
8080/tcp   open  http-proxy
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 250.81 seconds
```

- **Using Nikto to scan for vulnerabilities**

One method to check for vulnerabilities in Kali Linux is to use the powerful open-source tool Nikto web scanner, which is part of the popular operating system for penetration testing and ethical hacking. Nikto is specifically designed to identify and assess server and web application vulnerabilities.

When checking target web servers for known vulnerabilities, common security issues, and misconfigurations, Nikto can be used from the Kali Linux command line. Nikto searches for issues including outdated software, possibly unsafe scripts, security headers, and other online vulnerabilities. It helps ethical hackers and security professionals understand and reduce such threats by providing comprehensive information on the vulnerabilities discovered.

Exploitation

I employed PWNXSS and SQLMAP tools to identify cross-site and SQL injection vulnerabilities in the target web application for the exploitations.

- **PwnXSS**

PwnXSS is a free and open-source application that may be found on GitHub. This program especially detects cross-site scripting. I execute several payloads in numerous web application directories while testing my target domain for XSS vulnerabilities. After the test, I discovered that indrive.com had no XSS vulnerabilities.

```
(tharusha@kali) ~/PwnXSS
$ python3 pwnxss.py -u https://help.chime.com/hc/en-us/search?query=testing
PWNXSS (v0.5 final)
https://github.com/pwn0sec/PwnXSS
<<<<<< STARTING >>>>>>

[13:26:50] [INFO] Starting PwnXSS ...
[13:26:50] [INFO] Checking connection to: https://help.chime.com/hc/en-us/search?query=testing
[13:26:51] [INFO] Connection established 200
[13:26:51] [WARNING] Found link with query: return_to=https%3A%2F%2Fhelp.chime.com%2Fhc%2Fen-us%2Fsearch%3Fquery%3Dtesting Maybe a vuln XSS point
[13:26:51] [INFO] Query (GET) : https://help.chime.com/hc/en-us/signin?return_to=<script>alert(6000/3000)</script>
[13:26:51] [INFO] Query (GET) : https://help.chime.com/hc/en-us/signin?return_to=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E
[13:26:51] [INFO] Parameter page using (GET) payloads but not 100% yet...
[13:26:51] [WARNING] Found link with query: data=BAh7DjoHaWRskWiXMI058g0d2FjY291bnRfaWRpA%2BTrCzo3dHlwZUkiDGFyZGljbGUGOG02FVDoIdXJsSS3PaHR0cHM6Ly9oZWxwLnMNoaW11LnMvbnV5S9oYy91bi11cy9hcnR0uhU0g5Z2FyZ2hfaWRJiik0ODQyN2FkM01mZj1LRjYVYtYXZlYVYVZmF1NmMzYjMGOWhG0glyYW5raQV6C2xvY2FzZUkiCmVuXVzBjsIVDoKcXVlcn1Jigx0ZXNoaW5uBjsIVDoScmVzdWx0c19jb3VudGkG--bfb93588aa5860c8
[13:26:51] [INFO] Query (GET) : https://help.chime.com/hc/en-us/search/click?data=<script>alert(6000/3000)</script>
[13:26:51] [INFO] Query (GET) : https://help.chime.com/hc/en-us/search/click?data=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E
[13:26:52] [INFO] Parameter page using (GET) payloads but not 100% yet...
[13:26:52] [WARNING] Found link with query: query=testing Maybe a vuln XSS point
[13:26:52] [INFO] Query (GET) : https://help.chime.com/hc/en-us/search?query=<script>alert(6000/3000)</script>
[13:26:52] [INFO] Query (GET) : https://help.chime.com/hc/en-us/search?query=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E
[13:26:52] [WARNING] Found link with query: query=testing Maybe a vuln XSS point
[13:26:52] [INFO] Parameter page using (GET) payloads but not 100% yet...
[13:26:52] [WARNING] Found link with query: query=testing Maybe a vuln XSS point
[13:26:52] [INFO] Query (GET) : https://help.chime.com/hc/en-us/search?query=<script>alert(6000/3000)</script>
[13:26:52] [INFO] Query (GET) : https://help.chime.com/hc/en-us/search?query=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E
[13:26:53] [INFO] Parameter page using (GET) payloads but not 100% yet...
[13:26:53] [WARNING] Found link with query: id=com.onedebit.chime0hl=en Maybe a vuln XSS point
[13:26:53] [INFO] Query (GET) : https://play.google.com/store/apps/details?id=<script>alert(6000/3000)</script>
[13:26:53] [INFO] Query (GET) : https://play.google.com/store/apps/details?id=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E6hl=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E
[13:26:53] [INFO] Parameter page using (GET) payloads but not 100% yet...
[13:26:53] [WARNING] Found link with query: query=testing Maybe a vuln XSS point
[13:26:53] [INFO] Query (GET) : https://help.chime.com/hc/en-us/search?query=<script>alert(6000/3000)</script>
[13:26:53] [INFO] Query (GET) : https://help.chime.com/hc/en-us/search?query=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E
[13:26:53] [WARNING] Found link with query: cid=5900795/ Maybe a vuln XSS point
[13:26:53] [INFO] Parameter page using (GET) payloads but not 100% yet...
[13:26:53] [WARNING] Found link with query: cid=5900795/ Maybe a vuln XSS point
[13:26:53] [INFO] Query (GET) : https://signup.cj.com/member/signup/publisher/?cid=<script>alert(6000/3000)</script>
[13:26:53] [INFO] Query (GET) : https://signup.cj.com/member/signup/publisher/?cid=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E
```

- **SQLmap**

An open-source penetration testing tool called SQL Map automatically locates and takes advantage of SQL injection vulnerabilities to take over databases.

In an attempt to locate any web application injection points, I experimented with various payloads and parameters. I tested this application and discovered that it is not injectable.

```
(root@kali) ~/home/tharusha
$ sqlmap -u 'https://app.chime.com/login'

[+] 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
responsible for any misuse or damage caused by this program

[*] starting @ 13:32:07 /2024-05-10/

[13:32:07] [WARNING] you've provided target URL without any GET parameters (e.g. 'http://www.site.com/article.php?id=1') and without providing any POST parameters through option '--data'
do you want to try URI injections in the target URL itself? [Y/n/q] y
[13:32:09] [INFO] testing connection to the target URL
[13:32:11] [WARNING] the web server responded with an HTTP error code (403) which could interfere with the results of the tests
you have not declared cookie(s), while server wants to set its own ('_cf_bm=RYK7s.CMLTR...x2L5tyoQJw'). Do you want to use those [Y/n] y
[13:32:12] [INFO] checking if the target is protected by some kind of WAF/IPS
[13:32:13] [INFO] testing if the target URL content is stable
[13:32:14] [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 ju
manual paragraph 'Page comparison
how do you want to proceed? [(C)ontinue/(s)tring/(r)egex/(q)uit] y
[13:32:15] [INFO] testing if URI parameter '#i*' is dynamic
[13:32:17] [WARNING] potential permission problems detected ('Access denied')
[13:32:17] [WARNING] URI parameter '#i*' does not appear to be dynamic
[13:32:18] [WARNING] heuristic (basic) test shows that URI parameter '#i*' might not be injectable
[13:32:20] [INFO] testing for SQL injection on URI parameter '#i*'
[13:32:20] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[13:32:27] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[13:32:28] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[13:32:29] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[13:32:30] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[13:32:31] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[13:32:33] [INFO] testing 'Generic inline queries'
[13:32:33] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[13:32:33] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[13:32:34] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[13:32:35] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[13:32:36] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[13:32:37] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[13:32:38] [INFO] testing 'Oracle AND time-based blind'
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
[13:32:43] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[13:32:46] [WARNING] URI parameter '#i*' does not seem to be injectable
[13:32:46] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. Please retry with the switch '--text-only'
as this case looks like a perfect candidate (low textual content along with inability of comparison engine to detect at least one dynamic parameter). If you suspect that there is some kind of protection mech
aybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'
[13:32:46] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 87 times
```

Vulnerabilities detect when Scanning

In order to process and find problems and vulnerabilities that are based on the OWASP top 10, I used tools like sub404, Netsparker.

- Sub404

Sub 404 is used to test for attempted subdomain takeovers.

```
(root@kali)-[/home/tharusha/PwnXSS/sub404]
# python3 sub404.py -d chime.com
```

SUB404

- By r3curs1v3_pr0xy

```
[~] Default http [use -p https]
[~] Gathering Information...
[~] Enumerating subdomains for chime.com
[~] Total Unique Subdomain Found: 241
[~] Getting URL's of 404 status code...
\-[~] URL Checked: 241
[~] Checking CNAME records...

/home/tharusha/PwnXSS/sub404/sub404.py:246: DeprecationWarning: please use dns.resolver.resolve() instead
resolve = dns.resolver.query(data.strip(), 'CNAME')

[~] Vulnerability Possible on: email.ethnio.chime.com
CNAME: mailgun.org.

[~] Vulnerability Possible on: email.talent.chime.com
CNAME: mailgun.org.

[~] links.account.chime.com
Not Vulnerable

[~] links.notify.chime.com
Not Vulnerable

[~] email.mg.chime.com
Not Vulnerable

[~] email.gh-mail.ext.chime.com
Not Vulnerable

[~] email.teamable.chime.com
Not Vulnerable

[~] 16002407.account.chime.com
Not Vulnerable

[~] monocle.chime.com
Not Vulnerable
```

```
[~] static-attachments.chime.com
Not Vulnerable

[~] Vulnerability Possible on: enterpriseregistration.chime.com
CNAME: enterpriseregistration.windows.net.

[~] 16002407.notify.chime.com
Not Vulnerable

[~] monocle-qa.chime.com
Not Vulnerable

[~] email.gh-mail.chime.com
Not Vulnerable

[~] monocle-dev1.chime.com
Not Vulnerable

[~] transaction.chime.com
Not Vulnerable
[*] Task Completed :)
```

- Netsparker

Software for scanning and managing vulnerabilities in web applications is called Netsparker. Its goal is to make it simpler for companies to identify and address security issues with their web applications. When evaluating web applications, Netsparker automatically looks for common security flaws like Remote Code Execution, SQL Injection, and Cross-Site Scripting (XSS).

To analyze and find problems and vulnerabilities based on the OWASP top 10, I used programs like Netsparker.

1. Vulnerability Title

1. HTTP Strict Transport Security (HSTS) Policy Not Enabled

MEDIUM  1

Vulnerability Description

The HTTP Strict Transport Security (HSTS) policy is not enabled, according to Netsparker. In addition to being delivered via HTTPS, the target website does not implement HSTS policies.

over the use of HTTP Strict Transport Security (HSTS), a web server can establish rules mandating that compliant user agents—like a web browser—interact with it exclusively over secure (HTTPS) connections. "Strict-Transport-Security" is an HTTP response header field that the server uses to transmit the HSTS Policy to the user agent. The user agent must only use secure methods to reach the server during a certain amount of time, according to the HSTS Policy.

User agents that comply with the HSTS Policy issued by a web application act as follows:

- Any links pointing to the web application that are not secure (HTTP) should automatically become secure (HTTPS) ones. (For example, before reaching the server, `http://example.com/some/page/` will be changed to `https://example.com/some/page/`.)
- User agents display an error message and prevent the user from accessing the web application if there is no way to guarantee the security of the connection (for example, the server's TLS certificate is self-signed).

How to mitigate

Set up your web server so that HTTP queries are forwarded to HTTPS.

i.e., the httpd.conf for Apache needs to be modified. Please see the External References section for additional setup options.

2. Vulnerability Title

2. Weak Ciphers Enabled

MEDIUM



1

CONFIRMED



1

Vulnerability Description

Weak ciphers are activated during secure communication (SSL), according to Netsparker's detection.

To safeguard secure communication with your visitors, you should only permit robust ciphers on your web server.

How to mitigate

Set up your web server to prevent the use of weak ciphers.

3. Vulnerability Title

3. Cookie Not Marked as HttpOnly

LOW



1

CONFIRMED



1

Vulnerability Description

An unmarked HTTPOnly cookie was found by Netsparker.

Designating a cookie as HTTPOnly can give an extra degree of defense against cross-site scripting attacks because it prevents client-side scripts from reading the cookie. It is possible for an attacker to quickly access cookies and take control of the victim's session via a cross-site scripting attack.

How to mitigate

Set the cookie's HTTPOnly setting. This will provide an additional line of protection against XSS. This won't, however, shield the system from cross-site scripting attacks and isn't a panacea. An attacker can get around HTTPOnly security by using a program like XSS Tunnel.