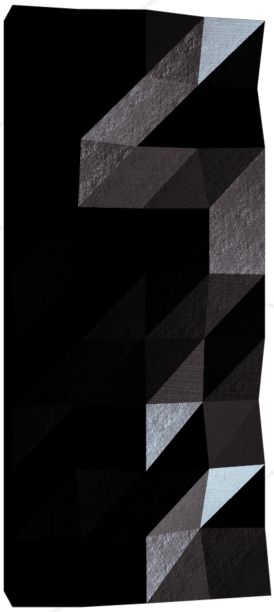

Project SECURITE

Darkly

42 Staff pedago@staff.42.fr

Résumé: Ce projet est une introduction à la sécurité en informatique dans le domaine du Web.

Table des matières

Chapitre I

Préambule

There is something wrong..

Chapitre II

Introduction

Lorsque vous développez vos premiers sites web, vous n'avez généralement pas la moindre idée des vulnérabilités existantes dans le monde du web.

Ce petit projet a pour but de combler ce manque : vous allez prendre conscience de ces vulnérabilités en faisant un audit d'un site web simple. Ce site présente des failles encore régulièrement présentes sur des sites que vous visitez tous les jours.

Voici donc une grosse introduction aux vulnérabilités générales que l'on retrouve dans le monde du web.

Chapitre III

Objectifs

Ce projet a pour but de vous faire découvrir la sécurité en informatique dans le domaine du web.

Vous allez pouvoir découvrir OWASP, qui est, ni plus ni moins, le plus gros projet de sécurité web à ce jour.

Vous allez aussi comprendre ce que beaucoup de frameworks font de manière automatique et complètement transparente pour vous.

Chapitre IV

Consignes générales

- Ce projet ne sera corrigé que par des humains.
- Vous pouvez être amené, durant votre soutenance, à prouver vos résultats. Il faut vous y préparer.
- Vous allez devoir utiliser une machine virtuelle (i386) pour valider ce projet. Une fois votre machine lancée avec l'ISO fourni avec le sujet, si tout est bien configuré, vous aurez un simple prompt avec une IP :

- Vous avez uniquement besoin de choisir votre navigateur pour y lancer l'adresse ip affichée.
- Merci de prévenir la pédago si vous trouvez un bug !
- Vous pouvez poser vos questions sur le forum, sur jabber, IRC, slack...

Chapitre V

Partie obligatoire

- Votre dossier de rendu ne doit contenir que les choses qui vous ont permises de résoudre chacune des failles exploitées.

- Votre rendu sera de la forme :

```
$> ls -al
[..]
drwxr-xr-x 2 root root 4096 Dec 3 XX:XX {Nom de faille}
[..]
$> ls -alR {Nom de faille}
{Nom de faille}:
total 16
drwxr-xr-x 3 root root 4096 Dec 3 15:22 .
drwxr-xr-x 6 root root 4096 Dec 3 15:20 ..
-rw-r--r-- 1 root root  5 Dec  3 15:22 flag
drwxr-xr-x 2 root root 4096 Dec 3 15:22 Ressources

{Nom de faille}/Ressources:
total 8
drwxr-xr-x 2 root root 4096 Dec 3 15:22 .
drwxr-xr-x 3 root root 4096 Dec 3 15:22 ..
-rw-r--r-- 1 root root  0 Dec  3 15:22 whatever.wahtever
$> cat {Nom de faille}/flag | cat -e
XXXXXXXXXXXXXXXXXXXXXXXXXXXX$
$>
```

- Dans le dossier Ressources vous placerez tout ce dont vous aurez besoin pour prouver votre résolution en soutenance.

ATTENTION: Tout ce qui est présent dans ce dossier doit pouvoir être expliqué clairement sans aucune hésitation. AUCUN binaire ne doit être présent dans ce dossier.

- Si vous avez besoin d'utiliser un fichier spécifique présent sur l'ISO du projet, vous devez le télécharger en soutenance. Vous ne devez sous aucun prétexte mettre celui-ci dans votre dépôt.

- Dans le cas d'utilisation d'un logiciel spécifique externe, vous devez préparer un environnement spécifique (VM, docker, Vagrant).

- Dans le cadre de votre partie obligatoire, vous devez compléter 14 failles différentes.
- Lors de votre soutenance, dans certains cas, il vous sera demandé des possibles fix pour les failles que vous avez exploitées. Il est donc fortement conseillé de bien comprendre tout ce que vous exploitez.
- Savoir expliquer est souvent plus important que l'exploitation en elle-même : prenez bien le temps de comprendre, et surtout de faire en sorte que vous puissiez être compris clairement.

Pour les malins (ou pas)... Bien sûr vous n'avez pas le droit d'utiliser des scripts type sqlmap dans le but de rendre triviale l'exploitation. Vous devrez de toute façon expliquer clairement votre démarche durant votre soutenance.

Chapitre VI

Partie bonus

Les bonus ne seront comptabilisés que si votre partie obligatoire est PARFAITE. Par PARFAITE, on entend bien évidemment qu'elle est entièrement réalisée, et qu'il n'est pas possible de mettre son comportement en défaut, même en cas d'erreur aussi vicieuse soit-elle, de mauvaise utilisation, etc ... Concrètement, cela signifie que si votre partie obligatoire n'est pas validée, vos bonus seront intégralement IGNORÉS.

Dans le cadre de votre partie bonus, vous devez simplement fournir des explications avancées pour les failles les plus reconnues que vous aurez rencontré.

Chapitre VII

Rendu et peer-évaluation

Rendez-votre travail sur votre dépot `GiT` comme d'habitude. Seul le travail présent sur votre dépot sera évalué en soutenance.