Hacking et Pentesting

Mai 2021 | **Serie 6**

Stéphane Küng

1 Administratif

Ce travail **individuel** doit être rendu avant la date indiquée sur le ScoreBoard au format **PDF** sur CyberLearn.

1.1 Clarification

Dans vos rapports d'exercices, faites attention à bien inclure:

- Captures d'écran de réussite
- Payload utilisés
- Tout code source utilisé pour l'exploitation (ou en annexe)
- Nom des outils utilisés

1.2 Proxy 0

Entrainement

Familiarisez-vous en premier avec un outil de proxy[1] en jouant avec les requêtes envoyées et reçues depuis votre navigateur. Modifiez ainsi les valeurs envoyées et reçues par l'application Web.

1.3 Proxy 1

Pour ce challenge vous devez modifier les données reçues/envoyées en `HTTPS` d'une application mobile[2] avec un outil de proxy de sorte à changer les informations affichées à l'écran. Exemple :

- accès à un menu
- score de jeu modifié
- température farfelue
- pièces ou diamants gratuits
- ...

Choisissez une application ni trop populaire, ni trop récente ou venant d'un éditeur trop exposé. Vous risquez d'être bloqué par du `certificate pinning`, mais on pourrait être surpris.

Il vous faudra :

- Configurer le proxy de votre téléphone mobile
- Déployer le certificat du Proxy sur votre téléphone portable
- Modifier les informations envoyées ou reçues lors de requêtes faites par l'application.
- Analyser le résultat à l'écran (**captures**)
- Documenter ce que vous avez fait

[1] Burp Suite, Charles Proxy, Zed Attack Proxy, mitmproxy, ...

[2] Android et dérivés, iOS, WindowsPhone, BlackBerry, Tizen, Sailfish OS, Palm OS, Symbian, (Il est possible d'utiliser un émulateur Android si besoin)

1.4 Proxy 2

Pour ce challenge **à but éducatif** essayez de trouver une application mobile simple, mais **différente du challenge Proxy 1** et d'accéder à son `API HTTPS` utilisée derrière (Sport, Météo, Programme TV, News, Champignons, Aviation, ...) dans une mini application[3] à vous.

Exemple : Script Python qui affiche les vols au départ d'un aéroport désiré. `API` que vous avez récupérée grâce à un outil de proxy depuis une application mobile.

- Incluez votre code source dans le rapport ou en annexe

1.5 Proxy 3

Ajoutez à votre code (du **Proxy 2**) une fonction de vérification du certificat (`certificate pinning`) lors de l'ouverture de la connexion. Utilisez le certificat valide actuel comme référence. Puis tentez avec un outil de proxy d'intercepter les données. Montrez que votre code détecte bien cette interception et l'empêche de fonctionner.

1.6 Certificate Pinning Bypass (difficile)

Trouvez une application mobile qui effectue du certificate Pinning (quasiment n'importe quel jeu populaire), et trouvez un moyen de contourner la protection de certificate pinning ou de quand même modifier les valeurs envoyées.

Vous pouvez par exemple :

- Modifier l'application APK et retirer ou modifier la protection.
- Avec des outils de debug (comme Frida) sur Android, faire des hooks sur les fonctions appelées par l'application et modifier les valeurs retournées/envoyées (peut nécessiter de root le téléphone).
- Il est possible de réaliser 2x ce challenge depuis deux OS mobiles différents (1x iOS et 1x Android par exemple).

[3] Langage libre : C#, Java, Python, Go, Rust, ...