Web安全入门篇

综合检测

Android 移动开发

目录 / CONTENTS

Part 01 Web 安全
介绍三种最常见的攻击手段

功能特点 Part 02
通过移动APP，进行Web测试

Part 03 后台服务及难点
扫描服务的搭建及APP实现的难点

功能演示 Part 04
演示APP的功能

Web安全

随着Web2.0、网络社交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，越来越多的应用都架设在Web平台上。Web业务的迅速发展吸引了黑客们的强烈关注，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。这使得越来越多的用户关注应用层的安全问题，Web应用安全的关注度也逐渐升温。

弱口令

弱口令：没有严格和准确的定义，通常认为容易被别人（他们有可能对你很了解）猜测到或被破解工具破解的口令均为弱口令。弱口令指的是仅包含简单数字和字母的口令，例如“123”、“abc”等，因为这样的口令很容易被别人破解，从而使用户的计算机面临风险，因此不推荐用户使用。

同时，提醒同学不要一直使用同一个密码。

Web安全

弱口令

案例 1. https://src.edu-info.edu.cn/post/16729/
2. https://src.edu-info.edu.cn/post/18565/
3. https://src.edu-info.edu.cn/post/16728/

Web安全

XSS检测

跨站脚本（英语：Cross-site scripting，通常简称为：XSS）是一种网站应用程序的安全漏洞攻击，是代码注入的一种。它允许恶意用户将代码注入到网页上，其他用户在观看网页时就会受到影响。这类攻击通常包含了HTML以及用户端脚本语言。

XSS攻击通常指的是通过利用网页开发时留下的漏洞，通过巧妙的方法注入恶意指令代码到网页，使用户加载并执行攻击者恶意制造的网页程序。这些恶意网页程序通常是JavaScript，但实际上也可以包括Java，VBScript，ActiveX，Flash或者甚至是普通的HTML。攻击成功后，攻击者可能得到更高的权限（如执行一些操作）、私密网页内容、会话和cookie等各种内容。

Web安全

反射型XSS　　最为常见

DOM型XSS　　通过DOM的节点触发，属于反射型XSS

存储型XSS　　可以存储于数据库

Web安全

Web安全

案例：

1.https://src.edu-info.edu.cn/post/15800/
2.https://src.edu-info.edu.cn/post/14750/

功能特点


功能特点
16:43
81
hlpureboy
登录
iu才是韩国妹子
16:43
81
弱口令
XSS检测
SQL注入
FQ二维码
18:17
76
112.74.204.232
检测
root:123pyj
18:18
76
202.194.188.29
检测
www:123456

功能特点

功能特点


112.74.204.232:5
000/
检测
http://112.74.204.232:5000//
<sCriPt>alert()</sCriPt>


zhbwdgsnry.asp?
gsid=5&cpfbfs=1
检测
http://222.206.181.203/bhdsweb/
zhbwdgsnry.aspgsid=Payload&cpfbf
s=1

后台服务及实现难点

后台实现： 1.python+Mysql
2.多个模块可以多次快速升级
3.实现速度快
4.poc方便实现

Android困难：1.申请网络权限
2.ListView的实现
3.如何发起网络请求
4.解析json数据
5.UI界面更新

功能演示