**WEB软件安全性测试课程**

**一、主讲老师**

顾翔

**二、培训内容背景**

 随着Web2.0、社交网络、微博等等一系列新型的互联网产品的诞生，基于Web环境的互联网应用越来越广泛，企业信息化的过程中各种应用都架设在Web平台上，Web业务的迅速发展也引起黑客们的强烈关注，接踵而至的就是Web安全威胁的凸显，黑客利用网站操作系统的漏洞和Web服务程序的SQL注入漏洞等得到Web服务器的控制权限，轻则篡改网页内容，重则窃取重要内部数据，更为严重的则是在网页中植入恶意代码，使得网站访问者受到侵害。  
 　　本课程将给大家介绍如何进行WEB软件安全测试

**三、课程介绍**

本课程总共8个大的章节，分别是“安全知识概要”“安全扫描工具”“前端安全性”“后端安全性”“APP安全高级安全技术安全测试步骤“实战”。

**四、培训对象**

软件安全测试工程师、软件测试高级工程师、软件测试经理、软件项目经理、软件安全领域相关人员

**五、学员基础**

有一定的软件测试经验，具有一定的Java、JavaScript、PHP或JSP脚本编码能力。数量掌握HTML、HTML5、XML

**六、教学时间**

3天

**七、教学内容**

1、安全知识概要

1.1 WEB安全知识

1.1.1 五大白帽子黑客

1.1.2 0 day & 1 day

1.1.3 白帽子兵法

1.1.4 同源策略

1.2 HTML知识概要

1.2.1 HTML数据包

1.2.2 HTML请求包

1.2.3 HTML响应包

1.2.4 HTML无连接性&无状态性

2、安全扫描工具

   2.1.1 Burp Suite

   2.1.2 AWVS

   2.1.3 AppScan

3、前端安全

3.1 XSS注入

       3.1.1 XSS注入介绍

         XSS原理

         XSS类型

         XSS会话挟持

         XSS蠕虫

       3.1.2 XSS测试技巧

          容易出现注入处

         富文本测试

          测试技巧

       3.1.3 XSS加固方法

          转义

OWASP ESAPI Encode

         其他API

         使用安全域

         加固总结

3.2 CSRF注入

3.2.1 CSRF原理

3.2.2 CSRF攻击场景-GET

3.2.3 CSRF攻击场景-POST

3.2.4 CSRF Test工具使用

3.2.5 CSRF token

3.2.6 CSRF防护方法

3.3点击挟持

3.3.1介绍

3.3.2 Google信息泄露事件

3.3.3测试方法

3.3.4防护方法

3.4 HTML5安全（0.5小时）

3.4.1 <audio>、<video>

3.4.2 iframe安全性

3.4.3 a标签的rel="noopener noreferrer" 属性

3.4.4 Canvas

3.4.5获取地理坐标

3.4.6本地存储

3.5 HTTP安全响应头

3.5.1安全响应头介绍

3.5.1工具

hsecscan

herokuapp

4、后端安全

4.1 SQL注入

4.1.1 SQL 注入基础知识

4.1.2 MySQL注入特性

4.1.3 SQL Server注入特性

4.1.4 Oracle注入特性简介

4.1.5测试方法和工具

SQL Map

Pangolin

Havij

4.1.6防护方法

4.2其他注入

4.2.1 XML注入

4.2.2 XPath注入

4.3.3 JSON注入

4.3.4 HTTP参数污染

4.3 信息侦探

4.3.1 Baidu Hack

4.3.2 Nmap

4.3.3 DirBuster

4.3.4指纹识别

4.4文件上传漏洞

解析漏洞

绕过上传漏洞

文本编辑器上传漏洞

修复上传漏洞

4.5 命令行漏洞

4.5.1 OS命令执行漏洞实例

4.5.2 PHP命令执行

4.5.3 JAVA命令执行

4.5.4框架执行漏洞

4.5.5防范命令行执行漏洞

4.6 XXE漏洞

4.6.1 XML介绍

4.6.2内部实体和外部实体

4.6.3参数实体

4.6.4通过XXE获取本地文件信息

4.6.5通过XXE获取远程文件信息

4.6.6 XXE加固措施

4.7文件包含漏洞

            4.7.1包含漏洞原理解析

            4.7.2 PHP命令执行

            4.7.3 JAVA命令执行

            4.7.4 构建安全的包含

4.8逻辑漏洞挖掘

            4.8.1水平越权

            4.8.2垂直越权

            4.8.3密码找回

            4.8.4支付漏洞

            4.8.5指定恶意账户登录-用户封锁

4.9加密与认证

            4.9.1对称密钥与非对称密钥

            4.9.2 MD5

            4.9.3认证防护

            4.9.4会话管理安全

            4.9.5 传输层安全

4.10 DDOS攻击

4.11 URL跳转与钓鱼

5、APP安全

5.1 APP安全介绍

5.2键盘挟持

5.3信息泄露

5.4 NFC卡信息泄露

5.5反编译工具介绍

            5.5.1 dex2jar+jdgui

            5.5.2 apktool

6、高级安全技术

6.1拖库

6.2暴力测试

6.3旁注攻击

6.4提权

6.5 ARP欺骗

7、安全测试步骤

7.1需求设计阶段

7.2代码阶段

7.3测试阶段

8 实战

案例：

演示二、Dom Bass XSS

演示三：cookie挟持

演示四：Post攻击

演示五：获取验证码

演示六：获取浏览器版本

演示七：绕过长度（一）用FireFox

演示八：绕过长度（二），用FireFox

演示九：绕过长度（三） 用FireFox

演示十：windows.name的妙用（一）

演示十一：windows.name的妙用（二）

演示十二：两种Cookie

演示十四：通过POST发送CSRF请求

演示十五：点击挟持（ClickJacking）

演示十六：HTML5 audio/video的支持

演示十七：验证码的破解

演示十八：显示当前坐标位置

演示十九：SQL注入的测试探索（一）,显示所有字段

演示二十：SQL注入的测试探索（二）,非法登录

演示二十一：检查数据库中是否存在某个表和某个字段

演示二十二:利用文件上传实现钓鱼

演示二十三:访问控制

演示二十四:绕过javascript控制

演示二十五:用FireFox开发者工具分析Referrer

演示二十六:iframe标签 用FireFox

演示二十七:HTTPOnly

演示二十八:PHP命令执行（一）代码执行

演示二十九:PHP命令执行（二）动态函数执行

演示三十:PHP命令执行（三）函数代码执行漏洞

演示三十一:PHP包含示例（一）本地包含

演示三十一:PHP包含示例（二）远程包含

演示三十二:PHP包含漏洞示例

演示三十三：JSP文件包含

演示三十四:HPP参数污染(一),PHP

演示三十五:HPP参数污染(二),JavaSevelet

演示三十六：参数污染(三)，绕过检查

演示三十七：客户端跳转

演示三十八：服务端跳转

演示三十八：钓鱼

演示三十九:模板安全

演示四十:构造PHP注入点

演示四十一:构造JSP注入点

演示四十二:CSRF攻击

演示四十三:xsser.me

演示四十四:XXE漏洞

演示四十五：HPP参数污染(二),jsp

演示四十六：显示本地浏览器及其版本

演示四十七：iframe属性

演示四十八：rel="noopener noreferrer"

演示四十九：防钓鱼

演示五十:CSRF注入

演示五十一:OS命令执行漏洞

演示五十二:PHP命令执行

演示五十三:命令行执行模型

演示五十四:CVE-2019-0803漏洞提权

演示五十五:XML注入

演示五十六:XPath注入

演示五十七:XXE for Java

演示:XXE for Java