mercoledì 2 ottobre 2024 19:24

Esercizio:

Effettuare il File Upload di una shell ai livelli di sicurezza:

● Medium

● High

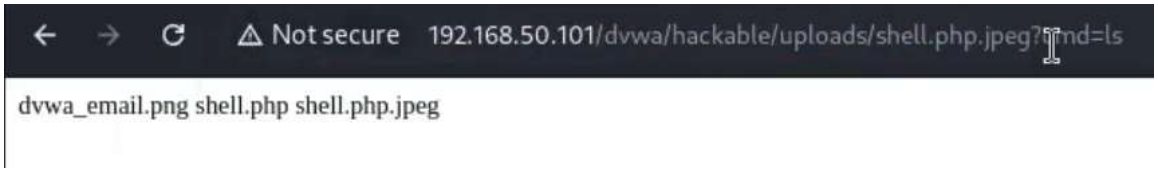
Utilizzare sempre BurpSuite per monitorare tutti gli step.

Questo esercizio può essere svolto in due modi:

1. **Security Medium:** Prendere il file di cui si vuole fare l'upload e tramite BurpSuite, intercettare la richiesta per poi modificare il Content-Type del file caricato, in modo tale che risulti essere un immagine in formato jpeg o jpg, in quanto per questo livello di sicurezza vengono accettati solo questi file.

```
100000
------WebKitFormBoundaryzWYDsUyReUGNxPAb
Content-Disposition: form-data; name="uploaded"; filename="shell.php"
Content-Type: image/jpeg
```

come possiamo vedere dalle immagini sotto il nostro file è stato caricato con successo e la nostra richiesta è stata eseguita



1. **Security High:** Differentemente dal medium in questo livello di sicurezza non basterà cambiare solamente il Content-Type ma anche il nome del file in jpeg o jpg in modo da ingannare la richiesta, per farlo leggere come se fosse appunto, un file jpg o jpeg.

```
------WebKitFormBoundaryGDxwpc4fMPNZ8DQY
Content-Disposition: form-data; name="uploaded"; filename="shell.php.jpeg
"
Content-Type: image/jpeg
```

2. La seconda soluzione è valida per entrambi i livelli di sicurezza e basta semplicemente cambiare il nome del file in **.jpg**