Challenge 01

Flag: FLAG{My_F15st_b@By_St3ps}

I ran the php on a local server using WAMP. I was greeted with "May the 4th be with you"

Opening up the php file, I first beautify it.

I noticed most of the stuff is base64encoded so I just have to decode them.

I noticed that mt_srand and mt_rand. Not sure what those are for except for randoming values so I am just going to ignore it first.

The random function generates random number from a string of a-zA-Z0-9. So $rP and $rIV will be a random 8 characters string. Hmm

There's only one eval function in this php, which evaluates the ed function. Let's look at ed.

ed uses AES-256-CBC encryption and sha256 to hash the $rP and $rIV to $key and $iv respectively etcetc.

$o is the returning value to be evaluated. Let's see what is $o.

Reading the documentation for openssl_decrypt, $o basically returns the decrypted String on success or empty String on failure.

So I initially thought I can run a loop to bruteforce it, such that the loop will keep randoming my $rP and $rIV until $o returns a none empty String.

I ended up with a bunch of garbage values when the loop ends. Went to do my research, and found out that openssl_decrypt does return garbage when incorrect key is used. I realised that it’s kind of impossible to bruteforce it.

Tried to run the php multiple times to see the $rP and $rIV values. I realised that they do not change. Studied the mt_srand and found out that the seed will create a deterministic randomness, such that calling mt_rand will give the same set of numbers.

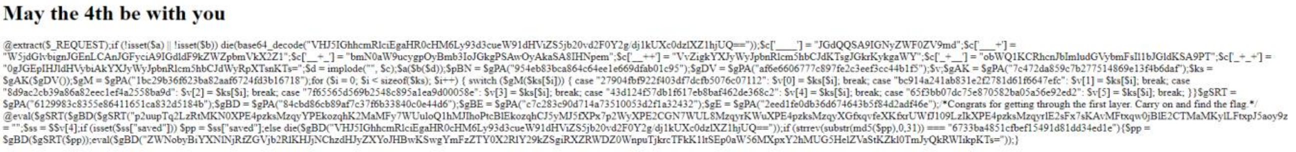
This means that the seed will generate a fixed $key and $iv value despite the “randomness”.

Since the seed is set using the value, I should focus on manipulating the $date value to get my flag.

I can bruteforce it, but the header gave me a hint "May the 4th be with you". So I tried to change $date = “20190504” and echo the eval part. Error, this means that it’s garbage or empty String. Tried a few different 2000s year, still not working.

Went to Google about it, some Star Wars reference. Someone mentioned that the line “May the Force Be With You” is spoken famously in the Star Wars 1977 movie. Tried $date = “19770504”

Boom, I got some additional codes. Beautify time.



May the 4th be with you

```
@extract($_REQUEST);if (!isset($a) || !isset($b)) die(base64_decode("VHJ5IGhhcmRlciEgaHR0cHM6Ly93d3cueW91dHViZS5jb20vd2F0Y2g/dj1kUXc0dzlXZ1hjUQ=="));$c['____'] = "JGdQQSA9IGNyZWF0ZV9md";$c['___+'] =
"W5jdGlvbignJGEnLCAnJGFyciA9IGdldF9kZWZpbmVkX2Z1";$c['__+_'] = "bmN0aW9ucygpOyBmb3IoJGkgPSAwOyAkaSA8IHNpem";$c['__++'] = "VvZigkYXJyWyJpbnRlcm5hbCJdKTsgJGkrKykgaWY";$c['_+__'] = "obWQ1KCRhcnJbImludGVybmFsIl1bJGldKSA9PT";$c['_+_+'] =
"0gJGEpIHJldHVybiAkYXJyWyJpbnRlcm5hbCJdWyRpXTsnKTs=";$d = implode("", $c);$a($b($d));$pBN = $gPA("954eb83bca864c64ee1e669dfab01c95");$gDV = $gPA("af6e6606777c897fe2c3eef3cc44b1f5");$v;$gAK = $gPA("7c472da859c7b277514869e13f4b6daf");$ks =
$gAK($gDV());$gM = $gPA("1bc29b36f623ba82aaf6724fd3b16718");for ($i = 0; $i < sizeof($ks); $i++) { switch ($gM($ks[$i])) { case "27904fbf922f403df7dcfb5076c07112": $v[0] = $ks[$i]; break; case "bc914a241ab831e2f2781d61f6647efc": $v[1] = $ks[$i]; break; case
"8d9ac2cb39a86a82eec1ef4a2558ba9d": $v[2] = $ks[$i]; break; case "7f65565d569b2548c895a1ea9d00058e": $v[3] = $ks[$i]; break; case "43d124f57db1f617eb8baf462de368c2": $v[4] = $ks[$i]; break; case "65f3bb07dc75e870582ba05a56e92ed2": $v[5] = $ks[$i]; break; }}$gSRT =
$gPA("6129983c8355e86411651ca832d5184b");$gBD = $gPA("84cbd86cb89af7c37f6b33840c0e44d6");$gBE = $gPA("c7c283c90d714a73510053d2f1a32432");$gE = $gPA("2eed1fe0db36d674643b5f84d2adf46e");/*Congrats for getting through the first layer. Carry on and find the flag.*/
@eval($gSRT($gBD($gSRT("p2uupTq2LzRtMKN0XPE4pzksMzqyYPEkozqhK2MaMFy7WUuloQ1hMJIhoPtcBlEkozqhCJ5yMJ5fXPx7p2WyXPE2CGN7WUL8MzqyrKWuXPE4pzksMzqyXGfxqvfeXKfxrUWfJ109LzIkXPE4pzksMzqyrlE2sFx7sKAvMFtxqw0jBlE2CTMaMKylLFtxpJ5aoy9z
= "";$ss = $$v[4];if (isset($ss["saved"])) $pp = $ss["saved"];else die($gBD("VHJ5IGhhcmRlciEgaHR0cHM6Ly93d3cueW91dHViZS5jb20vd2F0Y2g/dj1kUXc0dzlXZ1hjUQ=="));if (strrev(substr(md5($pp),0,31)) === "6733ba4851cfbef15491d81dd34ed1e"){$pp =
$gBD($gSRT($pp));eval($gBD("ZWNobyBiYXNlNjRfZGVjb2RlKHJjNChzdHJyZXYoJHBwKSwgYmFzZTY0X2RlY29kZSgiRXZRWDZ0WnpuTjkrcTFkK1ltSEp0aW56MXpxY2hMUG5HelZVaStKZkl0TmJyQkRWIikpKTs="));}
```

After scanning through the code, I realised $gPA is used very often. Time to figure it out.

Base64decode it gave me a create_function in the form of a string. Within it there's a get_defined_functions(). So $gPA basically creates variable functions from our current list of functions. Obfuscation.

$a($b($d)) probably creates the actual function out. Probably that's why the "if" sentence on line 6 has to be set to true to continue the execution. Since I know what it does, I comment both the line 6 "if" sentence and $a($b($d)) and write the $gPA as a function. (Can be seen in part2Final.php) I did try to send "?a=eval&b=base64_decode" as a GET Request but somehow there's an issue with it.

I found out most of the variable functions(part2Final.php) and the first eval is basically an rc4 encryption function.

$ss=$$v[4] is a tricky one but I can't get it to work until I made $ss = ${$v[4]}.

$v[4] is _COOKIE , so $$v[4] is the content of _COOKIE, which is an Array.

Now the thing is $ss["saved"] is not SET before. So what do I do? Should I create one and throw random strings until it works?

However, after that I noticed that there's a string comparison condition before the second eval. The secondeval takes in $pp as an argument so we definitely need to find the value of $pp aka $$ss["saved"].

strrev(substr(md5($pp),0,31))==="6733ba4851cfbef15491d81dd34ed1e" can be translated to

substr(md5($pp),0,31) ==="e1de43dd18d19451febfc1584ab3376"

Now this makes finding $pp easy as I have the first 31 values of the md5 hash. The last value can only be from 0 to f. Simply run all 16 hashes against an online hash cracker, and I found a result for this hash = e1de43dd18d19451febfc1584ab33767. $pp = "Recruitment".

All I need to do now is to set my "saved" cookie with:

setcookie("saved","Recruitment, time()+60);

Refresh the php to set the cookie and refresh it again. I get my flag: FLAG{My_F15st_b@By_St3ps}

Check out part2Final.php for the documentation.