

## Struttura della web shell PHP

L'immagine mostra il codice di `shell.php`, che implementa una semplice web shell in PHP con un form HTML che invia il parametro `cmd` tramite metodo GET allo stesso file.

All'interno dei tag `<pre>` il codice verifica la presenza di `$_GET['cmd']` e lo passa direttamente alla funzione `system`, permettendo l'esecuzione di comandi arbitrari sul sistema operativo della macchina Metasploitable attraverso l'interfaccia web.

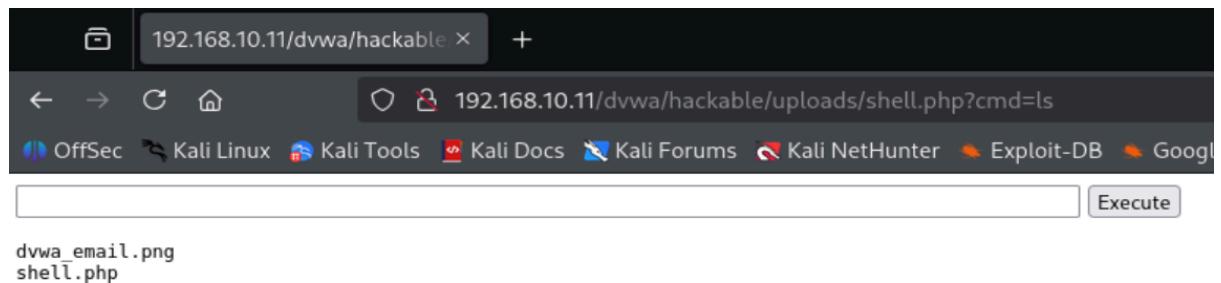
## **Upload della web shell su DVWA**

Name	Last modified	Size	Description
 <a href="#">Parent Directory</a>		-	
 <a href="#">dvwa_email.png</a>	16-Mar-2010 01:56	667	
 <a href="#">shell.php</a>	15-Jan-2026 02:16	347	

Nell' immagine viene mostrata la directory `/dvwa/hackable/uploads/` raggiunta da browser, dove compaiono il file `dvwa_email.png` e la web shell `shell.php` caricata tramite la funzionalità vulnerabile di file upload di DVWA con livello di sicurezza basso.

Questo conferma che il server non applica adeguati controlli sull'estensione dei file o sul contenuto e permette l'upload di codice PHP eseguibile, condizione tipica del laboratorio DVWA per dimostrare la vulnerabilità di upload insicuro.

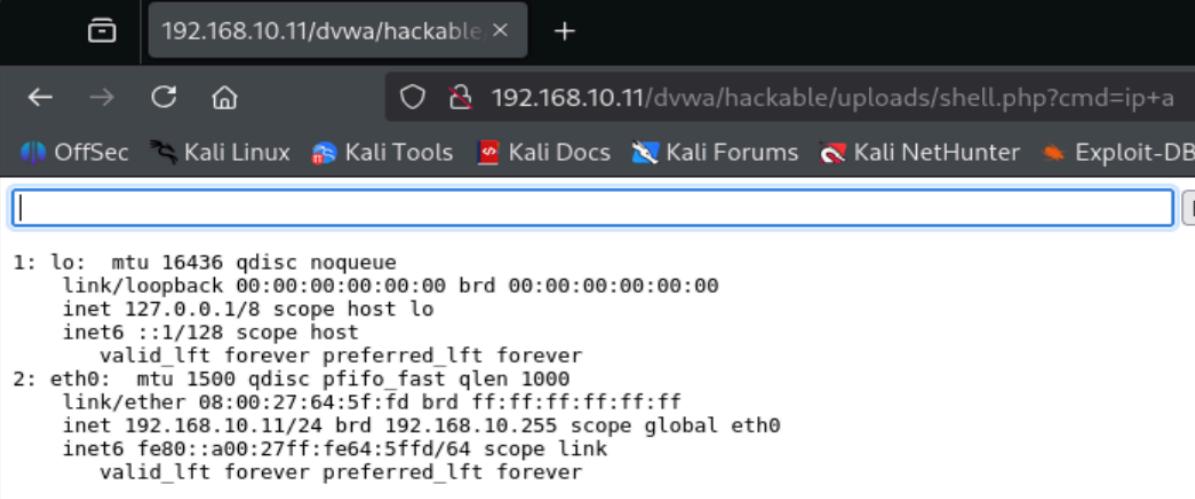
## Esecuzione di comandi remoti



L' immagine illustra l'accesso diretto a `shell.php` all'interno della cartella `uploads` con l'URL che include il parametro `cmd=ls`, il quale restituisce l'elenco dei file presenti nella directory, compresi `dvwa_email.png` e `shell.php` stessa.

Questo dimostra di aver ottenuto una shell di comando sul server web, che ora può essere usata per esplorare il filesystem, scaricare file o lanciare ulteriori comandi di cognizione.

## Raccolta di informazioni sulla macchina bersaglio



The screenshot shows a web browser window with the URL `192.168.10.11/dvwa/hackable`. Below the address bar, there's a navigation bar with icons for back, forward, search, and refresh. The main content area displays the output of the command `ip a`, which lists the network interfaces and their configurations. The output shows two interfaces: `lo` (loopback) and `eth0` (physical interface). The `lo` interface has an IP of `127.0.0.1/8`. The `eth0` interface has an IP of `192.168.10.11/24` and a MAC address of `fe80::a00:27ff:fe64:5ffd/64`.

```
1: lo: mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:64:5f:fd brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.11/24 brd 192.168.10.255 scope global eth0
        inet6 fe80::a00:27ff:fe64:5ffd/64 scope link
            valid_lft forever preferred_lft forever
```

L'ultima immagine mostra l'output del comando `ip a` eseguito tramite la web shell, che elenca le interfacce di rete `lo` ed `eth0` e l'indirizzo IP assegnato alla macchina Metasploitable, in questo caso `192.168.10.11/24` su `eth0`.

Questa informazione dimostra come, a partire da una semplice vulnerabilità di upload, sia possibile ottenere Remote Code Execution e mappare la configurazione di rete del target per pianificare eventuali step successivi di attacco o movimento laterale.