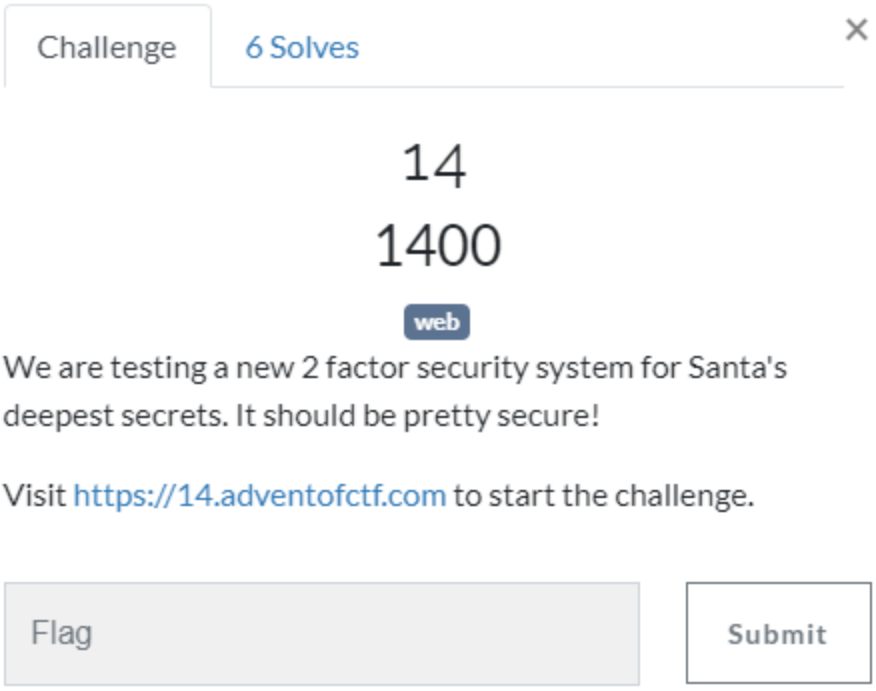
# AdventOfCTF-14



# Advent of CTF 14

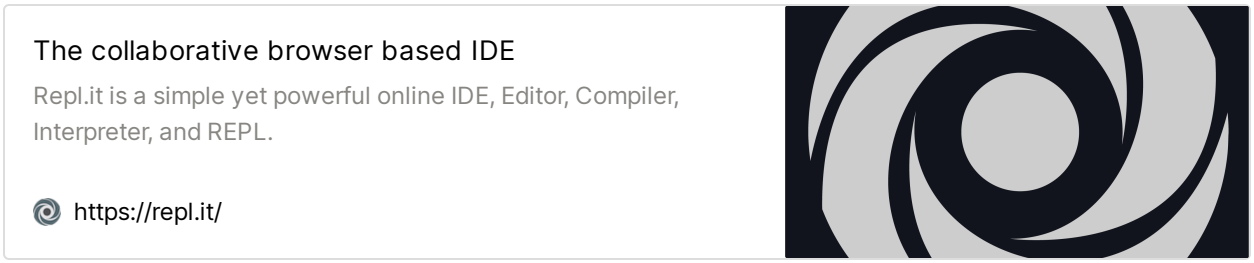
Your daily dose of CTF for December

Login ()

```php
<?php

ini_set('display_errors', 0);

include("flag.php");

if (isset($_POST["password"], $_POST["verifier"])) {
    $password = $_POST["password"];
    $verifier = $_POST["verifier"];

    $hash = sha1($password + $secret_salt);
    $reference = substr($hash, 0, 7);

    if ($verifier === $reference) {
        echo $flag;
        die();
    }
}

header("Location: /index.php?error=That was not right.");
exit();

?>
```

Enter the Password | Enter the verifier | Submit

The code here is not very readable. I hosted the code myself on this website.




This is my setup.

```
//get_flag.php
<?php

ini_set('display_errors', 0);

include("flag.php");

if (isset($_POST["password"], $_POST["verifier"])) {
    $password = $_POST["password"];
    $verifier = $_POST["verifier"];

    $hash = sha1($password + $secret_salt);
    echo "".($password + $secret_salt)."<br>";
    $reference = substr($hash, 0, 7);
    echo "Reference ".$reference."<br>";
    echo "hash ".$hash."<br>";

    if ($verifier === $reference) {
        echo $flag;
        die();
    }
    die();
}

header("Location: /index.php?error=That was not right.");
exit();

?>
```

get_flag.php

```php
<?php

ini_set('display_errors', 0);

include("flag.php");

if (isset($_POST["password"], $_POST["verifier"])) {
    $password = $_POST["password"];
    $verifier = $_POST["verifier"];

    $hash = sha1($password + $secret_salt);
    echo "".($password + $secret_salt)."<br>";
    $reference = substr($hash, 0, 7);
    echo "Reference ".$reference."<br>";
    echo "hash ".$hash."<br>";

    if ($verifier === $reference) {
        echo $flag;
        die();
    }
    die();
}

header("Location: /index.php?error=That was not right.");
exit();

?>
```

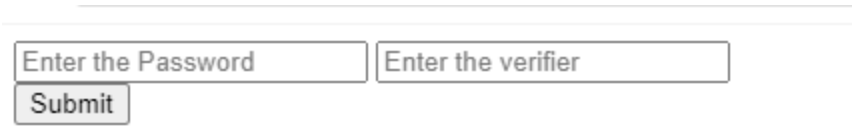
```
//flag.php
<?php
$secret_salt = 2;
$flag = "Here is the flag {....}";
?>
```

flag.php

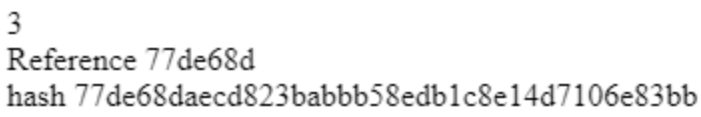
```php
<?php
$secret_salt = 2;
$flag = "Here is the flag {....}";
?>
```

```
//index.php
<html>
  <head>
```

```
    <title></title>
  </head>
  <body>
    <form action="/get_flag.php" method="POST">
    <div class="input-group">
    <input type="text" class="form-control" id="password" name="password"  placeholde
r="Enter the Password">
    <input type="text" class="form-control" id="verifier" name="verifier"  placeholde
r="Enter the verifier">
    <div class="input-group-append">
        <button type="submit" class="btn btn-warning">Submit</button>
    </div>
    </div>
    </form>
  </body>
</html>
```




Here i've tried entering a password 1 and no verifier.




As we can see the page get_flag.php adds up the $secret_salt and the given password. If we give an big enough number it will go to infinity.

```
Password: 1000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
Verifier:
```

This is what we see.

INF
Reference 55c1943
hash 55c1943f65c7c105ae98e6703cd64127b6585656

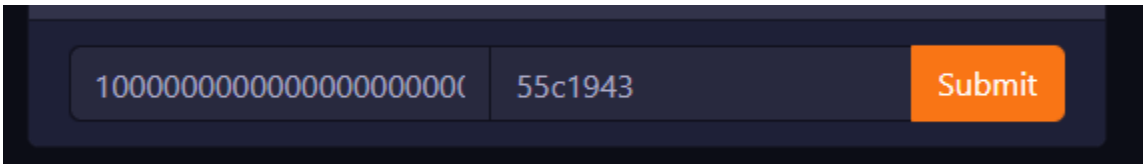
So if we put the password to the big value and the verifier to 55c1943 we should get the flag.

```
Password: 1000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
Verifier: 55c1943
```

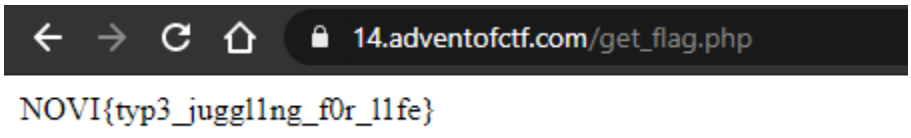
INF
Reference 55c1943
hash 55c1943f65c7c105ae98e6703cd64127b6585656
Here is the flag {....}

Nice!

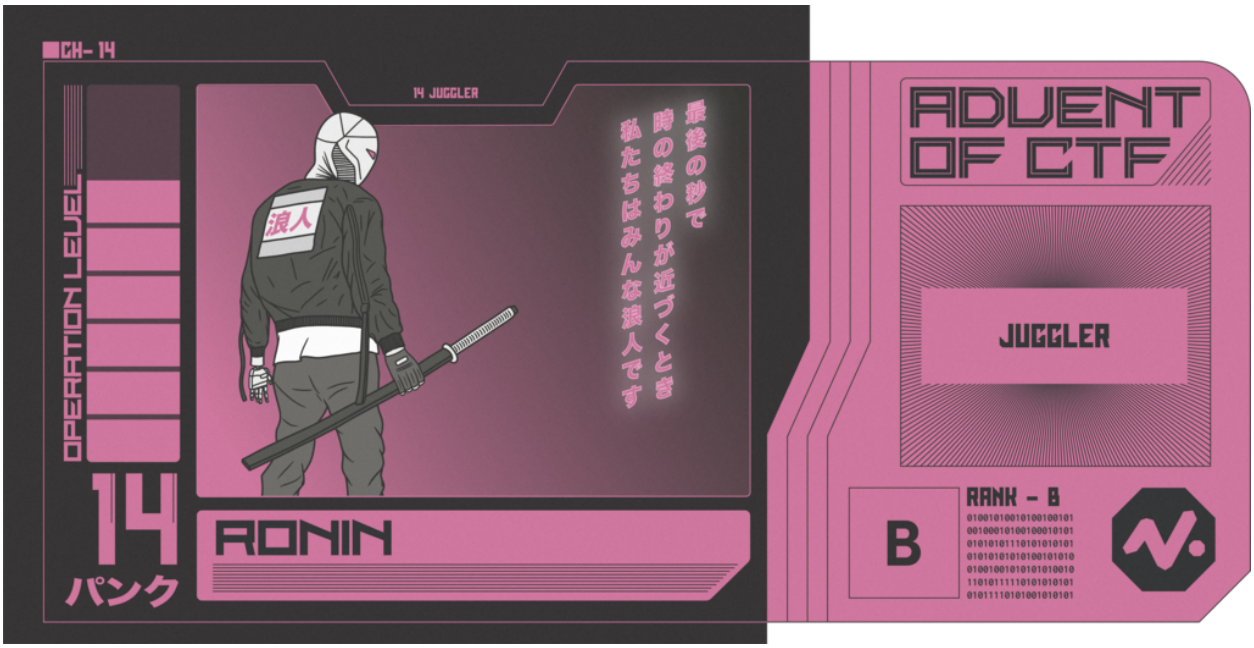
Now let's go back to the ctf website and set the password and verifier to those values.




And we get redirected to the flag page.




Flag: NOVI{typ3_juggl1ng_f0r_l1fe}


CH- 14
14 JUGGLER
最後の秒で
時の終わりが近づくとき
私たちはみんな浪人です
浪人
OPERATION LEVEL
14
パンク
RONIN
ADVENT OF CTF
JUGGLER
RANK - B
B