Sri Lanka Institute of Information Technology

BUG BOUNTY REPORT 06

(Stripe Web site)

IE2062 – Web Security

W.A.K.S Wijethunga

IT23361768

Table of Contents

1. Introduction to bug bounty program and audit scope

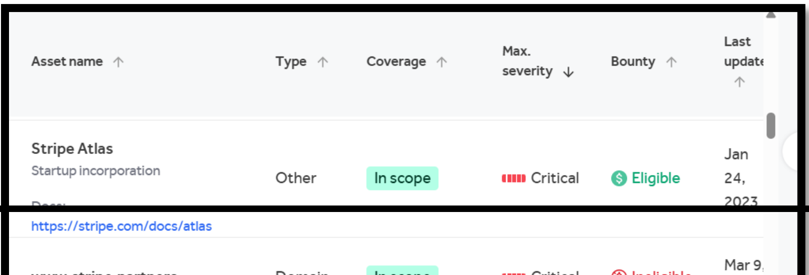
❖ Stripe

Stripe is a leading financial technology platform that provides payment processing software and application programming interfaces (APIs) for e-commerce websites and mobile applications. Founded in 2010, Stripe allows individuals and businesses to accept online payments, manage revenue, and handle complex financial workflows.

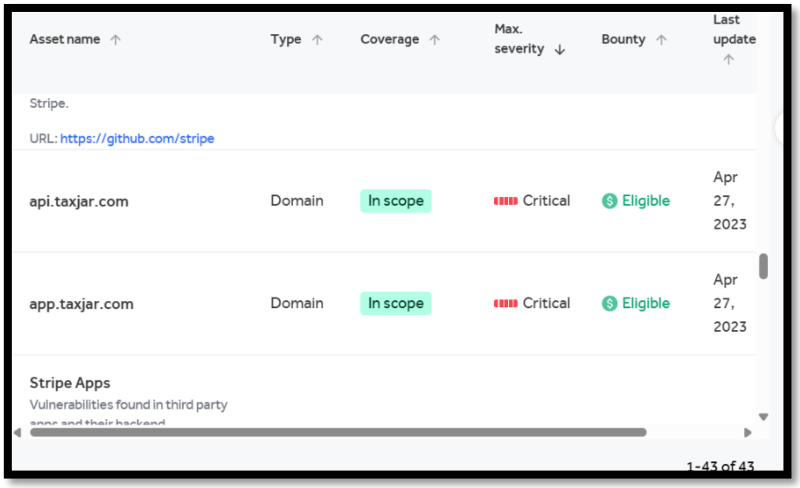
The platform is widely used by startups and large enterprises alike for its simplicity, scalability, and developer-friendly tools. Stripe's services include online payment processing, billing, fraud prevention, financial reporting, and issuing virtual or physical cards.

- **www.stripe.partners**
- **api.taxjar.comps**
- **app.taxjar.com**
- **js.stripe.com**
- **api.stripe.com**

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

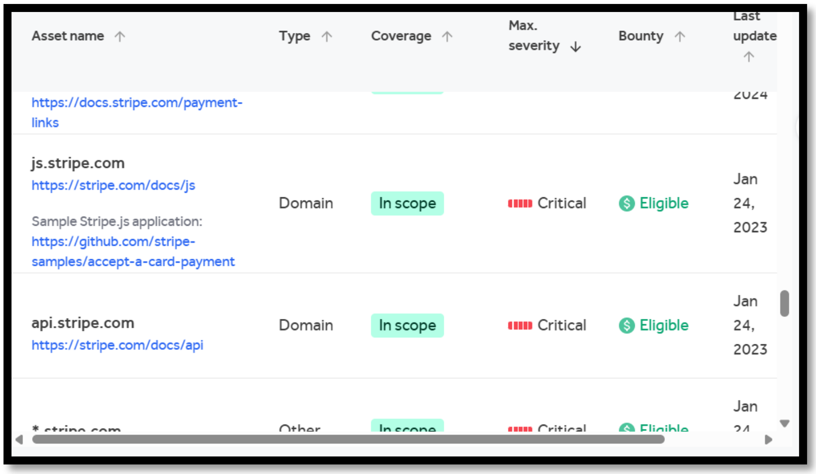


Asset name ↑	Type ↑	Coverage ↑	Max. severity ↓	Bounty ↑	Last update ↑
Stripe Atlas Startup incorporation Docs: https://stripe.com/docs/atlas	Other	In scope	Critical	Eligible	Jan 24, 2023
www.stripe.partners	Domain	In scope	Critical	Ineligible	Mar 9,



Asset name	Type	Coverage	Max. severity	Bounty	Last update
Stripe. URL: https://github.com/stripe					
api.taxjar.com	Domain	In scope	Critical	Eligible	Apr 27, 2023
app.taxjar.com	Domain	In scope	Critical	Eligible	Apr 27, 2023
Stripe Apps Vulnerabilities found in third party apps and their backend					

1-43 of 43



Asset name	Type	Coverage	Max. severity	Bounty	Last update
https://docs.stripe.com/payment-links					2024
js.stripe.com https://stripe.com/docs/js Sample Stripe.js application: https://github.com/stripe-samples/accept-a-card-payment	Domain	In scope	Critical	Eligible	Jan 24, 2023
api.stripe.com https://stripe.com/docs/api	Domain	In scope	Critical	Eligible	Jan 24, 2023
*.stripe.com	Other	In scope	Critical	Eligible	Jan 24

`

2. Reconnaissance

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

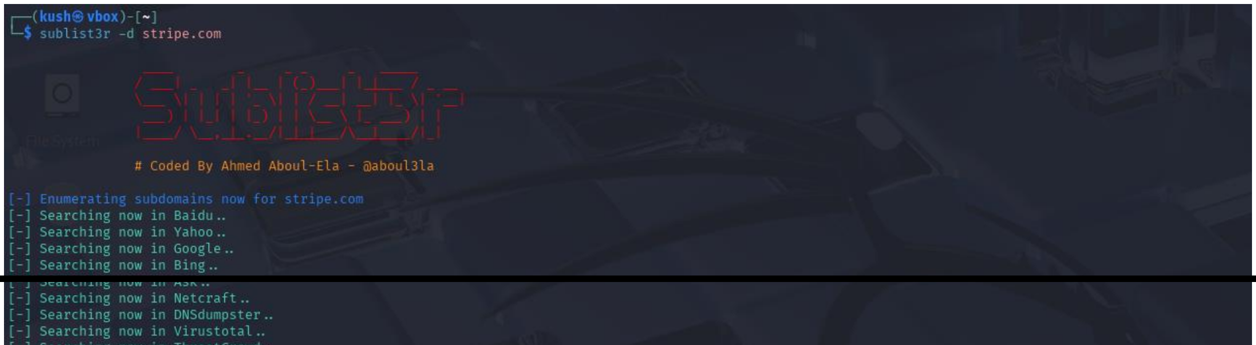
After downloading the files, go inside the 'Sublist3r' directory and install the requirements by entering,

sudo pip install -r requirements.txt

After installing the requirements, enter

sublist3r -d stripe.com -o subdomains.txt

to find subdomains under the mentioned domain.

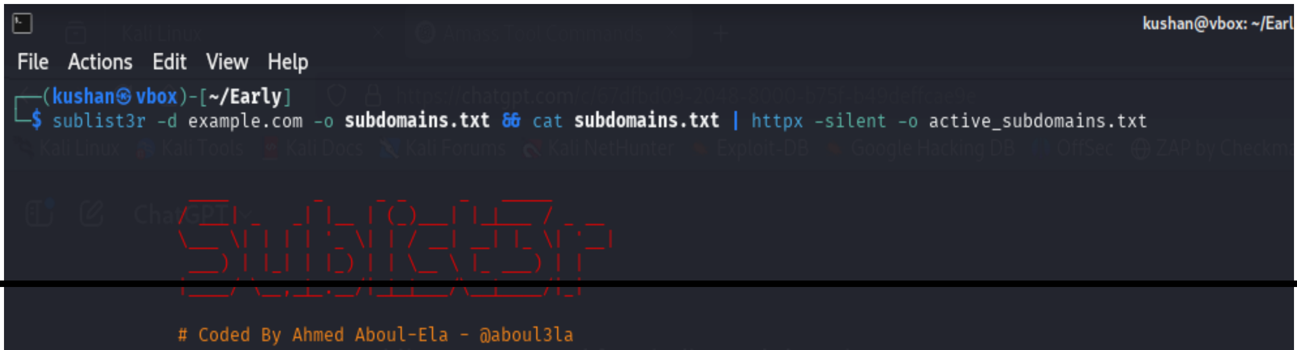


```
┌──(kush㉿vbox)-[~]
└─$ sublist3r -d stripe.com

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for stripe.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..
```

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.

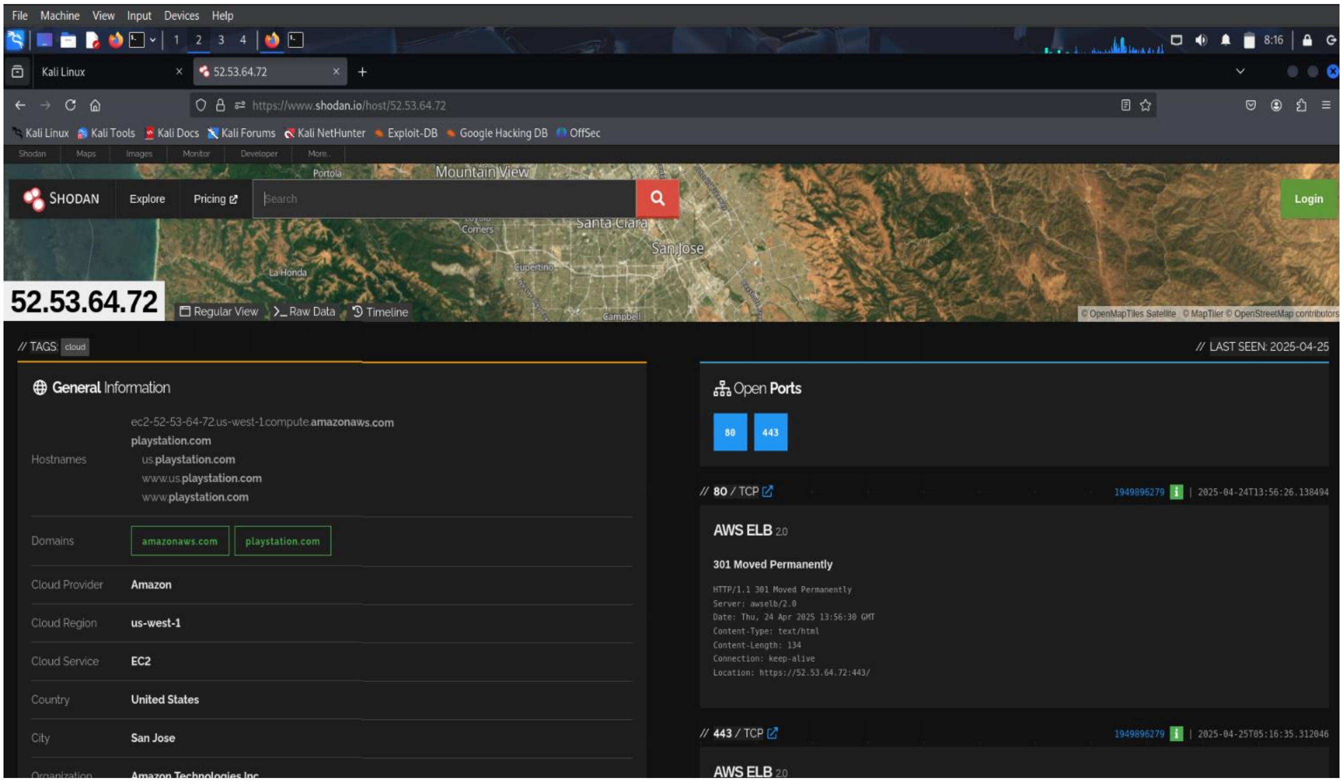
Following the completion of the scan, the findings reveal that the majority of the subdomains are indeed active.



```
┌──(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.


File Machine View Input Devices Help
Kali Linux
52.53.64.72
https://www.shodan.io/host/52.53.64.72
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Shodan Maps Images Monitor Developer More...
SHODAN Explore Pricing Search Login
Regular View Raw Data Timeline
© OpenMapTiles Satellite © MapTiler © OpenStreetMap contributors

52.53.64.72

// TAGS: cloud

// LAST SEEN: 2025-04-25

General Information

Hostnames	ec2-52-53-64-72.us-west-1.compute.amazonaws.com playstation.com us.playstation.com www.us.playstation.com www.playstation.com
Domains	amazonaws.com playstation.com
Cloud Provider	Amazon
Cloud Region	us-west-1
Cloud Service	EC2
Country	United States
City	San Jose
Organization	Amazon Technologies Inc

Open Ports

80 443

// 80 / TCP 1949896279 | 2025-04-24T13:56:26.138494

AWS ELB 2.0

301 Moved Permanently

```
HTTP/1.1 301 Moved Permanently
Server: awselb/2.0
Date: Thu, 24 Apr 2025 13:56:30 GMT
Content-Type: text/html
Content-Length: 134
Connection: keep-alive
Location: https://52.53.64.72:443/
```

// 443 / TCP 1949896279 | 2025-04-25T05:16:35.312046

AWS ELB 2.0

III. Detect technologies using Whatweb

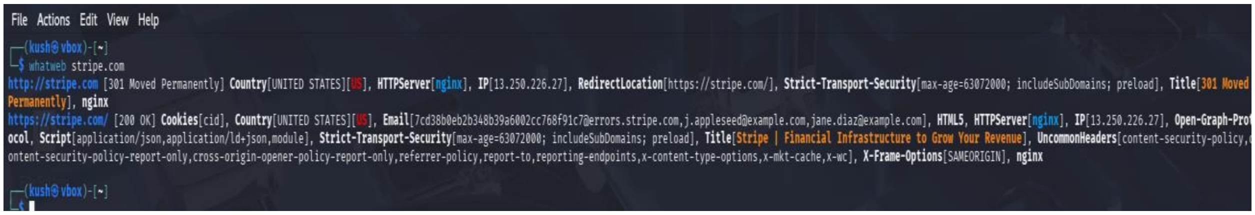
Whatweb is a powerful open-source tool designed to identify the technologies used by websites. It works by analyzing the responses from a web server, such as

HTTP headers, HTML content, cookies, and scripts, to detect the underlying technologies.

To detect technologies used by a website, simply run :

whatweb stripe.com

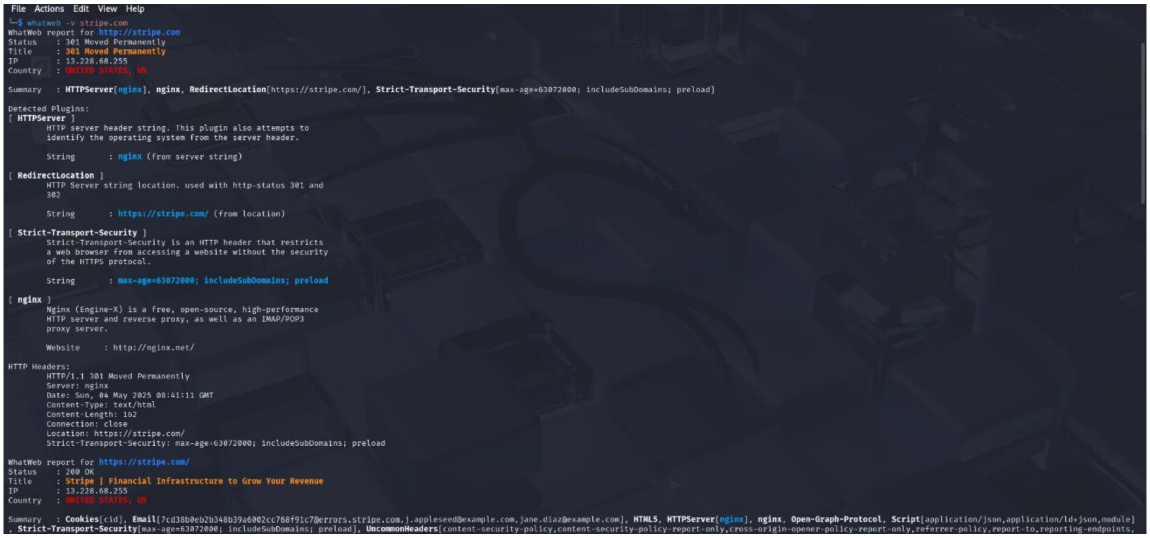
This command will analyze the website and display a summary of the detected technologies**.**



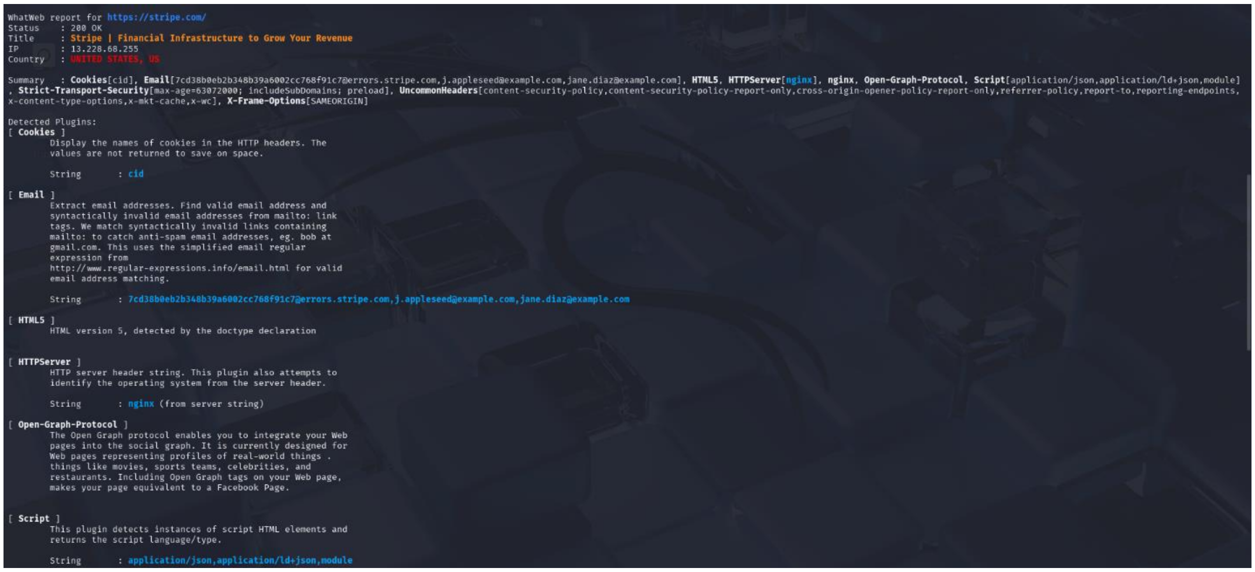
```
┌──(kush㉿vbox)-[~]
└─$ whatweb stripe.com
http://stripe.com [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[nginx], IP[13.250.226.27], RedirectLocation[https://stripe.com/], Strict-Transport-Security[max-age=63072000; includeSubDomains; preload], Title[301 Moved
Permanently], nginx
https://stripe.com/ [200 OK] Cookies[cid], Country[UNITED STATES][US], Email[7cd38b0eb2b348b39a6002cc768f91c7@errors.stripe.com,j.appleseed@example.com,jane.diaz@example.com], HTML5, HTTPServer[nginx], IP[13.250.226.27], Open-Graph-Prot
ocol, Script[application/json,application/ld+json,module], Strict-Transport-Security[max-age=63072000; includeSubDomains; preload], Title[Stripe | Financial Infrastructure to Grow Your Revenue], UncommonHeaders[content-security-policy,c
ontent-security-policy-report-only,cross-origin-opener-policy-report-only,referrer-policy,report-to,reporting-endpoints,x-content-type-options,x-mkt-cache,x-wc], X-Frame-Options[SAMEORIGIN], nginx

┌──(kush㉿vbox)-[~]
└─$ 
```

To get detailed information about the detection process:

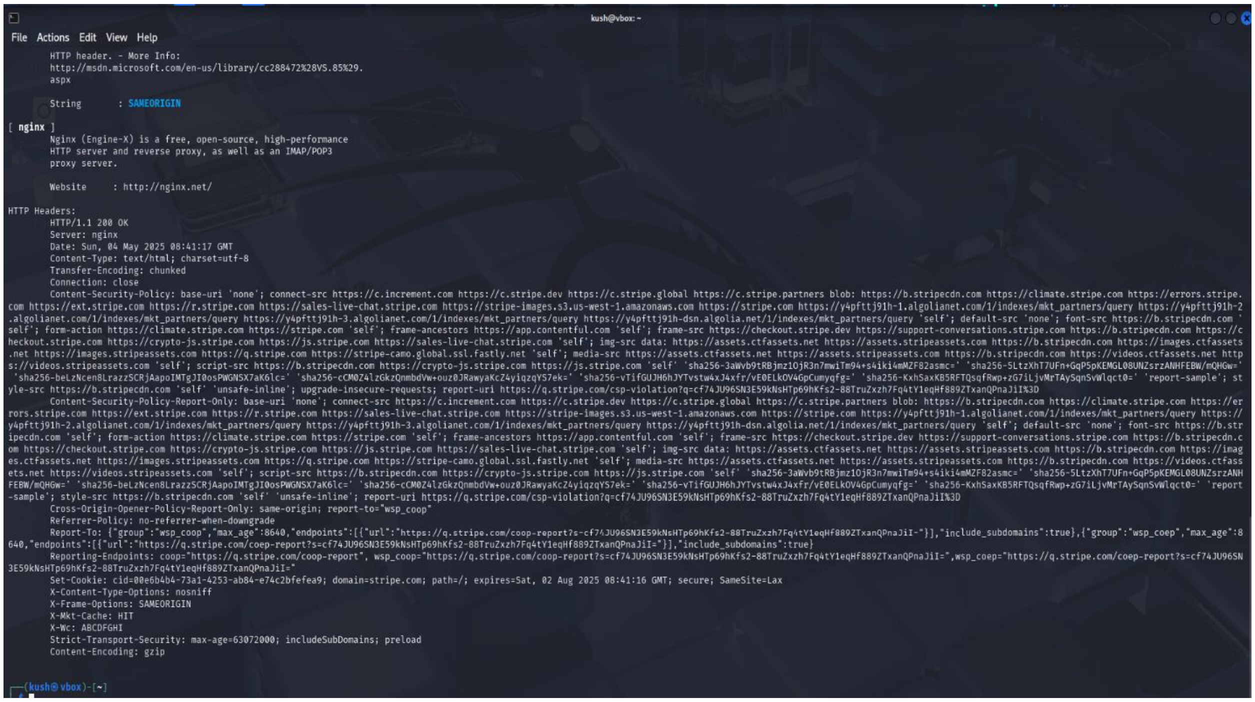
whatweb -v stripe.com



```
└─$ whatweb -v stripe.com
WhatWeb report for http://stripe.com
Status    : 301 Moved Permanently
Title     : 301 Moved Permanently
IP        : 13.228.68.255
Country   : UNITED STATES, US

Summary   : HTTPServer[nginx], nginx, RedirectLocation[https://stripe.com/], Strict-Transport-Security[max-age=63072000; includeSubDomains; preload]

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

        String       : nginx (from server string)

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

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

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

        String       : max-age=63072000; includeSubDomains; preload

[ nginx ]
        Nginx (Engine-X) is a free, open-source, high-performance
        HTTP server and reverse proxy, as well as an IMAP/POP3
        proxy server.

        Website     : http://nginx.net/

HTTP Headers:
        HTTP/1.1 301 Moved Permanently
        Server: nginx
        Date: Sun, 04 May 2025 08:41:11 GMT
        Content-Type: text/html
        Content-Length: 162
        Connection: close
        Location: https://stripe.com/
        Strict-Transport-Security: max-age=63072000; includeSubDomains; preload

WhatWeb report for https://stripe.com/
Status    : 200 OK
Title     : Stripe | Financial Infrastructure to Grow Your Revenue
IP        : 13.228.68.255
Country   : UNITED STATES, US

Summary   : Cookies[cid], Email[7cd38b0eb2b348b39a6002cc768f91c7@errors.stripe.com,j.appleseed@example.com,jane.diaz@example.com], HTML5, HTTPServer[nginx], nginx, Open-Graph-Protocol, Script[application/json,application/ld+json,module]
, Strict-Transport-Security[max-age=63072000; includeSubDomains; preload], UncommonHeaders[content-security-policy,content-security-policy-report-only,cross-origin-opener-policy-report-only,referrer-policy,report-to,reporting-endpoints,
```



```
WhatWeb report for https://stripe.com/
Status     : 200 OK
Title      : Stripe | Financial Infrastructure to Grow Your Revenue
IP         : 13.228.68.255
Country    : UNITED STATES, US

Summary    : Cookies[cid], Email[7cd38b0eb2b348b39a6002cc768f91c7@errors.stripe.com,j.appleseed@example.com,jane.diaz@example.com], HTML5, HTTPServer[nginx], nginx, Open-Graph-Protocol, Script[application/json,application/ld+json,module]
, Strict-Transport-Security[max-age=63072000; includeSubDomains; preload], UncommonHeaders[content-security-policy,content-security-policy-report-only,cross-origin-opener-policy-report-only,referrer-policy,report-to,reporting-endpoints,
x-content-type-options,x-mkt-cache,x-wc], X-Frame-Options[SAMEORIGIN]

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

        String       : cid

[ 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       : 7cd38b0eb2b348b39a6002cc768f91c7@errors.stripe.com,j.appleseed@example.com,jane.diaz@example.com

[ 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       : nginx (from server string)

[ Open-Graph-Protocol ]
        The Open Graph protocol enables you to integrate your Web
        pages into the social graph. It is currently designed for
        Web pages representing profiles of real-world things .
        things like movies, sports teams, celebrities, and
        restaurants. Including Open Graph tags on your Web page,
        makes your page equivalent to a Facebook Page.


[ Script ]
        This plugin detects instances of script HTML elements and
        returns the script language/type.

        String       : application/json,application/ld+json,module
```



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

        String       : SAMEORIGIN

[ nginx ]
        Nginx (Engine-X) is a free, open-source, high-performance
        HTTP server and reverse proxy, as well as an IMAP/POP3
        proxy server.

        Website     : http://nginx.net/

HTTP Headers:
        HTTP/1.1 200 OK
        Server: nginx
        Date: Sun, 04 May 2025 08:41:17 GMT
        Content-Type: text/html; charset=utf-8
        Transfer-Encoding: chunked
        Connection: close
        Content-Security-Policy: base-uri 'none'; connect-src https://c.increment.com https://c.stripe.dev https://c.stripe.global https://c.stripe.partners blob: https://b.stripecdn.com https://climate.stripe.com https://errors.stripe.
com https://ext.stripe.com https://r.stripe.com https://sales-live-chat.stripe.com https://stripe-images.s3.us-west-1.amazonaws.com https://stripe.com https://y4pfttj91h-1.algolianet.com/1/indexes/mkt_partners/query https://y4pfttj91h-2
.algolianet.com/1/indexes/mkt_partners/query https://y4pfttj91h-3.algolianet.com/1/indexes/mkt_partners/query https://y4pfttj91h-dsn.algolia.net/1/indexes/mkt_partners/query 'self'; default-src 'none'; font-src https://b.stripecdn.com '
self'; form-action https://climate.stripe.com https://stripe.com 'self'; frame-ancestors https://app.contentful.com 'self'; frame-src https://checkout.stripe.dev https://support-conversations.stripe.com https://b.stripecdn.com https://c
heckout.stripe.com https://crypto-js.stripe.com https://js.stripe.com https://sales-live-chat.stripe.com 'self'; img-src data: https://assets.ctfassets.net https://assets.stripeassets.com https://b.stripecdn.com https://images.ctfassets
.net https://images.stripeassets.com https://q.stripe.com https://stripe-camo.global.ssl.fastly.net 'self'; media-src https://assets.ctfassets.net https://assets.stripeassets.com https://b.stripecdn.com https://videos.ctfassets.net http
s://videos.stripeassets.com 'self'; script-src https://b.stripecdn.com https://crypto-js.stripe.com https://js.stripe.com 'self' 'sha256-3aWvb9tRBjmz1OjR3n7mwiTm94+s4iki4mMZF82asmc=' 'sha256-5LtzXhT7UFn+GqP5pKEMGL08UNZsrzANHFEBW/mQHGw='
 'sha256-beLzNcen8LrazzSCRjAapoIMTgJI0osPWGNSX7aK6lc=' 'sha256-cCM0Z4lzGkzQnmbdVw+ouz0JRawyaKcZ4yiqzqYS7ek=' 'sha256-vTifGUJH6hJYTvstw4xJ4xfr/vE0ELkOV4GpCumyqfg=' 'sha256-KxhSaxKB5RFTQsqfRwp+zG7iLjvMrTAySqnSvWlqct0=' 'report-sample'; st
yle-src https://b.stripecdn.com 'self' 'unsafe-inline'; upgrade-insecure-requests; report-uri https://q.stripe.com/csp-violation?q=cf74JU96SN3E59kNsHTp69hKfs2-88TruZxzh7Fq4tY1eqHf889ZTxanQPnaJiI%3D
        Content-Security-Policy-Report-Only: base-uri 'none'; connect-src https://c.increment.com https://c.stripe.dev https://c.stripe.global https://c.stripe.partners blob: https://b.stripecdn.com https://climate.stripe.com https://er
rors.stripe.com https://ext.stripe.com https://r.stripe.com https://sales-live-chat.stripe.com https://stripe-images.s3.us-west-1.amazonaws.com https://stripe.com https://y4pfttj91h-1.algolianet.com/1/indexes/mkt_partners/query https://
y4pfttj91h-2.algolianet.com/1/indexes/mkt_partners/query https://y4pfttj91h-3.algolianet.com/1/indexes/mkt_partners/query https://y4pfttj91h-dsn.algolia.net/1/indexes/mkt_partners/query 'self'; default-src 'none'; font-src https://b.str
ipecdn.com 'self'; form-action https://climate.stripe.com https://stripe.com 'self'; frame-ancestors https://app.contentful.com 'self'; frame-src https://checkout.stripe.dev https://support-conversations.stripe.com https://b.stripecdn.c
om https://checkout.stripe.com https://crypto-js.stripe.com https://js.stripe.com https://sales-live-chat.stripe.com 'self'; img-src data: https://assets.ctfassets.net https://assets.stripeassets.com https://b.stripecdn.com https://imag
es.ctfassets.net https://images.stripeassets.com https://q.stripe.com https://stripe-camo.global.ssl.fastly.net 'self'; media-src https://assets.ctfassets.net https://assets.stripeassets.com https://b.stripecdn.com https://videos.ctfass
ets.net https://videos.stripeassets.com 'self'; script-src https://b.stripecdn.com https://crypto-js.stripe.com https://js.stripe.com 'self' 'sha256-3aWvb9tRBjmz1OjR3n7mwiTm94+s4iki4mMZF82asmc=' 'sha256-5LtzXhT7UFn+GqP5pKEMGL08UNZsrzANH
FEBW/mQHGw=' 'sha256-beLzNcen8LrazzSCRjAapoIMTgJI0osPWGNSX7aK6lc=' 'sha256-cCM0Z4lzGkzQnmbdVw+ouz0JRawyaKcZ4yiqzqYS7ek=' 'sha256-vTifGUJH6hJYTvstw4xJ4xfr/vE0ELkOV4GpCumyqfg=' 'sha256-KxhSaxKB5RFTQsqfRwp+zG7iLjvMrTAySqnSvWlqct0=' 'report
-sample'; style-src https://b.stripecdn.com 'self' 'unsafe-inline'; report-uri https://q.stripe.com/csp-violation?q=cf74JU96SN3E59kNsHTp69hKfs2-88TruZxzh7Fq4tY1eqHf889ZTxanQPnaJiI%3D
        Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="wsp_coop"
        Referrer-Policy: no-referrer-when-downgrade
        Report-To: {"group":"wsp_coop","max_age":8640,"endpoints":[{"url":"https://q.stripe.com/coop-report?s-cf74JU96SN3E59kNsHTp69hKfs2-88TruZxzh7Fq4tY1eqHf889ZTxanQPnaJiI-"}],"include_subdomains":true},{"group":"wsp_coep","max_age":8
640,"endpoints":[{"url":"https://q.stripe.com/coep-report?s=cf74JU96SN3E59kNsHTp69hKfs2-88TruZxzh7Fq4tY1eqHf889ZTxanQPnaJiI="}],"include_subdomains":true}
        Reporting-Endpoints: coop="https://q.stripe.com/coop-report", wsp_coop="https://q.stripe.com/coop-report?s=cf74JU96SN3E59kNsHTp69hKfs2-88TruZxzh7Fq4tY1eqHf889ZTxanQPnaJiI=",wsp_coep="https://q.stripe.com/coep-report?s=cf74JU96SN
3E59kNsHTp69hKfs2-88TruZxzh7Fq4tY1eqHf889ZTxanQPnaJiI="
        Set-Cookie: cid=00e6b4b4-73a1-4253-ab84-e74c2bfefea9; domain=stripe.com; path=/; expires=Sat, 02 Aug 2025 08:41:16 GMT; secure; SameSite=Lax
        X-Content-Type-Options: nosniff
        X-Frame-Options: SAMEORIGIN
        X-Mkt-Cache: HIT
        X-Wc: ABCDFGHI
        Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
        Content-Encoding: gzip


┌──(kush㉿vbox)-[~]
```

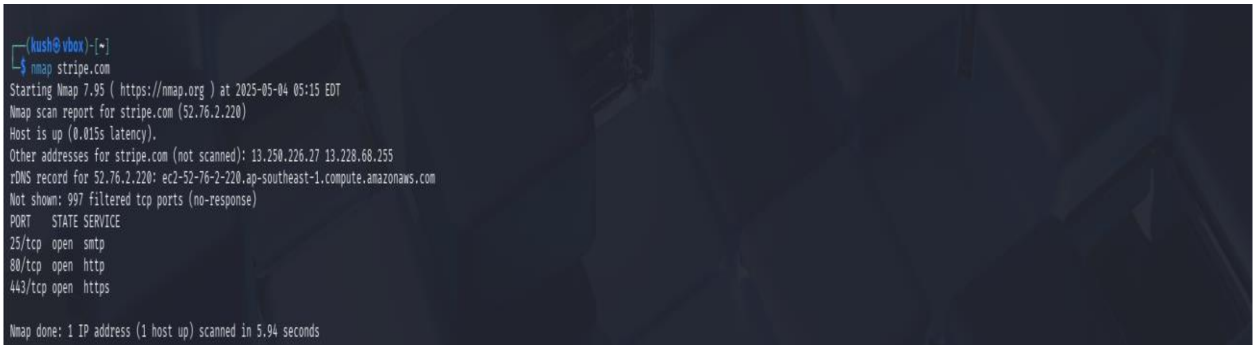
3. Scanning Vulnerability Identifies

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**

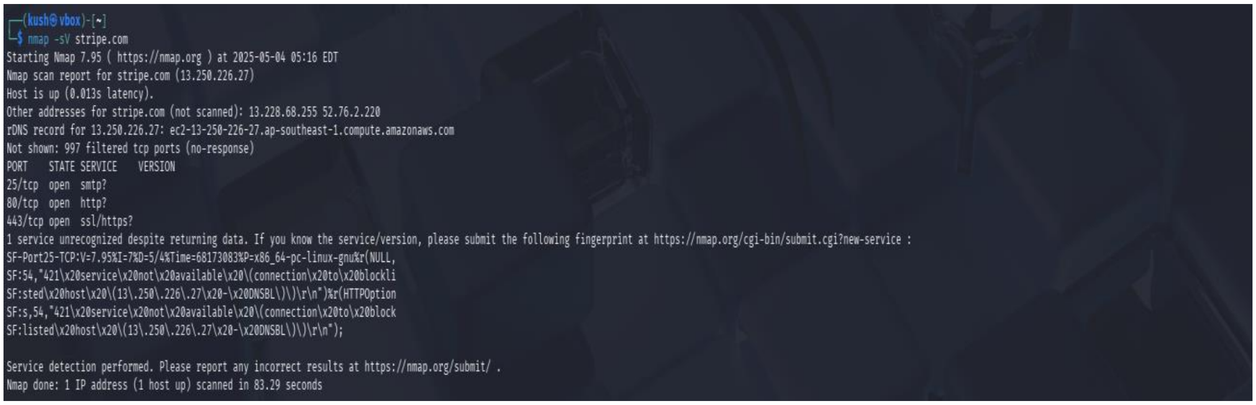
Nmap (Network Mapper) is a powerful tool for scanning open ports and identifying running services on a target system. By using the **nmap -sV** command, you can detect the version of services running on open ports, helping assess potential vulnerabilities. The -p- option scans all 65,535 ports, while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



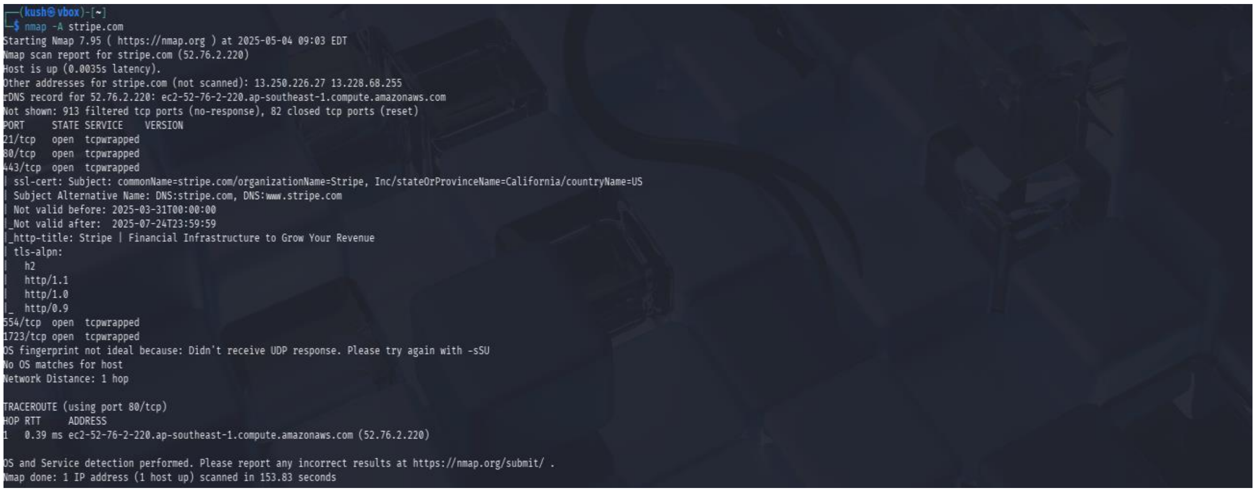
```
┌──(kush㉿vbox)-[~]
└─$ nmap stripe.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 05:15 EDT
Nmap scan report for stripe.com (52.76.2.220)
Host is up (0.015s latency).
Other addresses for stripe.com (not scanned): 13.250.226.27 13.228.68.255
rDNS record for 52.76.2.220: ec2-52-76-2-220.ap-southeast-1.compute.amazonaws.com
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 5.94 seconds
```

Identify services running on open ports,



```
┌──(kush㉿vbox)-[~]
└─$ nmap -sV stripe.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 05:16 EDT
Nmap scan report for stripe.com (13.250.226.27)
Host is up (0.013s latency).
Other addresses for stripe.com (not scanned): 13.228.68.255 52.76.2.220
rDNS record for 13.250.226.27: ec2-13-250-226-27.ap-southeast-1.compute.amazonaws.com
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE    VERSION
25/tcp  open  smtp?
80/tcp  open  http?
443/tcp open  ssl/https?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port25-TCP:V=7.95%I=7%D=5/4%Time=68173083%P=x86_64-pc-linux-gnu%r(NULL,
SF:54,"421\x20service\x20not\x20available\x20\(connection\x20to\x20blockli
SF:sted\x20host\x20\(13\.250\.226\.27\x20-\x20DNSBL\)\)\r\n")%r(HTTPOption
SF:s,54,"421\x20service\x20not\x20available\x20\(connection\x20to\x20block
SF:listed\x20host\x20\(13\.250\.226\.27\x20-\x20DNSBL\)\)\r\n");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 83.29 seconds
```

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

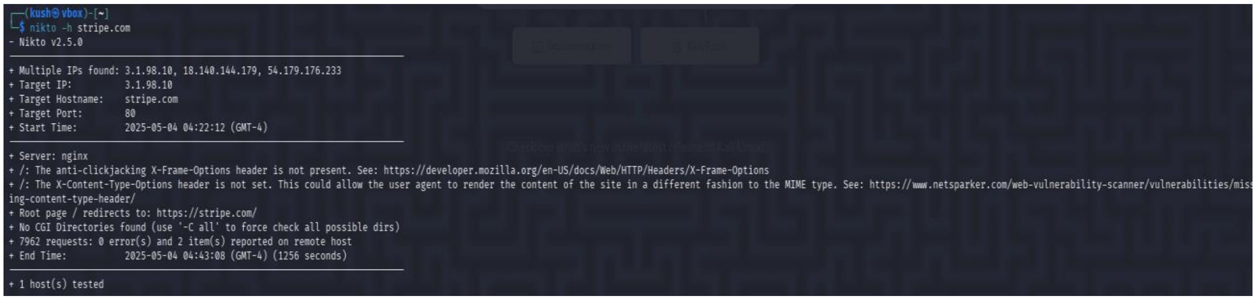


```
┌──(kush㉿vbox)-[~]
└─$ nmap -A stripe.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 09:03 EDT
Nmap scan report for stripe.com (52.76.2.220)
Host is up (0.0035s latency).
Other addresses for stripe.com (not scanned): 13.250.226.27 13.228.68.255
rDNS record for 52.76.2.220: ec2-52-76-2-220.ap-southeast-1.compute.amazonaws.com
Not shown: 913 filtered tcp ports (no-response), 82 closed tcp ports (reset)
PORT     STATE SERVICE    VERSION
21/tcp   open  tcpwrapped
80/tcp   open  tcpwrapped
443/tcp  open  tcpwrapped
| ssl-cert: Subject: commonName=stripe.com/organizationName=Stripe, Inc/stateOrProvinceName=California/countryName=US
| Subject Alternative Name: DNS:stripe.com, DNS:www.stripe.com
| Not valid before: 2025-03-31T00:00:00
|_Not valid after:  2025-07-24T23:59:59
|_http-title: Stripe | Financial Infrastructure to Grow Your Revenue
| tls-alpn:
|   h2
|   http/1.1
|   http/1.0
|_  http/0.9
554/tcp  open  tcpwrapped
1723/tcp open  tcpwrapped
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
No OS matches for host
Network Distance: 1 hop

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.39 ms ec2-52-76-2-220.ap-southeast-1.compute.amazonaws.com (52.76.2.220)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 153.83 seconds
```

ii. Web vulnerabilities

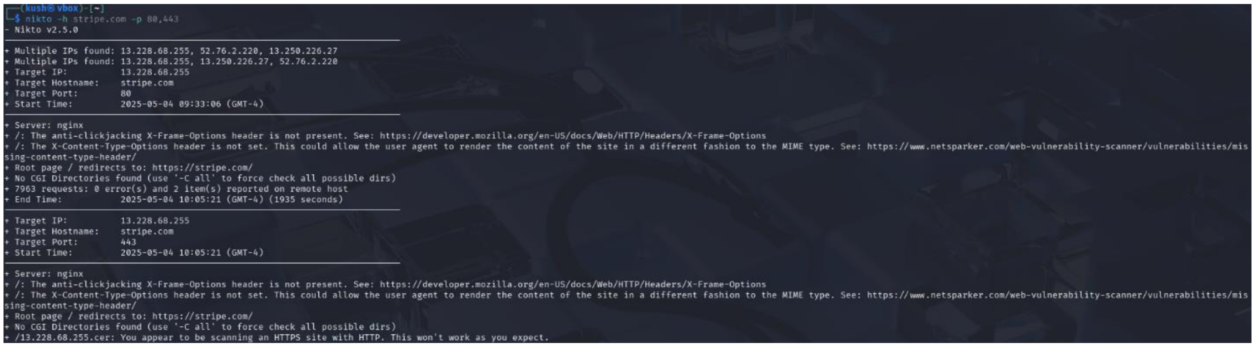
Nikto is an open-source web server scanner designed to identify vulnerabilities, outdated software, and security misconfigurations on web servers. It performs comprehensive testing for over 6700 vulnerabilities, including misconfigured files, outdated server software, and security holes.

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



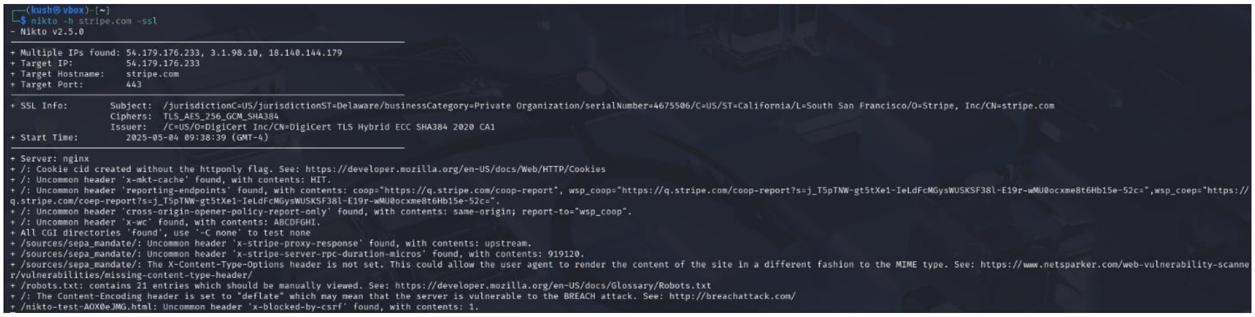
```
┌──(kush㉿vbox)-[~]
└─$ nikto -h stripe.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 3.1.98.10, 18.140.144.179, 54.179.176.233
+ Target IP:          3.1.98.10
+ Target Hostname:    stripe.com
+ Target Port:        80
+ Start Time:         2025-05-04 04:22:12 (GMT-4)
---------------------------------------------------------------------------
+ Server: nginx
+ /: 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/miss
ing-content-type-header/
+ Root page / redirects to: https://stripe.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7962 requests: 0 error(s) and 2 item(s) reported on remote host
+ End Time:           2025-05-04 04:43:08 (GMT-4) (1256 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Scans both HTTP and HTTPS,



```
┌──(kush㉿vbox)-[~]
└─$ nikto -h stripe.com -p 80,443
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 13.228.68.255, 52.76.2.220, 13.250.226.27
+ Multiple IPs found: 13.228.68.255, 13.250.226.27, 52.76.2.220
+ Target IP:          13.228.68.255
+ Target Hostname:    stripe.com
+ Target Port:        80
+ Start Time:         2025-05-04 09:33:06 (GMT-4)
---------------------------------------------------------------------------
+ Server: nginx
+ /: 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://stripe.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7963 requests: 0 error(s) and 2 item(s) reported on remote host
+ End Time:           2025-05-04 10:05:21 (GMT-4) (1935 seconds)
---------------------------------------------------------------------------
+ Target IP:          13.228.68.255
+ Target Hostname:    stripe.com
+ Target Port:        443
+ Start Time:         2025-05-04 10:05:21 (GMT-4)
---------------------------------------------------------------------------
+ Server: nginx
+ /: 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://stripe.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /13.228.68.255.cer: You appear to be scanning an HTTPS site with HTTP. This won't work as you expect.
```

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



```
┌──(kush㉿vbox)-[~]
└─$ nikto -h stripe.com -ssl
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 54.179.176.233, 3.1.98.10, 18.140.144.179
+ Target IP:          54.179.176.233
+ Target Hostname:    stripe.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /jurisdictionC=US/jurisdictionST=Delaware/businessCategory=Private Organization/serialNumber=4675506/C=US/ST=California/L=South San Francisco/O=Stripe, Inc/CN=stripe.com
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=DigiCert Inc/CN=DigiCert TLS Hybrid ECC SHA384 2020 CA1
+ Start Time:         2025-05-04 09:38:39 (GMT-4)
---------------------------------------------------------------------------
+ Server: nginx
+ /: Cookie cid created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Uncommon header 'x-mkt-cache' found, with contents: HIT.
+ /: Uncommon header 'reporting-endpoints' found, with contents: coop="https://q.stripe.com/coop-report", wsp_coop="https://q.stripe.com/coop-report?s=j_T5pTNW-gt5tXe1-IeLdFcMGysWUSKSF38l-E19r-wMU0ocxme8t6Hb15e-52c=",wsp_coep="https://
q.stripe.com/coep-report?s=j_T5pTNW-gt5tXe1-IeLdFcMGysWUSKSF38l-E19r-wMU0ocxme8t6Hb15e-52c=".
+ /: Uncommon header 'cross-origin-opener-policy-report-only' found, with contents: same-origin; report-to="wsp_coop".
+ /: Uncommon header 'x-wc' found, with contents: ABCDFGHI.
+ All CGI directories 'found', use '-C none' to test none
+ /sources/sepa_mandate/: Uncommon header 'x-stripe-proxy-response' found, with contents: upstream.
+ /sources/sepa_mandate/: Uncommon header 'x-stripe-server-rpc-duration-micros' found, with contents: 919120.
+ /sources/sepa_mandate/: 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-scanne
r/vulnerabilities/missing-content-type-header/
+ /robots.txt: contains 21 entries 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-test-AOX0eJMG.html: Uncommon header 'x-blocked-by-csrf' found, with contents: 1.
```

Automated Testing

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

OWASP ZAP

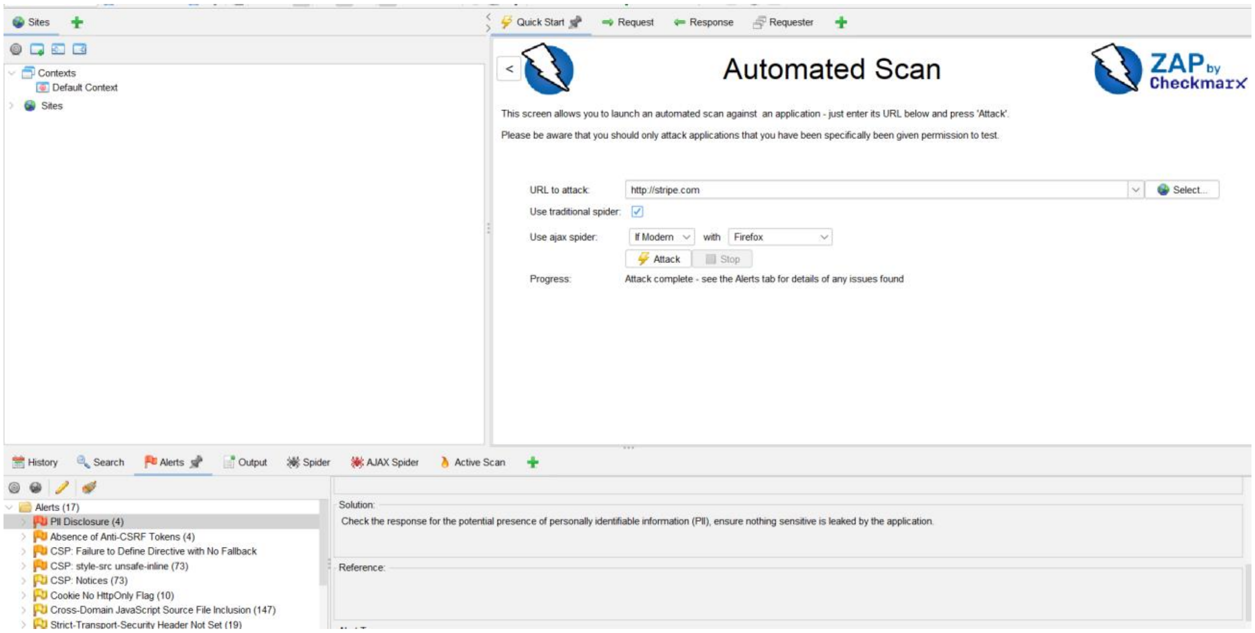
The Open Web Application Security Project Zed Attack Proxy (OWASP ZAP) is an open-source vulnerability scanner renowned for its capability to function as a Man-in-the-Middle (MITM) proxy. It assesses various vulnerabilities by scrutinizing responses from the web application or server. Notably convenient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



Automated Scan

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

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

URL to attack: http://stripe.com

Use traditional spider: ☑

Use ajax spider: If Modern with Firefox

Progress: Attack complete - see the Alerts tab for details of any issues found

Alerts (17)
- PII Disclosure (4)
- Absence of Anti-CSRF Tokens (4)
- CSP: Failure to Define Directive with No Fallback
- CSP: style-src unsafe-inline (73)
- CSP: Notices (73)
- Cookie No HttpOnly Flag (10)
- Cross-Domain JavaScript Source File Inclusion (147)
- Strict-Transport-Security Header Not Set (19)

Solution:
Check the response for the potential presence of personally identifiable information (PII), ensure nothing sensitive is leaked by the application.

Reference:

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.

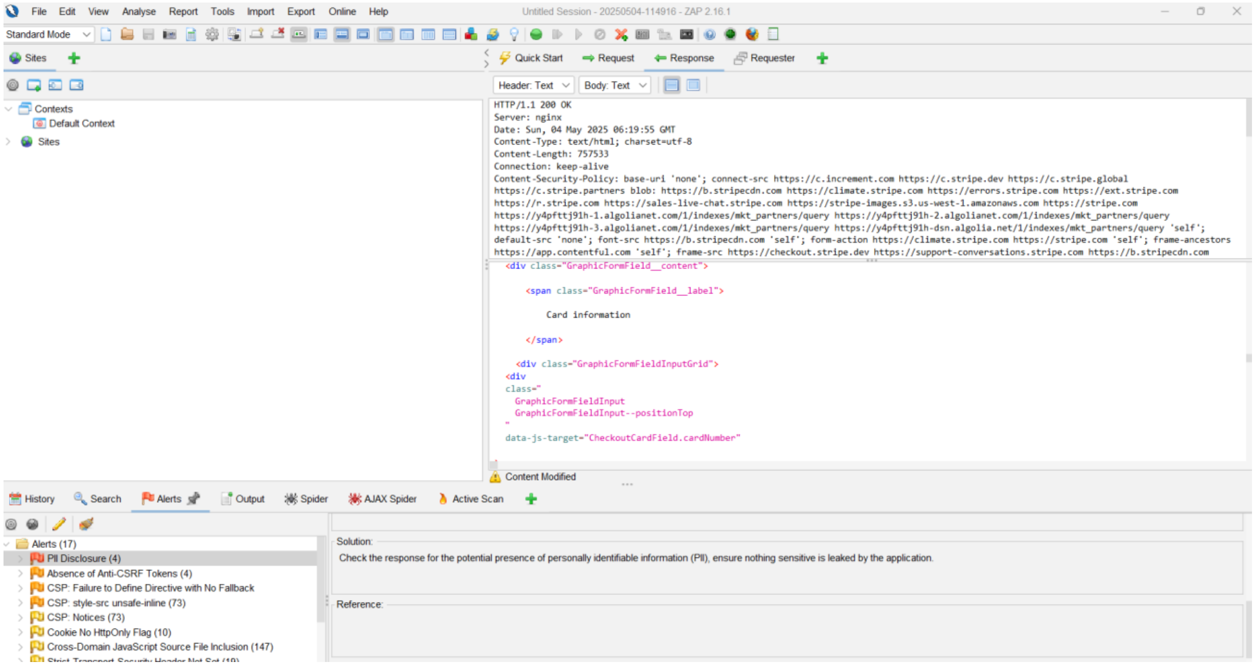
4. **Exploitation & Validation**

PII Disclourse Attack Analysis

PII (Personally Identifiable Information) disclosure refers to the unintended exposure of private information about users in an application's response, logs, or error messages.

Examples of PII:

- Full name
- Email address
- Credit card numbers
- Phone numbers
- Social Security Numbers (SSN)
- Bank account details
- IP addresses (in some contexts)



```
HTTP/1.1 200 OK
Server: nginx
Date: Sun, 04 May 2025 06:19:55 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 757533
Connection: keep-alive
Content-Security-Policy: base-uri 'none'; connect-src https://c.increment.com https://c.stripe.dev https://c.stripe.global
https://c.stripe.partners blob: https://b.stripecdn.com https://climate.stripe.com https://errors.stripe.com https://ext.stripe.com
https://r.stripe.com https://sales-live-chat.stripe.com https://stripe-images.s3.us-west-1.amazonaws.com https://stripe.com
https://y4pfttj91h-1.algolianet.com/1/indexes/mkt_partners/query https://y4pfttj91h-2.algolianet.com/1/indexes/mkt_partners/query
https://y4pfttj91h-3.algolianet.com/1/indexes/mkt_partners/query https://y4pfttj91h-dsn.algolia.net/1/indexes/mkt_partners/query 'self';
default-src 'none'; font-src https://b.stripecdn.com 'self'; form-action https://climate.stripe.com https://stripe.com 'self'; frame-ancestors
https://app.contentful.com 'self'; frame-src https://checkout.stripe.dev https://support-conversations.stripe.com https://b.stripecdn.com
```

```
  <div class="GraphicFormField__content">

      <span class="GraphicFormField__label">

          Card information

      </span>

    <div class="GraphicFormFieldInputGrid">
  <div
  class="
    GraphicFormFieldInput
    GraphicFormFieldInput--positionTop
  "
  data-js-target="CheckoutCardField.cardNumber"
```

Alerts (17)
- PII Disclosure (4)
- Absence of Anti-CSRF Tokens (4)
- CSP: Failure to Define Directive with No Fallback
- CSP: style-src unsafe-inline (73)
- CSP: Notices (73)
- Cookie No HttpOnly Flag (10)
- Cross-Domain JavaScript Source File Inclusion (147)
- Strict Transport Security Header Not Set (19)

Solution:

Check the response for the potential presence of personally identifiable information (PII), ensure nothing sensitive is leaked by the application.

Reference:

Exploit PII Disclosure

1. Passive Discovery (No Login Required)

- Intercept HTTP responses using Burp Suite, OWASP ZAP, or browser DevTools.
- Sensitive data may be accidentally included in:

  - JSON/XML API responses
  - HTML source code
  - JavaScript variables
  - Debug/Error messages

2. Logged-In Exploitation

- Log in as a low-privileged user and:
  - View other users' data through APIs (IDOR)
  - Capture PII in error messages (try invalid input)
  - Inspect analytics, debug panels, or dev/test endpoints

3. Headers and Logs

- Look at HTTP headers or meta data for email/username leaks.
- Use error response codes (500/404/etc.) to trigger info leaks.

5. **Report Writing**

Title:

PII Exposure via Sensitive Data in Response on https://stripe.com/use-cases/ecommerce

Summary:

A security misconfiguration was identified on **https://stripe.com/use-cases/ecommerce** where the server response contains **personally identifiable information (PII)**, including a **credit card number (Visa: 4242 4242 4242 4242)**. This constitutes a severe information disclosure risk, violating data protection principles. The exposure of such data — even in demo or placeholder form — can mislead threat detection tools or, worse, be abused if production data is ever inadvertently leaked. This issue highlights inadequate data handling or sanitization in the application response, potentially breaching compliance standards such as PCI DSS.

Affected Endpoint:

https://stripe.com/use-cases/ecommerce

Vulnerability Type:

- **Information Disclosure**
- **Security Misconfiguration**
- **CWE-359: Exposure of Private Personal Information ('Privacy Violation')**
- **WASC-13: Information Leakage**
- **OWASP Top 10:**
  - **2021 A01: Broken Access Control** (If data should be restricted)
  - **2021 A06: Vulnerable and Outdated Components** (if demo/test data unintentionally exposed)

Steps to Reproduce:

Step 1: Access the URL
Navigate to https://stripe.com/use-cases/ecommerce via browser or proxy tool (e.g., Burp Suite, OWASP ZAP).

Step 2: Intercept the Server Response
Capture the HTTP response from the endpoint.

Step 3: Identify Sensitive Data
Observe the presence of a credit card number in the response body. Example:

yaml

CopyEdit

4242 4242 4242 4242

Step 4: Analyze Context
Even if this is sample/demo data, its inclusion in live responses without obfuscation may mislead security scanners and increase false positives or mask real issues.

Impact:

- **PII Exposure:** Credit card numbers in plaintext violate data protection standards.
- **User Trust Erosion:** Demonstrating unsafe data handling practices can undermine user confidence.
- **Compliance Violation:** Exposure of sensitive information may breach PCI DSS and privacy laws such as GDPR or CCPA.
- **Recon for Attackers:** Such responses may be leveraged in phishing schemes or as a basis for further exploitation.

Risk:

- **Risk Rating:** High
- **Confidence:** Medium
- **Exploitability:** Low (Passive detection)
- **Impact:** Severe (Sensitive Data Disclosure)

Recommendations:

- **Audit All Response Bodies:** Ensure no PII (real or mock) is present in production responses.
- **Mask/Obfuscate Demo Data:** Use placeholder formats that are clearly non-sensitive, e.g., XXXX XXXX XXXX XXXX.
- **Implement Automated Scanning:** Include PII detection in your CI/CD pipeline to prevent regressions.
- **Review for Similar Patterns:** Investigate whether other endpoints contain similar leaks.
- **Comply with PCI DSS:** Ensure adherence to standards regarding sensitive data handling and transmission.

Supporting Evidence:

- **Parameter:** N/A (Passive scan)
- **Input Vector:** Server response
- **Evidence:** 4242 4242 4242 4242
- **Source:** Passive Scan (ZAP Alert 10062 - PII Disclosure)
- **Other Info:** Detected card type: Visa

Additional Notes:

Even if test data, sensitive-looking values can desensitize security tools or personnel to actual issues. Maintaining a clean, compliant response structure is critical in public-facing applications — especially for finance-related services like Stripe.

References:

- CWE-359: Privacy Violation
- PCI DSS Requirements

- OWASP: Sensitive Data Exposure