

# **Sri Lanka Institute of Information Technology**




## **WEB SECURITY (IE2062)**

### **BUG BOUNTY REPORT 8**

**Thilakarathna S.T.D- IT22578914**

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

# Overview of the website



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](#)

Submit report

Bug Bounty Program

Launched in Feb 2016

Includes retesting

Reports resolved1027

Assets in scope17

Average bounty\$200-\$250

Give feedback

Bookmark

Subscribe

Overview Scope Hacktivity Thanks Updates (20)

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

Rewards

Last updated on April 1, 2024. [View changes](#)

Asset	Low	Medium	High	Critical
	Avg. bounty \$135 31.50% submissions	Avg. bounty \$312 39.63% submissions	Avg. bounty \$615 19.03% submissions	Avg. bounty \$1,612 9.84% submissions
All Blinkit assets (in s...	\$100-\$200	\$200-\$500	\$500-\$1,000	\$1,000-\$2,000

Response Efficiency

1 hour

Average time to first response

1 hour

Average time to triage

...

Average time from triage to bounty

...

Popular and easy to use, Zomato.com is an online resource that offers detailed information about restaurants, food delivery services, and dining experiences in different cities across the globe. In order to make knowledgeable eating selections, users can visit the website to browse a large database of restaurants, read reviews, see menus, and find ratings and images. Zomato is a one-stop shop for foodies since it provides the ease of online ordering and delivery of meals. Zomato.com's global reach has made it the go-to source for those looking for delicious food and eating options when they're traveling or in their hometown.

# Scope

## • InScope

com.application.zomatomerchant	Android: Play Store	In scope	Critical	Ineligible	Sep 14, 2018	5 (0%)
<b>Scope Questions: Items not explicitly listed here</b> If you have a question about something that is not explicitly listed as out-of-scope or in-scope, please submit a report and we will provide clarification. We will allow you to self close that report after we answer your question.						
	Other	In scope	Critical	Ineligible	Feb 8, 2020	2 (0%)
*.zdev.net	Wildcard	In scope	Critical	Eligible	May 15, 2023	3 (0%)
All Assets (other than Blinkit) Bounty table header	Other	In scope	Critical	Eligible	Jul 13, 2023	5 (0%)
winecellar.zomato.com	Domain	In scope	Critical	Eligible	Jul 24, 2017	0 (0%)
blinkit.com	Domain	In scope	Critical	Eligible	May 4, 2023	5 (0%)
api.grofers.com	Domain	In scope	Critical	Eligible	May 4, 2023	3 (0%)
*.hyperpure.com	Wildcard	In scope	Critical	Eligible	May 15, 2023	28 (3%)
434613896 Zomato: Food Delivery & Dining	iOS: App Store	In scope	Critical	Eligible	May 4, 2023	8 (1%)
*.runnr.in Amazon Web Services Go Rails Ruby	Wildcard	In scope	Critical	Eligible	May 15, 2023	100 (10%)
http://*.grofer.io	Wildcard	In scope	Critical	Eligible	May 26, 2023	1 (0%)
com.application.zomato	Android: Play Store	In scope	Critical	Eligible	Jul 24, 2017	40 (4%)
http://*.grofers.com	Wildcard	In scope	Critical	Eligible	Nov 22, 2023	2 (0%)
*.zomans.com This domain is mainly used for internal applications that are hosted in AWS. Our area of interest is any issue that can potentially give anyone unrestricted access or expose internal or confidential data.	Wildcard	In scope	Critical	Eligible	May 15, 2023	15 (1%)
api2.grofers.com	Domain	In scope	Critical	Eligible	May 4, 2023	5 (0%)
*.zomato.com	Wildcard	In scope	Critical	Eligible	May 15, 2023	496 (48%)
All Blinkit assets (in scope)	Other	In scope	Critical	Eligible	Jun 8, 2023	10 (1%)

## • OutScope

www.zomatobook.com	Domain	Out of scope	<div><div></div></div> None	\$ Ineligible	Feb 23, 2021	0 (0%)
business-blog.zomato.com	Domain	Out of scope	<div><div></div></div> None	\$ Ineligible	Jul 24, 2017	0 (0%)
com.application.zomato.ordering	Android: Play Store	Out of scope	<div><div></div></div> None	\$ Ineligible	Oct 5, 2020	0 (0%)
blog.zomato.com	Domain	Out of scope	<div><div></div></div> None	\$ Ineligible	Jul 24, 2017	0 (0%)
community.zomato.com	Domain	Out of scope	<div><div></div></div> None	\$ Ineligible	Jul 24, 2017	0 (0%)
dev.hyperpure.com	Domain	Out of scope	<div><div></div></div> None	\$ Ineligible	Nov 25, 2020	0 (0%)
devapi.hyperpure.com	Domain	Out of scope	<div><div></div></div> None	\$ Ineligible	Nov 25, 2020	0 (0%)
devpod.hyperpure.com	Domain	Out of scope	<div><div></div></div> None	\$ Ineligible	Nov 25, 2020	0 (0%)
success.zomato.com	Domain	Out of scope	<div><div></div></div> None	\$ Ineligible	Mar 4, 2020	0 (0%)
send.zomato.com	Domain	Out of scope	<div><div></div></div> None	\$ Ineligible	Jan 18, 2021	0 (0%)
staging*.runnr.in Please don't test on staging/dev instances. Instead, we have created a dedicated environment <code>bugbounty.runnr.in</code> which is a replica of the same for testing.	Wildcard	Out of scope	<div><div></div></div> None	\$ Ineligible	May 15, 2023	0 (0%)
http://*.blinkit.support	Wildcard	Out of scope	<div><div></div></div> None	\$ Ineligible	May 4, 2023	0 (0%)
http://*.blinkit.in	Wildcard	Out of scope	<div><div></div></div> None	\$ Ineligible	May 4, 2023	0 (0%)
http://*.blinkit.com	Wildcard	Out of scope	<div><div></div></div> None	\$ Ineligible	May 4, 2023	0 (0%)
960335206 Blinkit's iOS App. The app itself is out of scope, but the APIs used by it are in scope: api.grofers.com, api2.grofers.com.	iOS: App Store	Out of scope	<div><div></div></div> None	\$ Ineligible	Jul 13, 2023	0 (0%)
*.zomatoportugal.com	Wildcard	Out of scope	<div><div></div></div> None	\$ Ineligible	Jul 17, 2023	0 (0%)

# Information Gathering

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

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

## Subdomains for Hunting

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

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

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

- **Sublist3r**

Sublist3r is an open-source program used for efficient subdomain enumeration. Penetration testers, security experts, and ethical hackers utilize Sublist3r to locate subdomains linked to a target website. It accomplishes this by using methods like search engine scraping and DNS requests. Sublist3r only needs the target domain to be input; once that is done, it will look for relevant subdomains on its own and provide useful data that may be utilized for vulnerability assessments and security evaluations.

```

(tharusha@kali)-[~]
$ sublist3r -d zomato.com -SS/dirsearch
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 08:31 EDT
Nmap scan report for zomato.in (11.122.141.18)
Host is up (0.011s latency).
Other addresses for zomato.in (11.122.141.18): 11.122.141.17
rDNS record for 11.122.141.18: ec2-111-141-17-ap-1.theeast-1.compute.amazonaws.com
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    open  smtp

[-] Enumerating subdomains now for zomato.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..(1 host up) scanned in 5.61 seconds
[-] Searching now in Bing..
[-] Searching now in Ask..XSS/dirsearch
[-] Searching now in Netcraft..in zomato.com
[-] Searching now in DNSDumpster..ap.org ) at 2024-05-10 08:31 EDT
[-] Searching now in Virustotal..completed (1 up), 1 undergoing Script Scan
[-] Searching now in ThreatCrowd..: 08:36 (0:00:03 remaining)
[-] Searching now in SSL Certificates..1122,17)
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found:139.141.18.in-addr.arpa
www.zomato.com
148api.zomato.com
api.zomato.com
apibeta.zomato.com: Couldn't find any DOM based XSS.
apitest.zomato.com: Couldn't find any CSRF vulnerabilities.
cert1.zomato.com: Couldn't find any stored XSS vulnerabilities.
www.cert1.zomato.com
cert2.zomato.comaddress (1 host up) scanned in 370.79 seconds
cert3.zomato.com
chat-emqx.zomato.com ~/PwnXSS/dirsearch
www.chat-emqx.zomato.com
community.zomato.com
culture.zomato.com
www.culture.zomato.com
developer.zomato.com
engineering.zomato.com
www.engineering.zomato.com
fddkim.zomato.com
jumbo.zomato.com
link.zomato.com
payments-preprod.zomato.com
www.payments-preprod.zomato.com
success.zomato.com
www.success.zomato.com
techblog.zomato.com
www.techblog.zomato.com
trace.zomato.com

```

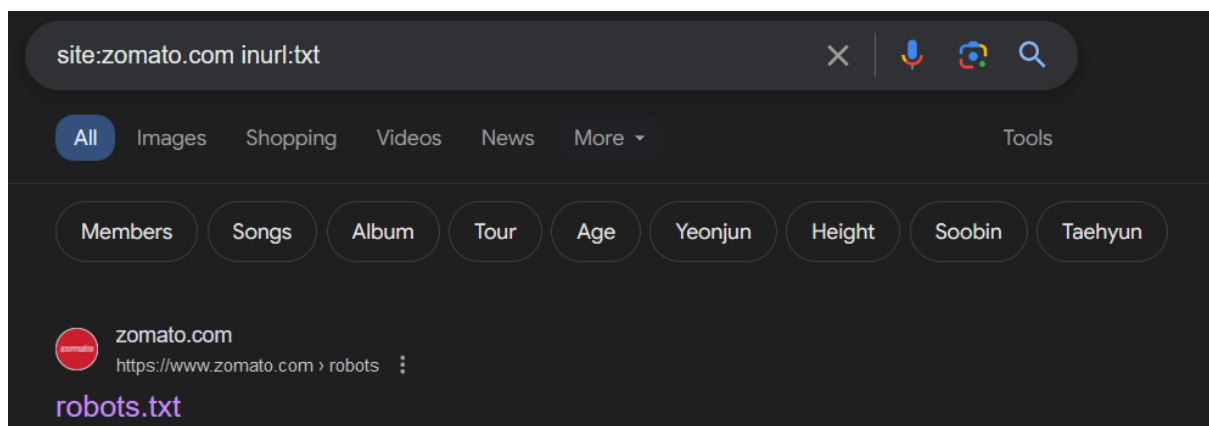
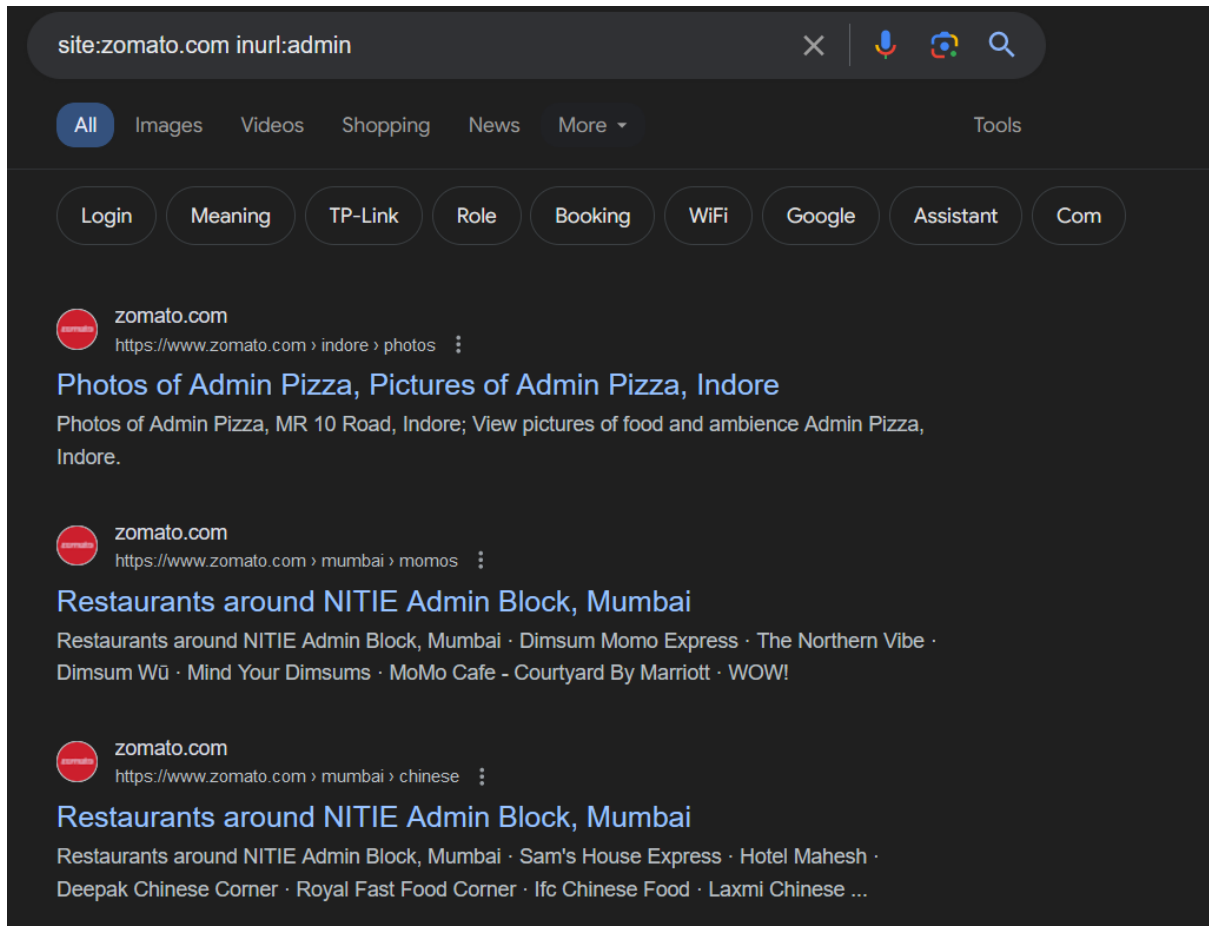
```

trace.zomato.com
www.trace.zomato.com
traceapi.zomato.comress (1 host up) scanned in 5.61 seconds
www.traceapi.zomato.com
upload.zomato.com ~/PwnXSS/dirsearch
www.upload.zomato.com
w4b.zomato.com: 94SVN ( https://nmap.org ) at 2024-05-10 08:31 EDT
winecellar.zomato.com: 0 hosts completed (1 up), 1 undergoing Script Scan
www.winecellar.zomato.com: 08:36 (0:00:03 remaining)
winecellar-internal.zomato.com (11.122.141.17)
zpay.zomato.com (not scanned): 11.122.141.18
www.zpay.zomato.com (not scanned): 11.122.141.18
zpay-test.zomato.com (11.122.141.17, 17.122.141.18, in-addr.arpa

```

- Google dorking

Google Dorking, also called Google Hacking, is the practice of using sophisticated search operators and specific queries on the Google search engine to locate publicly accessible resources, configuration problems, or private information that isn't often indexed in the results of ordinary searches.



- **Dnsdumpster**

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

















## Result of Zomato.com

dns recon & research, find & lookup dns records
















zomato.com|

Search ➔

### DNS Servers

ns-1286.awsdns-32.org.    	205.251.197.6	AMAZON-02 United States
ns-1692.awsdns-19.co.uk.    	205.251.198.156	AMAZON-02 United States
ns-290.awsdns-36.com.    	205.251.193.34	AMAZON-02 United States
ns-671.awsdns-19.net.    	205.251.194.159	AMAZON-02 United States

### MX Records \*\* This is where email for the domain goes...

1 aspmx.l.google.com.   	142.251.16.27	GOOGLE United States
10 alt3.aspmx.l.google.com.   	142.250.27.27	GOOGLE United States
10 alt4.aspmx.l.google.com.   	142.250.153.27	GOOGLE United States
5 alt1.aspmx.l.google.com.   	209.85.202.27	GOOGLE United States
5 alt2.aspmx.l.google.com.   	64.233.184.26	GOOGLE United States

### TXT Records \*\* Find more hosts in Sender Policy Framework (SPF) configurations

"1pnjjb976t7ibv64fgrj493rru"
"6vtg3aj924ngq9aihmjdubmatr"
"MS=681EABA93C6738668E47C44B5C6F731BCC209CBA"
"MS=ms61350724"
"OSSRH-79203"
"ZOOM_verify_LuCSrep5aiBpuCPrBRJAt"
"adobe-sign-verification=6a09126310927f379735c2b7d09e1928"
"amazonses:3ufcI9pD6ZqyPNibcDPmG70sgJIGL96bhztrM07aetY="
"apple-domain-verification=Rk06Ca9pwkhEVb3j"
"asv=ee90273cd94d45be0643f9560ab11a13"
"atlassian-domain-verification=ij/zffeNyj/cdw9nnzBhqAewaQ8jbKcdZ6MhkaED5oCmIINjjnnE2d4MMHBRv0ra"
"atlassian-domain-verification=xk1sbtz9KG90VSRfeHaeL+vc+9DRfFAqj3u+VN31tRUuchQyL4oQ0IwrkV58Z+ca"
"facebook-domain-verification=1ruwb1jydxmw9hzm1k1l3fslew576w"
"google-site-verification=6DiggAJt4qMxLocEM80xq8VDJSdn9bXLSfQdkpXX4hI"
"google-site-verification=Sp13-UHI3mhI_6mGbZ72rjIBjVcp4aJ-IKw4mEfMhN4"
"mongodb-site-verification=pStQEfLyuqXcvxeCLWbclfnUKZlkxE9"
"new-relic-domain-verification=f46254d748a3482685d5f42e31380261"
"twilio-domain-verification=35e81b8100d53ee70ce9f5c2d7f17078"
"v=spf1 include:_spf.google.com include:helpscoutemail.com include:_spf.salesforce.com include:amazonses.com include:_spf.zoho.com include:transmail.net -all"
"yandex-verification: 40f795c808dc1e7e"
"zoho-verification=zb78844917.zmverify.zoho.com"



- **DNSrecon**

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

```
(root@kali)-[/home/tharusha]
# dnsrecon -d zomato.com
[*] std: Performing General Enumeration against: zomato.com...
[-] DNSSEC is not configured for zomato.com
[*] SOA ns-1692.awsdns-19.co.uk 205.251.198.156
[*] SOA ns-1692.awsdns-19.co.uk 2600:9000:5306:9c00::1
[*] NS ns-1692.awsdns-19.co.uk 205.251.198.156
[*] NS ns-1692.awsdns-19.co.uk 2600:9000:5306:9c00::1
[*] NS ns-290.awsdns-36.com 205.251.193.34
[*] NS ns-290.awsdns-36.com 2600:9000:5301:2200::1
[*] NS ns-671.awsdns-19.net 205.251.194.159
[*] NS ns-1286.awsdns-32.org 205.251.197.6
[*] NS ns-1286.awsdns-32.org 2600:9000:5305:600::1
[*] MX alt2.aspmx.l.google.com 142.250.141.26
[*] MX alt3.aspmx.l.google.com 142.250.115.26
[*] MX alt1.aspmx.l.google.com 173.194.202.27
[*] MX aspmx.l.google.com 64.233.170.26
[*] MX alt4.aspmx.l.google.com 64.233.171.27
[*] MX alt2.aspmx.l.google.com 2607:f8b0:4023:c0b::1a
[*] MX alt3.aspmx.l.google.com 2607:f8b0:4023:1004::1b
[*] MX alt1.aspmx.l.google.com 2607:f8b0:400e:c00::1b
[*] MX aspmx.l.google.com 2404:6800:4003:c02::1a
[*] MX alt4.aspmx.l.google.com 2607:f8b0:4003:c15::1a
[*] A zomato.com 13.250.78.23
[*] A zomato.com 18.141.122.17
[*] AAAA zomato.com 64:ff9b::dfa:4e17
[*] AAAA zomato.com 64:ff9b::128d:7a11
[*] TXT _dmarc.zomato.com v=DMARC1; p=reject; pct=100; sp=reject; aspf=r
[*] Enumerating SRV Records
[-] No SRV Records Found for zomato.com
```

- **WHOIS**

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

```
(root@kali)-[/home/tharusha]
# whois zomato.com
Domain Name: ZOMATO.COM
Registry Domain ID: 357990270_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.101domain.com
Registrar URL: http://101domain.com
Updated Date: 2023-05-22T22:09:13Z
Creation Date: 2006-02-24T23:57:07Z
Registry Expiry Date: 2033-02-24T23:57:07Z
Registrar: 101domain GRS Limited
Registrar IANA ID: 1011
Registrar Abuse Contact Email: abuse@101domain.com
Registrar Abuse Contact Phone: +17604448674
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS-1286.AWSDNS-32.ORG
Name Server: NS-1692.AWSDNS-19.CO.UK
Name Server: NS-290.AWSDNS-36.COM
Name Server: NS-671.AWSDNS-19.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-05-10T13:04:17Z <<<
```

```
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: ZOMATO.COM
Registrar WHOIS Server: whois.101domain.com
Registrar URL: https://www.101domain.com/
Updated Date: 2023-05-22T22:09:13Z
Creation Date: 2006-02-24T23:57:07Z
Registrar Registration Expiration Date: 2033-02-24T23:57:07Z
Registrar: https://www.101domain.com/
Registrar IANA ID: 1011
Registrar Abuse Contact Email: abuse@101domain.com
Registrar Abuse Contact Phone: +1.8582954626
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: serverTransferProhibited http://www.icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited http://www.icann.org/epp#serverUpdateProhibited
Domain Status: serverDeleteProhibited http://www.icann.org/epp#serverDeleteProhibited
Registrant State/Province:
Registrant Country: IN
TO CONTACT REGISTRANT, COMPLETE THIS FORM: https://my.101domain.com/contact-registrant/ZOMATO.COM.html
Name Server: NS-1692.AWSDNS-19.CO.UK
Name Server: NS-290.AWSDNS-36.COM
Name Server: NS-1286.AWSDNS-32.ORG
Name Server: NS-671.AWSDNS-19.NET
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net
For more information on Whois status codes, please visit https://www.icann.org/resources/pages/epp-status-codes-2014-06-16-en.
>>> Last update of WHOIS database: 2024-05-10T13:03:45Z <<<
```

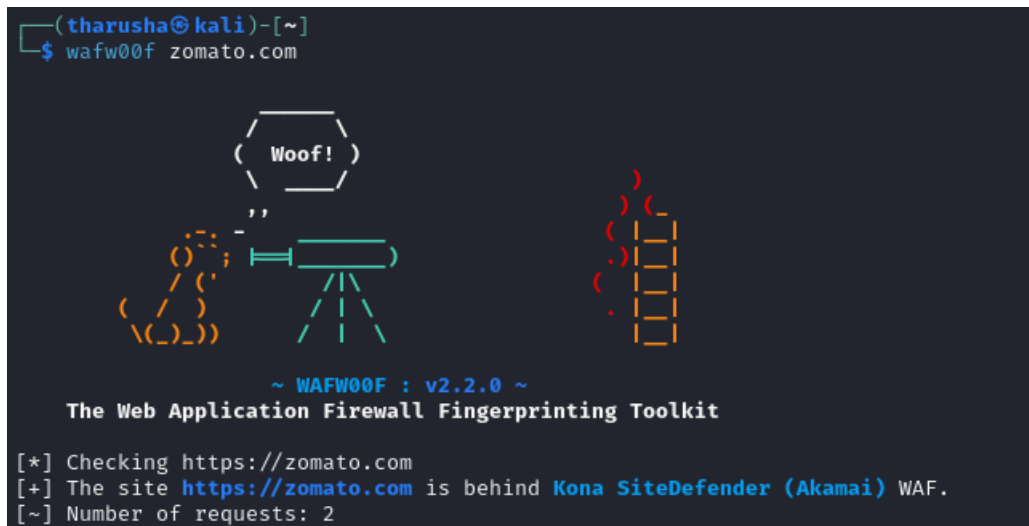
- **Whatweb**

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

```
(tharusha@kali): ~
# whatweb zomato.com
http://zomato.com [301 Moved Permanently] Country[UNITED STATES][us], HTTPServer[awselb/2.0], IP[13.250.78.23], RedirectLocation[https://www.zomato.com:443/], Title[301 Moved Permanently]
https://www.zomato.com/ [403 Forbidden] Akamai-Global-Host, Country[UNITED STATES][us], HTTPServer[AkamaiGObject], IP[96.12.150.177], Strict-Transport-Security[max-age=31536000], Title[Access Denied], UncommonHeaders[alt-svc]
```

- **Wafw00f**

We can see that Kona SiteDefender WAF is protecting zomato.com.



- **Using nmap, open port enumeration**

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

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

```
(tharusha@kali)-[~/PwnXSS/dirsearch]
$ sudo nmap -sS zomato.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 08:31 EDT
Nmap scan report for zomato.com (18.141.122.17)
Host is up (0.015s latency).
Other addresses for zomato.com (not scanned): 13.250.78.23
rDNS record for 18.141.122.17: ec2-18-141-122-17.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 5.61 seconds

(tharusha@kali)-[~/PwnXSS/dirsearch]
$ sudo nmap -p 80 --script vuln zomato.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 08:31 EDT
Stats: 0:04:58 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.12% done; ETC: 08:36 (0:00:03 remaining)
Nmap scan report for zomato.com (18.141.122.17)
Host is up (0.032s latency).
Other addresses for zomato.com (not scanned): 13.250.78.23
rDNS record for 18.141.122.17: 17.122.141.18.in-addr.arpa
PORT      STATE SERVICE
80/tcp    open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
Nmap done: 1 IP address (1 host up) scanned in 370.79 seconds
```

- **Using Nikto to scan for vulnerabilities**

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

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

```
(tharusha@kali) [~/PwnXSS/dirsearch]
$ sudo nikto -h 18.141.122.17
- Nikto v2.5.0

+ Target IP: 18.141.122.17
+ Target Hostname: 18.141.122.17
+ Target Port: 80
+ Start Time: 2024-05-10 08:51:53 (GMT-4)

+ 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 site in a different fashion to the
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

## Exploitation

I employed SQLMAP tool to identify SQL injection vulnerabilities in the target web application for the exploitations.

- **SQLmap**

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

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

```
(tharusha@kali) [~]
$ sqlmap -u 'https://www.zomato.com/colombo/goodbye'

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 09:21:10 /2024-05-10/

[09:21:10] [WARNING] you've provided target URL without any GET parameters (e.g. 'http://www.site.com/article.php?id=1') and without providing any POST parameters through option '--data'
do you want to try URI injections in the target URL itself? [Y/n/a] y
[09:21:11] [INFO] testing connection to the target URL
[09:21:11] [CRITICAL] WAF/IPS identified as 'Kuna Site Defender (Akamai Technologies)'
[09:21:11] [WARNING] potential permission problems detected ('Access Denied')
[09:21:11] [WARNING] the web server responded with an HTTP error code (403) which could interfere with the results of the tests
[09:21:11] [INFO] checking if the target URL content is stable
[09:21:11] [WARNING] target URL content is not stable (i.e. content differs), sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case of junk results, refer to user's manual paragraph "Page comparison"
how do you want to proceed? [(Continue)/(string)/(regex)/(quit)] y
[09:21:10] [INFO] testing if URI parameter 'id*' is dynamic
[09:21:10] [INFO] URI parameter 'id*' appears to be dynamic
[09:21:10] [CRITICAL] heuristic (basic) test shows that URI parameter 'id*' might not be injectable
[09:21:10] [INFO] testing for SQL injection on URI parameter 'id*'
[09:21:10] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[09:21:10] [WARNING] reflective value(s) found and filtering out
[09:21:10] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[09:21:10] [INFO] testing 'MySQL > 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[09:21:10] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[09:21:10] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[09:21:10] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (SQLType)'
[09:21:10] [INFO] testing 'Generic inline queries'
[09:21:10] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[09:21:10] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[09:21:10] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[09:21:10] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (query SLEEP)'
[09:21:10] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[09:21:10] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[09:21:10] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n/a] y
[09:21:10] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[09:21:10] [WARNING] URI parameter 'id*' does not seem to be injectable
[09:21:10] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=spacecomment') and/or switch '--random-agent'
[09:21:10] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 78 times
```

## Vulnerabilities detect when Scanning

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

Software for scanning and managing vulnerabilities in web applications is called Netsparker.

Its goal is to make it simpler for companies to identify and address security issues with their

web applications. When evaluating web applications, Netsparker automatically looks for common security flaws like Remote Code Execution, SQL Injection, and Cross-Site Scripting (XSS).

## 1. Vulnerability Title

# 1. HTTP Strict Transport Security (HSTS) Errors and Warnings

MEDIUM  1

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

### Impact

The HSTS Warning and Error may allow attackers to bypass HSTS, effectively allowing them to read and modify your communication with the website.

### Vulnerabilities

1.1. <https://www.zomato.com/>

## How to mitigate

Ideally, you should think about adding your domain to the HSTS preload list after resolving the issues and warnings. By doing this, you can make sure that browsers connect to your website automatically using HTTPS, proactively blocking users from accessing it through HTTP. Because this list is hardcoded into users' browsers, it will activate HSTS before they even visit your page, removing the requirement for Trust On First Use (TOFU) and all of its drawbacks. Your website won't meet the requirements necessary to be included to the browser's preload list unless you address the issues and warnings.

Browser vendors declared:

- Serve a valid certificate
- If you are listening on port 80, redirect all domains from HTTP to HTTPS on the same host. Serve all subdomains over HTTPS:
  - In particular, you must support HTTPS for the www subdomain if a DNS record for that subdomain exists
- Serve an HSTS header on the base domain for HTTPS requests:
  - The max-age must be at least 31536000 seconds (1 year)
  - The includeSubDomains directive must be specified
  - The preload directive must be specified

- If you are serving an additional redirect from your HTTPS site, that redirect must have the HSTS header (rather than the page it redirects to)

## 2. Vulnerability Title

## 2. Insecure HTTP Usage

MEDIUM  1

Netsparker identified that the target website allows web browsers to access to the website over HTTP and doesn't redirect them to HTTPS.

HSTS is implemented in the target website however HTTP requests are not redirected to HTTPS. This decreases the value of HSTS implementation significantly.

For example visitors who haven't visited the HTTPS version of the website previously will not be able to take advantage of HSTS.

### Impact

Users will not be able to take advantage of HSTS which almost renders the HSTS implementation useless. Not having HSTS will make MITM attacks easier for attackers.

If there is a client side redirect to HTTPS version of the website (via JavaScript or Meta tags) then you can ignore this vulnerability.

### Vulnerabilities

2.1. <http://www.zomato.com/>

## How to mitigate

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

Specifically, you should have modified the httpd.conf file for Apache. Please see the External References section for additional setup options.



### 3. Vulnerability Title

## 3. Missing X-Frame-Options Header

LOW  1

---

Netsparker detected a missing X-Frame-Options header which means that this website could be at risk of a clickjacking attack.

The X-Frame-Options HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a frame or an iframe. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.

#### Impact

Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to other another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

### How to mitigate

- Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.
  - X-Frame-Options: DENY It completely denies to be loaded in frame/iframe.
  - X-Frame-Options: SAMEORIGIN It allows only if the site which wants to load has a same origin.
  - X-Frame-Options: ALLOW-FROM URL It grants a specific URL to load itself in a iframe. However please pay attention to that, not all browsers support this.
- Employing defensive code in the UI to ensure that the current frame is the most top level window