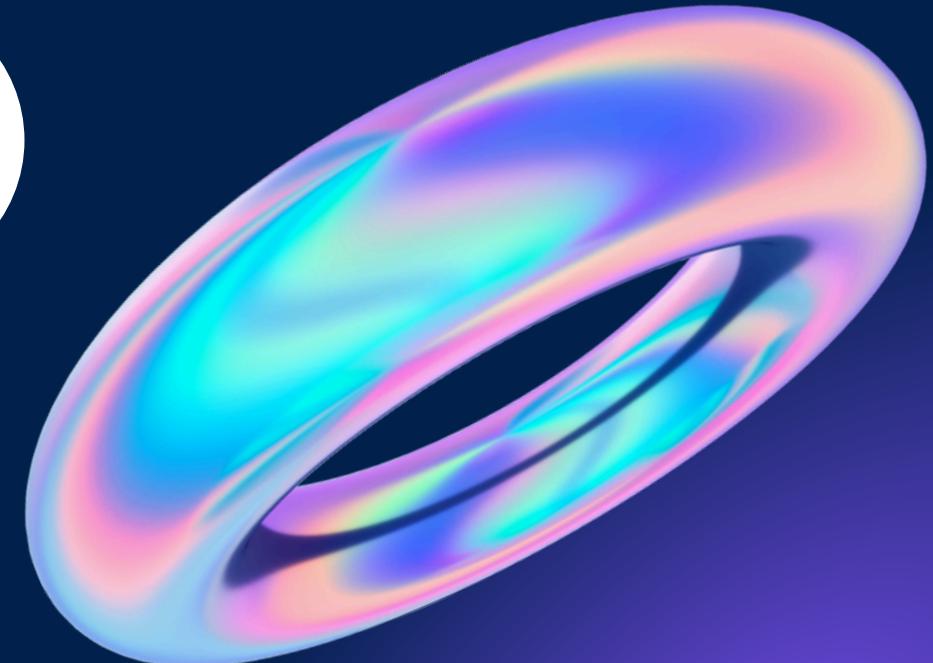


Mercredi 28 janvier 2026

Bienvenue!

SÉANCE 10: Web Vuln -
Command Injection



Qu'est-ce que l'injection de commande ?

- Exécution de commandes (système) arbitraires sur le serveur via une application vulnérable.
 - Les entrées de l'utilisateur sont directement passées à un interpréteur de commande (shell).



8.8.8.8

User



ping 8.8.8.8

Server

Pourquoi ça existe ?

- Confiance excessive en l'entrée utilisateur
- Utilisation de fonction dangereuses/à risque:
 - PHP: system(), exec().
 - Python: os.system().
- Absence/Insuffisance de filtrage

Où on peut la retrouver ?



- URL, via les paramètres:
<http://target.com/?param=value>
- Éléments recevant des entrées utilisateur.
- Outils d'automatisation/ CD-CI (Jenkins, GitLab,...)



Technique Commune

Chaining commands

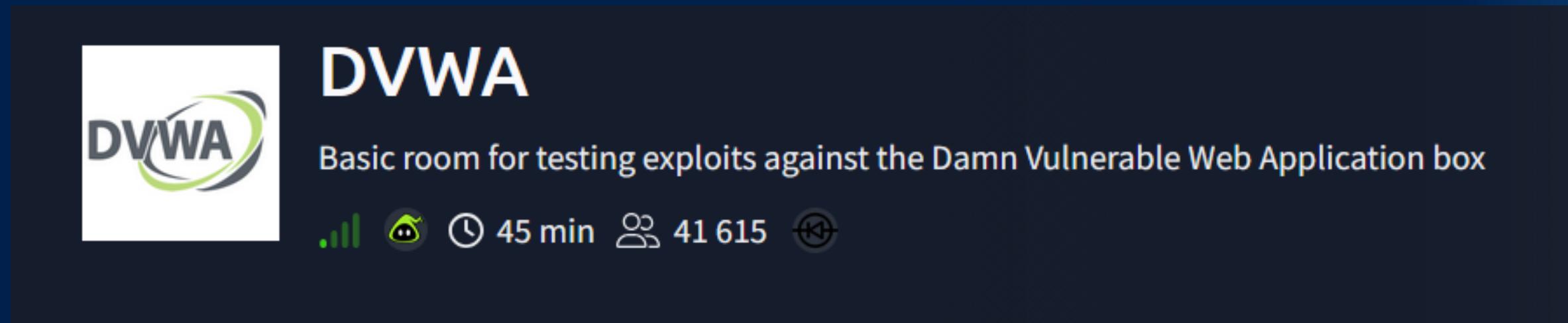
- Avec ; → cmd1; cmd2 → cmd2 s'exécute toujours
- Avec & → cmd1 & cmd2 → cmd1 s'exécute en bg.
- Avec && → cmd1 && cmd2 → cmd2 s'exécute si cmd1 réussie
- Avec | → cmd1 | cmd2 → utilise l'output de cmd1 en tant qu'input pour cmd2
- Avec || → cmd1 || cmd2 → cmd2 s'exécute si cmd1 échoue



Loot après RCE

- **Identités et comptes utilisateurs:**
 - **cat /etc/passwd**
 - **id, whoami**
 - **Fichiers de configuration web:**
 - **configuration.php,...**
 - **contient des credentials (DB,...)**
 - **Fichiers .txt, .sql,...**
- 

La room du jour

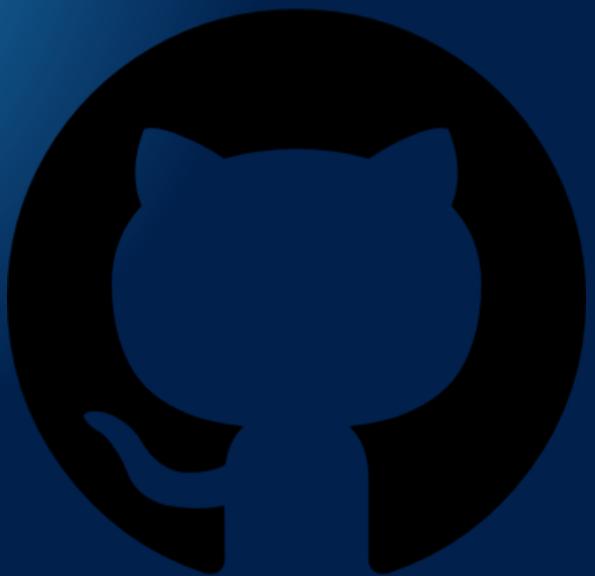


<https://tryhackme.com/room/dvwa>

Remédiations

- Utilisation de whitelist (et non de blacklist)
- Validation de l'entrée utilisateur.

Approfondissements



- [PayloadAllTheThings](#)
- [Burp Suite Academy](#)

Merci et à la semaine prochaine !



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



@cyber.mines