Sri Lanka Institute of Information Technology

IE2062 – Web Security

Assignment – Bug bounty assignment
Domain – www.indeed.com

Submitted by

Student Registration Number	Student Name
IT20007874	Thalawattage T.A.H.S

Date of submission
October 15th 2021

Purpose

The overall purpose of this bug bounty is to scan and find security flaws in a well-known website, and students must apply their academic knowledge to a real-world security inspection. For this security web audit, we were suggested to utilize both automated and manual testing. Sublist3r, Nikto, Nmap, D-TECT, Nessus, and Amass, Nmap, Netsparker and Owas zap were used to check the vulnerabilities using the automated technique.

Abstract

Cybercrime, deception, and data breach are all risks that pose significant risks to businesses. A great deal has been lost, and organizations must devise ways to prevent the threats from becoming serious and to avert additional catastrophes. This investigation looked into the mechanisms involved with IT security web audits and how they might help companies enhance their IT security. The study assessed IT administrators' and employees' awareness of cybercrime risks, as well as their understanding of IT security audit norms and regulations and the impact of IT security audit on the organization's growth. This research used an organization as a setting, assessing the organization's flow IT security audit state and determining the adaptability for the establishment of an IT security audit strategy and system. To get more detailed information on cybercrime, a quantitative investigation was conducted. This study plainly demonstrated that an IT security audit is critical for the growth of every organization that uses technology.

Contents

1. Introduction - 4

2.Domain collection- -- - - - - - - - - - - 5

2. Automated testing - 8

i. Sublist3r- -- -8

ii. Nmap- 10

iii. Nikto -12

iv. Amass - 14

v. Netsparker - 17

vi. Nessus- -19

vii.OWASP ZAP - 23

viii. D-TECT - - - - - - - - - - -- - - - - - - - - - - - -- - - - - - -- 26

ix. Burp suite - - - -- -36

x. Skipfish -

4. Conclusion - 37

5. References - 37

Introduction

This Is a fantastic place to start for anyone with a website who wants to increase its search engine exposure. The website audit is a thorough examination of all aspects that impact a website's visibility in search engines. This fundamental method provides a comprehensive picture of any website, including all traffic and specific pages. The website audit is carried out only for marketing objectives. The goal is to identify flaws in web-based marketing strategies. A comprehensive website audit reveals inconsistencies that may result in Google penalties. On Google's ranking page, penalties have an effect on search engine ranking. The audit also assesses the site's vulnerability to security breaches.

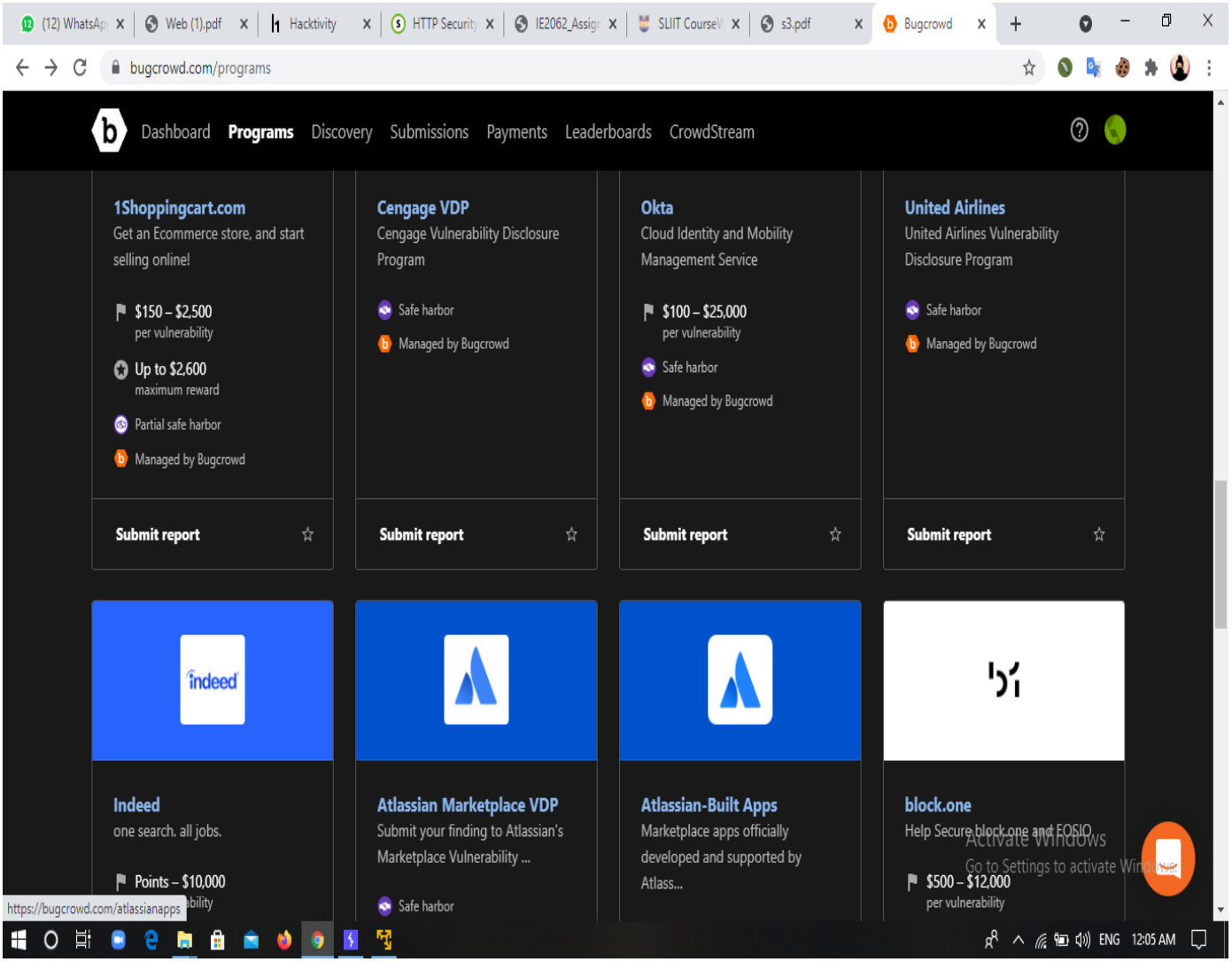
Cybercrime is a threat that every organization must deal with, and there is growing concern about the best way to combat it. Every day, cybercrime wreaks havoc on organizations' data systems, resulting in significant financial loss and reputational damage. Smugness has no place here. To protect an organization's IT from cybercrime, misrepresentation, and data breach, it is critical to have a strong data framework security. It is the responsibility of each organization to ensure that the organization's information is safe, confidential, and trustworthy. In any event, how can an organization determine what needs to be protected and by what means it should be protected? Where should the organization begin? This is where it all begins: web security auditing. Despite the fact that some writing claims that web security auditing is a critical step in securing an organization's data framework against Cybercrime, misrepresentation and data penetration should be done on a regular basis, as an orderly assessment by a free master on adherence, to find a shortcoming in the organization's IT. This examination report will explain how and why an efficient Web security audit is carried out, as well as whether or not the technique aids in enhancing IT security. To achieve this goal, I'll look at how certain Linux frameworks are currently audited on the chosen foreign site Indeed.com.

In any event, the cost of a cybercrime, deception, or data breach can be substantial. As a result, avoiding it pays off. The main goal of this investigation is to present the importance of online security auditing and to examine the benefits of IT security auditing as a useful tool for improving the data security of an organization. In addition, the investigation looks at the organization's approach to cybercrime risks, how well they use global security norms and rules, and how they conduct

periodic IT security audits. To evaluate and test a web security audit, a website called indeed is utilized.

Domain Collection.

- I used "https://www.bugcrowd.com/ " website to select domain for bug bounty.
- There are many websites and web applications in this bug bounty list as in the figure 01

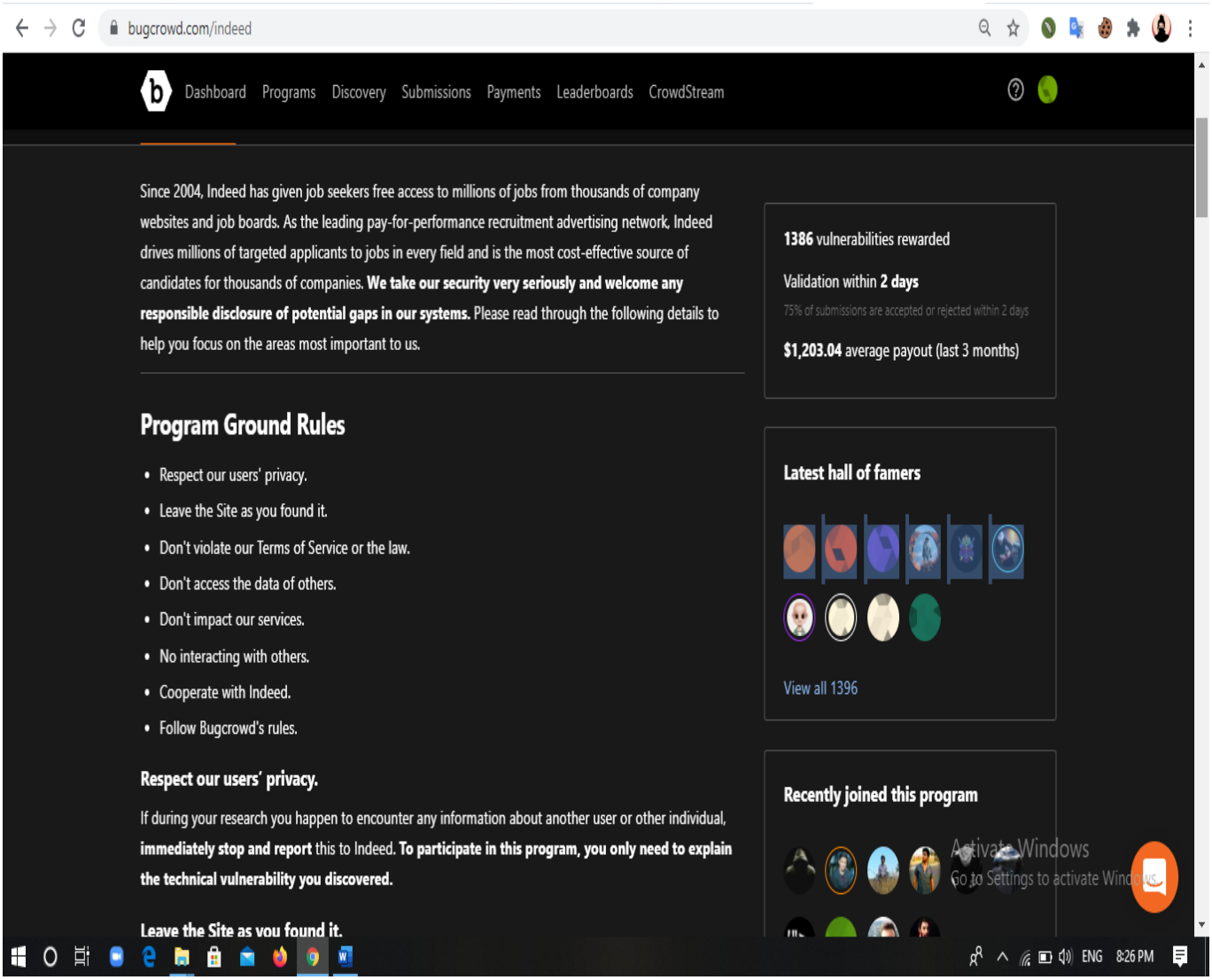


-Figure 01-

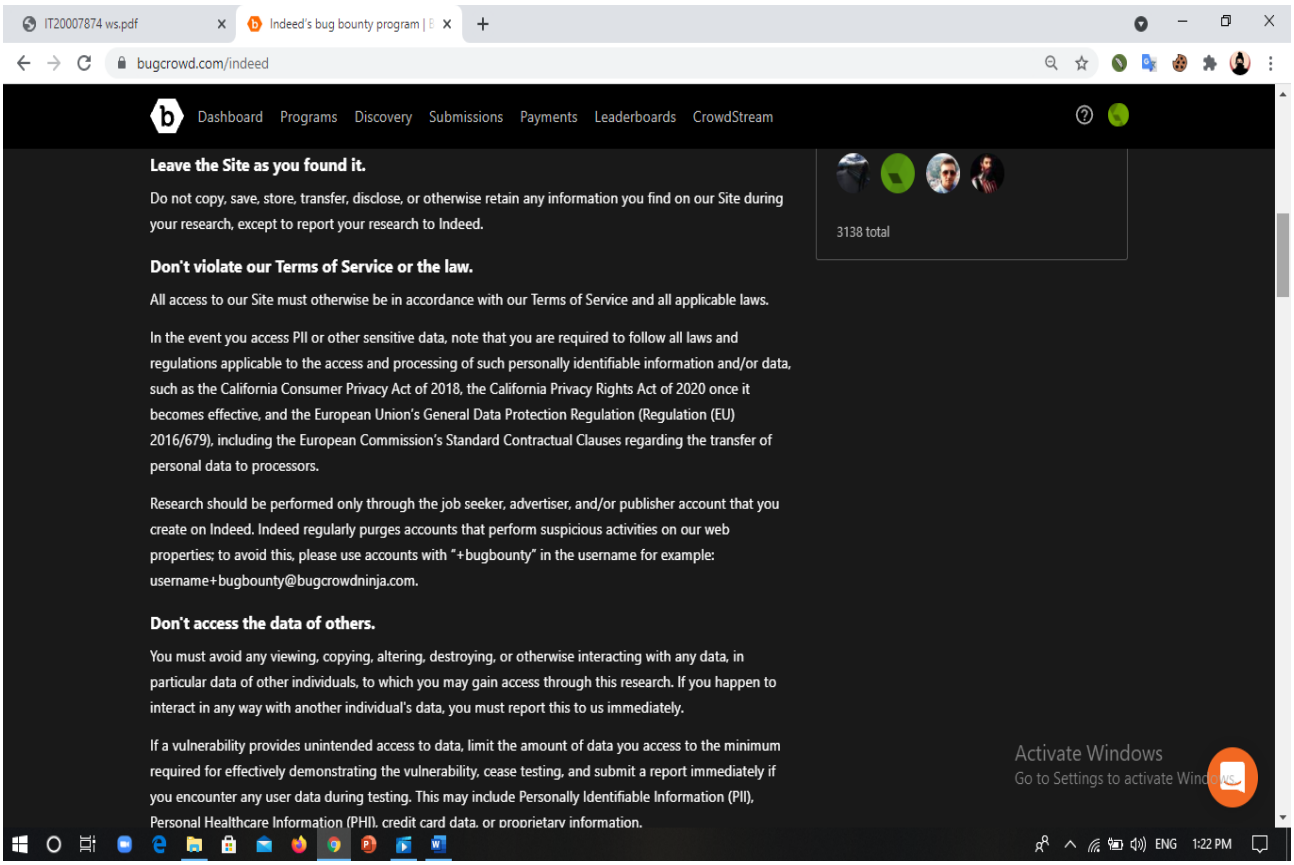
- I selected "**indeed.com**" from above list as my bug bounty domain.

indeed.com

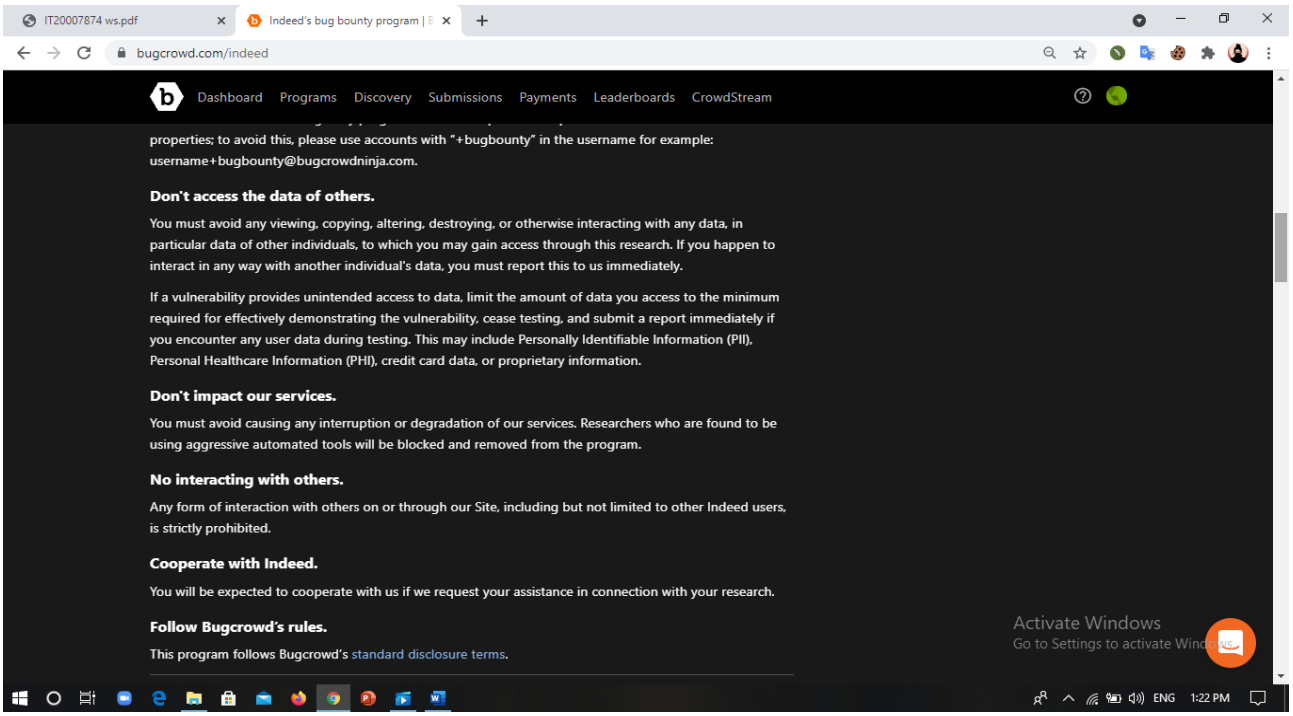
- Figure 02,03,04 shows do's and don'ts for the selected website.



-figure 02-

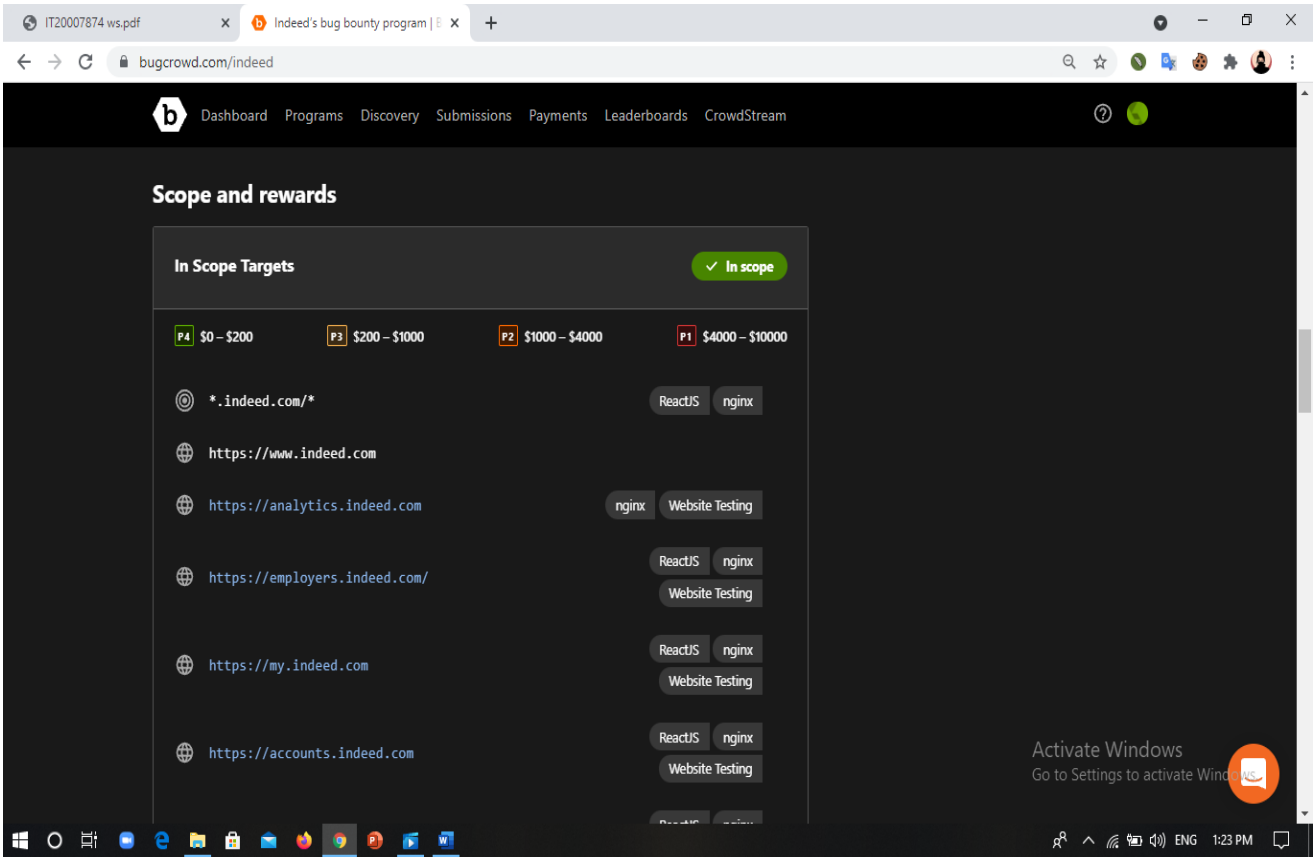


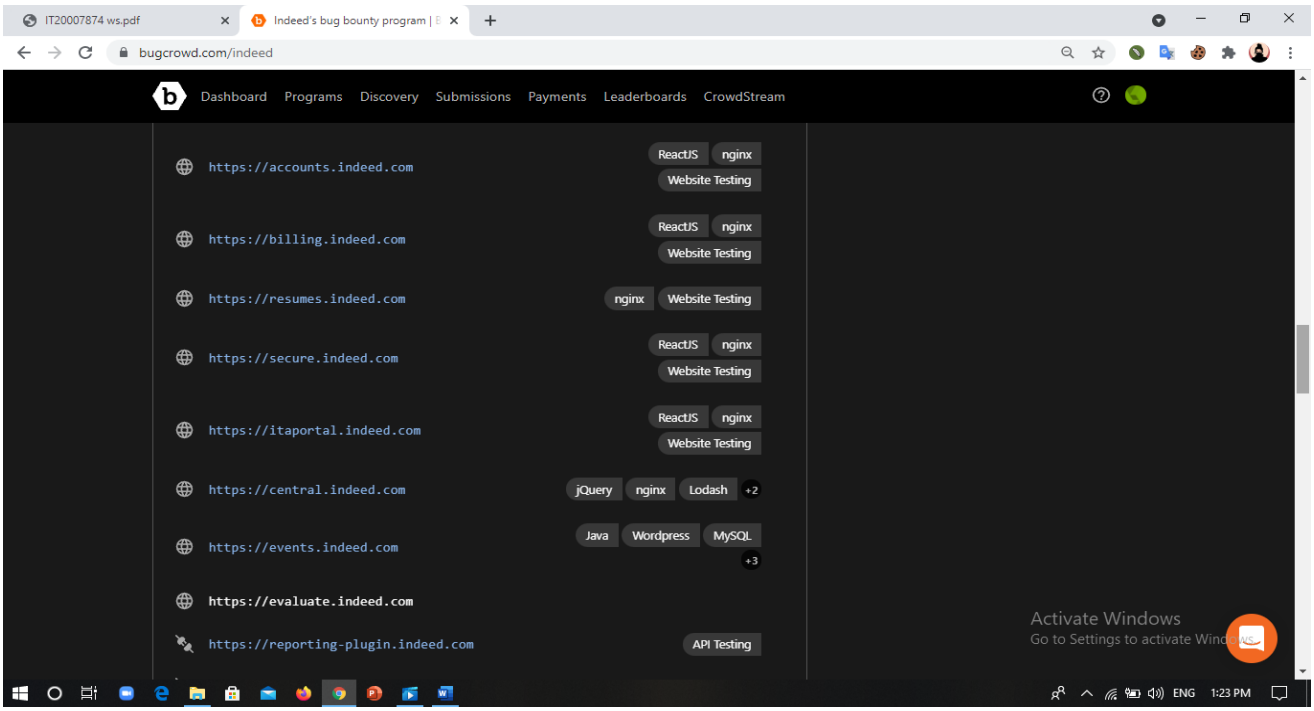
-figure 03-

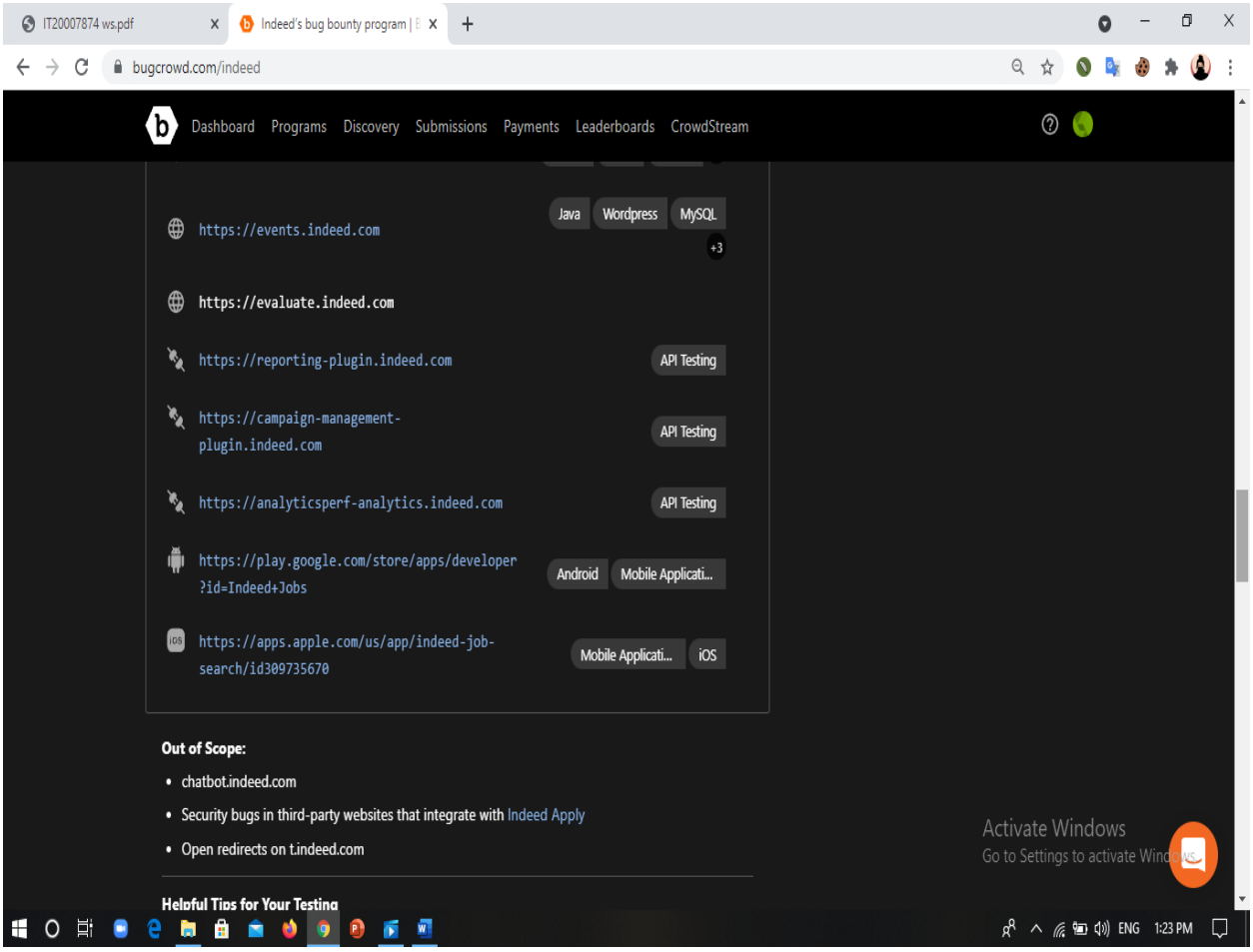


-figure 04-

These are my subdomain scope

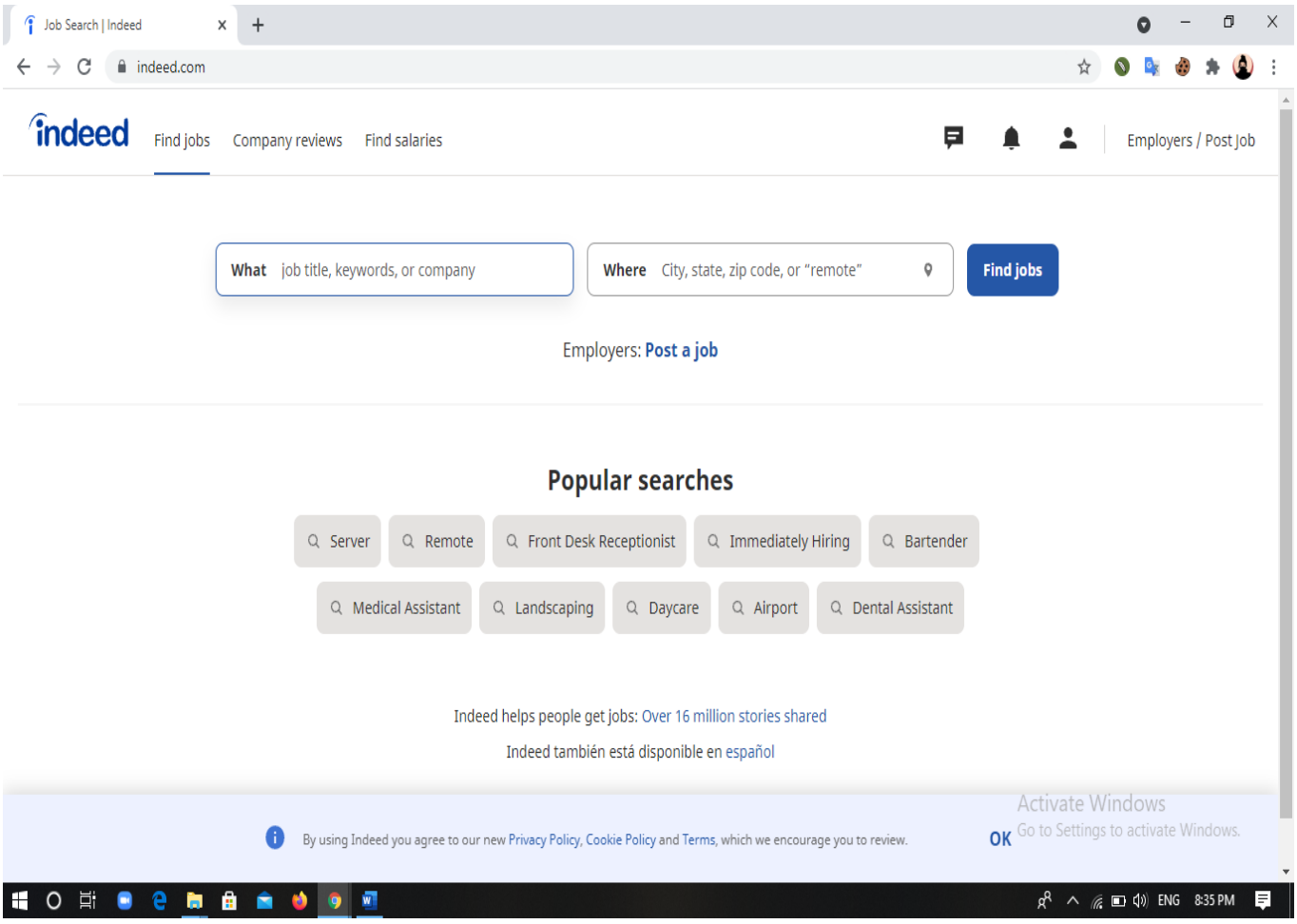





IT20007874 ws.pdf
Indeed's bug bounty program |
bugcrowd.com/indeed
Dashboard
Programs
Discovery
Submissions
Payments
Leaderboards
CrowdStream
https://events.indeed.com
Java
Wordpress
MySQL
+3
https://evaluate.indeed.com
https://reporting-plugin.indeed.com
API Testing
https://campaign-management-plugin.indeed.com
API Testing
https://analyticsperf-analytics.indeed.com
API Testing
https://play.google.com/store/apps/developer?id=Indeed+Jobs
Android
Mobile Applicati...
https://apps.apple.com/us/app/indeed-job-search/id309735670
Mobile Applicati...
iOS
Out of Scope:
chatbot.indeed.com
Security bugs in third-party websites that integrate with Indeed Apply
Open redirects on t.indeed.com
Helpful Tips for Your Testing
Activate Windows
Go to Settings to activate Windows.
ENG
1:23 PM

- Interface of my selected domain as shown in the figure 05.

Indeed is a job-search website based in the United States that was founded in November 2004. It is a subsidiary of Recruit Co. Ltd. of Japan, having offices in Austin, Texas and Stamford, Connecticut, as well as other locations throughout the world. It is also an example of vertical search because it is a single-topic search engine. Indeed is available in over 60 countries and 28 languages at the moment. Indeed.com surpassed Monster.com as the most popular employment website in the United States in October 2010.



-figure 05-

Automated Testing

Automated integration of your reconnaissance data, system and software fingerprinting, real-time exploit and malware searches, automated attacks and exploitation, and automated assaults and exploitation effectively minimize risk.

Vulnerability scanning tools and relative screenshots of the results

1.Sublist3r

Sublist3r is a Python-based application that uses OSINT to identify subdomains of websites. It aids penetration testers and bug hunters in gathering and collecting subdomains for the site they are targeting.
It enumerates subdomains using many search engines such as:

Google
Yahoo
Bing
Baidu
Ask

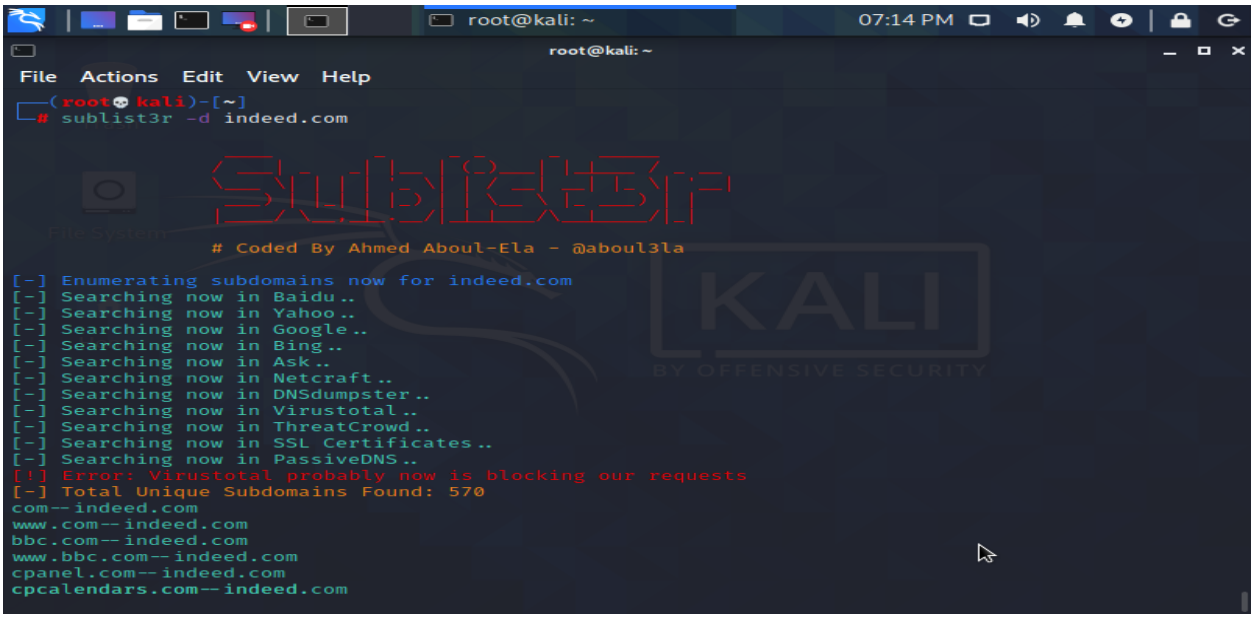
The tool also enumerates subdomains using:

Netcraft
Virustotal
ThreatCrowd
DNSdumpster
ReverseDNS

- Following the selection of the web domain, we must locate the domain's subdomains.
- I used **sublist3r** tool to find the subdomains
- By using following command, we can get the subdomains

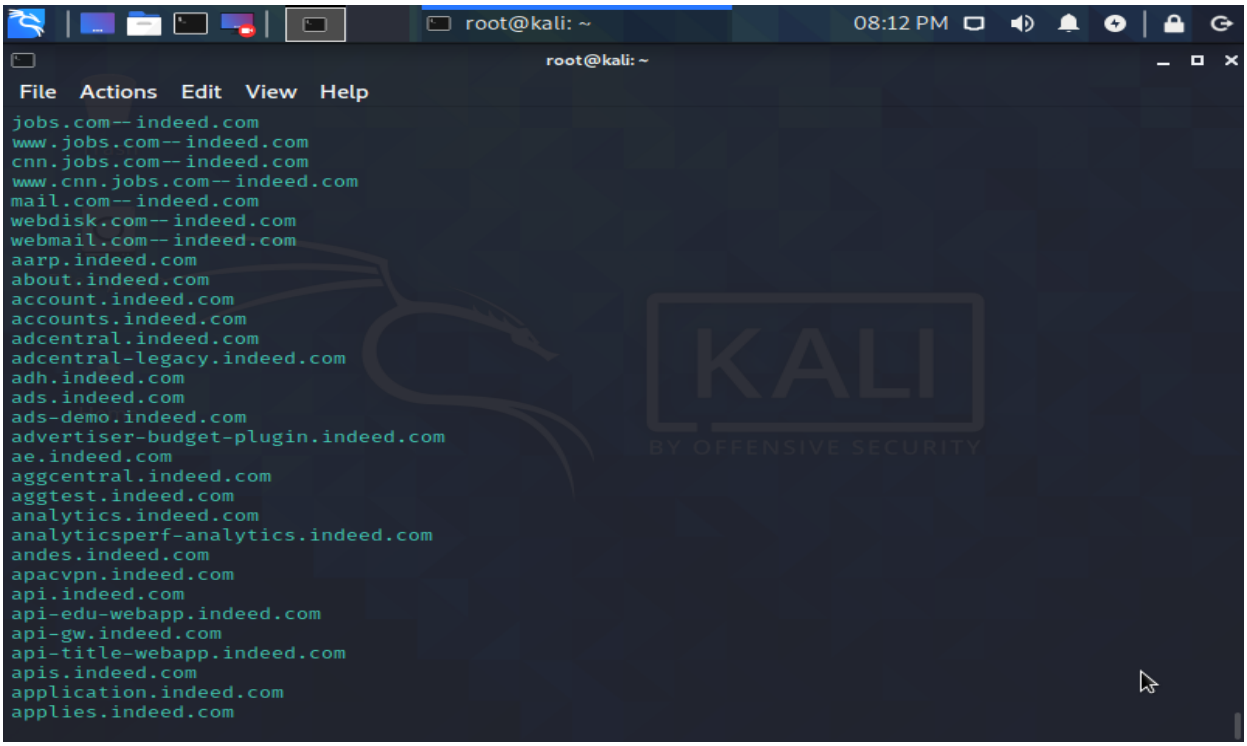
```
/sublist3r.py -d indeed.com
```

- After running above command, I got the result as shown in the figure 06.



- figure 06 –

The sublist3r python file to find the subdomains and the total number of them. In this case it is **570 sub domains**.



-figure 07-

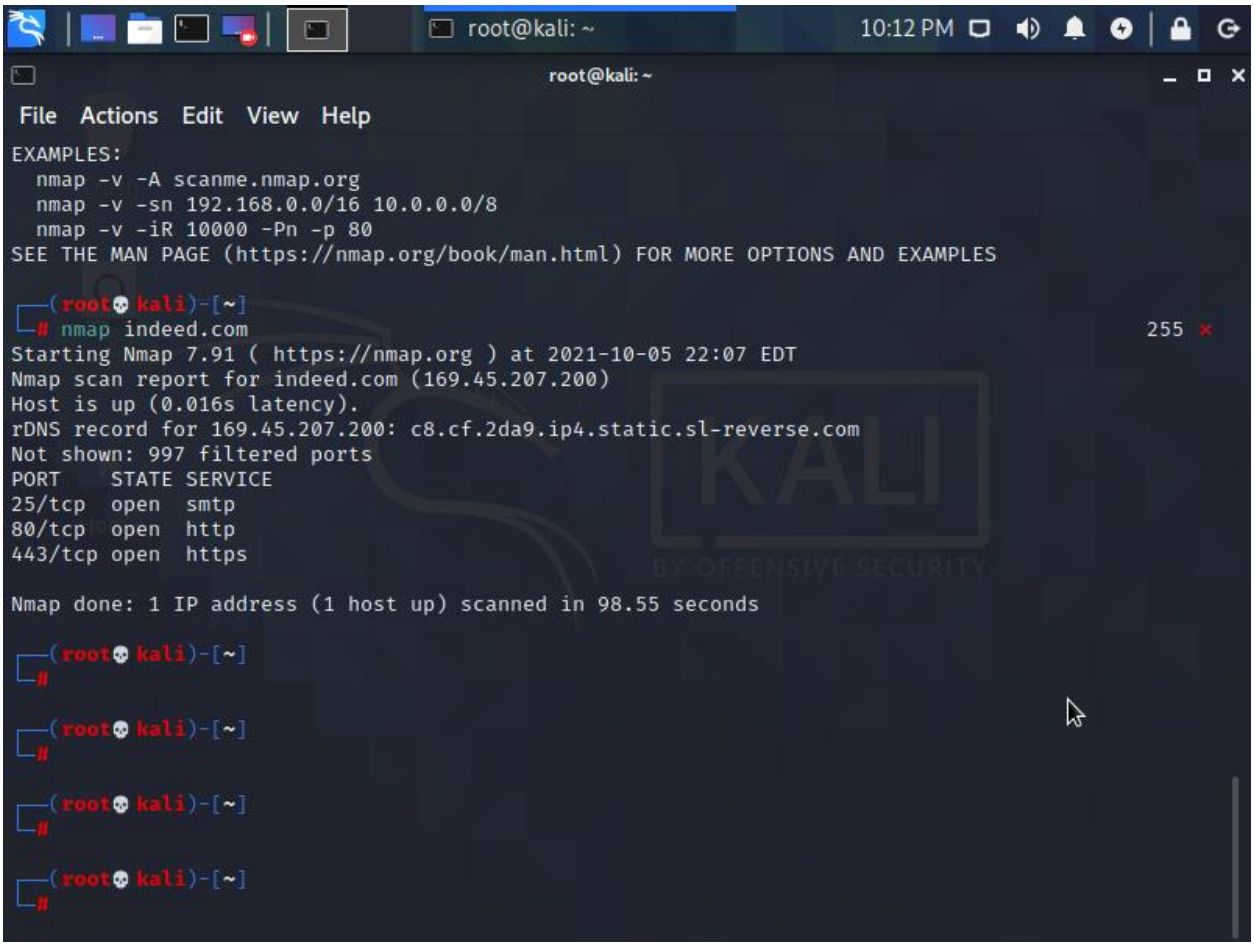
2. Nmap

Nmap is a network scanning and security auditing tool. It includes ping scanning (finding out which hosts are online), a variety of port scanning techniques, version detection (finding out which service protocols and application versions are listening on ports), and TCP/IP fingerprinting (remote host OS or device identification). Nmap also has decoy/stealth scanning, sunRPC scanning, and more. In both GUI and commandline mode, most Unix and Windows systems are supported. The Sharp Zaurus and the iPAQ are two of the most popular handheld devices that are supported. Nmap will generally operate on any platform on which source code or binaries are available. To run Nmap, no documented hardware or software specs are necessary. Newer, faster hardware, on the other hand, almost always results in improved performance. On the other hand, keep in mind that the majority of what happens when you run Nmap happens on the network.

It was designed to swiftly check large organizations, but it also works well with single hosts. The Nmap suite includes a serious GUI and results watcher (Zenmap), an adaptable information move, redirection, and investigating apparatus (Ncat), a utility for looking at check results (Ndiff), and a bundle age and reaction examination device, in addition to the exemplary order line Nmap executable (Nping).

I run **Nmap** tool by using below command

Nmap www.indeed.com -v



-figure 08-

• After running above command, I got the result as shown in the figure 08

• Then I found ip address of my domain and three open ports.

3.Nikto

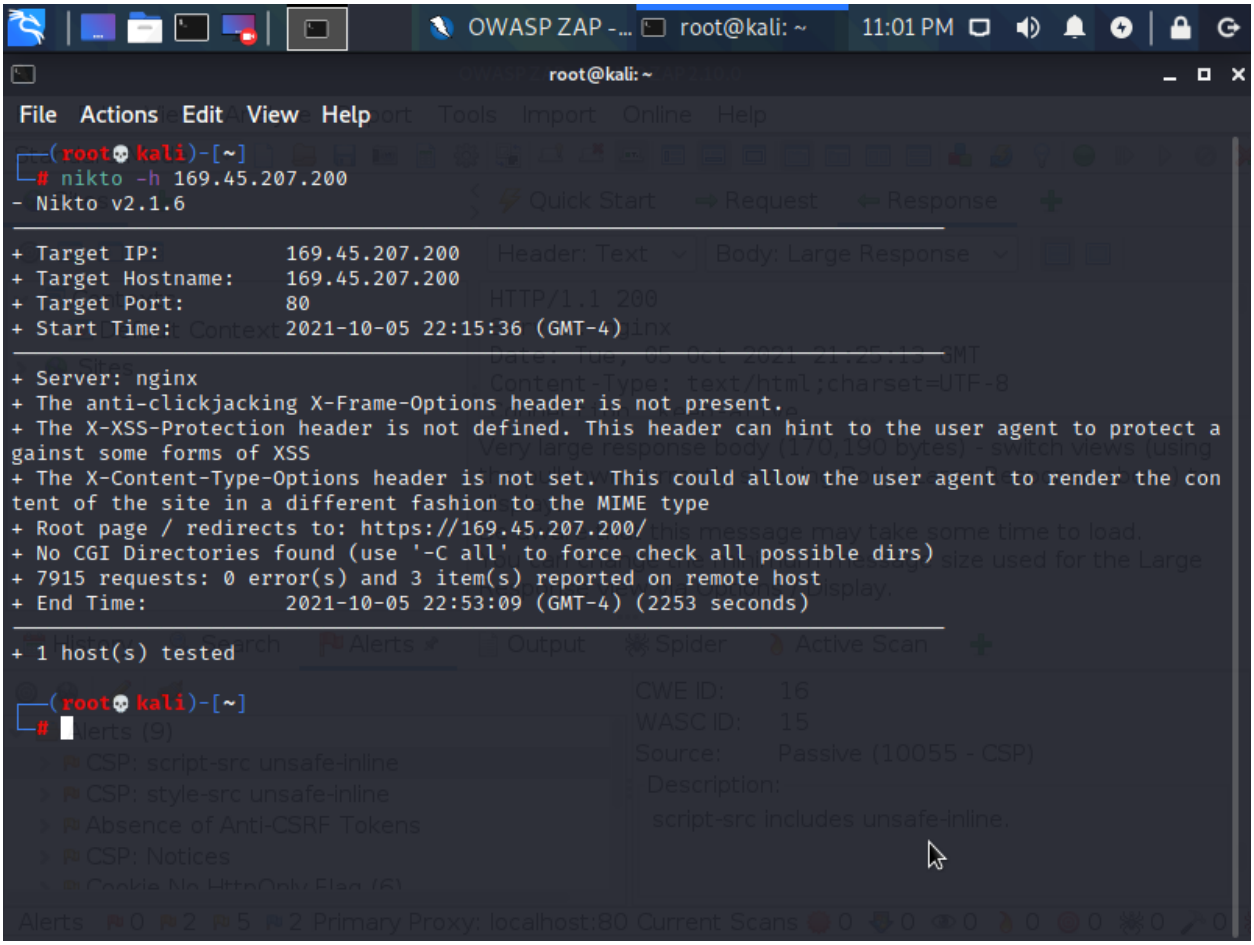
Nikto is a Perl-based open-source vulnerability scanner that focuses on web servers. It was first released in late 2001. It scans web servers for 6400 potentially harmful files and scripts, 1200 out-of-date server versions, and over 300 version-specific issues. It's even possible to have Nikto run immediately from Nessus when a web server is discovered. We'll run Nikto from the command line in a BackTrack terminal. If you're utilizing virtual hosts to host numerous websites on your web server. To obtain better vulnerability coverage, you should test each virtual host using Nikto. In fact, scanning the server's IP address as well as the hostname can assist guarantee that all routes are checked for susceptible web applications and scripts.

Benefits :--

- Inspect a website for known web application and script vulnerabilities.
- Check for web server configuration issues that might harm security.
- Headers, favicons, and files can be used to identify installed software on web servers.
- Examine how effective an intrusion detection system is (IDS)
- Access to 27 vulnerability scanners and OSINT tools is included with membership.
- Open Source Tools You Can Trust.

Using below command, we can run Nikto scanner by using our target domain's ip address.

```
nikto -h 169.45.207.200
```



- figure 09 -

- After running above command, I got the result as shown in the figure 09.

- This scanner could find,

  The anti-clickjacking x-frame option is not present.
  x-xss protection header is not defined.
  x-content-type-option header is not set.

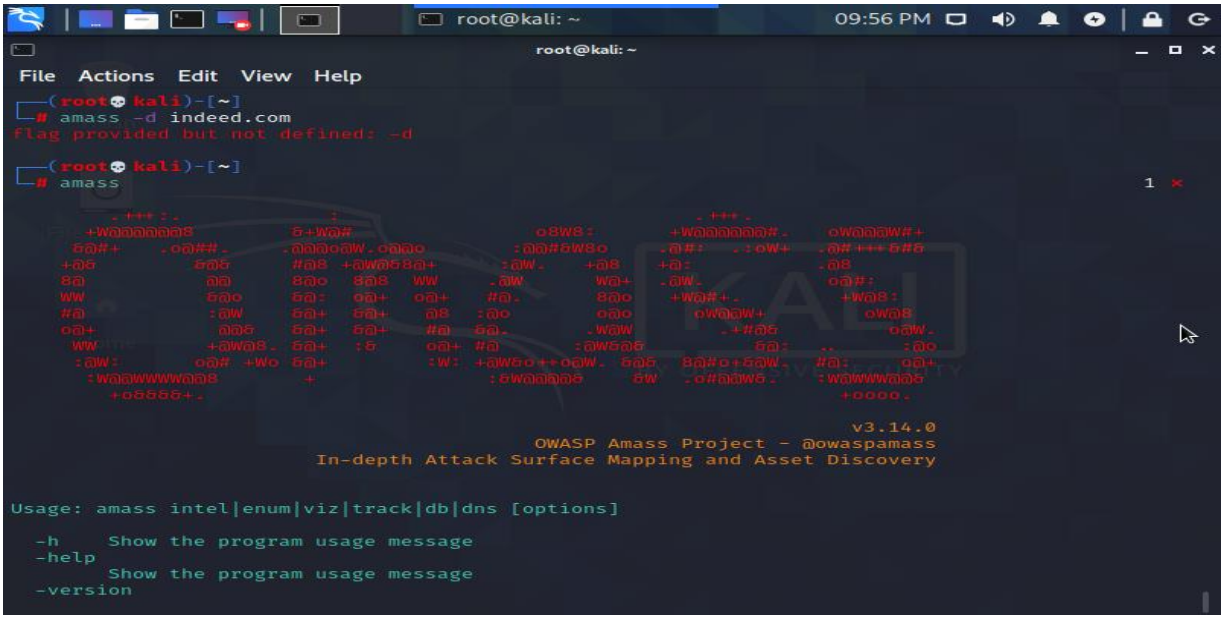
4.Amass

Amass comes with a plethora of functions. It's a strange tool since, despite its name, it's not used for bug bounty hunting. For a few minutes, Amass hums away, skulking around the internet's slums, begging for subdomains from anyone who will listen, and then sending them back to you, the hacker. You get your loot and leave, satisfied with your slew of subdomains and a sense of accomplishment.

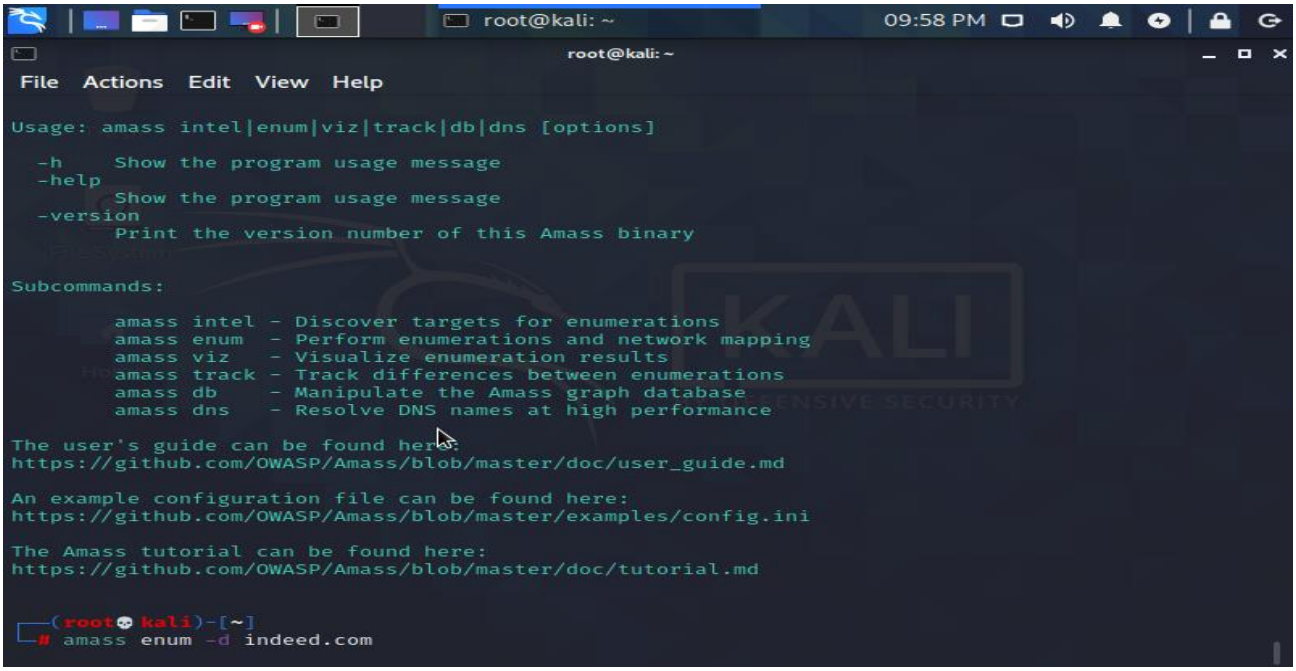
However, there is an issue. Because, like most people, you just used one Amass feature, you have the same same subdomains as everyone else! You're aware of how competitive bounty hunts can be, right? You don't want to put yourself at a disadvantage by not knowing how to use one of the most powerful recon tools available, do you? Having said that, amass offers a lot of features, most of which you won't use.

- First download the amass tool using following link.

https://github.com/OWASP/Amass



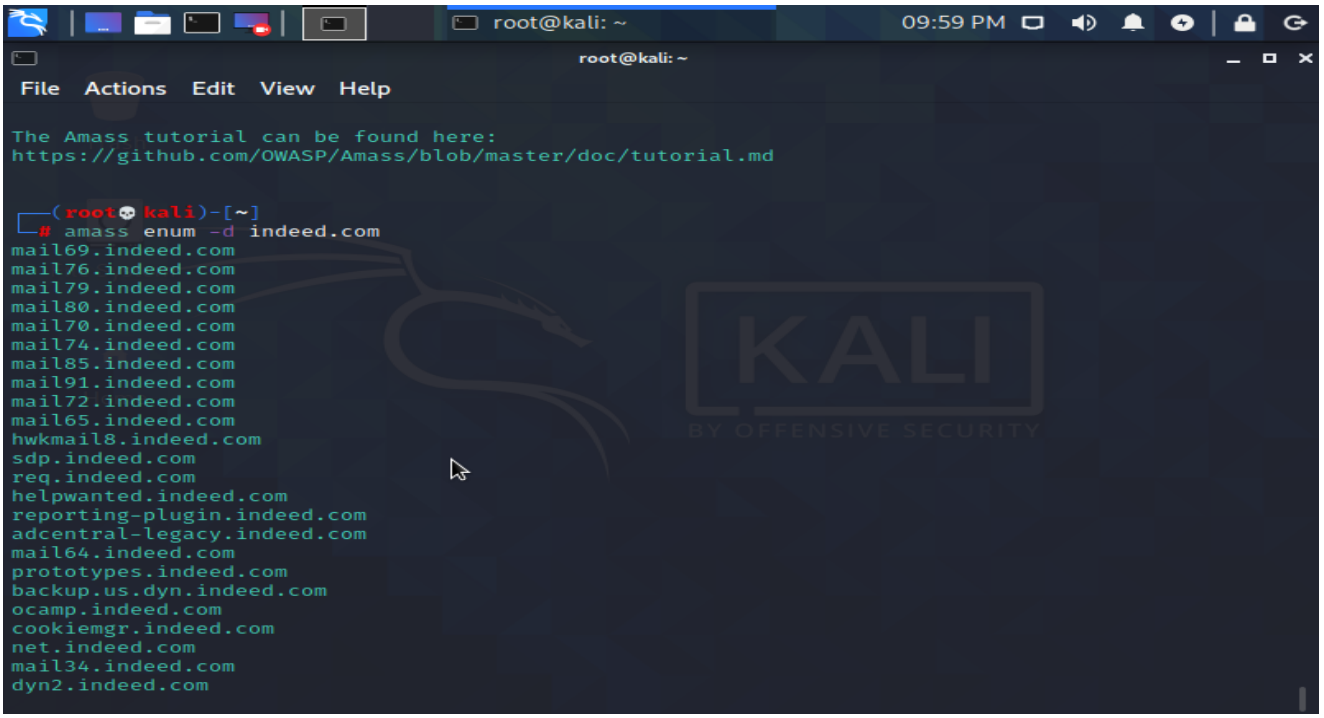
-figure 10-

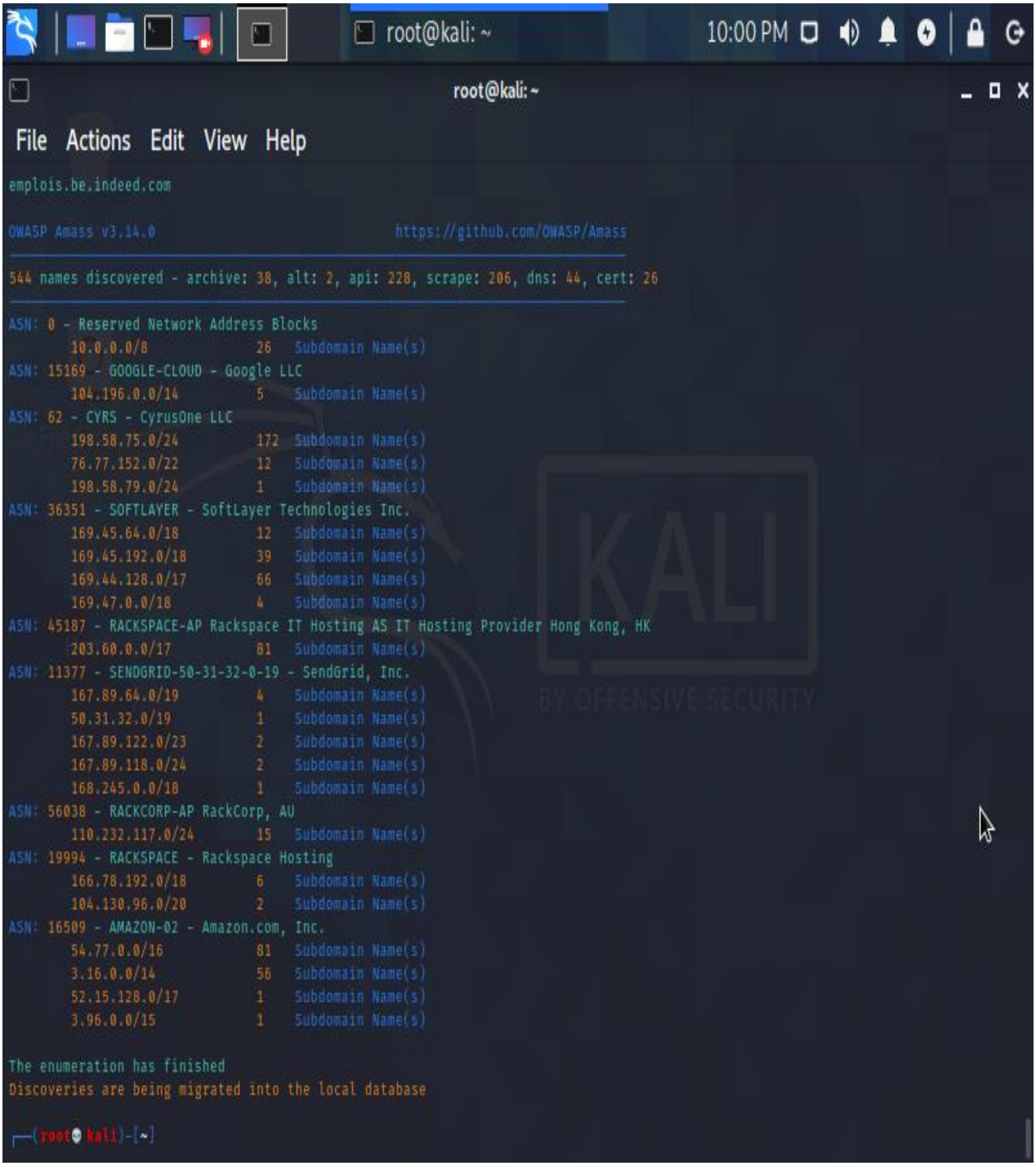


-figure11-

- After that I run the amass tool using below command.

Amass enum -d indeed.com





-figure12-

- After running above command, I got the result as shown in the figure 10, 11 and 12 It provide all ip addresses available subdomains.

5.Netsparker

Netsparker is an automated online application security scanner that allows you to scan websites, web applications, and web services for security vulnerabilities while being fully customisable. Netsparker can scan any online application, independent of the platform or programming language used to create it.

- Netsparker is the only online web application security scanner that exploits reported vulnerabilities in a read-only and secure manner to validate problems.

- It also provides evidence of the vulnerability, so you don't have to waste time manually confirming it. For example, if a SQL injection vulnerability is discovered, the database name will be displayed as proof of exploit.

This scanning technique is intended to assist you in quickly and simply securing web applications so that you can concentrate on resolving the vulnerabilities that have been detected. If Netsparker is unable to automatically confirm a vulnerability, it will notify you by prefixing it with '[Possible]' and giving a Certainty value, letting you know what has to be corrected right away.

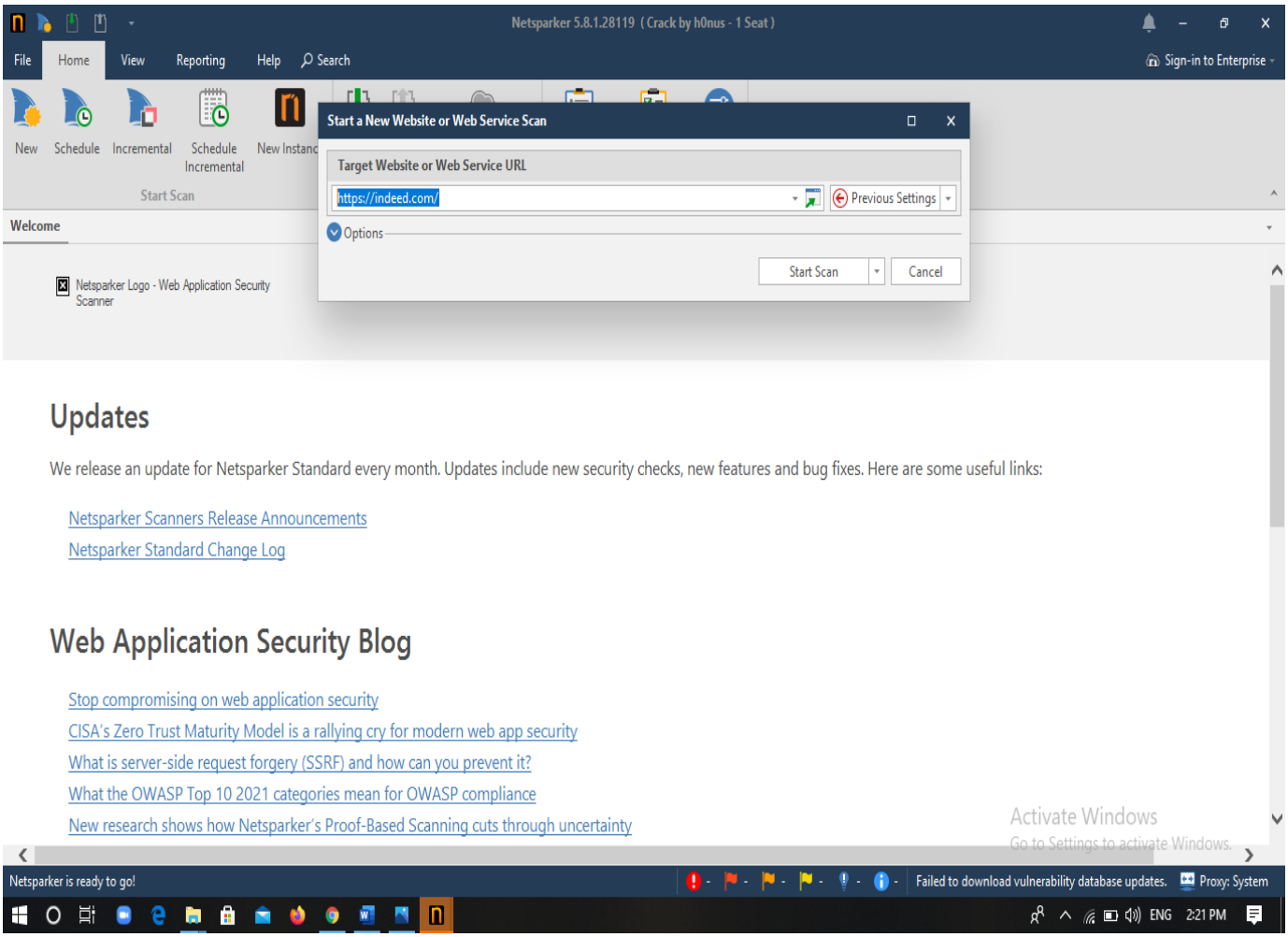
When Netsparker scanners find the following vulnerability categories, they can create a proof:

- SQL Injection
- Boolean SQL Injection
- Blind SQL Injection
- Remote File Inclusion (RFI)
- Command Injection
- Blind Command Injection
- XML External Entity (XXE) Injection
- Remote Code Evaluation
- Local File Inclusion (LFI)

- Server-side Template Injection
- Remote Code Execution
- Injection via Local File Inclusion

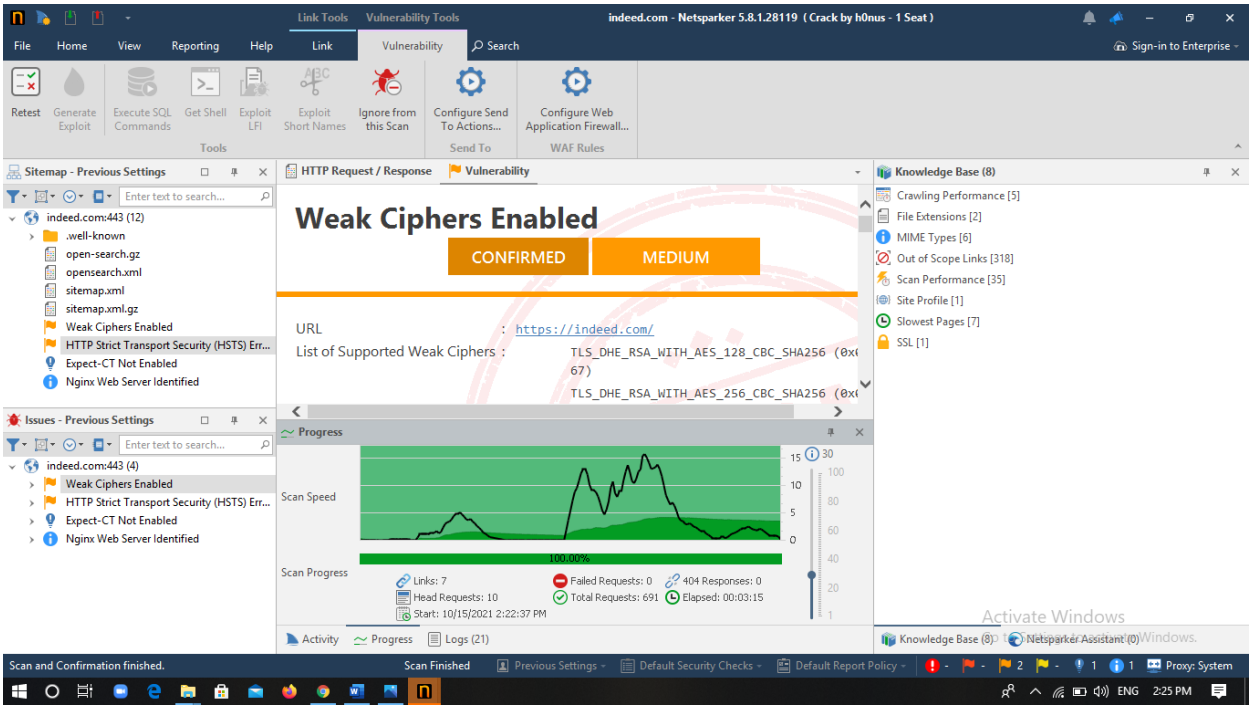
You will be notified if Netsparker is unable to automatically verify the vulnerability exists so that you may double-check its results.

- I run tool to scan shows in figure 13.

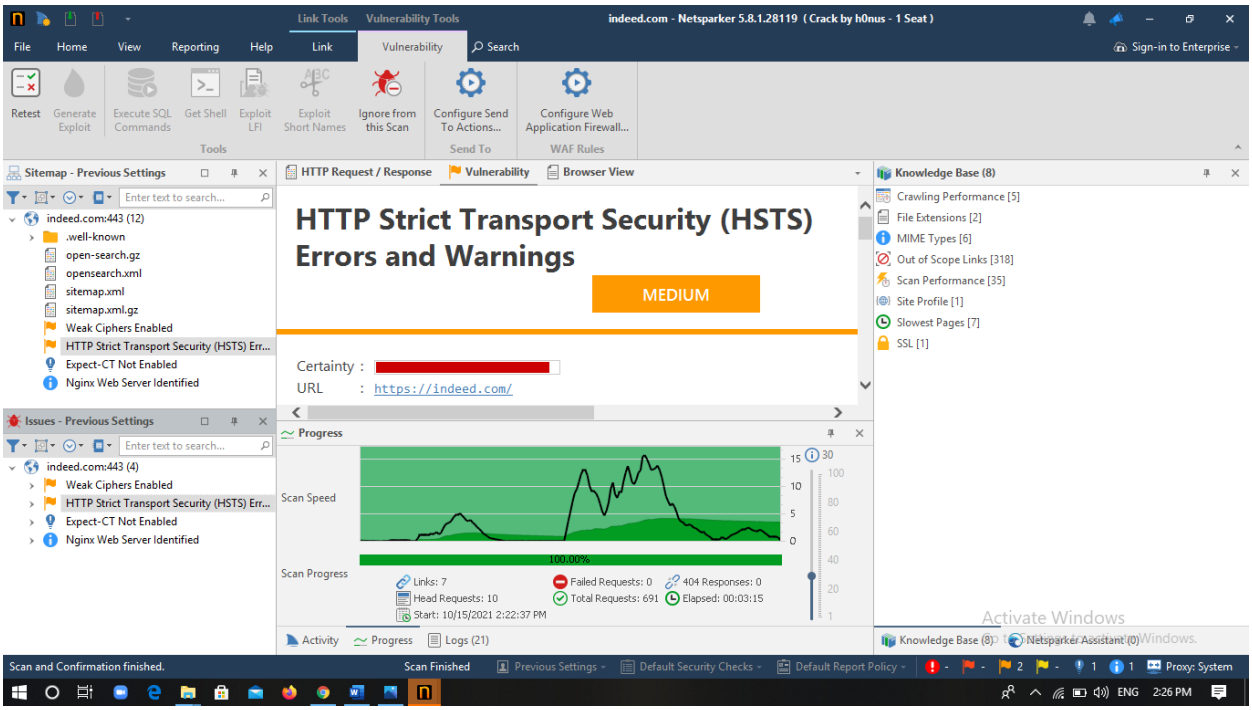


-Figure 13-

- I run this tool as a windows application and get the results.



-figure 14-



-figure 15-

- After I run netsparker , I got the result as shown in the figure 14 and 15.
- In this scan include only medium and low vulnerabilities.

6.Nessus

Nessus is a remote security scanning program that analyzes a computer and alerts you if it finds any vulnerabilities that hostile hackers may exploit to get access to any machine on your network. It accomplishes this by doing over 1200 tests on a particular machine, determining whether any of these assaults may be used to break into or harm the computer.

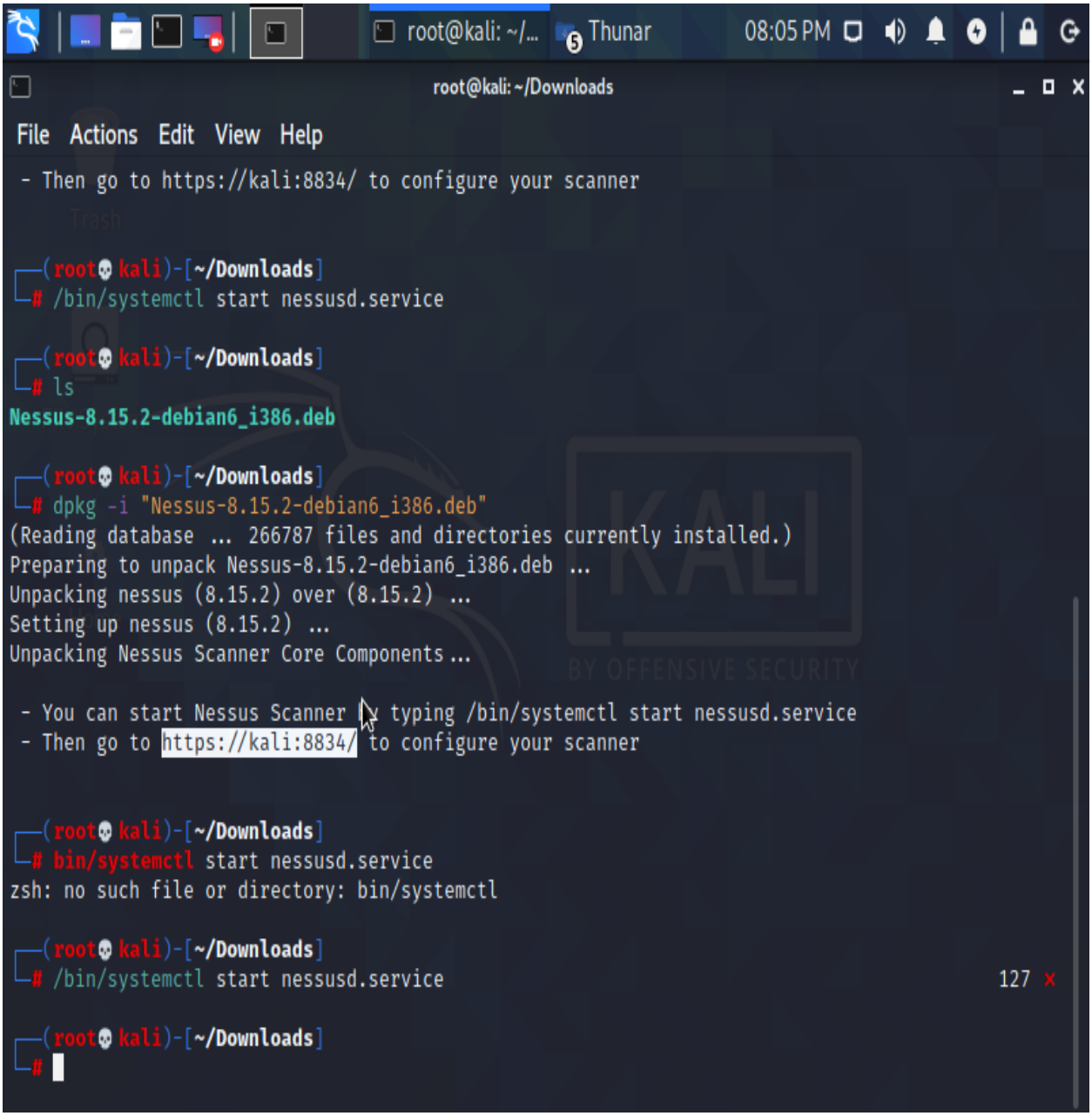
To understand how Nessus and other port-scanning security tools work, you must first understand how various services (like a web server, SMTP server, FTP server, and so on) are accessed on a remote server. The majority of high-level network traffic, such as email and web pages, is routed through a high-level protocol that is consistently delivered by a TCP stream. A computer separates its physical connection to the network into thousands of logical channels, known as ports, to prevent various streams from interfering with one other.

Every computer contains thousands of ports, some of which may or may not be used by services (for example, a server for a certain high-level protocol). Nessus works by analyzing each port on a computer, determining what service it is running, and then testing that service for vulnerabilities that may be exploited by a hacker to launch a hostile attack. Because it does not require installation on a computer to test it, Nessus is referred to as a "remote scanner." You can instead install it on just one computer and test it on as many as you want.

First we download and run nessus using the command

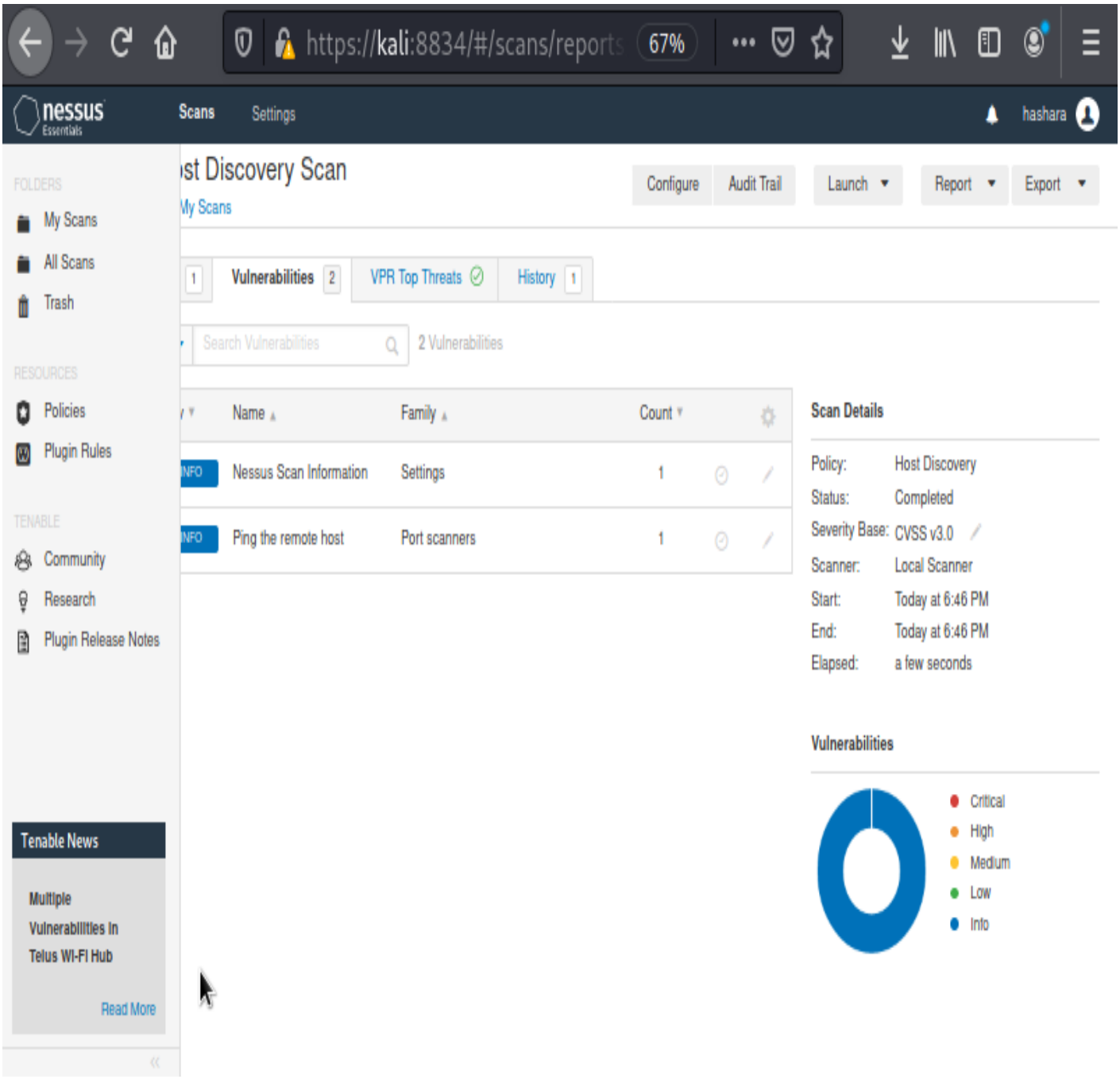
```
/bin/systemctl start nessusd.service
```

- It shows figure 16.



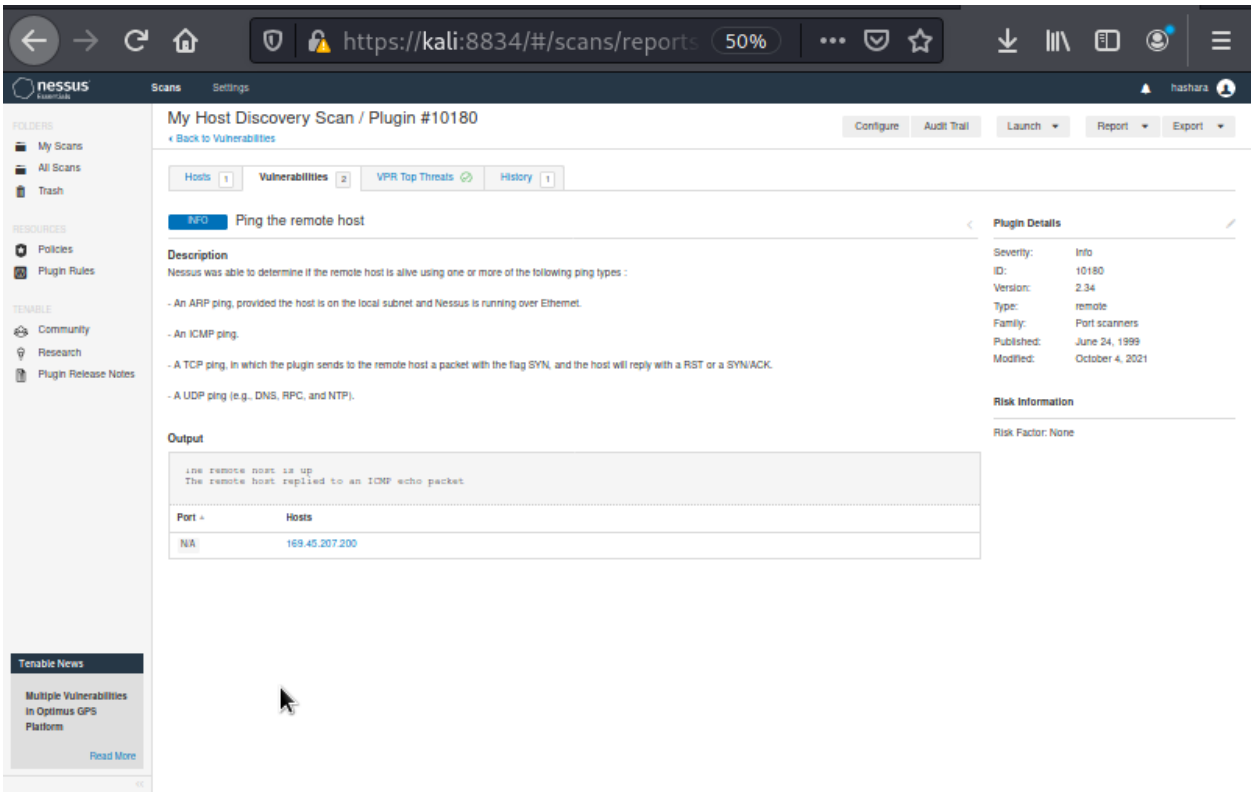
- Figure 16-

- I got the results after running the nessus scan as figure 16 ,17, 18 shows.

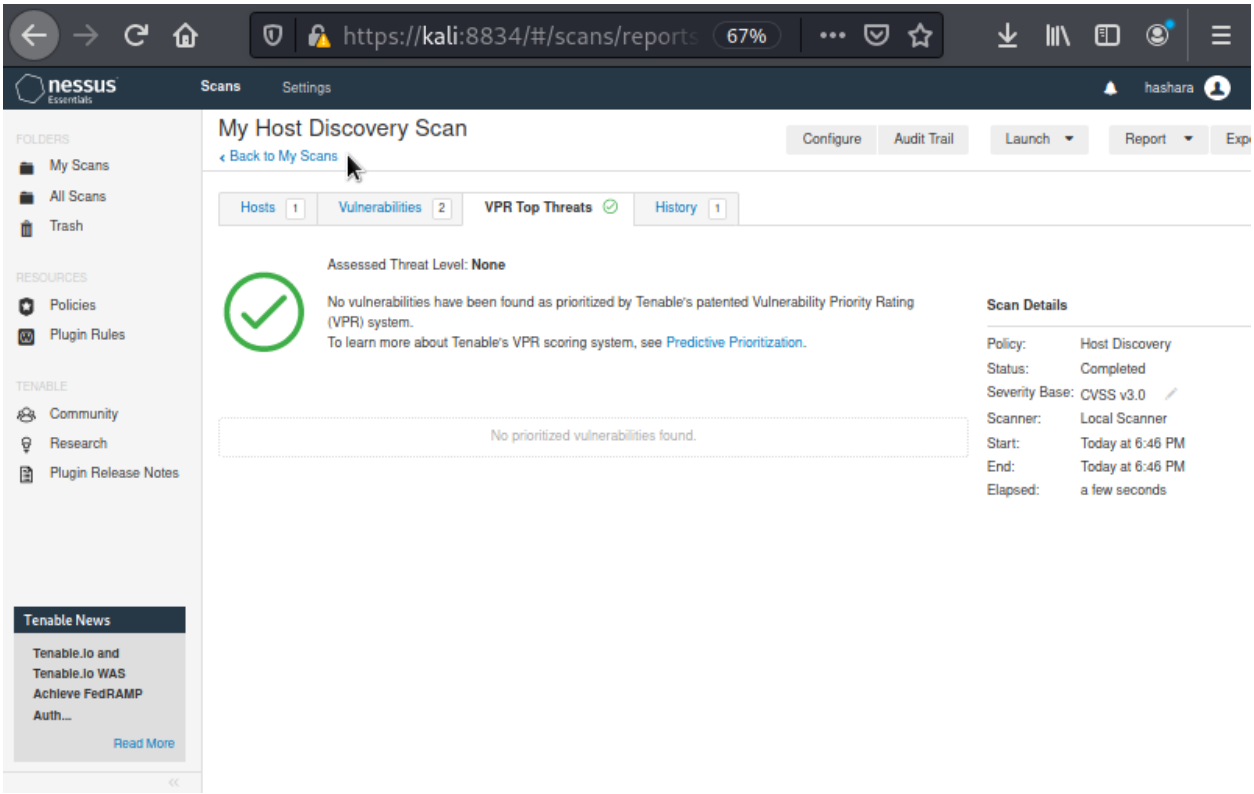


-figure 17-

This scan provided only information which are openned ports cookies used etc. which is a informative P5 in the vulnerability scale.



- Figure 18-



- figure 19 -

7.OWASP ZAP

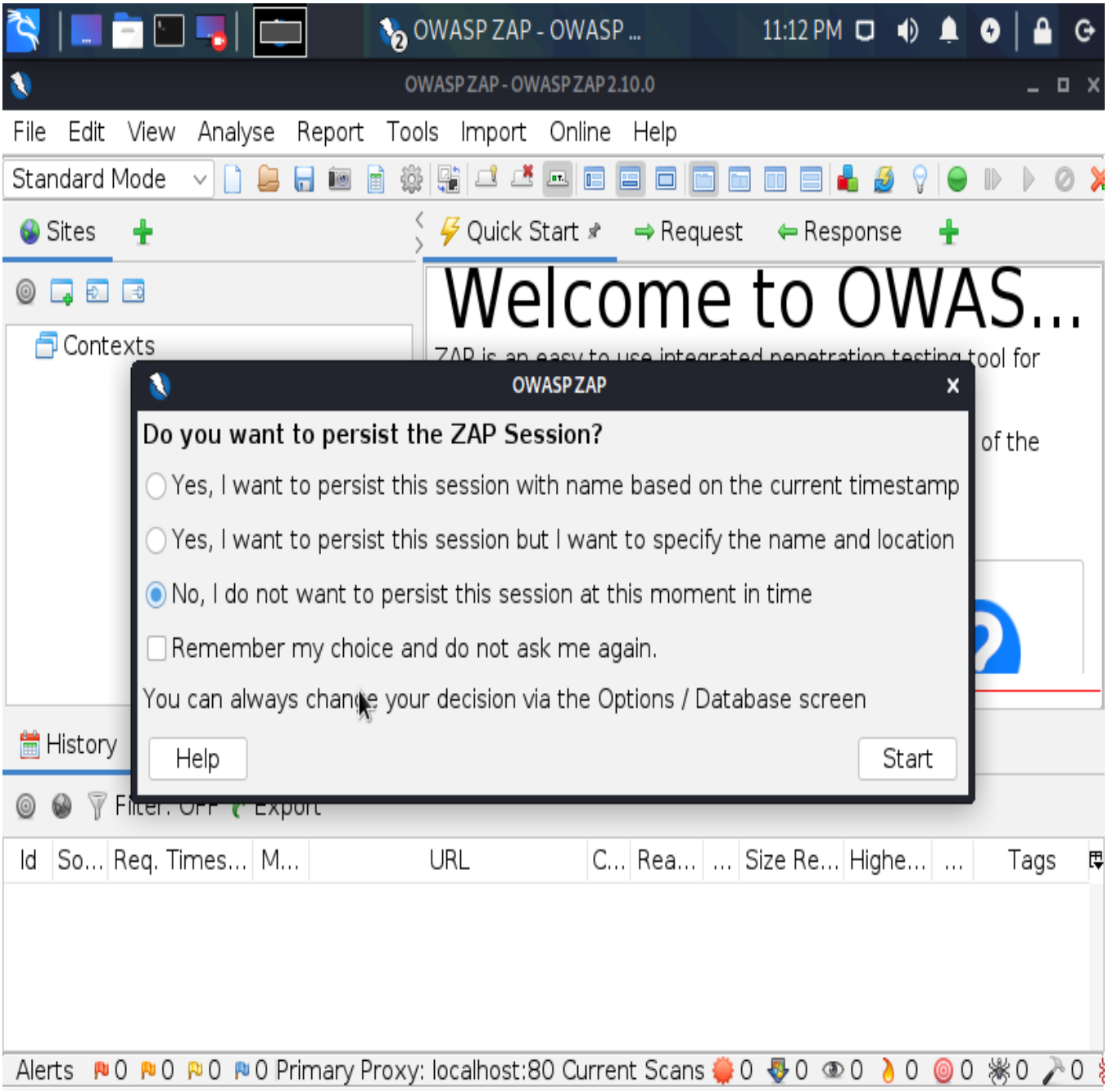
One of the most widely used web application security testing tools is the OWASP Zed Attack Proxy (ZAP). OWASP contributes to and maintains it as an open source project, which is available for free. The Open Web Application Security Project (OWASP) is a vendor-neutral, non-profit group of volunteers dedicated to making web applications more secure. The OWASP ZAP tool can be used during web application development by web developers or by experienced security experts during penetration tests to assess web applications for vulnerabilities.

Why use OWASP ZAP tool?

Web application testing must include security testing. The top OWASP security dangers that your website/application may encounter are listed below.

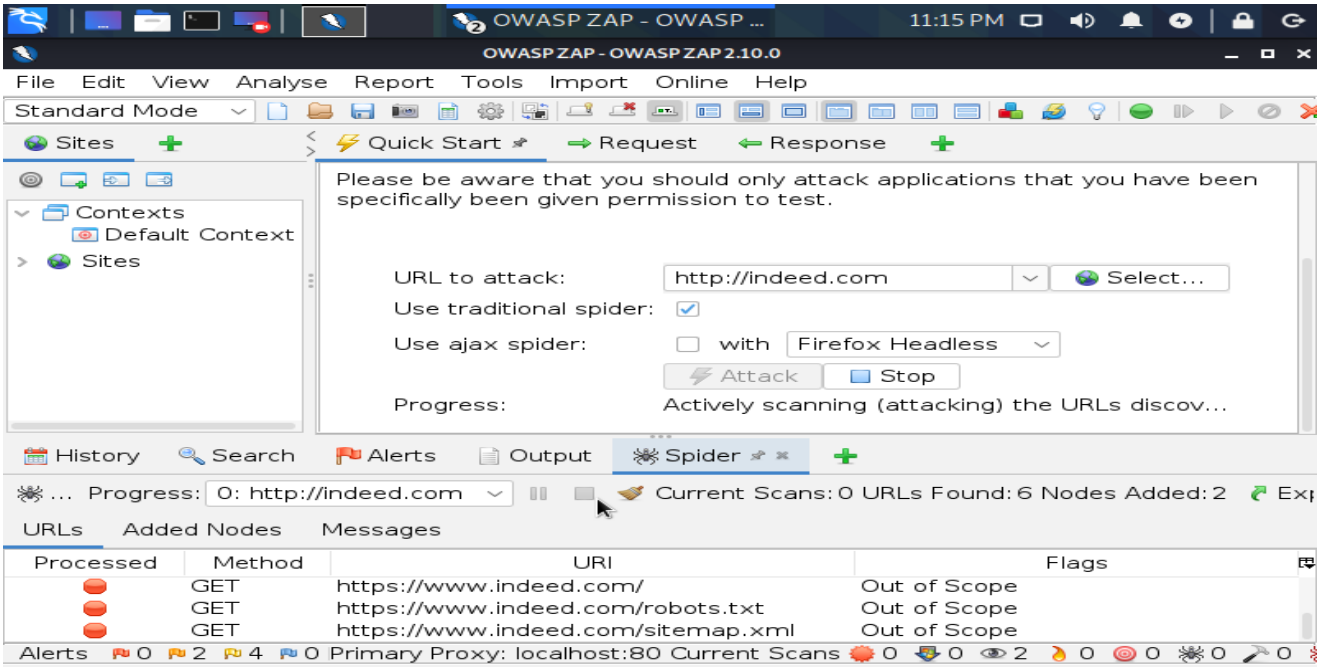
- SQL injection
- Broken authentication and session management
- Cross-site scripting (XSS)
- Broken access control
- Security misconfiguration
- Sensitive data exposure
- Insufficient attack protection
- Cross-site request forgery (CSRF)
- Using components with known vulnerabilities.
- Underprotected APIs

- Now above screenshots describe how to work this tool.

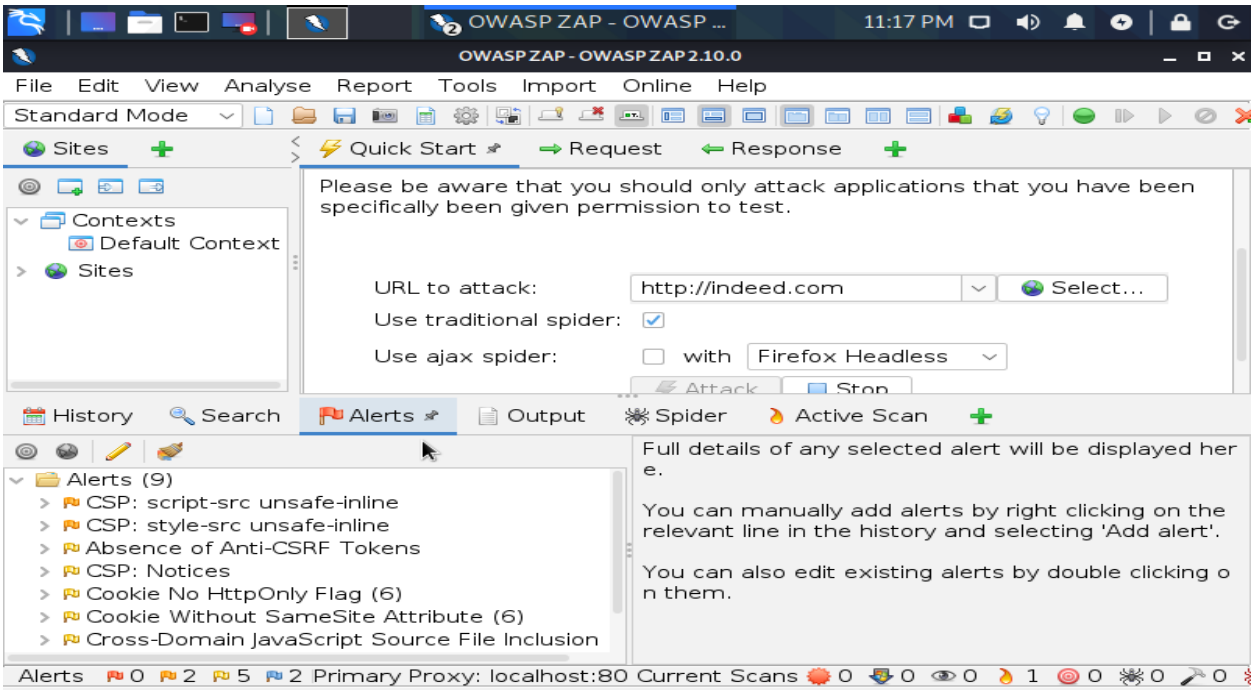


-figure 20-

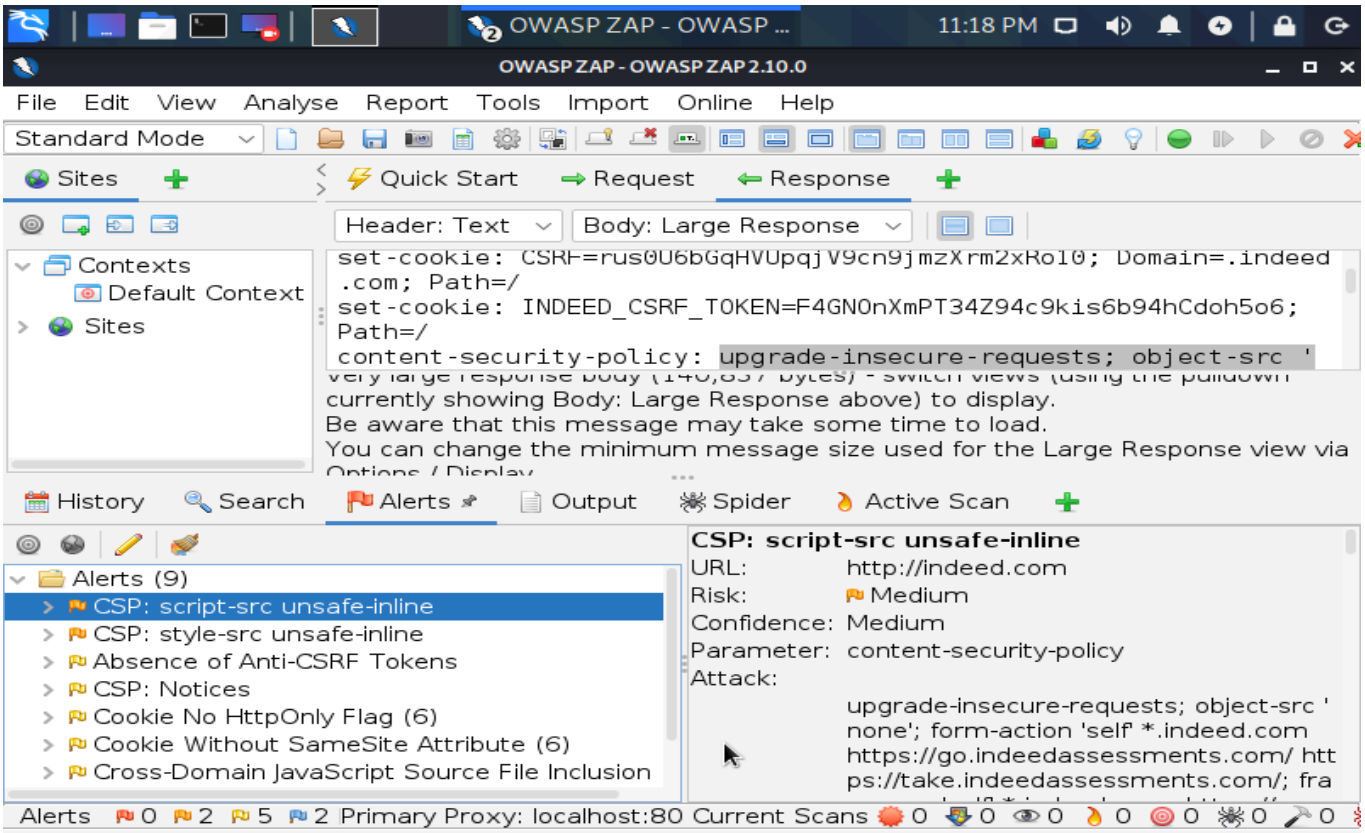
After several hours of scanning it will show some information some headers are missing. Below screenshots shows it.



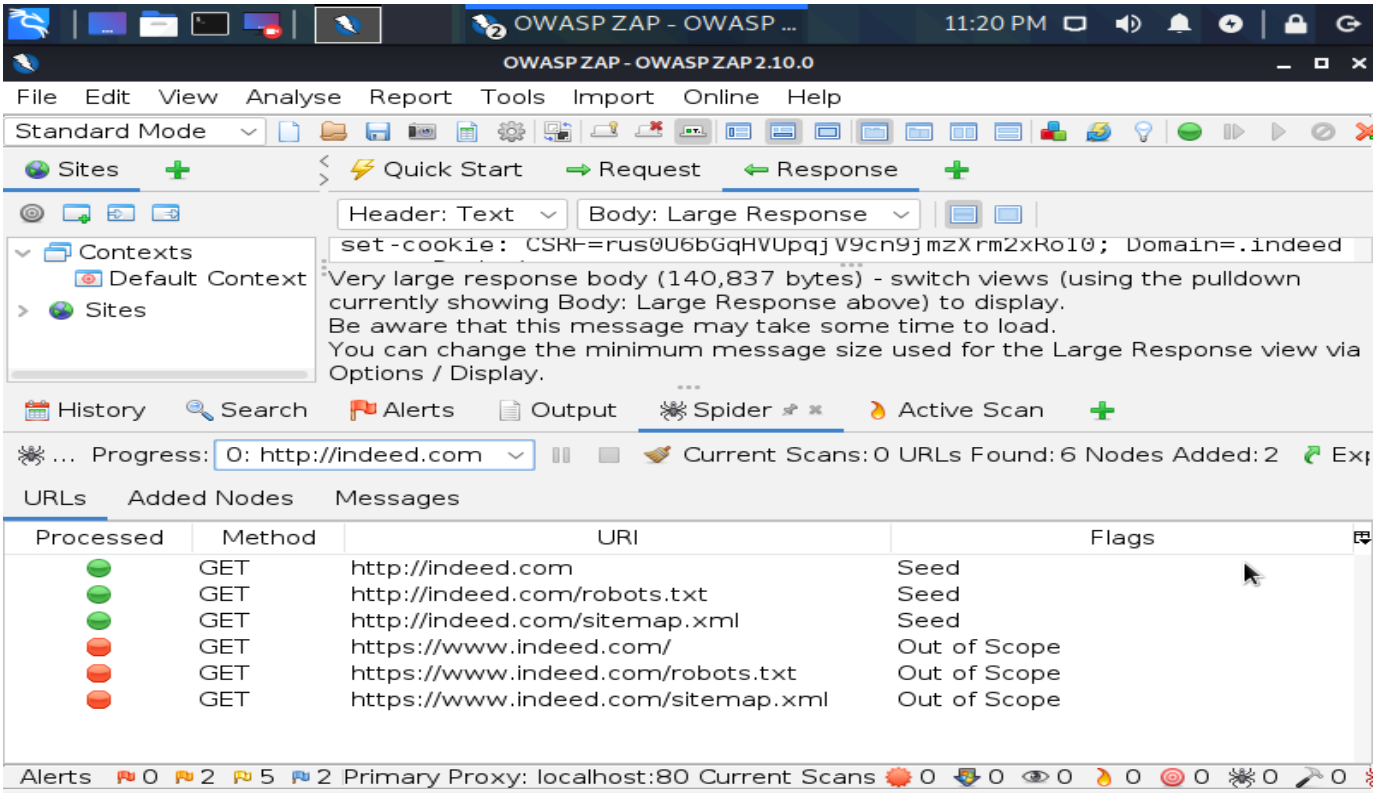
-figure 21-



-figure 22-


OWASP ZAP - OWASP ...
11:18 PM
OWASP ZAP - OWASP ZAP 2.10.0
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Quick Start
Request
Response
Header: Text
Body: Large Response
Contexts
Default Context
Sites
set-cookie: CSRF=rus0U6bGqHVUpqjV9cn9jmzXrm2xRo10; Domain=.indeed
.com; Path=/
set-cookie: INDEED_CSRF_TOKEN=F4GNOnXmPT34Z94c9kis6b94hCdoh5o6;
Path=/
content-security-policy: upgrade-insecure-requests; object-src '
currently showing Body: Large Response above) to display.
Be aware that this message may take some time to load.
You can change the minimum message size used for the Large Response view via
History
Search
Alerts
Output
Spider
Active Scan
Alerts (9)
CSP: script-src unsafe-inline
CSP: style-src unsafe-inline
Absence of Anti-CSRF Tokens
CSP: Notices
Cookie No HttpOnly Flag (6)
Cookie Without SameSite Attribute (6)
Cross-Domain JavaScript Source File Inclusion
CSP: script-src unsafe-inline
URL: http://indeed.com
Risk: Medium
Confidence: Medium
Parameter: content-security-policy
Attack:
upgrade-insecure-requests; object-src '
none'; form-action 'self' *.indeed.com
https://go.indeedassessments.com/ htt
ps://take.indeedassessments.com/; fra
Alerts 0 2 5 2 Primary Proxy: localhost:80 Current Scans 0 0 0 0 0 0 0

- Figure 23-


OWASP ZAP - OWASP ...
11:20 PM
OWASP ZAP - OWASP ZAP 2.10.0
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Quick Start
Request
Response
Header: Text
Body: Large Response
Contexts
Default Context
Sites
set-cookie: CSRF=rus0U6bGqHVUpqjV9cn9jmzXrm2xRo10; Domain=.indeed
Very large response body (140,837 bytes) - switch views (using the pulldown
currently showing Body: Large Response above) to display.
Be aware that this message may take some time to load.
You can change the minimum message size used for the Large Response view via
Options / Display.
History
Search
Alerts
Output
Spider
Active Scan
Progress: 0: http://indeed.com
Current Scans: 0 URLs Found: 6 Nodes Added: 2
URLs
Added Nodes
Messages
Processed
Method
URI
Flags
GET http://indeed.com Seed
GET http://indeed.com/robots.txt Seed
GET http://indeed.com/sitemap.xml Seed
GET https://www.indeed.com/ Out of Scope
GET https://www.indeed.com/robots.txt Out of Scope
GET https://www.indeed.com/sitemap.xml Out of Scope
Alerts 0 2 5 2 Primary Proxy: localhost:80 Current Scans 0 0 0 0 0 0 0

8. D-TECT

D-TECT is a Penetration Testing All-In-One Tool. This has been customized specifically for Penetration Testers and Security Researchers to make their jobs easier rather than deploying many devices to conduct various tasks. D-TECT provides a number of highlights and recognition highlights that help to gather target data and identify flaws.

Similarity:
Any stage utilizing Python 2.7

Requirements for the scanner:
Python 2.7
Modules(included): Colorama, BeautifulSoup

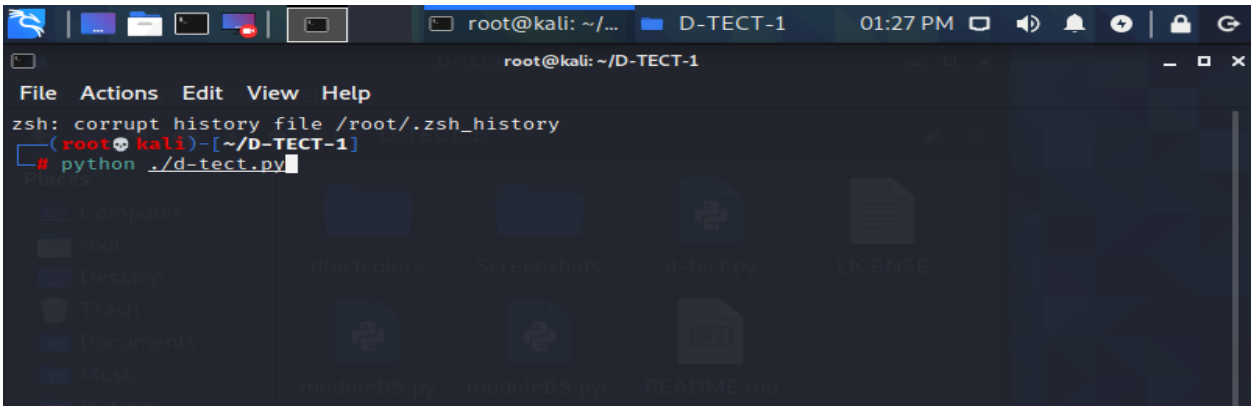
Features of the scanner :
Sub-area Scanning
Port Scanning
Wordpress Scanning
Wordpress Username Enumeration
Wordpress Backup Grabbing
Delicate File Detection
Same-Site Scripting Scanning
Snap Jacking Detection
Incredible XSS weakness checking
SQL Injection weakness checking
Easy to understand UI

How it is work?

By adjusting the succession number, you may get the optimum checking capacity (module). For example, we may use the terminal to seek for sensitive web application records by entering the arrangement number of the touchy document indicator. The device requests that the filtering cycle be continued by the target web host. D-TECT pings the target host to confirm its availability after receiving the host address. The examining cycle comes to a halt if the target host is unavailable or unavailable. In any event, if the objective space is available, D-TECT gathers some useful information about the aim before moving on to the real task, which is finding sensitive documents. The information includes the target IP address, URL diverts, backend worker information, and header information. If the X-Frame-Options header is missing, the device sends out an alert message, indicating the possibility of Click jacking in the target host.

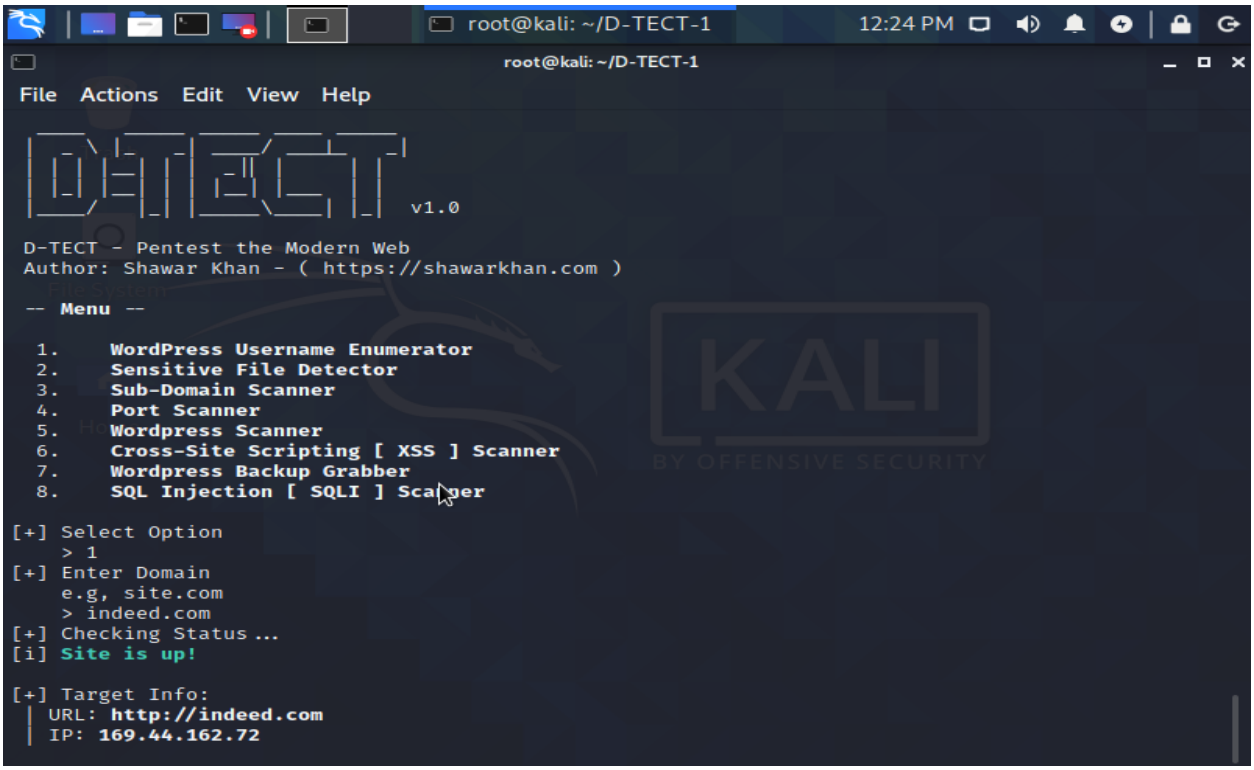
- In this scanner the git clone command is used to download the scanner and then we run it by entering the appropriate folder using the command

```
python ./d-tect.py
```

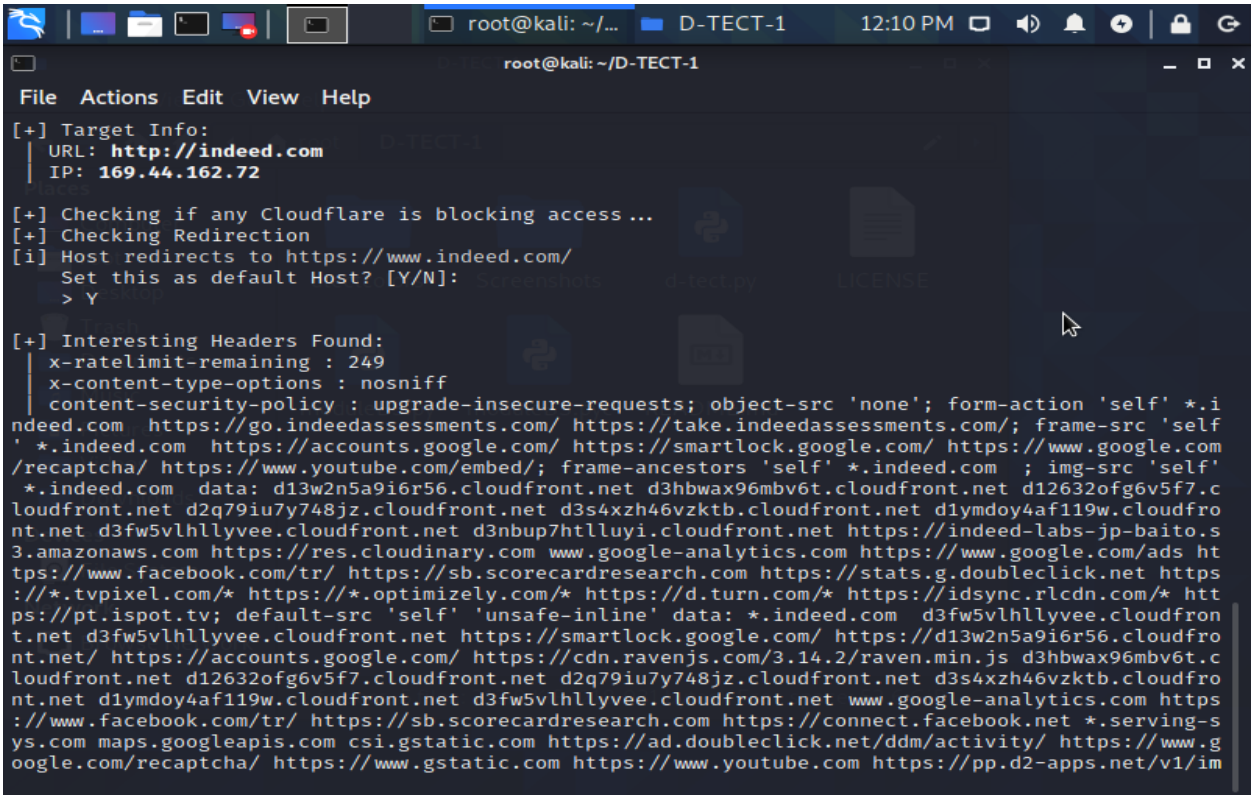


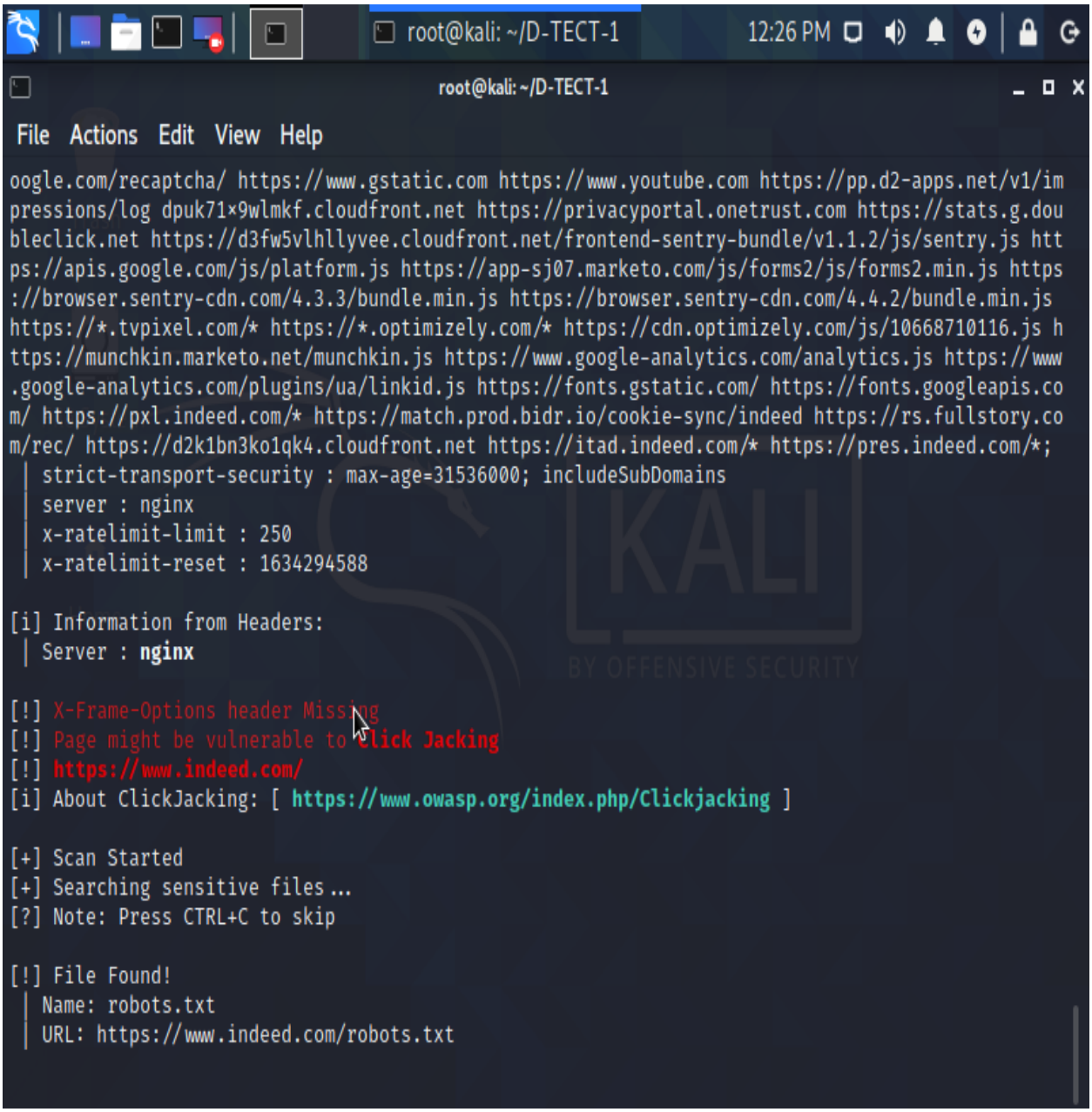
-figure 23-

. Then we select an option and enter the the domain



- Figure 24 –

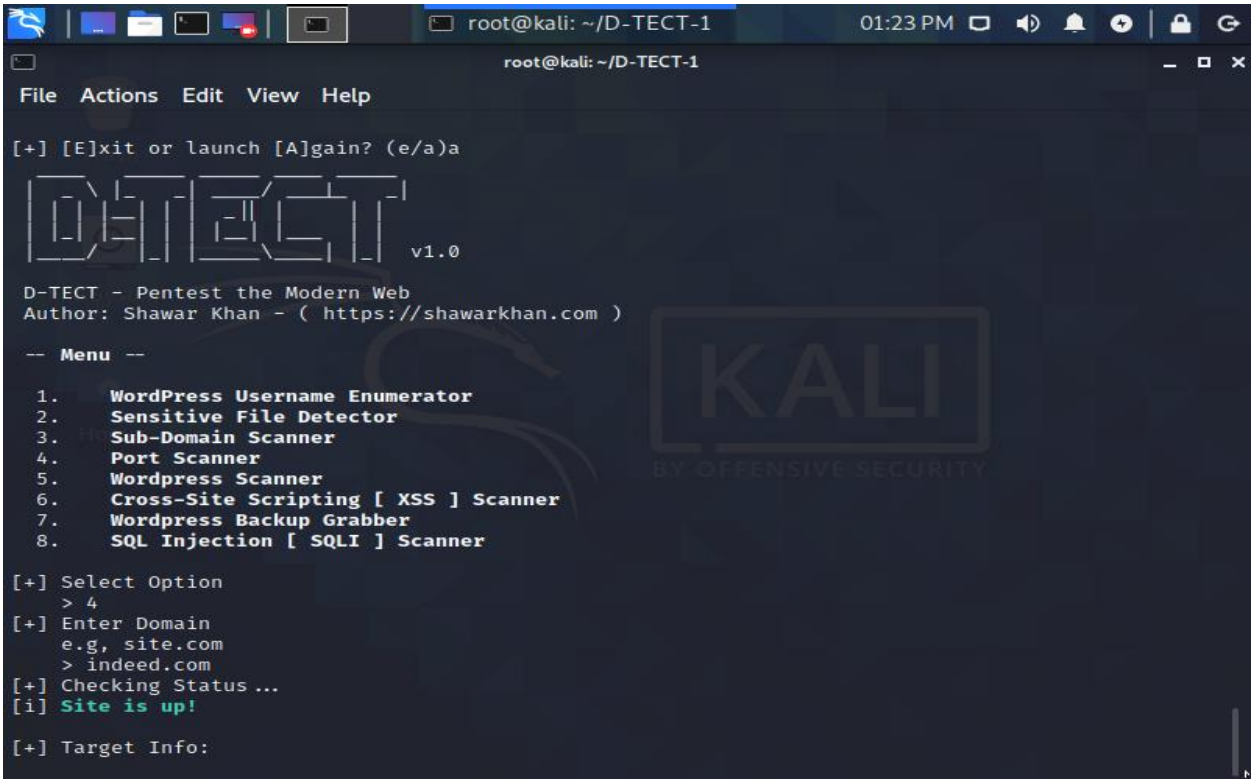


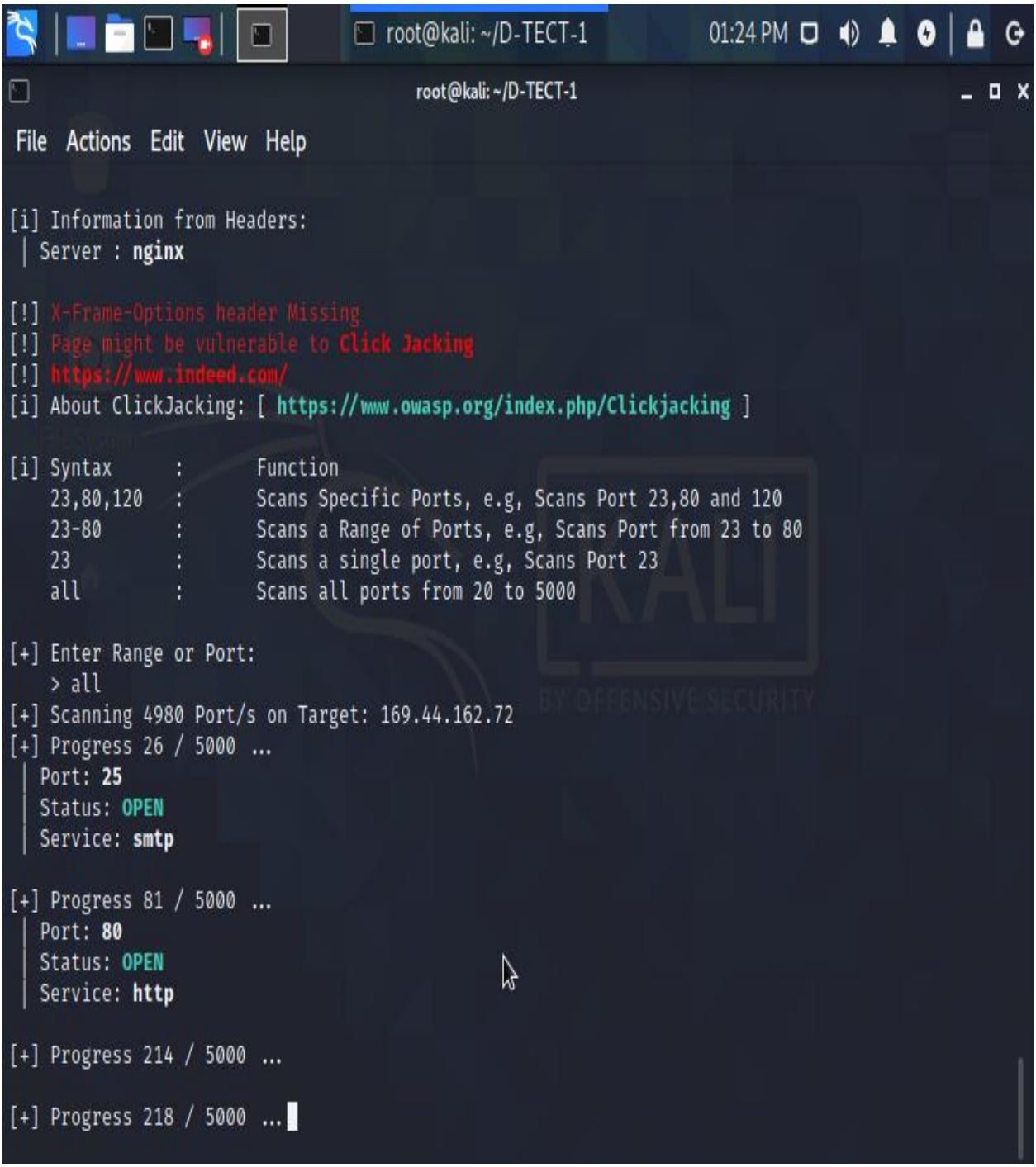


In this case we can see it shows that the page is vulnerable to Click Jacking

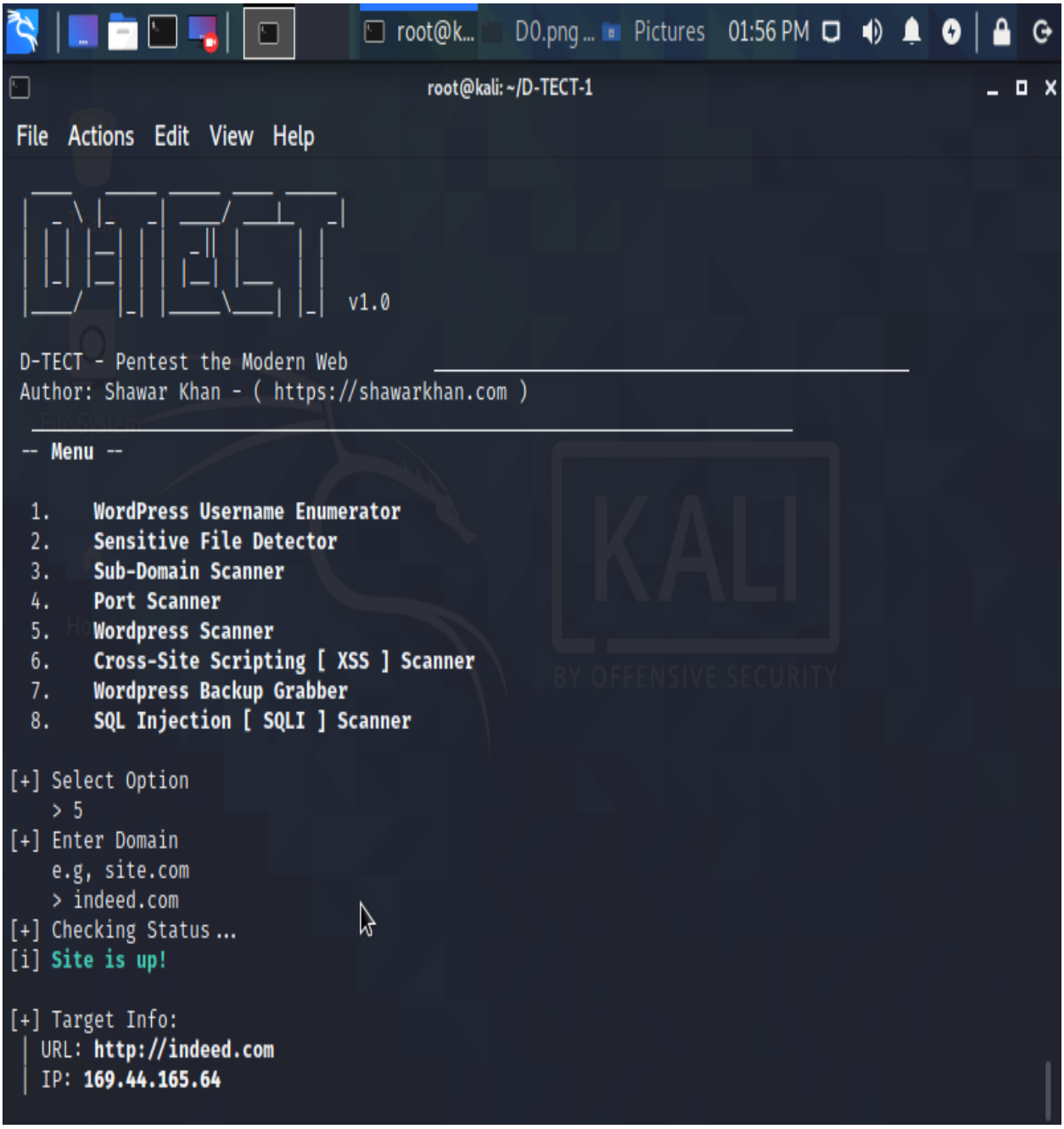
- Figure 24-

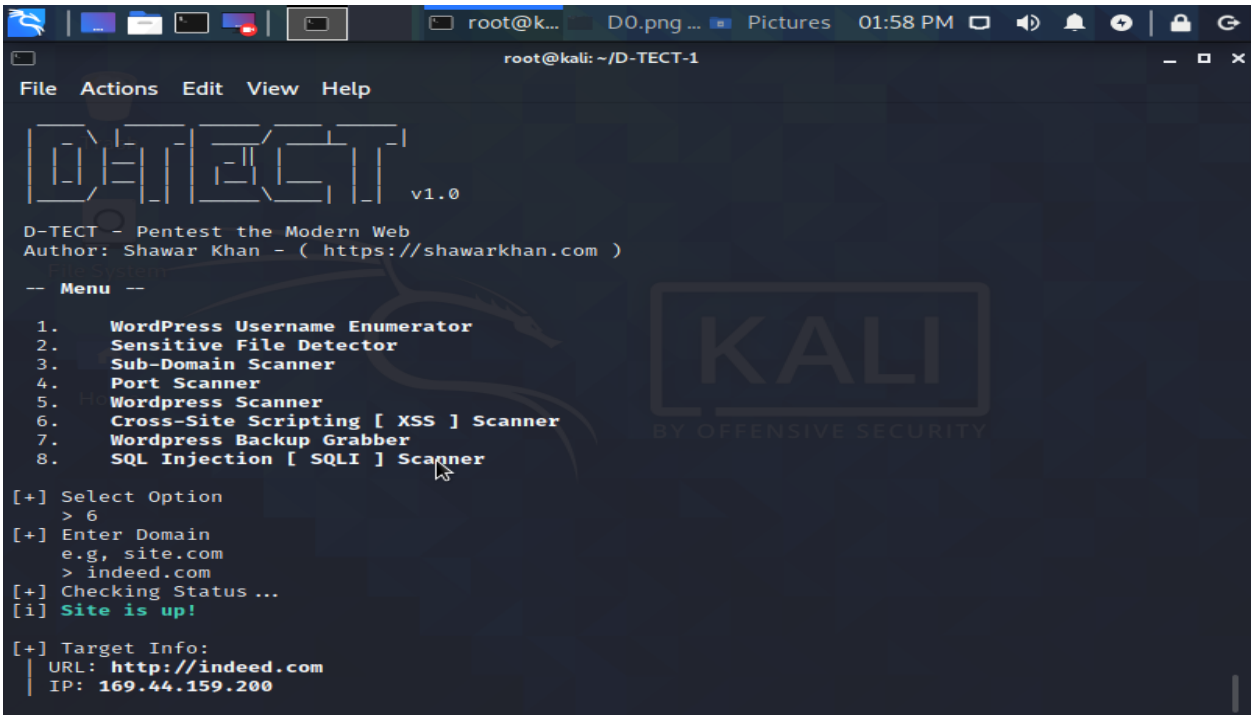
- Now we run the 4th option which is the port scanner which took 20 hours to scan and gave a result of 2 open ports.

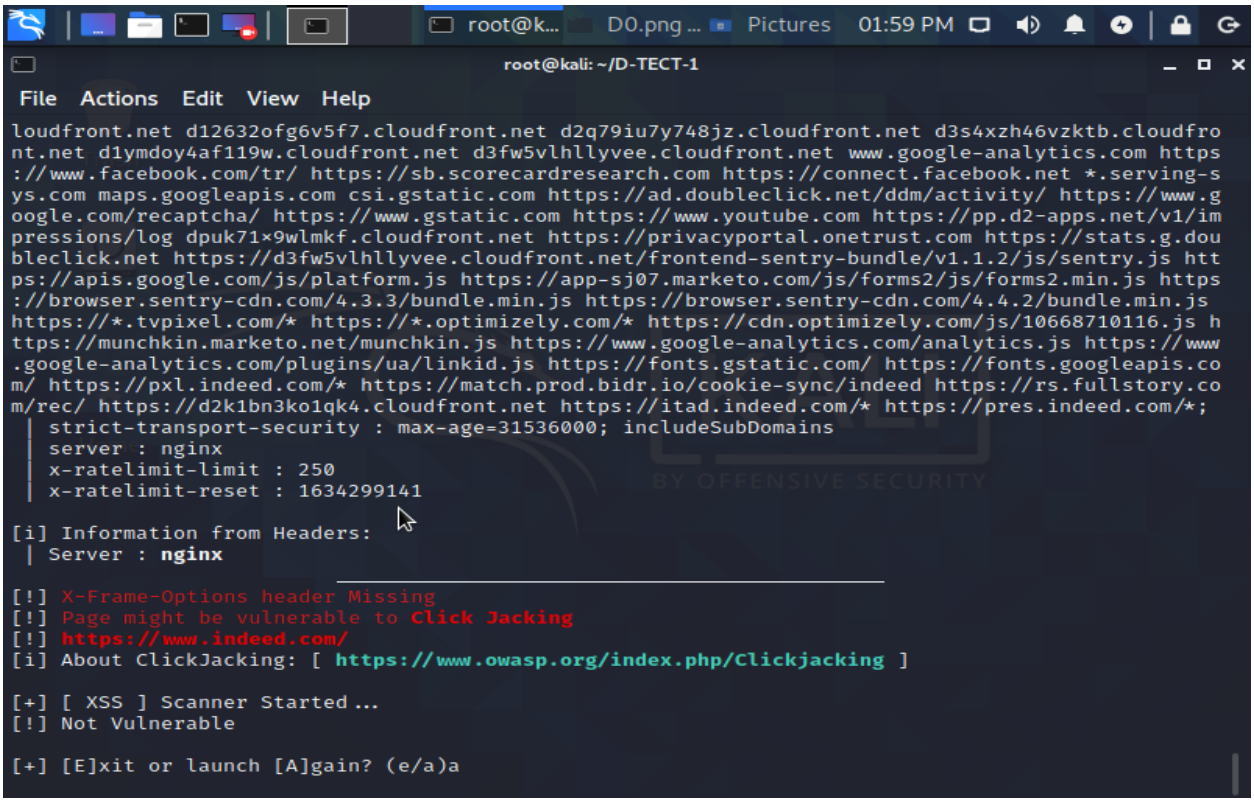


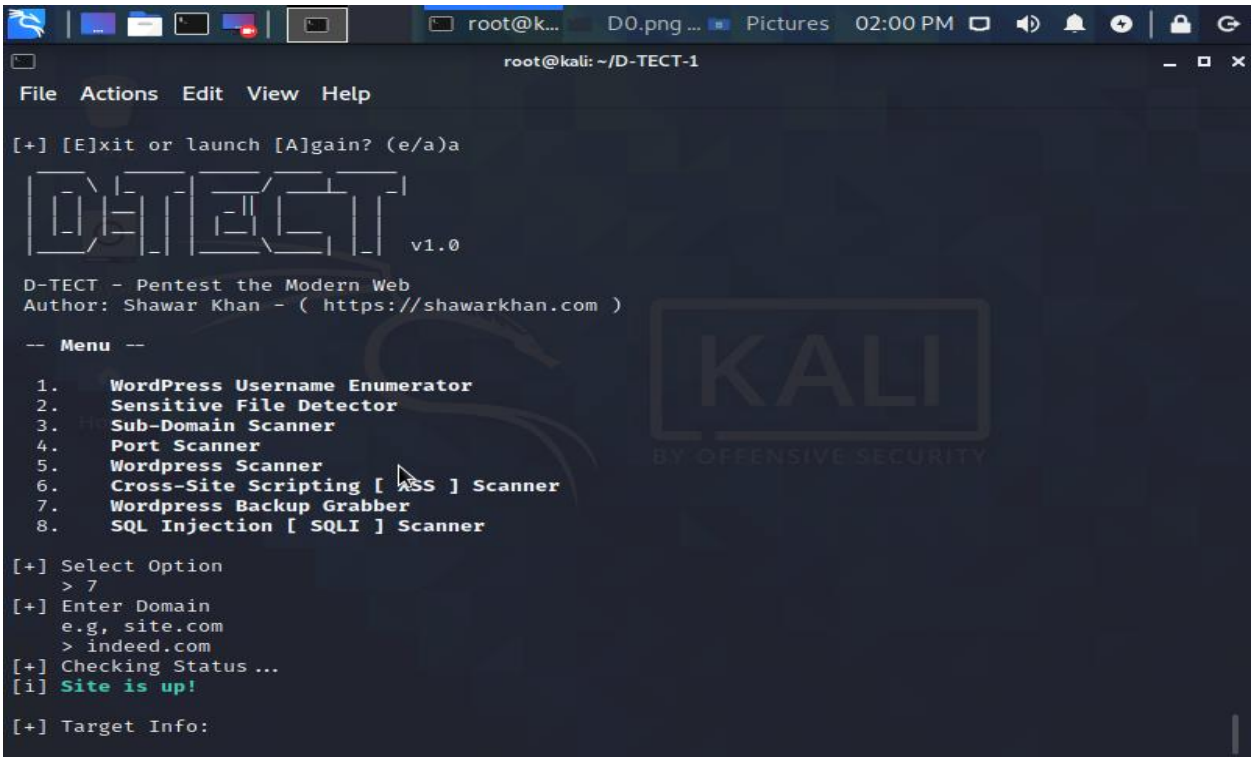

root@kali: ~/D-TECT-1
01:24 PM
root@kali: ~/D-TECT-1
File Actions Edit View Help
[i] Information from Headers:
| Server : nginx
[!] X-Frame-Options header Missing
[!] Page might be vulnerable to Click Jacking
[!] https://www.indeed.com/
[i] About ClickJacking: [https://www.owasp.org/index.php/Clickjacking]
[i] Syntax : Function
23,80,120 : Scans Specific Ports, e.g, Scans Port 23,80 and 120
23-80 : Scans a Range of Ports, e.g, Scans Port from 23 to 80
23 : Scans a single port, e.g, Scans Port 23
all : Scans all ports from 20 to 5000
[+] Enter Range or Port:
> all
[+] Scanning 4980 Port/s on Target: 169.44.162.72
[+] Progress 26 / 5000 ...
| Port: 25
| Status: OPEN
| Service: smtp
[+] Progress 81 / 5000 ...
| Port: 80
| Status: OPEN
| Service: http
[+] Progress 214 / 5000 ...
[+] Progress 218 / 5000 ...

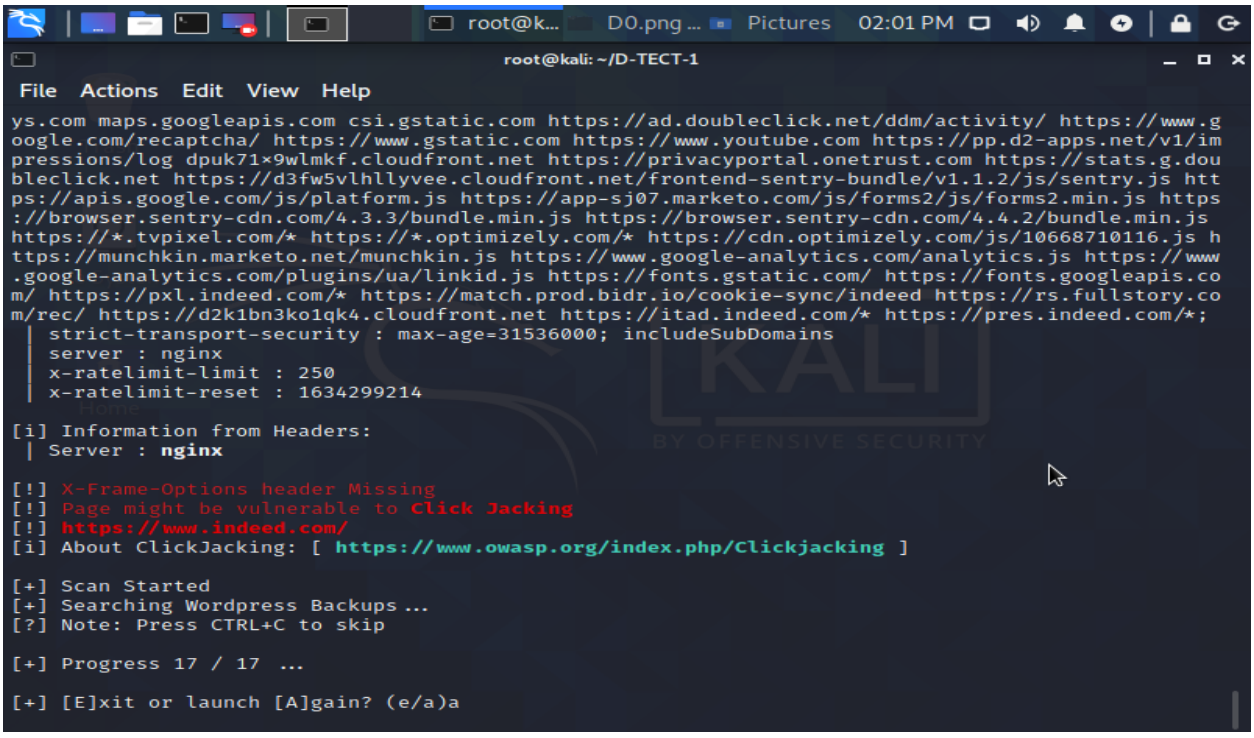
Now we run the 5th , 6th , 7th and 8th option which is the word press scanner, XXS scripting, wordpress backup generator and SQL injection. Which gave a result of not vulnerable, but vulnerability of click jacking.

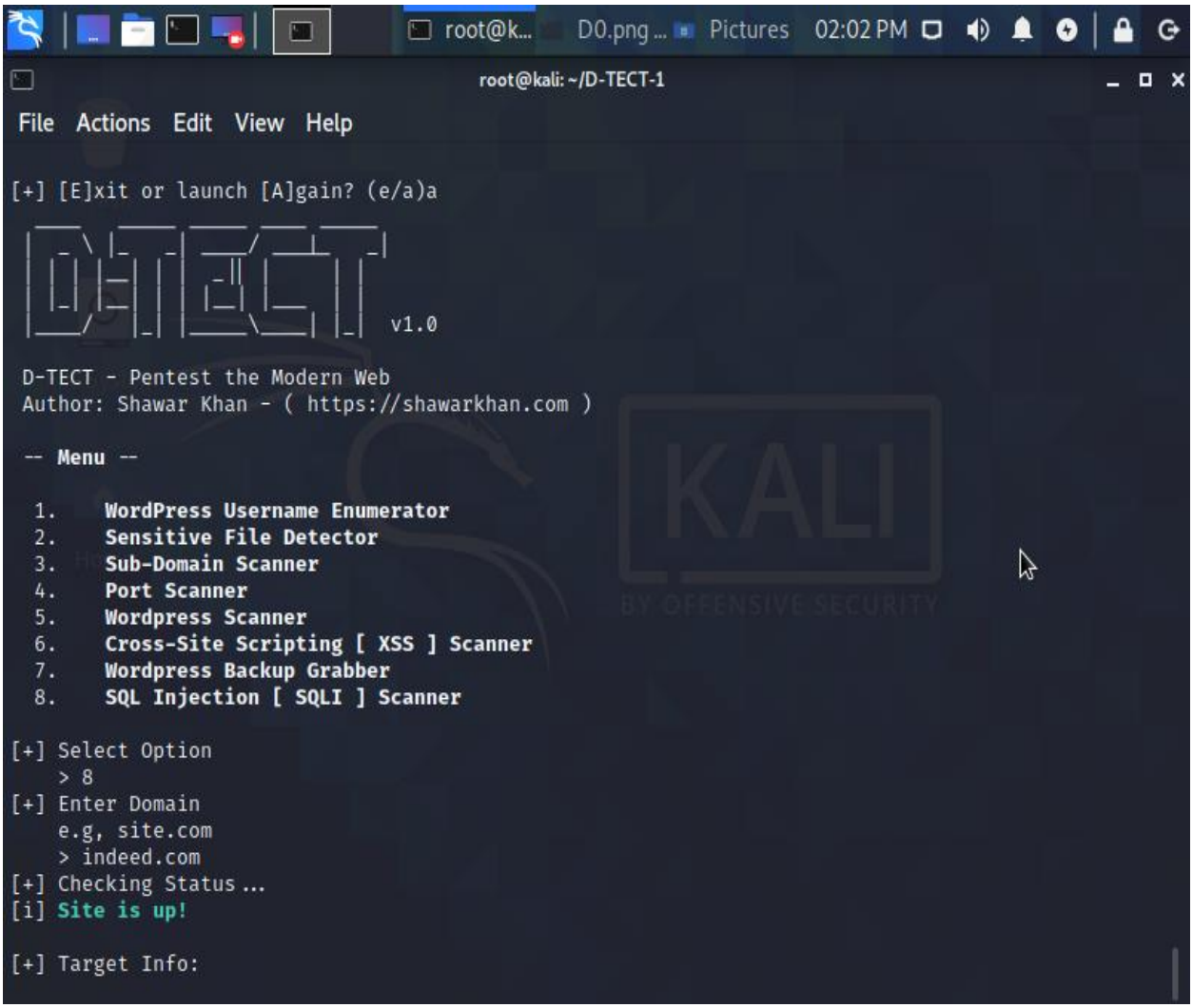



root@k... DO.png ... Pictures 01:58 PM
root@kali: ~/D-TECT-1
File Actions Edit View Help
v1.0
D-TECT - Pentest the Modern Web
Author: Shawar Khan - (https://shawarkhan.com)
-- Menu --
1. WordPress Username Enumerator
2. Sensitive File Detector
3. Sub-Domain Scanner
4. Port Scanner
5. Wordpress Scanner
6. Cross-Site Scripting [XSS] Scanner
7. Wordpress Backup Grabber
8. SQL Injection [SQLI] Scanner
[+] Select Option
> 6
[+] Enter Domain
e.g, site.com
> indeed.com
[+] Checking Status ...
[i] Site is up!
[+] Target Info:
| URL: http://indeed.com
| IP: 169.44.159.200


root@k... DO.png ... Pictures 01:59 PM
root@kali: ~/D-TECT-1
File Actions Edit View Help
loudfront.net d12632ofg6v5f7.cloudfront.net d2q79iu7y748jz.cloudfront.net d3s4xzh46vzktb.cloudfront.net d1ymdoy4af119w.cloudfront.net d3fw5vlhllyvee.cloudfront.net www.google-analytics.com https://www.facebook.com/tr/ https://sb.scorecardresearch.com https://connect.facebook.net *.serving-sys.com maps.googleapis.com csi.gstatic.com https://ad.doubleclick.net/ddm/activity/ https://www.google.com/recaptcha/ https://www.gstatic.com https://www.youtube.com https://pp.d2-apps.net/v1/impressions/log dpuk71x9wlmkf.cloudfront.net https://privacyportal.onetrust.com https://stats.g.doubleclick.net https://d3fw5vlhllyvee.cloudfront.net/frontend-sentry-bundle/v1.1.2/js/sentry.js https://apis.google.com/js/platform.js https://app-sj07.marketo.com/js/forms2/js/forms2.min.js https://browser.sentry-cdn.com/4.3.3/bundle.min.js https://browser.sentry-cdn.com/4.4.2/bundle.min.js https://*.tvpixel.com/* https://*.optimizely.com/* https://cdn.optimizely.com/js/10668710116.js https://munchkin.marketo.net/munchkin.js https://www.google-analytics.com/analytics.js https://www.google-analytics.com/plugins/ua/linkid.js https://fonts.gstatic.com/ https://fonts.googleapis.com/ https://pxl.indeed.com/* https://match.prod.bidr.io/cookie-sync/indeed https://rs.fullstory.com/rec/ https://d2k1bn3ko1qk4.cloudfront.net https://itad.indeed.com/* https://pres.indeed.com/*;
| strict-transport-security : max-age=31536000; includeSubDomains
| server : nginx
| x-ratelimit-limit : 250
| x-ratelimit-reset : 1634299141
[i] Information from Headers:
| Server : nginx
[!] X-Frame-Options header Missing
[!] Page might be vulnerable to Click Jacking
[!] https://www.indeed.com/
[i] About ClickJacking: [https://www.owasp.org/index.php/Clickjacking]
[+] [XSS] Scanner Started ...
[!] Not Vulnerable
[+] [E]xit or launch [A]gain? (e/a)a


root@k... D0.png ... Pictures 02:00 PM
root@kali: ~/D-TECT-1
File Actions Edit View Help
[+] [E]xit or launch [A]gain? (e/a)a
v1.0
D-TECT - Pentest the Modern Web
Author: Shawar Khan - (https://shawarkhan.com)
-- Menu --
1. WordPress Username Enumerator
2. Sensitive File Detector
3. Sub-Domain Scanner
4. Port Scanner
5. Wordpress Scanner
6. Cross-Site Scripting [XSS] Scanner
7. Wordpress Backup Grabber
8. SQL Injection [SQLI] Scanner
[+] Select Option
> 7
[+] Enter Domain
e.g, site.com
> indeed.com
[+] Checking Status ...
[i] Site is up!
[+] Target Info:


root@k... D0.png ... Pictures 02:01 PM
root@kali: ~/D-TECT-1
File Actions Edit View Help
ys.com maps.googleapis.com csi.gstatic.com https://ad.doubleclick.net/ddm/activity/ https://www.g
oogle.com/recaptcha/ https://www.gstatic.com https://www.youtube.com https://pp.d2-apps.net/v1/im
pressions/log dpuk71x9wlmkf.cloudfront.net https://privacyportal.onetrust.com https://stats.g.dou
bleclick.net https://d3fw5vlhllyvee.cloudfront.net/frontend-sentry-bundle/v1.1.2/js/sentry.js htt
ps://apis.google.com/js/platform.js https://app-sj07.marketo.com/js/forms2/js/forms2.min.js https
://browser.sentry-cdn.com/4.3.3/bundle.min.js https://browser.sentry-cdn.com/4.4.2/bundle.min.js
https://*.tvpixel.com/* https://*.optimizely.com/* https://cdn.optimizely.com/js/10668710116.js h
ttps://munchkin.marketo.net/munchkin.js https://www.google-analytics.com/analytics.js https://www
.google-analytics.com/plugins/ua/linkid.js https://fonts.gstatic.com/ https://fonts.googleapis.co
m/ https://pxl.indeed.com/* https://match.prod.bidr.io/cookie-sync/indeed https://rs.fullstory.co
m/rec/ https://d2k1bn3ko1qk4.cloudfront.net https://itad.indeed.com/* https://pres.indeed.com/*;
| strict-transport-security : max-age=31536000; includeSubDomains
| server : nginx
| x-ratelimit-limit : 250
| x-ratelimit-reset : 1634299214
[i] Information from Headers:
| Server : nginx
[!] X-Frame-Options header Missing
[!] Page might be vulnerable to Click Jacking
[!] https://www.indeed.com/
[i] About ClickJacking: [https://www.owasp.org/index.php/Clickjacking]
[+] Scan Started
[+] Searching Wordpress Backups ...
[?] Note: Press CTRL+C to skip
[+] Progress 17 / 17 ...
[+] [E]xit or launch [A]gain? (e/a)a



By using the D-TECT scanner we can see that this site is vulnerable for a click jacking attack which is a Medium (P3) in a vulnerable scale

What is clickjacking ?

Clickjacking is a type of attack in which a client is tricked into clicking a page component that is hidden or disguised as another component. Clients may unintentionally download malware, view malicious website pages, provide credentials or sensitive data, transfer money, or make online purchases as a result of this.
Clickjacking is most commonly accomplished by inserting an undetected page or HTML component into an iframe at the top of the client's website. The customer acknowledges that they are touching the visible page, but in reality, they are clicking an inconspicuous component on the additional page translated over top of it.
The invisible page might be a malicious page or a legitimate page that the client didn't expect to see - for as a page on the customer's financial site that approves a cash transaction.

There are several types of clickjacking attacks, for example.

1. **Likejacking** – a procedure where the Facebook "Like" button is controlled, making clients "like" a page they really didn't expect to like.

2. **Cursorjacking** – a UI reviewing method that changes the cursor for the position the client sees to another position.

Solutions to prevent this attack

To defend yourself against clickjacking, you can choose one of two approaches:

Client side strategies – Frame Busting is the most well-known of them. Customer-side approaches can be effective at times, but they are not regarded best practices because they are easily circumvented.

Server side strategies - X-Frame-Options is the most well-known. Security experts recommend worker-side methods as a powerful way to protect against clickjacking.

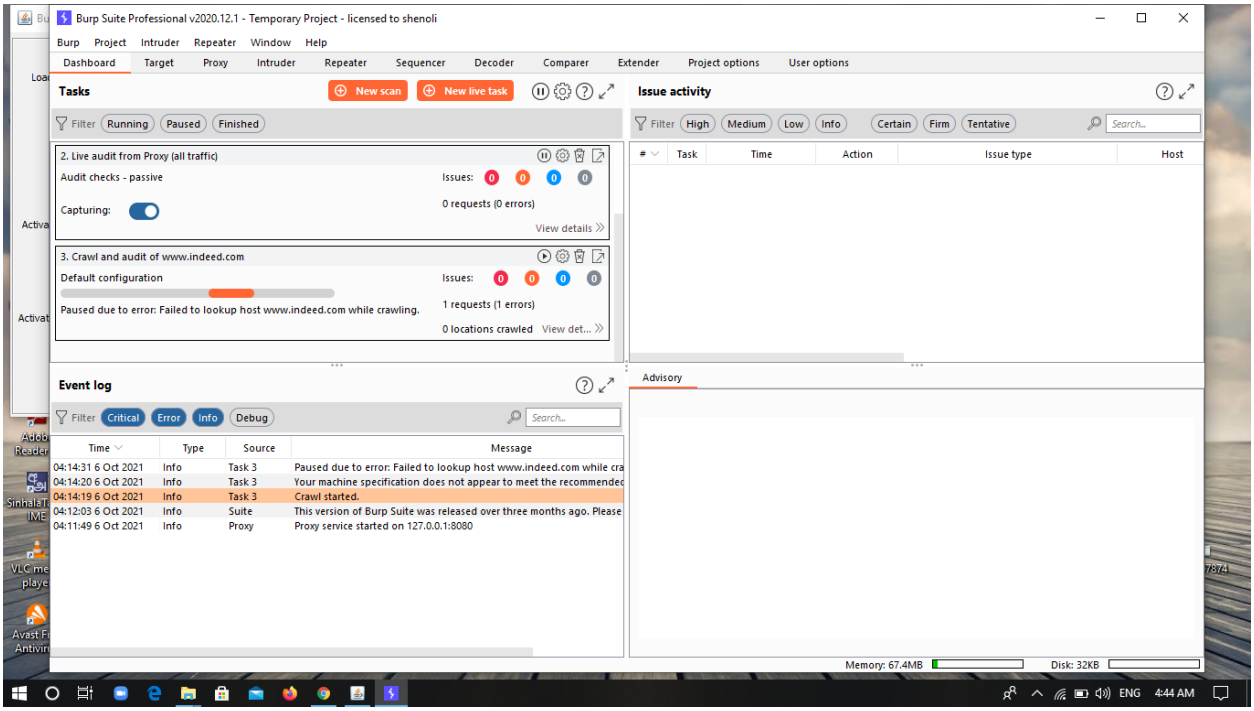
9. Burp suite

Burp Suite is a full-featured web application assault tool that can perform nearly any task you can think of while penetrating a website.

Burp Suite's ability to intercept HTTP requests is one of its most useful capabilities. Normally, HTTP requests are sent directly from your browser to a web server, and the web server answer is sent to your browser. HTTP requests, on the other hand, are sent directly from your browser to Burp Suite, which intercepts the traffic.

Before passing the request to the web server, you may alter the raw HTTP in Burp Suite in a variety of ways. This technology essentially acts as a proxy, or "man in the middle," between you and the web service, allowing you to have more precise control over the traffic you transmit and receive.

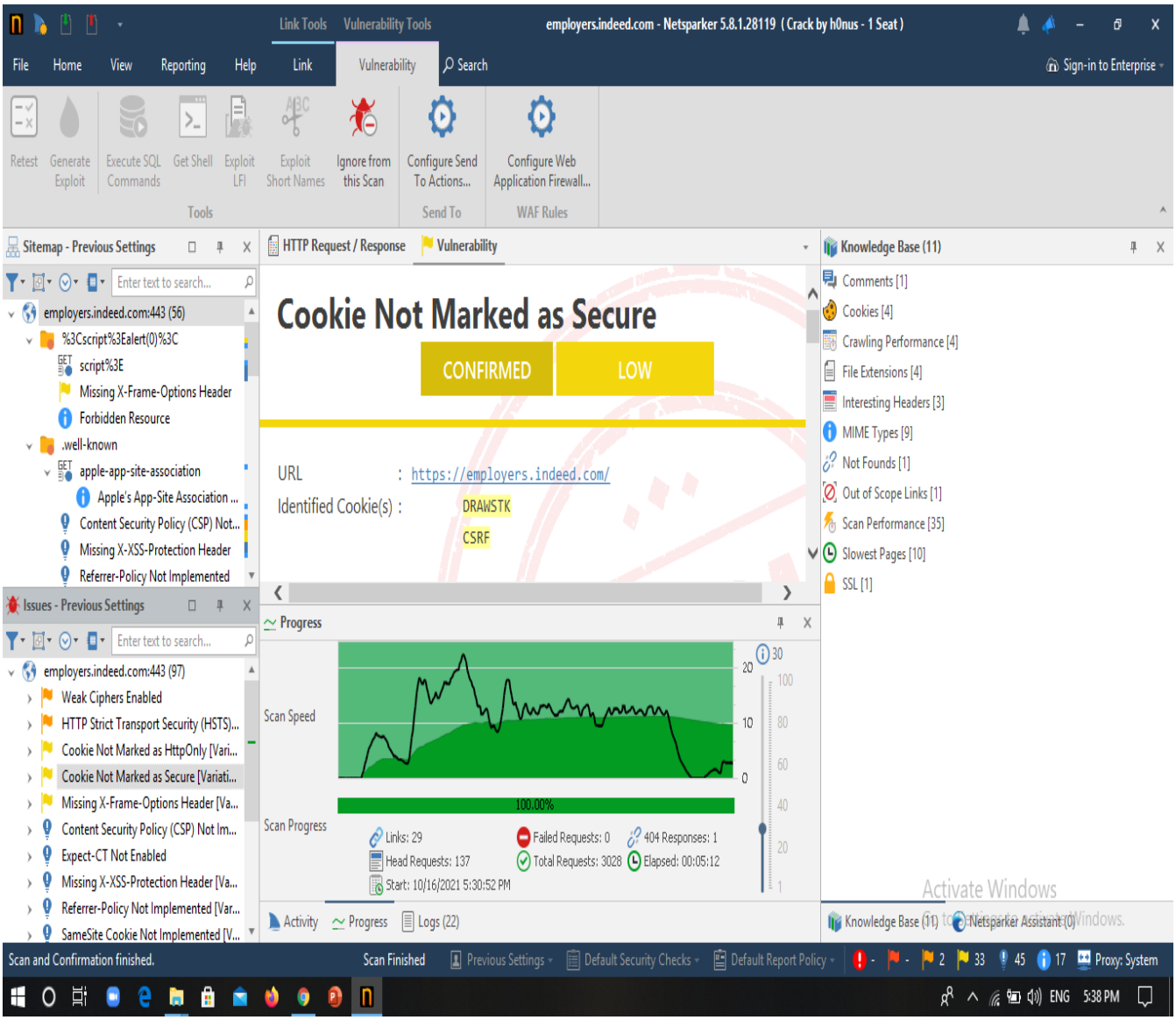
The objective of the Burp intercepting proxy functionality is to change requests such that they still respect HTTP rules but can cause the application to behave unpredictably.



I used BurpSuite to scan my domain, I leave it to run about two hours, but it did not give any result after two hours. Then I close the scan.

I selected some subdomains.

1. https://employers.indeed.com/



This subdomain show this kind of vulnerabilities. this risk level is Low.

10. Skipfish

What is skipfish?

Skipfish is a web application security reconnaissance tool that is currently in use. It uses a recursive crawl and dictionary-based probes to create an interactive sitemap for the chosen site. The output of a number of active (but presumably non-disruptive) security tests is then marked on the resultant map. The tool's final report is intended to be used as a starting point for professional web application security evaluations.

Why should I bother with this particular tool?

There are a variety of commercial and open source programs with similar capabilities (e.g., Nikto, Websecurify, Netsparker, w3af, Arachni); choose the one that best meets your needs. Skipfish, on the other hand, seeks to solve some of the most typical issues with web security scanners. Some of the benefits are as follows:

High performance: With a very small CPU, network, and memory footprint, 500+ requests per second against responsive Internet targets, 2000+ requests per second over LAN / MAN networks, and 7000+ requests against local instances have been recorded. This can be attributable to the following factors:

- Memory management, scheduling, and IPC inefficiencies found in certain multi-threaded clients are eliminated with our multiplexing single-thread, completely asynchronous network I/O and data processing approach.
- Range requests, content compression, and stay-alive connections, as well as mandatory response size restriction, are advanced HTTP/1.1 capabilities that minimize network-level overhead to a minimum.
- To reduce needless traffic, smart response caching and sophisticated server behavior heuristics are applied.
- Implementation in pure C that focuses on performance and includes a bespoke HTTP stack.

Ease of use: **skipfish:** is highly adaptive and reliable. The scanner features:

- Detection of cryptic path- and query-based parameter handling techniques using heuristics.
- Graceful handling of multi-framework sites when various pathways have entirely different semantics or are filtered differently.
- Automatic wordlist generation based on content analysis of the website.
- Periodic, time-bound examinations of arbitrarily complex locations are possible because to probabilistic scanning characteristics.

Well-designed security checks : the tool is meant to provide accurate and meaningful results:

- Handcrafted dictionaries provide good coverage and allow for full testing of $keyword.$extensions in a reasonable amount of time.
- For discovering vulnerabilities, three-step differential probes are preferable over signature checks.
- To detect minor security vulnerabilities like as cross-site request forgeries, cross-site script inclusion, mixed content, MIME- and charset incompatibilities, erroneous caching directives, and so on, Ratproxy-style logic is utilized.
- Stored XSS (path, arguments, headers), blind SQL or XML injection, or blind shell injection are all instances that bundled security checks are meant to address.

Most curious! What specific tests are implemented?

- High risk flaws (potentially leading to system compromise):
    - Server-side SQL / PHP injection (including blind vectors, numerical parameters).
    - Explicit SQL-like syntax in GET or POST parameters.
    - Server-side shell command injection (including blind vectors).
    - Server-side XML / XPath injection (including blind vectors).
    - Format string vulnerabilities.
    - Integer overflow vulnerabilities.
    - Locations accepting HTTP PUT.

- Medium risk flaws (potentially leading to data compromise):
    - Stored and reflected XSS vectors in document body (minimal JS XSS support present).
    - Stored and reflected XSS vectors via HTTP redirects.
    - Stored and reflected XSS vectors via HTTP header splitting.
    - Directory traversal / file inclusion (including constrained vectors).
    - Assorted file POIs (server-side sources, configs, etc).
    - Attacker-supplied script and CSS inclusion vectors (stored and reflected).
    - External untrusted script and CSS inclusion vectors.
    - Mixed content problems on script and CSS resources (optional).
    - Password forms submitting from or to non-SSL pages (optional).
    - Incorrect or missing MIME types on renderables.
    - Generic MIME types on renderables.
    - Incorrect or missing charsets on renderables.
    - Conflicting MIME / charset info on renderables.
    - Bad caching directives on cookie setting responses.

- Low risk issues (limited impact or low specificity):
    - Directory listing bypass vectors.
    - Redirection to attacker-supplied URLs (stored and reflected).
    - Attacker-supplied embedded content (stored and reflected).
    - External untrusted embedded content.
    - Mixed content on non-scriptable subresources (optional).
    - HTTPS -> HTTP submission of HTML forms (optional).
    - HTTP credentials in URLs.
    - Expired or not-yet-valid SSL certificates.
    - HTML forms with no XSRF protection.
    - Self-signed SSL certificates.
    - SSL certificate host name mismatches.
    - Bad caching directives on less sensitive content.

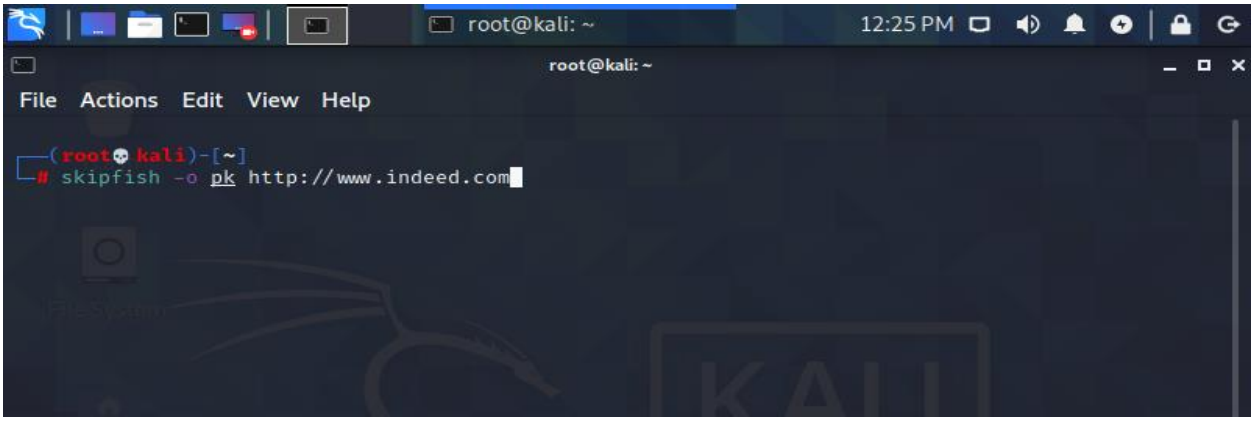
- Internal warnings:
    - Failed resource fetch attempts.
    - Exceeded crawl limits.
    - Failed 404 behavior checks.
    - IPS filtering detected.
    - Unexpected response variations.
    - Seemingly misclassified crawl nodes.

- Non-specific informational entries:
    - General SSL certificate information.
    - Significantly changing HTTP cookies.
    - Changing Server, Via, or X-... headers.
    - New 404 signatures.
    - Resources that cannot be accessed.
    - Resources requiring HTTP authentication.
    - Broken links.
    - Server errors.
    - All external links not classified otherwise (optional).
    - All external e-mails (optional).
    - All external URL redirectors (optional).
    - Links to unknown protocols.
    - Form fields that could not be autocompleted.
    - Password entry forms (for external brute-force).
    - File upload forms.
    - Other HTML forms (not classified otherwise).
    - Numerical file names (for external brute-force).
    - User-supplied links otherwise rendered on a page.
    - Incorrect or missing MIME type on less significant content.
    - Generic MIME type on less significant content.
    - Incorrect or missing charset on less significant content.
    - Conflicting MIME / charset information on less significant content.

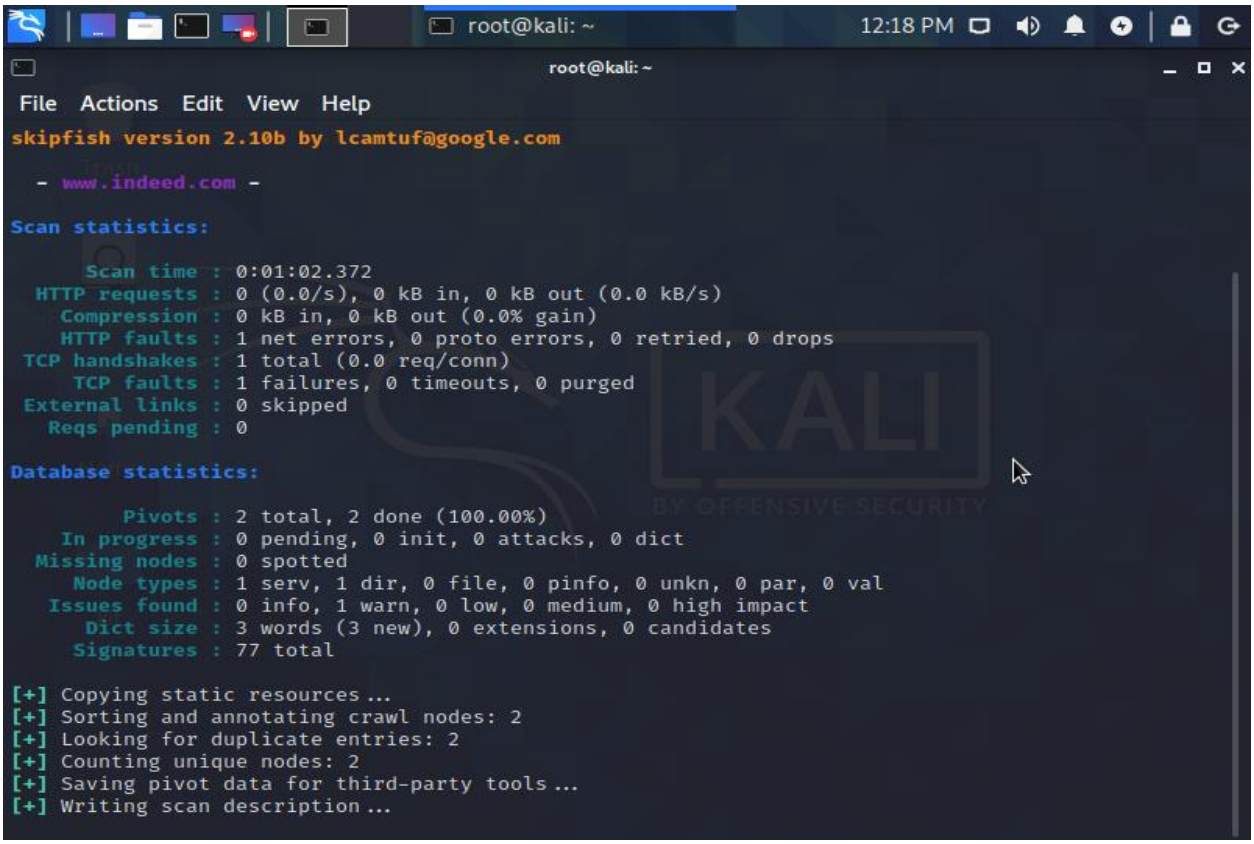
Screenshots after run this skipfish scanner

Skipfish -o pk http://www.indeed.com

Run this command in the skipfish scanner.



After we get this kind of results.



Conclusion

After many scans I did not get any high/critical vulnerabilities related to my selected domain www.indeed.com only the Netsparker showed a medium vulnerability. To complete the information gathering part respectively I have used Sublist3r, Amass, Namp, Nikto, Netsparker, Nessus, zap and BurpSuite. Therefore, I can conclude that this domain “indeed.com” is a secured web application.

References.

1. https://www.bugcrowd.com/bug-bounty-list/
2. https://www.youtube.com/watch?v=8PaVBe0cbIU
3. https://www.kali.org/tools/nikto/
4. https://securitytrails.com/blog/open-ports
5. https://www.csoonline.com/article/3032743/web-application-firewall-a-must-have-security-control-or-an-outdated-technology.html
6. https://en.wikipedia.org/wiki/Indeed
7. https://www.indeed.com/about
8. https://www.srijan.net/resources/blog/intro-owasp-zed-attack-proxy