Exploit File upload

Consegna:

1. Codice php

2. Risultato del caricamento (screenshot del browser)

3. Intercettazioni (screenshot di burpsuite)

4. Risultato delle varie richieste

Per prima cosa abbiamo creato un file .php con il codice che segue nell’immagine caricato all’interno del fileA computer screen shot of a computer program

Description automatically generated

Nella fase successiva siamo andati su burpsuite e cercato nel suo browser di ricerca l’ip di dvwa e cosi siamo stati indirizzati alla pagina di dvwa

Di seguito abbiamo messo la sicurezza su low per poter risolvere l’esercizio

Caricato il file shell.php su upload cliccato su forward da burpsuite

E abbiamo ottenuto il risultato nella seguente foto, quindi ci è apparso in rosso un percorso che andremo a copiare nell’url appena dopo dvwa/ (come vediamo in foto burpsuite intercetta sempre tutto quello che succede)

A screenshot of a computer

Description automatically generated

Dopo aver ricopiato il percorso sull’url abbiamo aggiunto il ?cmd=ls cosi facendo stiamo dando dei comandi a dvwa direttamente dall’url (perché si tratta di un metodo GET)

Il risltato sarà che dvwa ci porta alla pagina caricata successivamente ( da notare burpsuite che tiene traccia di tutto)

Con il coamndo ls abbiamo detto di mostrarci una lksta di cio che è presente all’interno di dvwa

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Terminato l’esercizio ho provato a creare un file di testo per vedere se i comandi che riportavo andassero a creare altro all’interno della dvwa

Il risltutato è statto un file con scritto ciao al suo interno che è venuto stampato in questo modo

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Questo è solo un esempio di cosa si puo fare con