

Homework 2

1. Cryptography

1. DES

- a. If you use the key above and encrypt the message a second time, the attacker will be able to see the encrypted text in plain text (see Figure 1 and Figure 2). This is due in part to DES performing exclusive or (XOR) operations on half of the message, which is then swapped throughout the encryption algorithm. This affects DES implementations that take into account the parity bits of the cipher text, in most cases. There are also keys that apply to implementations that do not take into account the parity bits.
- b. Other Weak keys (in hex, including the parity bits):
 - i. 0x0101010101010101
 - ii. 0xFEFEFEFEFEFEFEFE
 - iii. 0xE0E0E0E0F1F1F1F1
 - iv. 0x1F1F1F1F0E0E0E0E

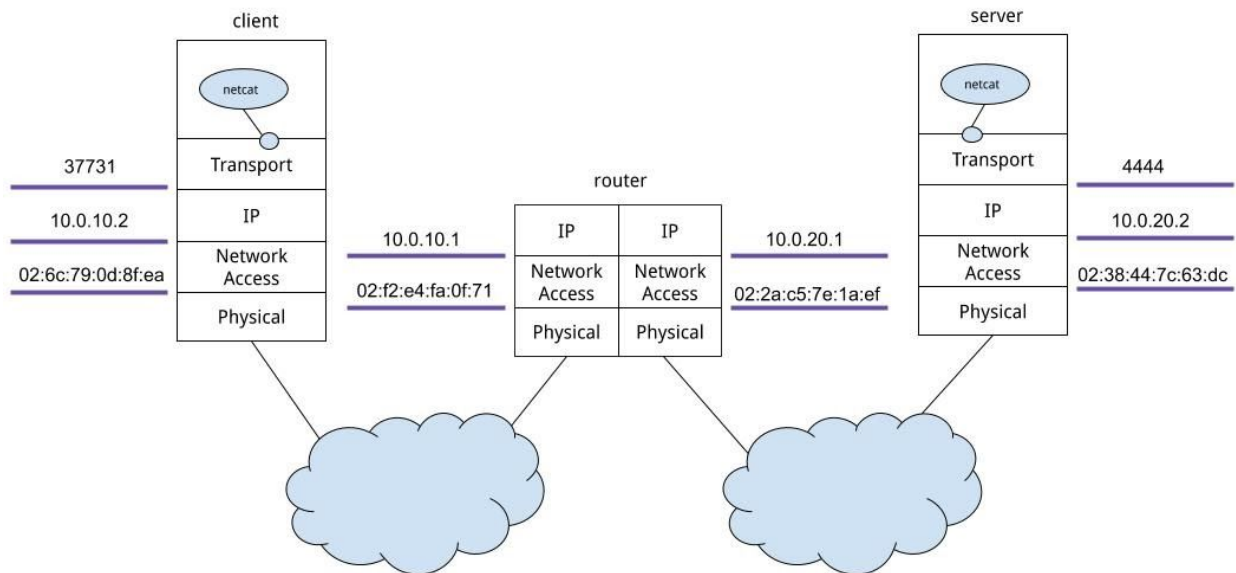
2. RSA

- a. For any value of p and q , where p and q are both prime numbers, $(p \bmod 3)$ nor $(q \bmod 3)$ will be equal to zero because only $(3 \bmod 3)$ will result in zero. Due to the definition of prime numbers, no other number is divisible by that given number. Coupling this with the constraint stating that the prime number must be larger than five leads us to conclude that $(p \bmod 3)$ nor $(q \bmod 3)$ will ever equal zero.
- b. e is considered a good exponent for RSA if it is an integer and is not a factor of n . This exponent must be within the bounds of $1 < e < (p-1)*(q-1)$. If the exponent does not satisfy these requirements, the integrity of the encryption is jeopardized due to one of the primes for n being transmitted with the public key since RSA is asymmetric encryption.
- c. In order for the key to be considered secure, t (or ϕ) which equals $(p-1)*(q-1)$ must be co-prime with e . By being co-prime to e , the greatest common denominator between t and e must be 1. With $e = 3$, there are certain prime numbers that do not satisfy this principle.
 - i. For example when $p = 7$ and $q = 19$:
 - ii. $(p - 1) \% 3$ and $(q - 1) \% 3$ both should not equal 0

- iii. Substituting the values of p and q we get: $(7 - 1) \% 3 = 0$ and $(19 - 1) \% 3 = 0$
- iv. Therefore, $(p - 1) \% 3 = 0$ and $(q - 1) \% 3 = 0$
- v. However, the values of $p = 7$ and $q = 19$ do not produce a gcd with e that equals 1 when multiplied together as: $t = (p - 1) * (q - 1)$ and $\text{gcd}(t, e) \neq 1$
- vi. Therefore, these values of p and q are not valid under the current constraints with $e = 3$
- d. With the constraints of $e = 3$, $\text{gcd}(t, e) = 1$, and $n \% e \neq 0$, $p \% 3$ and $q \% 3$ will always be equal to 0 when $e = 3$. When $e = 3$, the first possible combination of p and q to satisfy the rule would be $p = 11$ and $q = 17$. When substituted into $p \% 3 = q \% 3 = 2$, $11 \% 3 = 2$ and $17 \% 3 = 2$.
- e. $n = p * q$, which then translates to $n = 11 * 17$, $n = 187$, and $187 \% 3 = 1$.

2. TCP/IP Stack

- a. See the picture below for the lab exercise



3. IP Routing

a. Ready status:

The screenshot shows the GENI Portal interface in a Mozilla Firefox browser. The URL is https://portal.geni.net/secure/slice.php?slice_id=bf9e1ca-763c-49b1-acc8-815ce3ecd7be. The page has a navigation bar with links: Home, Tools, Partners, Help, and Patrick McCabe. Below this is a tabbed interface with 'Resources' selected. The main content area shows slice details for 'HW2-prmccabe2' and 'Project: CSC1345_02_S20'. It indicates the slice expires in 6 days and the project expires in 189 days. There are buttons for 'Add Resources', 'Renew', 'Update SSH Keys', and 'Tools'. A 'Manage Resources' section shows a message 'Resources on FIU ExoGENI are ready.' and a 'View RSpec' button. Below this is a network diagram showing three nodes: NodeA, NodeB, and NodeC. NodeA and NodeC are connected to NodeB. At the bottom, there is a footer with version information: 'GENI Portal Version 3.26', 'Copyright © 2017 Ragonese BBN Technologies', 'All Rights Reserved - NSF Award CNS-0714570', and 'GENI is sponsored by the National Science Foundation'.

b. Questions:

- i. It gets 4 hops away then it can't resolve the host

Output for traceroute to C:

traceroute to 192.168.2.12 (192.168.2.12), 30 hops max, 60 byte packets

```
1 10.10.11.1 (10.10.11.1) 0.271 ms 0.244 ms 0.235 ms
2 cr1.cs.fiu.edu (131.94.144.4) 0.477 ms 0.469 ms 0.461 ms
3 fw1.cs.fiu.edu (131.94.131.92) 0.315 ms 0.354 ms 0.335 ms
4 br1.cs.fiu.edu (131.94.134.134) 0.491 ms 0.491 ms 0.563 ms
5 * * *
6 * * *
7 * * *
8 * * *
9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
```

```

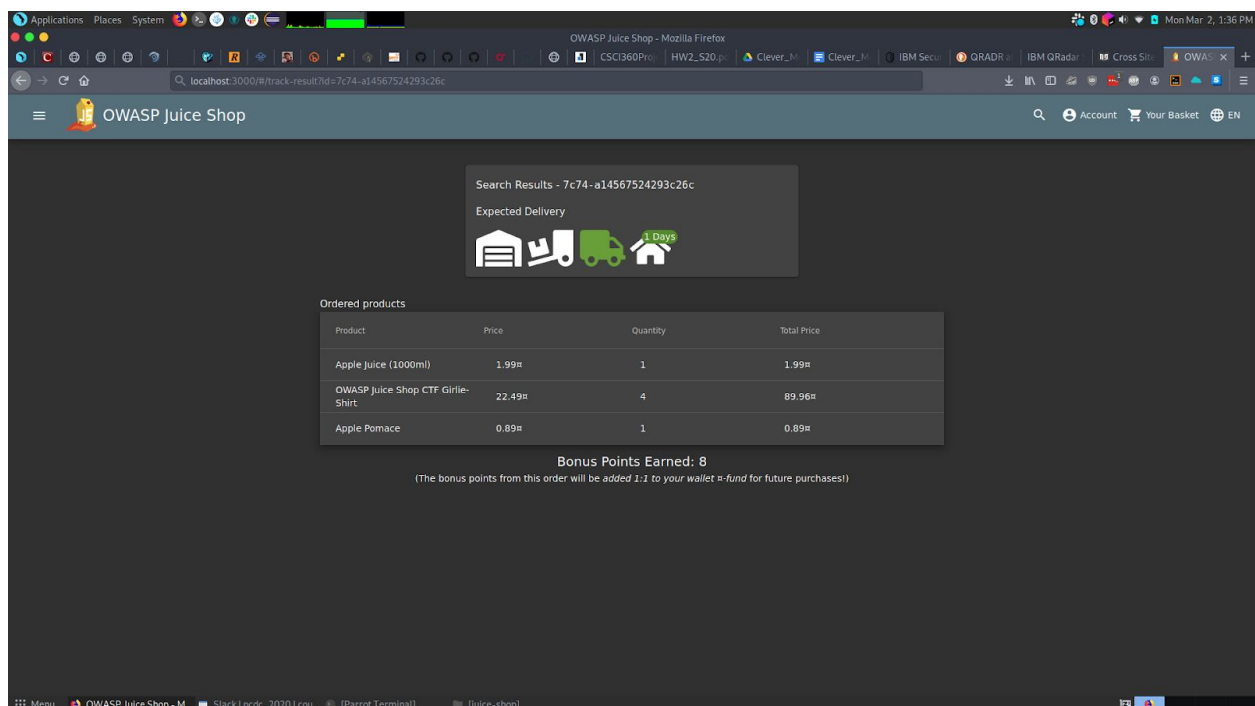
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *

```

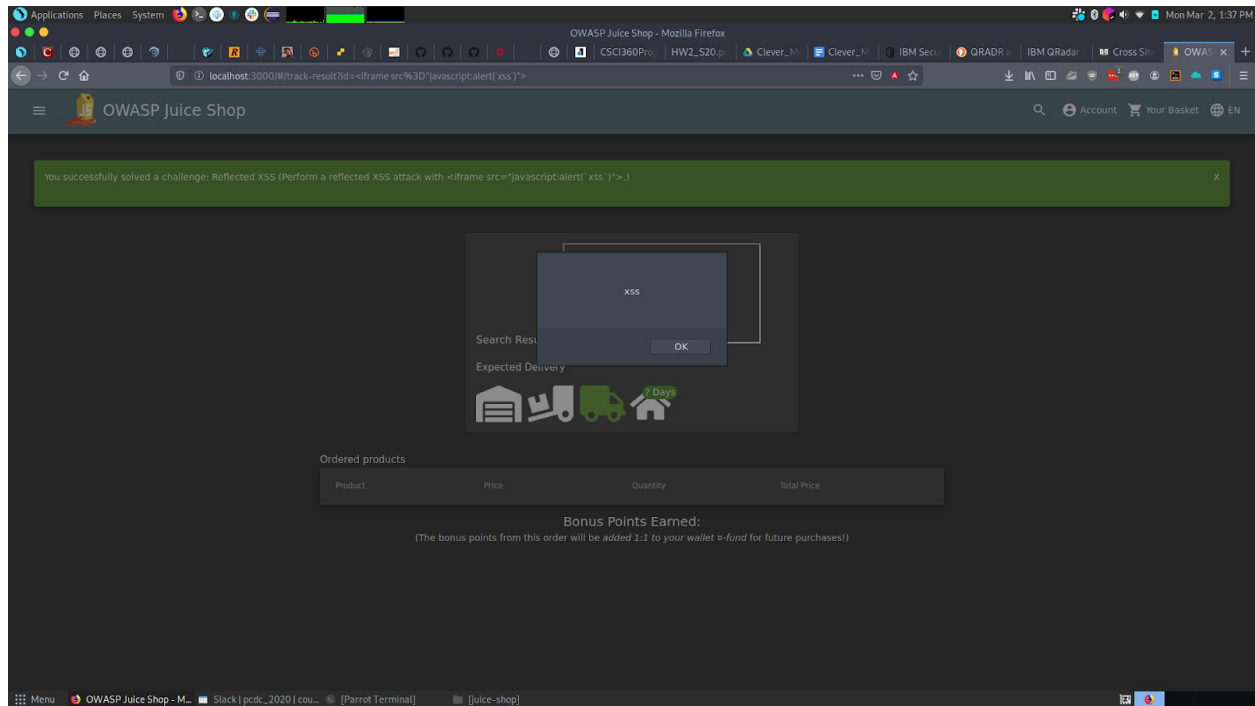
- c. We got stuck when trying to route from the 10.0.1.0/24 subnet to the 10.0.2.0/24 subnet. We tried altering the routing tables. We tried the old and new commands for IP routing to no avail.

4. OWASP Juice Shop

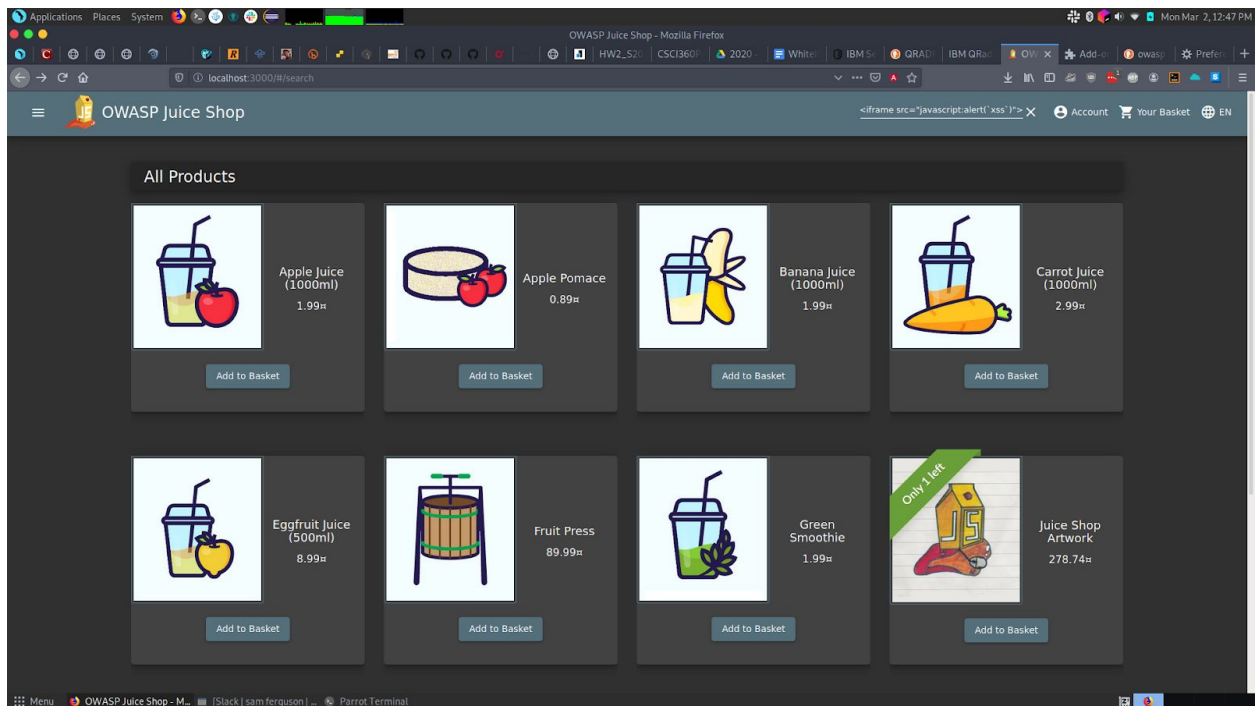
a. Reflected XSS (before)



b. Reflected XSS (After)

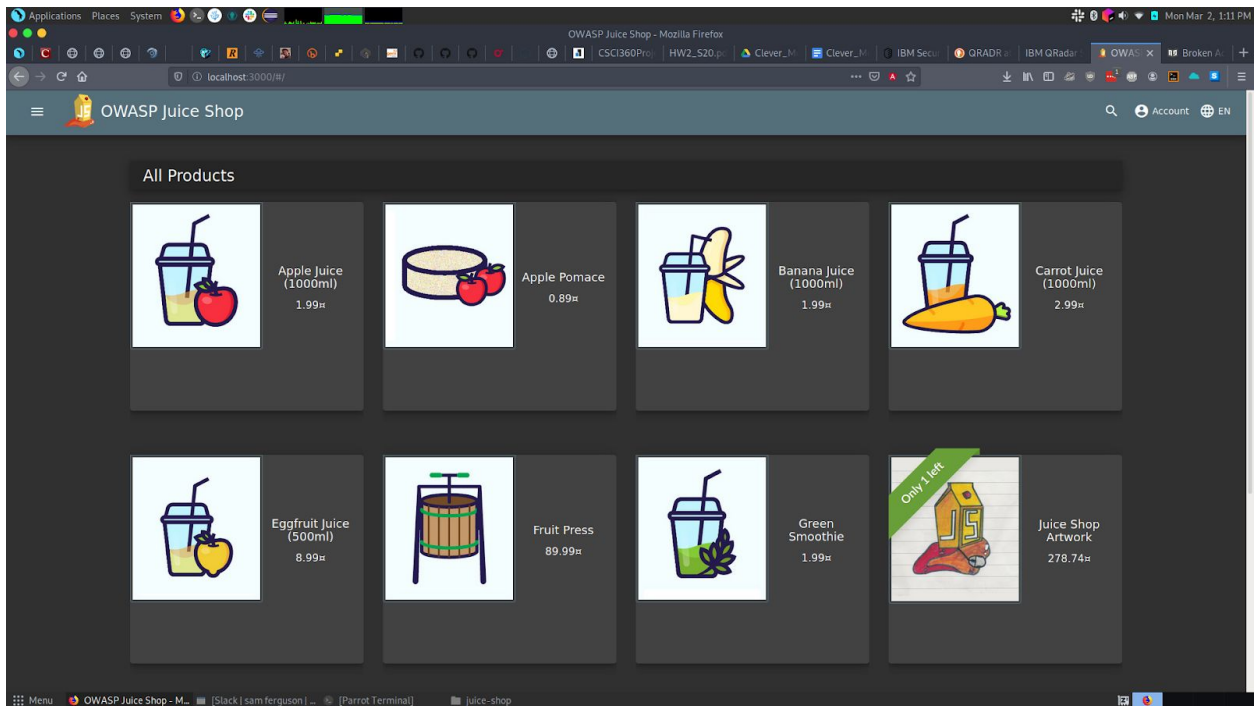


c. Administration page

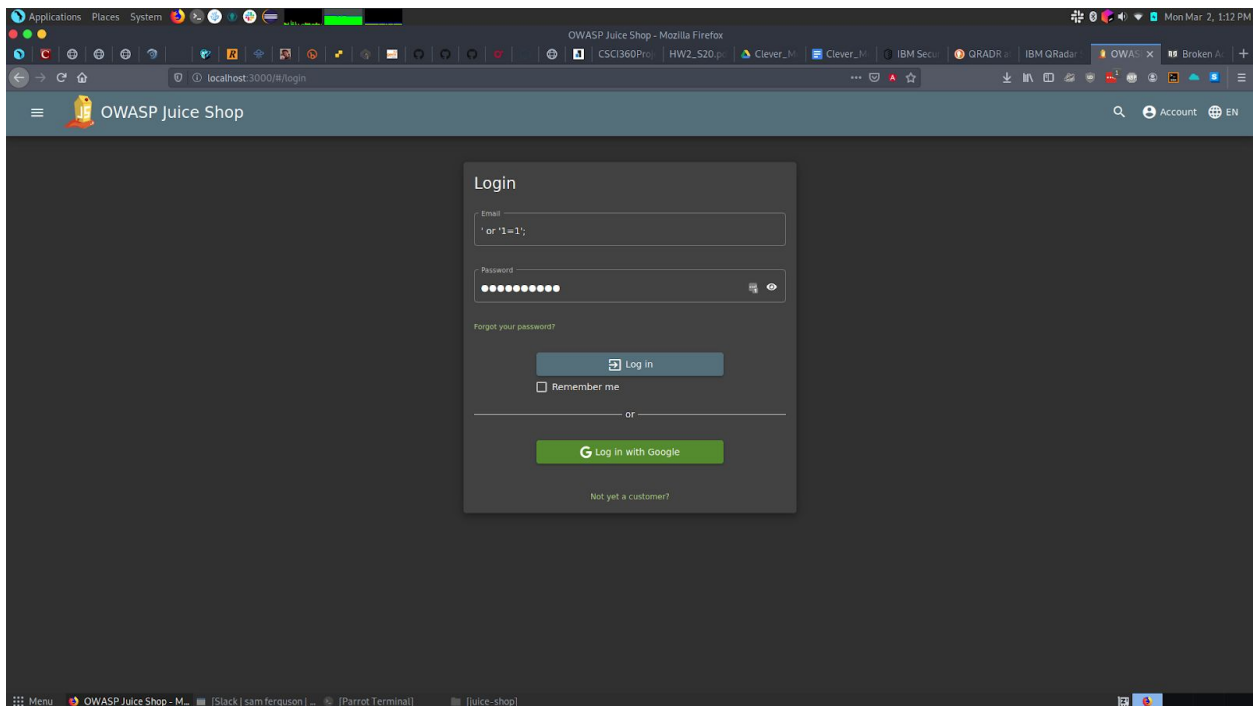


i.

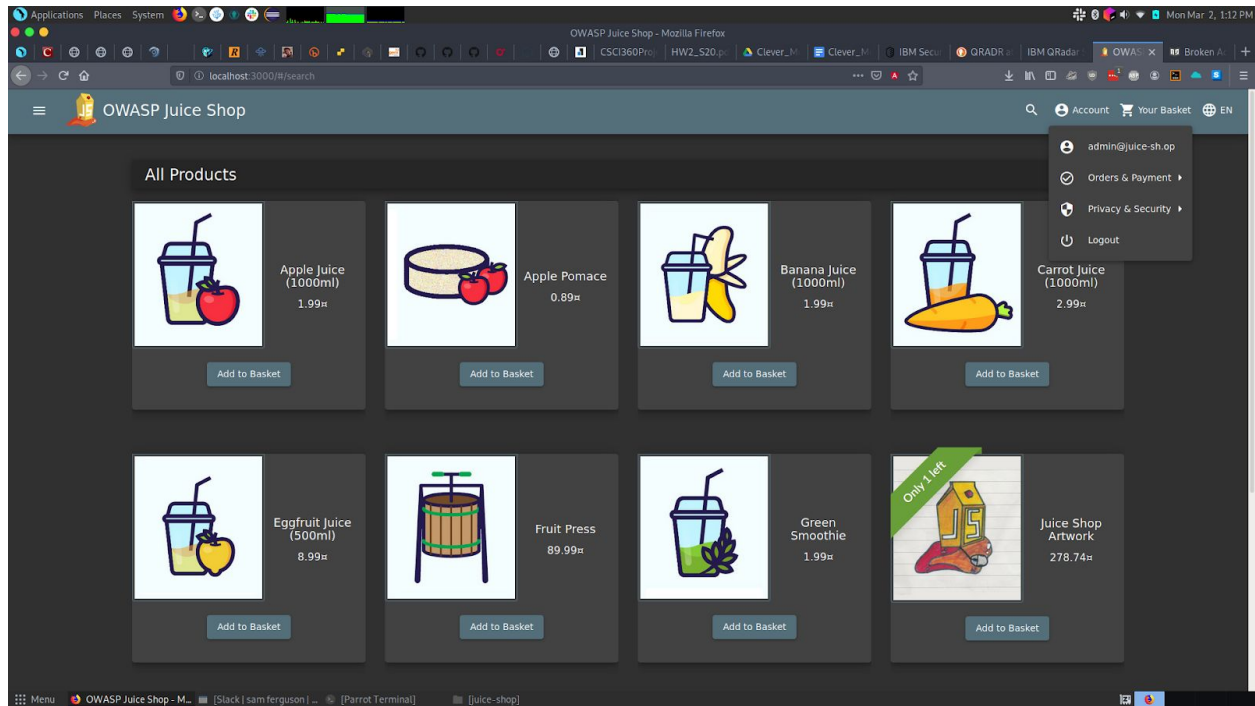
Before Admin page



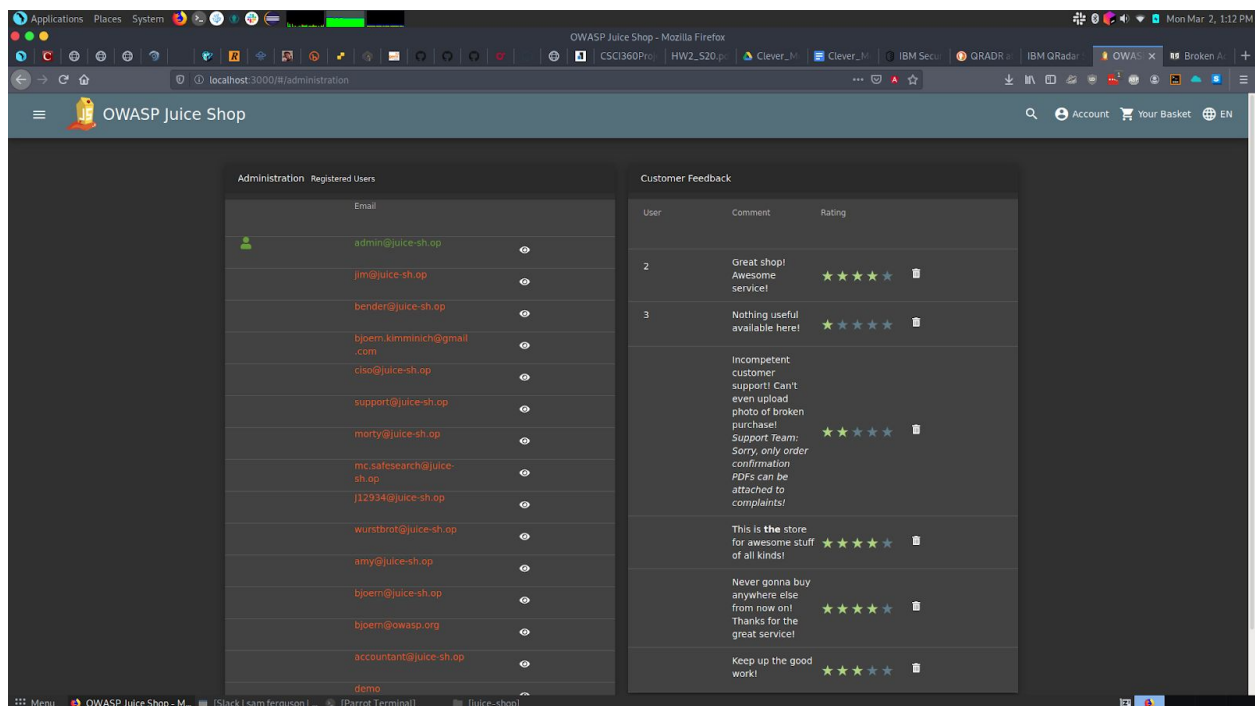
ii. Login to admin with SQL injection



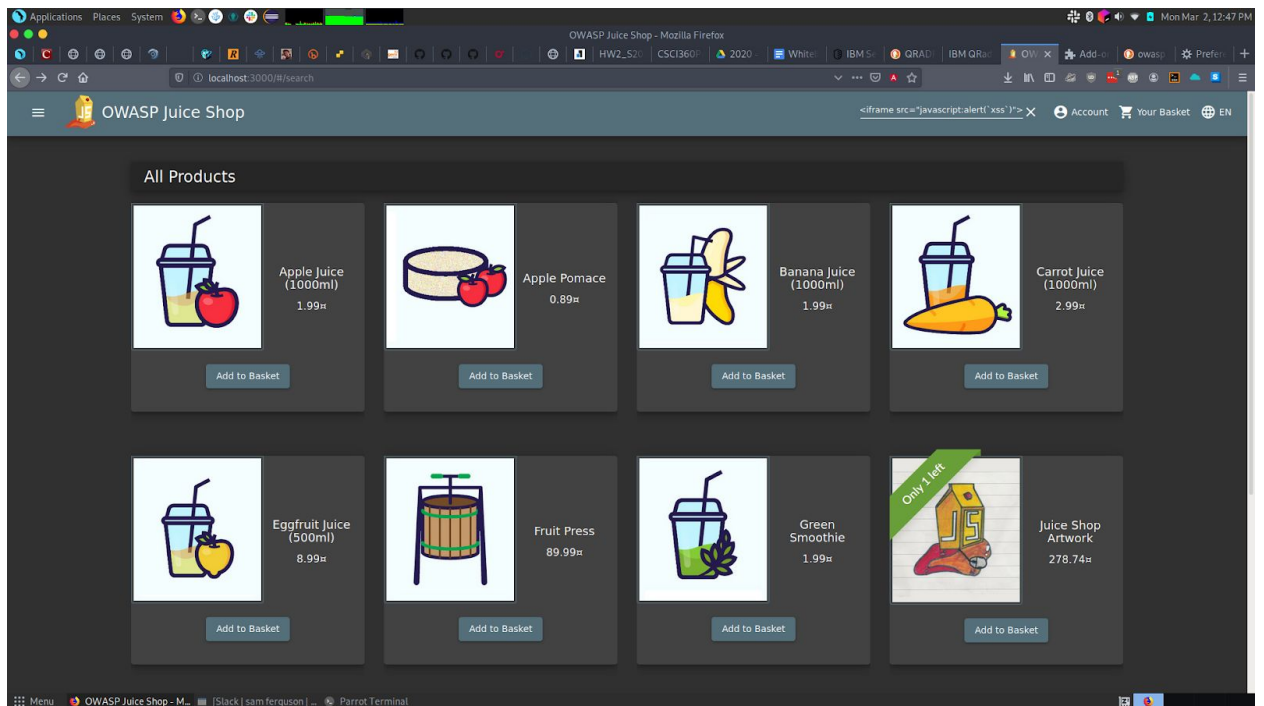
iii. Admin page



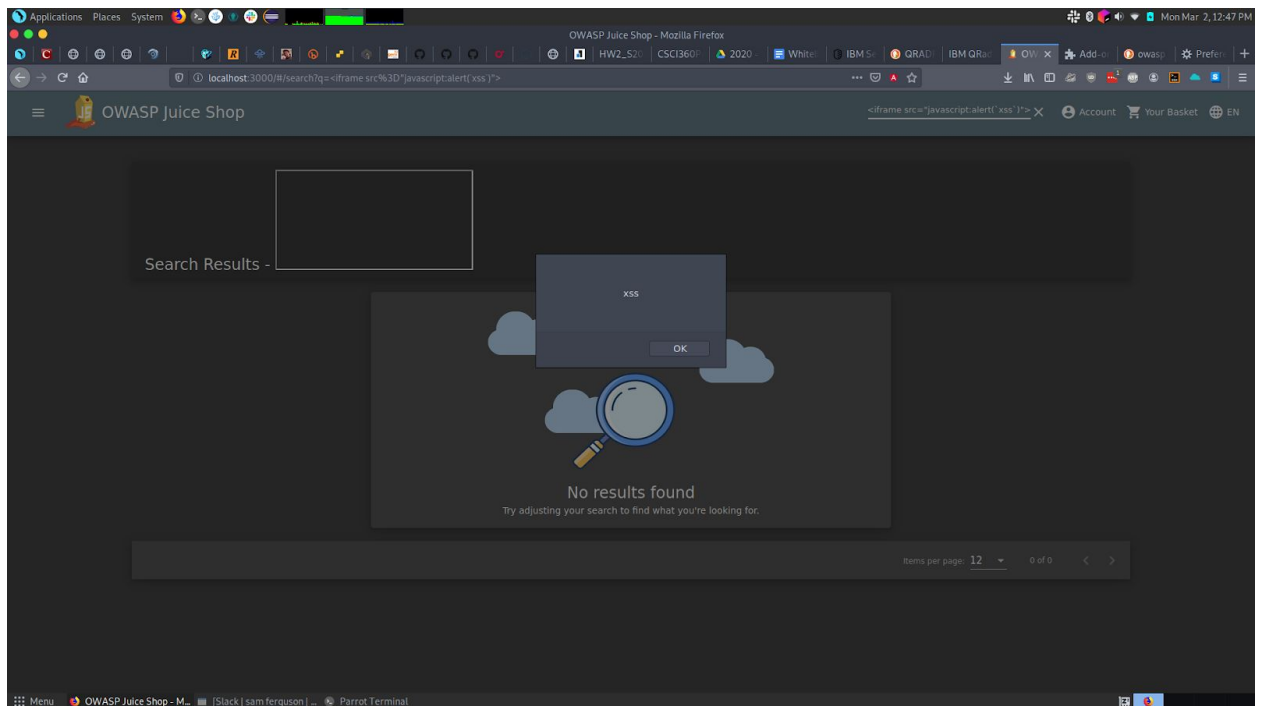
iv. Administration Page



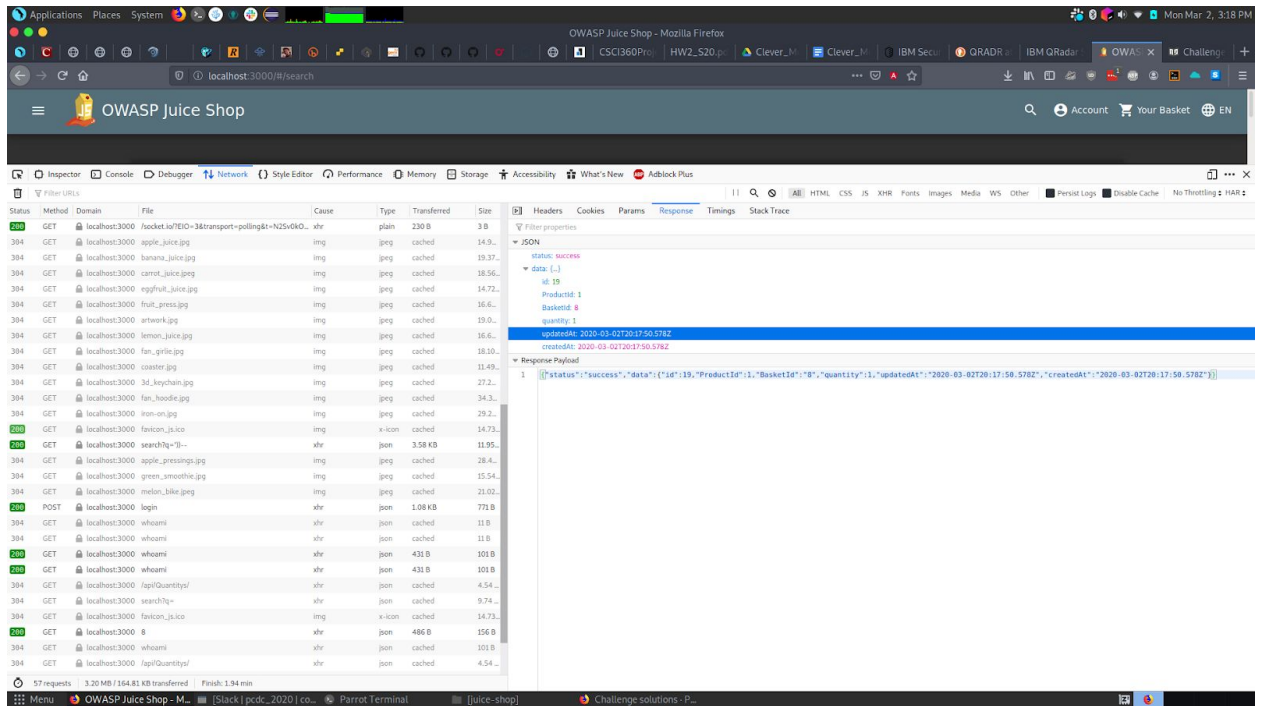
d. Before Persistent XSS



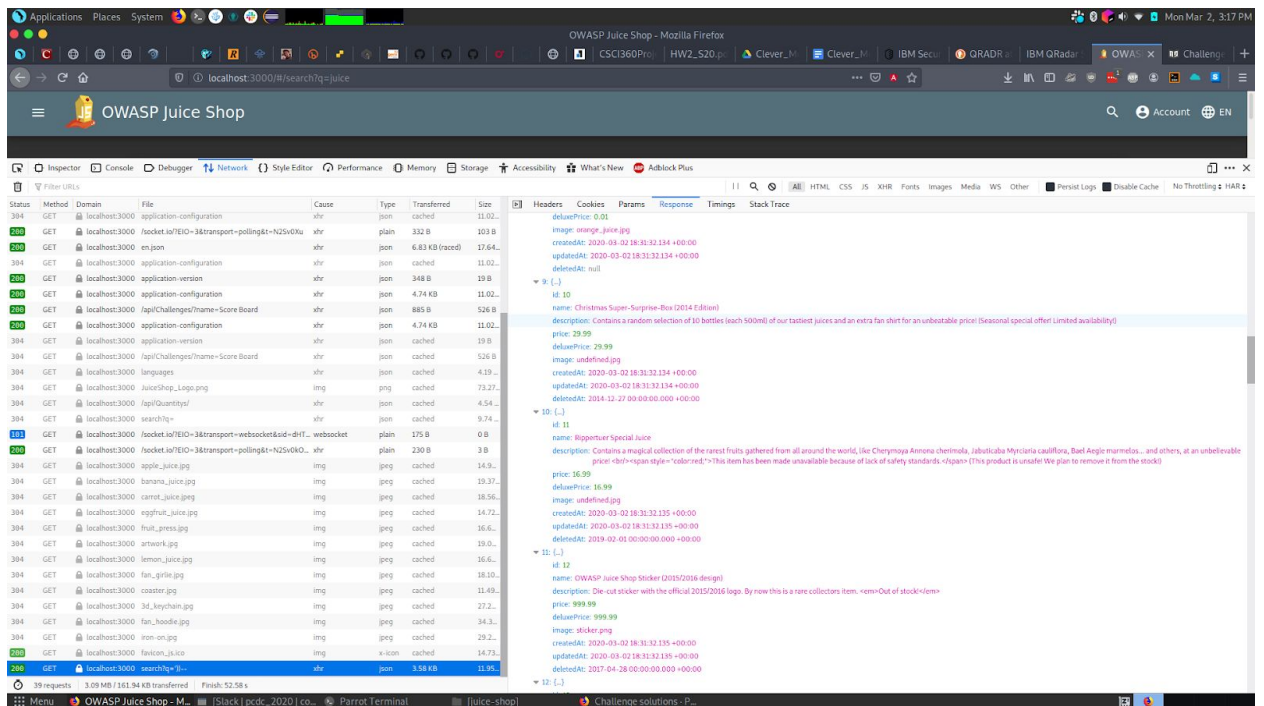
e. After Persistent XSS



f. Christmas Package (Normal POST request)



g. Proof of Christmas Items



h. Our way of modification of POST

Applications Places System Thu Mar 5, 3:23 PM

OWASP Juice Shop - Mozilla Firefox

CSCI360Project_F19.p... HW2_S20.pdf IBM Security Learning : x Damn Vulnerable Web : x OWASP Juice Shop

localhost:3000/#search

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility What's New Adblock Plus

Filter URLs

Status	Method	Domain	File	Cause	Type	Transferred	Size	Time
200	GET	localhost:3000	/	xhr	json	857 B	526 B	38 ms
200	POST	localhost:3000	/api/BasketItems/	xhr	json	488 B	158 B	16 ms
200	GET	localhost:3000	241d - Thu Mar 05 2020	xhr	json	706 B	375 B	39 ms
200	POST	localhost:3000	/api/BasketItems/	xhr	json	488 B	158 B	16 ms

xhr

4 requests 1.19 KB / 2.48 KB transferred Finish: 17.30 s

Menu [Markdown Cheatsheet... Parrot Terminal OWASP Juice Shop - M... Take Screenshot Save Screenshot

Cart after POST Request:

Applications Places System Thu Mar 5, 3:23 PM

OWASP Juice Shop - Mozilla Firefox

CSCI360Project_F19.p... HW2_S20.pdf IBM Security Learning : x Damn Vulnerable Web : x OWASP Juice Shop

localhost:3000/#basket

Image	Product	Price	Quantity	Total Price
	Apple Juice (1000ml)	1.99€	1	1.99€
	Christmas Super-Surprise-Box (2014 Edition)	29.99€	1	29.99€
	Apple Pomace	0.89€	1	0.89€

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility What's New Adblock Plus

Filter URLs

Status	Method	Domain	File	Cause	Type	Transferred	Size	Time
200	GET	localhost:3000	/	xhr	json	857 B	526 B	38 ms
200	POST	localhost:3000	/api/BasketItems/	xhr	json	488 B	158 B	16 ms
200	GET	localhost:3000	241d - Thu Mar 05 2020	xhr	json	706 B	375 B	39 ms
200	POST	localhost:3000	/api/BasketItems/	xhr	json	488 B	158 B	16 ms
200	GET	localhost:3000	/	xhr	json	0.99 KB	1.55 KB	38 ms
304	GET	localhost:3000	/wheels	xhr	json	cached	99 B	38 ms
304	GET	localhost:3000	/undefined.jpg	img	html	cached	1.79 KB	38 ms

4 requests 4.63 KB / 3.47 KB transferred Finish: 50.70 s

Menu [Markdown Cheatsheet... Parrot Terminal OWASP Juice Shop - M... Take Screenshot Save Screenshot