

??(?129?)

[illegible]

????????????????? ?????,????? ?????? ?????????????????????????????? ???
 ?????????????????? ?????????????????????? ?

渗透测试基础篇			
章目	课程小节	章目	课程小节
第一章：渗透测试的常见环境搭建	ASP	第二章：HTTP协议讲解	魔法CMS的部署
	JSP		Apache Or Pylitudy
	PHP		环境搭建
	Tomcat安装		Tomcat
	dwms 漏洞演练平台安装及功能介绍		安装与介绍
	Linux Kali安装		kali
第二章：HTTP协议讲解	环境搭建之JAVA/Python	环境搭建	
	环境搭建集合之总结	安装安装	
	http协议的状态码及返回状态	状态码及返回状态有错错	
	常见的请求方式及消息	get, post, put的请求方式	
	消息中的作用	WAROCDF的扫描原理及地方	
第三章：常见Web后门木马的查杀方法	(1) ASP、PHP、JSP脚本后门手工及工具检测	手工及工具检测	
	(2) webshell后门手工及工具检测	漏洞木马病毒	
	(3) 中国菜刀后门检查	一句话木马病毒	
	(4) shift/放大键/等键后门木马查杀	后门木马病毒	
	(5) 免杀后门/后门用户等后门木马检测	后门木马病毒	
	(6) 病毒分析后门检测	病毒分析	
第四章：渗透测试中的信息收集	(1) 网站持有者信息收集	① 搜索引擎	
		② 站内搜集	
		③ 搜索引擎	
		④ whois查询	
		⑤ 管理用户	
	(2) 通过DOC搜集持有者信息	⑥ 安全策略的扫描	
		⑦ 搜索引擎	
		⑧ 安全策略	
	(3) 网站子域名收集	⑨ 安全策略	
		⑩ 安全策略	
		⑪ 安全策略	
		⑫ 安全策略	
第四章：渗透测试中的信息收集	(4) Google黑客语法的使用	关键词及敏感信息	
	(5) 目标开放服务探测	① 数据库介绍	
		② 数据库的C/S架构及探测	
		③ 数据库的C/S架构及探测	
		④ 数据库的C/S架构及探测	
	(6) 目标所属网络探测	⑤ 数据库的C/S架构及探测	
		⑥ 数据库的C/S架构及探测	
		⑦ 数据库的C/S架构及探测	
		⑧ 数据库的C/S架构及探测	
		⑨ 数据库的C/S架构及探测	
		⑩ 数据库的C/S架构及探测	
		⑪ 数据库的C/S架构及探测	
	⑫ 数据库的C/S架构及探测		
渗透测试漏洞原理篇			
章目	课程小节	章目	课程小节
xss漏洞讲解及防御	(1) 反射型xss注入漏洞原理剖析	命令执行漏洞讲解及防御	(1) 命令注入原理及常用命令
	(2) 存储型xss注入漏洞原理剖析		(2) 命令注入绕过过滤
	(3) dom型xss注入漏洞原理剖析		(3) 命令注入其他姿势
	(4) xss注入漏洞的防御及利用		(4) 如何在代码中防范
	(5) xss注入漏洞的防御及利用		(1) 文件包含漏洞原理
	(6) xss注入漏洞的防御及利用		(2) 文件包含漏洞利用之远程文件包含
csrf漏洞讲解及防御	(1) csrf漏洞的原理剖析	文件包含漏洞讲解及防御	(3) 文件包含漏洞利用之本地文件包含
	(2) csrf漏洞的防御及利用		(4) 如何修复文件包含漏洞
	(3) csrf漏洞的防御及利用		文件包含漏洞案例分析
	(4) csrf漏洞的防御及利用		(1) ssrf漏洞原理剖析
	(5) csrf漏洞的防御及利用		(2) ssrf漏洞与内网探测
	(6) csrf漏洞的防御及利用		(3) ssrf与redia联动getshell的技巧
sql注入漏洞讲解及防御	(1) sql注入原理	ssrf漏洞讲解及防御	(1) 业务逻辑漏洞的任意密码修改
	(2) 常用数据库注入		(2) 如何绕过网站密码修改验证
	(3) sql注入之读写文件		(3) 支付逻辑漏洞分析
	(4) sql注入之密码注入		(4) 四个业务逻辑漏洞案例分析
	(5) SQL注入之备注		
	(6) sql注入之执行命令		
文件上传漏洞讲解及防御	(1) 任意文件上传漏洞	业务逻辑漏洞讲解及防御	
	(2) java文件上传漏洞		
	(3) mine类型上传漏洞		
	(4) 条件竞争上传漏洞		
	(5) 内存溢出上传漏洞		
	(6) 服务器软件解析漏洞		
渗透工具篇			
章目	课程小节	章目	课程小节
Metasploit 渗透工具详解	(1) metasploit安装	扫描器工具技巧	(1) Burpsuite自带的scanner模块
	(2) metasploit使用介绍		(2) Awwws使用介绍
	(3) metasploit更新		(3) Nessus 使用介绍
	(4) metasploit多模块介绍		(4) Appscan 使用介绍
	(5) metasploit与nmap及nessus的协作		(5) Zap 使用介绍
	(6) metasploit实现渗透攻击		(6) Nikto 使用介绍
Nmap工具使用技巧	(7) metasploit后门利用	抓包/协议分析程序使用技巧	(7) Jispy 使用介绍
	(8) metasploit的安全引擎技术		Metasploit 实现扫描
	(9) metasploit授权技术及渗透测试		(1) Wireshark使用及xpcio分析pcap包文件
	(10) metasploit维护访问		(2) Flidder简单使用
	(11) Nmap 安装		(3) Burpsuite简介
	(12) Nmap 的脚本介绍		(4) Burpsuite安装及资源获取
kali	(13) 利用Nmap进行简单的扫描	国产优秀工具讲解	(5) Burpsuite代理设置
	(14) Nmap渗透的多种方式扫描		(6) Burpsuite抓包https响应及手机抓包方法
	(15) Nmap 的信息探测功能		(7) Burpsuite的Repeater模块讲解
	(16) Nmap与安全审计		(8) Burpsuite的Intruder模块讲解
	(17) Kali的优化工作		(9) Burpsuite的Comparer模块讲解
	(18) 常用信息搜集工具		(10) Burpsuite的Scanner模块讲解
总结篇	(19) 常用漏洞利用工具	分享各类实用脚本	(11) Burpsuite扩展插件
	(20) 常用漏洞利用工具		
总结篇课程		课程目录	
后台权限风险检查（上）	渗透测试常见错误理解纠正	上课方式：直播+录播+1对1问题解答	
后台权限风险检查（中）	Windows本地权限提升漏洞	报名方式：联系微信405221068	
后台权限风险检查（下）	Linux本地权限提升漏洞		
蚁安零基础课程未完结（编程篇）			
1. PHP编程基础篇	2. PHP代码审计篇	3. HTML基础+ClickJacking讲解	4. Python编程及安全脚本开发

??????????

[illegible][illegible]

???????????????? ???? ????????????? ???? ????????????? ????5????? ?????? ?
 ?????????? ????????? ???? ???? ?????? ?????? ?????????? ?????????
 ??? ?????????????? ????????????? ?????????????? ?

?????????????? ?????????????? ?????????????? ?????????? ??????????????????
 ?????? ?????????????????? ?????????????????? ?????????????????????? ?????????????????? ???
 ?????????? ?? ?

2.1?????

[illegible]

?????,???????????? ???? ????? ????????????? ?????? ????????????? ??????????????
?? ????????????? ????????? ?

2.2?????

????????? ?????????????? ?????????????????????????? ?????????????????? ??????????
 ????? ?????????????? ?????????????????????????????? ?????????????????? ?????????? ???
 ?????????? ??????????????? ??????? ?

??????????



????????????? ?????????????? ?????????????? ?????????????? ?????????? ?????????????? ??????????
? ?????????? ?????????????? ?

3???

????????????????????????? ?????????????????????? ?????????????????? ?????? ?????????????? ??????????????????
????????????????????? ?????????????????????? ?

4?????

[PDF?????????????????????.pdf](#) [word?????????????????????.doc](#) [?????????????????????](#) [?????????????????????](#)
[?????????????????](#) [?????????????????????????????????](#) [?????????????????????](#) [?????????????????????](#)
[?????????????????????????????????](#)

?????

??????????

????

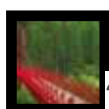
- ? ? ? ? ?
- ? ? ? ? ? 1970-01-01 08:00:00
- ? ? ? ? ? ? ?
- ? ? ? ? ? ? ? ? ? ?
- ? ? ? ? ¥74.00 ?
- ? ? ? ? ? ? ? ? ?



????

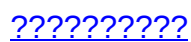
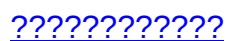
- • •

??56???



???

~~77~~ 52.???.????????????????????? ?????????? ???? ???? ?? ?



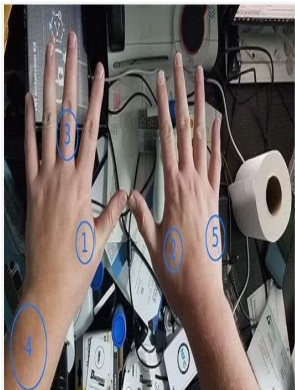
??????????



????????????????????



??????????????



????????

??????????



[????????????????](#)



[???????](#)

????
1205?
[??](#)

?????????
[??](#) | [????](#)