Sri Lanka Institute of Information Technology

Assignment report 05

IT22357762

Web Security -IE2062

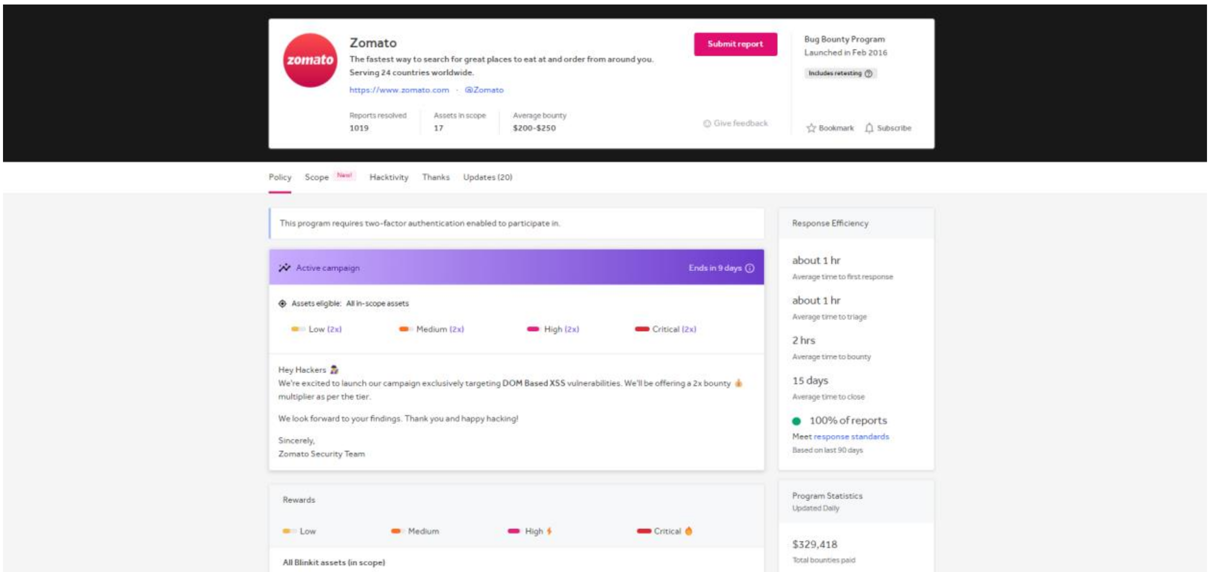
**Web Security – IE2062**

B.Sc. (Hons) in Information

# Contents

# 1 Zomato.com

A website which is for foodies to order their preferences through the site in India and UAE.



Zomato

The fastest way to search for great places to eat at and order from around you. Serving 24 countries worldwide.

https://www.zomato.com · @Zomato

| Reports resolved | Assets in scope | Average bounty |
|---|---|---|
| 1019 | 17 | $200-$250 |

Bug Bounty Program
Launched in Feb 2016

Includes retesting

This program requires two-factor authentication enabled to participate in.

Active campaign — Ends in 9 days

Assets eligible: All in-scope assets

Low (2x) Medium (2x) High (2x) Critical (2x)

Hey Hackers
We're excited to launch our campaign exclusively targeting **DOM Based XSS** vulnerabilities. We'll be offering a 2x bounty multiplier as per the tier.

We look forward to your findings. Thank you and happy hacking!

Sincerely,
Zomato Security Team

Response Efficiency

about 1 hr
Average time to first response

about 1 hr
Average time to triage

2 hrs
Average time to bounty

15 days
Average time to close

100% of reports
Meet response standards
Based on last 90 days

Rewards

Low Medium High Critical

All Blinkit assets (in scope)

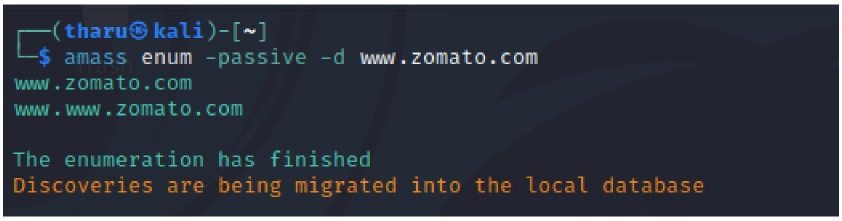
Program Statistics
Updated Daily

$329,418
Total bounties paid

## 1.1 Sub- domain list

Tool – amass

Command – amass enum -passive -d zomato.com



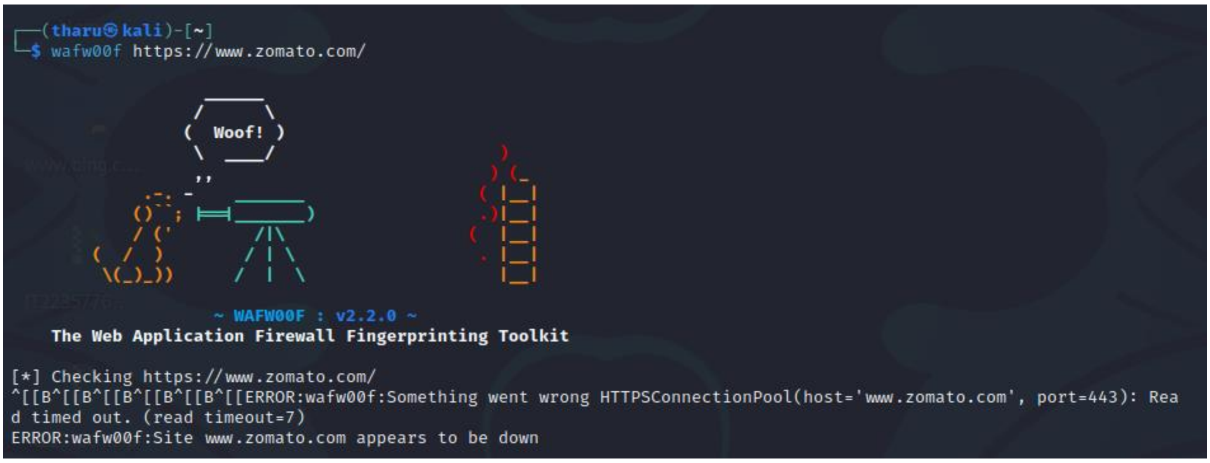
```
┌──(tharu㉿kali)-[~]
└─$ amass enum -passive -d www.zomato.com
www.zomato.com
www.www.zomato.com

The enumeration has finished
Discoveries are being migrated into the local database
```

Sub domain list –

- www.zomato.com
- www.www.zomato.com

## 1.2 Firewall detection

Command – wafw00f https://zomato.com /



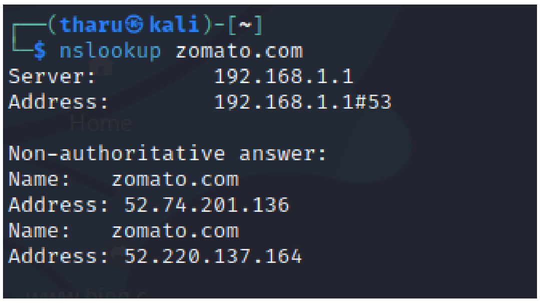
```
┌──(tharu㉿kali)-[~]
└─$ wafw00f https://www.zomato.com/
```

```
                ~ WAFW00F : v2.2.0 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://www.zomato.com/
^[[B^[[B^[[B^[[B^[[B^[[ERROR:wafw00f:Something went wrong HTTPSConnectionPool(host='www.zomato.com', port=443): Rea
d timed out. (read timeout=7)
ERROR:wafw00f:Site www.zomato.com appears to be down
```

## 1.3 IP scanning

Tool – nslookup

Command – nslookup zomato.com

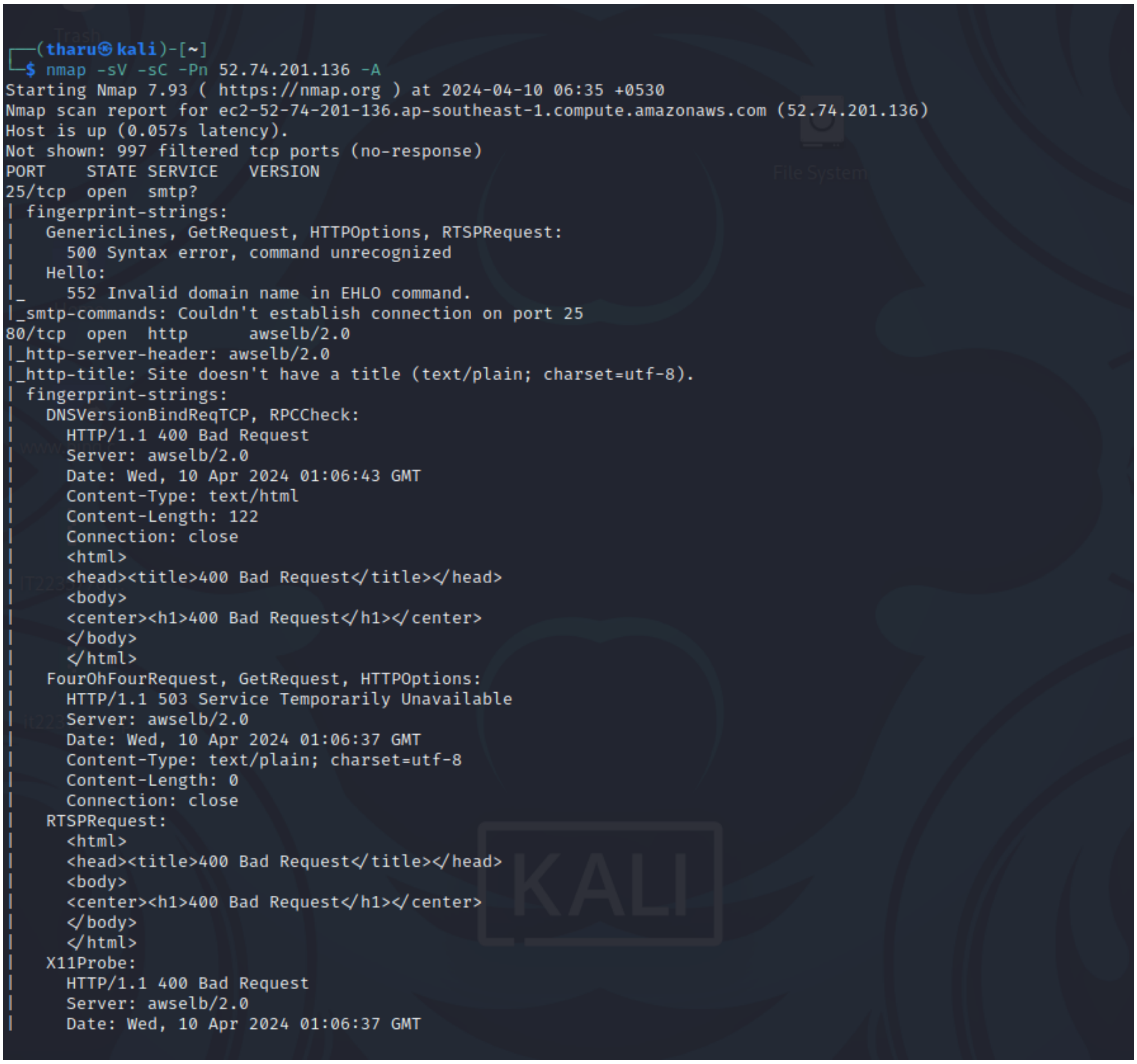


```
┌──(tharu㉿kali)-[~]
└─$ nslookup zomato.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
Name:   zomato.com
Address: 52.74.201.136
Name:   zomato.com
Address: 52.220.137.164
```

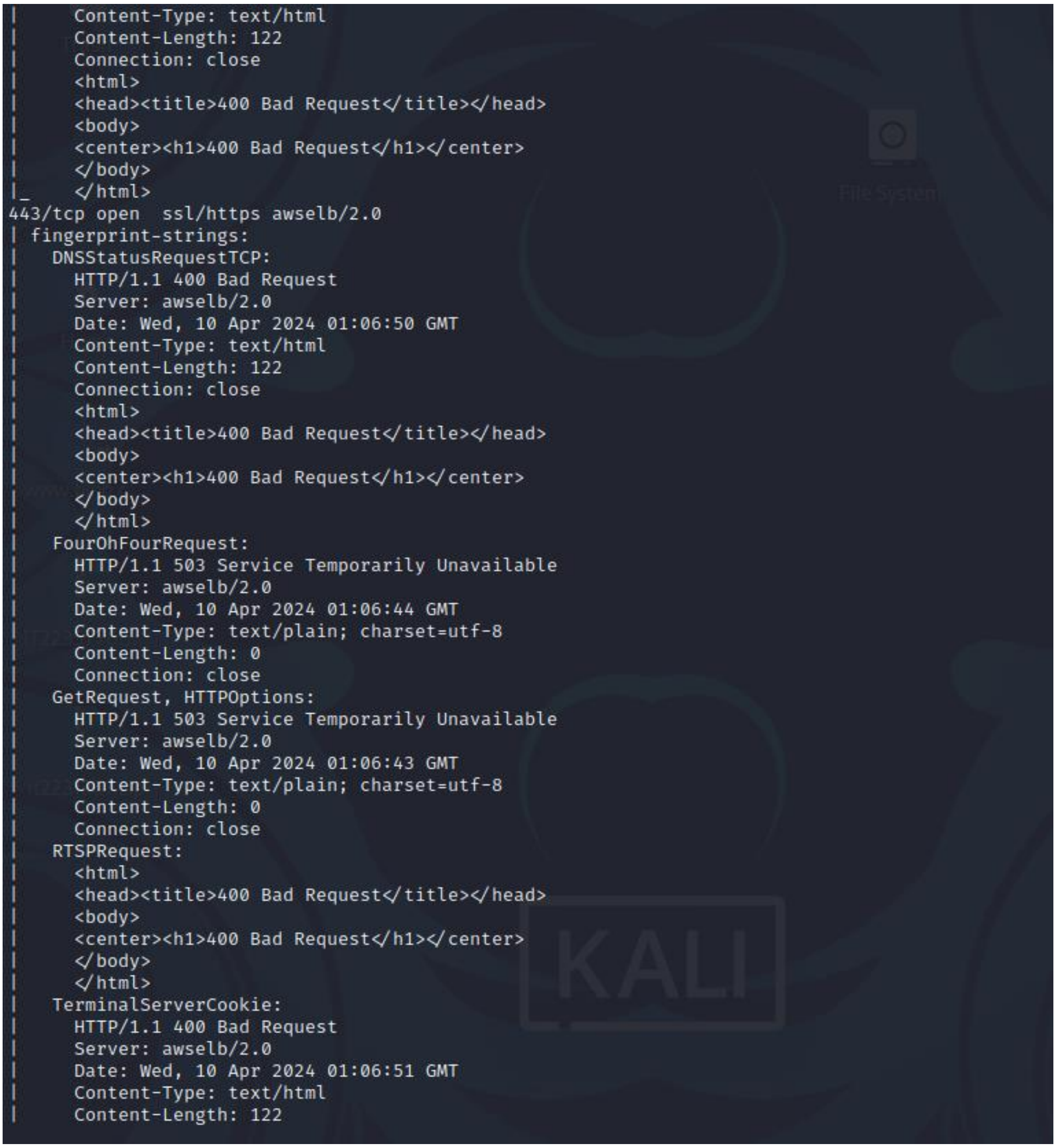
## 1.4 Port scanning

Tool - nmap

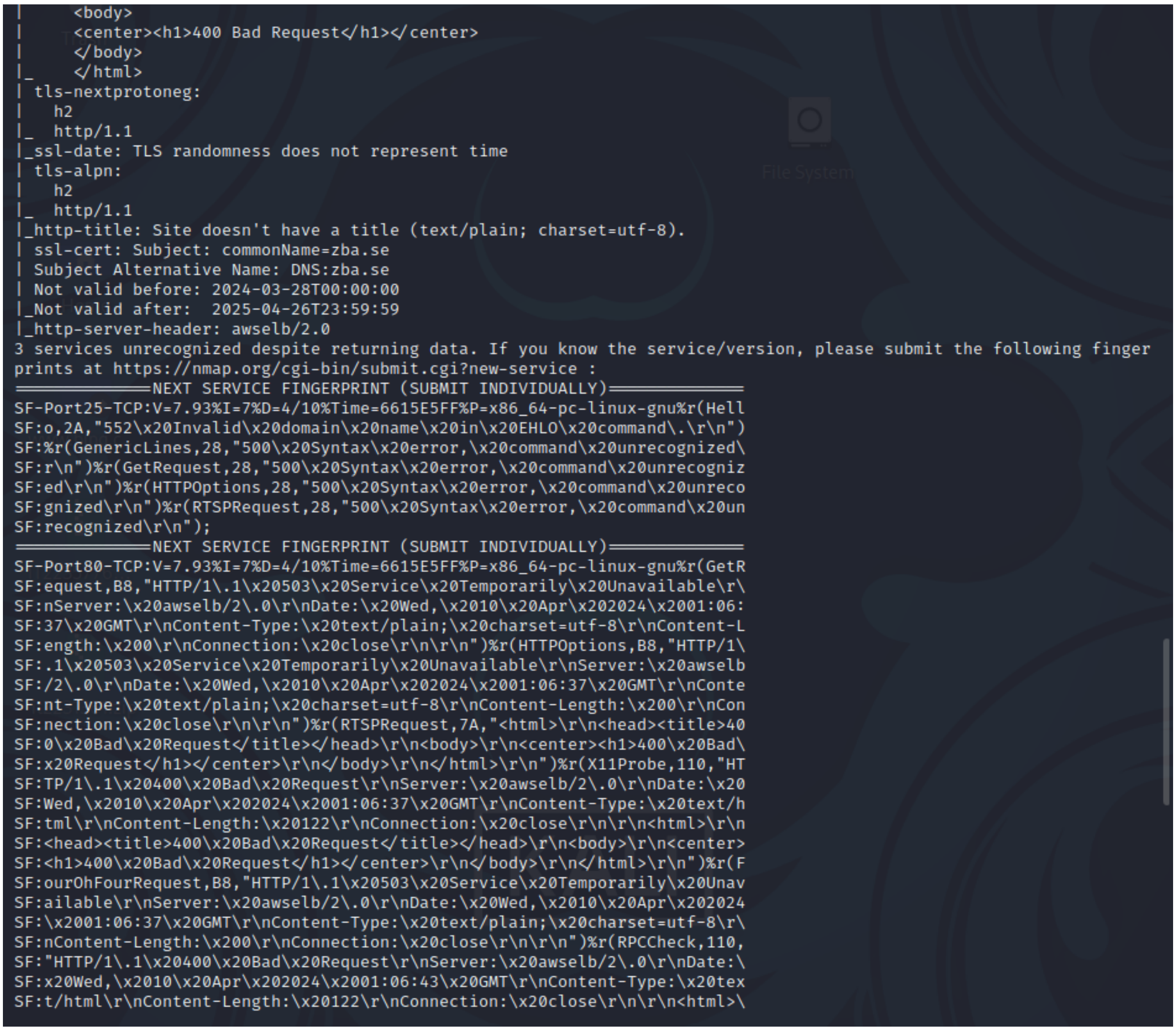
Command – nmap -sV -sC -Pn 108.156.133.112 -A



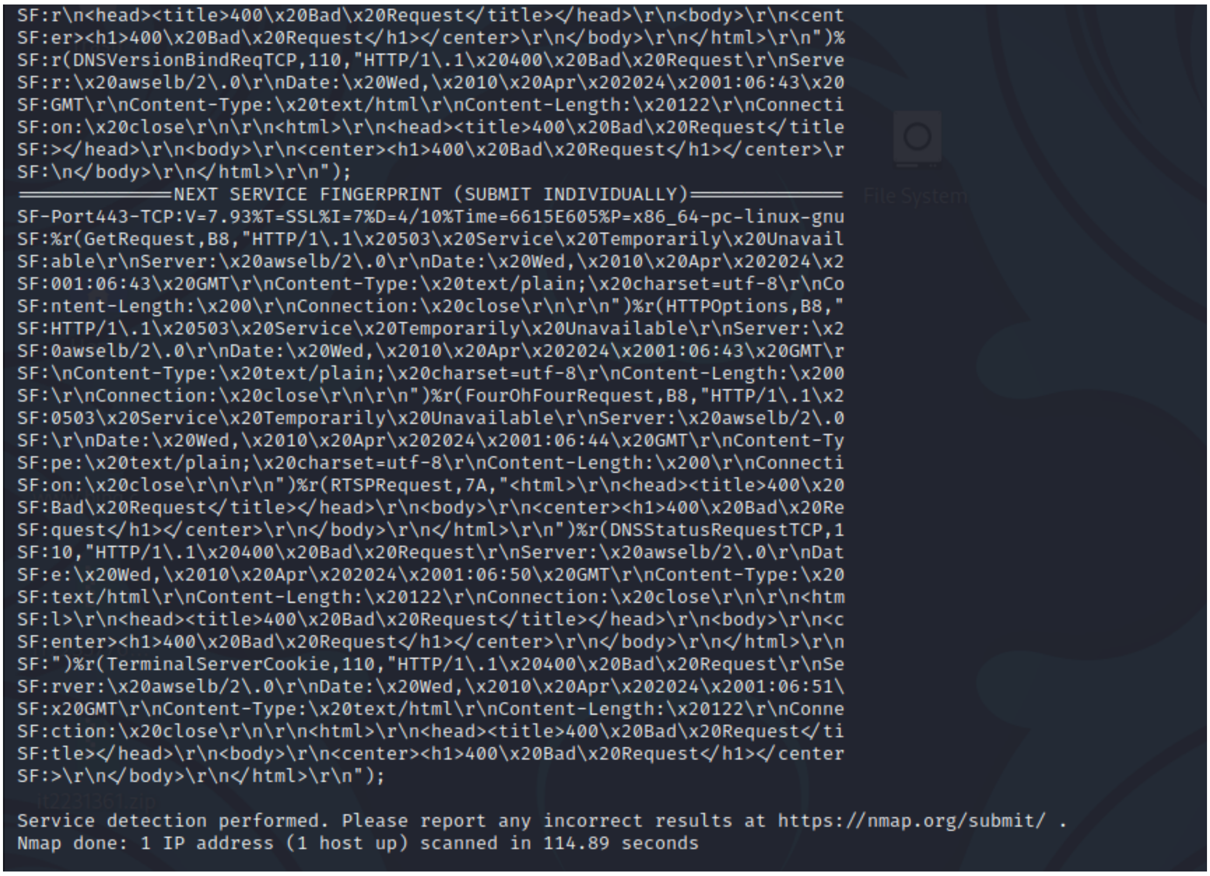
```
┌──(tharu㉿kali)-[~]
└─$ nmap -sV -sC -Pn 52.74.201.136 -A
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-10 06:35 +0530
Nmap scan report for ec2-52-74-201-136.ap-southeast-1.compute.amazonaws.com (52.74.201.136)
Host is up (0.057s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE   VERSION
25/tcp  open  smtp?
| fingerprint-strings:
|   GenericLines, GetRequest, HTTPOptions, RTSPRequest:
|     500 Syntax error, command unrecognized
|   Hello:
|_    552 Invalid domain name in EHLO command.
|_smtp-commands: Couldn't establish connection on port 25
80/tcp  open  http      awselb/2.0
|_http-server-header: awselb/2.0
|_http-title: Site doesn't have a title (text/plain; charset=utf-8).
| fingerprint-strings:
|   DNSVersionBindReqTCP, RPCCheck:
|     HTTP/1.1 400 Bad Request
|     Server: awselb/2.0
|     Date: Wed, 10 Apr 2024 01:06:43 GMT
|     Content-Type: text/html
|     Content-Length: 122
|     Connection: close
|     <html>
|     <head><title>400 Bad Request</title></head>
|     <body>
|     <center><h1>400 Bad Request</h1></center>
|     </body>
|     </html>
|   FourOhFourRequest, GetRequest, HTTPOptions:
|     HTTP/1.1 503 Service Temporarily Unavailable
|     Server: awselb/2.0
|     Date: Wed, 10 Apr 2024 01:06:37 GMT
|     Content-Type: text/plain; charset=utf-8
|     Content-Length: 0
|     Connection: close
|   RTSPRequest:
|     <html>
|     <head><title>400 Bad Request</title></head>
|     <body>
|     <center><h1>400 Bad Request</h1></center>
|     </body>
|     </html>
|   X11Probe:
|     HTTP/1.1 400 Bad Request
|     Server: awselb/2.0
|     Date: Wed, 10 Apr 2024 01:06:37 GMT
```



```
|     Content-Type: text/html
|     Content-Length: 122
|     Connection: close
|     <html>
|     <head><title>400 Bad Request</title></head>
|     <body>
|     <center><h1>400 Bad Request</h1></center>
|     </body>
|_    </html>
443/tcp open  ssl/https awselb/2.0
| fingerprint-strings:
|   DNSStatusRequestTCP:
|     HTTP/1.1 400 Bad Request
|     Server: awselb/2.0
|     Date: Wed, 10 Apr 2024 01:06:50 GMT
|     Content-Type: text/html
|     Content-Length: 122
|     Connection: close
|     <html>
|     <head><title>400 Bad Request</title></head>
|     <body>
|     <center><h1>400 Bad Request</h1></center>
|     </body>
|     </html>
|   FourOhFourRequest:
|     HTTP/1.1 503 Service Temporarily Unavailable
|     Server: awselb/2.0
|     Date: Wed, 10 Apr 2024 01:06:44 GMT
|     Content-Type: text/plain; charset=utf-8
|     Content-Length: 0
|     Connection: close
|   GetRequest, HTTPOptions:
|     HTTP/1.1 503 Service Temporarily Unavailable
|     Server: awselb/2.0
|     Date: Wed, 10 Apr 2024 01:06:43 GMT
|     Content-Type: text/plain; charset=utf-8
|     Content-Length: 0
|     Connection: close
|   RTSPRequest:
|     <html>
|     <head><title>400 Bad Request</title></head>
|     <body>
|     <center><h1>400 Bad Request</h1></center>
|     </body>
|     </html>
|   TerminalServerCookie:
|     HTTP/1.1 400 Bad Request
|     Server: awselb/2.0
|     Date: Wed, 10 Apr 2024 01:06:51 GMT
|     Content-Type: text/html
|     Content-Length: 122
```



```
|     <body>
|     <center><h1>400 Bad Request</h1></center>
|     </body>
|_    </html>
| tls-nextprotoneg:
|   h2
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|   h2
|_  http/1.1
|_http-title: Site doesn't have a title (text/plain; charset=utf-8).
| ssl-cert: Subject: commonName=zba.se
| Subject Alternative Name: DNS:zba.se
| Not valid before: 2024-03-28T00:00:00
|_Not valid after:  2025-04-26T23:59:59
|_http-server-header: awselb/2.0
3 services unrecognized despite returning data. If you know the service/version, please submit the following finger
prints at https://nmap.org/cgi-bin/submit.cgi?new-service :
══════════════NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)══════════════
SF-Port25-TCP:V=7.93%I=7%D=4/10%Time=6615E5FF%P=x86_64-pc-linux-gnu%r(Hell
SF:o,2A,"552\x20Invalid\x20domain\x20name\x20in\x20EHLO\x20command\.\r\n")
SF:%r(GenericLines,28,"500\x20Syntax\x20error,\x20command\x20unrecognized\
SF:r\n")%r(GetRequest,28,"500\x20Syntax\x20error,\x20command\x20unrecogniz
SF:ed\r\n")%r(HTTPOptions,28,"500\x20Syntax\x20error,\x20command\x20unreco
SF:gnized\r\n")%r(RTSPRequest,28,"500\x20Syntax\x20error,\x20command\x20un
SF:recognized\r\n");
══════════════NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)══════════════
SF-Port80-TCP:V=7.93%I=7%D=4/10%Time=6615E5FF%P=x86_64-pc-linux-gnu%r(GetR
SF:equest,B8,"HTTP/1\.1\x20503\x20Service\x20Temporarily\x20Unavailable\r\
SF:nServer:\x20awselb/2\.0\r\nDate:\x20Wed,\x2010\x20Apr\x202024\x2001:06:
SF:37\x20GMT\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nContent-L
SF:ength:\x200\r\nConnection:\x20close\r\n\r\n")%r(HTTPOptions,B8,"HTTP/1\
SF:.1\x20503\x20Service\x20Temporarily\x20Unavailable\r\nServer:\x20awselb
SF:/2\.0\r\nDate:\x20Wed,\x2010\x20Apr\x202024\x2001:06:37\x20GMT\r\nConte
SF:nt-Type:\x20text/plain;\x20charset=utf-8\r\nContent-Length:\x200\r\nCon
SF:nection:\x20close\r\n\r\n")%r(RTSPRequest,7A,"<html>\r\n<head><title>40
SF:0\x20Bad\x20Request</title></head>\r\n<body>\r\n<center><h1>400\x20Bad\
SF:x20Request</h1></center>\r\n</body>\r\n</html>\r\n")%r(X11Probe,110,"HT
SF:TP/1\.1\x20400\x20Bad\x20Request\r\nServer:\x20awselb/2\.0\r\nDate:\x20
SF:Wed,\x2010\x20Apr\x202024\x2001:06:37\x20GMT\r\nContent-Type:\x20text/h
SF:tml\r\nContent-Length:\x20122\r\nConnection:\x20close\r\n\r\n<html>\r\n
SF:<head><title>400\x20Bad\x20Request</title></head>\r\n<body>\r\n<center>
SF:<h1>400\x20Bad\x20Request</h1></center>\r\n</body>\r\n</html>\r\n")%r(F
SF:ourOhFourRequest,B8,"HTTP/1\.1\x20503\x20Service\x20Temporarily\x20Unav
SF:ailable\r\nServer:\x20awselb/2\.0\r\nDate:\x20Wed,\x2010\x20Apr\x202024
SF:\x2001:06:37\x20GMT\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\
SF:nContent-Length:\x200\r\nConnection:\x20close\r\n\r\n")%r(RPCCheck,110,
SF:"HTTP/1\.1\x20400\x20Bad\x20Request\r\nServer:\x20awselb/2\.0\r\nDate:\
SF:x20Wed,\x2010\x20Apr\x202024\x2001:06:43\x20GMT\r\nContent-Type:\x20tex
SF:t/html\r\nContent-Length:\x20122\r\nConnection:\x20close\r\n\r\n<html>\
```

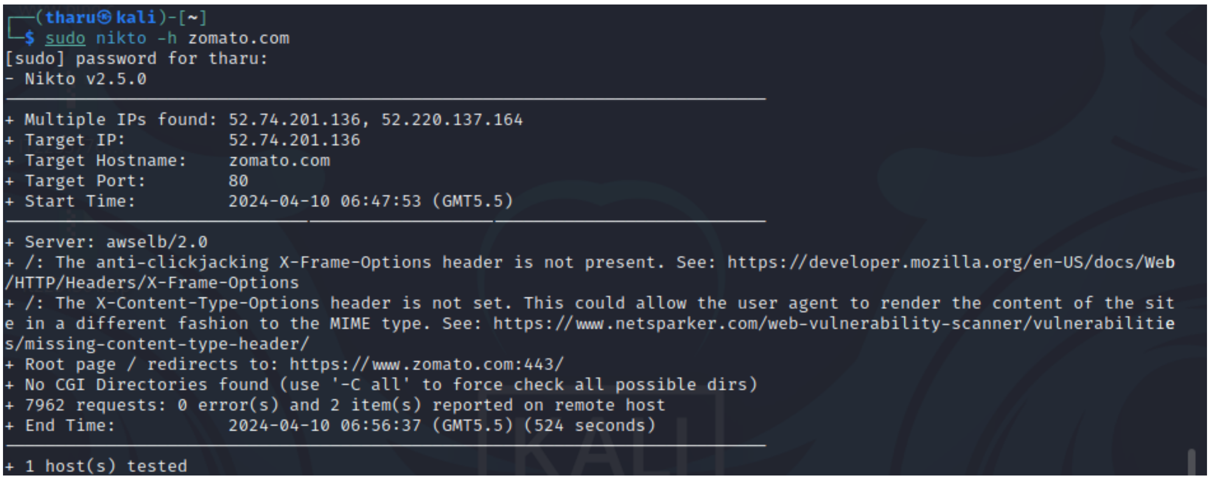


```
SF:r\n<head><title>400\x20Bad\x20Request</title></head>\r\n<body>\r\n<cent
SF:er><h1>400\x20Bad\x20Request</h1></center>\r\n</body>\r\n</html>\r\n")%
SF:r(DNSVersionBindReqTCP,110,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nServe
SF:r:\x20awselb/2\.0\r\nDate:\x20Wed,\x2010\x20Apr\x202024\x2001:06:43\x20
SF:GMT\r\nContent-Type:\x20text/html\r\nContent-Length:\x20122\r\nConnecti
SF:on:\x20close\r\n\r\n<html>\r\n<head><title>400\x20Bad\x20Request</title
SF:></head>\r\n<body>\r\n<center><h1>400\x20Bad\x20Request</h1></center>\r
SF:\n</body>\r\n</html>\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port443-TCP:V=7.93%T=SSL%I=7%D=4/10%Time=6615E605%P=x86_64-pc-linux-gnu
SF:%r(GetRequest,B8,"HTTP/1\.1\x20503\x20Service\x20Temporarily\x20Unavail
SF:able\r\nServer:\x20awselb/2\.0\r\nDate:\x20Wed,\x2010\x20Apr\x202024\x2
SF:001:06:43\x20GMT\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nCo
SF:ntent-Length:\x200\r\nConnection:\x20close\r\n\r\n")%r(HTTPOptions,B8,"
SF:HTTP/1\.1\x20503\x20Service\x20Temporarily\x20Unavailable\r\nServer:\x2
SF:0awselb/2\.0\r\nDate:\x20Wed,\x2010\x20Apr\x202024\x2001:06:43\x20GMT\r
SF:\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nContent-Length:\x200
SF:\r\nConnection:\x20close\r\n\r\n")%r(FourOhFourRequest,B8,"HTTP/1\.1\x2
SF:0503\x20Service\x20Temporarily\x20Unavailable\r\nServer:\x20awselb/2\.0
SF:\r\nDate:\x20Wed,\x2010\x20Apr\x202024\x2001:06:44\x20GMT\r\nContent-Ty
SF:pe:\x20text/plain;\x20charset=utf-8\r\nContent-Length:\x200\r\nConnecti
SF:on:\x20close\r\n\r\n")%r(RTSPRequest,7A,"<html>\r\n<head><title>400\x20
SF:Bad\x20Request</title></head>\r\n<body>\r\n<center><h1>400\x20Bad\x20Re
SF:quest</h1></center>\r\n</body>\r\n</html>\r\n")%r(DNSStatusRequestTCP,1
SF:10,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nServer:\x20awselb/2\.0\r\nDat
SF:e:\x20Wed,\x2010\x20Apr\x202024\x2001:06:50\x20GMT\r\nContent-Type:\x20
SF:text/html\r\nContent-Length:\x20122\r\nConnection:\x20close\r\n\r\n<htm
SF:l>\r\n<head><title>400\x20Bad\x20Request</title></head>\r\n<body>\r\n<c
SF:enter><h1>400\x20Bad\x20Request</h1></center>\r\n</body>\r\n</html>\r\n
SF:")%r(TerminalServerCookie,110,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nSe
SF:rver:\x20awselb/2\.0\r\nDate:\x20Wed,\x2010\x20Apr\x202024\x2001:06:51\
SF:x20GMT\r\nContent-Type:\x20text/html\r\nContent-Length:\x20122\r\nConne
SF:ction:\x20close\r\n\r\n<html>\r\n<head><title>400\x20Bad\x20Request</ti
SF:tle></head>\r\n<body>\r\n<center><h1>400\x20Bad\x20Request</h1></center
SF:>\r\n</body>\r\n</html>\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 114.89 seconds
```

## 1.5 Nikto scanning

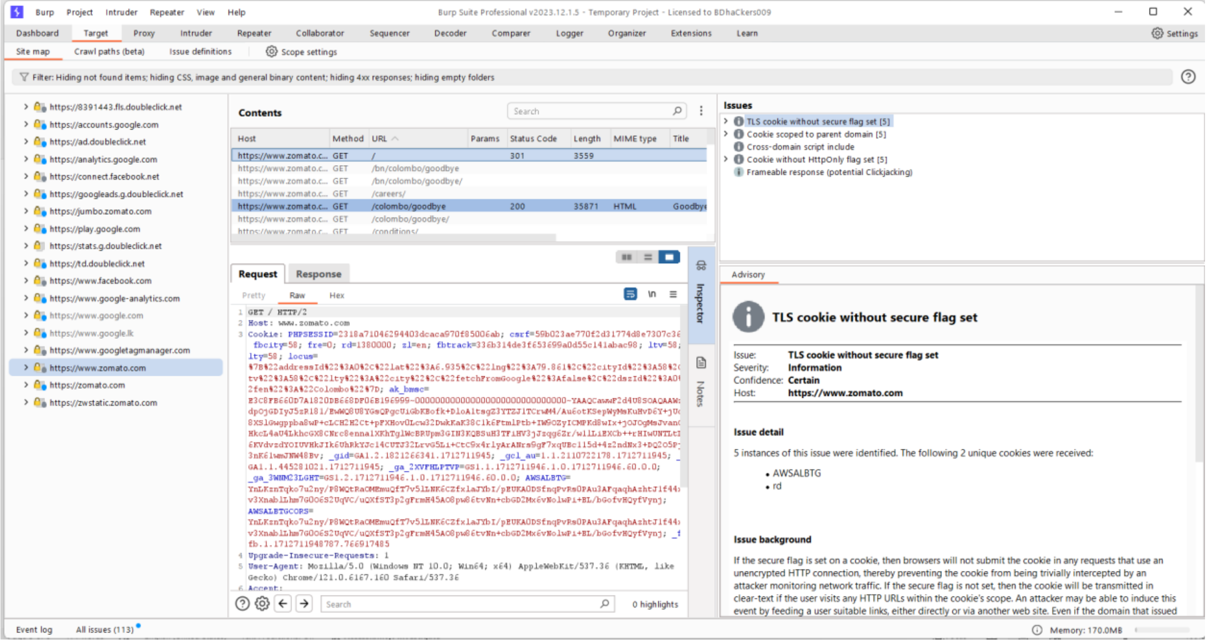
Tool – Nikto

Command - sudo nikto -h zomato.com



```
┌──(tharu㉿kali)-[~]
└─$ sudo nikto -h zomato.com
[sudo] password for tharu:
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 52.74.201.136, 52.220.137.164
+ Target IP:          52.74.201.136
+ Target Hostname:    zomato.com
+ Target Port:        80
+ Start Time:         2024-04-10 06:47:53 (GMT5.5)
---------------------------------------------------------------------------
+ Server: awselb/2.0
+ /: 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 sit
e in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilitie
s/missing-content-type-header/
+ Root page / redirects to: https://www.zomato.com:443/
+ 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:           2024-04-10 06:56:37 (GMT5.5) (524 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

## 1.6 Burpsuite scanning



Burp Suite Professional v2023.12.1.5 - Temporary Project - Licensed to BDhaCkers009

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

- https://8391443.fls.doubleclick.net
- https://accounts.google.com
- https://ad.doubleclick.net
- https://analytics.google.com
- https://connect.facebook.net
- https://googleads.g.doubleclick.net
- https://jumbo.zomato.com
- https://play.google.com
- https://stats.g.doubleclick.net
- https://td.doubleclick.net
- https://www.facebook.com
- https://www.google-analytics.com
- https://www.google.com
- https://www.google.lk
- https://www.googletagmanager.com
- https://www.zomato.com
- https://zomato.com
- https://zwstatic.zomato.com

Contents

| Host | Method | URL | Params | Status Code | Length | MIME type | Title |
|---|---|---|---|---|---|---|---|
| https://www.zomato.c... | GET | / | | 301 | 3559 | | |
| https://www.zomato.c... | GET | /bn/colombo/goodbye | | | | | |
| https://www.zomato.c... | GET | /bn/colombo/goodbye/ | | | | | |
| https://www.zomato.c... | GET | /careers/ | | | | | |
| https://www.zomato.c... | GET | /colombo/goodbye | | 200 | 35871 | HTML | Goodbye |
| https://www.zomato.c... | GET | /colombo/goodbye/ | | | | | |
| https://www.zomato.c... | GET | /conditions/ | | | | | |

Request

```
GET / HTTP/2
Host: www.zomato.com
Cookie: PHPSESSID=2318a71046294403dcaca970f85006ab; csrf=59b023ae770f2d31774d8e7307c36
 fbcity=58; fre=0; rd=1380000; zl=en; fbtrack=336b314de3f653699a0d55c141abac98; ltv=58;
lty=58; locus=
%7B%22addressId%22%3A0%2C%22lat%22%3A6.935%2C%22lng%22%3A79.861%2C%22cityId%22%3A58%2C
tv%22%3A58%2C%22lty%22%3A%22city%22%2C%22fetchFromGoogle%22%3Afalse%2C%22dszId%22%3A0
2fen%22%3A%22Colombo%22%7D; ak_bmsc=
E3C8FB660D7A1820DB668DF06B196999~000000000000000000000000000000~YAAQCawwF2d4U8SOAQAAW
dpOjGDIyJ5zR181/BwWQ8U8YGsQPgcUiGbKBofk+DloAltsgZ3YTZJ1TCrwM4/Au6otKSepWyMsKuHvD6Y+jU
8XSlGwgppba8wP+cLCH2H2Ct+pFXHovOLcw32DwkKaK38C1k6FtmlPtb+IW9OZyICMPKd8wIx+jOJOgMsJvan
HkcL4aU4LkhcGX8CNrc8ennalXKhTglWcBRUpm3GIN3KQBSuH3TFiHV3jJzqg6Zr/wilLiEXCb++rHIwUNTLt
6KVdvzdYOIUVHkJIk6UhRkYJc14CUTJ32LrvG5Li+CtC9x4rlyArANrs9gF7xqUBc115d+4z2ndNx3+DQ2O5P
3nK61wmJNW48Bv; _gid=GA1.2.1821266341.1712711945; _gcl_au=1.1.2110722178.1712711945; _
GA1.1.445281021.1712711945; _ga_2XVFHLPTVP=GS1.1.1712711946.1.0.1712711946.60.0.0;
_ga_3WNM23LGHT=GS1.2.1712711946.1.0.1712711946.60.0.0; AWSALBTG=
YnLKznTqko7u2ny/P8WQtRaOMEmuQfT7v5lLNK6CZfxlaJYbI/pEUKAODSfnqPvRsOPAu3AFqaqhAzhtJ1f44
v3XnablLhm7GOO6S2UqVC/uQXfST3p2gFrmH45AO8pw86tvNn+cbGD2Mx6vNolwPi+BL/bGofvHQyfVynj;
AWSALBTGCORS=
YnLKznTqko7u2ny/P8WQtRaOMEmuQfT7v5lLNK6CZfxlaJYbI/pEUKAODSfnqPvRsOPAu3AFqaqhAzhtJ1f44
v3XnablLhm7GOO6S2UqVC/uQXfST3p2gFrmH45AO8pw86tvNn+cbGD2Mx6vNolwPi+BL/bGofvHQyfVynj; _f
fb.1.1712711948787.766917485
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.6167.160 Safari/537.36
Accept:
```

0 highlights

Issues

- TLS cookie without secure flag set [5]
- Cookie scoped to parent domain [5]
- Cross-domain script include
- Cookie without HttpOnly flag set [5]
- Frameable response (potential Clickjacking)

Advisory

**TLS cookie without secure flag set**

| | |
|---|---|
| Issue: | **TLS cookie without secure flag set** |
| Severity: | **Information** |
| Confidence: | **Certain** |
| Host: | **https://www.zomato.com** |

**Issue detail**

5 instances of this issue were identified. The following 2 unique cookies were received:

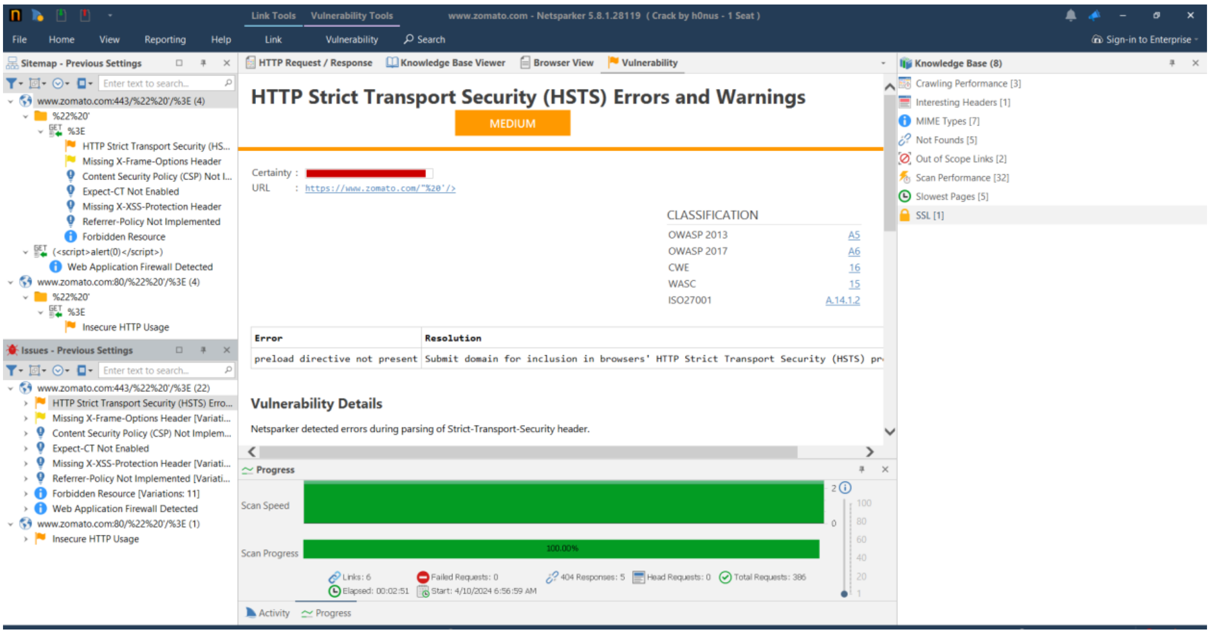
- AWSALBTG
- rd

**Issue background**

If the secure flag is set on a cookie, then browsers will not submit the cookie in any requests that use an unencrypted HTTP connection, thereby preventing the cookie from being trivially intercepted by an attacker monitoring network traffic. If the secure flag is not set, then the cookie will be transmitted in clear-text if the user visits any HTTP URLs within the cookie's scope. An attacker may be able to induce this event by feeding a user suitable links, either directly or via another web site. Even if the domain that issued

Event log  All issues (113)  Memory: 170.0MB

## 1.7 Netspaker scan



www.zomato.com - Netsparker 5.8.1.28119 ( Crack by h0nus - 1 Seat )

Sitemap - Previous Settings

- www.zomato.com:443/%22%20'/%3E (4)
  - %22%20'
    - %3E
      - HTTP Strict Transport Security (HS...
      - Missing X-Frame-Options Header
      - Content Security Policy (CSP) Not I...
      - Expect-CT Not Enabled
      - Missing X-XSS-Protection Header
      - Referrer-Policy Not Implemented
      - Forbidden Resource
  - (<script>alert(0)</script>)
    - Web Application Firewall Detected
- www.zomato.com:80/%22%20'/%3E (4)
  - %22%20'
    - %3E
      - Insecure HTTP Usage

Issues - Previous Settings

- www.zomato.com:443/%22%20'/%3E (22)
  - HTTP Strict Transport Security (HSTS) Erro...
  - Missing X-Frame-Options Header [Variati...
  - Content Security Policy (CSP) Not Implem...
  - Expect-CT Not Enabled
  - Missing X-XSS-Protection Header [Variati...
  - Referrer-Policy Not Implemented [Variati...
  - Forbidden Resource [Variations: 11]
  - Web Application Firewall Detected
- www.zomato.com:80/%22%20'/%3E (1)
  - Insecure HTTP Usage

**HTTP Strict Transport Security (HSTS) Errors and Warnings**

MEDIUM

Certainty :
URL : https://www.zomato.com/"%20'/>

CLASSIFICATION

| | |
|---|---|
| OWASP 2013 | A5 |
| OWASP 2017 | A6 |
| CWE | 16 |
| WASC | 15 |
| ISO27001 | A.14.1.2 |

| Error | Resolution |
|---|---|
| preload directive not present | Submit domain for inclusion in browsers' HTTP Strict Transport Security (HSTS) pr |

**Vulnerability Details**

Netsparker detected errors during parsing of Strict-Transport-Security header.

Knowledge Base (8)

- Crawling Performance [3]
- Interesting Headers [1]
- MIME Types [7]
- Not Founds [5]
- Out of Scope Links [2]
- Scan Performance [32]
- Slowest Pages [5]
- SSL [1]

Progress

Scan Speed
Scan Progress 100.00%

Links: 6  Failed Requests: 0  404 Responses: 5  Head Requests: 0  Total Requests: 386
Elapsed: 00:02:51  Start: 4/10/2024 6:56:59 AM

## 1.8 Vulnerabilities

**Vulnerability Title:** Unsecured HTTP Access Despite HSTS Implementation

**Vulnerability Description**: The target website does not redirect users to HTTPS, even though it has implemented HTTP Strict Transport Security (HSTS). This puts users at risk of security breaches, as HSTS becomes ineffective for those who haven't visited the HTTPS version of the site before.

**Affected Components:** Web server configuration, specifically handling of HTTP requests and redirections.

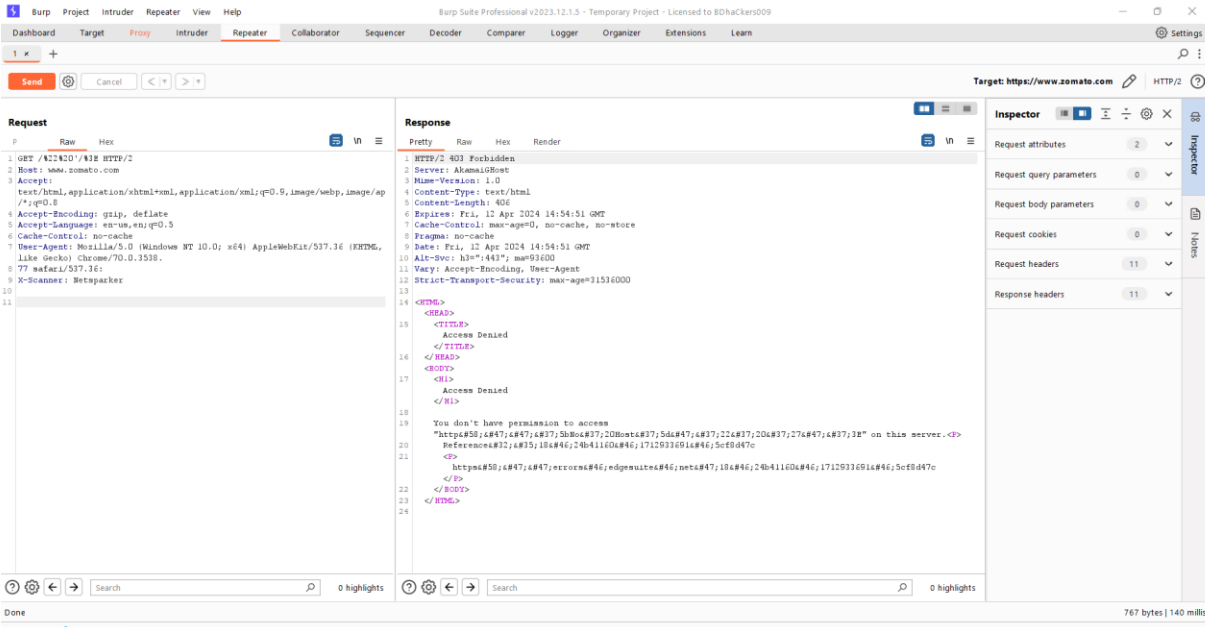
**Impact Assessment:** Impact of vulnerability includes,

- Users do not fully get the benefits of HSTS protection.
- Increases vulnerability to MITM attacks.
- Puts user security and privacy at risk.

**Steps to Reproduce:**

1. Open a web browser and navigate to the target website using an HTTP connection.
2. Observe that the connection is not automatically redirected to HTTPS.
3. Confirm the absence of HSTS enforcement for HTTP connections.

**Proof of concept:**



```
GET /%22%20'/%3E HTTP/2
Host: www.zomato.com
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/70.0.3538.
77 safari/537.36:
X-Scanner: Netsparker
```

```
HTTP/2 403 Forbidden
Server: AkamaiGHost
Mime-Version: 1.0
Content-Type: text/html
Content-Length: 406
Expires: Fri, 12 Apr 2024 14:54:51 GMT
Cache-Control: max-age=0, no-cache, no-store
Pragma: no-cache
Date: Fri, 12 Apr 2024 14:54:51 GMT
Alt-Svc: h3=":443"; ma=93600
Vary: Accept-Encoding, User-Agent
Strict-Transport-Security: max-age=31536000

<HTML>
  <HEAD>
    <TITLE>
      Access Denied
    </TITLE>
  </HEAD>
  <BODY>
    <H1>
      Access Denied
    </H1>

    You don't have permission to access
    "http&#58;&#47;&#47;&#37;5bNo&#37;20Host&#37;5d&#47;&#37;22&#37;20&#37;27&#47;&#37;3E" on this server.<P>
      Reference&#32;&#35;18&#46;24b41160&#46;1712933691&#46;5cf8d47c
      <P>
        https&#58;&#47;&#47;errors&#46;edgesuite&#46;net&#47;18&#46;24b41160&#46;1712933691&#46;5cf8d47c
      </P>
    </BODY>
  </HTML>
```

**Proposed Mitigation or Fix:**

Configure the web server to automatically redirect all HTTP requests to HTTPS. Below is an example configuration for Apache web server:'

# redirect all HTTP to HTTPS

```
<VirtualHost *:80>
 ServerAlias *
 RewriteEngine On
 RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [redirect=301]
</VirtualHost>
```

### 1.8.1 Other vulnerabilities

1. Missing X-Frame-Options Header
2. Content Security Policy (CSP) Not Implemented
3. Expect-CT Not Enabled
4. Missing X-XSS-Protection Header
5. Referrer-Policy Not Implemented
6. Web Application Firewall Detected