TryHackMe

Julien ROYON CHALENDARD

CTF :
OWASP Juice Shop

Catégorie :
Web

2020

Sommaire

1 Let's go on an adventure !

1.1 Question #1 : What's the Administrator's email address ?

Il y a juste a recopier l'adresse email de l'image dans l'énoncé : admin@juice-sh.op

1.2 Question #2 : What parameter is used for searching ?

Encore une fois, il faut recopier : q

1.3 Question #3 : What show does Jim reference in his review ?

Star Trek

2 Inject the juice

2.1 Question #1 : Log into the administrator account !

32a5e0f21372bcc1000a6088b93b458e41f0e02a

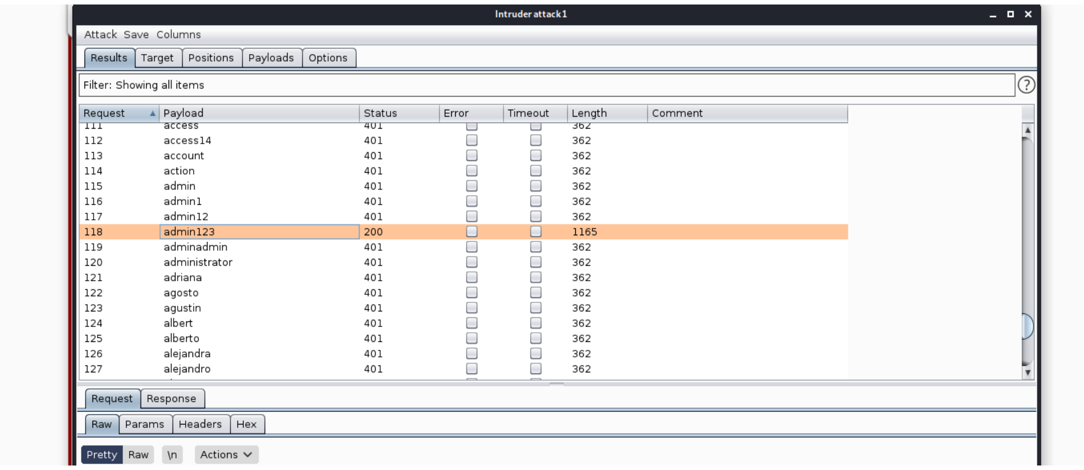
2.2 Question #2 : Log into the Bender account !

fb364762a3c102b2db932069c0e6b78e738d4066

3 Who broke my lock ? !

3.1 Question #1 : Bruteforce the Administrator account's password !

En utilisant Burp Suite, on arrive à trouver le mot de passe de l'admin qui est test123. Cela permet de nous connecter et d'avoir le flag



Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
111	access	401	□	□	362	
112	access14	401	□	□	362	
113	account	401	□	□	362	
114	action	401	□	□	362	
115	admin	401	□	□	362	
116	admin1	401	□	□	362	
117	admin12	401	□	□	362	
118	admin123	200	□	□	1165	
119	adminadmin	401	□	□	362	
120	administrator	401	□	□	362	
121	adriana	401	□	□	362	
122	agosto	401	□	□	362	
123	agustin	401	□	□	362	
124	albert	401	□	□	362	
125	alberto	401	□	□	362	
126	alejandra	401	□	□	362	
127	alejandro	401	□	□	362	

3.2 Question #2 : Reset Jim's password !

On change le mot de passe de Jim en suivant l'énoncé et on obtient le flag : 094fbc9b48e525150ba97d05b942bbf114987257

4 AH ! Don't look !

4.1 Question #1 : Access the Confidential Document !

On va dans le répertoire /ftp et on suit l'énoncé pour avoir le flag : edf9281222395a1c5fee9b89e32175f1ccf50c5b

4.2 Question #2 : Log into MC SafeSearch's account !

66bdcffad9e698fd534003fbb3cc7e2b7b55d7f0

4.3 Question #3 : Download the Backup file !

bfc1e6b4a16579e85e06fee4c36ff8c02fb13795

5 Who's flying this thing ?

5.1 Question #1 : Access the administration page !

Il suffit d'être connecté au compte admi, de visiter /administration et le flag apparaît.
946a799363226a24822008503f5d1324536629a0

5.2 Question #2 : View another user's shopping basket !

41b997a36cc33fbe4f0ba018474e19ae5ce52121

5.3 Question #3 : Remove all 5-star reviews !

50c97bcce0b895e446d61c83a21df371ac2266ef

6 Where did that come from ?

6.1 Question #1 : Perform a DOM XSS !

9aaf4bbea5c30d00a1f5bbcfce4db6d4b0efe0bf

6.2 Question #2 : Perform a persistent XSS !

149aa8ce13d7a4a8a931472308e269c94dc5f156

6.3 Question #3 : Perform a reflected XSS !

23cefee1527bde039295b2616eeb29e1edc660a0

7 Exploration !

7.1 Access the /#/score-board/ page

7efd3174f9dd5baa03a7882027f2824d2f72d86e