信息安全网站

转载

lover初学者 于 2018-02-22 11:43:20 发布 1413 收藏 3
文章标签： 信息安全网站
必备技能：
知识点：
一、常见数据库
Oracle、DB2、SqlServer、MySql、Access ..等

二、前端基础
JavaScript、CSS、HTML、ActionScript、Ajax、Jquery..

三、TCP/HTTP ..等协议
TCP、UDP、STMP、ICMP、ARP、
HTTP、SSL ...等

四、常见的上传/解析漏洞与版本
IIS、Nginx、Apache、
Fckeditor、Ewebeditor ..等

五、旁注、C段、CDN
椰树、御剑、layer ...

六、信息探测
端口、系统、DNS、域名、子域名、
目录、二级目录、语言、whois、
服务、Web容器、搜索引擎语法、
OA、Mail、旁站、C段、社工、
....等

七、漏洞利用
SqlMap、Metasploit、K8 ...

八、漏洞扫描/安全工具
AWVS、AppScan、Burp、Nikto2、
Vega、Safe3、WebInspect、
OWASPZAP、W3af、Netsparker、
Jsky、Nessue、WebScaerab、
N-Stealth、Weboecker ....
北极熊、椰树、御剑、Wpsan、wwwscan、
WebRobot、bugscan、X-Scan、OpenVAS、
cmsmap、LiQiDiS、zap ...

九、逻辑漏洞
用户密码重置、资料重置、
任意购买、刷积分 ...

十、暴力破解
端口、HTTP登陆口 ...等

十一、XSS
存储、反射、DOM
盲打、钓鱼、记录、XSS蠕虫、
XSS GETSHELL、Flash XSS...等

十二、CSRF
Cookie、Session机制、HTTP协议

十三、命令执行
Struts2命令执行、ThinkPHP命令执行、
PHP命令执行 ...等

十四、文件包含
本地包含、远程包含
...等

十五、注入
get注入、XML注入、Cookie注入、
HTTP请求头注入、Json注入、POST注入

十六、内网与提权
FTP提权、数据库提权、
启动项提权、后门维持访问、
虚拟主机提权、端口转发、
端口映射、劫持、爆破、泄露、
域渗透、
....等

十七、0day挖掘
开源-代码审计
非开源-逆向
安全产品（安全狗、护卫神、360）

十八、APT攻击与社工
信息刺探、心里学、潜伏能力、
针对性攻击、攻击的综合运用
信息泄露分析 ....等

漏洞挖掘：
开源-代码审计（Java、PHP ...等）
非开源-逆向（C/C++、C# ...等）
智能：（关键攻破点：可尝试通信）
有通信就有数据包....
尝试一切的可能连接无线网 Or 连接到你的电脑里
（系统升级、功能操作 ...）

没有渗透测试授权书情况下，一律算：攻击、违法
学习渗透测试，最好不去攻击以及试探别人的网站。
如果你想学习，请根据乌云以及其他漏洞平台，以及

你本地搭建网站进行漏洞复原等方式学习。
（千万不要直接看别人的教程，你也跟着你尝试攻击）
或许你心是好，但是对方就咬死你是攻击者！！！
小心谨慎...不要随波逐流去模仿别人！

移动：安卓、OC、Swift
脚本：Python、Perl、Ruby、Go
Win应用：C#、C/C++
服务端：PHP、ASP.NET、JavaWeb、ASP
Web前端：CSS、HTML、JavaScript、Jquery、Ajax
Linux：Python、Perl、Ruby、C/C++、Java、ShellCode
破解：汇编、反汇编、C

****

https://trailofbits.github.io/ctf/ --介绍
-->(翻译)http://blog.idf.cn/2015/02/ctf-field-guide/
****
综合：
http://wargame.kr/
http://www.ichunqiu.com/tiaozhans 《好多比赛题目都在里面》
http://www.simplexue.com/ctf/index 《西普学院》
http://canyouhack.it/
http://fun.coolshell.cn/
Online CTF:http://ringzer0team.com/challenges
****
i 春秋
http://www.ichunqiu.com/
网络信息安全攻防学习平台
http://hackinglab.cn/
白帽学院
http://www.baimaoxueyuan.com/
****
idf 实验室
http://ctf.idf.cn/
wechall
http://www.wechall.net/
**********合天
http://erange.heetian.com/
jctf
http://ctf.3sec.cn/
http://oj.xctf.org.cn/
****
渗透:
米安网
http://ctf.moonsos.com/pentest/index.php
http://webhacking.kr/
四叔叔写的一个http://hackit.sinaapp.com/
****
xss:
http://prompt.ml/0
http://xss.pkav.net/xss/
XSS:http://www.doscn.org/xss/
XSS:http://xss-quiz.int21h.jp/
XSS:http://escape.alf.nu/
实训平台:http://202.108.211.5/
****
逆向:

http://reversing.kr/
http://pwnable.kr/
http://exploit-exercises.com/
http://overthewire.org/
各种 writeup
https://github.com/ctfs/
bin 干货区
http://security.cs.rpi.edu/courses/binexp-spring2015/
各种赛事预告
https://ctftime.org/event/list/upcoming
继续补充：
SQL:
https://github.com/Audi-1/sqli-labs
sql:
http://redtiger.labs.overthewire.org/
****
http://ringzer0team.com/challenges --Online CTF
https://ctftime.org/ --ctf 竞赛时间
https://time.xctf.org.cn/ctfs/ --X-ctfhttp://ctf.sobug.com/Steganography.php --SSCTF --四叶草
https://bctf.cn/#/about --百度 ctf
http://www.hackdog.me/writeup/ --redrain 大大
https://www.cyberchallenge.com.au/solutions.html --国外站点
http://www.alictf.com/ --阿里 ctf
****
http://www.ichunqiu.com/ i 春秋 《推荐网站》
http://oj.xctf.org.cn/ --X-ctf 题目汇总
http://hackinglab.cn/ --网络信息安全攻防学习平台
http://hackgame.blackbap.org/ --习科
http://www.honyaedu.com/ -红亚
http://www.wechall.net/ --ctf 外国站点
http://ctf.idf.cn/ --IDF 实验室
http://ctf.3sec.cn/ --Jlu.CTF
http://erange.heetian.com/CTFrace.html --合天
http://www.simplexue.com/ --西普学院
http://1111.segmentfault.com/ --光棍节程序员闯关秀
http://www.helloisa.com/ --一个游戏又友链了几个游戏
https://redtiger.labs.overthewire.org/ --外国站点 web_sql
****
https://github.com/ctfs/ --git 上 writeup
http://bobao.360.cn/ctf/ --360 安全播报http://sec.yka.me/ --英文版 writeup
http://bobao.360.cn/ctf/learning/129.html --DUTCTF-2015-Writeup
http://ctf.idf.cn/index.php?g=portal&m=list&a=index&id=10 --writeup
https://ctf-team.vulnhub.com/ --国外 wp
https://www.91ri.org/9482.html --91ri
http://zhuanlan.zhihu.com/wooyun/19861125 --wooyun_writeup
http://drops.wooyun.org/?s=writeup&submit=%E6%90%9C%E7%B4%A2 --wooyun
****
http://attach.blackbap.org/down/ --习科工具下载
http://forum.cnsec.org/thread-93930-1-1.html --ctf_tools
http://mdsec.net/wahh/tools.html --tool 下载
http://tool.lu/ --在线工具集合
http://m.blog.csdn.net/blog/winkar/42458273 --一部分
http://www.ibeast.com/content/tools/ciscopassword/ --passwd_break
http://www.yellowpipe.com/yis/tools/encrypter/index.php --编码解码
http://www.jsfuck.com/ --js_fuck
http://www.objectif-securite.ch/ophcrack.php --hash 破解
****
http://217.logdown.com/ --217
http://www.blue-lotus.net --blue-lotus 蓝莲花

http://blog.0ops.net/ --0ops
http://le4f.net/ --le4f 大牛博客http://www.programlife.net/ --代码疯子
http://appleu0.sinaapp.com/ --apple 牛
http://www.syjzwjj.com/ --俊杰
http://blog.sycsec.com/ --三叶草
http://www.waitalone.cn/ --独自等待