Exploit File upload

L'esercitazione si è focalizzata sull'esplorazione delle vulnerabilità di file upload presenti nelle applicazioni web, in particolare utilizzando la DVWA come ambiente di test controllato. L'obiettivo era simulare un attacco reale, sfruttando la vulnerabilità per ottenere l'accesso remoto alla macchina bersaglio.

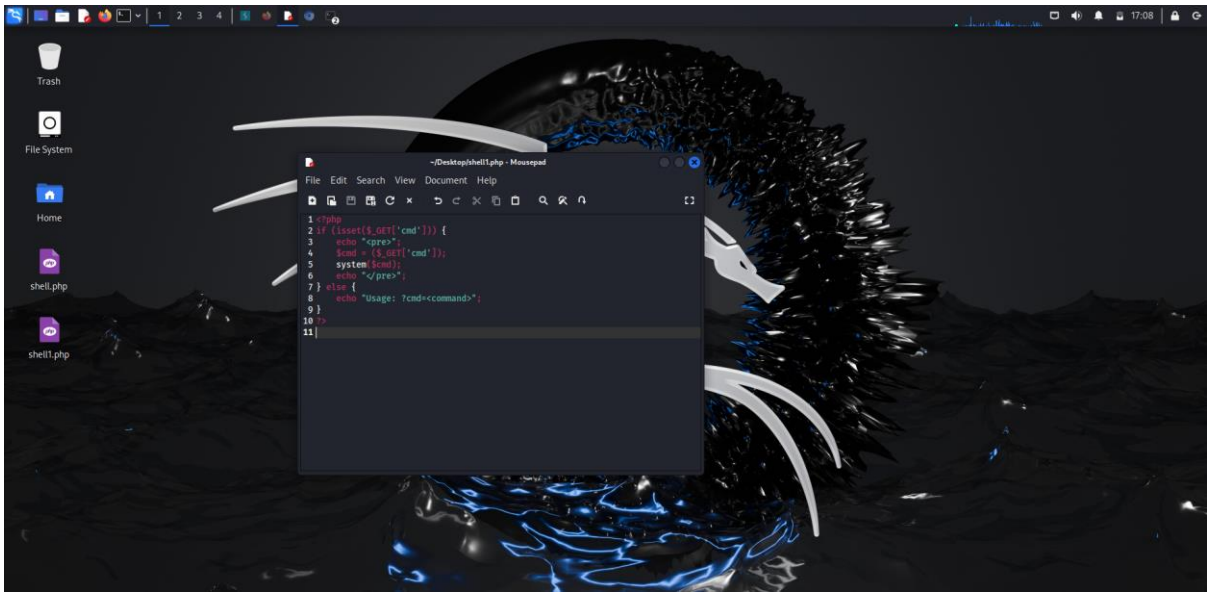
Configurazione dell'Ambiente

- **Ambiente Virtuale:** È stato configurato un ambiente virtuale composto da due macchine: Kali Linux (attaccante) e Metasploitable (bersaglio).
- **Connettività:** È stata stabilita una comunicazione bidirezionale tra le due macchine, assicurando che Kali Linux potesse raggiungere e interagire con Metasploitable. La connessione è stata verificata usando il comando Ping 192.168.1.1

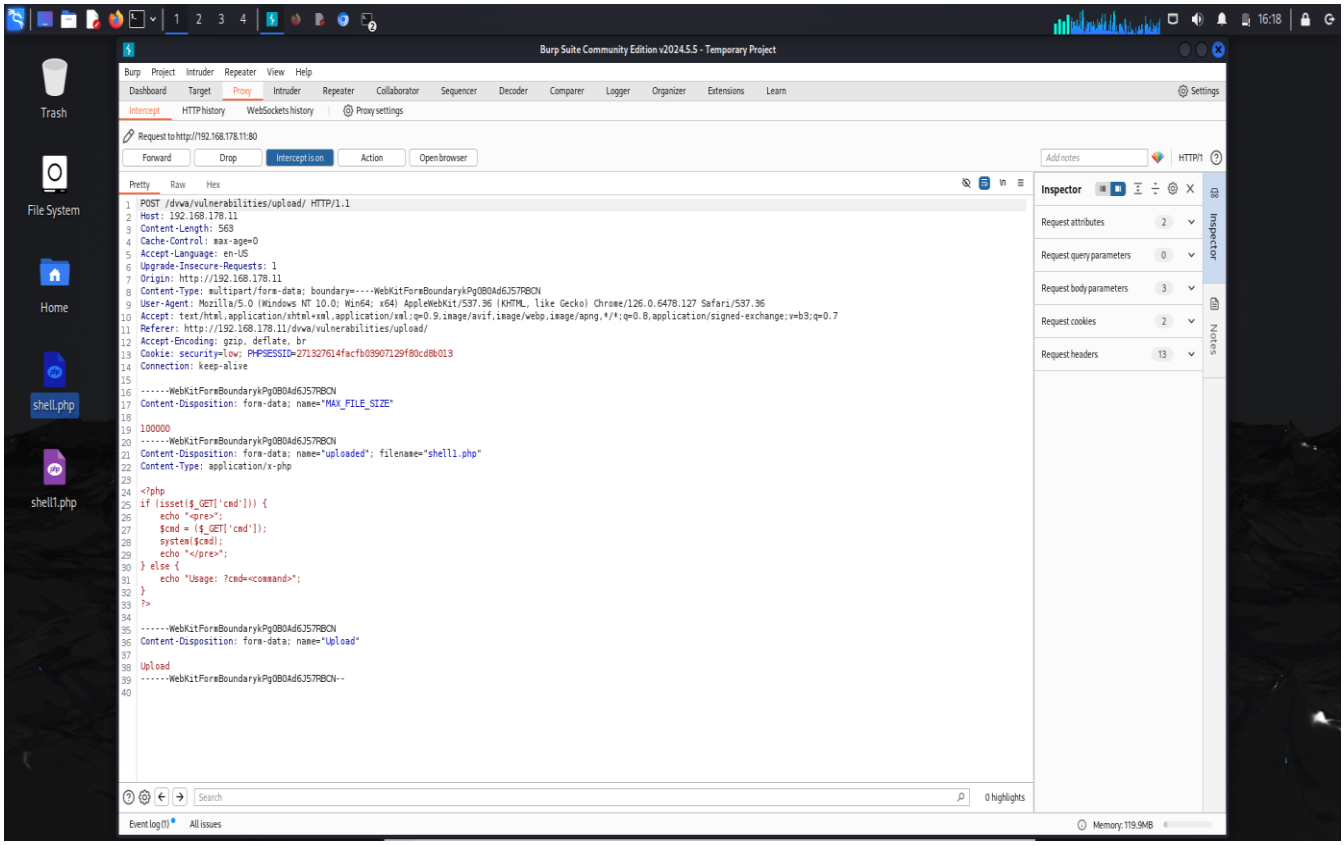
Sfruttamento della Vulnerabilità

- **DVWA:** È stata utilizzata la DVWA, una web application vulnerabile per design, per simulare un ambiente reale.
- **File Upload:** È stata identificata e sfruttata la vulnerabilità di file upload presente nella DVWA.
- **Shell PHP:** È stata caricata una semplice shell PHP attraverso l'interfaccia di upload della DVWA, consentendo l'esecuzione di comandi arbitrari sul server.
- **Controllo Remoto:** Utilizzando la shell, è stato ottenuto il controllo remoto della macchina Metasploitable, eseguendo comandi da remoto come un utente autenticato.

Shell.php



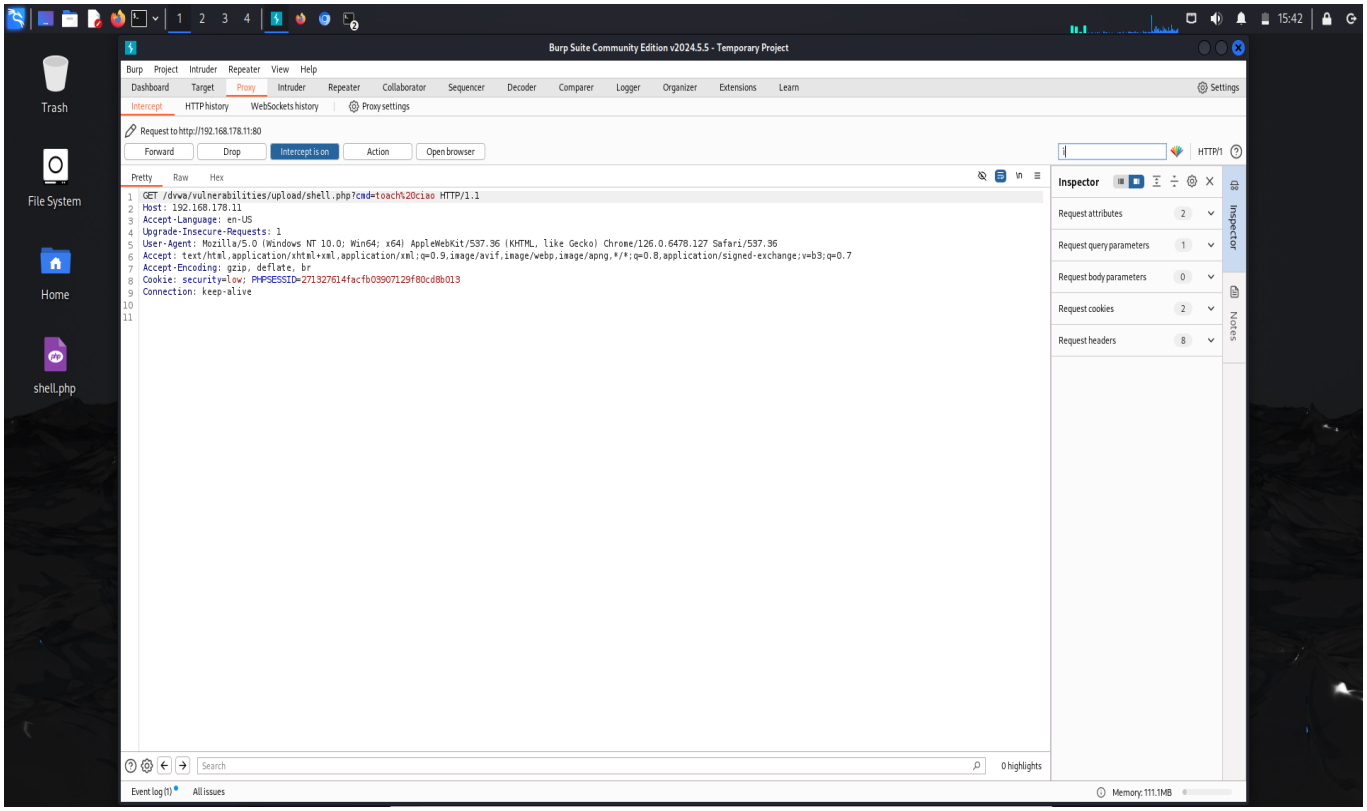
Possiamo vedere la shell caricata nell'immagine, si tratta del codice scritto in rosso dalla riga 24 alla riga 33. L'immagine sottostante è stata presa da BurpSuite tramite l'intercettazione.



Monitoraggio con BurpSuite

BurpSuite è un potente strumento utilizzato dagli esperti di sicurezza informatica, in particolare dai penetration tester, per analizzare la sicurezza delle applicazioni web. È una suite completa che offre una vasta gamma di funzionalità progettate per identificare e sfruttare le vulnerabilità presenti nei siti web.

- **Intercettazione:** BurpSuite è stato utilizzato per intercettare e analizzare tutte le richieste HTTP/HTTPS inviate alla DVWA.
- **Analisi:** L'analisi del traffico ha permesso di comprendere le dinamiche dell'attacco, identificando i punti deboli dell'applicazione e le tecniche utilizzate per sfruttare la vulnerabilità.

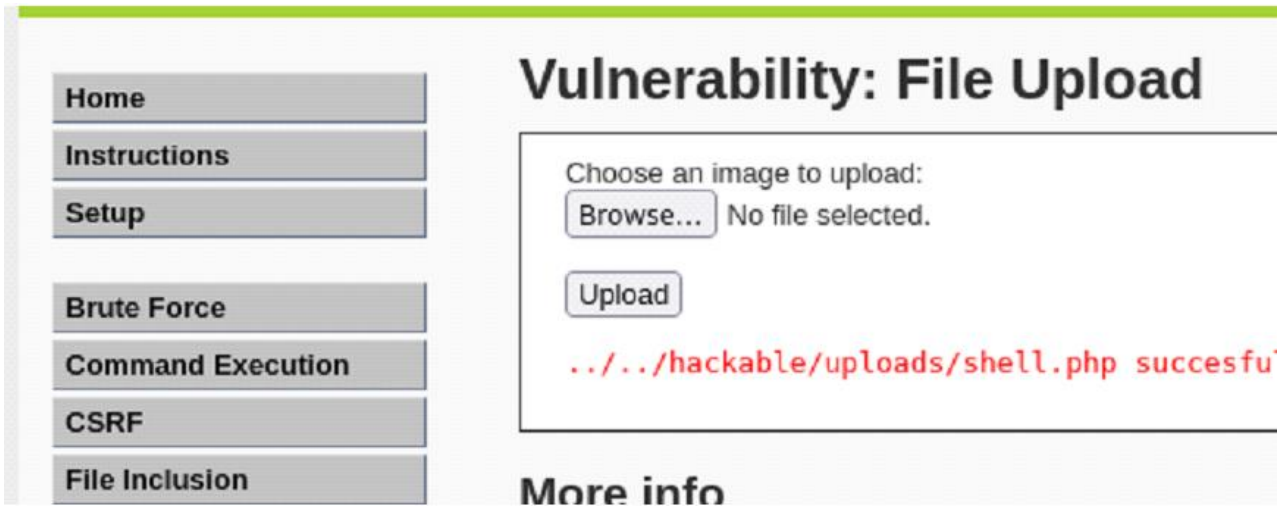


Caricamento della Shell PHP su DVWA

• Scopo: Verificare la possibilità di caricare il file shell.php sulla piattaforma DVWA tramite il modulo di File Upload, sfruttando la vulnerabilità di upload.

• Procedura: Il file shell.php è stato selezionato e caricato tramite la funzionalità di upload presente nella sezione File Upload di DVWA.

• Risultato: Il file shell.php è stato caricato con successo, come confermato dal messaggio di successo visualizzato nell'interfaccia di DVWA



Test della Shell PHP tramite Burp Suite

• Scopo: Utilizzare Burp Suite per intercettare e modificare le richieste HTTP alla shell PHP.

• Azione: Con Burp Suite in modalità Intercept, è stato inserito nel browser l'URL del file caricato, aggiungendo ?cmd=ls alla fine dell'URL per eseguire il comando ls: 192.168.1.1/dvwa/hackable/uploads/shell.php?cmd=ls

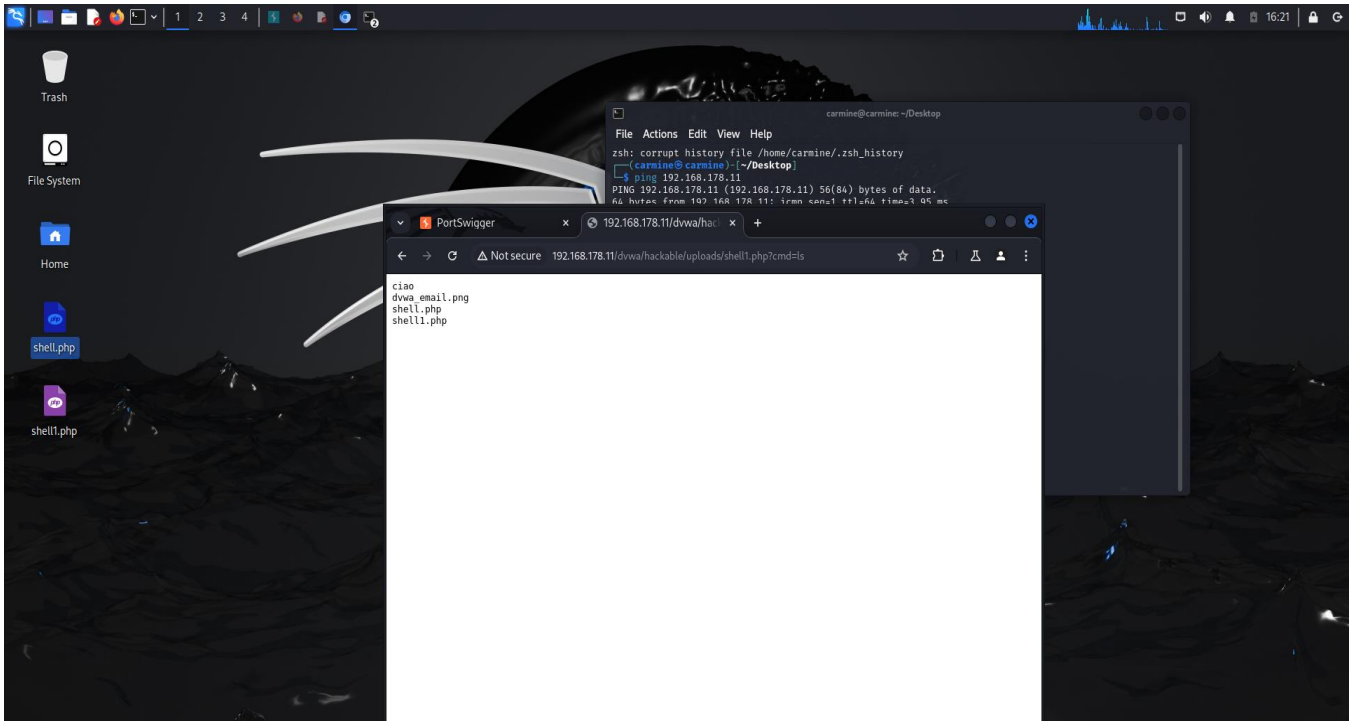
• Risultato: La richiesta è stata intercettata e inoltrata tramite Burp Suite, e l'output del comando ls è stato visualizzato correttamente sulla pagina web.

Esecuzione di Comandi Personalizzati

• Scopo: Verificare la possibilità di eseguire ulteriori comandi tramite la shell PHP caricata.

• Azione: Nella barra degli indirizzi, è stato inserito il seguente comando per creare un file vuoto con il nome "ciao":

• Risultato: Inoltrando la richiesta con Burp Suite, il comando touch ciao è stato eseguito con successo, creando il file "ciao" sul server. Il risultato è stato visibile direttamente attraverso l'interfaccia di DVWA.



Conclusioni

L'esercitazione ha dimostrato come una semplice vulnerabilità di file upload possa essere sfruttata per ottenere un accesso non autorizzato a un sistema. È fondamentale sottolineare l'importanza di implementare adeguate misure di sicurezza per prevenire questo tipo di attacchi, come:

- **Validazione rigorosa dei file caricati:** Verificare il tipo di file, le dimensioni e la presenza di codice malevolo.
- **Restrizione dei permessi:** Limitare i permessi di scrittura ai directory dove vengono caricati i file.
- **Utilizzo di Web Application Firewall (WAF):** Implementare un WAF per rilevare e bloccare gli attacchi comuni.
- **Aggiornamenti regolari:** Mantenere aggiornato il software e le librerie utilizzate