

STI - Projet Partie 2

Rapport

Léo Cortès

Steve Henriquet

7 janvier 2019



HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD
www.heig-vd.ch

Hes·SO

Haute Ecole Spécialisée
de Suisse occidentale
Fachhochschule Westschweiz
University of Applied Sciences and Arts
Western Switzerland

Contents

1	Introduction	3
2	Vulnérabilités	3
2.1	XSS	3

Introduction

Vulnérabilités

XSS

Le programme est vulnérable aux attaques XSS. Les balises HTML sont correctement interprétées, ainsi que les balises de script.

Voici le message envoyé par un attaquant quelconque :

Création utilisateur

Modification utilisateur

Changer de mot de passe

Nouveau message

Déconnexion

Nom d'utilisateur : c.l

Boîte de réception

Destinataire:

Sujet:

Message:

<script>alert('XSS');</script>

Envoyer

Figure 1: Message malicieux

Voici le résultat dans la boîte de réception de la victime.

c.l

Test

2019-01-07 13:07:48

Répondre

Supprimer

Figure 2: Boîte de réception

Lorsque la victime l'ouvre, voici le script est correctement exécuté.

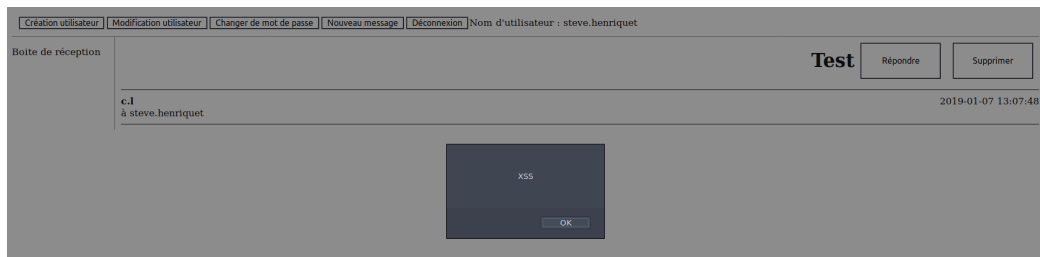


Figure 3: Exécution XSS