Sri Lanka Institute of Information Technology

IE2072 – WEB SECURITY

Year 2, Semester 2

(Assignment – Individual)-2023

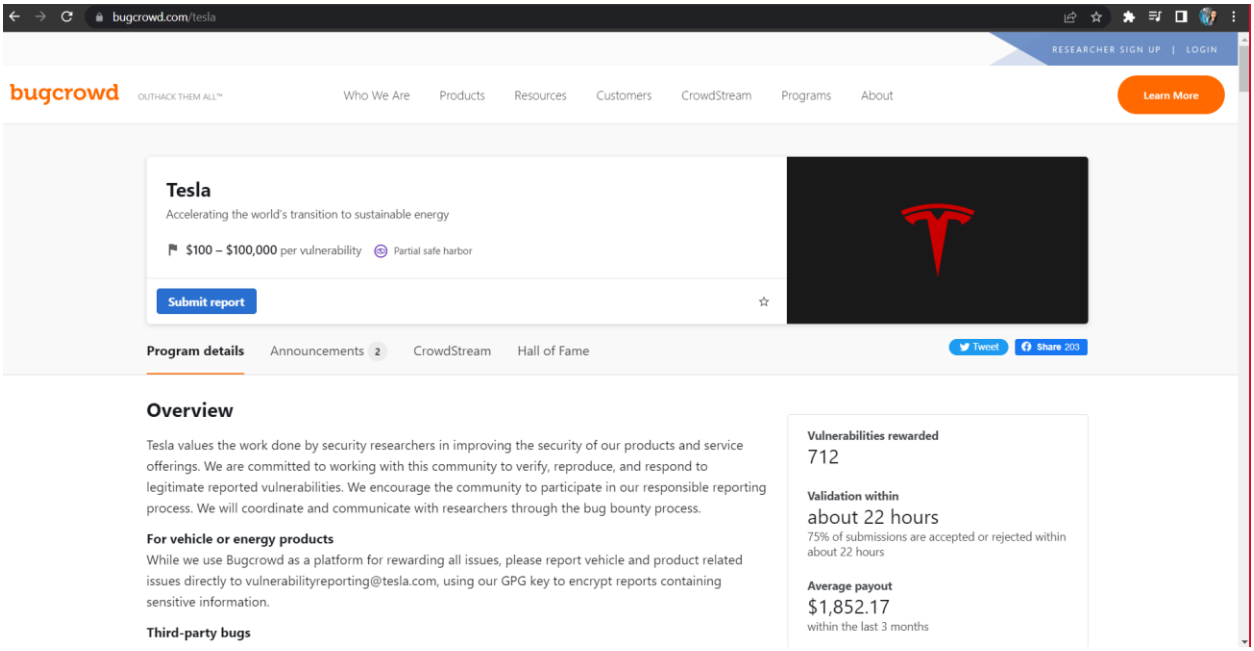
Bug Bounty vulnerabilities scanning Report 6

Student Register Number	Student Name
IT21167096	DE ZOYSA A.S.

Tesla Company

- **Overview**

Tesla appreciates the efforts made by security researchers to enhance the safety of our line of goods and services. We pledge to collaborate with this community in order to confirm, replicate, and address any legitimately identified vulnerabilities. We want everyone in the neighborhood to take part in our responsible reporting system. Through the bug bounty procedure, we will coordinate with researchers and keep them informed.



- ## Assessment Scope

Scope of the security audit according to https://bugcrowd.com/tesla is as follows,

Corporate Sites

- ✓ *.tesla.com
- ✓ *.tesla.cn
- ✓ *.teslamotors.com
- ✓ *.tesla.services
- ✓ *.teslainsuranceservices.com
- ✓ *.solarcity.com
- ✓ Any host verified to be owned by Tesla Motors Inc. (domains/IP space/etc.)

Scope and rewards

Non-vehicle vulnerabilities — ✓ In scope

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

*.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	

Out Of Scope

- ✓ Any domains from acquisitions, such as maxwell.com
- ✓ employeefeedback.tesla.com
- ✓ energysupport.tesla.com (you can report vulnerabilities to bugbounty.zoho.com)
- ✓ engage.tesla.com
- ✓ feedback.tesla.com
- ✓ feedback.teslamotors.com
- ✓ ir.teslamotors.com
- ✓ ir.tesla.com
- ✓ mkto.teslamotors.com
- ✓ shop.eu.teslamotors.com
- ✓ Any other third-party websites hosted by non-Tesla entities

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
shop.eu.teslamotors.com	Website Testing
Any other third-party websites hosted by non-Tesla entities	Website Testing

- <u>Information gathering</u>

You are a detective who wants to collect information on the client's assets during the information gathering phase, which is also known as reconnaissance. To build successful strikes, you'll need to gather as much information as possible about your target. The assault surface is widened in this way. This is the phase in which a professional security tester spends the most time. Always keep in mind that the goal of a professional security assessment is to find any and all security flaws: it is not a capture the flag event in which you must get root using any means you choose and then look for flags.

It is the process of collecting data from many sources for a range of purposes. Learning to create efficient information-gathering techniques will benefit studying in a variety of ways. Effective information collecting involves making better use of time, fostering critical thinking through the use of shifting/sorting strategies, and enlarging one's perspective and topic knowledge through the investigation of new sources. Additionally, obtaining knowledge may be useful for a number of purposes, but the major advantage in terms of academic studies is that one will become aware of more varied sources, viewpoints, and techniques that can improve one's academic work.

Target Area

- Web apps for Tesla's audiences
- For information on how to submit vulnerabilities in other Tesla Vehicles applications or concerns with their products through email in order to be eligible for a prize, read above.

- ## Subdomains for Hunting

Sub-domain enumeration is the process of listing sub-domains for one or more domains. In the process of reconnaissance, it's a crucial phase. Sub-domain enumeration can reveal several domains and sub-domains that are included in a security assessment, which increases the chance of finding vulnerabilities.

Finding applications using cryptic, abandoned sub-domains may reveal serious bugs.

Within a single company, the same vulnerabilities are routinely discovered across many domains and applications.

What is Knockpy?

With only a few lines of code, knockpy's python version of the knockoffs framework makes it simple to use knockoff-based inference. The modular design of Knockpy makes it simple for researchers and analysts to add features on top of it.

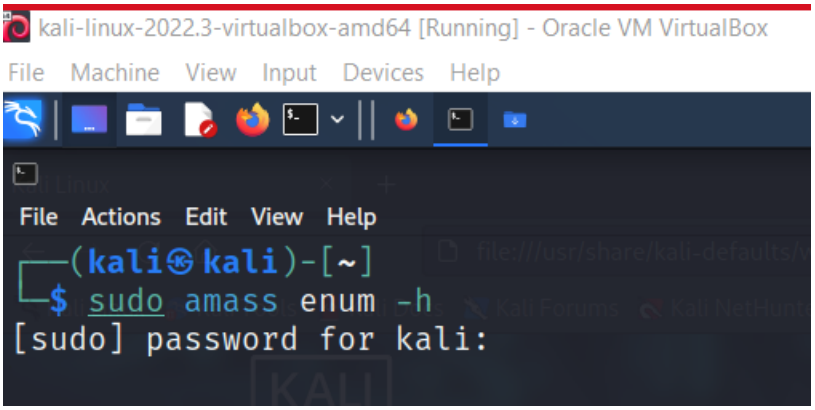
- searching subdomain by knockpy,

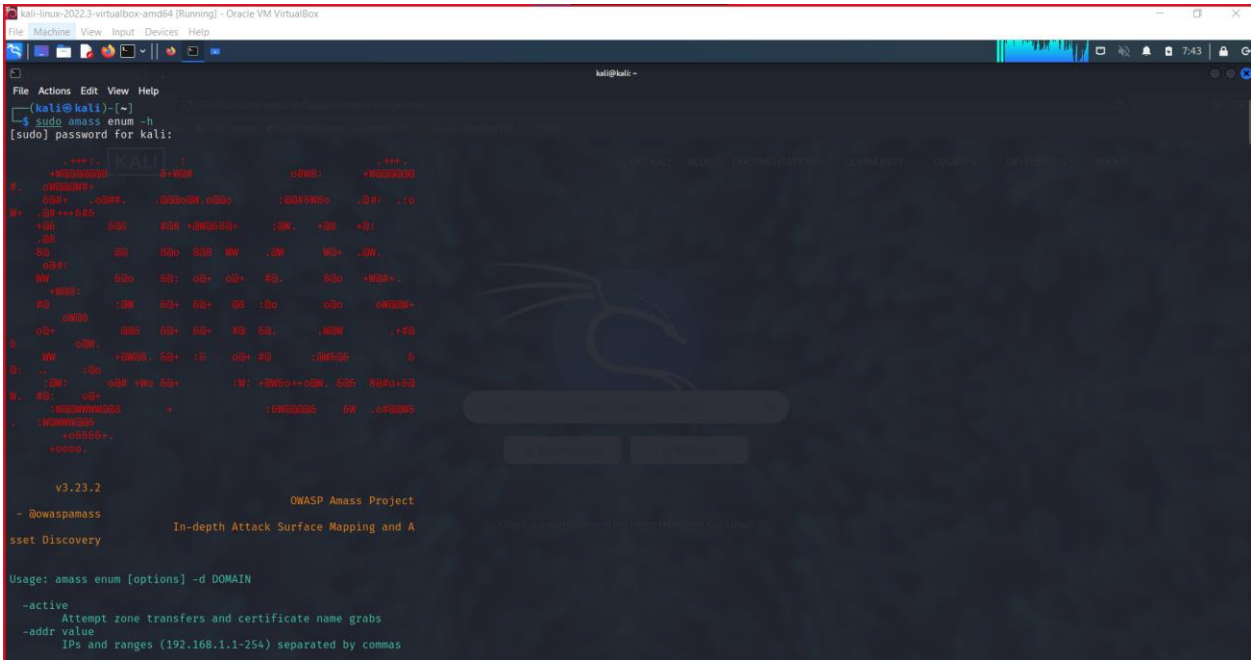
Knockpy is a portable and flexible Python3 utility that uses passive reconnaissance and dictionary scanning to swiftly enumerate subdomains on a specified domain.
How to Find Subdomain in Knockpy: knockpy <Domain Name>

```
kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ knockpy tesla.com

 _ __                 | |   v6.1.0
| |/ /  _ __   __ _  | |__  _ __  _   _
| ' /  | '_ \ / _ \ | '_ \| '_ \| | | |
| . \  | | | | (_) | | (_| |  <  | |_| |
|_|\_\ |_| |_|\__/ \ |_|\_\ .__/ \__, |
                     | |    |_|    |___/
                     |_|    |___/

local: 10757 | remote: 311

Wordlist: 11068 | Target: tesla.com | Ip: 23.201.26.71

11:01:45

Ip address      Code Subdomain                                          Server                                  Real hostname
_______________ ____ _______________________________________________    _______________________________________ ____________________
23.199.240.51   200  3.tesla.com                                                                                e1792.dscx.aka
maiedge.net
23.199.240.51   503  akamai-apigateway-fta.tesla.com                    AkamaiGHost                             e1792.dscx.aka
maiedge.net
23.199.240.51   503  akamai-apigateway-deliveryopsapi.tesla.com         AkamaiGHost                             e1792.dscx.aka
maiedge.net
23.199.240.51   503  akamai-apigateway-mfs-supplier-uat.tesla.com       AkamaiGHost                             e1792.dscx.aka
maiedge.net
23.199.240.51   503  akamai-apigateway-charging-ownership.tesla.com     AkamaiGHost                             e1792.dscx.aka
maiedge.net
23.199.240.51   503  akamai-apigateway-einvoicing.tesla.com             AkamaiGHost                             e1792.dscx.aka
maiedge.net
23.199.240.51   403  akamai-apigateway-vehicleextinfogw-prdsvc-st.tesla.com AkamaiGHost                         e1792.dscx.aka
maiedge.net
23.199.240.51   503  akamai-apigateway-stg-ops-warp3pl.tesla.com        AkamaiGHost                             e1792.dscx.aka
```

```
kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
kali@kali: ~
File  Actions  Edit  View  Help
maiedge.net
23.199.240.51   200  warp.tesla.com                                                                            e1792.dscx.aka
maiedge.net
199.66.9.83          warehouse-stg.tesla.com

13.111.49.179        view.emails.tesla.com

23.52.40.32          vehicle-files.eng.euw1.vn.cloud.tesla.com                                                 e92385.dscx.ak
amaiedge.net
23.52.40.19          vehicle-files.prd.usw2.vn.cloud.tesla.com                                                 e132349.dscx.a
kamaiedge.net
23.52.40.40          vehicle-files.prd.euw1.vn.cloud.tesla.com                                                 e73066.dscx.ak
amaiedge.net
23.199.240.51   200  workforce.tesla.com                                                                       e1792.dscx.aka
maiedge.net
23.199.240.51        www.tesla.com                                                                             e1792.dscx.aka
maiedge.net
52.36.185.222        wdm.kronos.tesla.com                                                                      kronos-wdm-nlb
-0558dc9e908f5182.elb.us-west-2.amazonaws.com
23.213.194.211       wire.tesla.com                                                                            a321.srip1.aka
srip.net.ad93a312.1.cn.akasripcn.net
199.66.9.47          www-uat.tesla.com


11:11:24

Ip address: 131 | Subdomain: 195 | elapsed time: 00:09:38
```

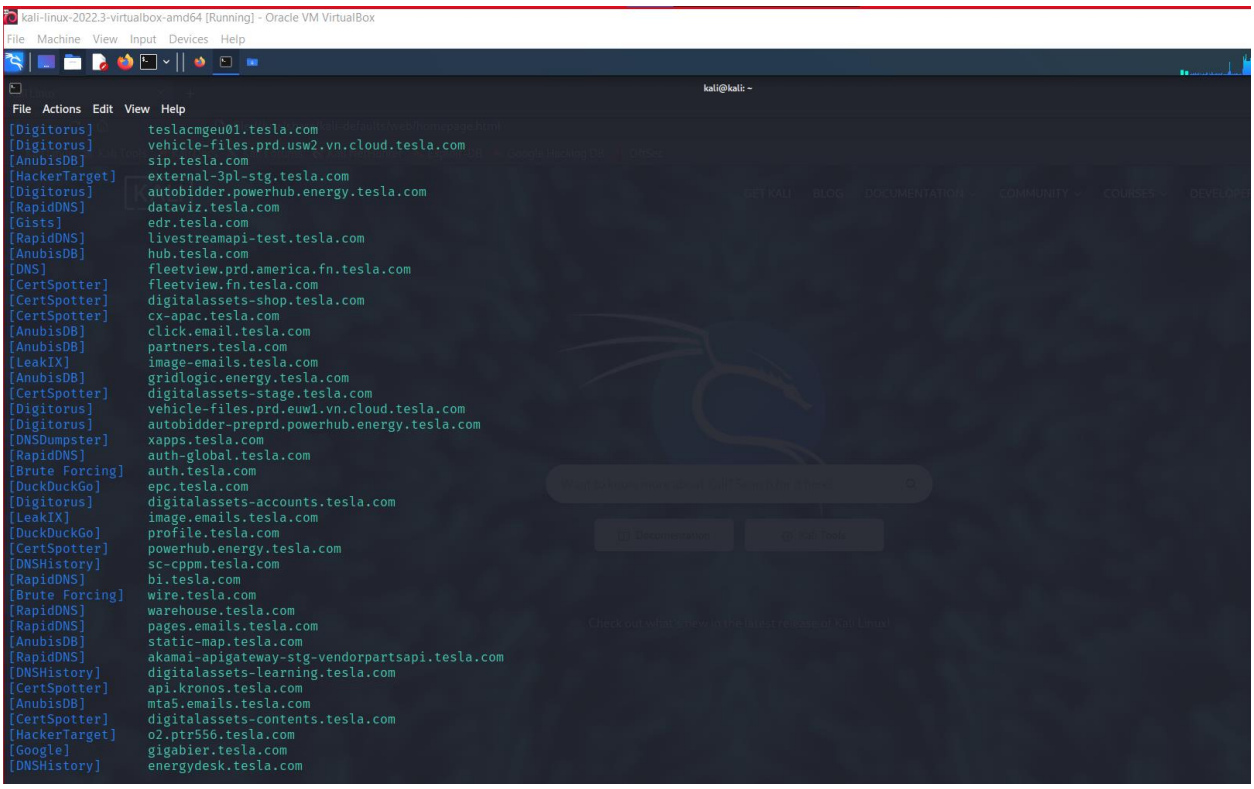
- searching subdomain by amass





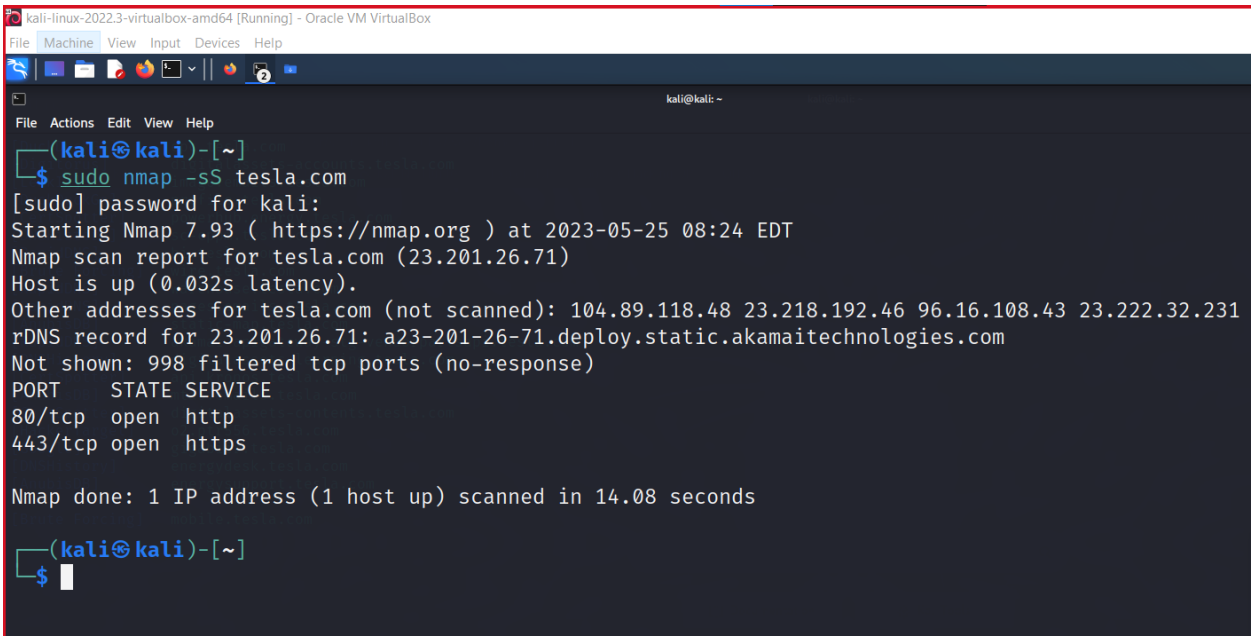
```
kali@kali: ~
File  Actions  Edit  View  Help
Usage: amass enum [options] -d DOMAIN

  -active
        Attempt zone transfers and certificate name grabs
  -addr value
        IPs and ranges (192.168.1.1-254) separated by commas
  -alts
        Enable generation of altered names
  -asn value
        ASNs separated by commas (can be used multiple times)
  -aw value
        Path to a different wordlist file for alterations
  -awm value
        "hashcat-style" wordlist masks for name alterations
  -bl value
        Blacklist of subdomain names that will not be investig
ated
  -blf string
        Path to a file providing blacklisted subdomains
  -brute
        Execute brute forcing after searches
  -cidr value
        CIDRs separated by commas (can be used multiple times)
  -config string
        Path to the INI configuration file. Additional details
 below
  -d value
        Domain names separated by commas (can be used multiple
 times)
  -demo
        Censor output to make it suitable for demonstrations
  -df value
        Path to a file providing root domain names
  -dir string
        Path to the directory containing the output files
  -dns-qps int
        Maximum number of DNS queries per second across all re
solvers
  -ef string
        Path to a file providing data sources to exclude
  -exclude value
        Data source names separated by commas to be excluded
```

```
kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo amass enum -src -brute -d tesla.com
[AnubisDB]        xmail.tesla.com
[AnubisDB]        mta4.emails.tesla.com
[AnubisDB]        mta2.email.tesla.com
[AnubisDB]        mta.email.tesla.com
[AnubisDB]        mta3.emails.tesla.com
[CertSpotter]     vpn2.tesla.com
[Digitorus]       view.emails.tesla.com
[HackerTarget]    external-3pl-prd.tesla.com
[HackerTarget]    apacvpn2.tesla.com
[HackerTarget]    o6.ptr9437.tesla.com
[HackerTarget]    apacvpn1.tesla.com
[HackerTarget]    o7.ptr6980.tesla.com
[CertSpotter]     apacvpn.tesla.com
[DNS]             tesla.com
[AnubisDB]        model3.tesla.com
[HackerTarget]    teamchatgl.tesla.com
[DNSDumpster]     origin-apps.tesla.com
[RapidDNS]        www-uat-qa.tesla.com
[RapidDNS]        origin-static-assets-pay.tesla.com
[AnubisDB]        mta.emails.tesla.com
[Digitorus]       engage.tesla.com
[HackerTarget]    mrsproxy06.tesla.com
[AnubisDB]        comparison.tesla.com
[RapidDNS]        stage-uat-dev.tesla.com
[Maltiverse]      turn6.usw2.vn.cloud.tesla.com
[AnubisDB]        view.email.tesla.com
[RapidDNS]        origin-finplat-prd.tesla.com
[AnubisDB]        www-static-prod.tesla.com
[HackerTarget]    origin-mobile.tesla.com
[Brute Forcing]   feedback.tesla.com
[AnubisDB]        pages.email.tesla.com
[HackerTarget]    paymentrecon-stage.tesla.com
[AnubisDB]        www-static-dev.tesla.com
[AnubisDB]        origin-aurora-ordering-ext.tesla.com
[CertSpotter]     vpn1.tesla.com
[RapidDNS]        stage-uat-qa.tesla.com
[DNSDumpster]     secureguest.tesla.com
[Digitorus]       cnvpn.tesla.com
[Maltiverse]      turn6.use1.vn.cloud.tesla.com
```



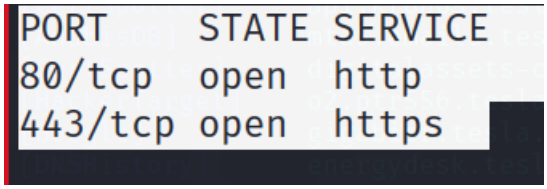
```
kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
kali@kali: ~
File  Actions  Edit  View  Help
[Digitorus]      teslacmgeu01.tesla.com
[Digitorus]      vehicle-files.prd.usw2.vn.cloud.tesla.com
[AnubisDB]       sip.tesla.com
[HackerTarget]   external-3pl-stg.tesla.com
[Digitorus]      autobidder.powerhub.energy.tesla.com
[RapidDNS]       dataviz.tesla.com
[Gists]          edr.tesla.com
[RapidDNS]       livestreamapi-test.tesla.com
[AnubisDB]       hub.tesla.com
[DNS]            fleetview.prd.america.fn.tesla.com
[CertSpotter]    fleetview.fn.tesla.com
[CertSpotter]    digitalassets-shop.tesla.com
[CertSpotter]    cx-apac.tesla.com
[AnubisDB]       click.email.tesla.com
[AnubisDB]       partners.tesla.com
[LeakIX]         image-emails.tesla.com
[AnubisDB]       gridlogic.energy.tesla.com
[CertSpotter]    digitalassets-stage.tesla.com
[Digitorus]      vehicle-files.prd.euw1.vn.cloud.tesla.com
[Digitorus]      autobidder-preprd.powerhub.energy.tesla.com
[DNSDumpster]    xapps.tesla.com
[RapidDNS]       auth-global.tesla.com
[Brute Forcing]  auth.tesla.com
[DuckDuckGo]     epc.tesla.com
[Digitorus]      digitalassets-accounts.tesla.com
[LeakIX]         image.emails.tesla.com
[DuckDuckGo]     profile.tesla.com
[CertSpotter]    powerhub.energy.tesla.com
[DNSHistory]     sc-cppm.tesla.com
[RapidDNS]       bi.tesla.com
[Brute Forcing]  wire.tesla.com
[RapidDNS]       warehouse.tesla.com
[RapidDNS]       pages.emails.tesla.com
[AnubisDB]       static-map.tesla.com
[RapidDNS]       akamai-apigateway-stg-vendorpartsapi.tesla.com
[DNSHistory]     digitalassets-learning.tesla.com
[CertSpotter]    api.kronos.tesla.com
[AnubisDB]       mta5.emails.tesla.com
[CertSpotter]    digitalassets-contents.tesla.com
[HackerTarget]   o2.ptr556.tesla.com
[Google]         gigabier.tesla.com
[DNSHistory]     energydesk.tesla.com
```

- Open Ports Enumeration applying with nmap



open ports are,

PORT	STATE	SERVICE
80/tcp	open	http
443/tcp	open	https



A port that is open is one that is actively receiving TCP or UDP packets. A port is in use and cannot be used for anything else if a service uses it. Open ports offer a security risk if the services operating on them are improperly configured, unsecure, or unpatched.

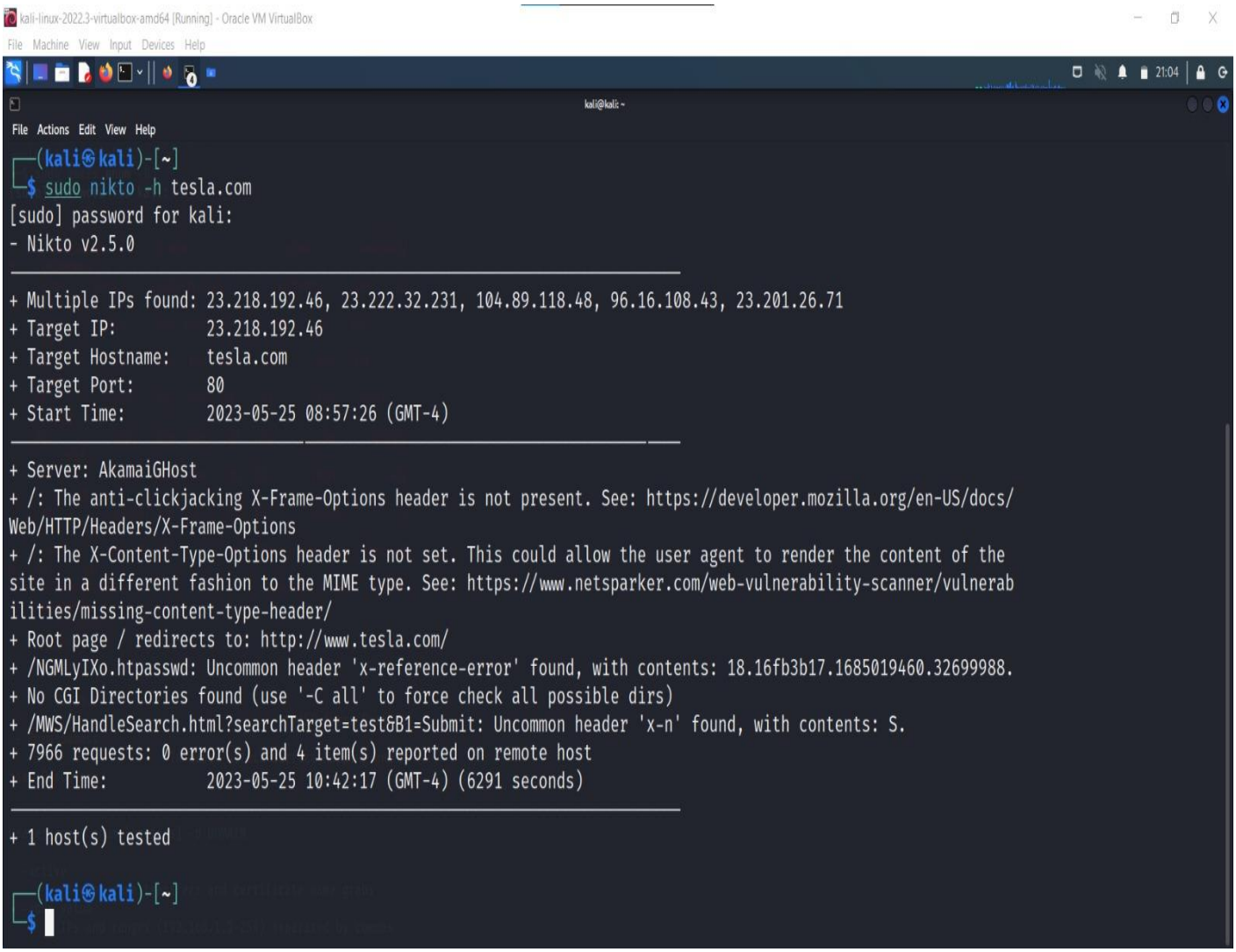
Using Nmap to List Open Ports

The most popular port security network scanner in the world is called Nmap. You may assess the efficacy of your firewall and security settings with the help of the Nmap hosted security tool.

Checking for Vulnerabilities using NIKTO

vulnerabilities are scanned by Nikto. But not any found vulnerability

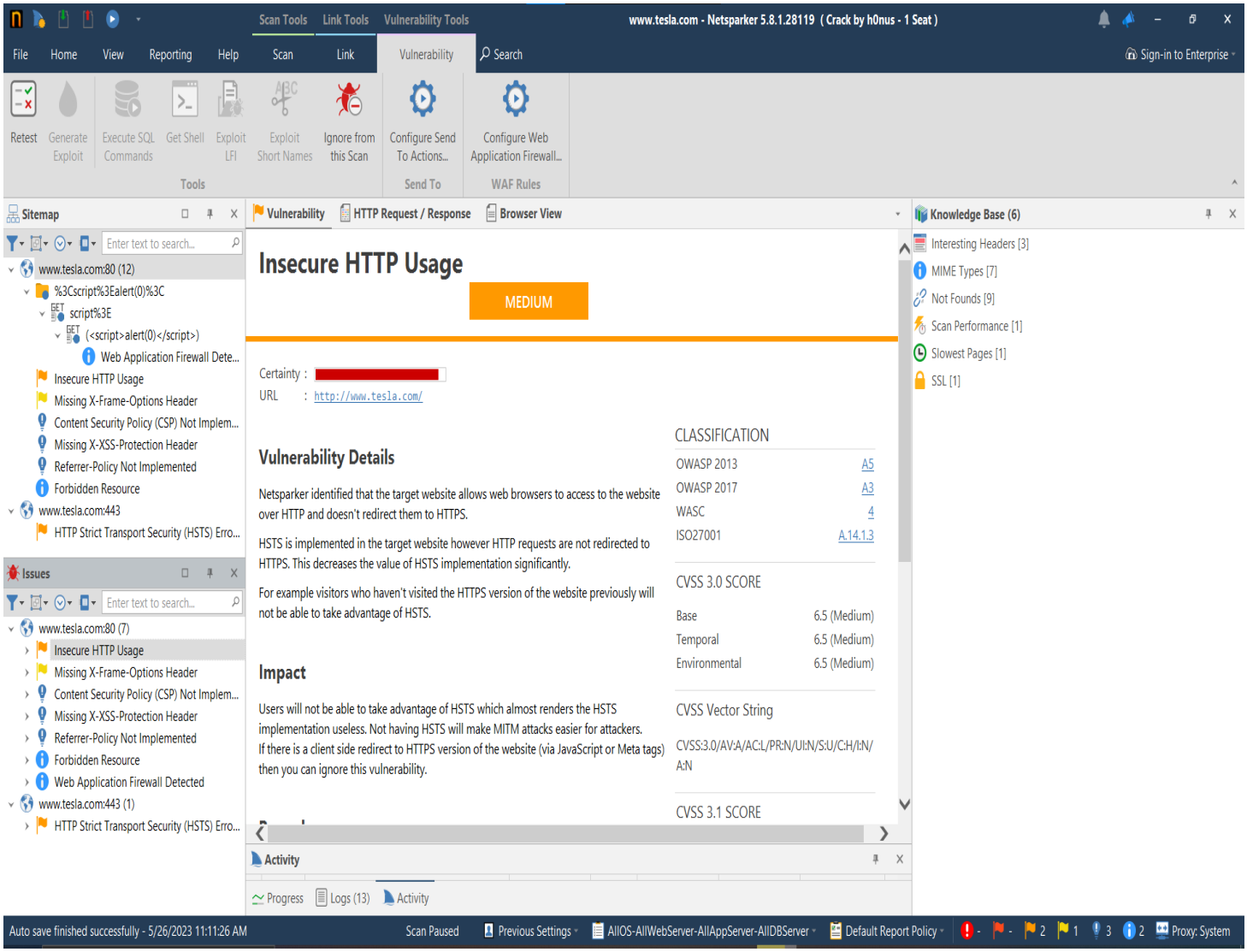
A security program called the Nikto web server scanner scans a website for thousands of possible security holes. This includes malicious files, services that have been set up improperly, vulnerable scripts, and other issues. It was created using plugins and is open source to allow for feature expansion. New security checks are frequently added to these plugins through regular updates. Many penetration testers and security analysts maintain the famous Nikto Web Vulnerability Scanner in their toolkit. It typically unearths valuable data about a web server or website that may be used for subsequent exploitation or vulnerability analysis.



```
┌──(kali㉿kali)-[~]
└─$ sudo nikto -h 23.201.26.71
[sudo] password for kali:
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          23.201.26.71
+ Target Hostname:    23.201.26.71
+ Target Port:        80
+ Start Time:         2023-05-25 09:23:04 (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-Fram
e-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 fas
hion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-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:
+ Scan terminated: 0 error(s) and 2 item(s) reported on remote host
+ End Time:           2023-05-25 11:25:47 (GMT-4) (7363 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
┌──(kali㉿kali)-[~]
└─$
```

Scanned Vulnerabilities Using Netsparker

1) Insecure HTTP usage



Risk type : Medium

- **Vulnerability Details**

  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.

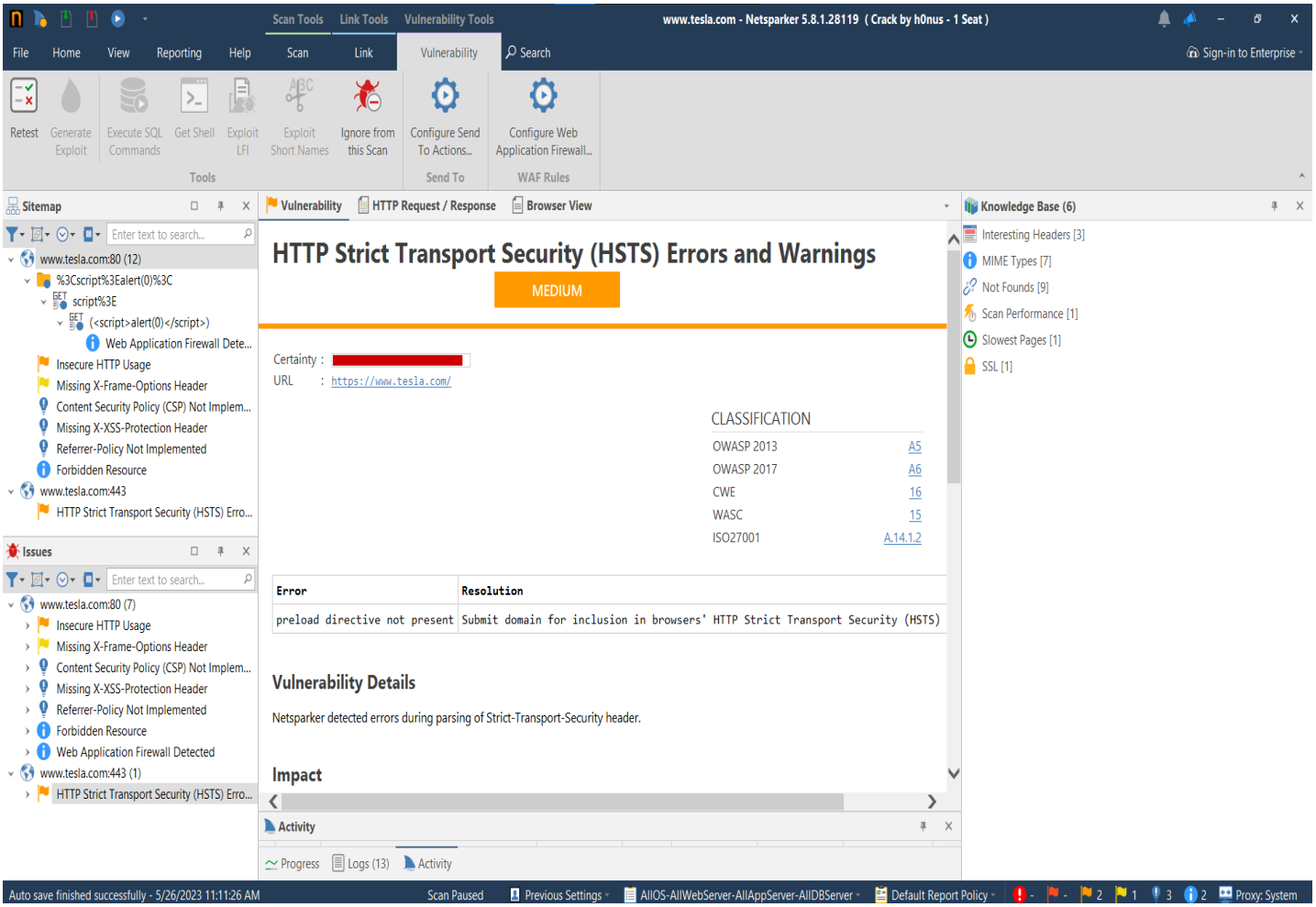
- **Remedy**

  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>
```

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



Risk type : Medium

Error : preload directive not present

Resolution : Submit domain for inclusion in browsers' HTTP Strict Transport Security (HSTS) preload list.

- **Vulnerability Details**

  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**

  Ideally, after fixing the errors and warnings, you should consider adding your domain to the the HSTS preload list. This will ensure that browsers automatically connect your website by using HTTPS, actively preventing users from visiting your site using HTTP. Since this list is hardcoded in users' browsers, it will enable HSTS even before they visit your page for the first time, eliminating the need for Trust On First Use (TOFU) with its associated risks and disadvantages. Unless you fix the errors and warnings your website won't meet the conditions required to enter the browser's preload list.

  Browser vendors declared:

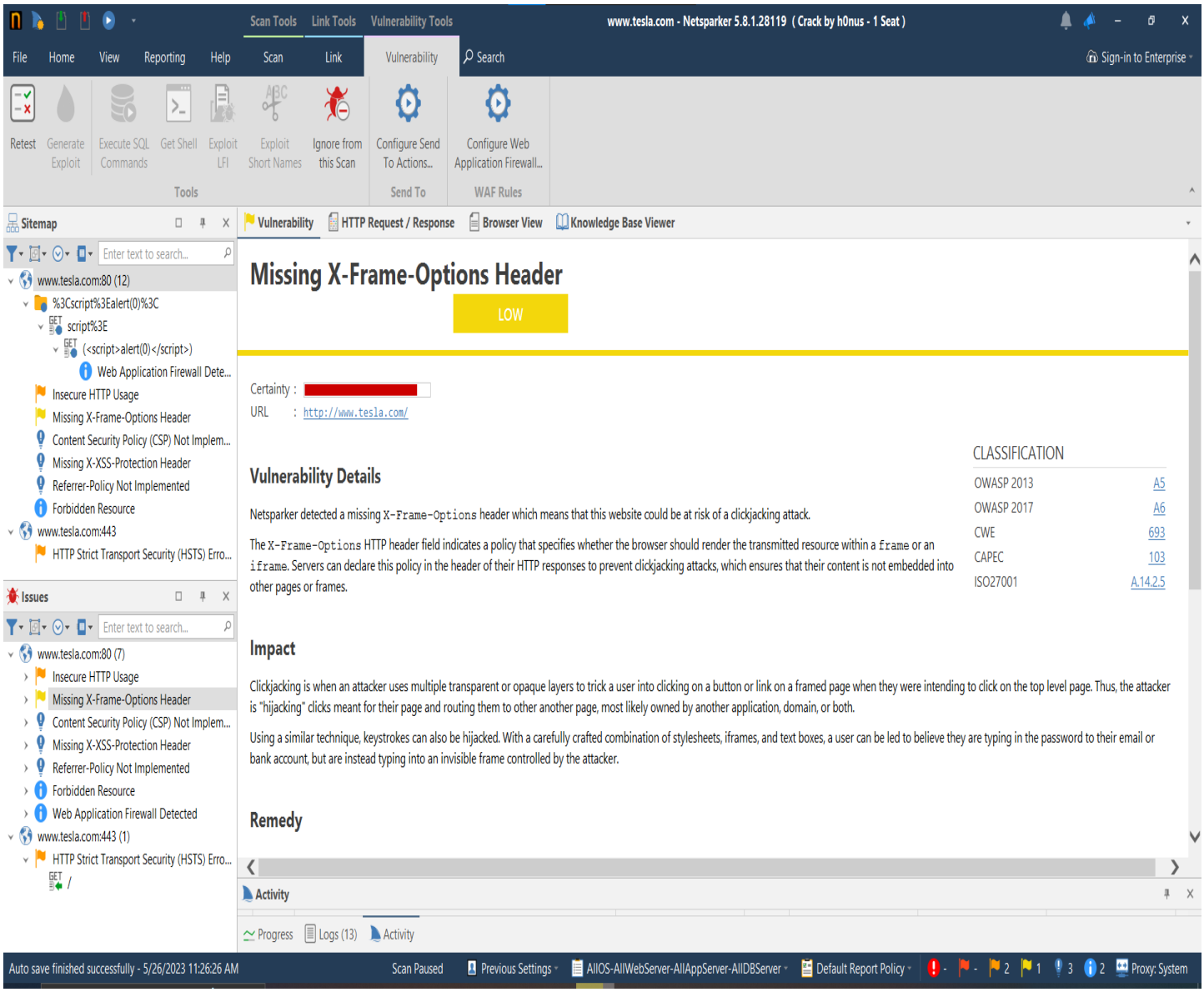
  - Serve a valid certificate

  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)

3) Missing X-Frame-Options Header



Risk type : Low

- **Vulnerability Details**

  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: 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.