Alban Gabillon
Université de la Polynésie Française
Punaauia
+68940803880
Alban.gabillon@upf.pf

SQL injection and XSS attack

Alban Gabillon

1 BURP SUITE

1.1 Prérequis

Dans ce TP, vous allez effectuer quelques attaques dans le cadre de l'académie de sécurité web du site portswigger.net.

- Créez un compte sur https://portswigger.net/
- Installez Burp Suite (version gratuite)

Notes :

- Certaines attaques peuvent être réalisées sans utiliser Burp Suite (en manipulant l'URL) notamment les attaques par injection SQL
- Pour chaque exercice, vous devrez peut-être lire la solution fournie par le site Web (surtout pour les attaques XSS). Ce qui est important, c'est que vous compreniez ce que vous faites
- De la même manière vous trouverez sur YouTube la solution à chaque exercice. N'hésitez pas à visionner une solution si vous êtes bloqué mais efforcez-vous de comprendre

2 SQL INJECTION

2.1 Premiers exemples

https://portswigger.net/web-security/sql-injection

Faites les exercices suivants:

2.1.1 SQL injection vulnerability in WHERE clause allowing retrieval of hidden data LAB

2.1.2 SQL injection vulnerability allowing login bypass LAB

2.2 SQL injection UNION attack

https://portswigger.net/web-security/sql-injection/union-attacks

Faites les exercices suivants:

2.2.1 Determining the number of columns returned by the query (2 solutions) LAB

2.2.2 Finding a column containing text LAB

2.2.3 Retrieving data from other tables LAB

2.2.4 Retrieving multiple values in a single column LAB

2.3 Examining the database in SQL injection attacks

https://portswigger.net/web-security/sql-injection/examining-the-database

Faites les exercices suivants:

2.3.1 Querying the database type and version on Oracle

2.3.2 Querying the database type and version on MySQL and Microsoft LAB

2.3.3 SQL injection attack, listing the database contents on non-Oracle databases LAB

2.3.4 SQL injection attack, listing the database contents on Oracle LAB

3 CROSS SITE SCRIPTING (XSS)

3.1 Reflected XSS attack

https://portswigger.net/web-security/cross-site-scripting/contexts

Faites les exercices suivants:

3.1.1 Reflected XSS into HTML context with nothing encoded LAB

3.1.2 Reflected XSS into HTML context with most tags and attributes blocked LAB

Cet exercice nécessite quelques explications :

- La solution utilisée par le serveur vulnérable pour se protéger contre l'attaque XSS est la validation (la plupart des balises/attributs sont sur black liste)
- Vous essayez d'abord de trouver les tags/attributs html qui ne sont pas filtrés par le pare-feu applicatif du site web vulnérable.
- Ensuite, vous utilisez un serveur d'exploit sous votre contrôle (n'oubliez pas que vous êtes l'attaquant) qui servira une page accédant à la fonction de recherche du site Web vulnérable.

Notes:

- En cliquant sur "Deliver exploit to victim ", vous simulez le fait qu'un utilisateur victime (piégé par de l'ingénierie sociale) visite votre serveur d'exploit.
- Cliquer sur "View Exploit" simule le fait que le script malveillant s'exécute dans le navigateur de l'utilisateur victime.

3.2 Persistent XSS attack

3.2.1 Stored XSS into HTML context with nothing encoded LAB

https://portswigger.net/web-security/cross-site-scripting/stored/lab-html-context-nothing-encoded

Faites l'exercice.

3.2.2 Exploiting XSS to perform CSRF LAB

https://portswigger.net/web-security/cross-site-scripting/exploiting

Faites l'exercice.

- Dans cet exercice, l'attaquant publie un JavaScript malveillant dans un commentaire de blog.
- Chaque fois qu'un utilisateur victime visite la page du blog, le JavaScript malveillant s'exécute.
- Le JavaScript malveillant,
    - Charge la page de paramétrage de l'e-mail de l'utilisateur victime
    - Extrait le jeton CSRF qui y est inclus

3.2.3 Exploiting cross-site scripting to capture passwords and steal cookies (optional)

Utilisez le précédent " Exploiting XSS to perform CSRF " pour compléter les deux laboratoires restants suivants comme suggéré dans leur solution

- Exploiting cross-site scripting to steal cookies LAB
- Exploiting cross-site scripting to capture passwords LAB