web 安全问题

- CSRF 的原理和防范措施

文件上传漏洞

- 防御

1. 前端检查
2. 对文件类型与扩展名进行限制
3. fgrep -R 'eval($_POST[' /var/www/dvwa
4. waf 防火墙限制

SQL注入

```
select use();
select database();
select now();
```

大写 按tab可以补全

```
show  create table users\G
```

字符串的查询需要加引号

```
select user,password from mysql.user where user = 'root';
```

若不加引号，代表查询的字段

数字是不可以作为字段的

基于错误注入

输入单引号，用于判断是否语法报错进而得知是否可以注入

基于or的注入 获取一个表

```
select user,password from mysql.user where user = 'root' or 1=1；
```

where后的条件为真

比如：在用户名输入框中输入:' or 1=1#,密码随便输入，这时候的合成后的SQL查询语句为：

```
select * from users where username='' or 1=1#' and password=md5('')
```

语义分析：“#”在mysql中是注释符,-- 也可以用作注释，这样井号后面的内容将被mysql视为注释内容，这样就不会去执行了，换句话说，以下的两句sql语句等价：

```
select * from users where username='' or 1=1#' and password=md5('')
```

等价于

```
select * from users where username='' or 1=1
```

基于union的注入 获取多个表

union前后字段数量一致

如果对union前的不关注则利用假的条件

例如：

```
select * from dvwa.users where 1=2 union select user_login,user_pwd,1,2 from wordpress.wp_users;
```

字段字段不一致，则可以不停的增减字段数尝试

如关注前面的数据则不使用where的假条件

information_schema (数据库字典)

查看数据库中所有的表

```
select * from information_schema.tables\G
```

查看去重后的所有数据库

```
select DISTINCT TABLE_SCHEMA from information_schema.tables;
```

等同于 show databases;

```
select TABLE_SCHEMA，TABLE_NAME from information_schema.tables WHERE TABLE_SCHEMA='HH';

select TABLE_SCHEMA，GROUP_CONCAT(TABLE_NAME) from information_schema.tables GROUP BY TABLE_SCHEMA;
```

通过前面获取的库与表获取表中的所有列

```
select COLOUMN_NAME from information_schema.columns WHERE TABLE_SCHEMA='database' and TABLE_NAME='table';
```

基于时间的盲注

```
1' and sleep(5)--'
```

归纳一下，主要有以下几点：

1.永远不要信任用户的输入。对用户的输入进行校验，可以通过正则表达式，或限制长度；对单引号和双"-"进行转换等。

2.永远不要使用动态拼装sql，可以使用参数化的sql或者直接使用存储过程进行数据查询存取。

3.永远不要使用管理员权限的数据库连接，为每个应用使用单独的权限有限的数据库连接。

4.不要把机密信息直接存放，加密或者hash掉密码和敏感的信息。

5.应用的异常信息应该给出尽可能少的提示，最好使用自定义的错误信息对原始错误信息进行包装

6.sql注入的检测方法一般采取辅助软件或网站平台来检测，软件一般采用sql注入检测工具jsky,网站平台就有亿思网站安全平台检测工具。

XSS跨站脚本攻击

- 跨站脚本（cross site script）为了避免与样式css混淆，所以简称为XSS。XSS是指恶意攻击者利用网站没有对用户提交数据进行转义处理或者过滤不足的缺点，进而添加一些代码，嵌入到web页面中去。使别的用户访问都会执行相应的嵌入代码。从而盗取用户资料、利用用户身份进行某种动作或者对访问者进行病毒侵害的一种攻击方式。

- XSS攻击的危害包括：
  1、盗取各类用户帐号，如机器登录帐号、用户网银帐号、各类管理员帐号
  2、控制企业数据，包括读取、篡改、添加、删除企业敏感数据的能力
  3、盗窃企业重要的具有商业价值的资料
  4、非法转账
  5、强制发送电子邮件
  6、网站挂马
  7、控制受害者机器向其它网站发起攻击

解决办法：
不信任任何客户端提交的数据，只要是客户端提交的数据就应该先进行相应的过滤处理然后方可进行下一步的操作。

web漏洞扫描

- AWVS
- APPSCAN
- Burpsuite

SSH暴力破解攻击

- 什么是SSH暴力破解攻击？

  - SSH暴力破解是指攻击者通过密码字典或随机组合密码的方式尝试登陆服务器（针对的是全网机器），这种攻击行为一般不会有明确攻击目标，多数是通过扫描软件直接扫描整个广播域或网段

- 怎样检测暴力破解攻击？

  i. 查看近期登陆日志：cat /var/log/secure
  ii. 计算近期失败的登陆次数：cat /var/log/secure|grep 'Failed passw ord for root'|w c -l
  宝塔面板上面的风险安全提醒是根据您的服务器日志统计出来的。

- 怎样防御暴力破解攻击？

  - 系统及网络安全
  i. 定期检查并修复系统漏洞
  ii. 定期修改SSH密码，或配置证书登陆
  iii. 修改SSH端口
  iv. 禁Ping
  v. 若你长期不需要登陆SSH，请在面板中将SSH服务关闭
  vi. 安装悬镜、云锁、安全狗等安全软件(只安装一个)
  - 购买企业运维版，开启安全隔离服务
  i. 宝塔企业运维版的安全隔离功能是专为拦截暴力破解而开发的功能
  ii. 安全隔离服务好比在您的服务器外面建立一道围场，只允许授权IP进来。

中间人攻击

- ARP 概念

  - ARP（Address Resolution Protocol）地址转换协议，工作在OSI模型的数据链路层，在以太网中，网络设备之间互相通信是用MAC地址而不是IP地址，ARP协议就是用来把IP地址转换为MAC地址的。而RARP和ARP相反，它是反向地址转换协议，把MAC地址转换为IP地址

- 防范ARP欺骗

  - 针对局域网
    1.在主机绑定网关MAC与IP地址为静态（默认为动态），命令：arp -s 网关IP 网关MAC
    2.在网关绑定主机MAC与IP地址
    3.使用ARP防火墙

  - 针对外网
    HTTPS加密