

AdventOfCTF-2

Challenge

188 Solves



2

200

web

For the 2nd challenge you will need to bypass the login mechanism.

Visit <https://02.adventofctf.com> to start the challenge.

Unlock Hint for 50 points

Flag

Submit

Advent of CTF 2

Your daily dose of CTF for December

Login

Username

Password

Submit

Do not try too hard



The Advent of CTF is brought to you by [NOVI Hogeschool](#). It is built by [@credmp](#). If you are looking for a Dutch Cyber Security Bachelor degree or bootcamp, [check us out](#). (Dutch follows) Als je al weet dat je een opleiding wilt volgen, neem dan [contact op met Valerie](#).

If we try to login with the credentials admin:admin we don't login, but a cookie gets set.

Application	Filter		Only show cookies with an issue							
	Name	Value	Domain	P...	Ex...	Size	Http...	Sec...	Sam...	Prio...
Manifest	authenticated	eyJndWVzdCI6InRydWUiLCJ...	.02.adventofc...	/	20...	59		✓		Med...
Service Workers										
Clear storage										
Storage										
Local Storage										
Session Storage										
https://02.adventofctf.com										
IndexedDB										
Web SQL										
Cookies										
https://02.adventofctf.com										

Using Cyberchef we can decode the value of this cookie.

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars

Input

eyJndWVzdCI6InRydWUiLCJhZG1pbiI6ImZhbHNlIn0%3D

Output

{ "guest": "true", "admin": "false" }7.

Knowing how the website checks for authentication we can craft a cookie with admin set to true.

Recipe

To Base64

Alphabet
A-Za-z0-9+/=

Input

```
{ "guest": "false", "admin": "true" }
```

Output

```
eyJndWVzdCI6ImZhbHNlIiwiaWVhYXRtaW4iOiJ0cnVliiB9
```

Notice that i've added a space in the input so that the output does not have padding (=).

Now replace this cookie with the one we had before and reload the page.

Name	Value	D...	Path	Expir...	Size	HttpO...	Secure	SameSi...	Priority
authenticated	eyJndWVzdCI6ImZhbHNlIiwiaWVhYXRtaW4iOiJ0cnVliiB9	.0...	/	2021...	57		✓		Medium

Advent of CTF 2

Your daily dose of CTF for December

Show me the flag....

FLAG

NOVI{cookies_are_bad_for_auth}

"Whoop Whoop" - @GevuldeCookie

Flag: NOVI{cookies_are_bad_for_auth}

