Juggle Juggle

date 24.10.2021

solved in time of CTF

category Web Exploitation score 100

Description

PHP string equality using `==` and `strlen`.

Attached files

PHP server source

```
if (isset($_GET['passkey']) &&
hash("md5", "DYAXWCA") == $_GET['passkey'] &&
strlen(hash("md5", "DYAXWCA")) != strlen($_GET['passkey'])) {
echo "FLAG";
} else if (isset($_GET['passkey'])) {
echo "False Password!";
} else {
"File";
}
?>
```

Summary

Set parameter `passkey` to `hash("md5", "DYAXWCA")` but keep the length not equal.

`hash("md5", "DYAXWCA")` -> `0e424759758842488633464374063001`

e.g: `0e42475975884248863346437406300`

Flag

```
hology4{eZ_jUg61inG_in1_m4salAh_uD4h_S3rinG}
```

Detailed solution

php - String comparison using '==' vs. 'strcmp()' - Stack Overflow TLDR; PHP will implicitly cast them to floats and do a numerical comparison if they appear numerical.

Another solutions

I hate PHP. BTW, my first thought was some kind of php `<?php ?>` injection, but I can't find such case if that possible.