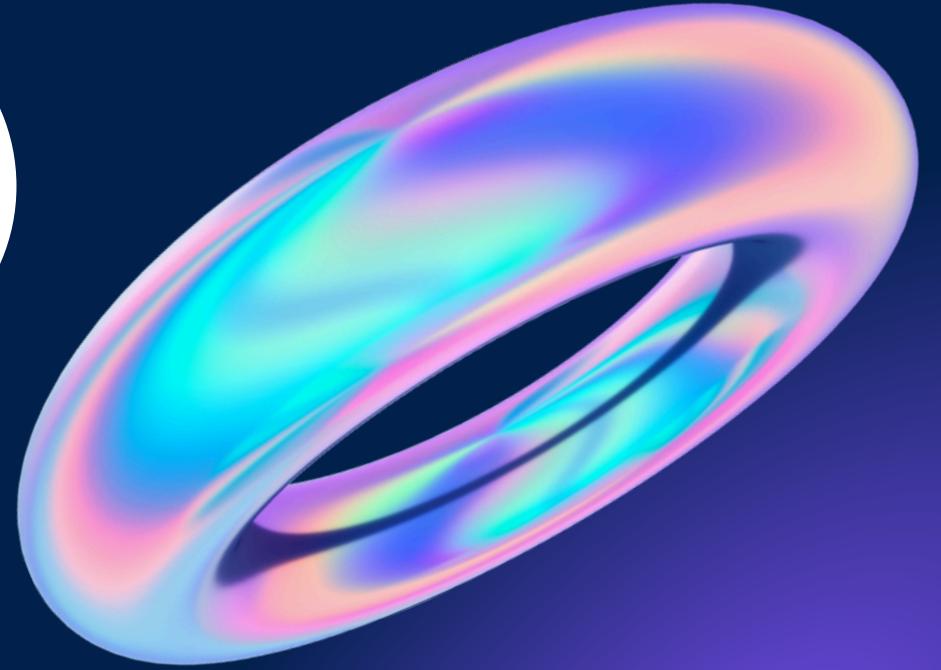


Mercredi 13 novembre 2024



Bienvenue!

SÉANCE 08: Exploitation des
failles de formulaire : Obtenir un
Reverse Shell



BurpSuite

BurpSuite est une plateforme intégrée utilisée pour **tester la sécurité des applications web**. Elle offre des outils puissants pour **déetecter** et **exploiter** les **vulnérabilités**.

BurpSuite

Fonctionnalités clés :

- **Intercept** : Capture le trafic entre votre navigateur et le serveur pour examiner et modifier les requêtes HTTP.
- **Repeater** : Permet de répéter une requête pour tester différentes configurations manuellement.
- **Intruder** : Automatise des tests d'intrusion pour tester diverses combinaisons de paramètres.

Plus d'informations : <https://tryhackme.com/module/learn-burp-suite>

BurpSuite

Objectifs de BurpSuite dans la room d'aujourd'hui :

- **Intercepter** les requêtes pour identifier et analyser le formulaire d'upload de fichiers.
- **Tester** différentes extensions pour détecter les fichiers autorisés.

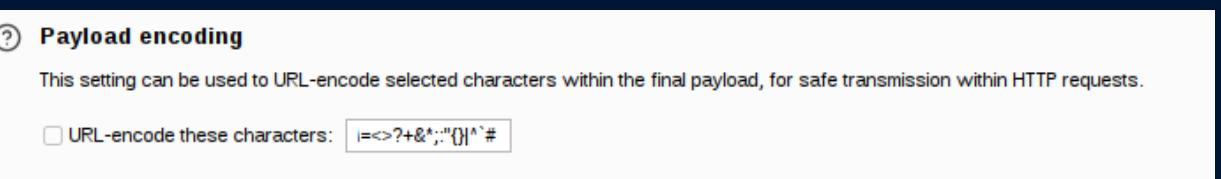
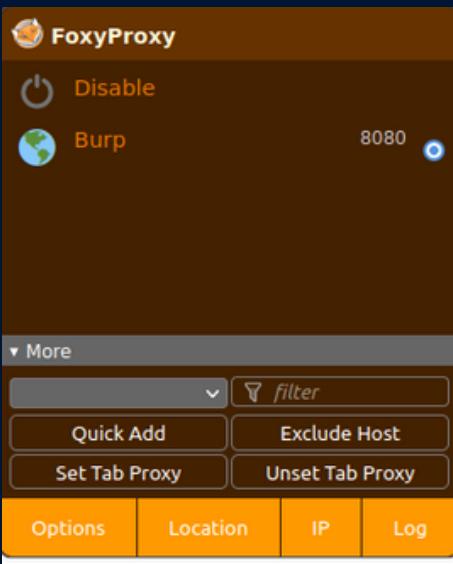
Étapes avec Burp Suite :

- **Interception des requêtes** : Utilisez l'intercepteur de BurpSuite pour capturer les requêtes d'upload et examiner les paramètres d'extension.
- **Modification et envoi de fichiers** : Changez les extensions ou paramètres dans l'outil Intruder pour tester plusieurs formats
- **Analyse de la réponse** : Repérez les réponses du serveur pour savoir quelles extensions sont acceptées ou rejetées, et déterminer celle qui déclenche l'exécution du fichier.



Astuces

- Activez le profil de Burp en cliquant sur celui-ci dans FoxyProxy. Cela redirigera tout le trafic du navigateur vers Burp.
- Décochez la case "URL-encode these characters" avant de lancer l'attaque dans Intruder
- N'hésitez pas à explorer certains fichiers standards pour y trouver le nom de l'utilisateur.
- N'oubliez pas d'utiliser GTFOBins pour l'escalade de privilèges !



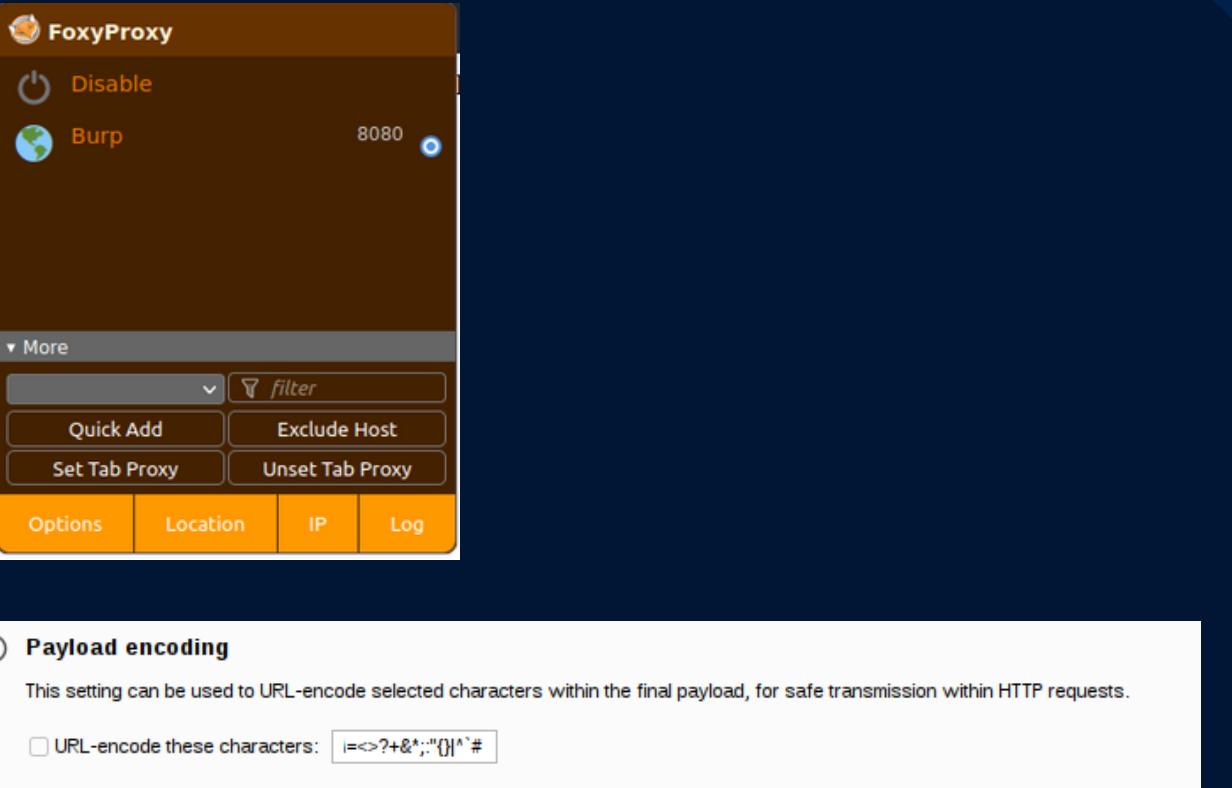
La room

<https://tryhackme.com/r/room/vulnversity>



Astuces

- Activez le profil de Burp en cliquant sur celui-ci dans FoxyProxy. Cela redirigera tout le trafic du navigateur vers Burp.
- Décochez la case "URL-encode these characters" avant de lancer l'attaque dans Intruder
- N'hésitez pas à explorer certains fichiers standards pour y trouver le nom de l'utilisateur.
- N'oubliez pas d'utiliser GTFOBins pour l'escalade de privilèges !



<https://gtfobins.github.io/gtfobins/systemctl/>

Commande pour récupérer le flag :

```
TF=$(mktemp).service
echo '[Service]
Type=oneshot
ExecStart=/bin/sh -c "cat
/root/root.txt > /tmp/output"
[Install]
WantedBy=multi-user.target' > $TF
/bin/systemctl link $TF
/bin/systemctl enable --now $TF
```

Merci et à la semaine prochaine !



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



@cyber.mines