# Sri Lanka Institute of Information Technology

**WEB SECURITY**

**(IE2062)**

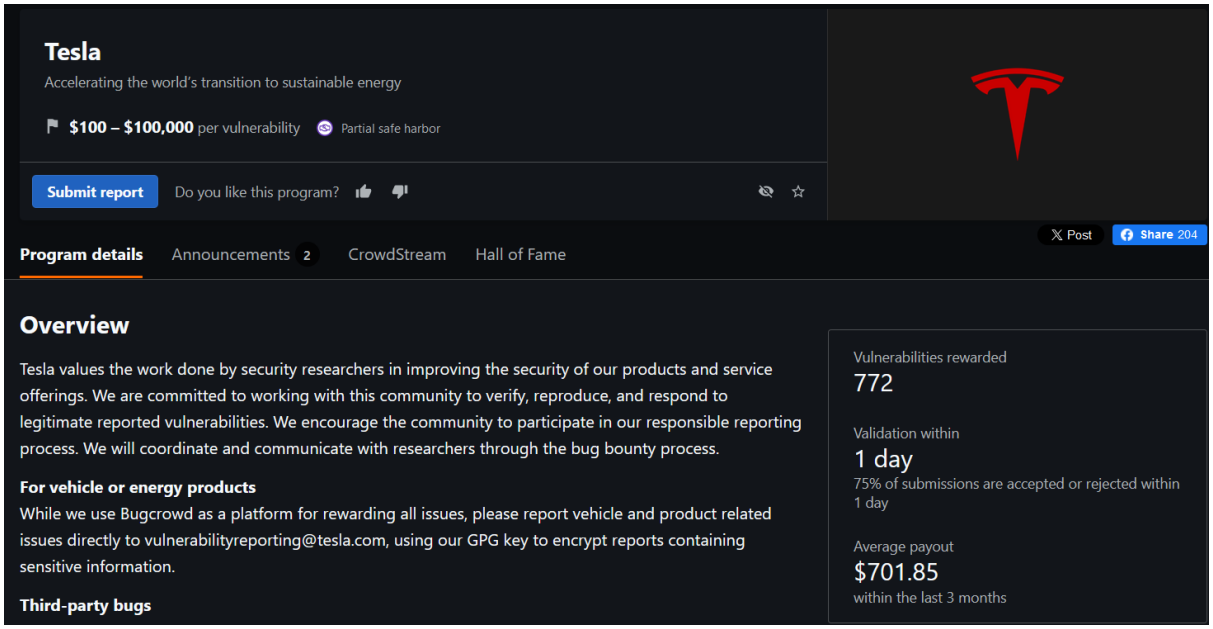
**BUG BOUNTY**

**REPORT 10**

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

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

# Overview of the website




The official website of the innovative American electric vehicle and clean energy corporation Tesla, Inc. is Tesla.com. This website acts as a digital entry point into the world of Tesla, providing details on their cutting-edge solar energy products, energy storage systems, and electric vehicles. On Tesla.com, customers may peruse the newest models, personalize and place orders for Tesla automobiles, and discover the company's dedication to environmental impact and sustainability. Updates on Tesla's technology developments, such as its Autopilot and Full Self-Driving capabilities, are also available on the website. It embodies Tesla's objective to hasten the global transition to sustainable energy and acts as a thorough resource for anybody interested in electric mobility and green energy solutions.

# Scope

- **InScope**

**Non-vehicle vulnerabilities** — In scope

| P1 | P2 | P3 | P4 |
|---|---|---|---|
| $3000 – $10000 | $500 – $4000 | $200 – $700 | $100 – $200 |

| | |
|---|---|
| *.tesla.com | Akamai CDN, Varnish, Drupal, +3 |
| *.tesla.cn | Akamai CDN, Cloudflare CDN, Varnish, +5 |
| *.teslamotors.com | Website Testing |
| *.tesla.services | Website Testing |
| *.teslainsuranceservices.com | Website Testing |
| *.solarcity.com | Website Testing |
| Any host verified to be owned by Tesla Motors Inc. (domains/IP space/etc.) | Website Testing |

| | |
|---|---|
| Official Tesla Android apps | Java, Android, Mobile Applicati..., +1 |
| Official Tesla iOS apps | Objective-C, SwiftUI, Swift, +2 |
| Tesla Energy hardware you own | |

- **OutScope**

| OUT OF SCOPE | Out of scope |
|---|---|
| Any domains from acquisitions, such as maxwell.com | Website Testing |
| employeefeedback.tesla.com | Website Testing |
| energysupport.tesla.com (you can report vulnerabilities to bugbounty.zoho.com) | Website Testing |
| engage.tesla.com | Website Testing |
| feedback.tesla.com | Website Testing |
| feedback.teslamotors.com | Website Testing |
| ir.teslamotors.com | Website Testing |
| ir.tesla.com | Website Testing |
| mkto.teslamotors.com | Website Testing |
| service.tesla.cn/docs/* | Website Testing |
| service.tesla.com/docs/* | Website Testing |
| shop.eu.teslamotors.com | Website Testing |
| Any other third-party websites hosted by non-Tesla entities | Website Testing |

# 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

Subdomain enumeration involves using Kali Linux's robust tools to locate and list subdomains that are linked to a target domain. Through the identification of potential entry points and weak spots, this process helps security experts and ethical hackers assess the company's digital environment. Due to its array of tools, including `Sublist3r} and `Amass} for DNS searches, search engine scraping, and other techniques, Kali Linux is a well-liked platform for security evaluations.

- **Sublist3r**

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

```
┌──(tharusha㉿kali)-[~]
└─$ sublist3r -d tesla.com

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for tesla.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 324
www.tesla.com
CitiApiEncProdv4.tesla.com
CitiApiEncSandboxv4.tesla.com
CitiApiSslProdv4.tesla.com
CitiApiSslSandboxv4.tesla.com
CitiBankStatementSHA512.tesla.com
OpenADRClient.tesla.com
Payx-CitiAPI-Prod.tesla.com
ai-api.tesla.com
ai-api-stg.tesla.com
ai-api-uat.tesla.com
akamai-apigateway-vehicleextinfogw-prdsvc-st.tesla.com
akamai-apigateway-vehicleextinfogw-stgsvc-st.tesla.com
ams13-gpgw1.tesla.com
apac-cppm.tesla.com
apacvpn.tesla.com
apacvpn1.tesla.com
apacvpn2.tesla.com
api-account-master.tesla.com
api-toolbox.tesla.com
sentry.app.tesla.com
appplayer.tesla.com
autodiscover.tesla.com
awsbtest.tesla.com
bctpay.tesla.com
billing.tesla.com
```

```
ciscoguest.tesla.com
citiapiencpoc.tesla.com
citiapiencpocV2.tesla.com
citiapiencpocV3.tesla.com
citiapisslpoc.tesla.com
citiapisslpocV2.tesla.com
citiapisslpocV3.tesla.com
fleetview.prd.america.vn.cloud.tesla.com
apf-api.eng.vn.cloud.tesla.com
mobile-links.eng.vn.cloud.tesla.com
mobile-links-cdn.eng.vn.cloud.tesla.com
owner-api.eng.vn.cloud.tesla.com
signaling-robotics.eng.vn.cloud.tesla.com
vehicle-files.eng.vn.cloud.tesla.com
fleet-api.prd.eu.vn.cloud.tesla.com
fleetview.prd.europe.vn.cloud.tesla.com
vehicle-files.eng.euw1.vn.cloud.tesla.com
vehicle-files.prd.euw1.vn.cloud.tesla.com
fleet-api.prd.na.vn.cloud.tesla.com
apf-api.prd.vn.cloud.tesla.com
mobile-links.prd.vn.cloud.tesla.com
mobile-links-cdn.prd.vn.cloud.tesla.com
mobile-ops-links.prd.vn.cloud.tesla.com
vehicle-files.prd.vn.cloud.tesla.com
acme-sentry-4.eng.use1.vn.cloud.tesla.com
acme-sentry-4a.eng.use1.vn.cloud.tesla.com
tripx.eng.usw2.vn.cloud.tesla.com
vehicle-files.eng.usw2.vn.cloud.tesla.com
vehicle-files.prd.usw2.vn.cloud.tesla.com
cn.tesla.com
cnvpn.tesla.com
cnvpn1.tesla.com
manager.courses.tesla.com
sandbox-manager.courses.tesla.com
sandbox-studio.courses.tesla.com
www.sandbox-studio.courses.tesla.com
studio.courses.tesla.com
cradlepointtest01.tesla.com
cryptopay.tesla.com
cryptopay2.tesla.com
cryptopay3.tesla.com
cryptopay4.tesla.com
cx-apac.tesla.com
cx-apac-stg.tesla.com
cx-api-apac.tesla.com
cx-api-apac-stg.tesla.com
cxadmin-apac.tesla.com
cxadmin-apac-stg.tesla.com
cxadmin-api-apac.tesla.com
cxadmin-api-apac-stg.tesla.com
cxengine-apac.tesla.com
cxengine-apac-stg.tesla.com
```

```
cxengine-apac-stg.tesla.com
cyberbeer.tesla.com
dal11-gpgw1.tesla.com
de.tesla.com
dev.tesla.com
dev-hermes-qd.tesla.com
dgf.tesla.com
digitalassets.tesla.com
digitalassets-accounts.tesla.com
digitalassets-contents.tesla.com
digitalassets-energy.tesla.com
digitalassets-learning.tesla.com
digitalassets-secure.tesla.com
digitalassets-shop.tesla.com
digitalassets-stage.tesla.com
doraemon-svc-apac.tesla.com
doraemon-svc-apac-stg.tesla.com
click.emails.tesla.com
image.emails.tesla.com
view.emails.tesla.com
employee-teslatequila.tesla.com
employeefeedback.tesla.com
energy.tesla.com
gridlogic.energy.tesla.com
www.gridlogic.energy.tesla.com
gridlogic-eng.energy.tesla.com
powerhub.energy.tesla.com
www.powerhub.energy.tesla.com
autobidder.powerhub.energy.tesla.com
autobidder-eng.powerhub.energy.tesla.com
autobidder-preprd.powerhub.energy.tesla.com
gridlogic.powerhub.energy.tesla.com
gridlogic-eng.powerhub.energy.tesla.com
energydesk.tesla.com
energysupport.tesla.com
engage.tesla.com
eua-origin.tesla.com
eumirror.tesla.com
events.tesla.com
factory-berlin.tesla.com
feedback.tesla.com
fleetview.america.fn.tesla.com
fleetview.prd.america.fn.tesla.com
fleetview.prd.eu.fn.tesla.com
fleetview.europe.fn.tesla.com
fleetview.prd.europe.fn.tesla.com
fleetview.prd.euw1.fn.tesla.com
fleetview.fn.tesla.com
fleetview.prd.na.fn.tesla.com
fleetview.prd.usw2.fn.tesla.com
forums.tesla.com
fra05-gpgw1.tesla.com
```

```
github.tesla.com
assets.github.tesla.com
avatars.github.tesla.com
codeload.github.tesla.com
docker.github.tesla.com
gist.github.tesla.com
maven.github.tesla.com
media.github.tesla.com
notebooks.github.tesla.com
npm.github.tesla.com
nuget.github.tesla.com
pages.github.tesla.com
raw.github.tesla.com
render.github.tesla.com
reply.github.tesla.com
rubygems.github.tesla.com
s3-sidekick-ssl.github.tesla.com
uploads.github.tesla.com
viewscreen.github.tesla.com
github-ap.tesla.com
assets.github-ap.tesla.com
avatars.github-ap.tesla.com
codeload.github-ap.tesla.com
docker.github-ap.tesla.com
gist.github-ap.tesla.com
maven.github-ap.tesla.com
media.github-ap.tesla.com
notebook.github-ap.tesla.com
notebooks.github-ap.tesla.com
npm.github-ap.tesla.com
nuget.github-ap.tesla.com
pages.github-ap.tesla.com
raw.github-ap.tesla.com
render.github-ap.tesla.com
reply.github-ap.tesla.com
rubygems.github-ap.tesla.com
uploads.github-ap.tesla.com
viewscreen.github-ap.tesla.com
github-fw.tesla.com
assets.github-fw.tesla.com
avatars.github-fw.tesla.com
codeload.github-fw.tesla.com
docker.github-fw.tesla.com
gist.github-fw.tesla.com
maven.github-fw.tesla.com
media.github-fw.tesla.com
notebook.github-fw.tesla.com
notebooks.github-fw.tesla.com
npm.github-fw.tesla.com
nuget.github-fw.tesla.com
pages.github-fw.tesla.com
raw.github-fw.tesla.com
```

```
github-it.tesla.com
assets.github-it.tesla.com
avatars.github-it.tesla.com
codeload.github-it.tesla.com
docker.github-it.tesla.com
gist.github-it.tesla.com
maven.github-it.tesla.com
media.github-it.tesla.com
notebook.github-it.tesla.com
notebooks.github-it.tesla.com
npm.github-it.tesla.com
nuget.github-it.tesla.com
pages.github-it.tesla.com
raw.github-it.tesla.com
render.github-it.tesla.com
reply.github-it.tesla.com
rubygems.github-it.tesla.com
uploads.github-it.tesla.com
viewscreen.github-it.tesla.com
githubmirror.tesla.com
githubmirroraus08.tesla.com
githubmirrorber02.tesla.com
gpv.tesla.com
hnd13-gpgw1.tesla.com
iad05-gpgw1.tesla.com
ion.tesla.com
ir.tesla.com
kronos.tesla.com
api.kronos.tesla.com
integration.kronos.tesla.com
mobile.kronos.tesla.com
wdm.kronos.tesla.com
wim.kronos.tesla.com
kronos-dev.tesla.com
kronosdb.tesla.com
dev.kronosdb.tesla.com
lax32-gpgw1.tesla.com
learning-apac.tesla.com
learning-apac-stg.tesla.com
lighthouse.tesla.com
lionpayshare.tesla.com
lionpaytest.tesla.com
lionshare.tesla.com
logcollector-ext.tesla.com
logtransit-ext.tesla.com
marketing.tesla.com
mfa-dev.tesla.com
mfamobile-dev.tesla.com
mfauser-dev.tesla.com
mfg.tesla.com
mirror.tesla.com
monitoring.tesla.com
```

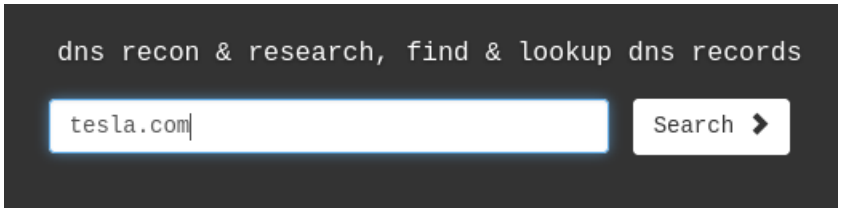
```
new-dev.tesla.com
nv.tesla.com
ny.tesla.com
obs.tesla.com
x3-eng.obs.tesla.com
x3-prod.obs.tesla.com
paloalto.tesla.com
paymentrecon.tesla.com
paymentrecon-stage.tesla.com
pilot-bpay.tesla.com
qa.tesla.com
raultest.tesla.com
referral.tesla.com
resources.tesla.com
rumipv6.tesla.com
studio.sandbox-courses.tesla.com
sc-cppm.tesla.com
sca.tesla.com
secureaccess.tesla.com
serviceapp.tesla.com
sin05-gpgw1.tesla.com
sjc36-gpgw1.tesla.com
sling.tesla.com
smarttax.tesla.com
smt.tesla.com
solarbonds.tesla.com
sso.tesla.com
sso-dec.tesla.com
sso-dev.tesla.com
sso-sandbox.tesla.com
sso-sig.tesla.com
stage.tesla.com
static.tesla.com
syd14-gpgw1.tesla.com
tesla-inc-docsys-eorg.tesla.com
teslacmgap01.tesla.com
teslacmgcn01.tesla.com
teslacmgeu01.tesla.com
teslacmgna01.tesla.com
teslacmgus01.tesla.com
teslaquila.tesla.com
www.teslaquila.tesla.com
teslatequila.tesla.com
www.teslatequila.tesla.com
toolbox.tesla.com
www.toolbox.tesla.com
toolbox-beta.tesla.com
track.tesla.com
triton-management.tesla.com
triton-management-stg.tesla.com
triton-management-uat.tesla.com
triton-server.tesla.com
```

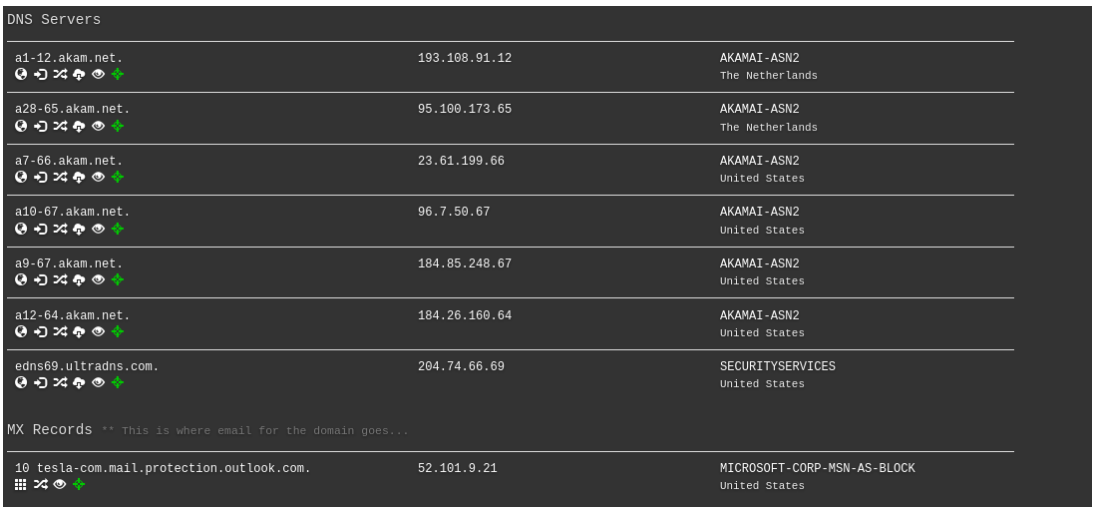
```
triton-server-stg.tesla.com
triton-server-uat.tesla.com
tvs.tesla.com
tvs-api.tesla.com
tvs-api-stg.tesla.com
tvs-api-uat.tesla.com
tvs-stg.tesla.com
tvs-uat.tesla.com
tx.tesla.com
ug.tesla.com
www.ug.tesla.com
vpn.tesla.com
vpn1.tesla.com
www.vpn1.tesla.com
vpn2.tesla.com
vpn3.tesla.com
vrp-stg.tesla.com
warpbilling.tesla.com
www-dev.tesla.com
www-stg2.tesla.com
www-test.tesla.com
www-uat.tesla.com
www-uat2.tesla.com
www45.tesla.com
```

- **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 tesla.com



DNS Servers

| | | |
|---|---|---|
| a1-12.akam.net. | 193.108.91.12 | AKAMAI-ASN2<br>The Netherlands |
| a28-65.akam.net. | 95.100.173.65 | AKAMAI-ASN2<br>The Netherlands |
| a7-66.akam.net. | 23.61.199.66 | AKAMAI-ASN2<br>United States |
| a10-67.akam.net. | 96.7.50.67 | AKAMAI-ASN2<br>United States |
| a9-67.akam.net. | 184.85.248.67 | AKAMAI-ASN2<br>United States |
| a12-64.akam.net. | 184.26.160.64 | AKAMAI-ASN2<br>United States |
| edns69.ultradns.com. | 204.74.66.69 | SECURITYSERVICES<br>United States |

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

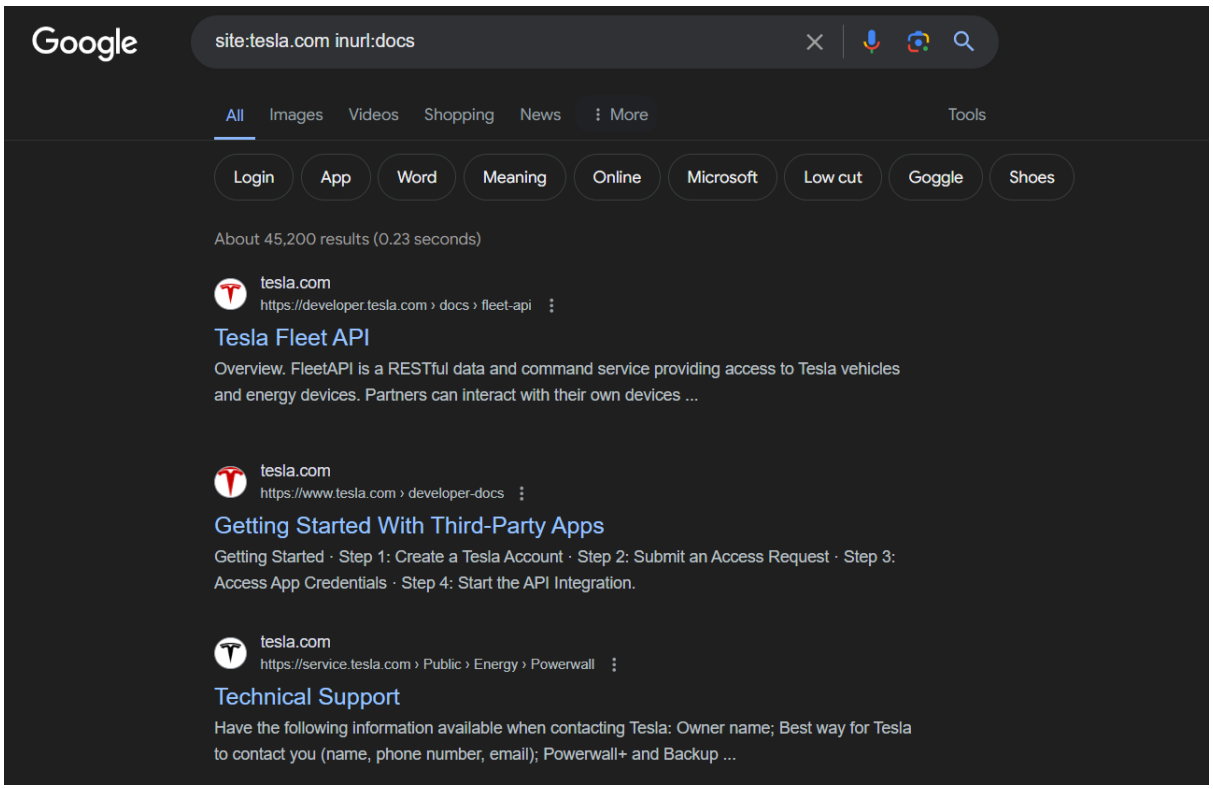
| | | |
|---|---|---|
| 10 tesla-com.mail.protection.outlook.com. | 52.101.9.21 | MICROSOFT-CORP-MSN-AS-BLOCK<br>United States |

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

```
"adobe-idp-site-verification=321c026a-3a8c-4206-a1fa-391a59585c54"
"onetrust-domain-verification=480735b10e124e23916192d7e4321902"
"onetrust-domain-verification=79a1328740f44bc48dd97ab52c0c3377"
"ms-domain-verification=e335cec9-0ff5-4a54-b8bc-8966a8d146db"
"SFMC-qkAv7SvlQaslp7NEALX8t68s_AZWOQB6ThKQS5l5"
"55zNJIDU0xk94IfGJtL+Hh+wje5JzOS6GY+ntggZF908AUsx0LBKgr+Nln3CgZEUifxSuN09M05jYpdbd6+cpw=="
"adobe-sign-verification=efb2da198047b7a154bd604d2721038b"
"apple-domain-verification=C9J7eOtEbm7Dqr88"
"bugcrowd-verification=40bd5dd89a6e4073ca9bc76feac3a47b"
"google-site-verification=Y7lbse5bSatjXaqSBOWXjsit4mOp9cQzfLDpnQUSZlg"
"logmein-domain-confirmation=9zxwVn2buGWrLtU24J88"
"MS=ms22358213"
"T0E0S29854"
"teamviewer-sso-verification=2fc989f75b19494fab5eb0e2c22dd625"
"traction-guest=b4f7ad59-bf17-4b3c-8b36-9c2d28f1de32"
"zapier-domain-verification-challenge=64e810e8-0fe1-4de0-b104-229592811c5b"
"docker-verification=74d1ec4e-a7a6-48a7-9568-9bd0faac833f"
"v=spf1 ip4:54.240.84.225/32 ip4:54.240.84.226/31 ip4:54.240.84.228/30 ip4:54.240.84.232/29 ip4:54.240.84.240/29 ip4:54.240.84.248/30
ip4:54.240.84.252/32 ip4:44.239.249.139 ip4:52.24.70.112 ip4:34.223.204.78 ip4:213.244.145.203 ip4:213.244.145.219 ip4:213" ".244.145.204
ip4:213.244.145.220 ip4:8.47.24.203 ip4:8.47.24.219 ip4:8.47.24.204 ip4:8.47.24.220 ip4:8.45.124.203 ip4:8.45.124.219 ip4:8.45.124.204
ip4:8.45.124.220 ip4:8.21.14.203 ip4:8.21.14.219 ip4:8.21.14.204 ip4:8.21.14.220 ip4:8.21.14.194 ip4:8.21.1" "4.211 ip4:212.49.145.0/24
ip4:91.103.52.0/22 ip4:168.245.123.10 ip4:216.81.144.165 ip4:149.72.247.52 ip4:149.72.134.64 ip4:149.72.152.236 ip4:149.72.163.58
ip4:149.72.172.170 ip4:167.89.90.62 ip4:158.228.129.79 ip4:216.81.144.165 ip4:117.50.14.178 ip4:117" ".50.35.199 ip4:54.240.42.110
ip4:54.240.42.111 include:u13494342.wl093.sendgrid.net include:spf.protection.outlook.com include:mail.zendesk.com
include:_spfsn.teslamotors.com include:_spf.qualtrics.com include:_spf.ultipro.com include:_spf.psm.knowbe4.com" "
include:spf1.sendcloud.org include:spf2.sendcloud.org -all"
```

- **Google dorking**

The practice of using advanced search operators and specialized queries on the Google search engine to locate publicly accessible resources, configuration errors, or private data that are not typically indexed in standard search results is known as "Google Dorking," also known as "Google Hacking."




- **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)-[~]
└─$ sudo nmap -sS tesla.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-06 04:40 EDT
Nmap scan report for tesla.com (23.218.192.46)
Host is up (0.026s latency).
Other addresses for tesla.com (not scanned): 104.80.228.227 96.16.108.43 104.85.4.91 23.220.132.93
rDNS record for 23.218.192.46: a23-218-192-46.deploy.static.akamaitechnologies.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 19.52 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)-[~]
└─$ sudo nikto -h tesla.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 23.218.192.46, 104.80.228.227, 96.16.108.43, 104.85.4.91, 23.220.132.93
---------------------------------------------------------------------------
+ 0 host(s) tested

┌──(tharusha㉿kali)-[~]
└─$ sudo nikto -h tesla.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 23.220.132.93, 104.85.4.91, 96.16.108.43, 104.80.228.227, 23.218.192.46
---------------------------------------------------------------------------
+ 0 host(s) tested

┌──(tharusha㉿kali)-[~]
└─$ sudo nikto -h 23.218.192.46
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          23.218.192.46
+ Target Hostname:    23.218.192.46
+ Target Port:        80
+ Start Time:         2024-05-06 04:43:51 (GMT-4)
---------------------------------------------------------------------------
+ Server: AkamaiGHost
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/mis
sing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

# Exploitation

To SQLi vulnerabilities in the target web application, I used the SQLMAP tool for the exploitations.

```
┌──(tharusha㉿kali)-[~]
└─$ sqlmap -u 'https://www.tesla.com/' --data='param1=blah&param2=blah'
                                                                                
                __H__                                                           
     ___ ___[.]_____ ___ ___  {1.8.2#stable}                                    
    |_ -| . [.]     | .'| . |                                                   
    |___|_  [.]_|_|_|__,|  _|                                                   
          |_|V...       |_|   https://sqlmap.org

[!] 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 r
esponsible for any misuse or damage caused by this program

[*] starting @ 05:13:05 /2024-05-06/

[05:13:05] [INFO] testing connection to the target URL
[05:13:36] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
[05:13:36] [WARNING] if the problem persists please check that the provided target URL is reachable. In case that it is, you can try to rerun with switch '--random-agent' and/or proxy switches ('--proxy', '--proxy-file' ...)
[05:14:55] [CRITICAL] connection timed out to the target URL

[*] ending @ 05:14:55 /2024-05-06/
```

# Vulnerabilities detect when scanning

## 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.

- **Remedy**

The best course of action would be to add your domain to the HSTS preload list after correcting the faults and warnings. As a result, consumers will be actively prevented from accessing your website via HTTP and browsers will automatically connect to it via HTTPS. Because users' browsers have this list hardcoded, HSTS will be enabled before they even visit your page, removing the need for Trust On First Use (TOFU) and all of its drawbacks. Your website will not satisfy the requirements necessary to be included to the browser's preload list unless the problems and warnings are fixed.

Vendors of browsers stated:

- Serve a valid certificate
- Redirect all domains on the same host from HTTP to HTTPS if you are listening on port 80. Serve all subdomains over HTTPS:
    - In particular, you must support HTTPS for the www subdomain if a DNS record for that subdomain exists
- Provide an HTTPS request with a HSTS header on the base domain:
    - 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. 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.

- **Remedy**

- Configure your webserver to redirect HTTP requests to HTTPS.

i.e. for Apache, you should have modification in the httpd.conf. For more configurations, please refer to External References section.

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

## 3. Weak Ciphers Enabled

MEDIUM | 1 CONFIRMED | 1

Netsparker detected that weak ciphers are enabled during secure communication (SSL).

You should allow only strong ciphers on your web server to protect secure communication with your visitors.

**Impact**

Attackers might decrypt SSL traffic between your server and your visitors.

- **Remedy**

- Configure your web server to disallow using weak ciphers.

## 4. 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.

- **Remedy**

- Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.
  - X-Frame-Options: DENYIt completely denies to be loaded in frame/iframe.
  - X-Frame-Options: SAMEORIGINIt allows only if the site which wants to load has a same origin.
  - X-Frame-Options: ALLOW-FROM URLIt 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.