Rapport Pentest – HacktheBox
Introduction to Web APP
HTML Injection

Notice de Confidentialité :

Ce rapport est un test pour la réalisation de rapport de test d'intrusion. Il se base sur la plateforme hackTheBox – Academy (https://academy.hackthebox.com/) et les sources sont disponibles au public moyennant un abonnement.

Les tests d'intrusions sont réalisés sur des Hosts confinés et générés automatiquement par la plateforme et les données fournies sont fictives.

Introduction

Ce rapport contient l'ensemble des actions réalisés dans le cadre du pentest. Le but de ce document est de se familiariser avec la génération de rapport et la compréhension complète des méthodologies de test d'intrusion ainsi que des connaissances techniques nécessaires pour le test d'intrusion.

Objectif

L'objectif de ce test d'intrusion est de réaliser une première approche sur la discipline.

Ce test doit simuler un test de pénétration réelle du début à la fin.

Rapport – Informations

Date : 02/03/2023

Host de test : Instance Linux HTB, Parrot OS.

Utilisateur de test : htb-ac712643

IP Host : 10.106.0.117

Host cible : 138.68.170.205 :32485

Type de vulnérabilité : HTML Injection

Durée du Pentest : 5 minutes

Sévérité : Low

Score CVSS de base estimé : 5.4

Base score metric estimé :

- **Attack Vector (AV)*** : Adjacent Network
- **Attack Complexity (AC) :** Low
- **Privileges Required (PR) :** None
- **User Interaction (UI) :** Required
- **Scope (S)** : Unchanged
- **Confidentiality Impact :** Low

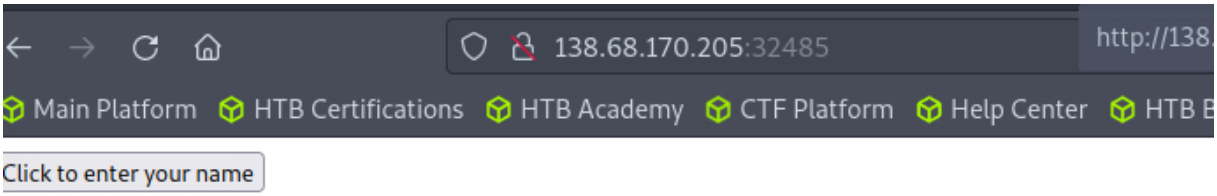
- **Integrity Impact :** Low
- **Availability Impact** : None

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N&version=3.0

Rapport – Actions réalisés

Connexion de à la VM fournit par HTB et génération de l'Host de test.

Ouverture de Firefox depuis l'host de test et accès à la page web cible 138.68.170.205 :32485



Une seule action possible sur le site : cliquer sur le bouton « Click to Enter Your Name »

Fonction du bouton d'un point de vue code source :

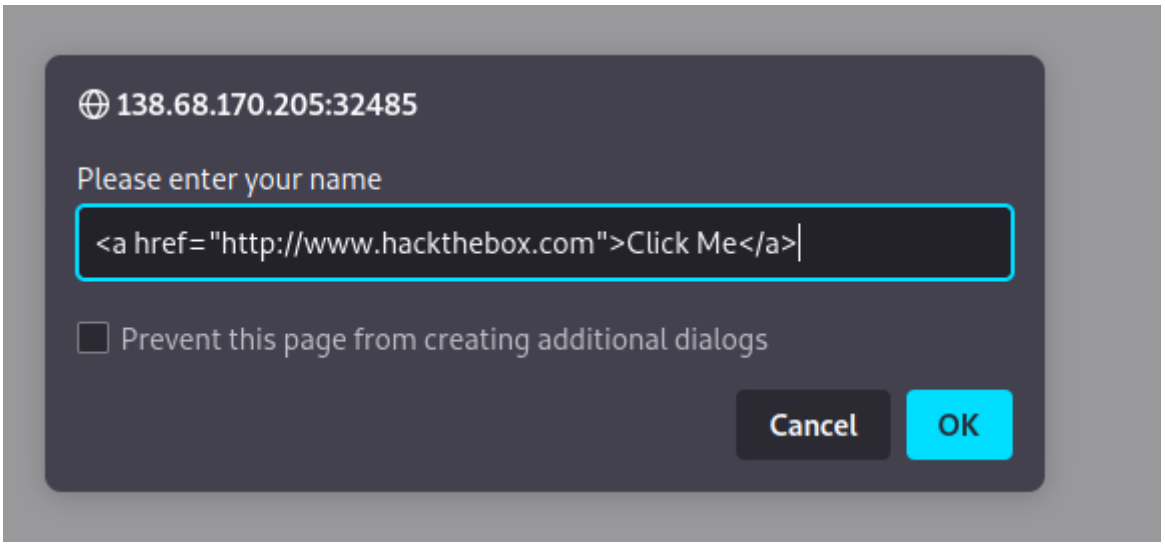
```
<button onclick="inputFunction()">Click to enter your name</button>
<p id="output"></p>

<script>
    function inputFunction() {
        var input = prompt("Please enter your name", "");

        if (input != null) {
            document.getElementById("output").innerHTML = "Your name is " + input;
        }
    }
```

Le script ouvrira un prompt demandant de rentrer un texte, en l'occurrence il est demandé un nom.

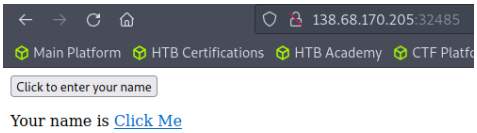
Si L'input est non null, le script JS utilise la methode « GetElementByID » de l'objet « document » de l'objet « outpout ». la propriété « inerHTML » permet de changer le contenu HTML est sera remplacé par «Your name is » suivi de la valeur de la variable « input ».

Code utilisé de compromission :

```
<a href="http://www.hackthebox.com">Click Me</a>
```



Ce code permettra d'insérer dans l'HTML le texte « Click Me » contenant une redirection vers le lien indiqué.



Le risque est donc d'injecter une URL malveillante.

Rapport – Correctifs proposés

A ce jour, les compétences de l'attaquant ne sont pas suffisantes pour proposer un correctif.

L'exercice ne demande pas cette action.