

JOHN-ALEX YANNOULIAS

W17751973

Word count (excluding references & questions) – **4999** (338 references, 803 questions)

Building your Scenario

Scenario: Online Car Rental Service

1. Type and size of business:

- My company was hired for a penetration test for a medium-sized car rental service with branches across the UK. Their web app lets customers search, compare prices, and reserve cars. The site stores personal information, but not financial data. Staff manages vehicle listings, availability, and receives inquiries by email. Staff credentials are in the database.

2. Type of data:

- Personal information: Name, email, phone, location of potential customers.
- Reservation data: Pick-up/drop-off dates, locations, preferences, special requests.
- Vehicle information: Make, model, year, color, features, availability, rental prices.
- Transaction data: Completed rentals records, customer info, vehicle details, duration. No full credit card details, but transaction records are stored.

3. Type of users :

- Customers: Registered users search, compare, reserve cars, manage contact info, view reservation history, and submit inquiries.
- Staff: Manages vehicle listings, availability, responds to inquiries, views reservations, adjusts availability, and communicates with customers via email.

Requirements and Deliverables

A- Information Gathering

(1) OSINT Activities

- TheHarvester

```
File Actions Edit View Help
[*] No IPs found.
[*] Emails found: 2
x22@cwscenarior.site
x30@cwscenarior.site
[*] No hosts found.

--(kali@kali)-[~]
$ theHarvester -d cwscenarior.site -b all

*****
*
* theHarvester 4.0.3
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****

[*] Target: cwscenarior.site

[*] Missing API key for zoomeye.
[*] Missing API key for Censys ID and/or Secret.
[*] Missing API key for Intelx.
[*] Missing API key for Hunter.
[*] Missing API key for Github.
[*] Missing API key for RocketReach.
[*] Missing API key for ProjectDiscovery.
[*] Missing API key for fullhunt.
[*] Missing API key for Spysse.
[*] Missing API key for Securitytrail.
[*] Missing API key for PentestTools.
[*] Missing API key for binaryedge.
An exception has occurred: 0, message='Attempt to decode JSON with unexpected mimetype: text/html; charset=utf-8', url=URL('https://api.threatminer.org/v2/domain.php?q=cwscenarior.site&rt=5')
[*] Searching Onys.
An exception has occurred: Cannot connect to host dns.bufferover.run:443 ssl:ssl.SSLContext object at 0x7f6ac54dac0 [Name or service not known]
[*] Searching Onys.
  Searching 100 results.
  Searching 100 results.
  Searching 200 results.
  Searching 200 results.
  Searching 300 results.
  Searching 300 results.
  Searching 400 results.
  Searching 400 results.
  Searching 500 results.
[*] Searching LinkedIn.
  Searching 500 results.
[*] Searching LinkedIn.
An exception has occurred: Cannot connect to host www.threatcrowd.org:443 ssl:True [SSLCertVerificationError: (1, "[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed: Hostname mismatch, certificate is not valid for 'www.threatcrowd.org'. (_ssl.c:997)")]
string indices must be integers
[*] Searching Threatcrowd.
  Searching results.
[*] Searching Censys.
[*] Searching Baidu.
[*] Searching Rapidms.
[*] Searching DuckDuckGo.
  Searching 0 results.
  Searching 100 results.
  Searching 0 results.
[*] Searching Trellix.
[*] Searching CxRisk.
Google is blocking your ip and the workaround, returning
  Searching 200 results.
[*] Searching Ambis.
  Searching 0 results.
[*] Searching Bing.
Google is blocking your ip and the workaround, returning
  Searching 300 results.
Google is blocking your ip and the workaround, returning
  Searching 400 results.
An exception has occurred: 0, message='Attempt to decode JSON with unexpected mimetype: text/html; charset=utf-8', url=URL('https://api.sublist3r.com/search.php?domain=cwscenarior.site')
[*] Searching Sublist3r.
Google is blocking your ip and the workaround, returning
  Searching 500 results.
[*] Searching Google.
[*] Searching Uriscan.
  Searching results.
[*] Searching VirusTotal.
An exception has occurred: 0, message='Attempt to decode JSON with unexpected mimetype: text/html', url=URL('https://api.n45ht.or.id/v1/subdomain-enumeration?domain=cwscenarior.site')
[*] Searching NmapTarget.
An exception has occurred: 0, message='Attempt to decode JSON with unexpected mimetype: text/html; charset=utf-8', url=URL('https://sonar.omnisint.io/all/cwscenarior.site?page=1')
[*] Searching Omnisint.

[*] ASNS found: 1
AS8560

[*] Interesting Urls found: 1
https://cwscenarior.site/

[*] No Twitter users found.

[*] LinkedIn Users found: 5
Your search

[*] LinkedIn Links found: 0
Your search

[*] No Trellio URLs found.
[*] IPs found: 3
50.87.192.155
217.160.0.219
2001:800:100f:f000::2b6

[*] No emails found.
[*] Hosts found: 10
autodiscover.cwscenarior.site:195.20.225.174
cpanel.cwscenarior.site
cpacendars.cwscenarior.site
cpcontacts.cwscenarior.site
mail.cwscenarior.site
webdisk.cwscenarior.site
webmail.cwscenarior.site
www.cwscenarior.site:217.160.0.219
```


SpiderFoot

[illegible][illegible]

Recon-Ng

```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali]~$ recon-ng  
[*] Version check disabled.  
  
Sponsored by ...  
www.blackhillsinfosec.com  
PRAXISEC  
www.practisec.com  
[recon-ng v5.1.2, Tim Tomes (@lanmaster53)]  
[*] No modules enabled/installed.  
[recon-ng][default] > marketplace install hackertarget  
[*] Module installed: recon/domains-hosts/hackertarget  
[*] Reloading modules ...  
[recon-ng][default] > modules load hackertarget  
[recon-ng][default][hackertarget] > options set source cwsценario.site  
SOURCE => cwsценario.site  
[recon-ng][default][hackertarget] > run  
  
CWSценARIO.SITE  
[*] Country: None  
[*] Host: cwsценario.site  
[*] Ip Address: 217.160.0.219  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*]  
  
SUMMARY  
[*] 1 total (1 new) hosts found.
```

Recon-ng further module investigation/exploration

```

[recon-ng v5.1.2, Tim Thomas (@lamnaster33)]

[9] Recon modules
[a] Reporting modules
[i] Import modules
[d] Disabled modules
[e] Exploitation modules
[c] Discovery modules

[recon-ng][default]> marketplace install all
Module installed: discovery/info_disclosure/cache_snoop
Module installed: discovery/info_disclosure/interesting_files
Module installed: exploitation/injection/command_injector
Module installed: exploitation/injection/spath_bruter
Module installed: import/icmp_file
Module installed: import/list
Module installed: import/macosx
Module installed: import/mmap
Module installed: recon/companies-contacts/bing_linkedln_cache
Module installed: recon/companies-contacts/censys_email_addresses
Module installed: recon/companies-contacts/censys_domains
Module installed: recon/companies-domains/censys_subdomains
Module installed: recon/companies-domains/censys_views_reverse_whois
Module installed: recon/companies-domains/whosy_dns
Module installed: recon/companies-hosts/censys_tls_subjects
Module installed: recon/companies-multi/github_miner
Module installed: recon/companies-multi/shodan_org
Module installed: recon/companies-multi/whois_miner
Module installed: recon/contacts-contacts/abc
Module installed: recon/contacts-contacts/mailtester
Module installed: recon/contacts-contacts/mangle
Module installed: recon/contacts-contacts/nomangle
Module installed: recon/contacts-credentials/hibp_breach
Module installed: recon/contacts-credentials/hibp_maste
Module installed: recon/contacts-domains/migrate_contacts
Module installed: recon/contacts-profiles/fullcontact
Module installed: recon/credentials-credentials/adobe
Module installed: recon/credentials-credentials/burpcrack
Module installed: recon/credentials-credentials/burpsuite
Module installed: recon/domains-companies/censys_companies
Module installed: recon/domains-companies/pen
Module installed: recon/domains-companies/whois_whois
Module installed: recon/domains-contacts/hunter.io
Module installed: recon/domains-contacts/metaspawler

[recon-ng][default]> modules load all
[recon-ng][default]> modules load companies-domains
[*] Multiple modules match "companies-domains".

Recon
-----
recon/companies-domains/censys_subdomains
recon/companies-domains/pen
recon/companies-domains/views_reverse_whois
recon/companies-domains/whosy_dns

[recon-ng][default]> modules load views_reverse_whois
[recon-ng][default][views_reverse_whois]> options set source cscenaria.site
SOURCE => cscenaria.site
[recon-ng][default][views_reverse_whois]> run

CSCENARIO.SITE
[recon-ng][default][views_reverse_whois]> run

CSCENARIO.SITE
[recon-ng][default][views_reverse_whois]> modules load pen
[*] Multiple modules match "pen".

Recon
-----
recon/companies-contacts/pen
recon/companies-domains/pen
recon/domains-companies/pen
recon/domains-contacts/pen

[recon-ng][default][views_reverse_whois]> run

CSCENARIO.SITE
[recon-ng][default][views_reverse_whois]> modules load list
[*] Multiple modules match "list".

Import
-----
import/list

Recon
-----
recon/domains-credentials/pwnedlist/api_usage
recon/domains-credentials/pwnedlist/domain_ispamed
recon/domains-credentials/pwnedlist/leak_lookup
recon/domains-credentials/pwnedlist/leaks_dump

Reporting
-----
reporting/list

[recon-ng][default][views_reverse_whois]> modules load txt
[recon-ng][default][views_reverse_whois]> modules load dns
[*] Multiple modules match "dns".

Recon
-----
recon/companies-domains/views_reverse_whois
recon/companies-domains/whosy_dns

[recon-ng][default][views_reverse_whois]> modules load whosy_dns
[recon-ng][default][whosy_dns]> run

CSCENARIO.SITE
[recon-ng][default][whosy_dns]> run

[recon-ng][default][whosy_dns]> options set source cscenaria.site
SOURCE => cscenaria.site
[recon-ng][default][whosy_dns]> run
[*] URL http://www.arin.net/rest/org/name=cscenaria.site
[*] No ORG found.
[*] URL http://www.arin.net/rest/customers/name=cscenaria.site
[*] No CUSTOMERS found.
[recon-ng][default][whosy_dns]> modules load whosy_dns
[recon-ng][default][whosy_dns]> options set source cscenaria.site
SOURCE => cscenaria.site
[recon-ng][default][whosy_dns]> run

CSCENARIO.SITE
[recon-ng][default][whosy_dns]> run

[recon-ng][default][whosy_dns]> options set source cscenaria.site
SOURCE => cscenaria.site
[recon-ng][default][whosy_dns]> run

```

Research and evaluate how OSINT can be effective and explain why it is one of the first activities that penetration testers carry out. [3 marks]

Open Source Intelligence (OSINT) is a crucial method for gathering data from public sources in the early stages of penetration testing. OSINT allows testers to collect target information without raising cybersecurity alarms, helping identify vulnerabilities and entry points for future hacking phases. Tools such as the Harvester, SpiderFoot, and Recon-ng streamline OSINT gathering. TheHarvester obtains data like email addresses and subdomains (Sudhanshu Chauhan and Nutan Kumar Panda, 2015), SpiderFoot automates data collection from various sources and Recon-ng organizes the gathered data systematically. These tools help penetration testers discover information about their target's infrastructure, network, and employees, exploitable in later test stages.

Scenario assessment: In your opinion, how dangerous are the information you were able to obtain for your allocated scenario [2 marks]

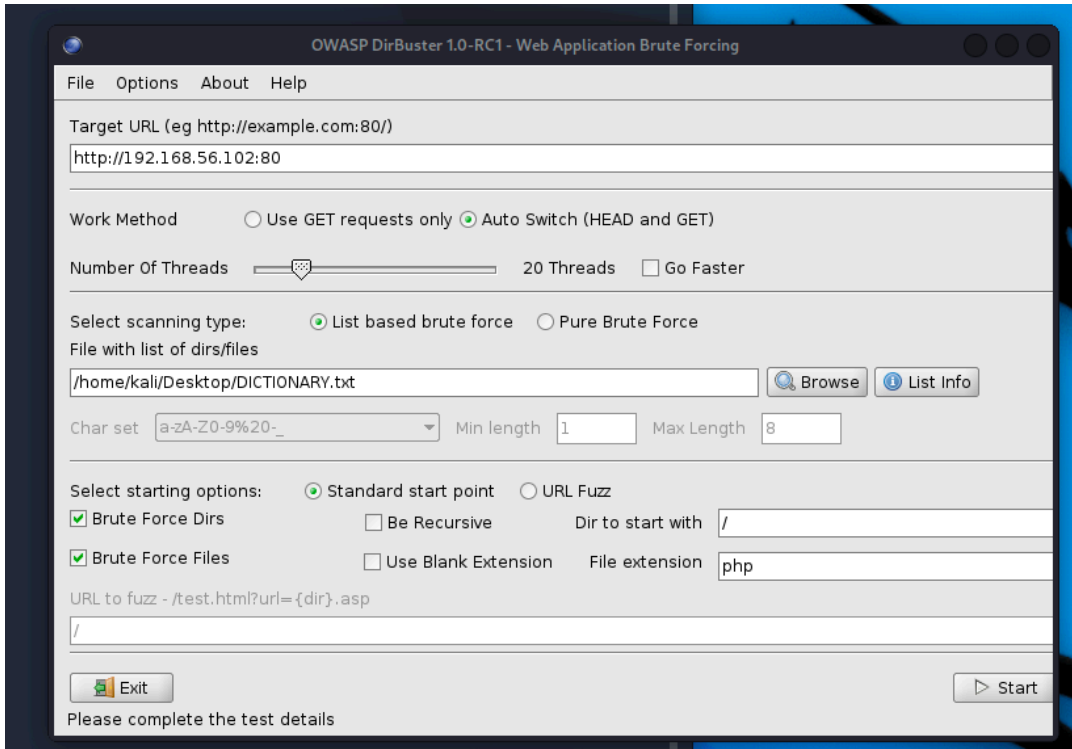
In the Online Car Rental Service scenario, each OSINT activity poses specific risks based on the information they collect:

1. TheHarvester: This tool retrieved staff and customer data, such as LinkedIn profiles, hosts, and IPs. While email addresses were inaccessible, limiting phishing risks, the hosts and IPs discovered could be exploited through Brute Force, DDoS, or DNS attacks.
2. SpiderFoot: Gathering a wide range of data, this tool provided domain and hosting information for cwscenario.site, including registration details, DNS records, Txt records, and associated IP addresses. Attackers could use this data to launch DDoS attacks or exploit misconfigurations.
3. Recon-ng: Collecting structured data, this tool helps attackers analyse and identify potential targets or entry points. Although limited in information from recon-ng methods(whois_miner and whoxy-dns), the identified subdomains and IP addresses can expose vulnerabilities, enabling network reconnaissance and targeted attacks.

(2) Reconnaissance

- DirBuster

~ DirBuster is a crawler and brute forcer; it follows all links in the pages it finds but also tries different names for possible files. By finding these unsecured directories, sensitive files or misconfigured resources, Dirbuster helps users assess a website's security and uncover potential vulnerabilities that could be exploited.



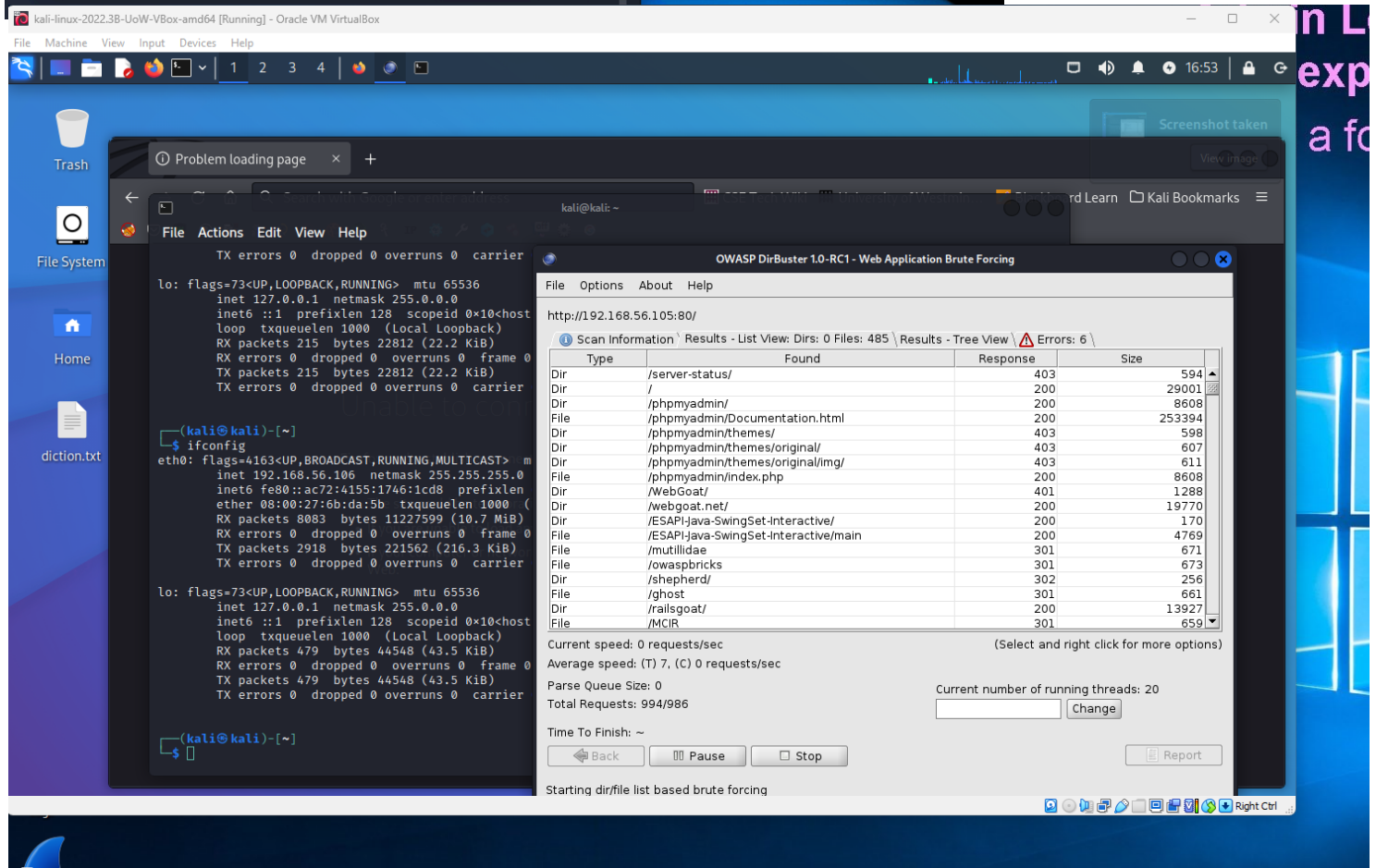
Test on

http://192.168.56.102:80/

Found 485: Files, 0: Directories.

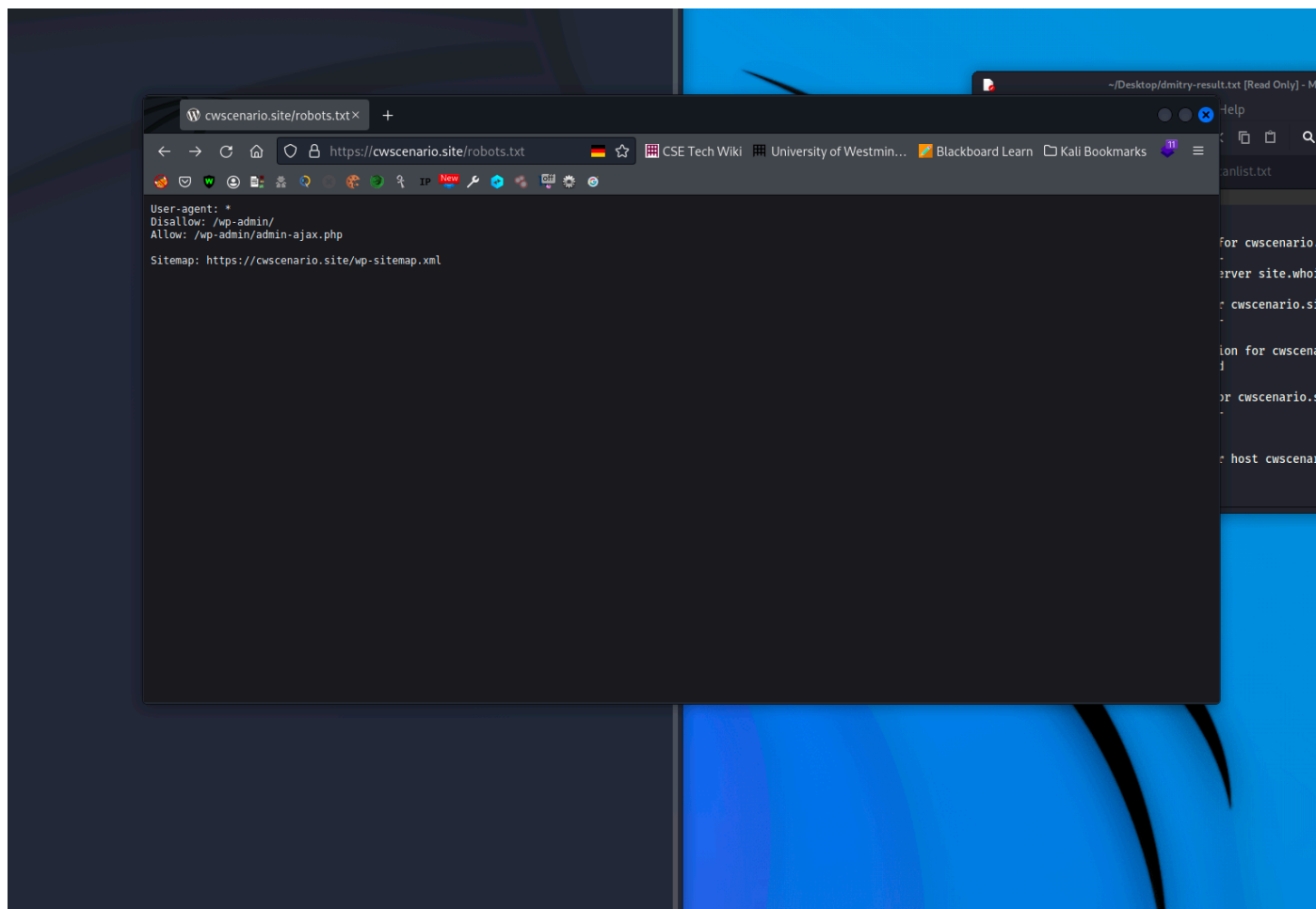
Some notable Findings:

- 1) /phpmyadmin/ with a 200 (OK) response, indicating presence of a phpMyAdmin instance.
- 2) /server-status/ with a 403 response (Forbidden), indicating restricted access



- Taking advantage of Robots.txt

~ Robots.txt guides search engines on indexing files and directories, but can also reveal hidden directories. This relies on "security through obscurity" and attackers can exploit it to access sensitive information or vulnerabilities.



XML Sitemap

This XML Sitemap is generated by WordPress to make your content more visible for search engines.

[Learn more about XML sitemaps.](#)

Number of URLs in this XML Sitemap: 4.

URL
https://cwsenario.site/wp-sitemap-posts-post-1.xml
https://cwsenario.site/wp-sitemap-posts-page-1.xml
https://cwsenario.site/wp-sitemap-taxonomies-category-1.xml
https://cwsenario.site/wp-sitemap-users-1.xml

Taking advantage of robot.txt file on cwsenario.site leading to discovery of /wp-sitemap.xml

- Web Enumeration

~ Enumeration collects network information, with DNS enumeration identifying DNS servers and entries to gather data such as usernames, computer names, and IP addresses, revealing insights into the organization's infrastructure.

```
(kali@kali)-[~]
$ dnsenum --enum cwsenario.site
dnsenum VERSION:1.2.6

----- cwsenario.site -----

Host's addresses:

cwsenario.site.                821      IN      A       217.160.0.219

Name Servers:

ns1093.ui-dns.com.             834      IN      A       217.160.82.93
ns1032.ui-dns.de.              990      IN      A       217.160.80.32
ns1108.ui-dns.org.             842      IN      A       217.160.83.108
ns1115.ui-dns.biz.             956      IN      A       217.160.81.115

Mail (MX) Servers:

mx00.ionos.co.uk.              896      IN      A       212.227.15.41
mx01.ionos.co.uk.              852      IN      A       217.72.192.67

Trying Zone Transfers and getting Bind Versions:

Trying Zone Transfer for cwsenario.site on ns1093.ui-dns.com ...
AXFR record query failed: NOTAUTH

Trying Zone Transfer for cwsenario.site on ns1032.ui-dns.de ...
AXFR record query failed: NOTAUTH

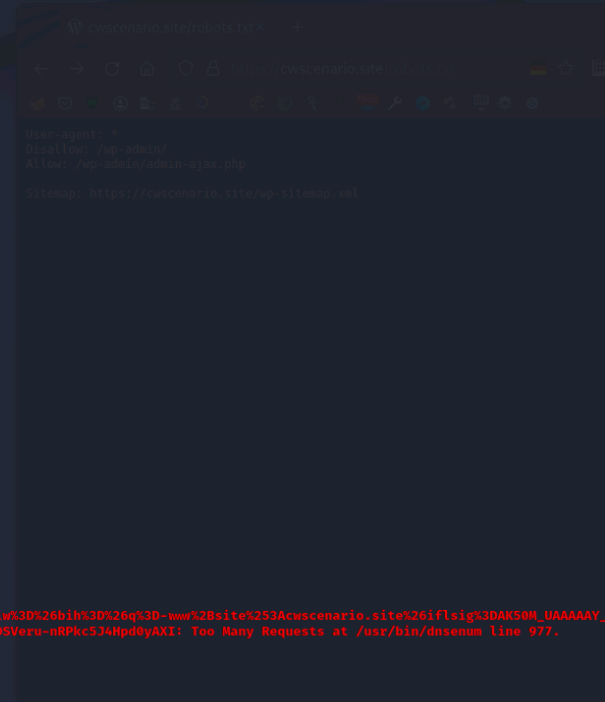
Trying Zone Transfer for cwsenario.site on ns1108.ui-dns.org ...
AXFR record query failed: NOTAUTH

Trying Zone Transfer for cwsenario.site on ns1115.ui-dns.biz ...
AXFR record query failed: NOTAUTH

Scraping cwsenario.site subdomains from Google:

Error GETing http://www.google.com/sorry/index?continue=http://www.google.com/search%3Fhl%3Den-GB%26source%3Dhp%26bih%3D%26bih%3D%26q%3D-www%2Bsite%253Acwsenario.site%26iflsig%3DAK50M_UAAAAAY_vuBeuVuvveFknzQN5N90cIZ87Kex3z%26gbv%3D18hl=en-GB&q=EgrRhfhYGKjDyJ8GIjCkzqyo5Yza9sbikGJL3IRlweHjg-cJjgppD9SeKLpww0XtdSVeru-nRPkc5J4Hpd0yAXI: Too Many Requests at /usr/bin/dnsenum line 977.

(kali@kali)-[~]
$
```



Web Enumeration performed on cwsenario.site

Revealing info such as :

- Host addresses
- Name Servers
- MX (mail) Servers

Scenario assessment: Explain how the information obtained by testing the web applications can be used at a later stage to exploit company's web services? Give an example of information that can be relevant to your scenario. [3 marks]

Testing web applications can reveal information to exploit a company's web services. In this scenario, web-enumeration, robots.txt, and DirBuster results exposed valuable data.

DNS enumeration provided IP addresses, name servers, and mail servers, potentially exposing network infrastructure and mail service vulnerabilities. Revealed MX-servers (mx00.ionos.co.uk and mx01.ionos.co.uk) could be exploited through email phishing attacks targeting staff, potentially gaining unauthorized access to car-rental systems and exploiting stored customer/reservation data. The robots.txt file disclosed the hidden /wp-sitemap directory, possibly leading to sensitive data exposure or exploitable elements.

DirBuster revealed phpMyAdmin, WebGoat and ESAPI-java-SwingSet-Interactive. Unauthorized access to phpMyAdmin could compromise the database, exposing staff credentials and customer information. WebGoat and ESAPI-java-SwingSet-Interactive are known vulnerable applications, which attackers might exploit.

The car rental service's web application stores personal and reservation data, which could be exploited to access customer information, manipulate vehicle availability, or intercept sensitive staff-customer email communications. By exploiting identified vulnerabilities, attackers could disrupt operations, compromise user data, and damage the company's reputation.

(3) Port Scanning and Enumeration

```
kali@kali:~$ nmap -sn 192.168.56.102
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-19 07:14 EST
Nmap scan report for 192.168.56.102
Host is up (0.0020s latency).
Nmap done: 1 IP address (1 host up) scanned in 13.07 seconds

kali@kali:~$ nmap 192.168.56.102
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-19 07:27 EST
Nmap scan report for 192.168.56.102
Host is up (0.000092s latency).
All 1000 scanned ports on 192.168.56.102 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)
Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds

kali@kali:~$ sudo nmap -sV -O 192.168.56.102
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-19 07:28 EST
Nmap scan report for 192.168.56.102
Host is up (0.000025s latency).
All 1000 scanned ports on 192.168.56.102 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.77 seconds

kali@kali:~$ man nmap

kali@kali:~$ nmap -sP 192.168.56.102
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-19 07:30 EST
Nmap scan report for 192.168.56.102
Host is up (0.000079s latency).
Nmap done: 1 IP address (1 host up) scanned in 13.03 seconds

kali@kali:~$ NMAP -Sp 192.168.56.*
NMAP: command not found

kali@kali:~$ nmap -sP 192.168.56.*
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-19 07:30 EST
Nmap scan report for 192.168.56.1
Host is up (0.0078s latency).
Nmap scan report for 192.168.56.2
Host is up (0.0059s latency).
Nmap scan report for 192.168.56.102
Host is up (0.000052s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 15.66 seconds

kali@kali:~$ nmap 192.168.56.102
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-19 07:31 EST
Nmap scan report for 192.168.56.102
Host is up (0.00015s latency).
All 1000 scanned ports on 192.168.56.102 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)
Nmap done: 1 IP address (1 host up) scanned in 13.09 seconds

kali@kali:~$ nmap -p 1-10000 192.168.56.102
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-19 07:33 EST
Nmap scan report for 192.168.56.102
Host is up (0.000091s latency).
All 10000 scanned ports on 192.168.56.102 are in ignored states.
Not shown: 10000 closed tcp ports (conn-refused)
Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds

kali@kali:~$ nmap -p 22 192.168.56.102
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-19 07:34 EST
Nmap scan report for 192.168.56.102
Host is up (0.00011s latency).

PORT      STATE SERVICE
22/tcp    closed ssh

Nmap done: 1 IP address (1 host up) scanned in 13.08 seconds

kali@kali:~$ nmap -p 22 192.168.56.* -oG ~/Desktop/myresults.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-19 07:35 EST
Nmap scan report for 192.168.56.1
Host is up (0.00096s latency).

PORT      STATE SERVICE
22/tcp    closed ssh

Nmap scan report for 192.168.56.2
Host is up (0.0013s latency).

PORT      STATE SERVICE
22/tcp    open  ssh

Nmap scan report for 192.168.56.102
Host is up (0.00032s latency).

PORT      STATE SERVICE
22/tcp    closed ssh

Nmap done: 256 IP addresses (3 hosts up) scanned in 15.62 seconds

kali@kali:~$ nmap -O 192.168.56.102
TCP/IP fingerprinting (for OS scan) requires root privileges.
QUITTING!

kali@kali:~$ sudo nmap -O 192.168.56.102
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-19 07:37 EST
Nmap scan report for 192.168.56.102
Host is up (0.000026s latency).
All 1000 scanned ports on 192.168.56.102 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.98 seconds

kali@kali:~$ nmap -sV 192.168.56.102
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-19 07:37 EST
Nmap scan report for 192.168.56.102
Host is up (0.00013s latency).
All 1000 scanned ports on 192.168.56.102 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.49 seconds

kali@kali:~$ sudo nmap -sS 192.168.56.102 -D 10.0.0.1,10.0.0.2,10.0.0.4
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-19 07:38 EST
Nmap scan report for 192.168.56.102
Host is up (0.0000090s latency).
All 1000 scanned ports on 192.168.56.102 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 13.15 seconds
```

First 3 commands – scanning/identifying services with nmap

First 2 commands – identifying active machines

Next 4 commands – Finding Open Ports.

Next 2 commands – Fingerprinting for Operating Systems.

Next 1 command – Fingerprinting for Services.

Next 1 command – Spoofing & Decoy Scan.

```
~/Desktop/myresults.txt - Mousepad
File Edit Search View Document Help

1 # Nmap 7.92 scan initiated Sun Feb 19 07:35:32 2023 as: nmap -p 22 -oG /
home/kali/Desktop/myresults.txt 192.168.56.*
2 Host: 192.168.56.1 () Status: Up
3 Host: 192.168.56.1 () Ports: 22/closed/tcp//ssh///
4 Host: 192.168.56.2 () Status: Up
5 Host: 192.168.56.2 () Ports: 22/open/tcp//ssh///
6 Host: 192.168.56.102 () Status: Up
7 Host: 192.168.56.102 () Ports: 22/closed/tcp//ssh///
8 # Nmap done at Sun Feb 19 07:35:48 2023 -- 256 IP addresses (3 hosts up)
scanned in 15.62 seconds
9
```

(Finding Open Ports – result)

Next 2 commands – UDP Scan.

Next 6 commands – List of Targets.

Next 1 command – Detecting WAF.

Next 2 commands – Fingerprinting WAF.

Next 1 command – Detecting WAF on server with firewall.

Determining Network Range – “Dmitry” tool

```
Nmap done: 1 IP address (1 host up) scanned in 13.49 seconds

(kali@kali)-[~]
└─$ sudo nmap -sS 192.168.56.102 -D 10.0.0.1,10.0.0.2,10.0.0.4
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-19 07:38 EST
Nmap scan report for 192.168.56.102
Host is up (0.0000090s latency).
All 1000 scanned ports on 192.168.56.102 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 13.15 seconds

(kali@kali)-[~]
└─$ sudo nmap -sU 192.168.56.102
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-19 07:40 EST
Nmap scan report for 192.168.56.102
Host is up (0.0000050s latency).
All 1000 scanned ports on 192.168.56.102 are in ignored states.
Not shown: 1000 closed udp ports (port-unreach)

Nmap done: 1 IP address (1 host up) scanned in 13.17 seconds

(kali@kali)-[~]
└─$ sudo nmap -sU --reason 192.168.56.102
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-19 07:41 EST
Nmap scan report for 192.168.56.102
Host is up, received localhost-response (0.0000040s latency).
All 1000 scanned ports on 192.168.56.102 are in ignored states.
Not shown: 1000 closed udp ports (port-unreach)

Nmap done: 1 IP address (1 host up) scanned in 13.16 seconds

(kali@kali)-[~]
└─$ mousepad scanlist.txt

(kali@kali)-[~]
└─$ nmap -il scanlist.txt
Failed to open input file scanlist.txt for reading: No such file or directory (2)

(kali@kali)-[~]
└─$ nmap -iL scanlist.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-19 07:43 EST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.07 seconds

(kali@kali)-[~]
└─$ sudo apt-get install hping3
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
hping3 is already the newest version (3.a2.ds2-10).
hping3 set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 20 not upgraded.

(kali@kali)-[~]
└─$ hping3 --traceroute -V -i cwsenario.site
Unable to resolve 'cwsenario.site'

(kali@kali)-[~]
└─$ hping3 --traceroute -V -l cwsenario.site
hping3: invalid option -- l
Try hping3 --help

(kali@kali)-[~]
└─$ nmap -p 80,443 --script-http-waf-detect 192.168.56.102
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-19 07:47 EST
Nmap scan report for 192.168.56.102
Host is up (0.000077s latency).

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

Nmap done: 1 IP address (1 host up) scanned in 13.42 seconds

(kali@kali)-[~]
└─$ nmap -p 80,443 --script-http-waf-fingerprint www.cwsenario.site
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-19 07:48 EST
Failed to resolve 'www.cwsenario.site'.
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.36 seconds

(kali@kali)-[~]
└─$ nmap -p 80,443 --script-http-waf-fingerprint www.cwsenario.site
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-19 07:49 EST
Nmap scan report for www.cwsenario.site (217.160.0.219)
Host is up (0.026s latency).
Other addresses for www.cwsenario.site (not scanned): 2001:8d8:100f:f000::2b6
rDNS record for 217.160.0.219: 217-160-0-219.elastic-ssl.ui-r.com

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

Nmap done: 1 IP address (1 host up) scanned in 0.75 seconds

(kali@kali)-[~]
└─$ nmap -p 80,443 --script-http-waf-detect www.cwsenario.site
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-19 07:50 EST
Nmap scan report for www.cwsenario.site (217.160.0.219)
Host is up (0.027s latency).
Other addresses for www.cwsenario.site (not scanned): 2001:8d8:100f:f000::2b6
rDNS record for 217.160.0.219: 217-160-0-219.elastic-ssl.ui-r.com

PORT      STATE SERVICE
80/tcp    open  http
| http-waf-detect: IDS/IPS/WAF detected:
|_ www.cwsenario.site:80/?p4yl04d3=<script>alert(document.cookie)</script>
443/tcp   open  https
| http-waf-detect: IDS/IPS/WAF detected:
|_ www.cwsenario.site:443/?p4yl04d3=<script>alert(document.cookie)</script>

Nmap done: 1 IP address (1 host up) scanned in 0.98 seconds
```

```
-Desktop/dmitry-result.txt [Read Only] - Mouse

File Edit Search View Document Help

myresults.txt x scanlist.txt x dmitry-result.txt x

1 HostIP:217.160.0.219
2 HostName:cwsenario.site
3
4 Gathered Inic-whois information for cwsenario.site
5
6 ERROR: Connection to InicWhois Server site.whois-servers.net failed
7
8 Gathered Netcraft information for cwsenario.site
9
10
11 Retrieving Netcraft.com information for cwsenario.site
12 Netcraft.com Information gathered
13
14 Gathered Subdomain information for cwsenario.site
15
16 Searching Google.com:80...
17 Searching Altavista.com:80...
18 Found 0 possible subdomain(s) for host cwsenario.site, Searched 0 pages
   containing 0 results
19
```

Discussion of findings:

The Nmap scan results for the target IP 192.168.56.102 show that all 1000 scanned ports are in ignored states, indicating no open ports were found. It suggests that the host may have a strict firewall in place or no active services running.

For the website cwscenario.site, two ports were identified: port 80 (HTTP) and port 443 (HTTPS). Both ports were open, and when running the http-waf-detect script, it was found that an IDS/IPS/WAF was detected on both ports. This indicates that the website is likely protected by a Web Application Firewall (WAF) or an Intrusion Detection/Prevention System (IDS/IPS), which may complicate further exploitation attempts.

Research and explain what an open port means and identify threats an open port can potentially causes? [3 marks]

An open port is a network communication channel on a device, allowing data exchange for applications. They are associated with specific protocols (TCP or UDP) and numbered for efficient data routing. Open ports enable network services to accept connections from remote systems for functions like web, email, or file sharing services (Kizza, 2013).

Open ports can pose security threats like unauthorized access, denial of service (DoS) attacks and also malware infection. Cybercriminals/hackers can exploit open ports to gain unauthorized access, launch attacks and/or steal sensitive data (Kizza, 2013). Implementing proper security measures, like firewalls, intrusion detection systems, and regular vulnerability assessments, can help minimize these risks. Regularly reviewing and closing unnecessary open ports can also reduce the attack surface.

Scenario assessment: Explain the threats of the open ports you have identified when carrying the port scanning and how dangerous they are for your scenario and the data your scenario company holds. [3 marks]

Open ports for cwscenario.site (port 80:HTTP, port 443:HTTPS) present potential threats to the Online Car Rental Service. These ports enable communication between the web app and its users, including customers and staff. However, a detected IDS/IPS/WAF on both ports lessens the risk of exploitation.

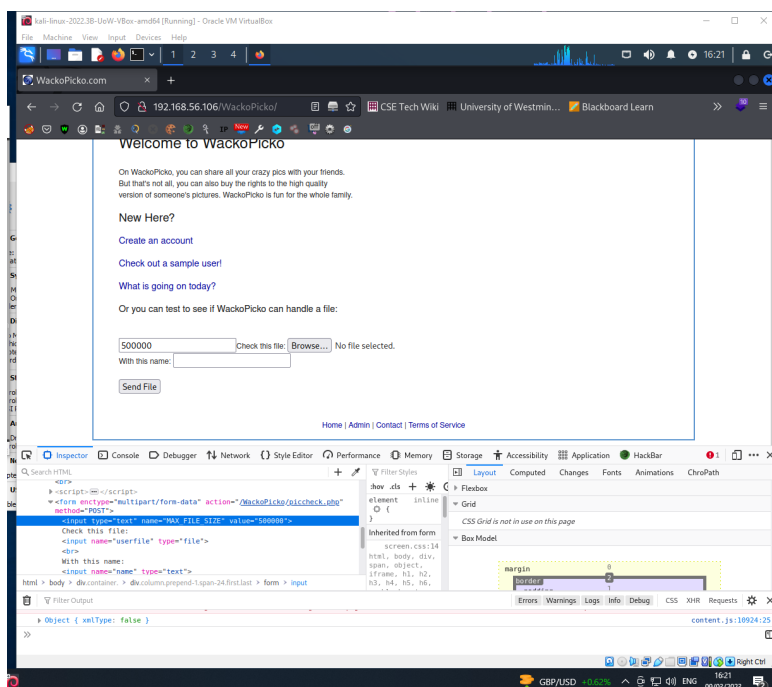
Threats may include DoS attacks, unauthorized access, or data interception. Sensitive customer data, such as personal information, reservation details, and transaction records, could be exposed through unauthorized web app access. Identity theft or fraud might result, harming the business's reputation and customer trust. Cybercriminals could access sensitive data by intercepting port 80 communication, revealing unencrypted information.

Compromise of staff credentials in the database could lead to unauthorized access to vehicle listings and availability management, disrupting platform operations and causing financial losses.

Despite a WAF or IDS/IPS, regular vulnerability assessments and strict security measures like encryption, access control, and strong authentication are vital for mitigating these threats.

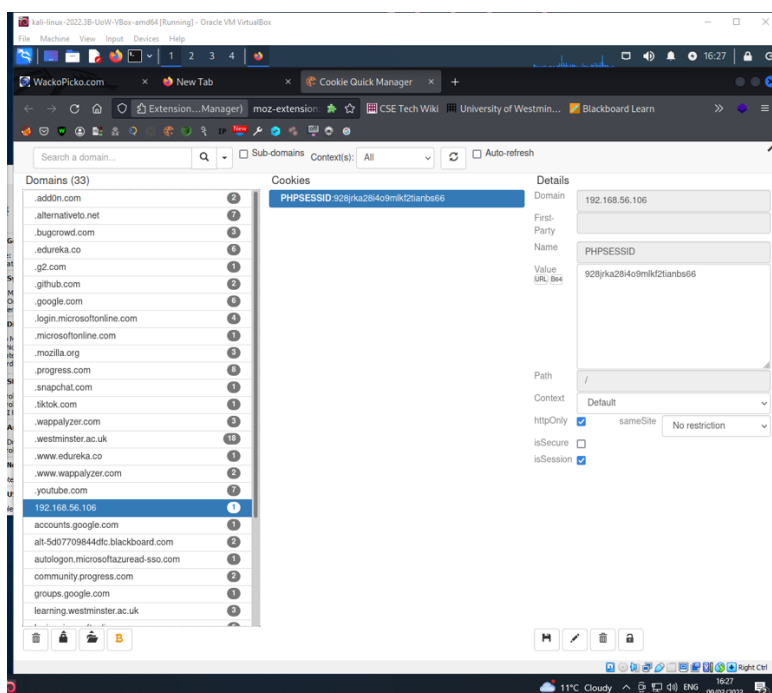
B- Server-Side Exploits

1) Data Tampering



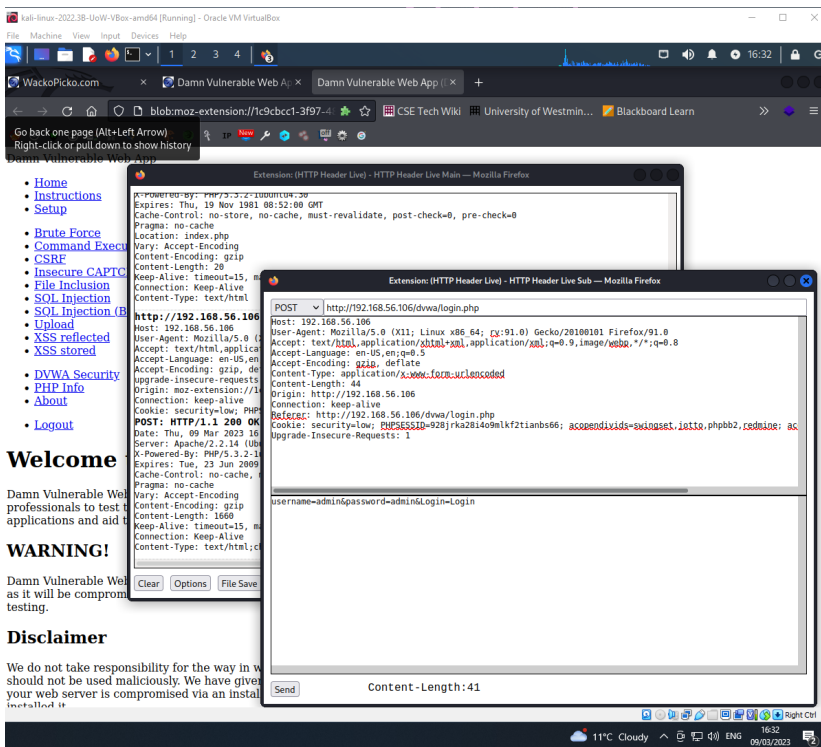
Using browsers developer tools to analyse & alter the basic behaviour:

- changed file size limit to 50000 from 3000 and added form field to change it.
- Web application **VULNERABLE**
- Browser-based alterations: Enables manipulation of web page interpretation.
- Reloaded pages: Temporarily overrides client-side modifications.
- Developer Tools: Exploits client-side restrictions, exposing vulnerabilities



Obtaining/modifying cookies

- Changed httpOnly parameter to yes.
- Web application **VULNERABLE**
- HttpOnly modification: Enables execution of malicious code via server compliance.
- Cookie manipulation: Injection of malicious patterns to alter behaviour or gain privileges.
- Session cookies: Vulnerable to impersonation through value replacement.



Using Tamper Data add-on to intercept and modify requests

Web application **VULNERABLE**

Tamper Data add-on: Intercepted

POST requests, modified test/password to admin/admin.

Bypassed client-side validation: Altered hidden forms and POST parameters.

Gained unauthorized access: Logged in with manipulated credentials, exposing web application vulnerability.

Briefly research and explain data tampering vulnerability. Which Cyber Security tenet this vulnerability violates? [2 marks].

Data tampering is a cybersecurity vulnerability where unauthorized individuals alter or manipulate digital data, including modifying database contents, changing network communications, or manipulating user input to gain unauthorized access or privileges (MBA Knowledge Base, 2014). Data tampering can lead to unauthorized access, compromised data integrity, or fraudulent activities. Attackers can exploit this vulnerability through various techniques such as developer tools exploiting, parameter tampering, or cookie manipulation.

Data tampering violates the **integrity** tenet of the CIA triad.

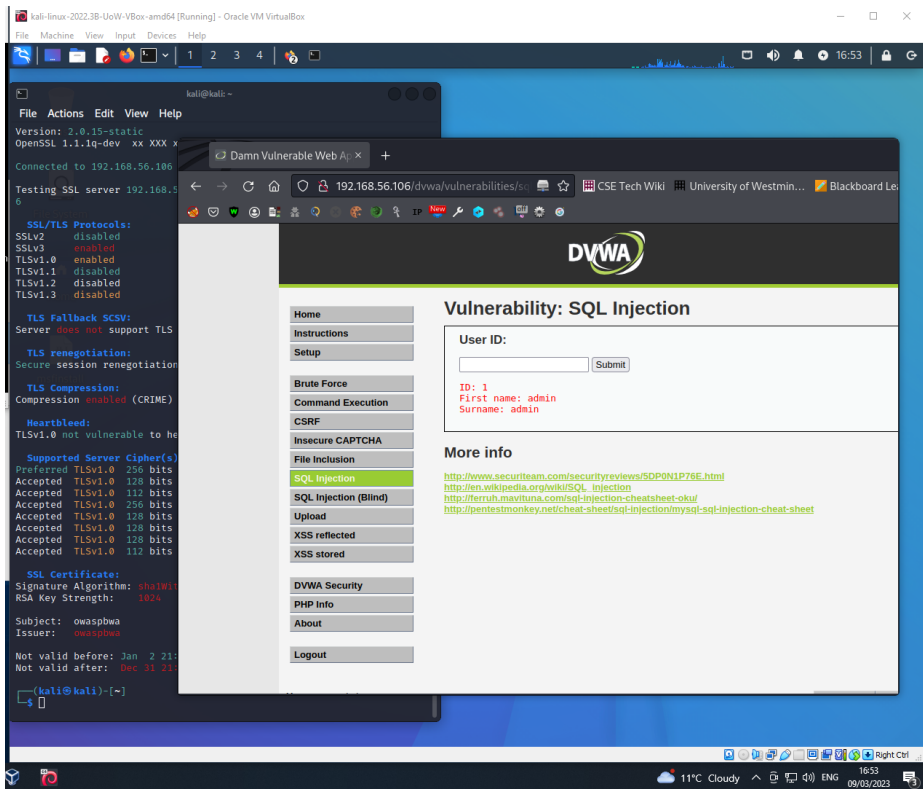
Scenario assessment: What is the vulnerable information for data tampering that attackers can obtain when this activity is carried out and how dangerous they are for your scenario? [2 marks]

In the scenario, data tampering techniques could potentially exploit the online car rental service as follows:

1. Browser-based alterations: Attackers might manipulate file size limits and form fields, bypassing client-side restrictions, allowing malicious file uploads or unauthorized requests, compromising web application security.
2. Cookie manipulation: If attackers obtain and modify cookies, such as changing the HttpOnly parameter, they could execute malicious code on the server and impersonate valid users, potentially exposing or misusing personal information and reservation data.
3. Tamper Data add-on: Intercepting and modifying POST requests, attackers could bypass client-side validation and alter hidden forms and parameters, enabling unauthorized access to staff accounts, compromising platform data integrity.

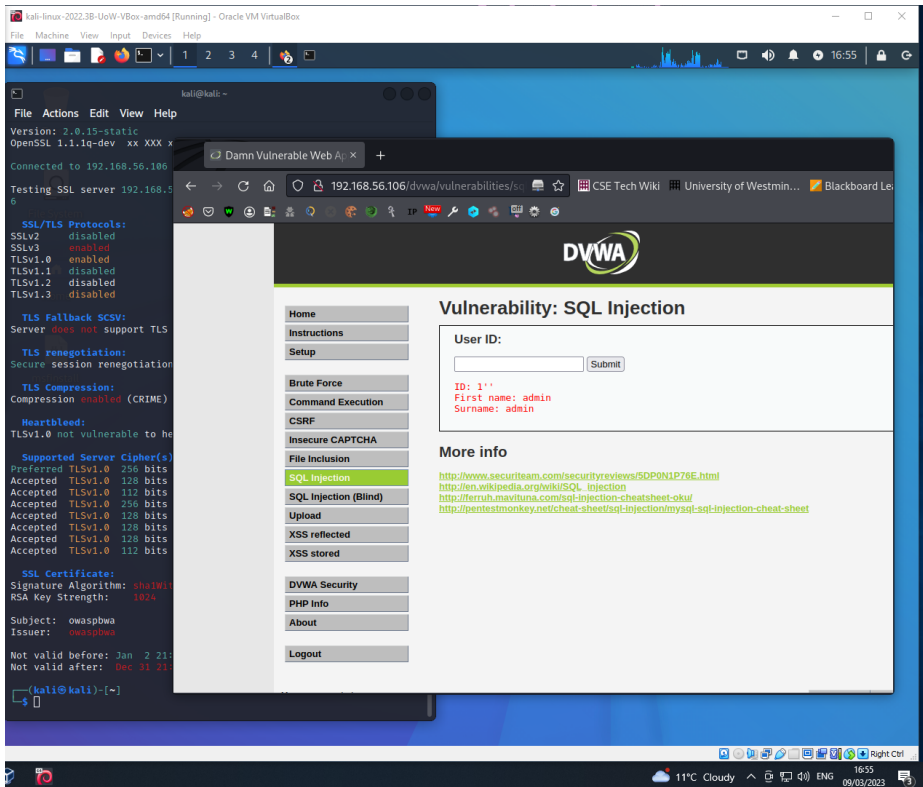
These vulnerabilities pose significant risk to the scenario, as unauthorized access to sensitive data like personal information, reservation data, vehicle information and transaction records could occur. Additionally, attackers might manipulate vehicle listings, disrupt reservation processes and compromise the platform's overall integrity and availability.

2) SQL Injection



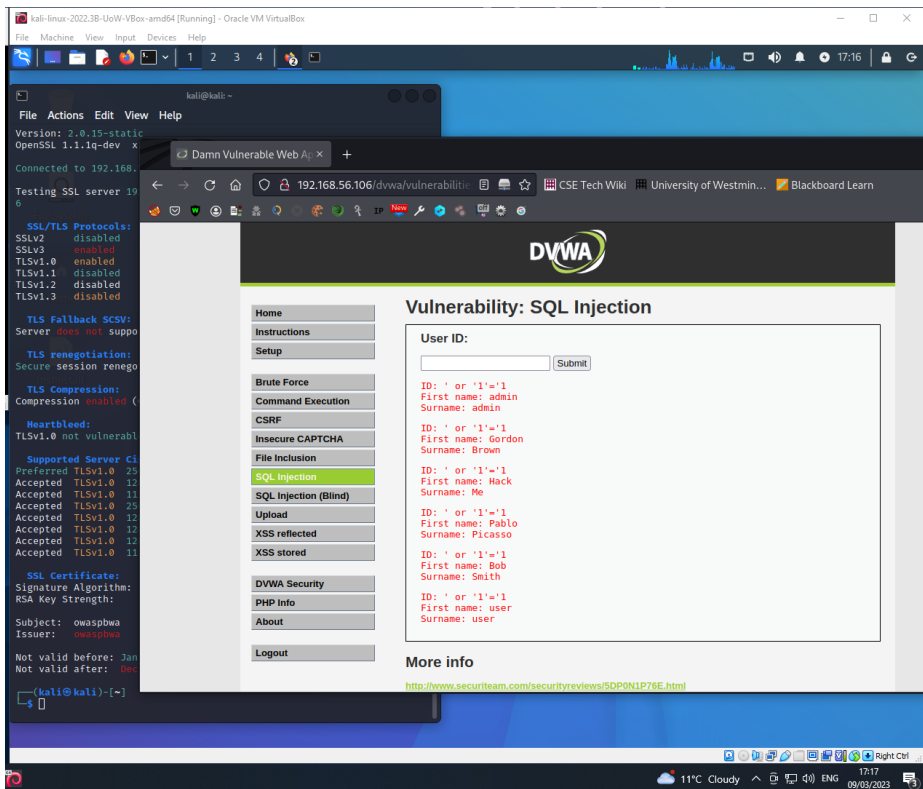
SQL Injection (Error Based) =
1

- Web application **VULNERABLE** due to improper input validation, allowing manipulation of database queries.
- Query **1** targets the record with ID 1 (admin)



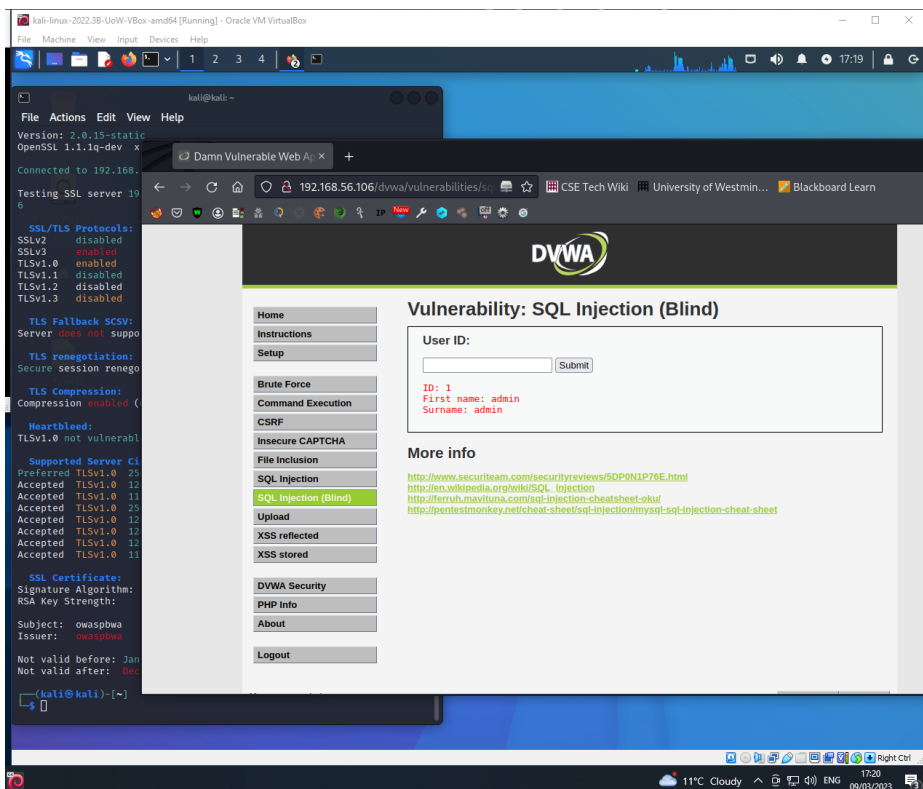
SQL Injection (Error Based) =
1''

- Web application **VULNERABLE** due to improper input validation, allowing manipulation of database queries.
- Query **1''** targets record with ID 1 (admin)



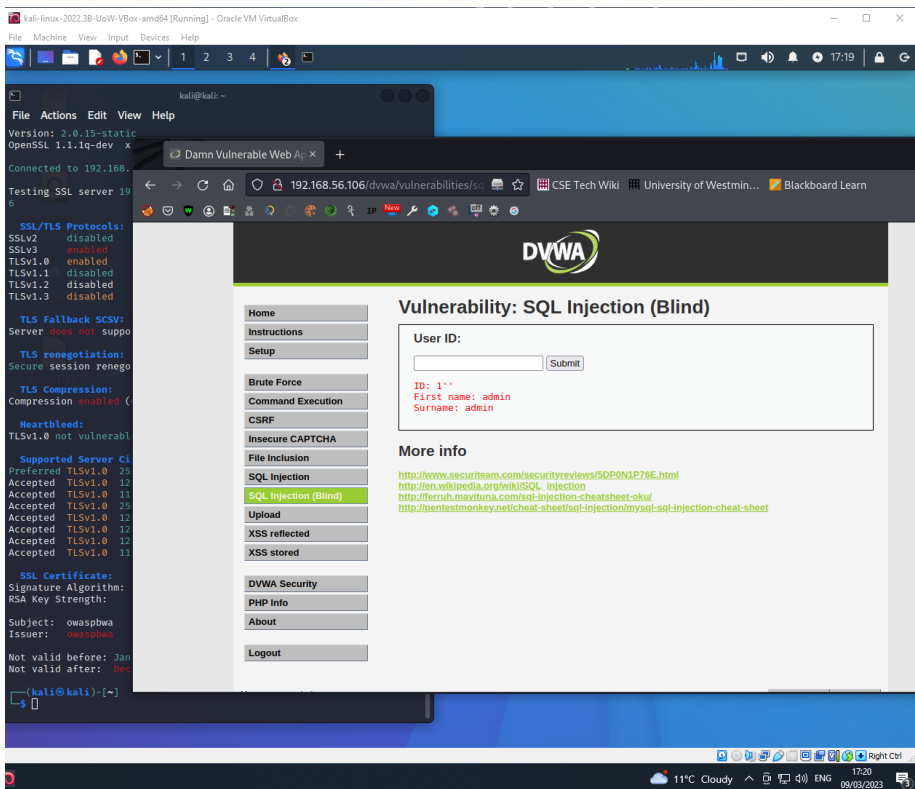
SQL Injection (Error Based) = ' or '1'='1

- Web application **VULNERABLE** due to improper input validation, allowing manipulation of database queries.
- Successfully retrieved sensitive user-data (ID, first name, and surname)- potential risk for data breaches / identity theft.
- Retrieves all records by altering the query condition to always be true.



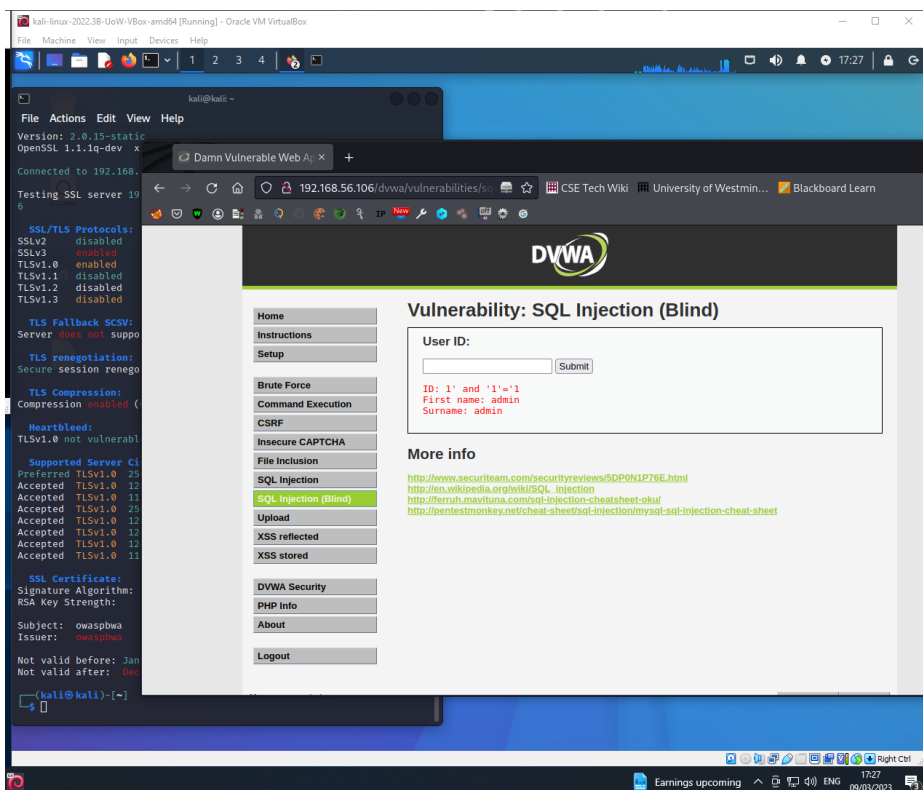
SQL Injection (Blind) = 1

- no error message, but no result either;



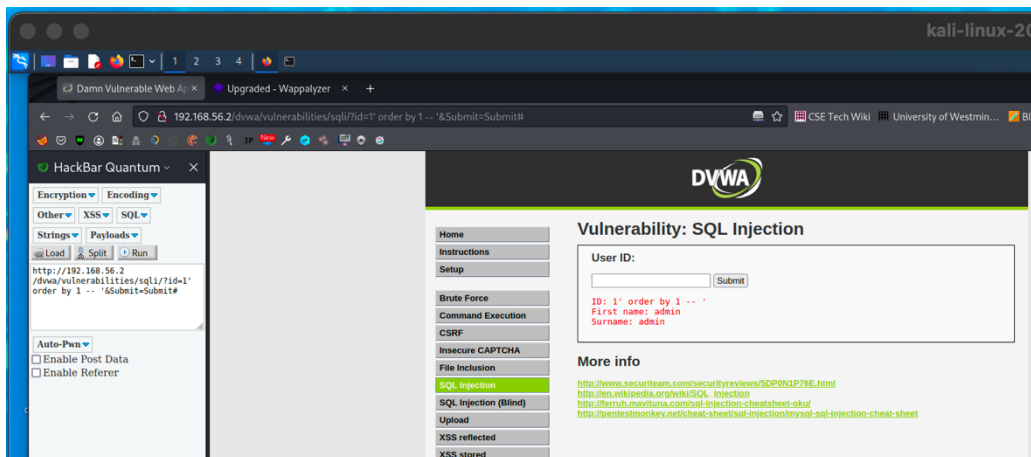
SQL Injection (Blind) =
1"

- Result for ID=1 is shown
- but it seems to be blind, no information about the database is shown

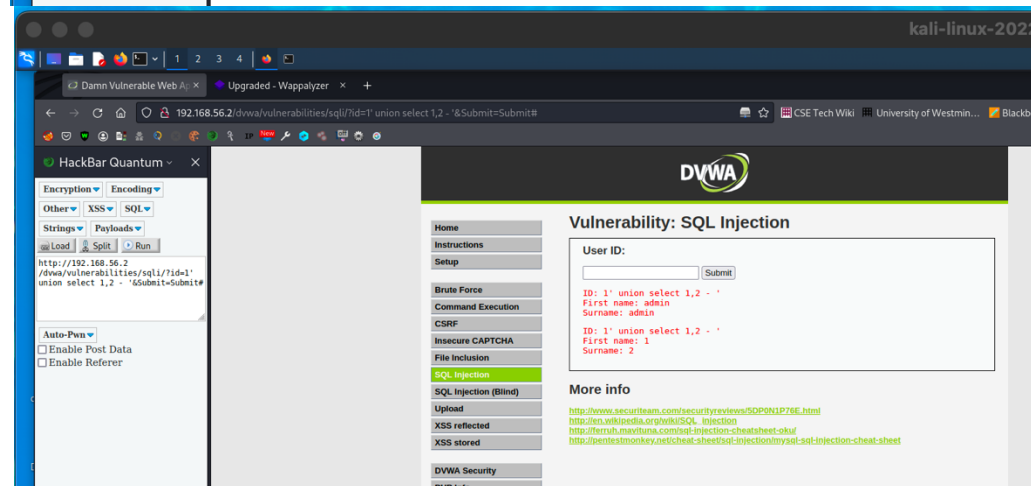
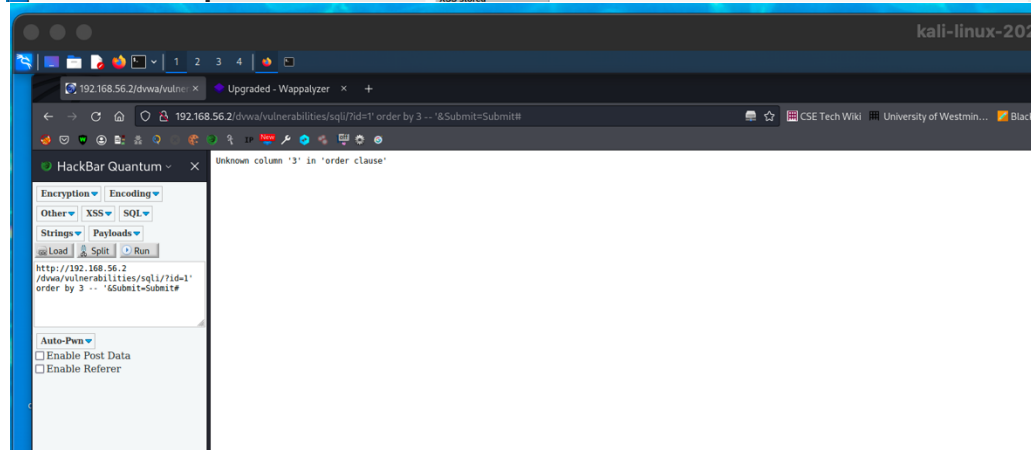


SQL Injection (Blind) =
1' and '1'='1

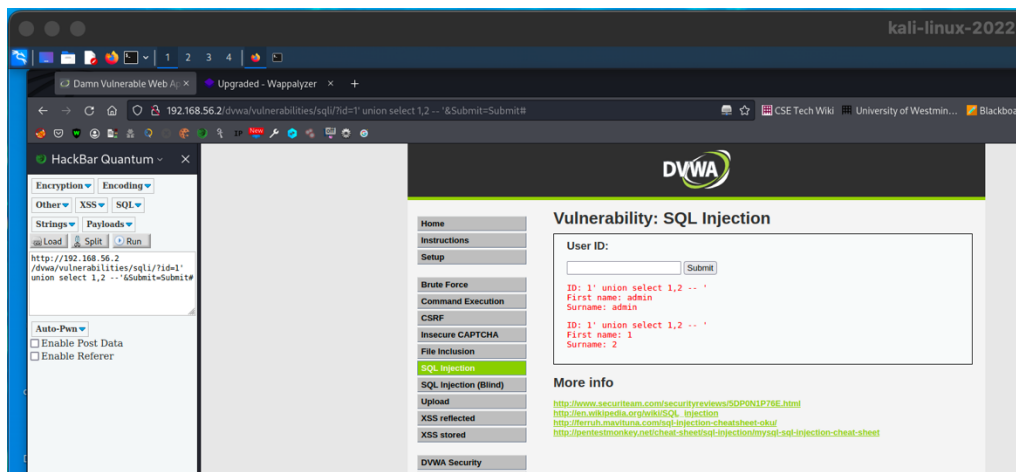
- A query that will always be true when the ID exists
- Demonstrates that there is a Blind SQL Injection in this page
- Web application **VULNERABLE**



Further SQLi –
Using Hackbar to
determine the query only
has 2 columns



Further SQLi –
Now we know it has 2
columns, further union
statement query to extract
information



Further SQLi –
query to union 2 columns
together

Briefly research and explain SQL injection vulnerability. Which Cyber Security tenet this vulnerability violates? [2 marks].

SQL injection is a common web application vulnerability where an attacker exploits poorly validated or unfiltered user input to manipulate SQL queries executed by the backend database. This vulnerability allows attackers to gain unauthorized access to sensitive data, modify or delete records, or execute arbitrary commands on the server (OWASP, 2013).

SQL injection attacks violate the "**CONFIDENTIALITY**" tenet of the CIA triad. When an SQL injection attack occurs unauthorized users can access confidential data which compromising the privacy of the system.

Scenario assessment: What is the information that attackers can obtain when this activity is carried out and how dangerous they are for your scenario? [2 marks]

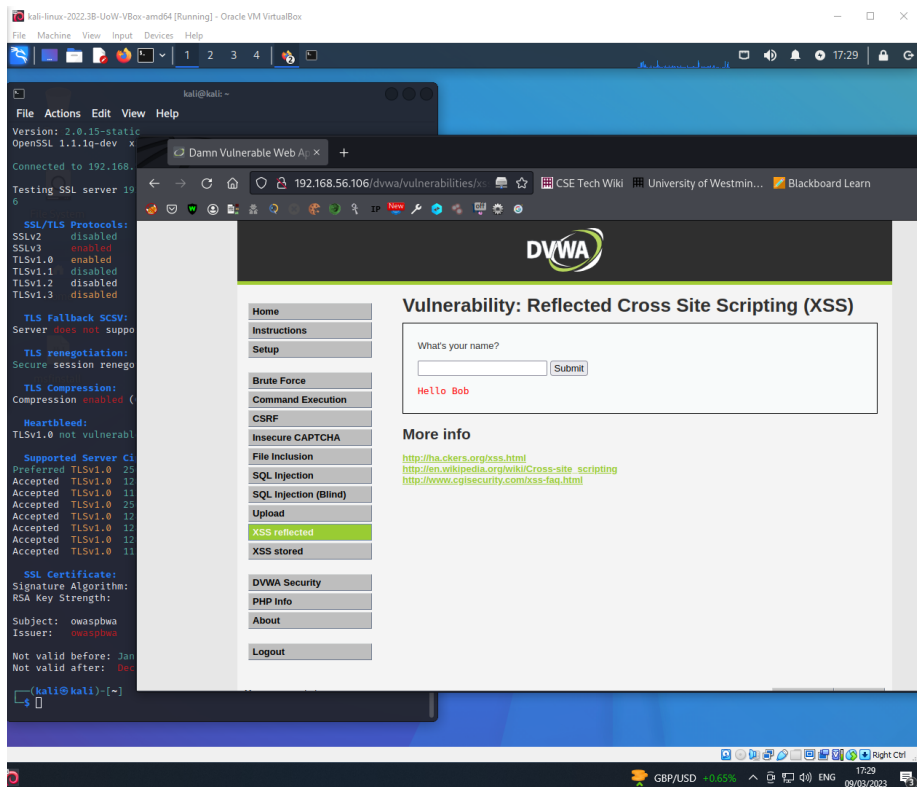
In the online car rental scenario, exploiting Error-Based and Blind SQLi vulnerabilities allows attackers to access sensitive information and manipulate data, compromising system confidentiality.

1. Error-Based SQLi: Queries (' or '1'=1) and (1") enable attackers to access user records, including names, emails, and phone numbers, potentially leading to unauthorized account access, personal information exposure, and identity theft.
2. Blind SQLi: Identified with queries (1') and ('1' and '1'=1), though the application doesn't display errors or reveal database information, attackers can exploit the vulnerability by guessing queries and observing responses, allowing unauthorized access to sensitive reservation data.
3. Further SQLi Exploits: Attackers could extract database user information, DBMS version, usernames and passwords, accessing customer/staff data. They could manipulate vehicle availability, pricing or delete reservation data, causing financial/operational issues.

Dangers:

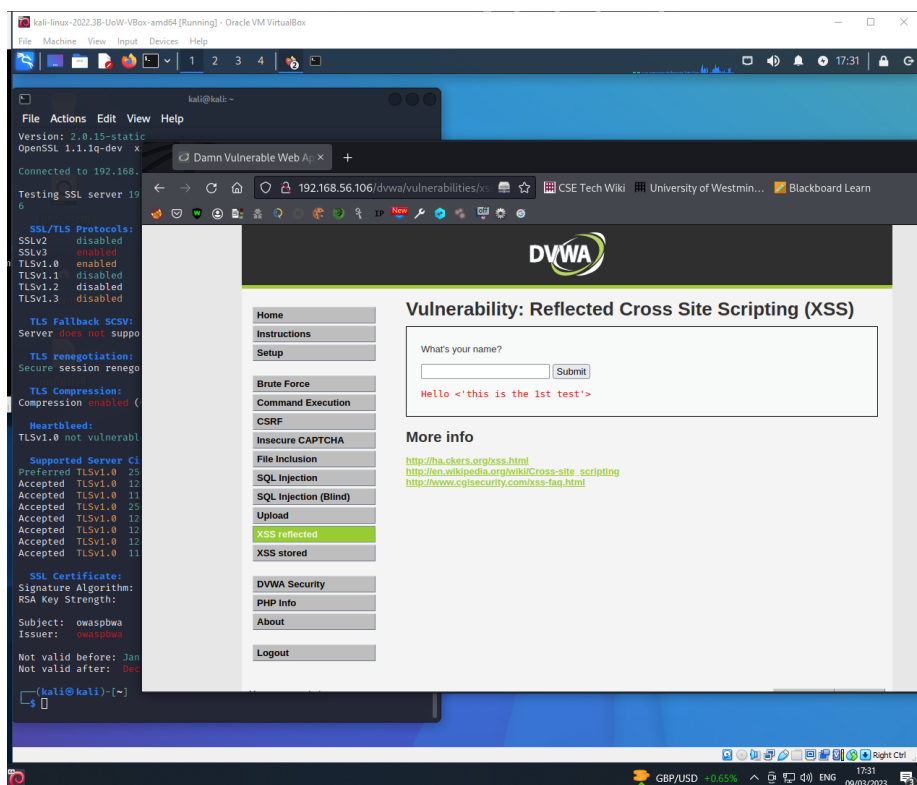
- Unauthorized access to data compromises privacy and security.
- Attackers manipulating or deleting reservation data lead to financial losses and operational issues.
- The company's reputation and customer trust may be severely damaged, resulting in business loss and potential legal consequences.

3) XSS Scripting



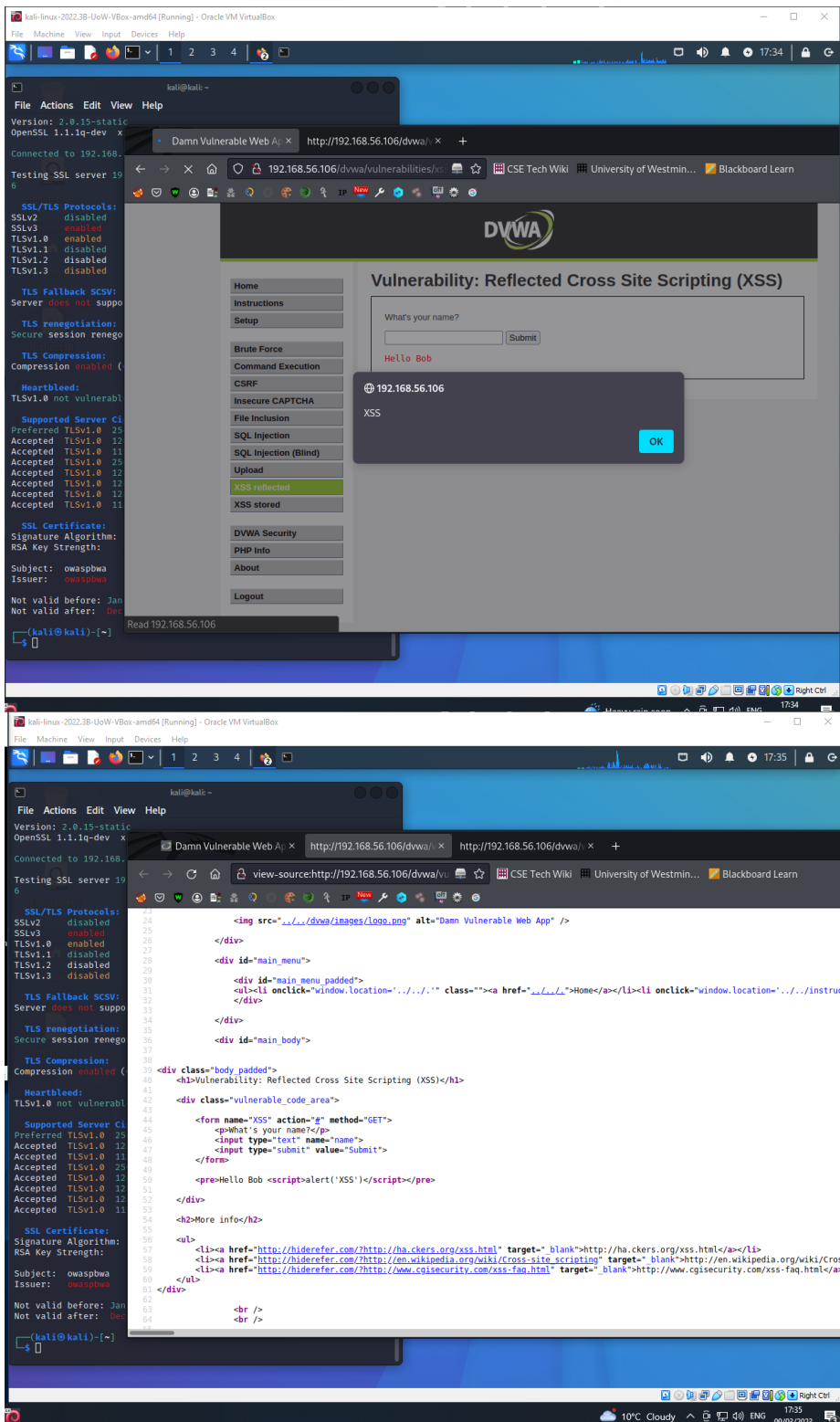
XSS Scripting =
Bob

- The application used the name we provided to form a phrase



XSS Scripting =
<'this is the 1st test'>

- Identified that anything put in the text box will be reflected in the response, it becomes a part of the HTML page in response.
- Identified VULNERABILITY



XSS Scripting =
Bob`<script>alert('XSS')</script>`

- Introduce **EXPLOIT** script to page html source
- Page executes the script causing the alert that this page is **VULNERABLE** to cross-site scripting.

Viewing page source to see
 EXPLOITS scripts effects on the
 page HTML source code

Briefly explain XSS scripting vulnerability. Which Cyber Security Tenet this vulnerability violates? [2 marks].

Cross-Site Scripting (or XSS) is a vulnerability (web application) where an attacker injects malicious code / scripts into web pages viewed by other Users. This kind of attack takes advantage of flaws in how the application handles user-supplied data and targets users rather than the application itself (Kirsten, 2020). Reflected, Stored, and DOM-based XSS vulnerabilities are the three different categories.

XSS attacks can lead to several severe consequences, including session hijacking, theft of sensitive information, defacement of web pages, and distribution of malware. The vulnerability primarily violates the **Confidentiality** tenet since the attackers can access, steal, or manipulate sensitive user data without authorization.

Scenario assessment: What are the information that attackers can obtain when this activity is carried out and how dangerous they are for your scenario? [2 marks]

In the Online Car Rental Service scenario, attackers exploiting Cross-Site Scripting (XSS) vulnerabilities could obtain sensitive information and pose serious threats.

Potential dangers:

Personal Information Exposure: Attackers could access customer and/or staff data including names, email addresses, phone numbers and Locations. This information could be used for identity theft or phishing attacks putting both customers and staff at risk.

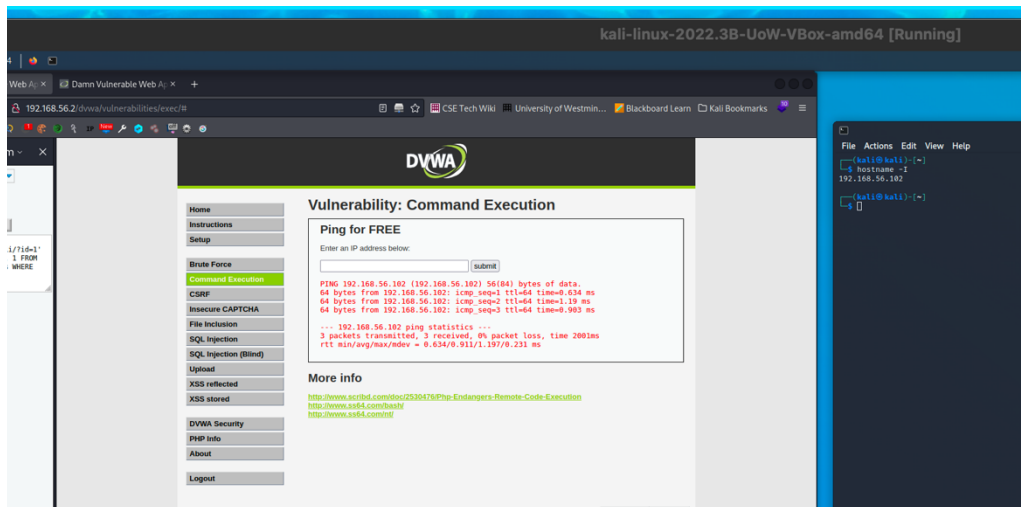
Manipulation of Reservation Data: By exploiting XSS vulnerabilities, attackers might alter reservation data, such as pick-up and drop-off dates, locations, car preferences, or special requests. This could lead to financial loss for the business and inconvenience for customers.

Unauthorized Access to Platform Features: Attackers could leverage XSS vulnerabilities to gain unauthorized access to the platform's features, such as managing vehicle listings or updating availability. This could result in false listings or inaccurate availability information, potentially damaging the company's reputation and customer trust.

In the examples provided, the lack of input validation and output encoding in the web application increases its vulnerability to XSS attacks. By exploiting these, attackers can manipulate the application's behaviour and steal sensitive information, causing significant harm to Online Car Rental Service and its users.

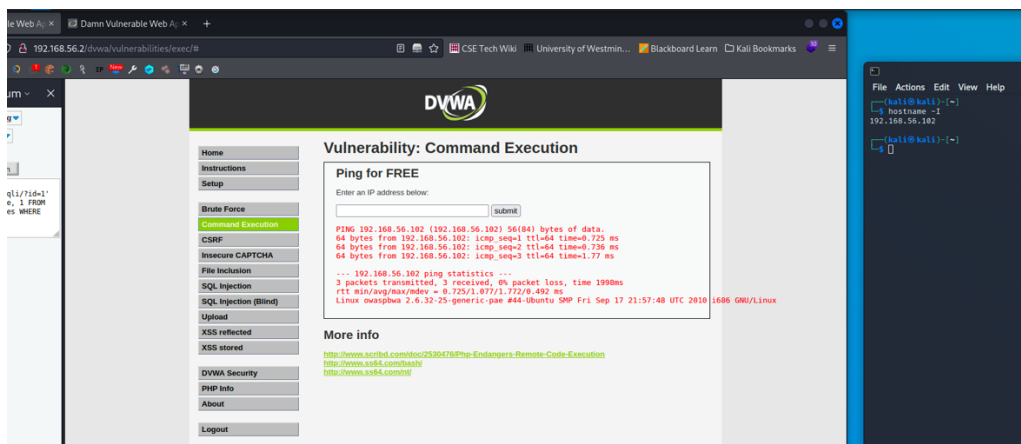
4) OWASP vulnerable machine contains several other vulnerabilities that can be exploited.

Exploiting OS command injections:



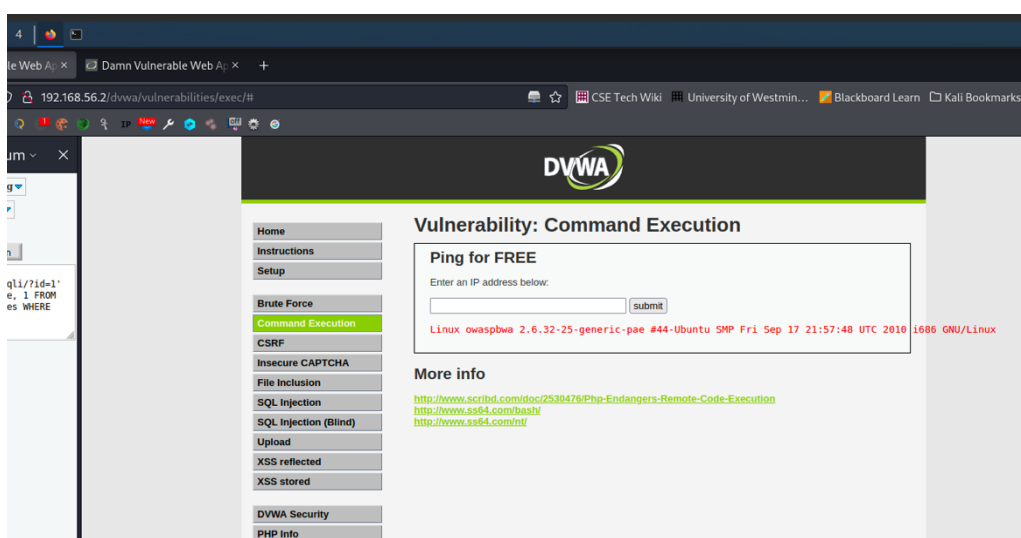
Ping to 192.168.56.102 (kali)

- Gives output that was taken directly from the ping command's output.
- Suggests the server is using an OS command to execute the ping
- So it may be possible to inject OS commands.

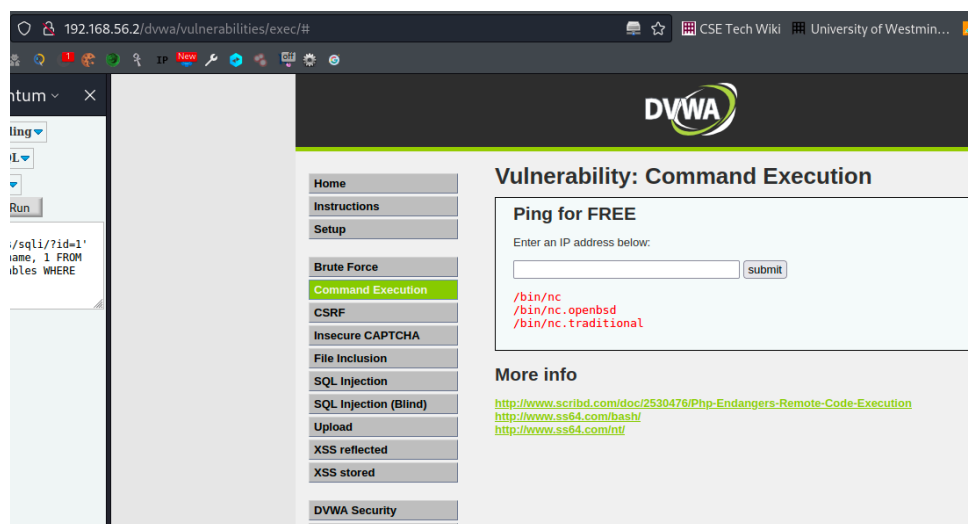


Inject simple OS Command - 192.168.56.101;uname -a

- See the uname command's output.
- There is a command injection **vulnerability** here

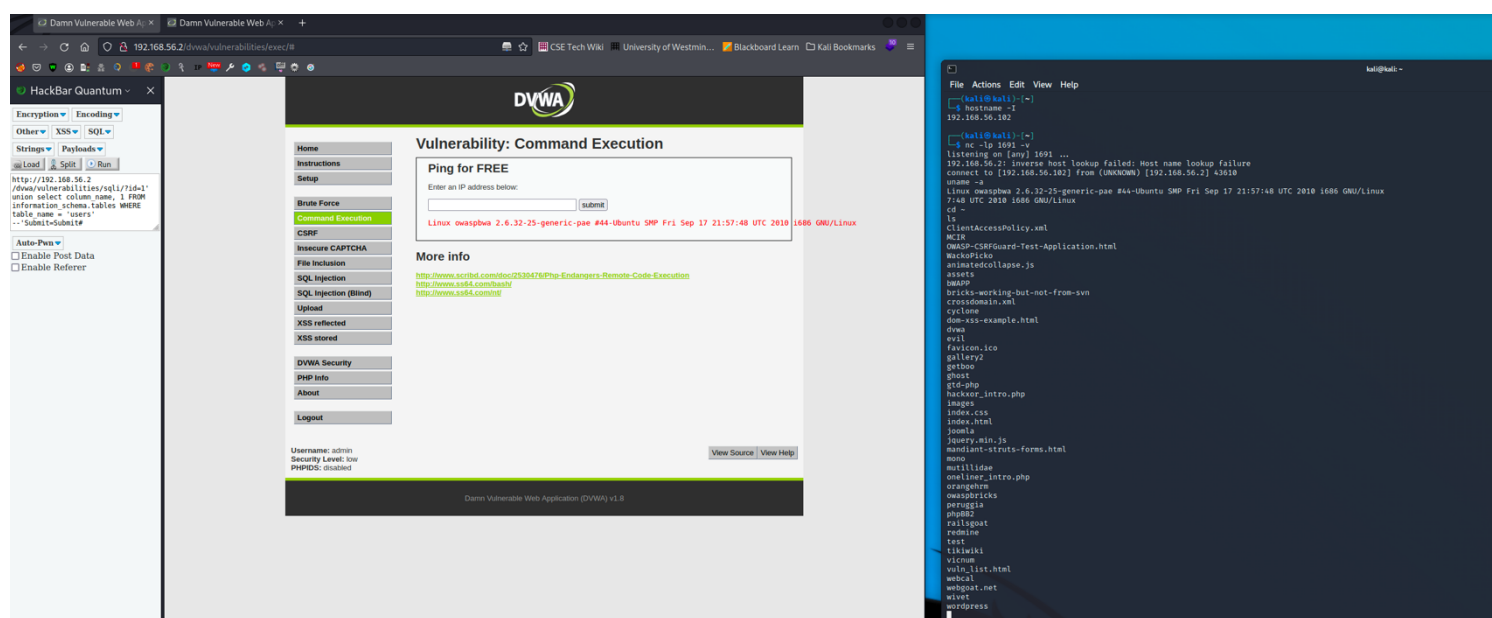


Using Command without the IP address to **isolate** the uname commands output



Identifying that NetCat is installed on the server in the bin folder using

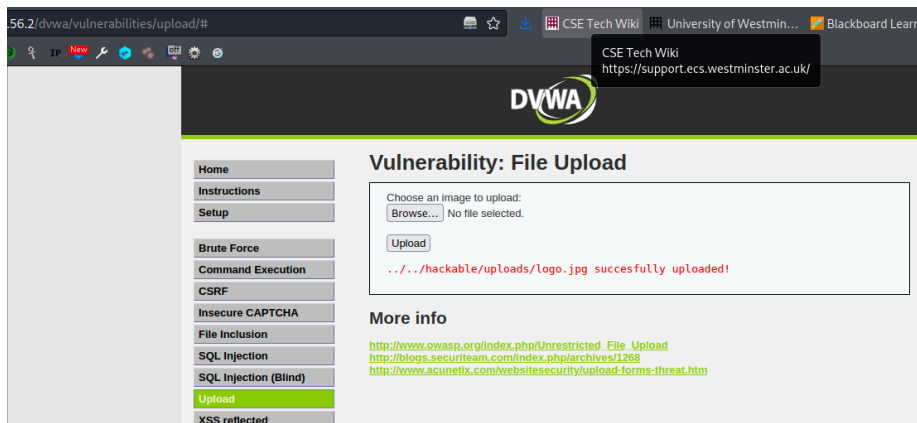
`;/ls /bin/nc*`



- Injecting a command to run netcat to give access to the server terminal.
- Listening on TCP port 1691 for a connection on my kali machine
- Allowing non-interactive commands to be executed
- For example, I used `cd~` to navigate to the home folder and get root access

⇒ OS Command Injection **VULNERABILITY** has been **EXPLOITED**

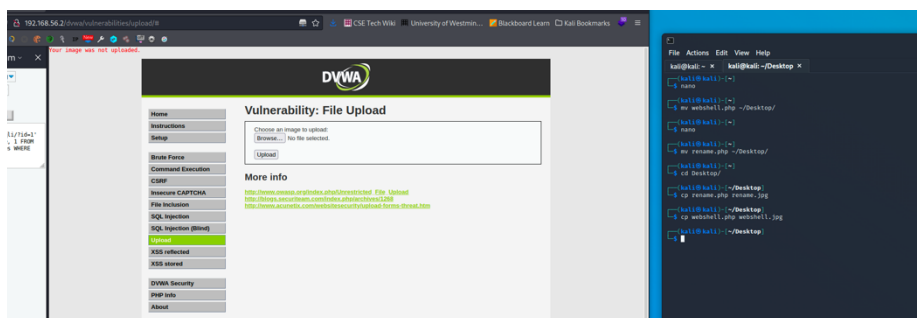
Abusing File inclusions & uploads



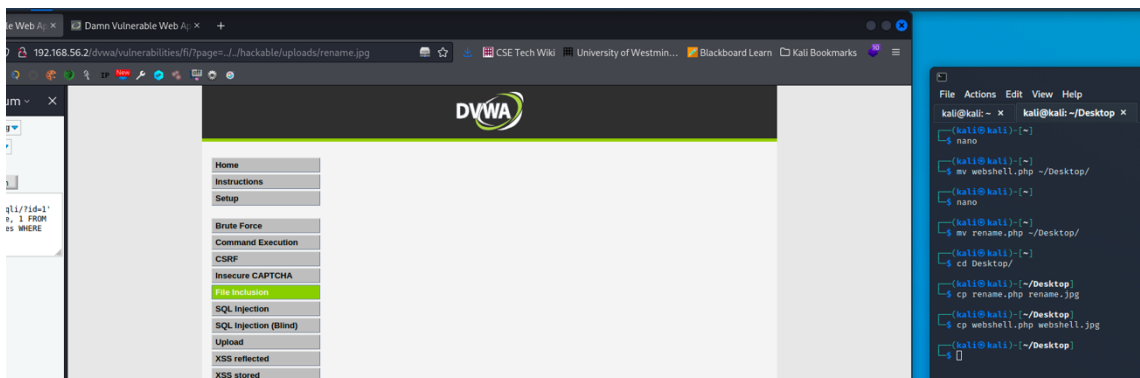
Uploading a File

Now I know the relative path where it saves the uploaded files

Possible vulnerability



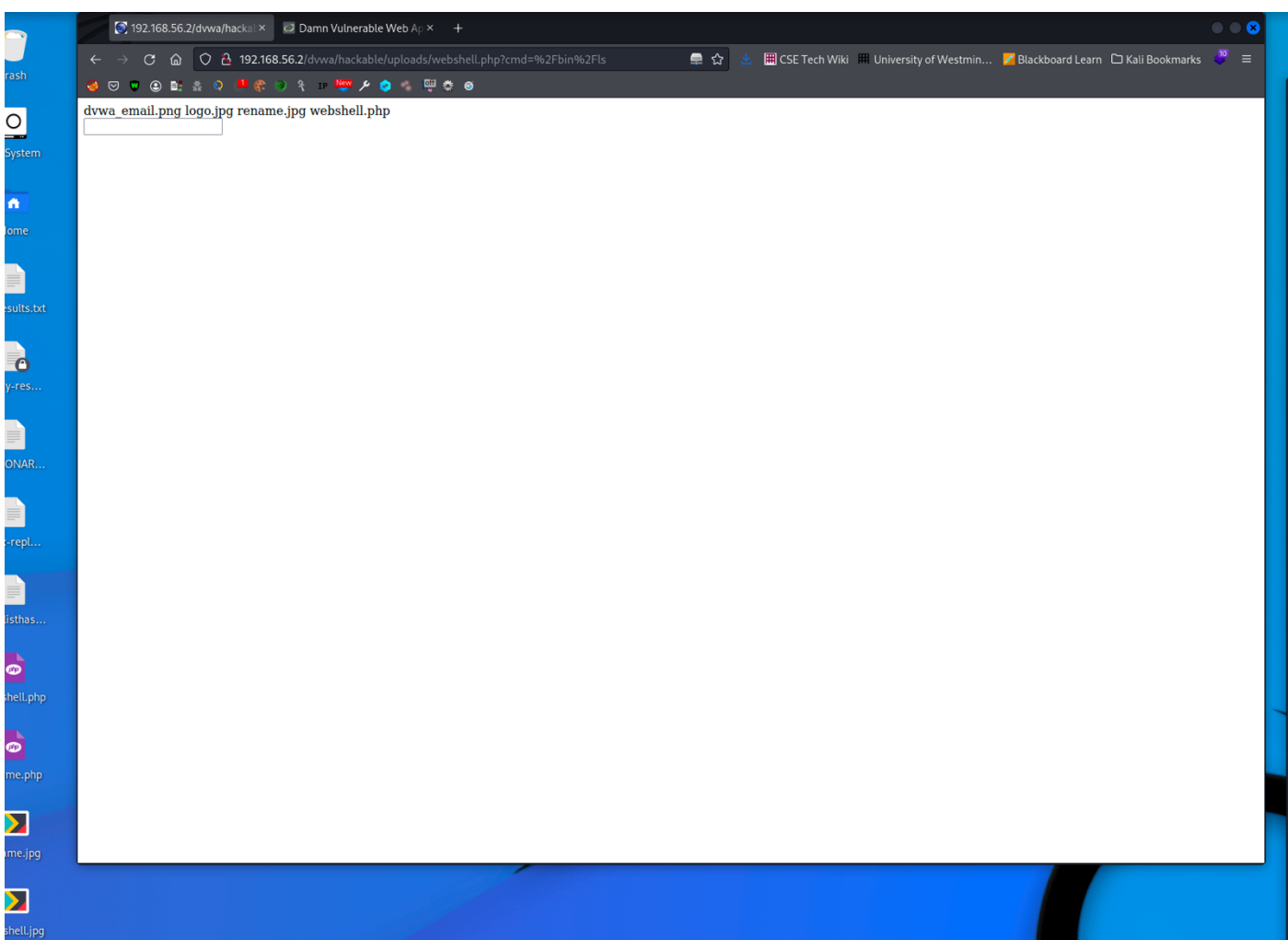
- Creating two php files – webshell.php & rename.php
- discovered a image type validation
- changing type of php to jpg to bypass validation



Uploading the disguised php files as jpgs (see url bar) & executing rename.jpg to rename the webshell.jpg file back to webshell.php so it can be used to remotely execute commands on the server by passing them as a parameter in the URL.


```
eth0 Link encap:Ethernet HWaddr 08:00:27:50:f0:5d inet addr:192.168.56.2 Bcast:192.168.56.255 Mask:255.255.255.0 inet6 addr: fe80::a00:27ff:fe50:f05d/64 Scope:Link UP BROADCAST  
RUNNING MULTICAST MTU:1500 Metric:1 RX packets:1018 errors:0 dropped:0 overruns:0 frame:0 TX packets:902 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX  
bytes:148748 (148.7 KB) TX bytes:745196 (745.1 KB) Interrupt:9 Base address:0xd020 lo Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0 inet6 addr: ::1/128 Scope:Host UP  
LOOPBACK RUNNING MTU:16436 Metric:1 RX packets:694 errors:0 dropped:0 overruns:0 frame:0 TX packets:694 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:0 RX  
bytes:116552 (116.5 KB) TX bytes:116552 (116.5 KB)
```

- navigating to ../../hackable/uploads/webshell.php page and parsing cmd value – ifconfig on the OWASP VM
- returning its IP



Parsing the cmd value /bin/ls

- This provides the contents of the current directory on the server

Scenario assessment: Research and investigate their threats for your scenario and identify which Cyber Security tenet these vulnerabilities violate? [2 marks]

In the online car rental service scenario, two types of vulnerabilities threaten the platform's cybersecurity tenets of confidentiality, integrity and availability.

Abusing file inclusions and uploads:

This allows attackers to create and execute a shell script remotely. By uploading disguised PHP files (e.g., webshell.php) and renaming them to bypass server validation, attackers can exploit local file inclusion vulnerabilities to gain control of the server. This can lead to unauthorized access to personal information, reservation data, and vehicle information, compromising **confidentiality**.

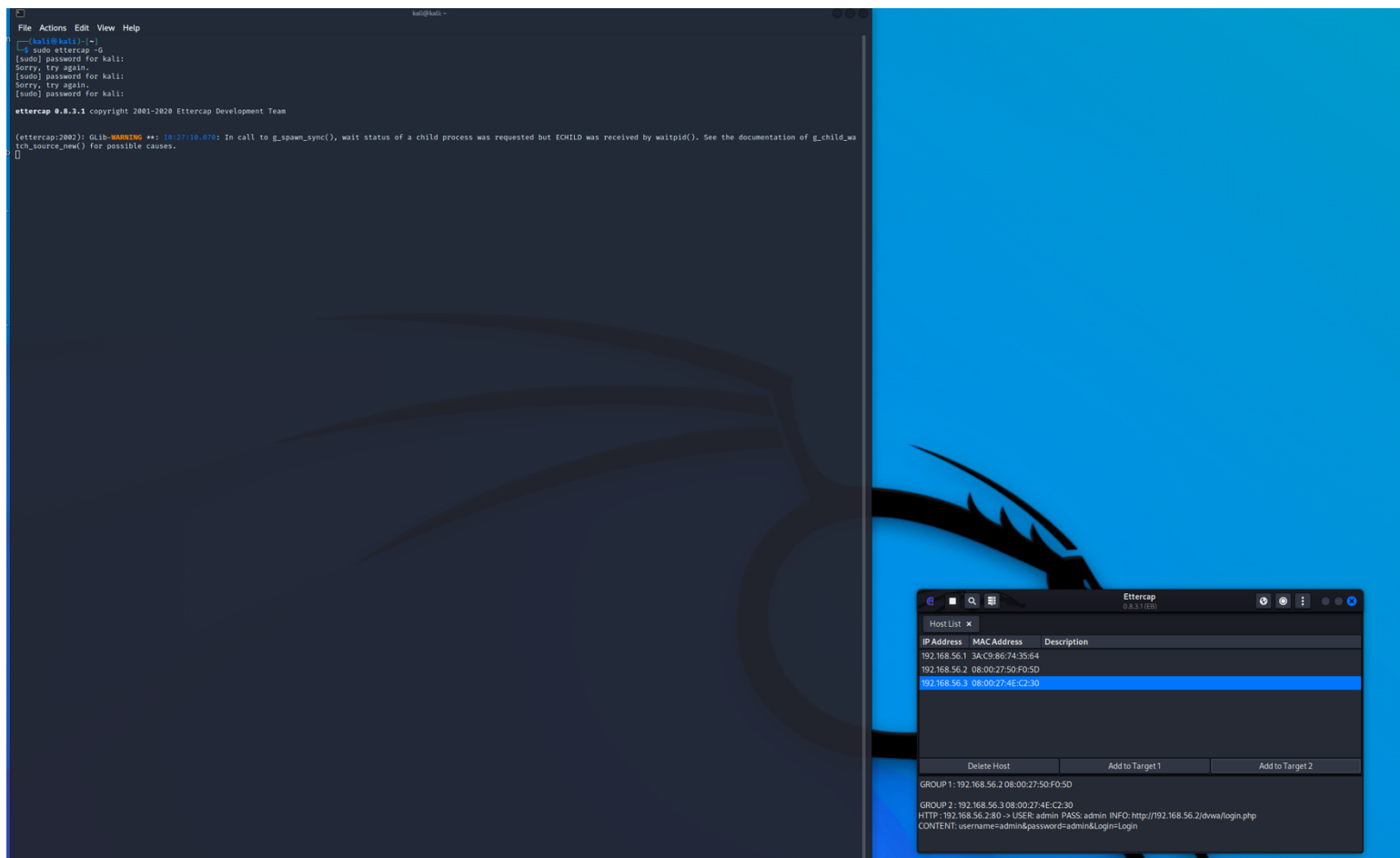
OS command injection attacks:

Exploiting OS command injections permits attackers to run unauthorized commands on the server, potentially gaining full control over the system. In the scenario, the command injection vulnerability is demonstrated by injecting OS commands through the Ping for FREE form (e.g., ';uname -a'). Attackers can leverage tools like Netcat to establish reverse shells, granting them access to the server terminal and compromising system **integrity** (Zhong, 2019).

Both attacks disrupt the normal functioning of the car rental service, impacting its **availability**. By exploiting these vulnerabilities, attackers could manipulate/delete reservation and transaction data, causing financial losses and disrupting the service for users.

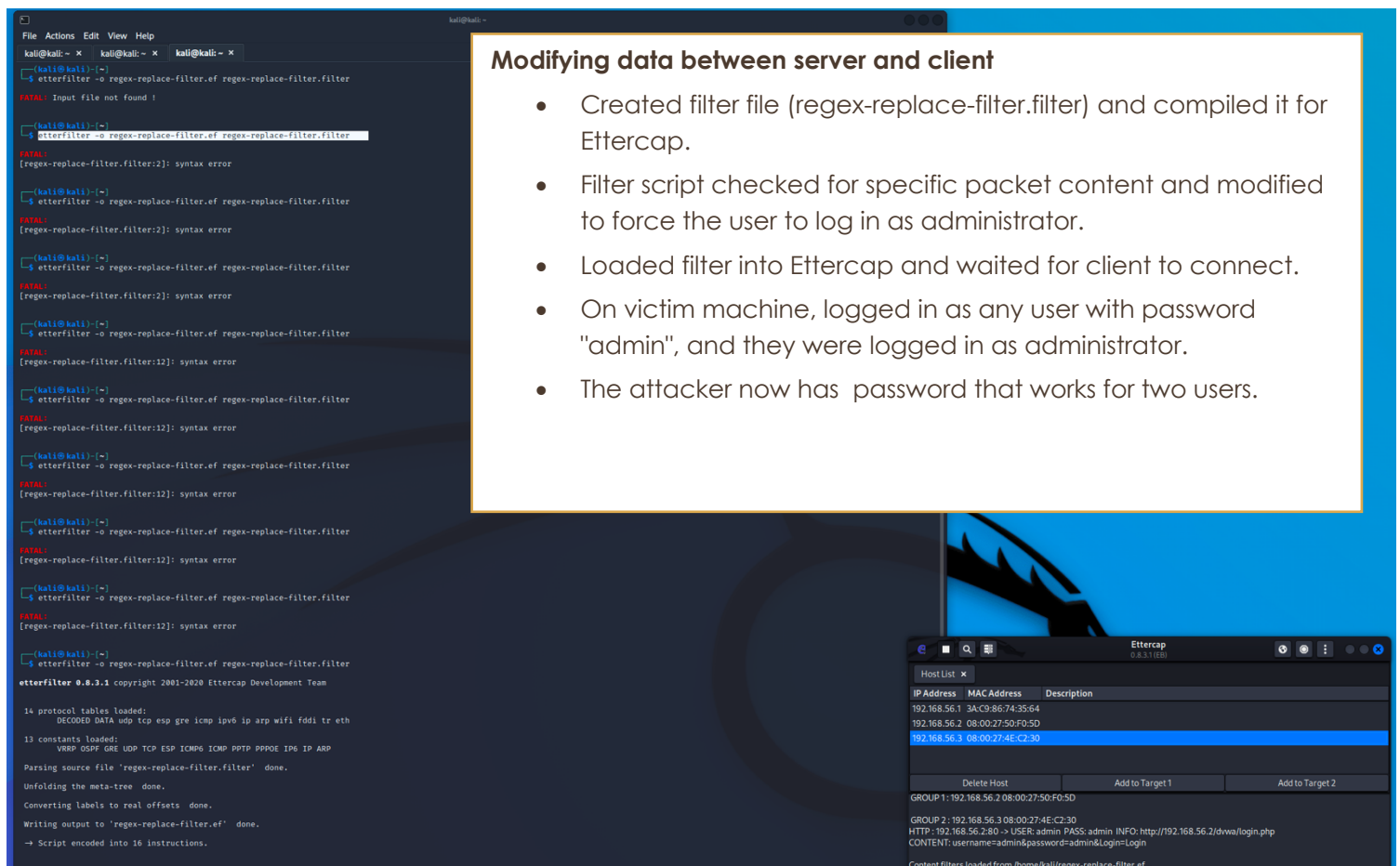
C- Client-Side Exploits

1) Man In the Middle Attacks



Setting up spoofing attack with Ettercap - ARP Spoofing

- Used three VMs: Windows victim machine, Kali Hacker machine and OWASP vulnerable server.
- Identified IP addresses for all running VMs and opened a root terminal on the Kali Linux host.
- Ran sudo ettercap -G, then scanned for network hosts and chose targets (192.168.56.2 and 192.168.56.3).
- Initiated an ARP Poisoning attack and enabled Sniff Remote Connection.
- On victim machine, Logged in to Damn Vulnerable Web Application with admin credentials.
- On attacker machine (Kali), was able to see all traffic, including admin login credentials, which were admin/admin.

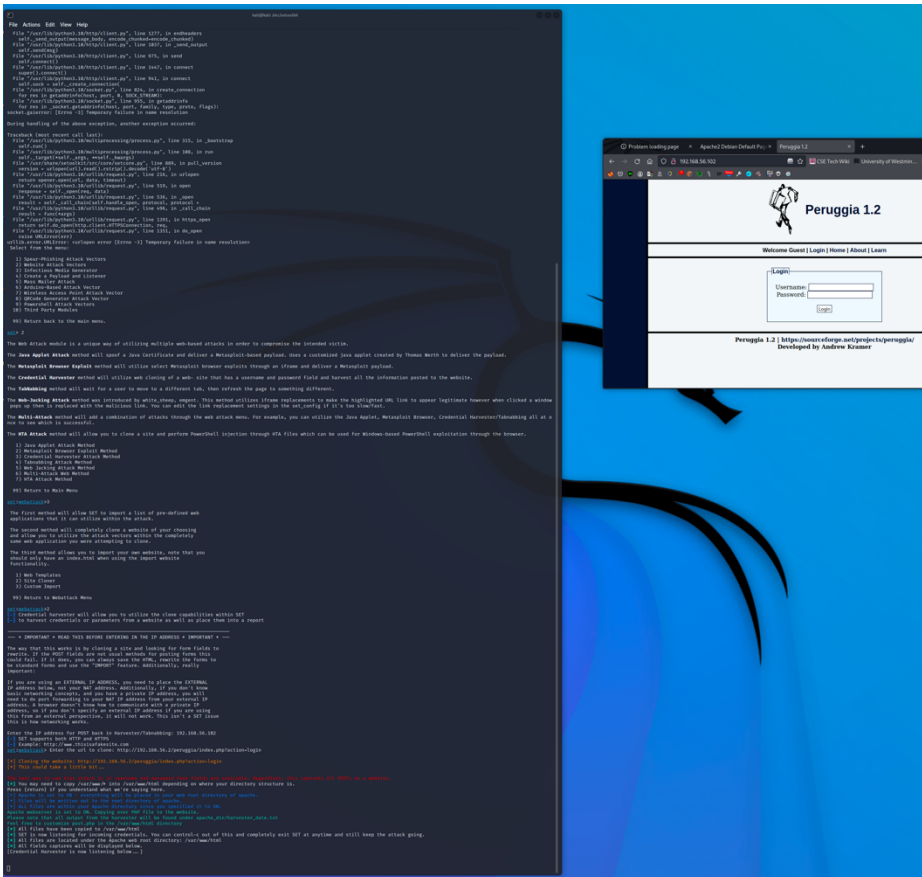


Scenario assessment: What is the information that attackers can obtain when this activity is carried out and how dangerous they are for your scenario? [4 marks]

Moreover, the attacker could intercept staff login credentials, gaining unauthorized access to the platform's management functions. This could allow them to view and manipulate customer reservations, vehicle availability, and sensitive communication with potential customers.

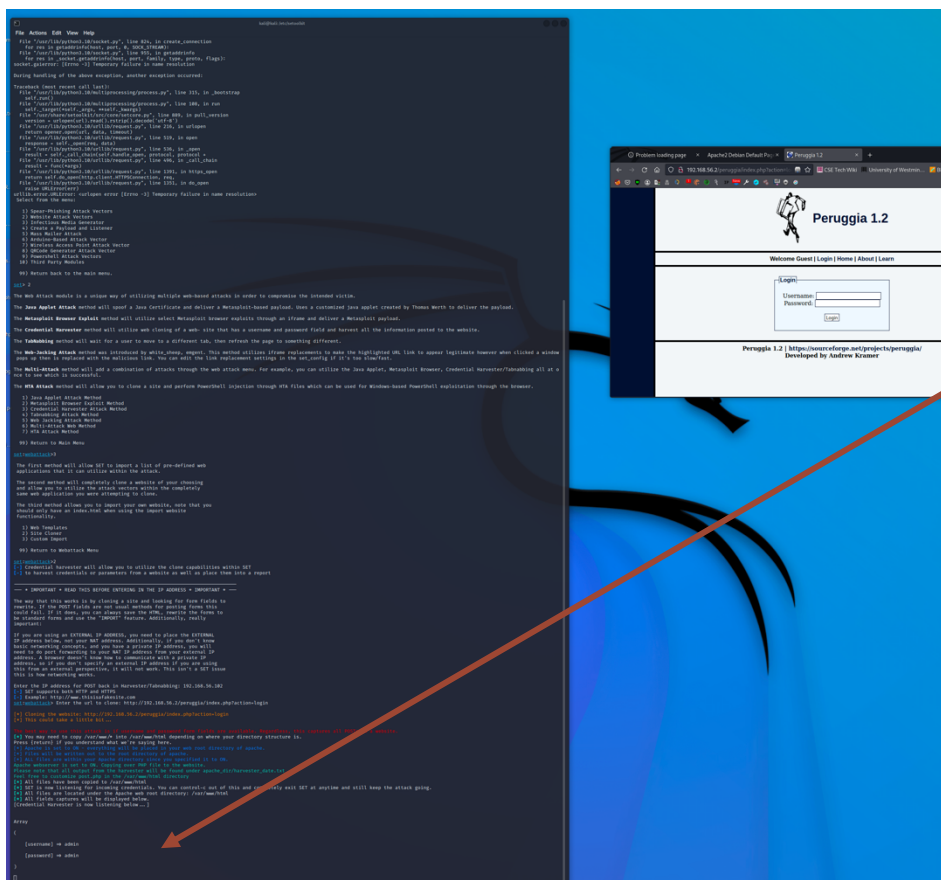
Overall, information attackers can obtain during this activity can lead to the compromise of customers' personal information, unauthorized access to the platform's functions, and manipulation of data, posing significant dangers to the online car rental service.

2) Social Engineering Attacks

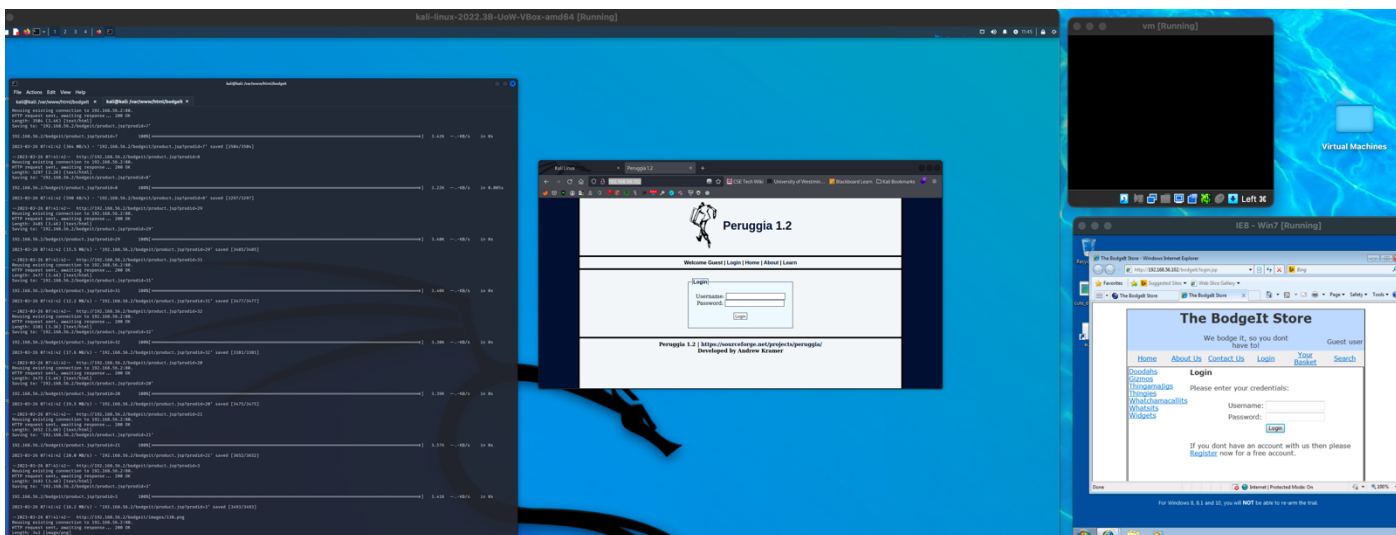


Creating a password harvester using SET

- Modify SET settings to use Apache
- Run SET and select "Site Cloner"
- Provide IP address for the POST back and URL to clone

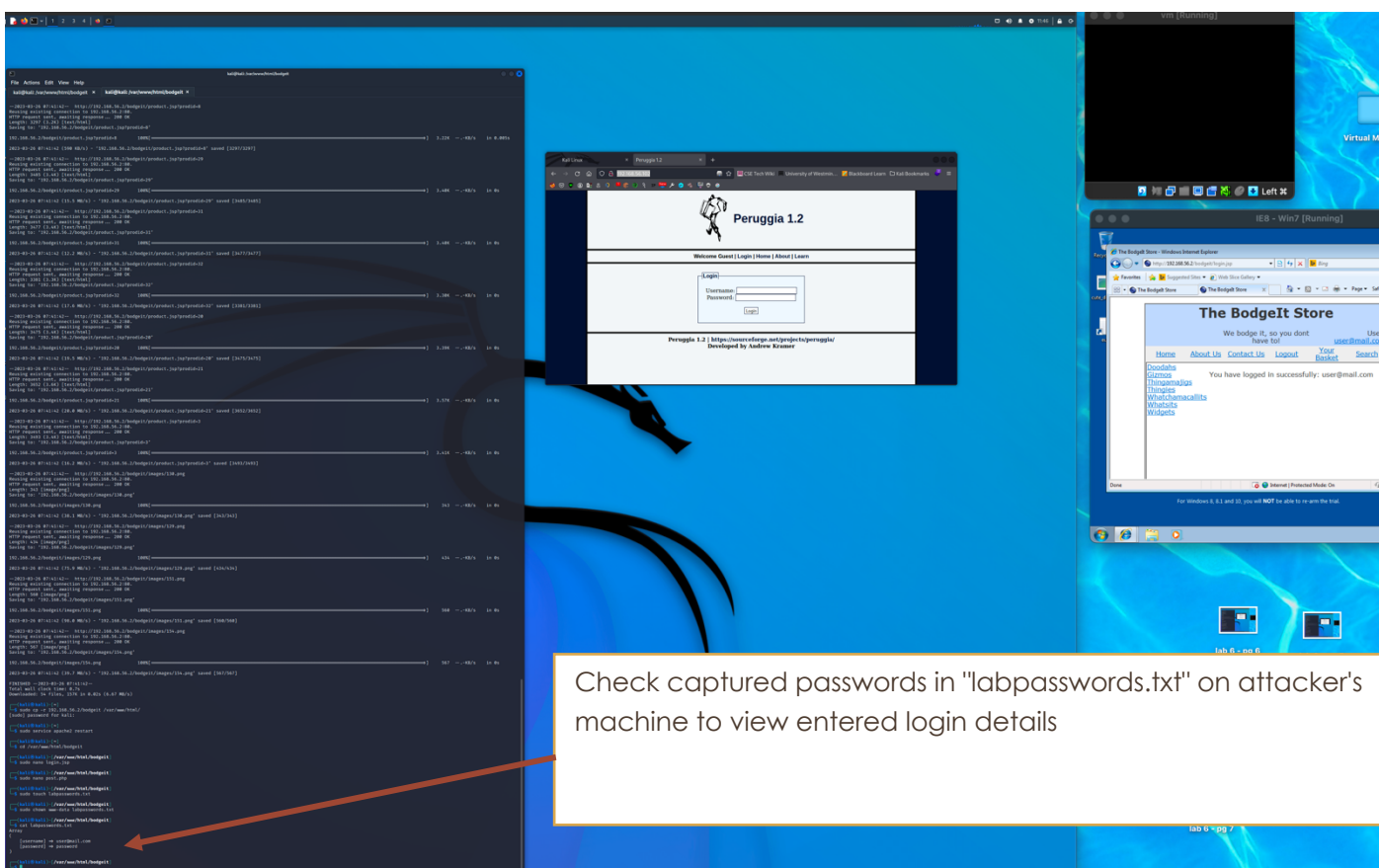


- User visits cloned-site thinking it's the original web server
- User enters username and password ("admin" for both)
- Page redirects to original login page
- On attacker machine, captured username and password are visible
- Captured credentials can also be found in `/var/www/html` on Kali Linux in files named "harvest" and with timestamp

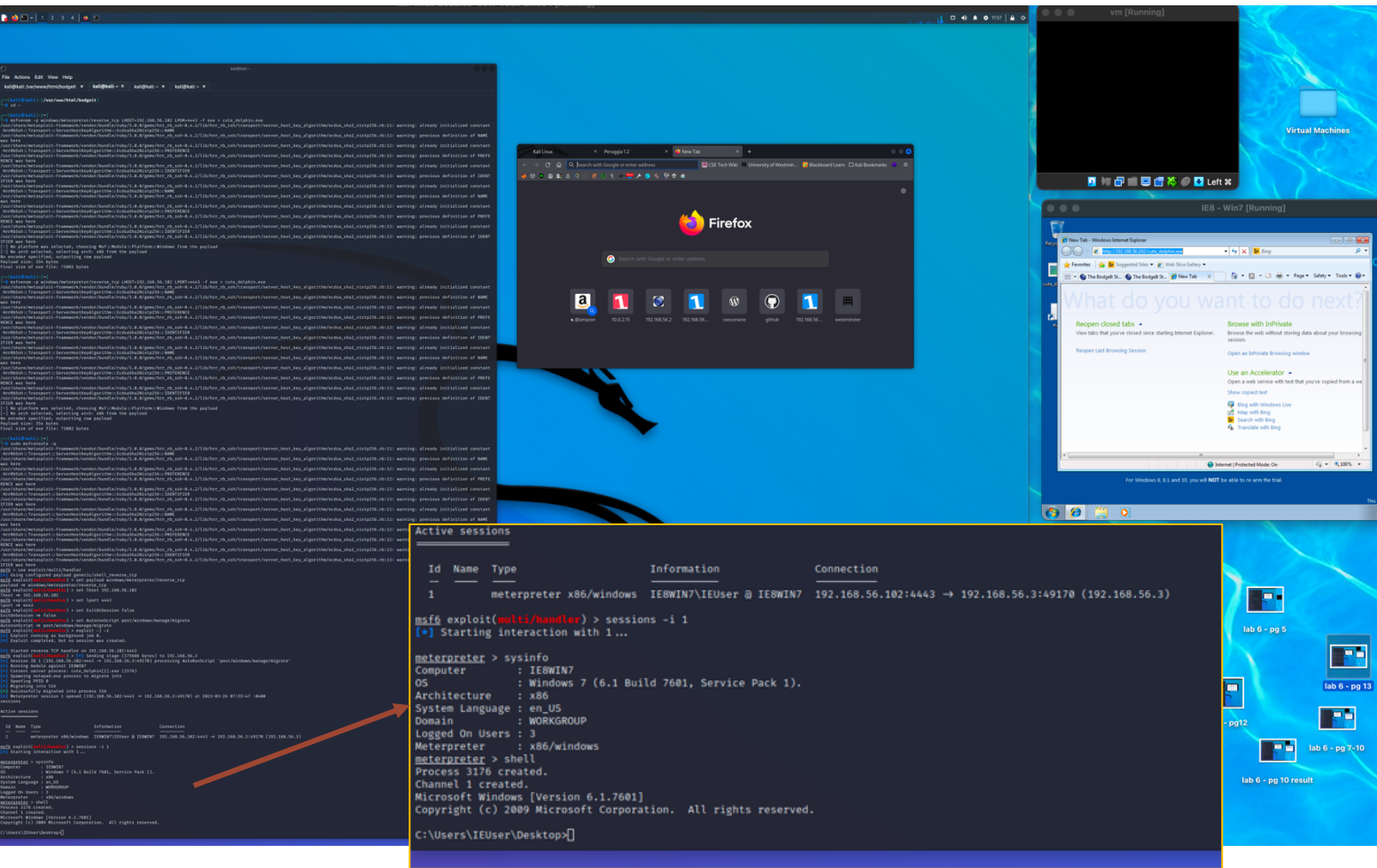


Using previously saved pages to create phishing site using WGET

- Download page with wget, store it in the "bodgeit" offline directory
- Update login.jsp file to redirect to post.php script
- Create post.php script to save captured credentials to "labpasswords.txt"
- Victim user (Windows) visits phishing site and logs in with valid credentials
- Script captures credentials and redirects to legitimate site, performing login



Check captured passwords in "labpasswords.txt" on attacker's machine to view entered login details



Phishing – with Metasploit – creating a reverse shell & capturing connections:

Used Metasploit's msfvenom to create reverse meterpreter shell, Set up listener on Kali Linux for the connection, Tricked victim (windows) into running the malicious file through social engineering, Gathered information about compromised system using sysinfo and shell commands from kali connection

Scenario assessment: What is the information that attackers can obtain when this activity is carried out and how dangerous they are for your scenario? [4 marks]

In the given scenario, attackers can obtain sensitive information through social engineering techniques, like creating a password harvester and using SET (Social-Engineer Toolkit) to clone legitimate websites. The attackers can potentially capture personal information, reservation data, vehicle information, and transaction data from customers, as well as staff credentials. Consequences of these attacks can be severe, including unauthorized access to customer accounts, potential identity theft, unauthorized reservations or changes to vehicle availability, and disruption of the car rental service's operations.

Danger increases when attackers use more elaborate phishing sites using WGET that feature full navigation and log in to the original site after capturing credentials. This technique makes it harder for users to detect the phishing attempt and the attackers can maintain access to the compromised accounts for a longer period.

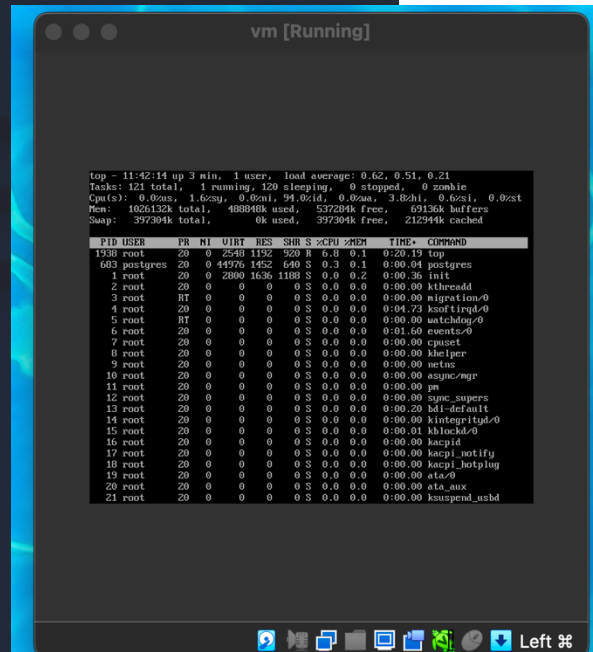
In addition, using reverse shell techniques attackers can gain control over a user's computer, enabling them to potentially access more sensitive information or launch further attacks. Combination of these social engineering techniques poses a significant threat to the online car rental service's security and could severely impact its reputation, customer trust, and overall business operations.

1) DoS the Web server

TCP fooding using hping3

~ TCP SYN Attack

CPU usage of target (OWASP) system spikes

[illegible]

Which Cyber Security Tenet this vulnerability violates? [1 mark]

(DDoS) attack on a web server violates cybersecurity tenet of Availability because availability of the web server is compromised.

Scenario assessment: What is the impact of this attack on your scenario company? [2 marks]

The online car rental service may face significant consequences from three attacks:

1. TCP flooding using hping3 and TCP SYN attack could spike the target system's CPU usage, resulting in sluggish performance and potential downtime. This could hinder platform access for customers and staff, leading to business loss and customer dissatisfaction.
2. Smurf DoS attack using DDoS Ripper might flood the system with ICMP packet requests, slowing the web application. Consequently, customers could face delays in car searches, price comparisons, and reservations. Staff may struggle to manage listings and respond to inquiries, impacting customer satisfaction and the company's reputation.
3. MHDDoS attack script may flood the system with TCP packet requests, rendering the server unresponsive. This prolonged unavailability could lead to significant loss of revenue, as customers may turn to competitors' services for their car rental needs. Additionally, the staff's inability to access the platform for managing vehicle listings, updating availability, and communicating with customers could further exacerbate the negative effects of the attack.

E- Recommendations to protect the scenario company server

(1) Briefly research what you can do to minimize the threats to the findings in the reconnaissance phase when you tested the web application in section A.2. [2 marks]

To minimize threats from reconnaissance findings, consider:

1. DirBuster: Defend against directory enumeration attacks by using mod_rewrite on Apache to rewrite directory requests into non-existing file requests (Pentestmonkey, 2019). For IIS, set the "hidden" attribute for private directories, preventing directory listing while keeping files accessible (Pentestmonkey, 2019).
2. Robots.txt: Avoid listing sensitive directories and use meta tags to prevent indexing (Watts, 2019). Implement proper access controls to secure hidden directories (Watts, 2019).
3. Web Enumeration: Employ DNSSEC to prevent DNS spoofing, disable DNS recursion, restrict zone transfers, and use isolated DNS servers (SecurityTrails Team, 2018). By implementing these practices, it can protect the web application and minimize risks from reconnaissance findings.

(2) Briefly research what port knocking is and explain how it can protect against threats you have identified in section A.3. [2 marks]

Port knocking can protect against unauthorized access to open ports, such as ports 80 and 443 found in Section A.3, by concealing their presence (ArchLinux, 2023). This technique requires a predetermined sequence of connection attempts to specific closed ports before the desired open port is revealed (ArchLinux, 2023). By keeping open ports hidden until the correct sequence is provided, port knocking reduces the likelihood of attackers discovering and exploiting these open ports, offering an additional layer of security to the existing IDS/IPS/WAF.

(3) Briefly research and explain how to protect your database against SQL injection exploited in section B.2. [3 marks]

To protect the database against SQL injection threats from Section B.2, implement prepared statements and parameterized queries (OWASP, 2021), use input validation to restrict allowed data and employ least privilege principles. For Error-Based SQL Injection, create custom error pages to hide database errors (OWASP, 2021). For Blind SQL Injection, utilize intrusion detection systems to monitor and detect unusual database activity (OWASP, 2021). Implementing these techniques will mitigate the risks of SQL injection vulnerabilities and protect the web application from potential data breaches and identity theft.

(4) Briefly research and explain how to protect your web application against cross site Scripting attacks exploited in section B.3. [3 marks]

To protect the web application against Cross site Scripting (XSS) attacks from Section B.3, the following steps can be used:

- 1) Validate and sanitize user-input to prevent the inclusion of malicious scripts,
- 2) Use secure output encoding when displaying user-generated content to ensure proper handling of special characters.
- 3) Implement a Content Security Policy(CSP) to restrict script execution from unauthorized sources (OWASP, 2019).
- 4) Enable the HttpOnly attribute for cookies to prevent unauthorized access.

By adopting these strategies, it reduces the risk of XSS vulnerabilities and maintains the security of the web application.

(5) Investigate what activities a security analyst can carry out to protect, or at least minimize the impact of Man in the Middle attack carried out in section C.1 [3 marks]

A security analyst can carry out the following activities to protect/minimize the impact of MITM attacks:

For ARP Spoofing, implement static ARP entries, use dynamic ARP inspection (DAI) on switches, and monitor the network for abnormal ARP behavior (Grimmick, 2021)

For modifying data between the server and the client, apply end-to-end encryption using HTTPS and SSL/TLS, ensuring secure data transmission (IanIndexsy, 2023). Additionally, use strong authentication methods like two-factor authentication(2FA) to reduce unauthorized access risks.

(6) Research the work that companies should do to ensure that their users do not fall victims to social engineering attacks similar to the attack you carried out in section C.2. [3 marks]

To counter social engineering attacks performed in Section C.2, companies should:

1. For SET Site Cloner attacks: Implement multi-factor authentication (MFA) to add an extra security layer, rendering captured credentials less useful (Chinnasamy, 2020).
2. For WGET phishing attacks: Educate users on verifying website URLs and using bookmarks for important sites to avoid visiting fake sites (Chinnasamy, 2020).
3. For reverse shell attacks: Promote awareness of unsolicited downloads and teach users to verify the source before downloading any files. Implement endpoint protection software to detect and block malicious executables (Chinnasamy, 2020).

Additionally Use intrusion detection systems (IDS) to monitor network traffic and block suspicious activity (Bello, Alashwal and Moustafa, 2022).

(7) Research and explain what companies do to protect their web services against a DoS attack similar to the one you have carried out in section D.1. [2 marks]

To protect against DoS attacks similar to those carried out in Section D.1, companies can implement the following measures:

1. For TCP flooding: Install Intrusion Prevention Systems (IPS) to detect anomalous traffic patterns, configure firewalls for SYN Attack Thresholds and SYN Flood protection, and use up-to-date networking equipment with rate-limiting capabilities (Firch, 2021).
2. For Smurf attacks: Disable IP-directed broadcasts on routers, apply outbound filters on perimeter routers, and configure hosts and routers not to respond to ICMP echo requests (Heimdal, 2021). Implement network monitoring, use firewalls, increase bandwidth, build redundancy, and protect DNS servers to avoid becoming a victim.

(8) Intrusion Detection and Prevention systems:

Show some examples of firewall and iptables rules that can protect your scenario company against attacks you identified in the assessment you carried out before. [3 marks]

The screenshot shows a Kali Linux terminal window with the following output:

```
root@kali:~# iptables -L -n
Chain INPUT (policy DROP)
target: DROP
Chain FORWARD (policy DROP)
target: DROP
Chain OUTPUT (policy ACCEPT)
target: ACCEPT
```

The terminal also shows the output of the `iptables` command, indicating that the firewall is enabled and blocking all connections.

A web browser window in the background shows a "Problem loading page" error for the URL "http://192.168.56.2". The message states: "The connection has timed out. The server at 192.168.56.2 is taking too long to respond." This indicates that the firewall rules are successfully blocking incoming traffic.

Ufw firewall enabled
~ blocked all connections

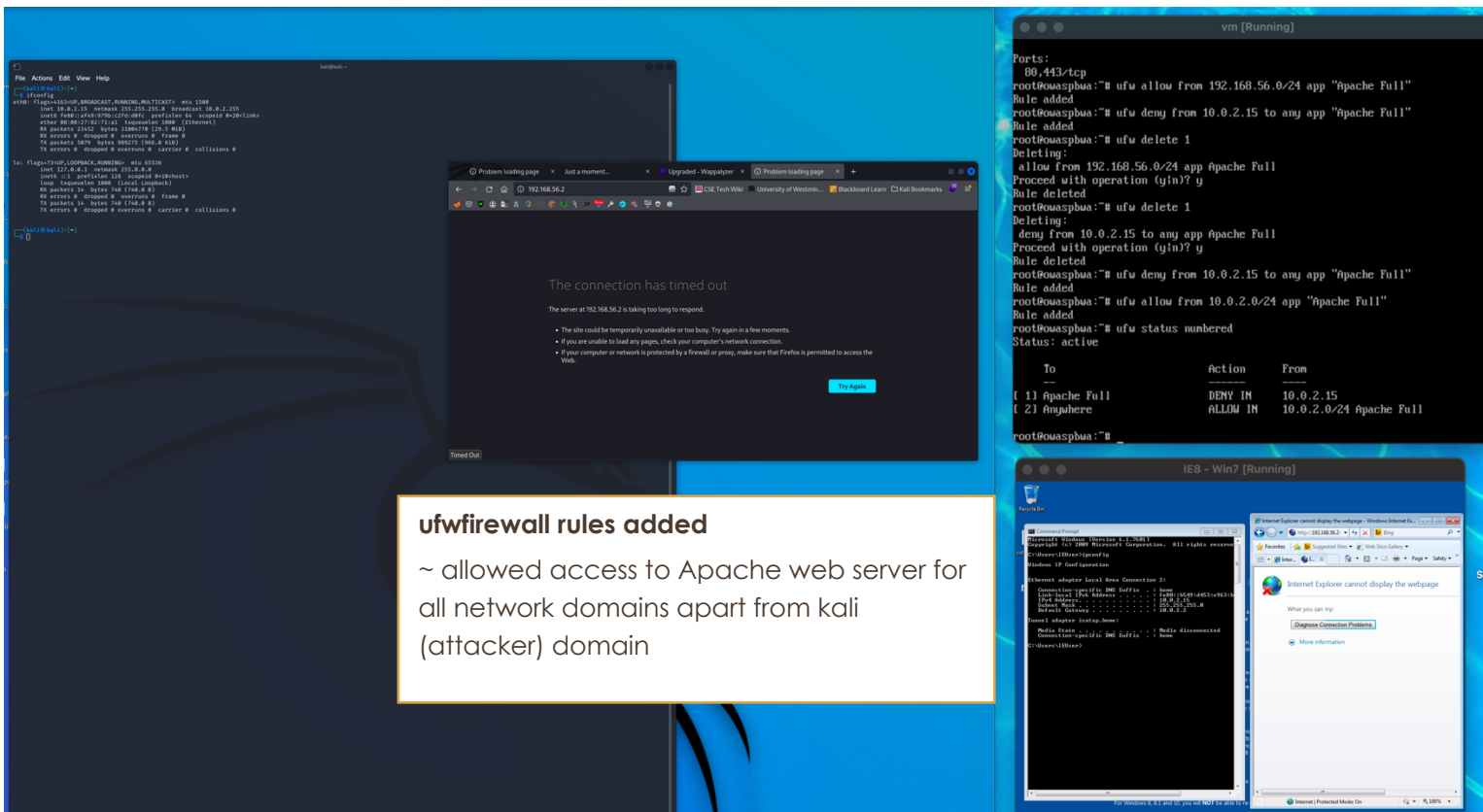
The screenshot shows a Kali Linux terminal window with the following output:

```
root@kali:~# iptables -L -n
Chain INPUT (policy DROP)
target: DROP
Chain FORWARD (policy DROP)
target: DROP
Chain OUTPUT (policy ACCEPT)
target: ACCEPT
```

The terminal also shows the output of the `iptables` command, indicating that the firewall is enabled and blocking all connections.

A web browser window in the background shows the OWASP Broken Web Applications Project page. The page title is "OWASP Broken Web Applications Project" and it contains information about the project and its goals.

ufw firewall rules added
~ "ufw allow 80/tcp" & "ufw allow 443/tcp"
~ open HTTP (80) and HTTPS (443) ports.
Allows incoming traffic using TCP.



ufwfirewall rules added

~ allowed access to Apache web server for all network domains apart from kali (attacker) domain

```
vm [Running]

Chain ufw-user-limit-accept (0 references)
target    prot opt source                destination
ACCEPT   all  --  0.0.0.0/0              0.0.0.0/0

Chain ufw-user-limit-forward (0 references)
target    prot opt source                destination

Chain ufw-user-limit-input (0 references)
target    prot opt source                destination

Chain ufw-user-limit-output (0 references)
target    prot opt source                destination

Chain ufw-user-limit (1 references)
target    prot opt source                destination
root@owaspbua:~# sudo ufw deny from 10.0.2.15 to any app "Samba"
Rule added
root@owaspbua:~# sudo ufw app info "Samba"
Profile: Samba
Title: LanManager-like file and printer server for Unix
Description: The Samba software suite is a collection of programs that implements the SMB/CIFS protocol for unix systems, allowing you to serve files and printers to Windows, NT, OS/2 and DOS clients. This protocol is sometimes also referred to as the LanManager or NetBIOS protocol.

Ports:
  137,138/udp
  139,445/tcp
root@owaspbua:~#
```

iptables

~ samba ufw rule added, seen in iptable

```
vm [Running]

Chain ufw-user-limit-accept (0 references)
target    prot opt source                destination

Chain ufw-user-limit (0 references)
target    prot opt source                destination

Chain ufw-user-limit-accept (0 references)
target    prot opt source                destination

Chain ufw-user-limit-forward (0 references)
target    prot opt source                destination

Chain ufw-user-limit-input (0 references)
target    prot opt source                destination

Chain ufw-user-limit-output (0 references)
target    prot opt source                destination

Chain ufw-user-limit (0 references)
target    prot opt source                destination

Chain ufw-user-limit-forward (0 references)
target    prot opt source                destination

Chain ufw-user-limit-input (0 references)
target    prot opt source                destination

Chain ufw-user-limit-output (0 references)
target    prot opt source                destination

Chain ufw-user-limit (0 references)
target    prot opt source                destination
root@owaspbua:~# sudo ufw deny from 10.0.2.15 to any app "Samba"
Skipping adding existing rule
root@owaspbua:~# iptables -A
iptables v1.4.4: option '-A' requires an argument
Try 'iptables -h' or 'iptables --help' for more information.

root@owaspbua:~# sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
root@owaspbua:~# sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
root@owaspbua:~#
```

iptables

~ 2 commands add rules to **iptables** firewall, allowing incoming TCP traffic on ports 80 (HTTP) and 443 (HTTPS).

```

vm [Running]
target    prot opt source                destination
Chain ufw-user-limit-accept (0 references)
target    prot opt source                destination
Chain ufw-user-logging-forward (0 references)
target    prot opt source                destination
Chain ufw-user-logging-input (0 references)
target    prot opt source                destination
Chain ufw-user-logging-output (0 references)
target    prot opt source                destination
Chain ufw-user-output (0 references)
target    prot opt source                destination
root@owaspbua:~# sudo ufw deny from 10.0.2.15 to any app "Samba"
Skipping adding existing rule
root@owaspbua:~# iptables -A
iptables v1.4.4: option '-A' requires an argument
Try 'iptables -h' or 'iptables --help' for more information.
root@owaspbua:~# * sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
*: command not found
root@owaspbua:~# sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
root@owaspbua:~# sudo iptables -A INPUT -s 10.0.2.15 -p tcp --destination-port 80 -j DROP
root@owaspbua:~# sudo iptables -A INPUT -s 10.0.2.15 -p tcp --destination-port 443 -j DROP
root@owaspbua:~#

```

iptables

~ deny **web server traffic** access from attacker machine IP

```

vm [Running]
:ufw-before-logging-input - [0:0]
:ufw-before-logging-output - [0:0]
:ufw-before-output - [0:0]
:ufw-logging-allow - [0:0]
:ufw-logging-deny - [0:0]
:ufw-not-local - [0:0]
:ufw-reject-forward - [0:0]
:ufw-reject-input - [0:0]
:ufw-reject-output - [0:0]
:ufw-skip-to-policy-forward - [0:0]
:ufw-skip-to-policy-input - [0:0]
:ufw-skip-to-policy-output - [0:0]
:ufw-track-input - [0:0]
:ufw-track-output - [0:0]
:ufw-user-forward - [0:0]
:ufw-user-input - [0:0]
:ufw-user-limit - [0:0]
:ufw-user-limit-accept - [0:0]
:ufw-user-logging-forward - [0:0]
:ufw-user-logging-input - [0:0]
:ufw-user-logging-output - [0:0]
:ufw-user-output - [0:0]
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
-A INPUT -s 10.0.2.15/32 -p tcp -m tcp --dport 80 -j DROP
-A INPUT -s 10.0.2.15/32 -p tcp -m tcp --dport 443 -j DROP
COMMIT
# Completed on Sat May 6 12:31:18 2023
root@owaspbua:~#

```

iptables

~ list of all rules including EXTRA rule that denies **all** access from attacker machine IP

The ufw/iptables rules above block an attacker IP which protect the web-application by restricting their access to the network, which reduces the risk of port scanning, emulation, reconnaissance, SQLi and XSS attacks. However, a skilled hacker can bypass these rules by using different IPs or proxy-servers enabling them to attack. Therefore, it's important to use ufw/iptables in conjunction with other security measures like IPS / IDS.

Evaluate the effectiveness of the following tools and specify which is more suitable for your scenario and justify your answers. [3 marks] – Firewall (ufw) – iptables

In the online car rental service, both ufw and iptables are effective tools for securing the network. However, ufw is more suitable for this case due to its simplicity and user-friendliness. Ufw allows easy management of firewall rules (Safe Security, 2021), ensuring that the web server is accessible while blocking unwanted connections. It also offers simple app-based configurations, making it efficient for controlling access to various services like Apache or Samba. While iptables is powerful and provides granular control, its complexity might lead to misconfigurations (Safe Security, 2021), which could compromise security. Overall, ufw is the better choice for this scenario due to its ease of use and adequate functionality.

Explain the differences between Intrusion Detection System IDS and Intrusion prevention System IPS. [3 marks]

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are both essential tools for network security, with some shared features such as monitoring, alerting, learning, and logging (OKTA, 2023). However, they differ in key aspects: IDS is a passive system that requires manual intervention after an alert, while IPS is an active control system that takes action automatically (OKTA, 2023). IDS arguably provides less protection since users must decide how to respond to threats, whereas IPS handles this process (OKTA, 2023). False positives from an IDS only inconvenience the user, while an IPS may impact multiple users by shutting down traffic (OKTA, 2023).

Scenario assessment: Suggest a recommendation for the scenario you have in hand and justify your answer. [3 marks]

In the scenario of an online car rental service, a combination of Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) is recommended (Cisco, 2021). The business involves sensitive personal information, which necessitates robust security measures. IDS monitors the network, detects suspicious activities, and alerts administrators, whereas IPS actively prevents intrusions by blocking or redirecting malicious traffic (OKTA, 2023). Implementing a hybrid solution, like a Network Intrusion Prevention System (NIPS), provides the benefits of both IDS and IPS (Palo Alto Networks, 2018), ensuring comprehensive security for the web app, personal data, and reservation details. This approach will enhance the overall protection and minimize potential breaches for the car rental service.

References

- ArchLinux. (2023). Port knocking - ArchWiki. *wiki.archlinux.org*. Available from https://wiki.archlinux.org/title/Port_knocking.
- Bello, A., Alashwal, H. and Moustafa, A.A. (2022). Chapter 2 - A dual integrated dynamic intrusion detection system (DID-IDS) for protection against network and social engineering attacks. *ScienceDirect*. Available from <https://www.sciencedirect.com/science/article/abs/pii/B9780323905701000139> [Accessed 6 May 2023].
- Chinnasamy, V. (2020). 10 Ways Businesses Can Prevent Social Engineering Attacks | Indusface Blog. *Indusface*. Available from <https://www.indusface.com/blog/10-ways-businesses-can-prevent-social-engineering-attacks/>.
- Cisco. (2021). Best Intrusion Detection and Prevention Systems (IDPS) in 2020 | G2. G2. Available from <https://www.g2.com/categories/intrusion-detection-and-prevention-systems-idps>.
- Firch, J. (2021). How To Prevent A SYN Flood Attack. *PurpleSec*. Available from <https://purplesec.us/prevent-syn-flood-attack/>.
- Grimmick, R. (2021). ARP Poisoning: What it is & How to Prevent ARP Spoofing Attacks. *www.varonis.com*. Available from <https://www.varonis.com/blog/arp-poisoning>.
- Heimdal. (2021). What Is a Smurf Attack and How to Prevent It. *Heimdal Security Blog*. Available from <https://heimdalsecurity.com/blog/smurf-attack-ddos/>.
- IanIndexsy. (2023). Man-in-the-Middle Attack: Prevention Best Practices and Detection. *Sapphire*. Available from <https://www.sapphire.net/cybersecurity/man-in-the-middle-attack-prevention/>.
- Joseph Migga Kizza. (2013). *Guide To Computer Network Security*. S.L.: Springer Nature.

- Kirsten, S. (2020). Cross Site Scripting (XSS) | OWASP. *Owasp.org*. Available from <https://owasp.org/www-community/attacks/xss/>.
- MBA Knowledge Base. (2014). Data Tampering - Meaning, Types and Countermeasures. *MBA Knowledge Base*. Available from <https://www.mbaknol.com/information-systems-management/data-tampering-meaning-types-and-countermeasures/>.
- OKTA. (2023). IDS vs. IPS: Definitions, Comparisons & Why You Need Both | Okta UK. *www.okta.com*. Available from <https://www.okta.com/uk/identity-101/ids-vs-ips/>.
- OWASP. (2013). SQL Injection. OWASP. Available from https://owasp.org/www-community/attacks/SQL_Injection.
- OWASP. (2019). Cross Site Scripting Prevention · OWASP Cheat Sheet Series. *Owasp.org*. Available from https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html.
- OWASP. (2021). SQL Injection Prevention · OWASP Cheat Sheet Series. *Owasp.org*. Available from https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html.
- Palo Alto Networks. (2018). What is an intrusion prevention system? - Palo Alto Networks. *Paloaltonetworks.com*. Available from <https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips>.
- Pentestmonkey. (2019). Preventing Web-based Directory Enumeration Attacks | pentestmonkey. *pentestmonkey.net*. Available from <https://pentestmonkey.net/blog/direnum>.
- SecurityTrails Team. (2018). 8 tips to prevent DNS attacks. *Securitytrails.com*. Available from <https://securitytrails.com/blog/8-tips-to-prevent-dns-attacks>.
- Sudhanshu Chauhan and Nutan Kumar Panda. (2015). *Hacking Web Intelligence : Open Source Intelligence and Web Reconnaissance Concepts and Techniques*. Burlington: Elsevier Science.
- Watts, S. (2019). How to Address Security Risks with Robots.txt Files. *Search Engine Journal*. Available from <https://www.searchenginejournal.com/robots-txt-security-risks/289719/>.
- Zhong, W. (2019). Command Injection | OWASP. *owasp.org*. Available from https://owasp.org/www-community/attacks/Command_Injection.