



第三届 全国网络与信息安全防护峰会

信息安全专业 - 大学生专业学习引导专场

对话·交流·合作

专业引导题目：Web安全实战

杨冀龙

知道创宇

现场演示

Windows 早期版本 系统登录绕过

net user wuda wudayinghuazhenhaokan /add



现场演示

路由器绕过登录

后门魔法: `xmlset_roodkcableoj28840ybtide`

现场演示

CMS绕过登录

CMS绕过登录原理



现场演示

Drupal博客系统注入漏洞 获取控制权

现场演示

震惊2014的破壳漏洞 获得控制权

```
() { ;; }; echo; /bin/cat /etc/passwd;
```

涉及的词汇概念



| | | | |
|-------|---------|---------|-------|
| 路由器 | Windows | 菜刀 | 输入法漏洞 |
| 后门 | Kali | Netcat | SQL注入 |
| 摄像头 | Linux | Firefox | 破壳漏洞 |
| 虚拟机 | Bash | Chrome | 登录绕过 |
| 网站 | Python | Hackbar | 后门控制 |
| | SQL | | |
| | CMS | | |
| | Drupal | | |
| | | | |

Web服务组件

插件或扩展

第三方内容：广告统计、mockup

Web前端框架：jQuery/Bootstrap/HTML5框架

Web应用：BBS/CMS/BLOG

Web开发框架：Django/Rails/ThinkPHP

Web服务端语言：PHP/JSP/.NET

Web容器：Apache/IIS/Nginx

存储：数据库存储/内存存储/文件存储

操作系统：Linux/Windows

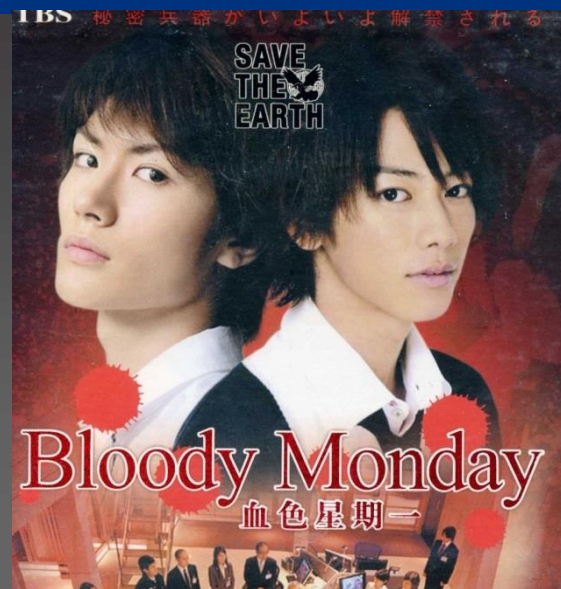
电影推荐

XDef 2014

黑客帝国



幽灵



剑鱼行动



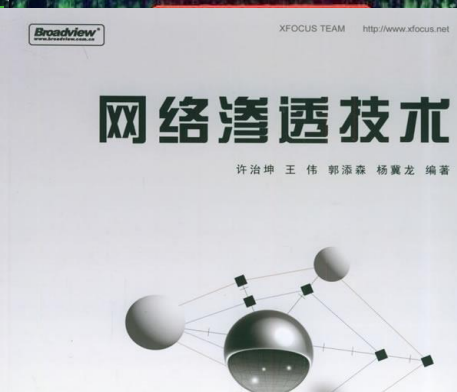
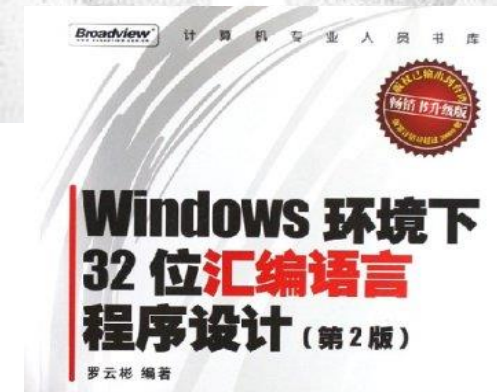
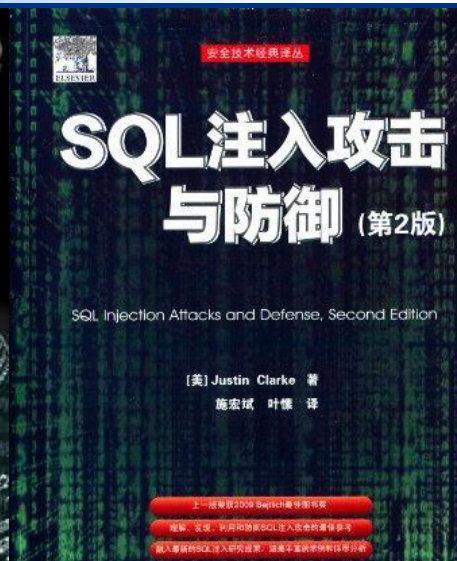
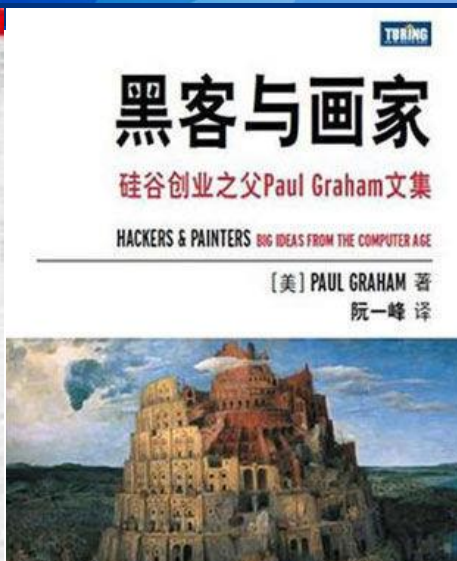
夏日大作战

- Python官方手册
- Python核心编程
- Bash新手指南
- 高级Bash脚本编程
- 深入理解计算机系统

.....



安全书籍



- Sebug: <http://www.sebug.net>
- 黑客防线: <http://www.hacker.com.cn/>
- WooYun: <http://www.wooyun.org/>
- FreeBuf: <http://www.freebuf.com/>
- EDB: www.exploit-db.com
- GitHub: <https://github.com/>



SEBUG

Security vulnerability DB

CTF夺旗赛



- SSCTF
- Alictcf: <http://alictf.com/>
- Bctf: <http://bctf.cn/>
- XDctf: <http://xdsec.org/>



知道创宇技能表

[http://blog.knownsec.com/Knownsec_RD_Ch
ecklist/v2.2.html](http://blog.knownsec.com/Knownsec_RD_Ch
ecklist/v2.2.html)



学习平台



- 漏洞靶场环境
- 漏洞分析文档
- 漏洞验证程序

| 名称 | 修改日期 | 类型 | 大小 |
|--|------------------|-------|-------|
| _0822_nginx_0_8_57_resolve_error.py | 2013/8/8 13:34 | PY 文件 | 7 KB |
| _0824_bom_bom_info_disclosure.py | 2013/8/8 13:34 | PY 文件 | 6 KB |
| _0825_supernews_2_6_1_funcao_sql_inj.py | 2013/8/8 13:34 | PY 文件 | 4 KB |
| _0826_alpaca_3_3_2_elem_sql_inj.py | 2013/8/8 13:34 | PY 文件 | 6 KB |
| _0827_5ucms_1_2_2024_ajax_sql_inj.py | 2013/8/8 13:34 | PY 文件 | 5 KB |
| _0828_6kbbs_8_0_ajaxmemeber_privilege_escalation.py | 2013/8/8 13:34 | PY 文件 | 6 KB |
| _0829_galette_0_63_3_picture_class_sql_inj.py | 2013/8/8 13:34 | PY 文件 | 4 KB |
| _0830_galette_0_63_3_picture_class_file_upload.py | 2013/8/8 13:34 | PY 文件 | 4 KB |
| _0831_fckeditor_2_4_3_upload_file_upload.py | 2013/8/8 13:34 | PY 文件 | 7 KB |
| _0832_phpcms_2008_field_sql_inj.py | 2013/8/8 13:34 | PY 文件 | 6 KB |
| _0833_jaow_2_4_5_ons_sql_inj.py | 2013/8/8 13:34 | PY 文件 | 6 KB |
| _0834_php_cgi_5_3_12_main_rfi.py | 2013/8/8 13:34 | PY 文件 | 9 KB |
| _0835_wp_property_1_35_0_uploadify_file_upload.py | 2013/8/8 13:34 | PY 文件 | 7 KB |
| _0836_phpldapadmin_1_2_1_1_function_code_exec.py | 2013/8/8 13:34 | PY 文件 | 8 KB |
| _0837_hdwiki_5_1_user2_remote_pass_change.py | 2013/8/8 13:34 | PY 文件 | 5 KB |
| _0838_cmseasy_5_0_act2_privilege_escalation.py | 2013/10/16 11:27 | PY 文件 | 5 KB |
| _0839_fckeditor_2_2_upload_file_upload.py | 2013/8/8 13:34 | PY 文件 | 5 KB |
| _0840_aspcms_2_0_reg_remote_pass_change.py | 2013/8/8 13:34 | PY 文件 | 5 KB |
| _0841_5ucms_3_mobile_index_sql_inj.py | 2013/8/8 13:34 | PY 文件 | 4 KB |
| _0842_metinfo_4_0_save_remote_pass_change.py | 2013/8/8 13:34 | PY 文件 | 5 KB |
| _0843_lxscms_1_5_info_sql_inj.py | 2013/8/8 13:34 | PY 文件 | 5 KB |
| _0844_testlink_1_9_3_getrequirementnodes_sql_inj.py | 2013/8/8 13:34 | PY 文件 | 4 KB |
| _0845_uccass_1_8_1_classes_results_class_sql_inj.py | 2013/8/8 13:34 | PY 文件 | 6 KB |
| _0846_shopex_4_8_5_goods_sql_inj.py | 2014/3/21 16:45 | PY 文件 | 6 KB |
| _0847_struts_2_1_8_1_code_exec.py | 2013/8/8 13:34 | PY 文件 | 26 KB |
| _0848_iis_7_5_short_filefolder_name_info_disclosure.py | 2013/8/8 13:34 | PY 文件 | 11 KB |
| _0849_freebsd_8_3_telnetd_buffer_overflow.py | 2014/1/20 16:52 | PY 文件 | 8 KB |
| _0850_wordpress_3_4_1_functions_path_disclosure.py | 2013/8/8 13:34 | PY 文件 | 6 KB |
| _0851_solaris_11_telnetd_login_bypass.py | 2013/8/8 13:34 | PY 文件 | 4 KB |
| _0852_phpcms_9_search_index_ffi.py | 2013/8/8 13:34 | PY 文件 | 4 KB |
| _0853_jboss_5_1_0_code_exec.py | 2013/8/8 13:34 | PY 文件 | 9 KB |
| _0854_phpcms_2008_block_inc_code_exec.py | 2013/8/8 13:34 | PY 文件 | 8 KB |
| _0855_phpcms_2008_product_code_exec.py | 2013/8/8 13:34 | PY 文件 | 7 KB |
| _0856_phpcms_9_17_add_favorite_sql_inj.py | 2013/8/8 13:34 | PY 文件 | 6 KB |
| _0857_dedecms_5_7_ajax_membergroup_sql_inj.py | 2013/8/8 13:34 | PY 文件 | 5 KB |
| _0858_phpcms_9_17_wap_sql_inj.py | 2013/8/8 13:34 | PY 文件 | 7 KB |
| _0859_hdwiki_5_1_gift_sql_inj.py | 2013/8/8 13:34 | PY 文件 | 8 KB |
| _0860_eschop_2_7_2_flow_sql_inj.py | 2013/8/8 13:34 | PY 文件 | 5 KB |
| _0861_phpmyadmin_3_5_2_2_sync_backdoor.py | 2013/8/8 13:34 | PY 文件 | 3 KB |

1000多个真实
漏洞模拟环境

方法

兴趣是最好的老师



@刘-开水

1万小时定理

作家格拉德威尔指出：

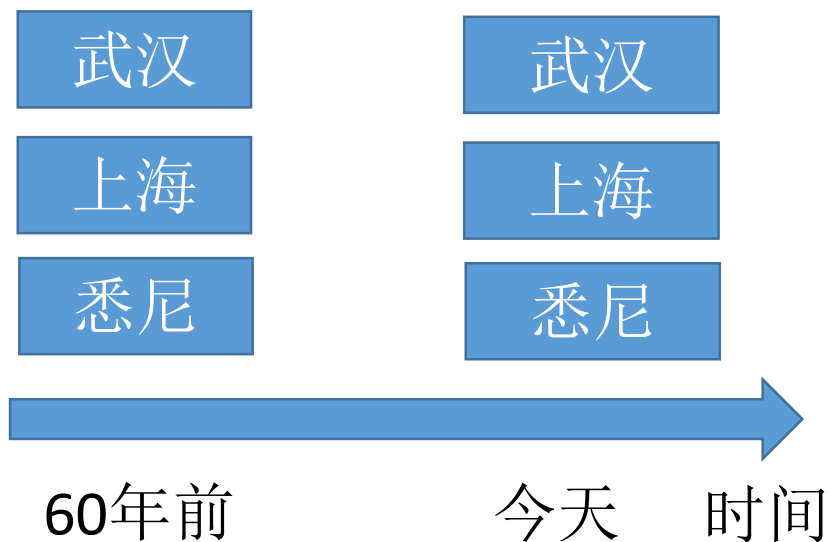
“人们眼中的天才之所以卓越非凡，并非天资超人一等，而是付出了持续不断的努力。只要经过1万小时的锤炼，任何人都能从平凡变成超凡。”




绝大部分失败者输在拼汗水阶段，还谈不上拼天赋

批判性思维

```
D:\gcc> dir
gcc.exe  gcc.c
运行
D:\gcc\gcc.exe gcc.c
会新生成一个gcc.exe
```







**这个世界是邪恶的
不是因为那些邪恶的人
而是那些无动于衷的人**



知道创宇：老杨
微信：laolaoyangyangyang

