Rapport TP Webapp TimeKORP

Table des matières

Rapport TP Webapp TimeKORP

By Clement ALLEGRE–COMMINGES and PETIT Lucien

Sommaire

Introduction

Pour ce deuxième exercice, l'objectif est d'obtenir un drapeau d'un site qui sera hébergé dans un conteneur docker sur notre Raspberry PI.

1. Approche boîte noire

Après avoir effectué l'installation du serveur cible sur notre Raspberry Pi en suivant les instructions données. Nous avons commencé à explorer les pages web nouvellement disponibles.

Nous y avons repéré les URL sur les 2 pages disponibles suspectes :

— `http://192.168.1.200:1338/?format=%H:%M:%S`
— `http://192.168.1.200:1338/?format=%Y-%m-%d`

Notamment la partie `format=%Y-%m-%d` et `format=%H:%M:%S`.

Nous avons alors essayé de modifier la partie format de l'url pour observer la réaction du site.

Avec `format=%H:%M:%S`le site nous retourne `>It's 10:24:25.` Avec `format=helloworld` le site nous retourne `>It's helloworld.`

Nous en avons déduit une stratégie d'attaque consistant à injecter une commande via cette URL pour être exécutée par le serveur.

Nous avons essayé avec du javascript en tâtonnant, cependant nous n'avons pas réussi à avoir de résultat autre que `time format incorect : --help for more information`.

2. Approche boîte blanche

Nous avons donc changé notre méthode d'approche de l'approche en boite noir à une approche en boite blanche. Nous avons trouvé dans les fichiers du serveur un fichier README.md qui nous a informé que nous cherchions bien dans la bonne direction. L'objectif étant d'injecter une commande dans l'url pour obtenir le drapeau. Nous avons ainsi obtenu l'url suivante :

`http://192.168.1.200:1338/?format=%25H%3a%25M%3a%25S%27%20%7Ccat%20/flag%20/%20/%20%23`

qui nous renvoie : `>It's Poly{t1m3_f0r_th3_ult1m4t3_pwn4g3}.`

Même si nous n'avons pas réussi à trouver le format de l'url nécessaire, nous sommes parvenus à obtenir la bonne approche en analysant le comportement de la page web.

Conclusion

Nous pouvons conclure sur ce premier exercice dont l'objectif est la "confidentialité" aka le flag en utilisant une attaque basée sur une injection de code via l'url.

Nous noterons aussi que cette attaque est rendue possible uniquement grâce au code du serveur qui est fragile.