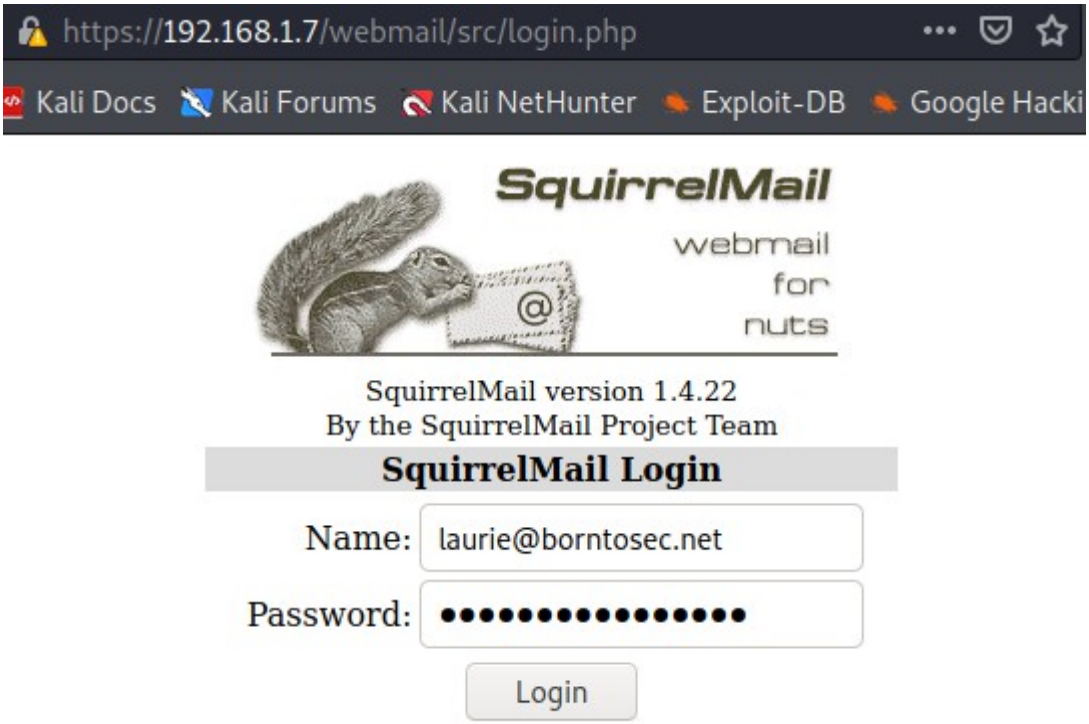
SQUIRRELMAIL RCE

Boot2root writeups

REMARQUE :

Ce writeup est une **variante** du premier writeup (CTF). Attention, la technique décrite dans ce writeup ne peut fonctionner dans le cadre d'un environnement d'entraînement simulé comme boot2root, car **SMTP n'est pas setup** (voir l'explication ci-dessous). La méthode aurait cependant fonctionnée dans un scénario "réel" de production, c'est pour cela que je le trouvais intéressant.

Dans le **writeup1**, a l'étape "Webmail scrapping", on dispose de credentials pour se connecter au serveur mail au path **/webmail** :



Dans le writeup classique, on se connectait, puis on récupérait des credentials **phpmyadmin** dans les mails reçus afin de drop une webshell.

Mais on aurait également pu remarquer ici que le software utilisé pour faire tourner le serveur mail est **SquirrelMail en version 1.4.22**. Cette version est vulnérable à CVE-2017-7692, une vulnérabilité de type RCE :
https://legalhackers.com/advisories/SquirrelMail-Exploit-Remote-Code-Exec-CVE-2017-7692-Vuln.html
https://legalhackers.com/videos/SquirrelMail-Exploit-Remote-Code-Exec-CVE-2017-7692-Vuln.html

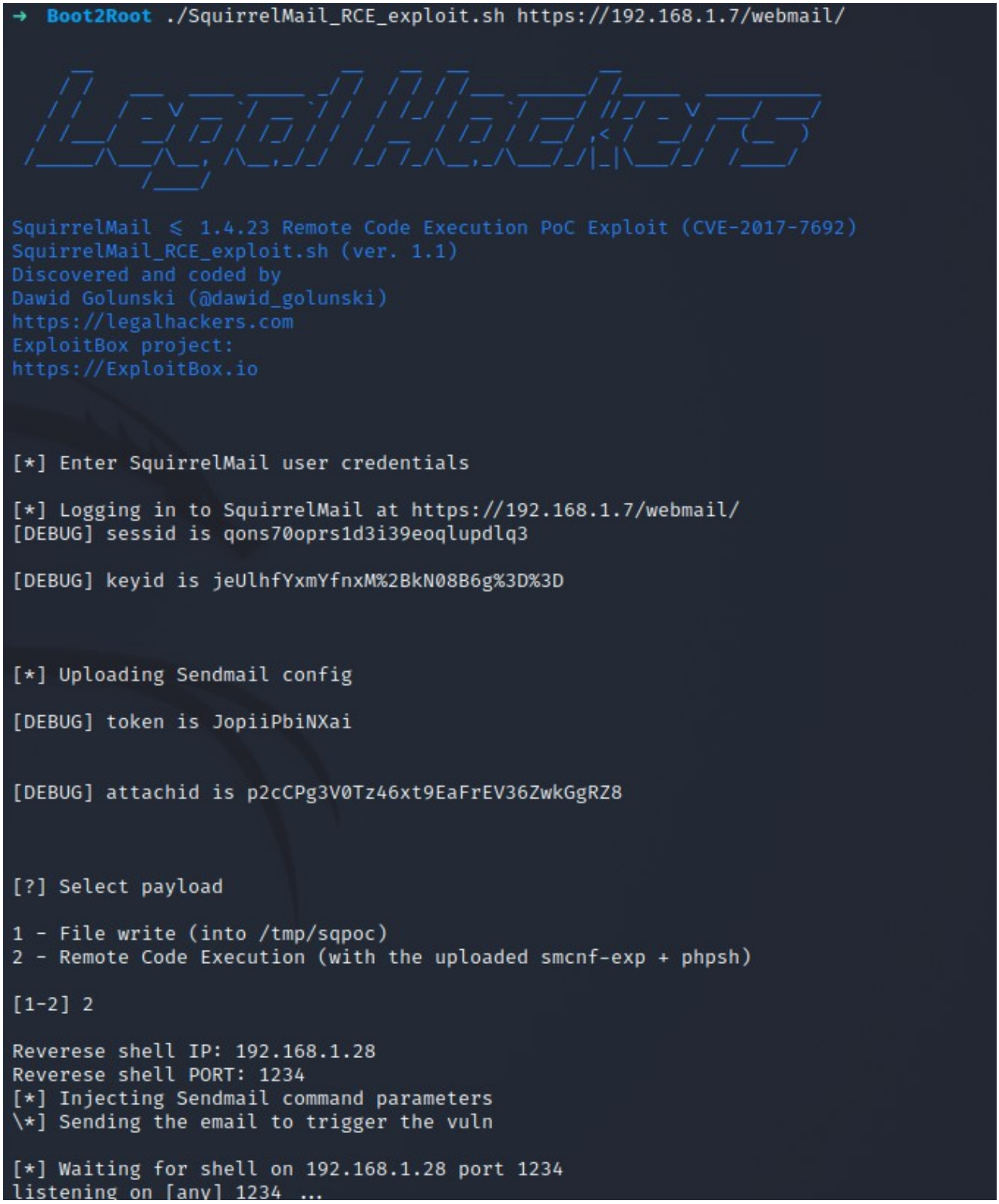
Un exploit publique est disponible. Il ne peut cependant pas fonctionner tel quel, il faut le modifier un peu afin :

- D'éviter les erreurs dûs aux caractères spéciaux du mot de passe de l'utilisateur laurie@borntosec.net.

- D'adapter les commandes curl effectuées à HTTPS (donc en gros rajouter un flag **-k**).

La version fonctionnelle de l'exploit dans notre cas de figure est celle présentée dans les scripts, **SquirrelMail_RCE_exploit.sh**.

Avec nos modifications, l'exploit fonctionne correctement **jusqu'à la dernière étape** (l'upload de la config fonctionne, de même que l'étape cruciale de l'injection des paramètres **sendmail**) :



On ne reçoit cependant pas la reverse shell, pour la simple raison suivante : le serveur mail est un

simple serveur de test / une simulation dans le cadre de l'exercice, et il ne permet pas réellement d'envoyer de mails par le bias de la commande **sendmail** car **SMTP n'est pas configuré** :

Si le flux SMTP avait été disponible et donc que **SquirrelMail** avait été véritablement fonctionnel, l'exploit aurait complété (la version est vulnérable, et l'injection des paramètres sendmail était réussie) ; cependant, puisqu'il s'agit d'un environnement de test, on ne peut trigger réellement la reverse shell.

Dans tous les cas, dans un réel environnement de production, on aurait pu utiliser cette technique alternative à l'upload de webshell via phpmyadmin pour récupérer plus simplement une reverse shell en tant que l'utilisateur **www-data**.