Forum:Hack Forums

Thread: Bypassing PHP if statements

Commander - *March 5, 2021, 4:26 pm*

Hello there. General Kenobi Glad to be here!
I'm going to be a bit vague in this thread, just to keep somewhat anonymity. I hope that what I write is sufficient!

I faced an issue when sending a request to a webserver. I attempt to bypass certain statements in PHP. Their backend script goes somewhat like this ...

PHP Code

```
<?php
$hex= "3355443";
 if ($hex== "0xffffff")
   echo("NOT OK 1");

 if (!isset($hex))
   echo("NOT OK 2");

 if ($hex== "null")
   echo("NOT OK 3");

 if ($hex!= "0x333333") {
   echo("NOT OK 4");
 } else {
   echo("SUCCESS 4");
 }
```

So what I'm trying to do, is only have the backend return "SUCCESS 4", none of the others.
I have tried with the corresponding decimal to the 0x333333 hex, I have tried some booleans and integers, but nothing has done everything just right!
A table from HydraSky (can't post links :/) has brought me great help, but yet it still hasn't solved my problem.

Hope that you awesome guys can help (if it's even possible!),
Thank you,
Commander

NobleSausage - *March 9, 2021, 12:21 am*

maybe this will help you... https://medium.com/swlh/php-type-juggling-vulnerabilities-3e28c4ed5c09

Commander - *March 9, 2021, 1:57 am*

(Mar 9, 2021 01:21 AM)NobleSausage Wrote: *[CITE]* maybe this will help you...
I'm afraid that this won't work. Although it would pass the fourth check, the first (and third) check would stop it. Do note that in the backend, it isn't an echo but rather a return function. This was just to simplify it.

Now, I might just be talking out of bounds, but if PHP compares hexadecimal (0x333333) to another

type (eg. 3355443, decimal) then may that work? Decimal doesn't work, though. I've tried that.

I should mention that this is PHP version 5!

Have got it working now, I was using the wrong Tryit editor, one in PHP version 7