

Hgame week1 write up

web1 之who eat my flag

一开始是毫无思路啊，后来提示了泄露，又提示了vim,查了一哈，了解了一下。

分布式版本控制系统(**git**)源码泄漏

.git

README.MD

.gitignore

集中式版本控制系统(**svn**)源码泄漏

.svn

#####

VIM编辑器

备份文件：

***.*~**

异常退出备份文件：

***.*.swp**

***.*.swo**

***.*.swl**

***.*.swm**

***.*.swl**

日志文件：

_viminfo

.viminfo

#####

Emacs编辑器

***.*~**

***.*~1~**

***.*~2~**

***.*~3~**

#####

nano编辑器

***.*.save**

***.*.save1**

***.*.save2**

***.*.save3**

#####

就试了第一个就出了，下载了一个文件，然后utf-8打开拿到flag。

web2之换头大作战：

然后提示要POST 改一哈

Raw Params Headers Hex

```
POST /week1/how/index.php?want=123 HTTP/1.1
Host: 120.78.184.111:8080
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://120.78.184.111:8080/week1/how/index.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: admin=0
Connection: close
Content-Length: 2
```

Raw Headers Hex HTML Render

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8" />
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title></title>
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="stylesheet" type="text/css" media="screen" href="main.css">
<script src="main.js"></script>
</head>
<body>
<form action="index.php" method="get">flag嘛 :
<input name="want" type="text">
<input type="submit" value="submit">
</form>
</body>
</html>
<br/>
request method is error.I think POST is better
```

琢磨一下，这样改是有问题的，首先post的数据不在url里。要写在body里，还有一点坑的是headers和data要有一个空行。打开然后不知道为啥它默认存在一个空行

Raw Params Headers Hex

```
POST /week1/how/index.php?want=123 HTTP/1.1
Host: 120.78.184.111:8080
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://120.78.184.111:8080/week1/how/index.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: admin=0
Connection: close
Content-Length: 2
```

Raw Headers Hex HTML Render

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8" />
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title></title>
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="stylesheet" type="text/css" media="screen" href="main.css">
<script src="main.js"></script>
</head>
<body>
<form action="index.php" method="get">flag嘛 :
<input name="want" type="text">
<input type="submit" value="submit">
</form>
</body>
</html>
<br/>
request method is error.I think POST is better
```

删掉它，再加上我们的数据，就OK了，接下来一路看提示改头就可以了。

```
Connection: close
Content-Length: 8
Content-Type: application/x-www-form-urlencoded
X-Forwarded-For: 127.0.0.1
want=123
```

哈哈我只是个代理服务器哦，真正的用户是localhost哟

改个User-Agent

Upgrade insecure requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) Waterfox/50.0 AppleWebKit/537.36
(KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36

这里有点坑的是如果全删了，然后加上这个就不行，把它插进去的话就可以

接下来再改个bilibili就OK了

WEB4之can you find me

顺手右键

the gate has been hidden

can you find it? xixixi



顺藤摸瓜之搞到password



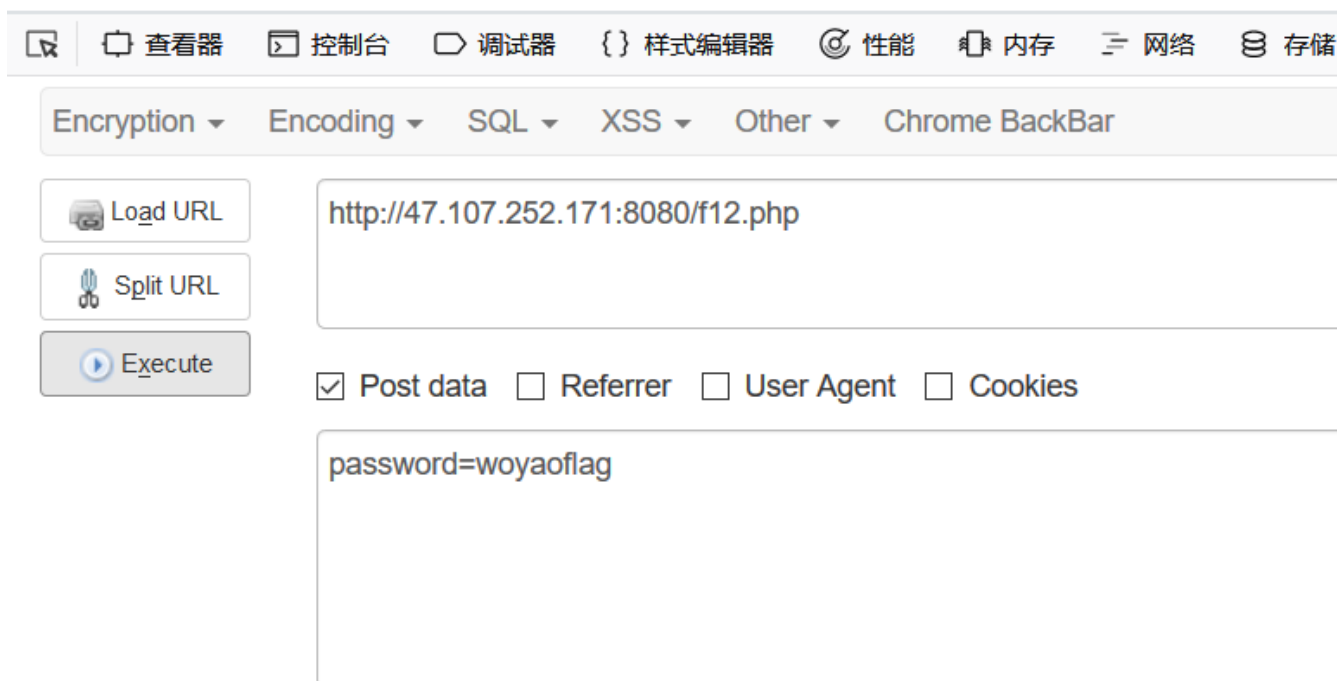
yeah!you find the gate

but can you find the password?

please post password to me! I will open the gate for you!

right!

[click me to get flag](#)



再来一手熟练的hackbar



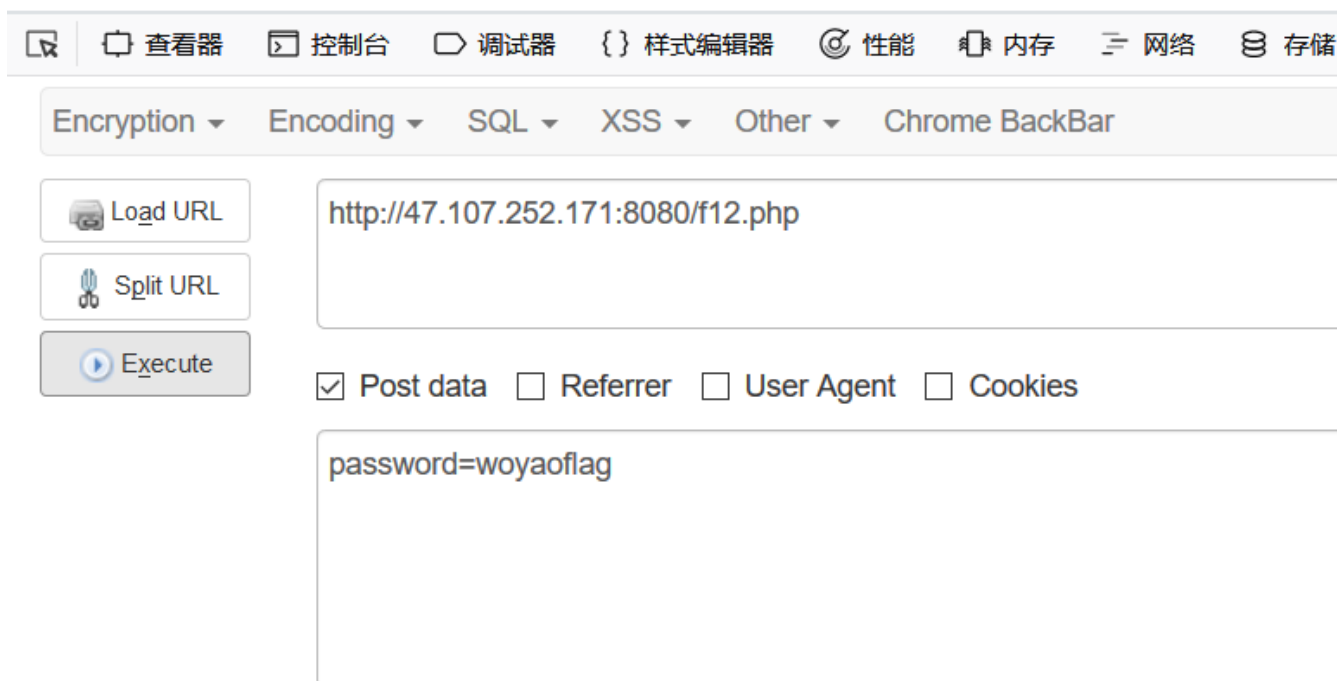
yeah!you find the gate

but can you find the password?

please post password to me! I will open the gate for you!

right!

[click me to get flag](#)



然后。。。

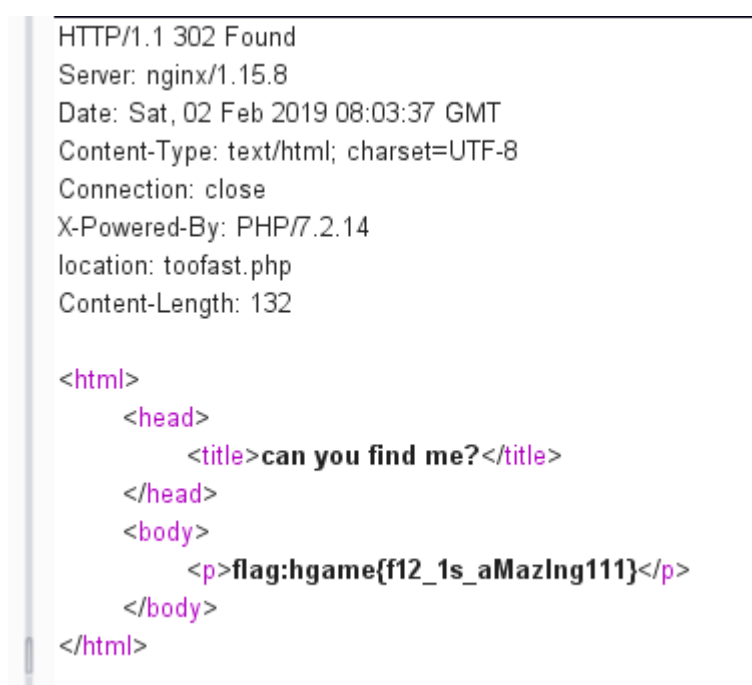
悄咪咪之重定向



在firefox里看不见响应 奇怪啊



换一哈burp



瞎××乱搞之HelloRe:

我是直接UTF-8打开就看到了。。

```
??[] ]?+[]D ?=[
?[]@ H???k?????u?[]@ ?????
[] Please input your key: hgame{welc0m3_t0_R3_world!} succes
```

python没啥好说呀，就是了解一下加密方式，然后操作就完了