Smart Internz

Group - 2.17

1. **Kartik Sharma – 20BCY10044**
2. **Mohammad Shoab – 20BCY10054**
3. **Aadil Haidar Ali – 20BCY10070**
4. **Om Sahare – 20BCY10091**
5. **Sanskar Kumar Burman – 20BCY10097**

Web Application Penetration Testing

1 INTRODUCTION

1.1 Overview

The purpose of this report is to present the findings of the foot-printing, reconnaissance, exploitation, and remediation activities conducted on the domain "cvent.com." The assessment aimed to gather information about the target domain's infrastructure, identify potential vulnerabilities, exploit those vulnerabilities to assess the impact, and provide recommendations for remediation to improve its security posture.

1.2 Purpose

The purpose of this project is to conduct a comprehensive web application penetration test on the domain "cvent.com." This involves gathering information about the target's infrastructure through foot-printing and reconnaissance, identifying potential vulnerabilities, exploiting those vulnerabilities to assess the impact, and providing recommendations for remediation. The objective is to enhance the security of the web application and mitigate potential risks.

2 LITERATURE SURVEY

2.1 Existing problem

The existing problem is the potential vulnerabilities and weaknesses present in the web application hosted on "cvent.com." These vulnerabilities may expose the application to various security threats, such as unauthorized access, data breaches, or denial-of-service attacks.

2.2 Proposed solution

The proposed solution is to conduct a thorough foot-printing and reconnaissance process to gather information about the target domain. This includes passive and active techniques to identify potential weaknesses or entry

points that could be exploited in subsequent stages of an attack. The findings will be used to enhance the security of the web application.

3 THEORITICAL ANALYSIS

3.1 Block diagram

This is the block diagram of steps to perform Web Application Penetration Testing

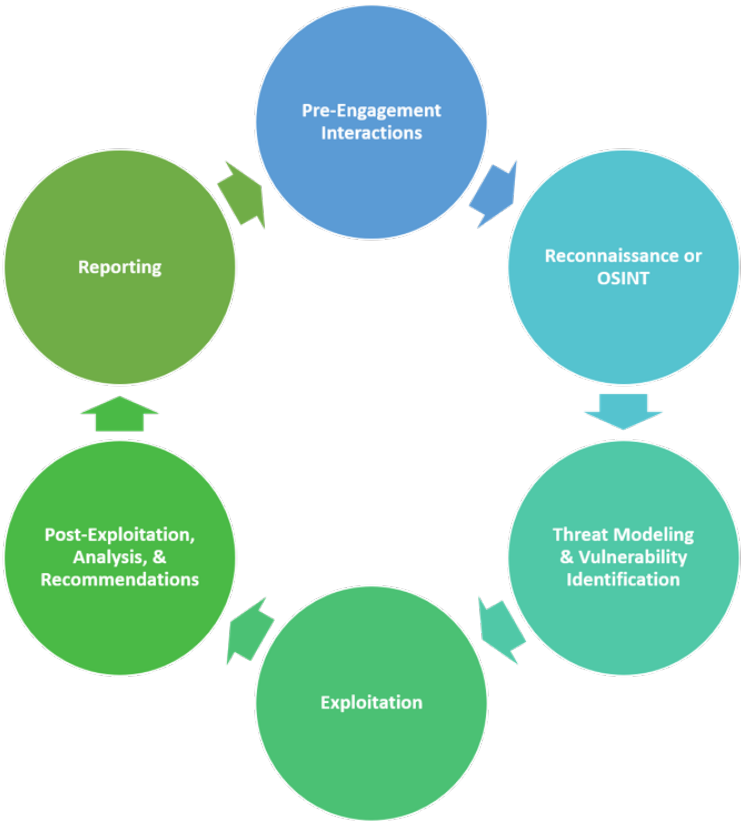


Diagram 1

3.2 Hardware / Software designing

Hardware Requirements:

- A computer with sufficient processing power and memory to run various tools for penetration testing.
- Stable internet connectivity to access the target domain and perform reconnaissance.

Software Requirements:

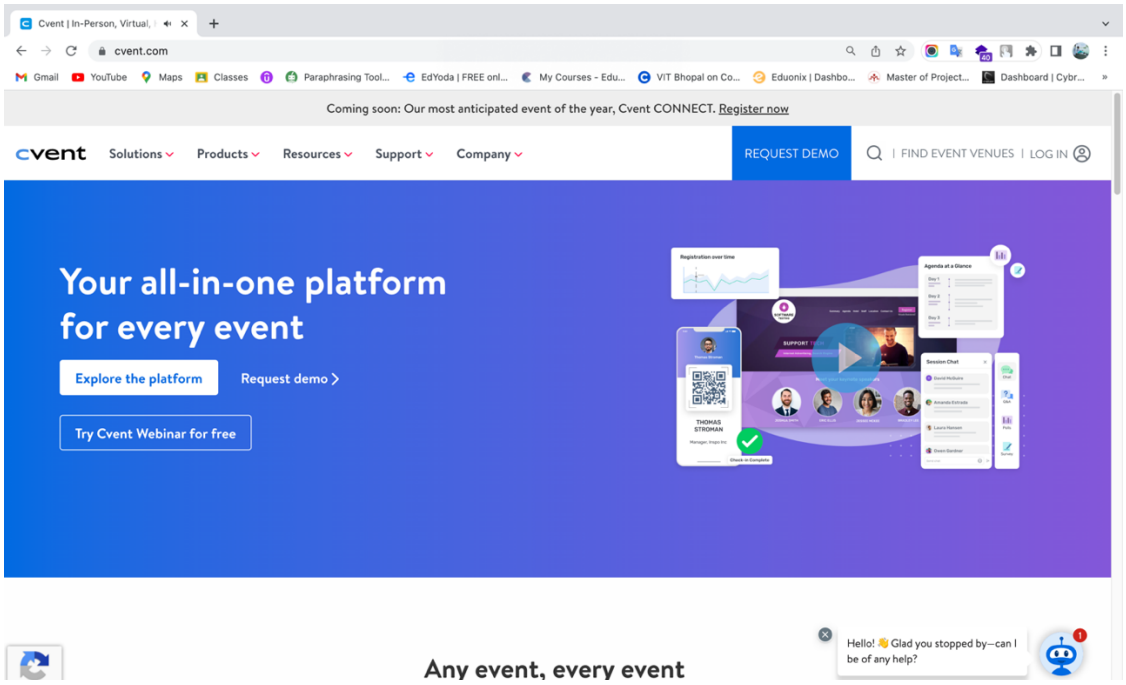
- Nmap: A powerful network scanning tool used for port scanning and vulnerability identification.
- Nessus: A comprehensive vulnerability scanning tool that can detect vulnerabilities in network services, web applications, and operating systems.
- Subfinder: A subdomain enumeration tool to discover all subdomains of the target.

- Httpx: A tool to filter out live subdomains from the obtained list.
- Scretfinder: A tool to discover sensitive data like API keys, access tokens, authorizations, etc., in JavaScript files.
- Dirb: A tool to enumerate directories and files on the target domain to discover hidden or sensitive information.

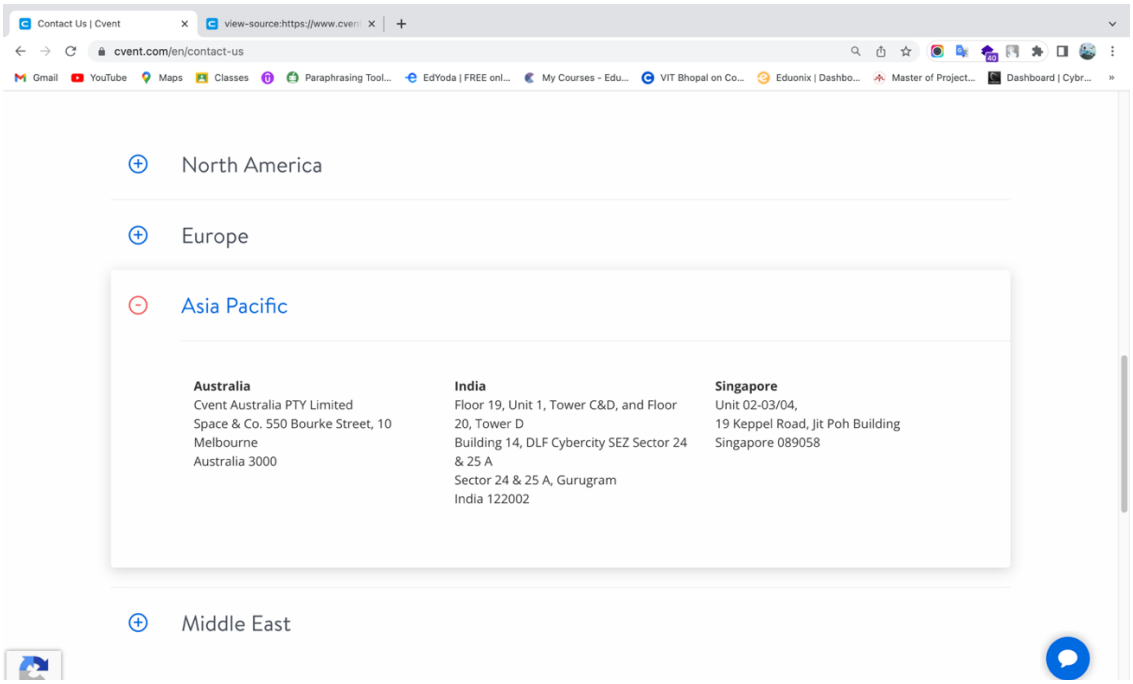
4 EXPERIMENTAL INVESTIGATIONS

4.1 Passive Footprinting or Reconnaissance:

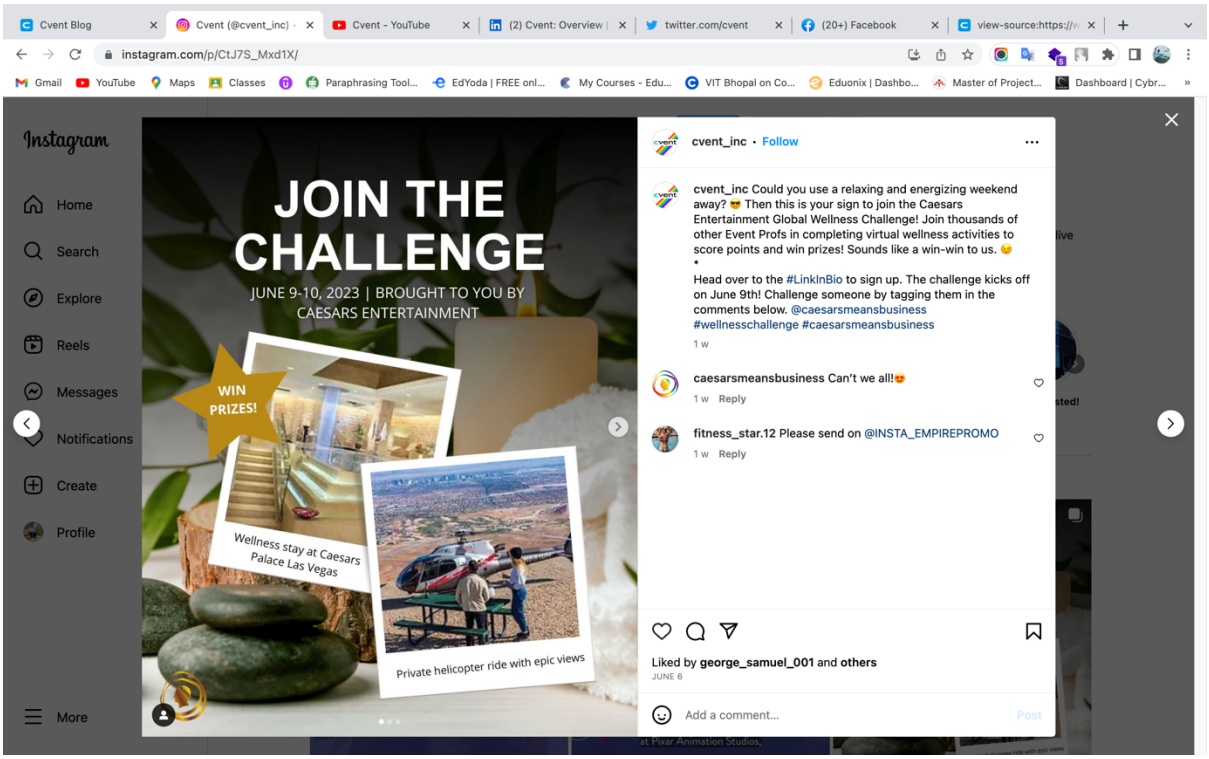
- Screenshot 1: cvent.com homepage, showing the layout and available information.
- Screenshot 2: Contact details found on the website, including the organization's address and phone number.
- Screenshot 3.1 & 3.2: Examining publicly shared content on social media platforms like Facebook, Twitter, LinkedIn, and Instagram to gather information about individuals, organizations, or events.
- Screenshot 4: WHOIS lookup results, revealing the domain registration details, such as the registrar and expiration date.
- Screenshot 5: (Dorking) Using advanced search operators and specific search queries on search engines like Google to identify information that is not typically indexed or easily accessible through regular searches.



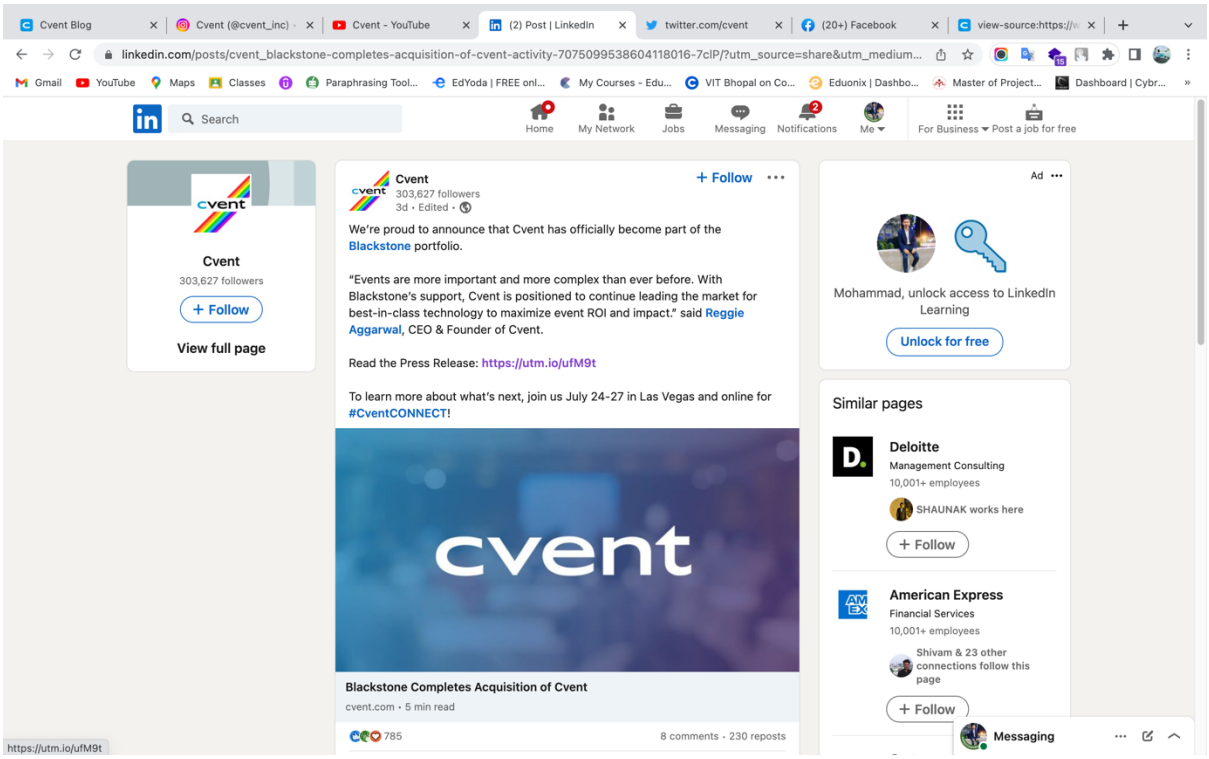
Screenshot 1



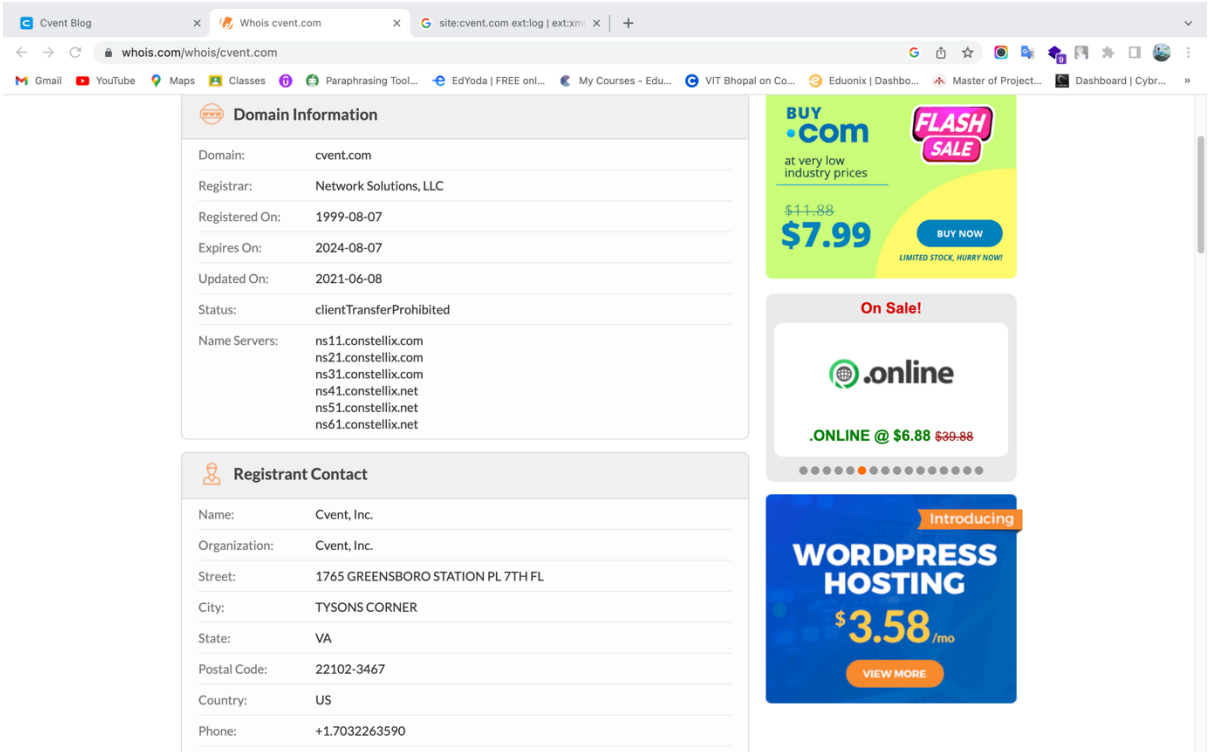
Screenshot 2



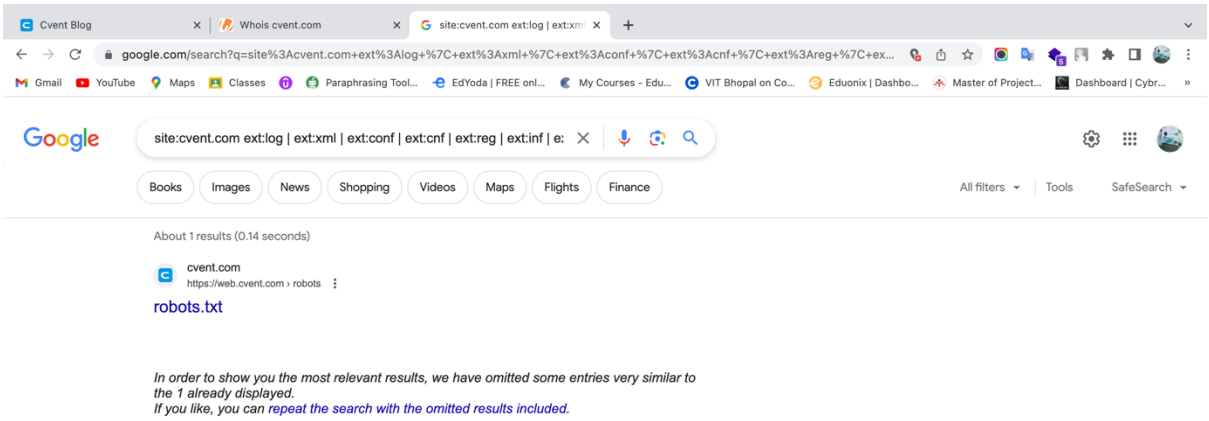
Screenshot 3.1



Screenshot 3.2



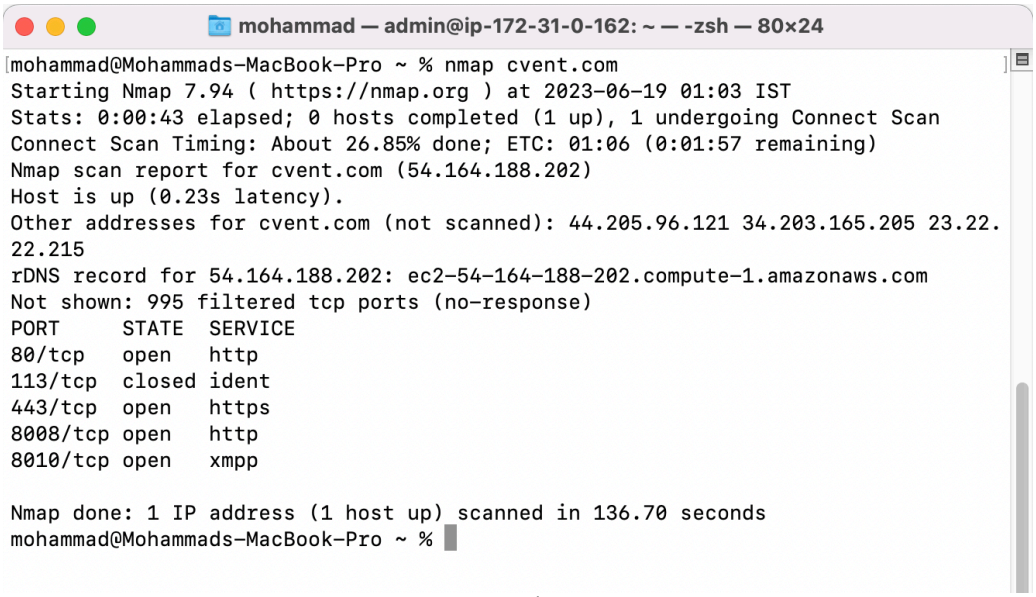
Screenshot 4



Screenshot 5

4.2 Active Footprinting or Reconnaissance:

- Screenshot 6: Nmap scan results showing open ports on cvent.com's IP address (54.164.188.202).
- Screenshot 7: (Subfinder) Subdomain enumeration to find out all subdomains of the target.
- Screenshot 8: (httpx) Filtering out live subdomains out of all subdomains.
- Screenshot 9.1 & 9.2: (Scretfinder) Discover sensitive data like apikeys, accesstoken, authorizations, jwt, …, etc in JavaScript files.
- Screenshot 9: (dirb) Enumerate directories and files on the target domain, aiming to discover hidden or sensitive information that may not be readily accessible through regular browsing.



Screenshot 6

```
mohammad@Mohammads-MacBook-Pro ~ % subfinder -d cvent.com

                __             __     __
   _____  __  / /_  / __(_)___  ____/ /__  _____
  / ___/ / / / __ \/ /_/ / __ \/ __  / _ \/ ___/
 (__  ) /_/ / /_/ / __/ / / / / /_/ /  __/ /
/____/\__,_/_.___/_/ /_/_/ /_/\__,_/\___/_/

                projectdiscovery.io

[INF] Loading provider config from /Users/mohammad/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for cvent.com
csc-x47.cvent.com
custom-eur.cvent.com
partners.cvent.com
origin-custom-ts20.cvent.com
cgc-x32.cvent.com
csc-x2.cvent.com
csc-x34.cvent.com
mx4.cvent.com
ccvpn.cvent.com
developer-portal-eur.cvent.com
ebs-ir-test.cvent.com
pdx01con001.cvent.com
csc-x41.cvent.com
csc-x25.cvent.com
csc-x16.cvent.com
csc-x37.cvent.com
csc-x5.cvent.com
csc-x48.cvent.com
dc-con-001.cvent.com
onsite.cvent.com
va01.cvent.com
csc-x12.cvent.com
mx2.cvent.com
csc-x8.cvent.com
socialwall.cvent.com
av.lync.cvent.com
is11-expresswaye-002.remotephone.cvent.com
app.cvent.com
cds1.cvent.com
origin-api-pr01.cvent.com
iad01con002.cvent.com
sedp-hq02.cvent.com
smtp2.cvent.com
api-platform-docs.cvent.com
attendeelogin-eur.cvent.com
isignatures.cvent.com
bartender2.cvent.com
cgc-x33.cvent.com
csc-x49.cvent.com
beta.cvent.com
```

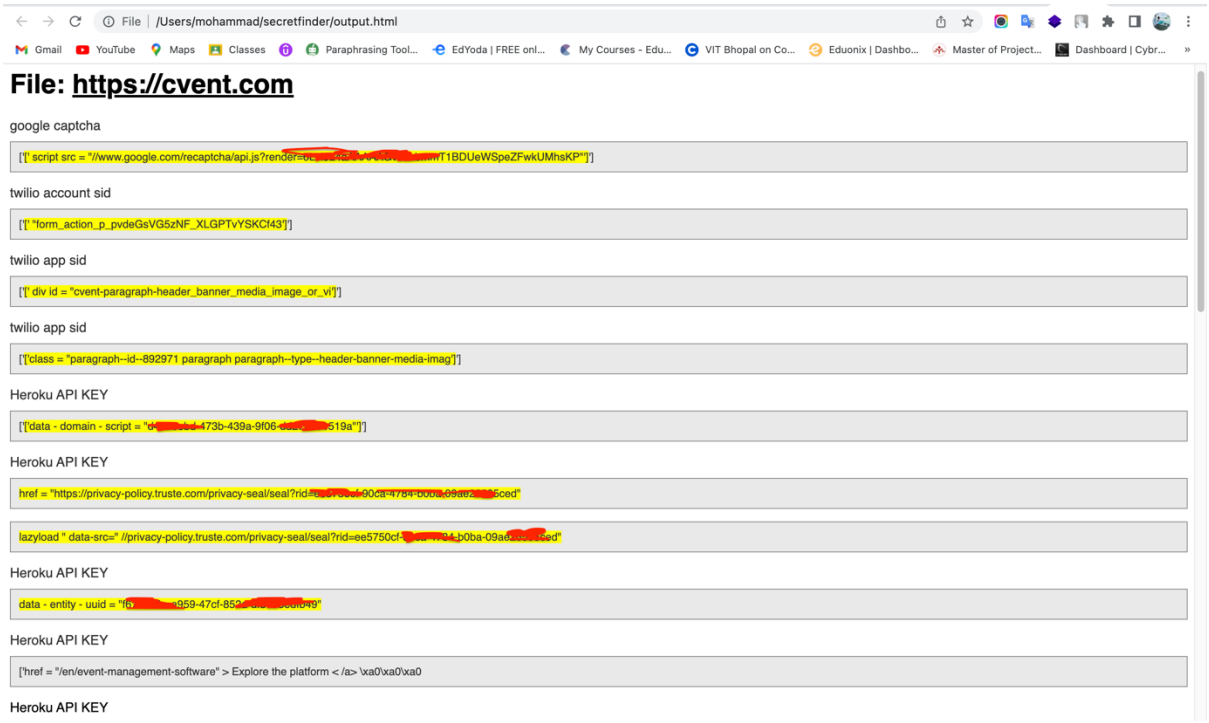
Screenshot 7

```
mohammad@Mohammads-MacBook-Pro ~ % cat cvent.txt | httpx

    __    __  __       _  __
   / /_  / /_/ /_____ | |/ /
  / __ \/ __/ __/ __ \|   /
 / / / / /_/ /_/ /_/ /   |
/_/ /_/\__/\__/ .___/_/|_|
             /_/             v1.2.5

                projectdiscovery.io

Use with caution. You are responsible for your actions.
Developers assume no liability and are not responsible for any misuse or damage.
http://autodiscover.cvent.com
https://badges.app-eur.cvent.com
https://attendee-hub-eur.cvent.com
https://attendee-login-sandbox.cvent.com
https://attendee-hub.cvent.com
https://attendeelogin-eur.cvent.com
https://astra-eu-west-1.elb.cvent.com
https://app-eur.cvent.com
https://badges.app.cvent.com
https://api-eur-dr.cvent.com
https://attendee-login.cvent.com
https://attendee-hub-sandbox.cvent.com
https://api-platform-docs.cvent.com
https://attendee-login-eur.cvent.com
https://advocates.cvent.com
https://bt-api-intg.cvent.com
https://api.cvent.com
https://bt-api.cvent.com
https://3d-pr50.cvent.com
https://badges.sandbox-app.cvent.com
https://app.cvent.com
https://api-staging.cvent.com
https://blog.cvent.com
https://3d.cvent.com
https://careers.cvent.com
https://connect-mumbai-2.cvent.com
https://community.cvent.com
https://connect-nvirginia.cvent.com
https://connect.cvent.com
https://connect-ohio.cvent.com
https://custom.cvent.com
https://developer-portal-staging.cvent.com
https://csn-chat-support.cvent.com
https://developer-portal-eur.cvent.com
https://developer-portal-sandbox.cvent.com
https://developer-portal.cvent.com
https://cventhelp.cvent.com
https://cvent.com
https://engineering.cvent.com
```

Screenshot 8

```
mohammad@Mohammads-MacBook-Pro secretfinder % python3 SecretFinder.py -i https://cvent.com
[ + ] URL: https://cvent.com
```

Screenshot 9.1



Screenshot 9.2

```
admin@ip-172-31-0-162:~$ dirb https://www.cvent.com

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Jun 18 20:30:09 2023
URL_BASE: https://www.cvent.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://www.cvent.com/ ----
+ https://www.cvent.com/403 (CODE:301|SIZE:51244)
+ https://www.cvent.com/404 (CODE:301|SIZE:51244)
+ https://www.cvent.com/500 (CODE:403|SIZE:143501)
==> DIRECTORY: https://www.cvent.com/a/
==> DIRECTORY: https://www.cvent.com/A/
+ https://www.cvent.com/abc (CODE:403|SIZE:143500)
+ https://www.cvent.com/abstract (CODE:301|SIZE:51344)
+ https://www.cvent.com/accessibility (CODE:301|SIZE:51284)
+ https://www.cvent.com/admin (CODE:403|SIZE:143500)
+ https://www.cvent.com/Admin (CODE:403|SIZE:143500)
+ https://www.cvent.com/ADMIN (CODE:403|SIZE:143500)
+ https://www.cvent.com/amazon (CODE:301|SIZE:51267)
+ https://www.cvent.com/api (CODE:200|SIZE:1554)
--> Testing: https://www.cvent.com/appliance
```

Screenshot 10

5 FLOWCHART

Below diagram is showing the control flow of the solution

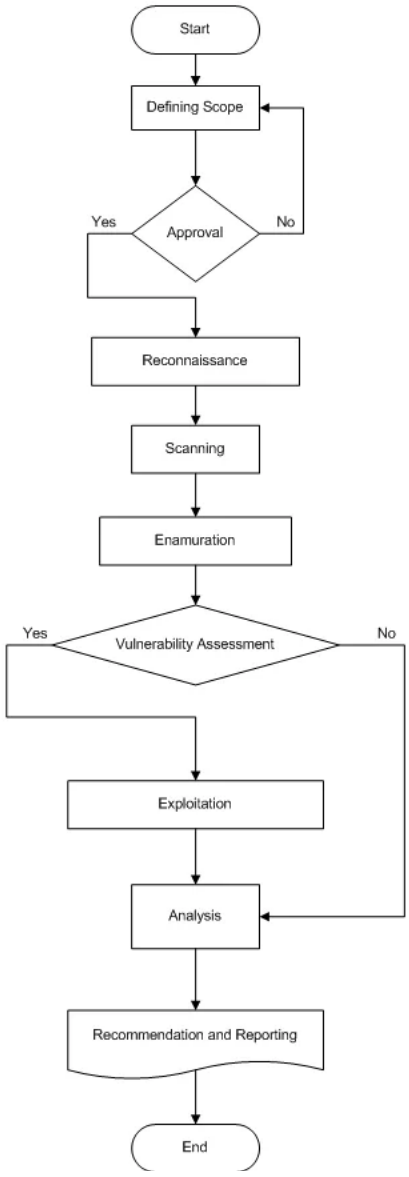


Diagram 2

6 RESULT

The findings from the web application penetration test are as follows:

6.1 Exploiting Vulnerabilities present on Open Ports

We have used **Nmap** to find open ports of our target web server.

Command Used to find open ports are:

a) Check for common open ports.
- **nmap <ip or domain>**

b) Check for all open ports.
- **nmap -p- <ip or domain>**

c) Check for specific port.
- **nmap -p <port_number> <ip or host>**

As we can see in Screenshot 6, I have run basic port scanning for common open ports.

Nmap found total 5 port which our target is using. Out of that four ports, one port i.e., port 113[ident] is closed and remaining 4 ports – 80[http], 443[https], 8008[http] and 8010[xmpp] is open.

As we know https and https is used for communication over a computer network. Whereas XMPP (Extensible Messaging and Presence Protocol) is an open XML technology for real-time communication.

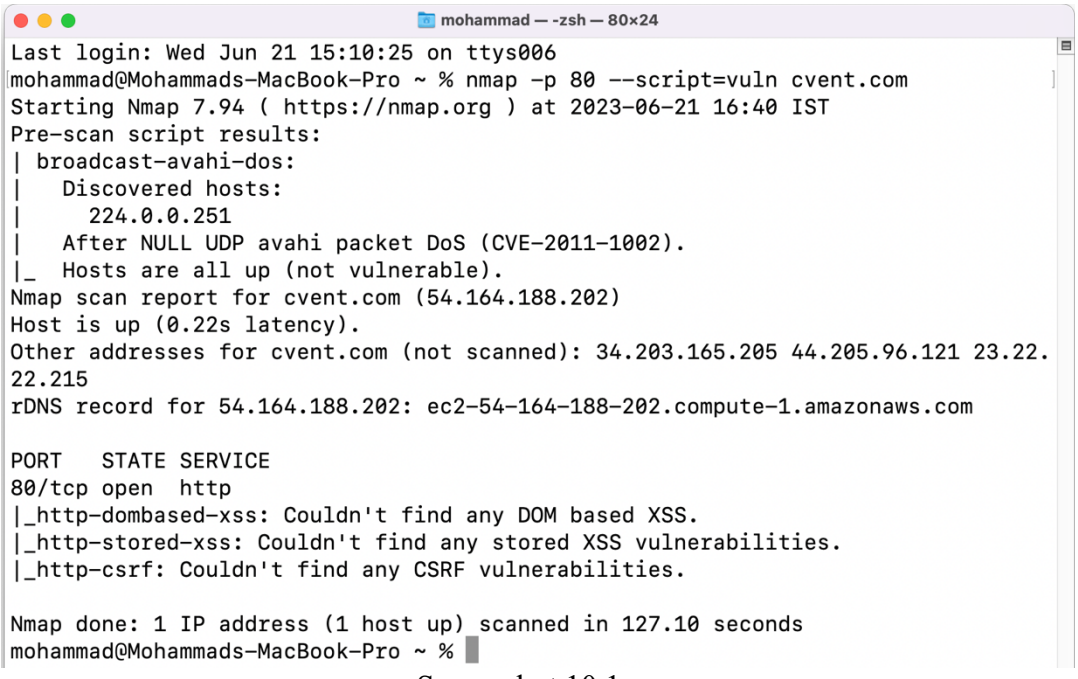
Nmap can be used for finding known vulnerabilities on open ports. So let's try to check for vulnerabilities on our target system's ports.

Command for checking vulnerabilities on any ports is:

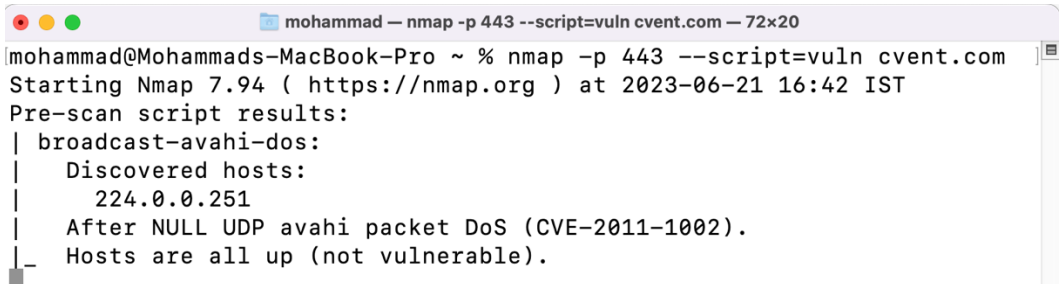
- **nmap -p <port_number> --script=vuln <ip or host>**

I have used Nmap for finding any vulnerabilities present in the open ports as show in Screenshot 10.1, 10.2, 10.3 and 10.4. As we can see, host is not vulnerable which means that Nmap has not found any vulnerability on that port.

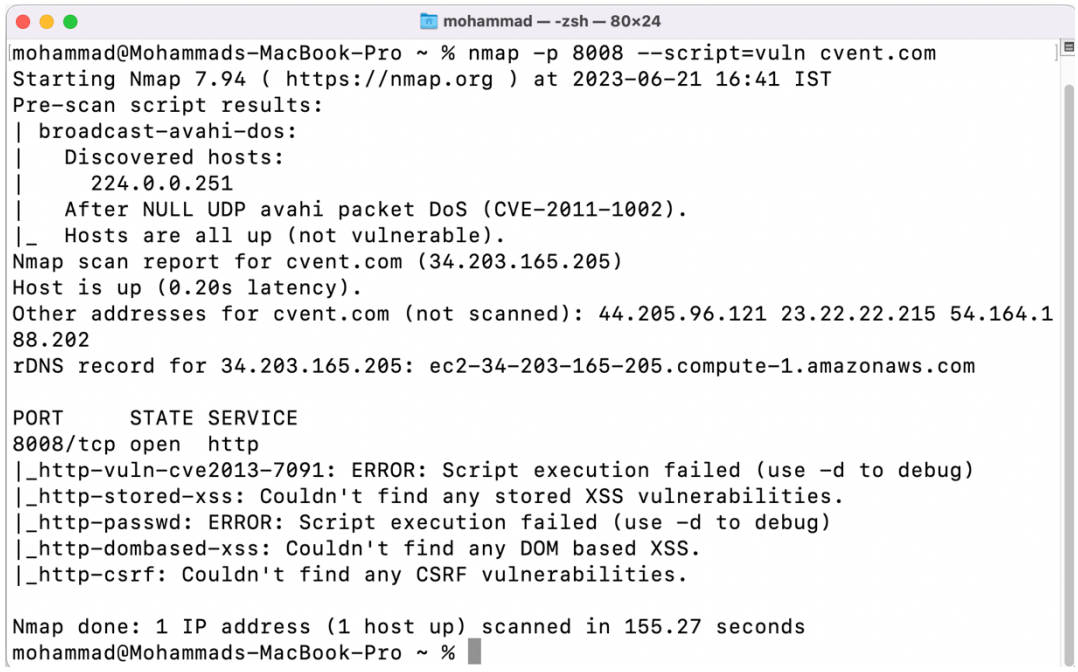
In case, if Nmap will found any vulnerability then, we will do some research for finding exploit of that vulnerability and test it to verify that identified vulnerability is true or false-positive.



Screenshot 10.1



Screenshot 10.2



Screenshot 10.3

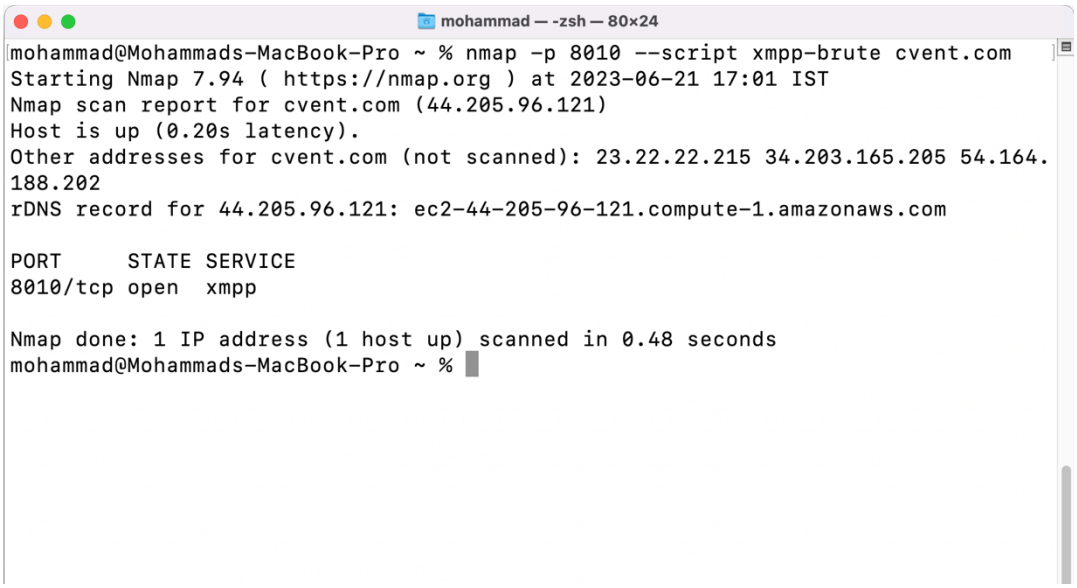
Screenshot 10.4

Now other than http and https, XMPP is only open port.
So let's search and find some exploit:

I have found an XMPP vulnerability. i.e., Perform brute force, password auditing against XMPP (Jabber) instant messaging servers.

- **nmap -p <port> --script xmpp-brute <ip or host>**

I have tried to exploit this vulnerability but it's not vulnerable. So attack is not performed as shown in Screenshot 11.



Screenshot 11

6.2 Nessus - Automated tool to find Vulnerabilities on Web Applications

We have used an automated tool Nessus for finding vulnerabilities and we have found four informational bugs which company should remediate for security best practices as shown in Screenshot 12.

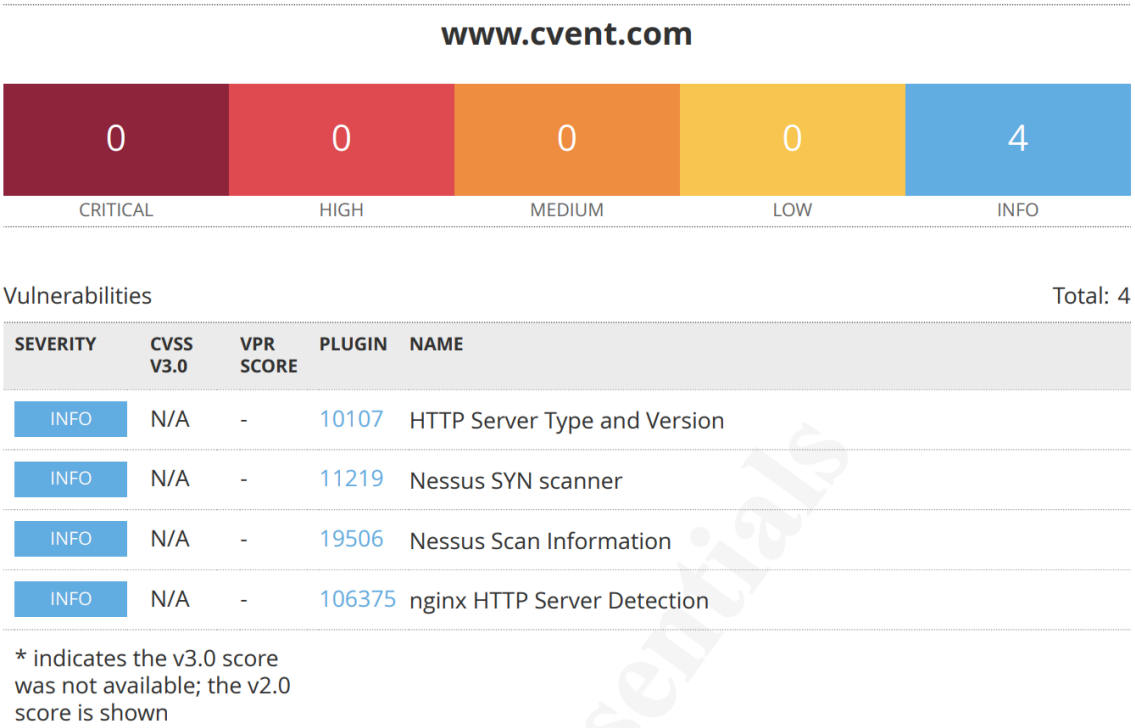
1. **HTTP Server Type and Version**
   Description:
   This plugin attempts to determine the type and the version of the remote web server.

2. **Nessus SYN scanner**
   Description:
   This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

3. **Nessus Scan Information**
   Description:
   This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

4. **nginx HTTP Server Detection**
   Description:
   Nessus was able to detect the nginx HTTP server by looking at the HTTP banner on the remote host.



www.cvent.com

0	0	0	0	4
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 4

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	106375	nginx HTTP Server Detection

* indicates the v3.0 score was not available; the v2.0 score is shown

Screenshot 12

7 ADVANTAGES & DISADVANTAGES

7.1 Advantages

- Identification of potential vulnerabilities and weaknesses in the web application.
- Proactive measures to enhance the application's security.
- Improved understanding of the target's infrastructure.

7.2 Disadvantages

- The process may take considerable time and resources.
- False positives may lead to unnecessary investigations.

8 APPLICATIONS

The proposed solution of conducting web application penetration testing can be applied to various domains, especially those with web applications that handle sensitive data or are prone to security threats. Industries such as e-commerce, banking, healthcare, and government sectors can benefit from regular penetration testing to strengthen their web application security.

9 CONCLUSION

The web application penetration test conducted on "cvent.com" helped in identifying potential vulnerabilities and weaknesses in the web application. The exploitation phase allowed for a thorough assessment of the impact of these vulnerabilities. The findings provide valuable insights for improving the security posture of the application and mitigating potential security risks.

10 FUTURE SCOPE

In the future, enhancements can be made to the web application penetration testing process by incorporating automated tools, advanced vulnerability scanning techniques, and comprehensive security assessments. Continuous monitoring and regular updates to security measures will be crucial to stay ahead of evolving security threats.

11 BIBILOGRAPHY

References:

1. https://nmap.org/nsedoc/scripts/xmpp-brute.html
2. https://github.com/v0re/dirb/tree/master
3. https://www.tenable.com/products/nessus/nessus-essentials
4. https://github.com/projectdiscovery/subfinder
5. https://github.com/m4ll0k/SecretFinder
6. https://www.whois.com/
7. https://github.com/projectdiscovery/httpx

APPENDIX

A. Tools:

- Dirb
- Nessus
- Subfinder
- SecretFinder
- Nmap
- Httpx