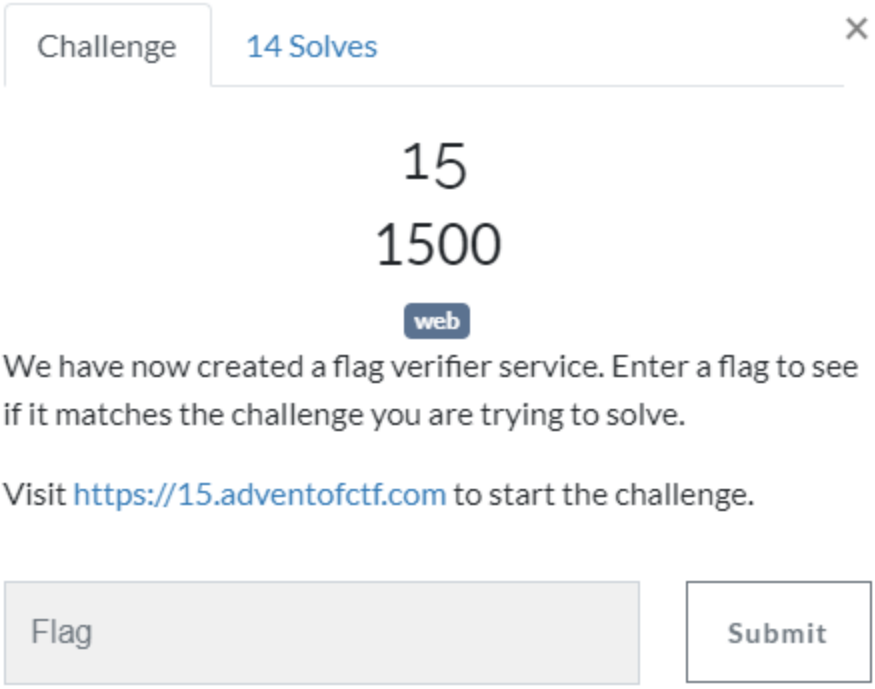
AdventOfCTF-15



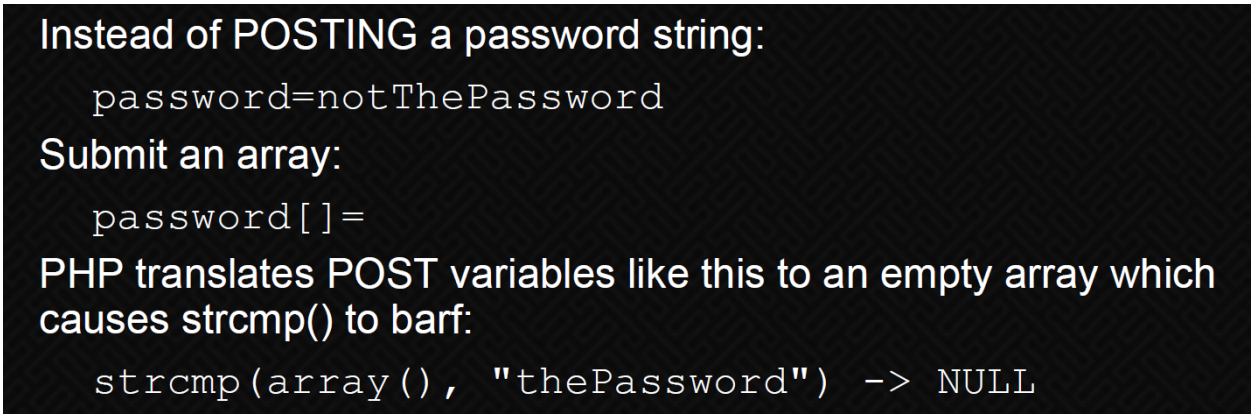
Here is the code:

```php
<?php

ini_set('display_errors', 0);

include("flag.php");

if (isset($_POST["flag"])) {
    $f = $_POST["flag"];

    if (strcmp($f, $flag) == 0 || sha1($flag) == sha1($f)) {
        echo $flag;
        die();
    }
}

header("Location: /index.php?error=Wrong flag");
exit();

?>
```

The strcmp function makes the code vulnerable because of how comparisons are made in php.

> https://owasp.org/www-pdf-archive/PHPMagicTricks-TypeJuggling.pdf

In the last part of this pdf we see this:



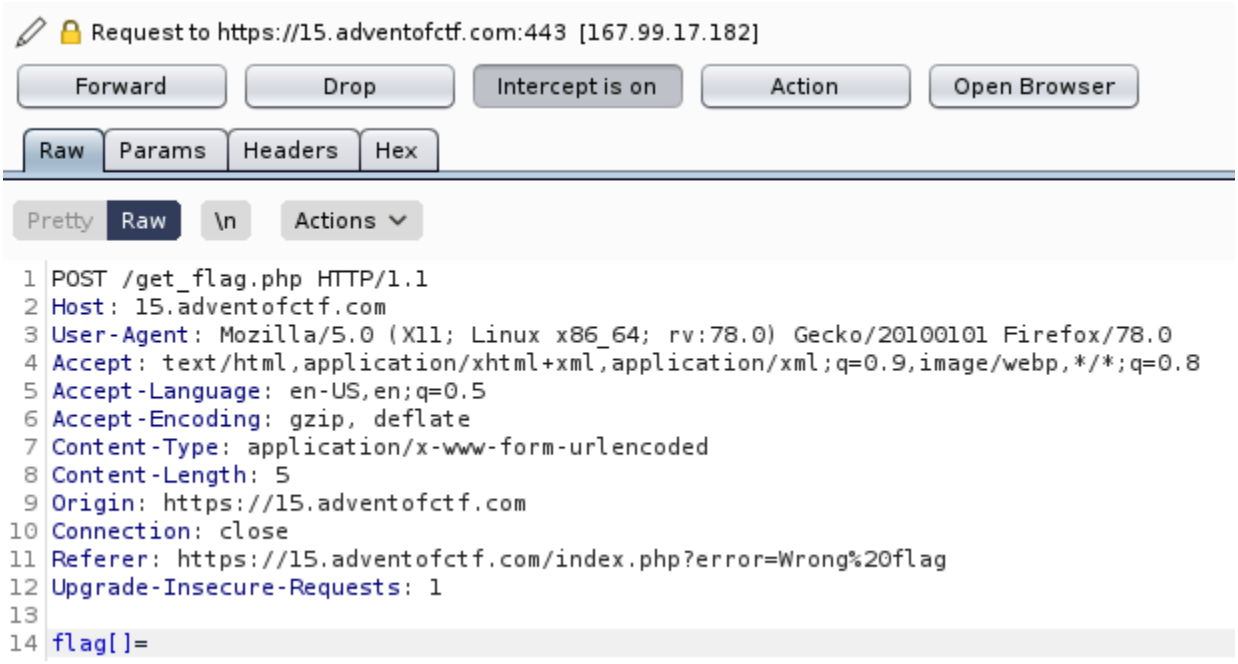
Lets take a look at the strcmp usage again:

```
if (strcmp($_POST['password'], 'thePassword') == 0) {
  // do authenticated things
}
```

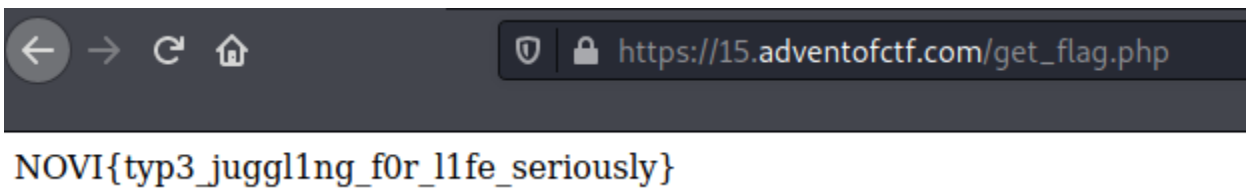
Lucky for us, thanks to type juggling, NULL == 0. Auth bypass!

This is exactly what we need.

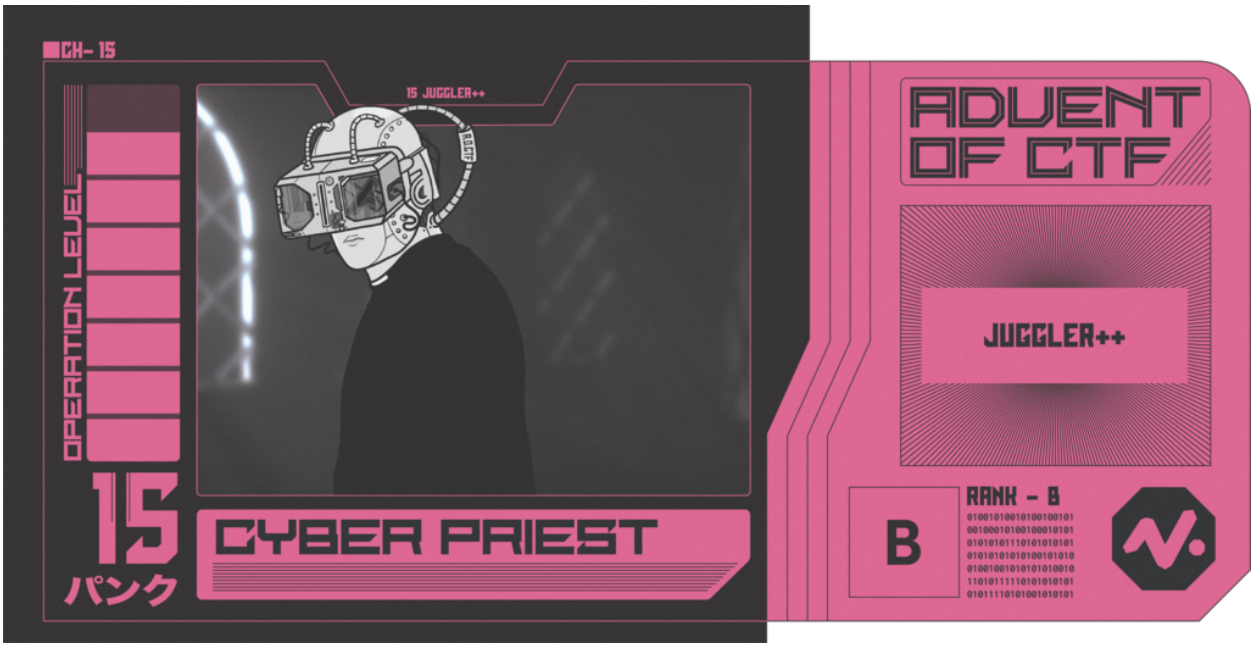
Using burp intercept a request and change the flag parameter to be an array.



Forward the request and we get the flag!



Flag: NOVI{typ3_juggl1ng_f0r_l1fe_seriously}


CH- 15
15 JUGGLER++
OPERATION LEVEL
15
パンク
CYBER PRIEST
ADVENT OF CTF
JUGGLER++
B
RANK - B