Mercredi 3 Décembre 2025

Bienvenue!

SÉANCE 09: DVWA (Partie 1) : File Inclusion

La room du jour

https://tryhackme.com/room/dvwa

File inclusion :

Machine potentiellement vulnérable : Applications exécutant des scripts au runtime (ex : php, javascript).
Si mal sécurisé, il peut être possible de controller le fichier exécuté sur la cible

LFI : Local File Inclusion

Le fichier est sur la machine cible.

Exemples d'utilisation :

- Récupérer des données sensibles sur la machine cible – Attaque par **directory traversal**
- Exécuter un code injecté par une autre vulnérabilité (ex : File Upload)

RFI : Remote File Inclusion

Le fichier est téléchargé depuis un serveur distant puis exécuté par la machine cible. Exemples d'utilisation :

- Obtenir un reverse shell
- ...

Mais, Souvent une RFI est impossible

DVWA : Damn Vulnerable Web Application

DVWA : Un environnement didactique (sur une VM ou en local)

Trois niveaux de difficulté :
Low / Medium / High
(+Impossible)

Une multitude de vulnérabilités :

- File injection
- Brute force
- File upload
- SQL injection

...

Outils utiles :

Liste de PHP wrapper :

file:// — Accessing local filesystem
http:// — Accessing HTTP(s) URLs
ftp:// — Accessing FTP(s) URLs
php:// — Accessing various I/O streams
data:// — Data (RFC 2397)
glob:// — Find pathnames matching pattern
expect:// — Process Interaction Streams

Création d'un serveur python dans le répertoire local:

```
python -m http.server [port]
```

Ecouter sur un port :

```
nc -lvp [port]
```

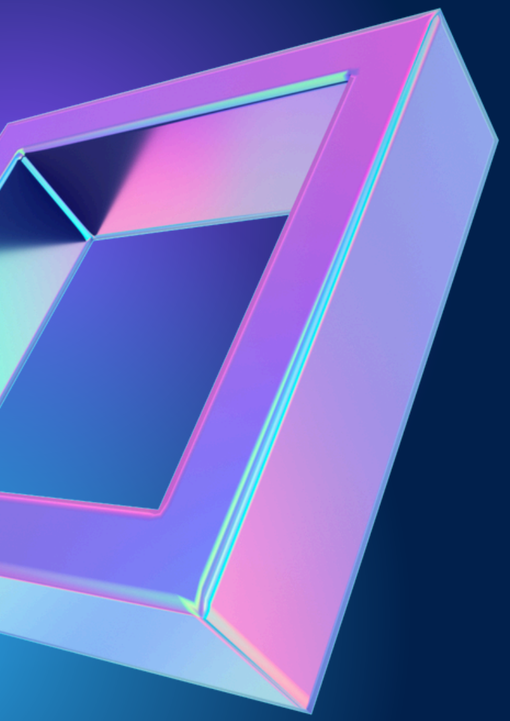
Encoder un fichier en base 64 avec des wrapper:

php://filter/convert.base64-encode/resource= [Fichier]

Root par défaut d'un serveur web : /var/www/html

Exemple d'attaque par directory traversal :

http://exemple.com/?page=../../../../../../../../etc/passwd



Merci et à la semaine prochaine !

La séance sur notre Github:
https://github.com/CyberMines-Nancy/SEANCES

@cyber.mines