NDG

NETLAB+®

ETHICAL HACKING V2
LAB SERIES

Lab 24: Web-Based Hacking

Document Version: 2021-05-18

| Material in this Lab Aligns to the Following	
Books/Certifications	**Chapters/Modules/Objectives**
All-In-One CEH Chapters ISBN-13: 978-1260454550	3: Scanning and Enumeration 6: Web-Based Hacking: Servers and Applications
EC-Council CEH v10 Domain Modules	2: Footprinting and Reconnaissance 11: Session Hijacking 14: Hacking Web Applications

Contents

Introduction

Most online services are implemented on web applications. In this lab, we will focus on identifying vulnerabilities, misconfigurations, and unpatched security flaws in web-based applications.

Objectives

- Footprinting and Enumerating
- Perform an OWASP Top 10 Attack
- Cookie Manipulation

Lab Topology
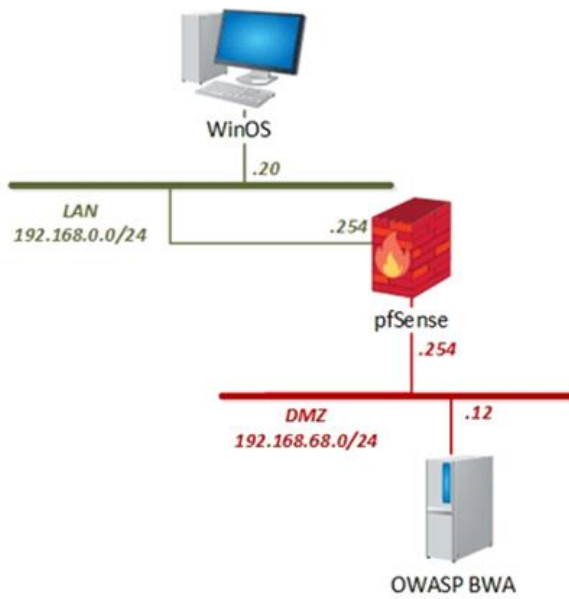
Lab Settings

The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address / Subnet Mask	Account (if needed)	Password (if needed)
WinOS	192.168.0.20	Administrator	Train1ng$
OpenSUSE	192.168.0.30	osboxes	osboxes.org
OWASP BWA	192.168.68.12	root	owaspbwa

# 1   Vulnerability Scanning with Subgraph's Vega

Vulnerability scanning is a great way to start a web server penetration test. Many vulnerability scanners exist but we will use the open-source scanner called Vega for this exercise. Using this tool, we can target a specific IP address or URI and collect information about the system. Vulnerability scanners can be "noisy" depending on how they were configured. We will not pay attention to that in this lab, however. Instead, we will run a scan on a vulnerable server and look at some of the results.

1. launch the **WinOS** virtual machine to access the graphical login screen.
   1.1. Select **Send CTRL+ALT+DEL** from the dropdown menu to be prompted with the login screen.
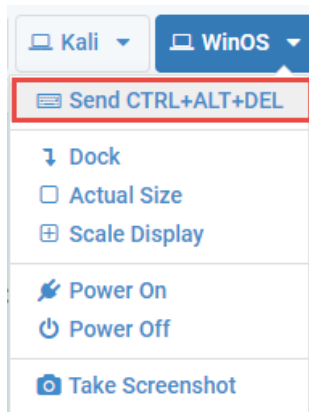
    1.2. Log in as `Administrator` using the password: `Train1ng$`

2. Let us begin by opening the *Vega* software. To do this, navigate to **Start > Vega > Vega,** as seen in *items* **1, 2,** and **3** below. Alternatively, you can open it by clicking the **Vega** icon from the Desktop.
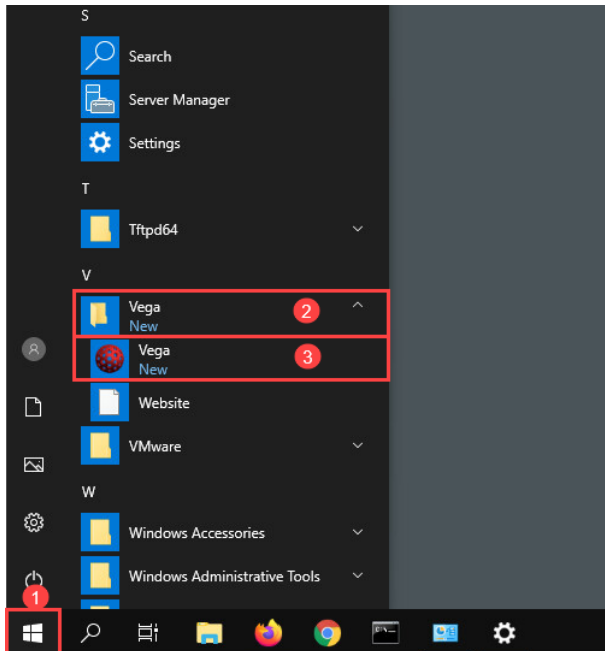
3. The *Vega* main window will open, as seen below. The table below the following screenshot outlines the different features that we will be using in this exercise.
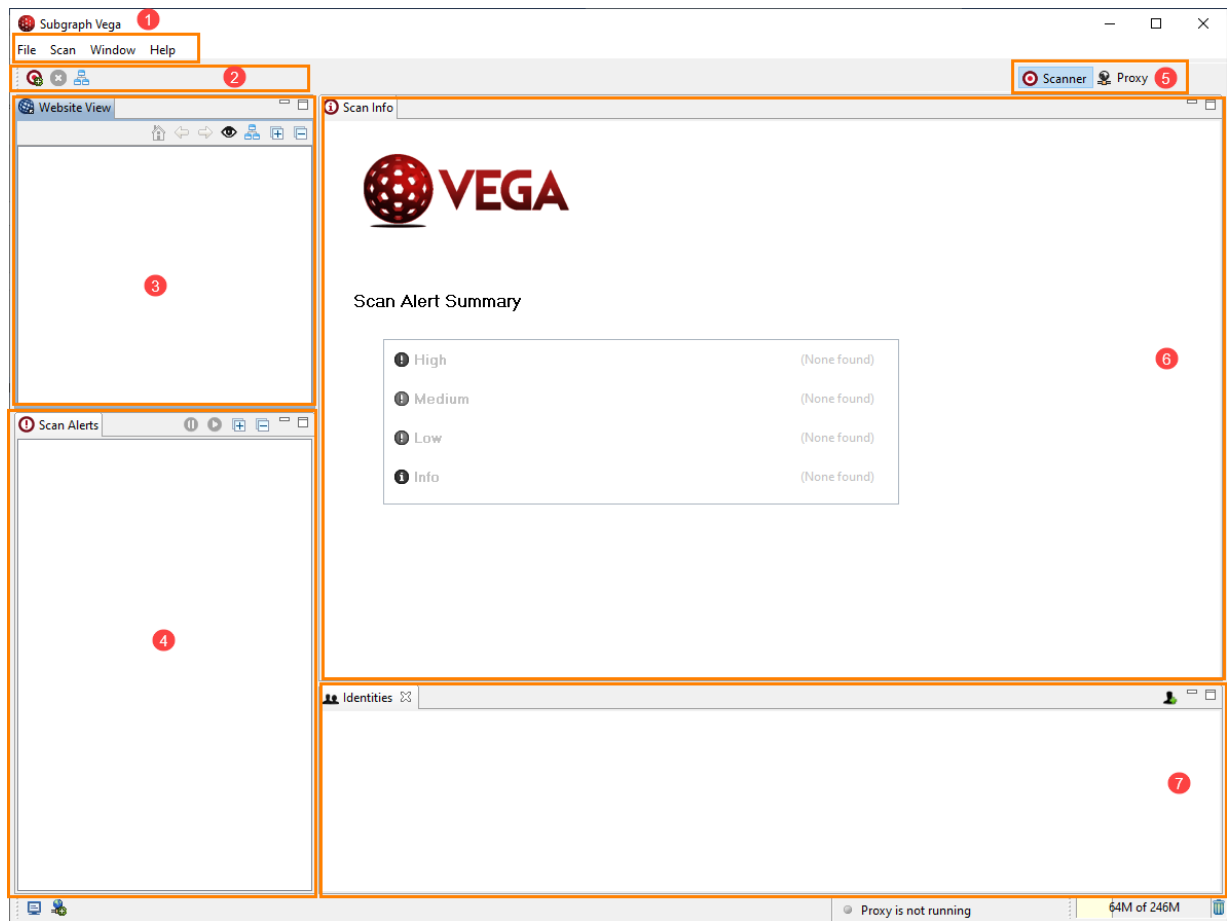

| #	Name	Description
1	Menu bar	Contains options to reset the windows, start a scan and adjust preferences etc.
2	Toolbar	Has quick access icons that you can use to run/stop a scan or edit the scan parameters
3	Website View pane	Contains the IP address or URLs of the scanned systems
4	Scan Alerts pane	Contains details of vulnerabilities
5	Scanner/Proxy tab	Allows you to choose between a vulnerability scanner or a proxy server
6	Scan Info pane	Shows the scan progress and gives a summary of the identified vulnerabilities
7	Identities	Allows you to add user credentials to allow automated login and scanning

4. Now that you are more familiar with the tool, let us test it out by scanning a specific web page. To begin, navigate to **Scan** and click **Start New Scan,** as seen in *items* **1** and **2** below.
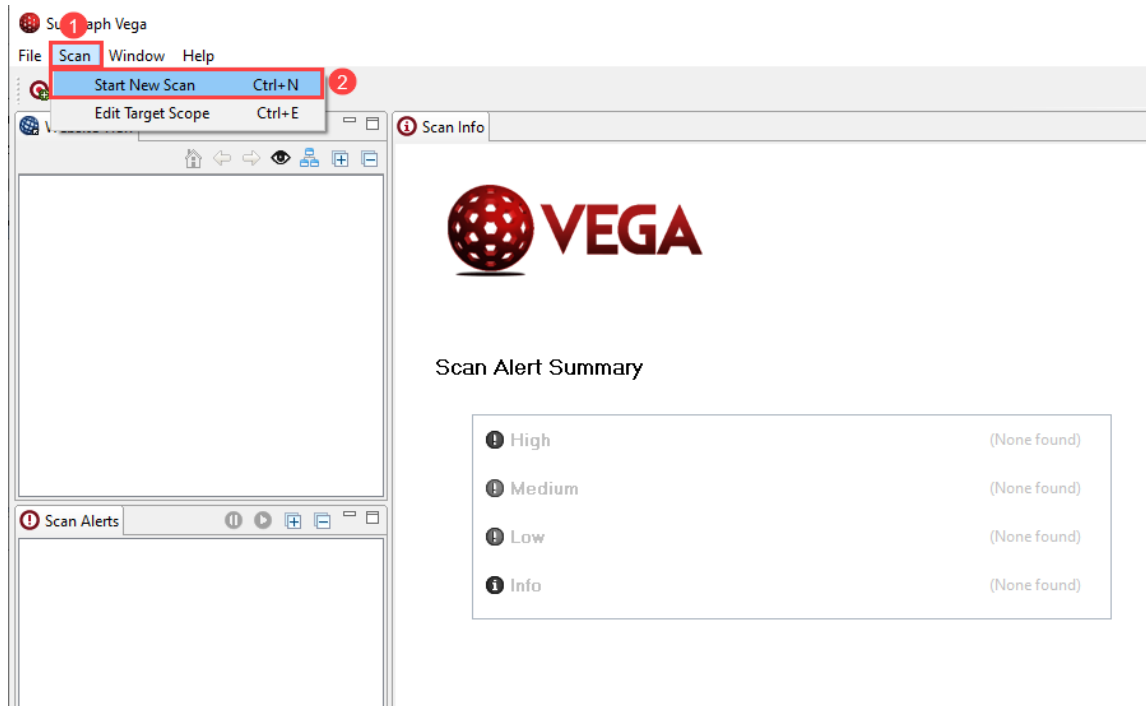

5. The *Select a Scan Target* window will appear as seen below. Enter the following IP address **192.168.68.12** in the *Scan Target* field as seen in *item* **1** below. Once it is entered, click **Finish,** as seen in *item* **2.**
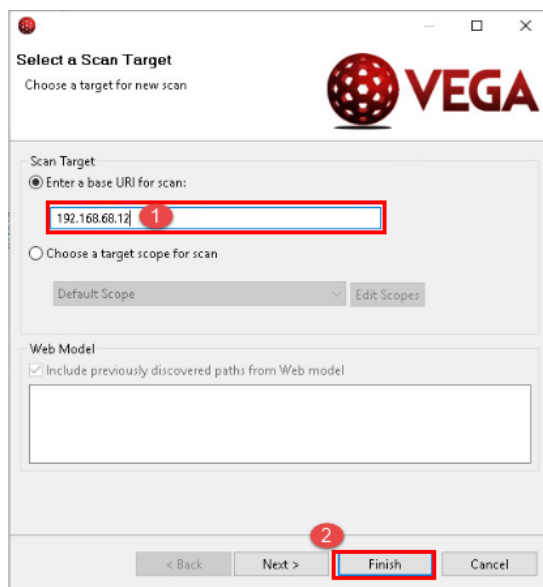
6. The scan will begin, and you can see the progress in the *Scan Info* window. This scan will take a long time, so we will stop the scan after it displays *11 out of,* as seen in *item* **1** below. To stop the scan, click the **Stop** icon seen in *item* **2** below. This will stop the scan abruptly. In the real world, we would allow it to run until complete or until practicable.
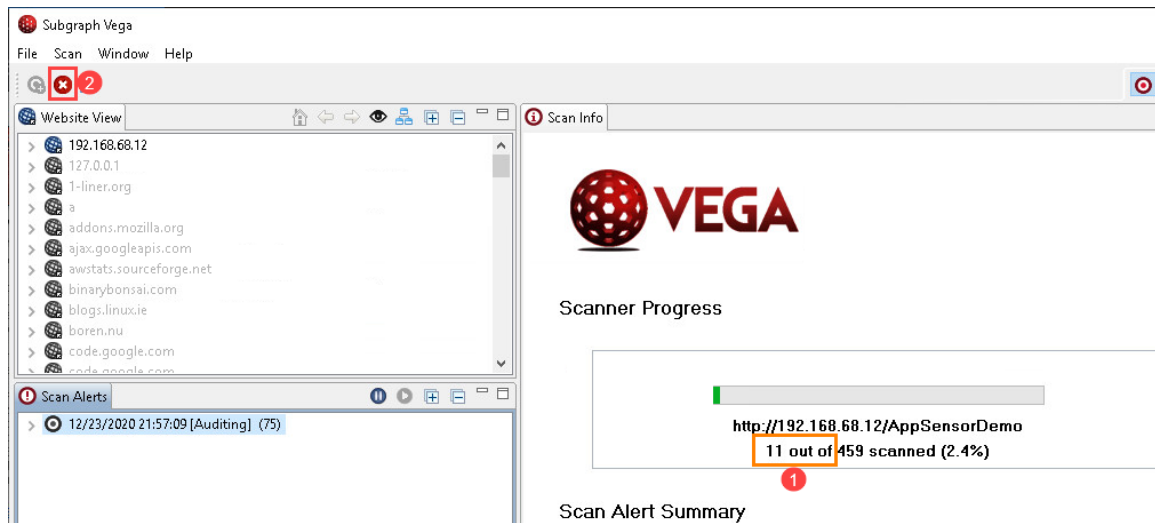

7. Now let us look at some of the results from the scan. The results can be seen in the *Scan Info* window seen in *item* **1.** As you can see, the scan revealed several results even though it was running for a short time. The name of the vulnerabilities can be seen in *item* **2,** and their severity can be seen in *item* **3.** You can scroll down using the scroll bar or the down arrow button seen in *item* **4**. This will reveal additional categories of results.
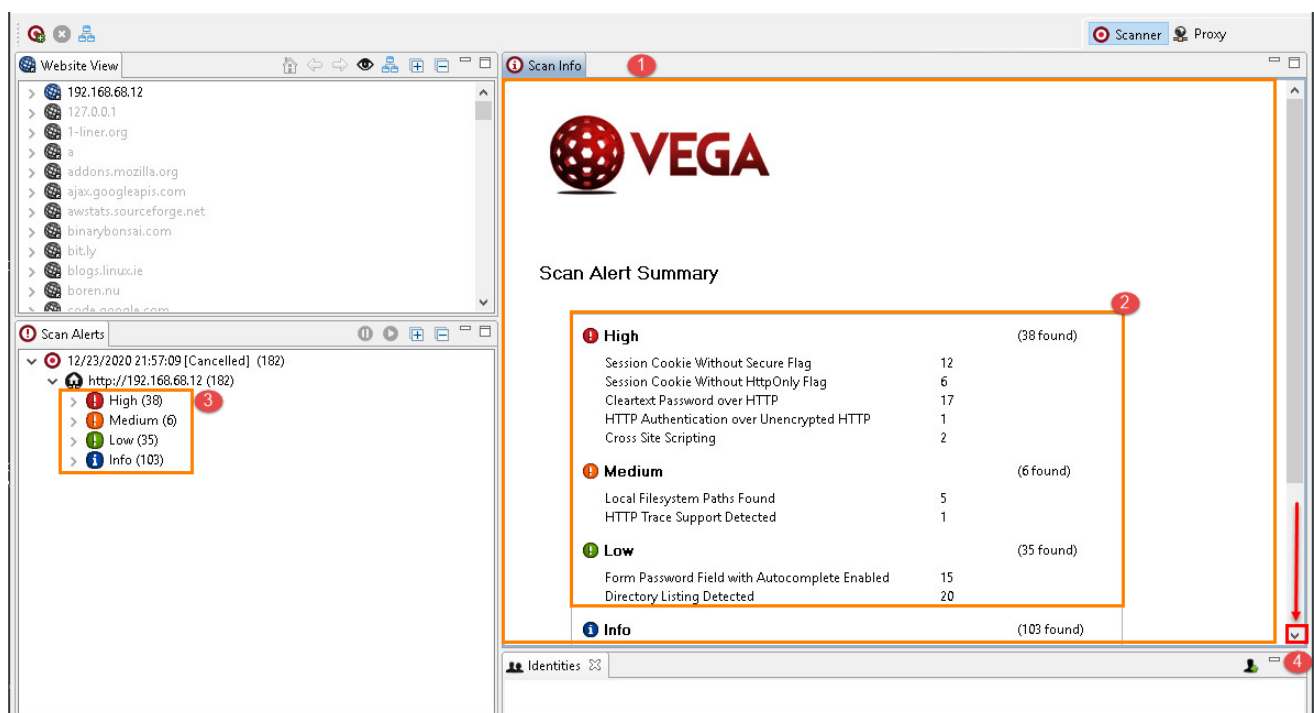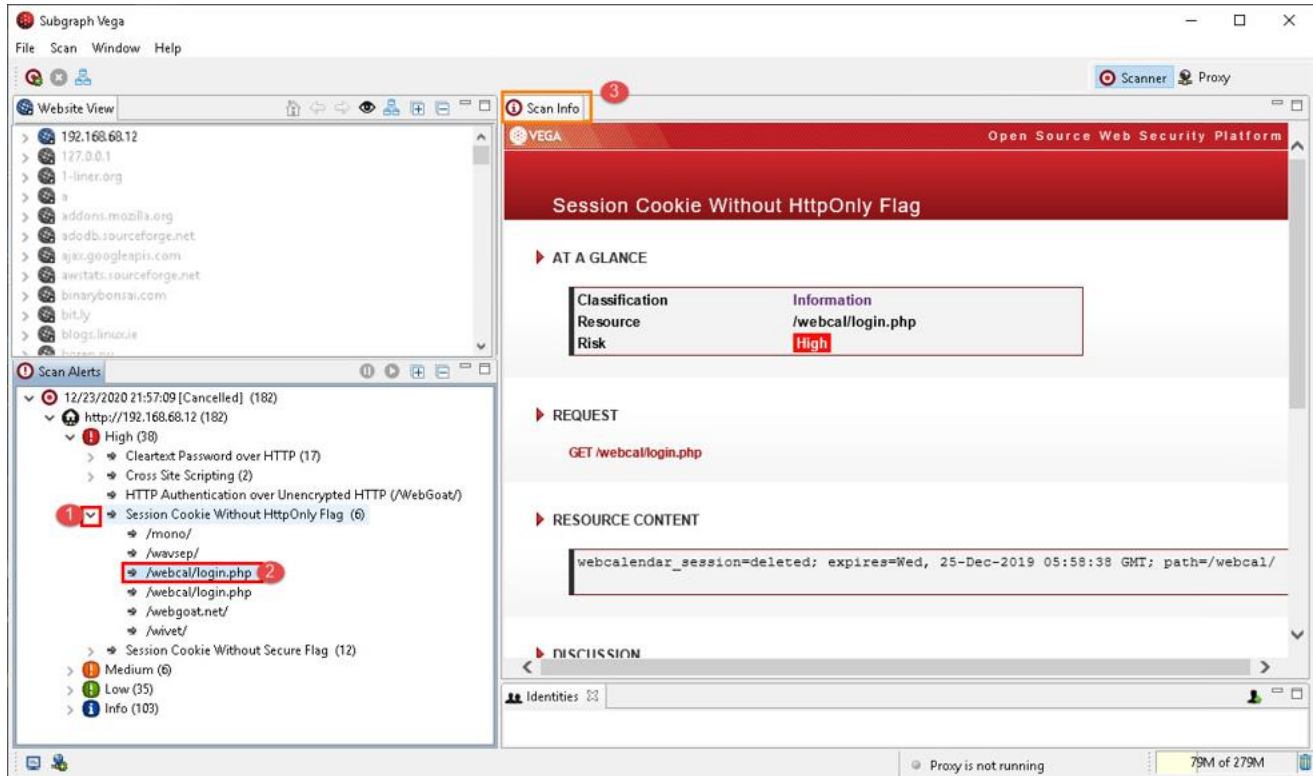
8. As you can see from the summary, there are lots of vulnerabilities in this target system, and there are several severe/critical vulnerabilities, which fall under the category *High,* that should be patched as soon as possible. Let us learn some more about one of these vulnerabilities. To do this, go to the *Scan Alerts* pane seen in *item* **1,** and click the arrow beside the entry for the scan you just ran to expand it as seen in *item* **2**.
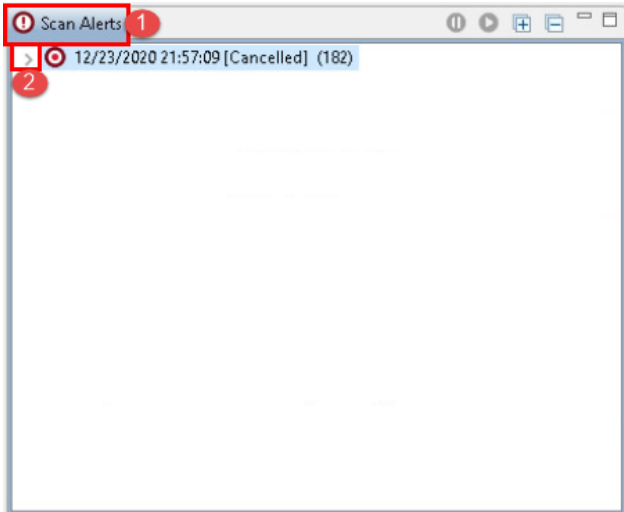
9. Next, click the arrows beside **http://192.168.68.12** to reveal the different categories of results, as seen in *item* **1** below. Once done, click the arrow beside **High** to expand it and reveal the vulnerabilities that are considered critical, as seen in *item* **2**.
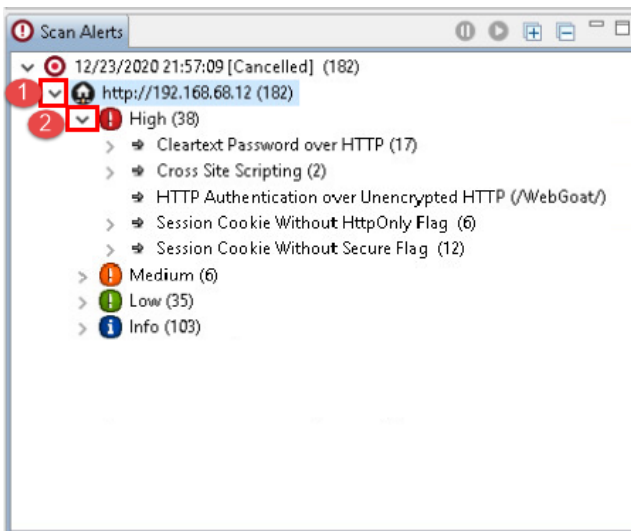
10. Now that we see the list of vulnerabilities, you can click on each one and view the details of the vulnerability in the *Scan Info* pane. Let us look at the results for **Session Cookie Without HttpOnly Flag** by clicking the arrow beside it, as seen in *item* **1.** As you can see, the different web resources where the vulnerabilities were found are listed. Click any of the results and then view the details in the *Scan Info* pane as seen in *items* **2** and **3** below.

11. In the *Scan Info* pane, you can see the name of the vulnerability seen in *item* **1,** the *AT A GLANCE* row that contains a summary of the details seen in *item* **2,** the *REQUEST* row that shows the request that *Vega* made seen in *item* **3** and the *RESOURCE CONTENT* row that shows the data inside the resource seen in *item* **4.**
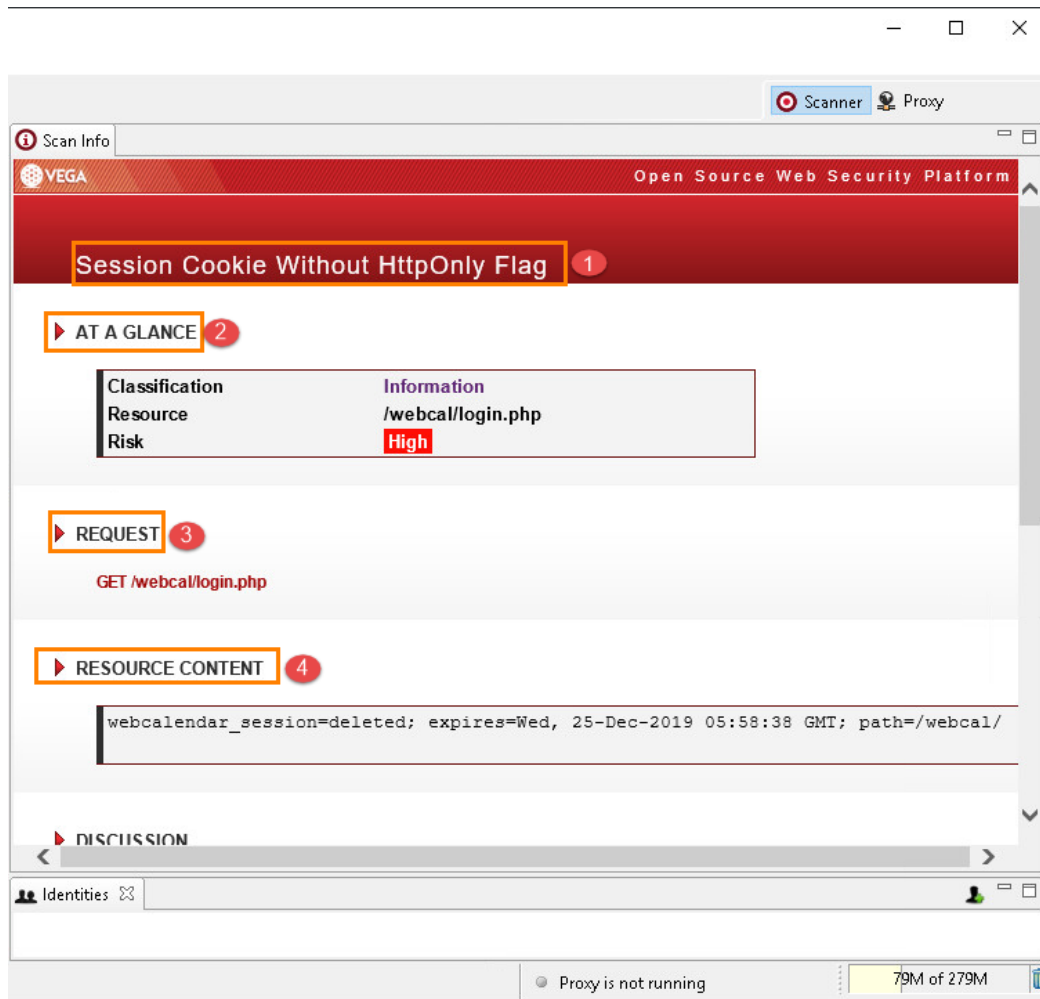
12. To see more information, use the scroll bar or the down arrow button as seen in *item* **1** to scroll down. There you will see the *DISCUSSION* row, which provides the specific details of the vulnerability as seen in *item* **2.** Next is the *REMEDIATION* row that tells you (generally) how to fix the problem, as seen in *item* **3**. Finally, the *REFERENCES* column provides links to the source of information about the vulnerabilities, as seen in *item* **4**.
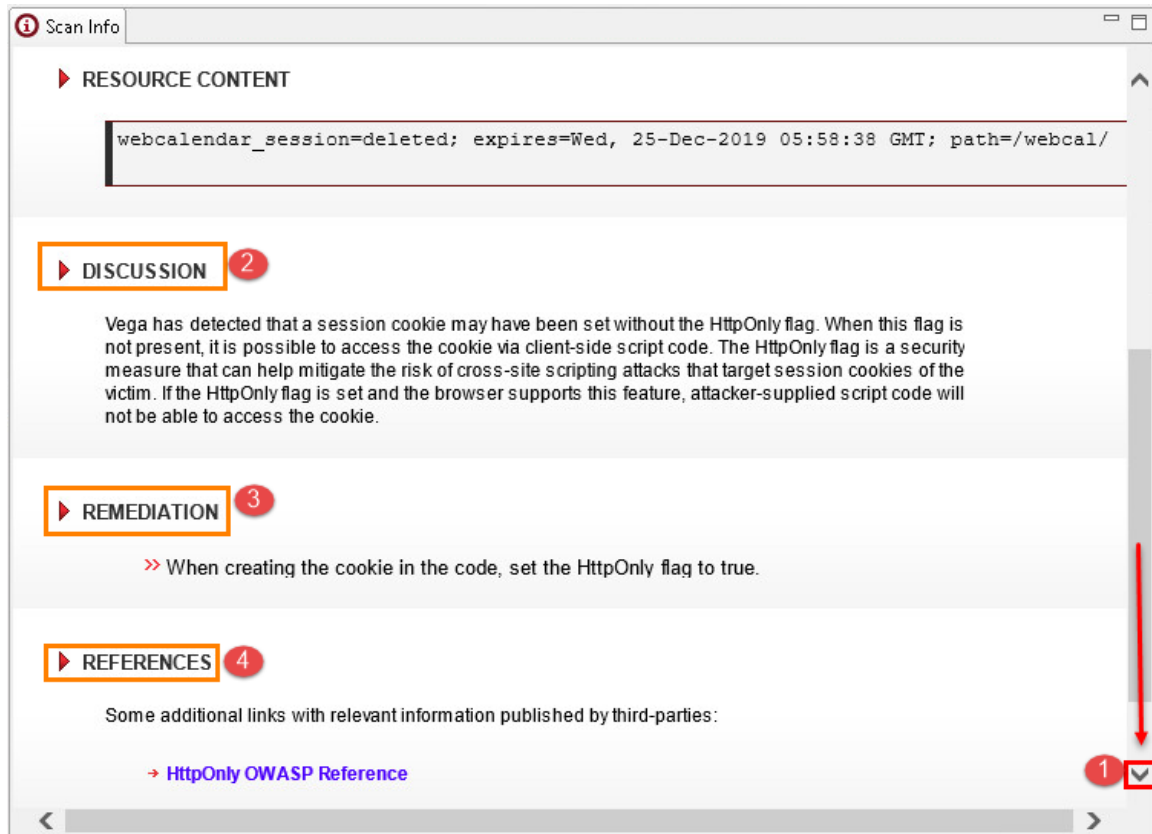
13. Feel free to review the different vulnerabilities that were identified and see what you can learn about them. Once you are done, close the *Vega* by clicking the **X** at the top-right corner of the main window to close it.
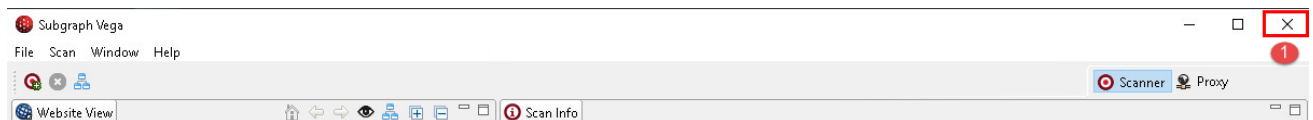
14. In the next exercise, we will perform some web hacking using the *Web Goat* platform.

2   Spoofing an Authentication Cookie

Since we discovered some session management vulnerabilities in the last exercise, we will be attempting to Spoof an Authentication Cookie which will allow us access to a web page that contains information that was not intended for us. Let us begin by starting up *Web Goat.*

1. To do this, navigate to **Start > Firefox,** as seen in *items* **1** and **2** below. Alternatively, you can click the **Firefox** icon from the taskbar, as seen in *item* **3** below.
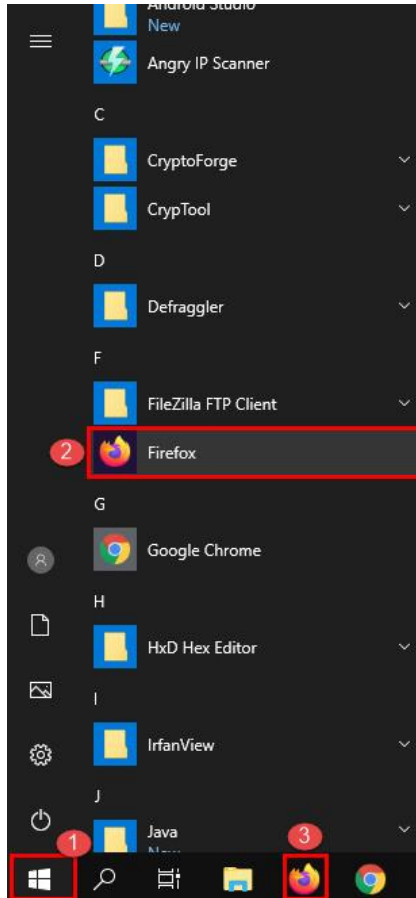
2. The *Firefox* web browser will appear. Navigate to the address bar, click inside it and type `192.168.68.12` as seen in *item* **1** below. This will open the OWASP server main window. Click the **OWASP WebGoat** option, as seen in *item* **2** below.
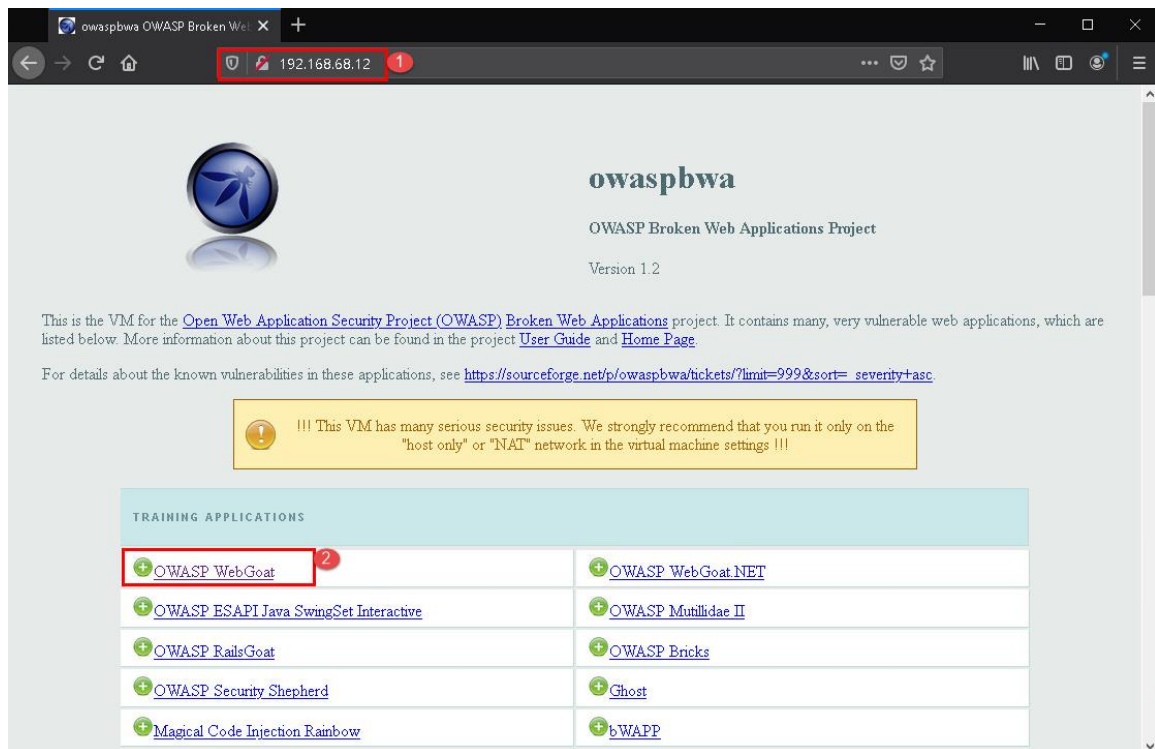
3. You will be prompted to enter a username and password. Log in with `root` and `owaspbwa` in the login window that appears, as seen in *item* **1,** to log in to the *WebGoat server*.
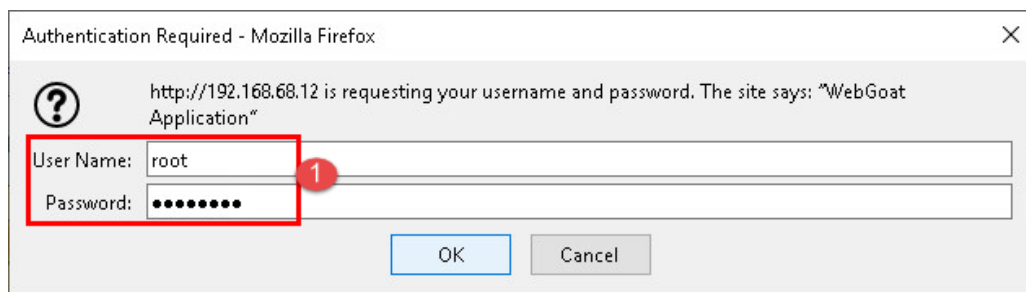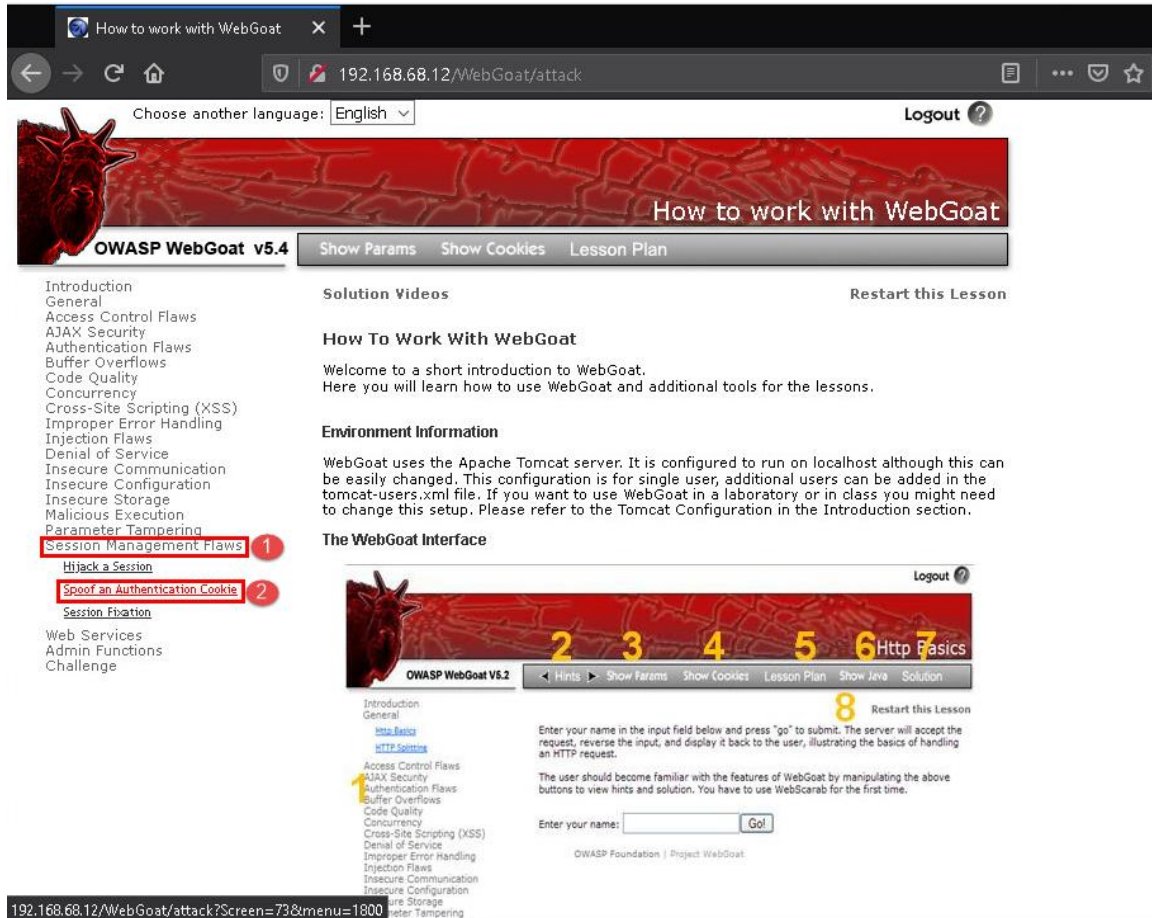
4. The *WebGoat* main window will appear. *WebGoat* is an intentionally vulnerable web application that contains several different exercises and is designed for teaching penetration testing. Once you are done reading the information on the main window, click **Start WebGoat,** as seen in *item* **1** below.
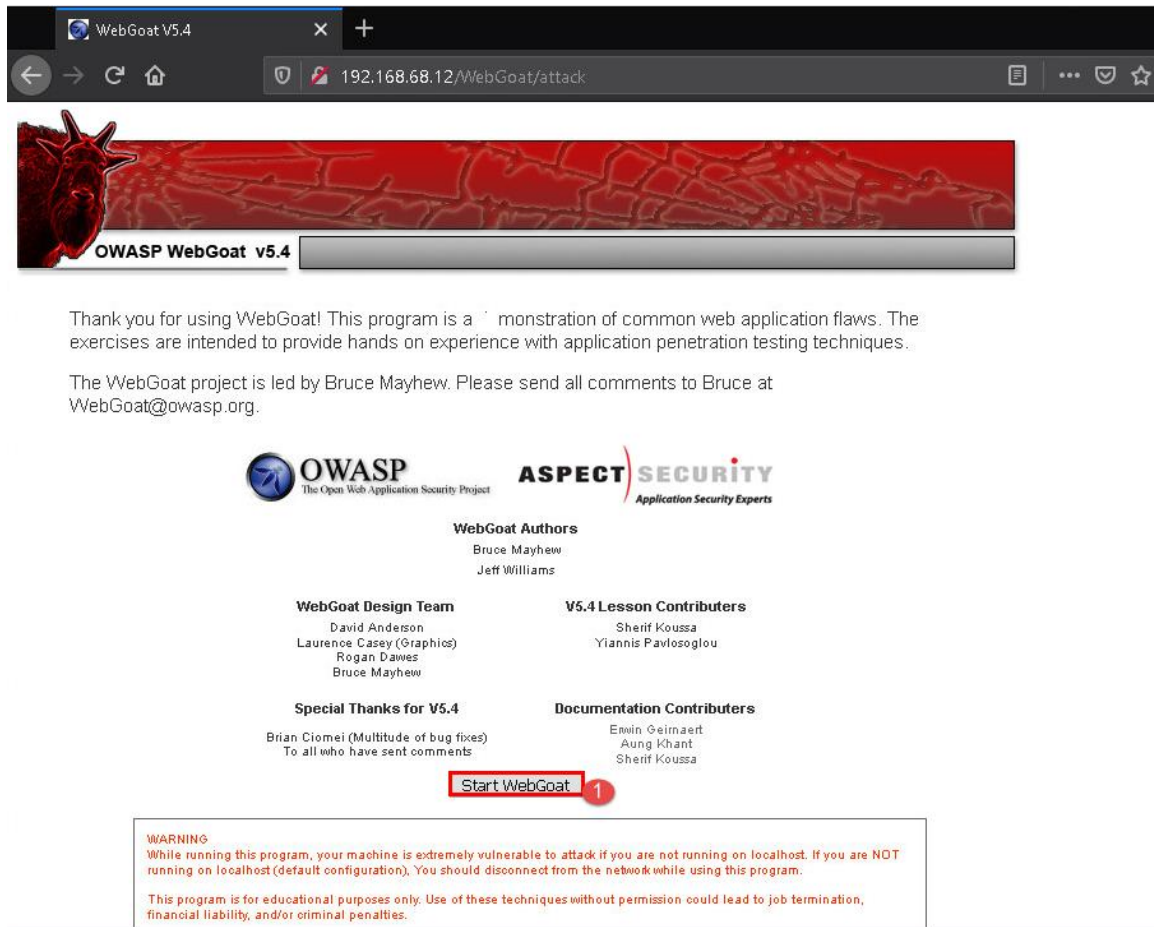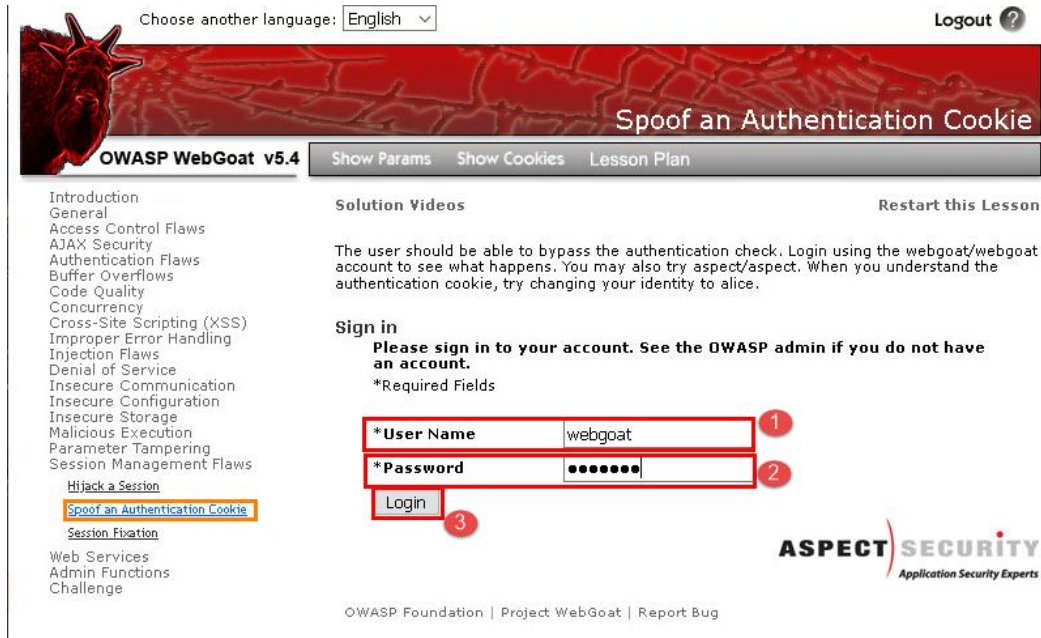
5. You will be taken to the *Introduction* window, which will teach you how to navigate *WebGoat*. Once you are done reading through the information on the page, navigate to **Session Management Flaws > Spoof an Authentication Cookie** as seen in *items* **1** and **2** below.

6. You will be taken to the *Spoof an Authentication Cookie* page, where you will see the instructions for the exercise. Read the instructions before beginning. Now type **webgoat** in the *User Name* and *Password* fields as seen in *items* **1** and **2** below. Once you are done typing, click **Login,** as seen in *item* **3.**

7. You will be authenticated and taken to a private page that displays the message, "*Your identity has been remembered*." Now, let us look at the authentication cookie to see if the session ID can be identified. The session ID is the value we need to use to imitate the authentication cookie. To begin, click on the **Open Menu** button at the top-right corner of *Firefox's* main window, as seen in *item* **1**. Next, click the **Web Developer** option from the dropdown menu that appears, as seen in *item* **2**.
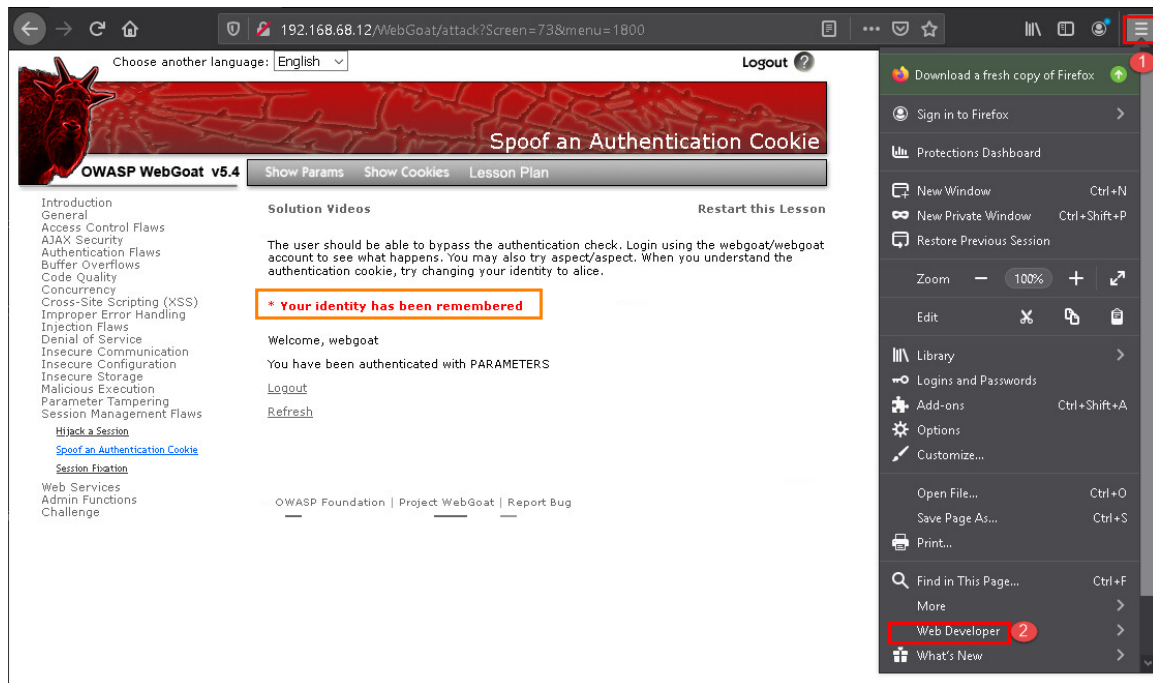

8. The *Web Developer* menu will appear. Click **Storage Inspector** to open it, as seen in *item* **1**. Since this view has several different options that we will not be using for this exercise, we will get to know the features as we go.
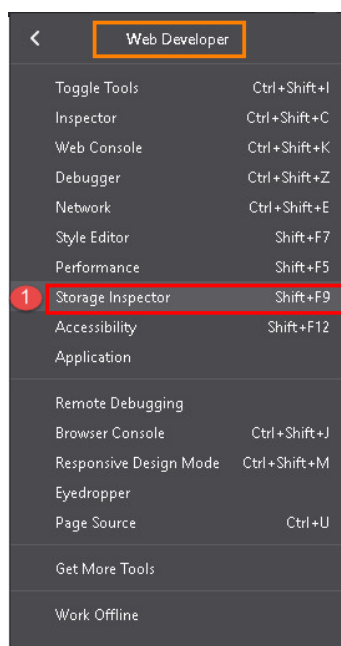
9. The *Storage Inspector* is one of the web developer tools provided by the *Firefox* web browser and allows you to inspect different types of storage that a web page uses. Since we are focused on the authentication cookie, the storage type we will focus on is the *Cookies* storage. Once the *Storage Inspector* opens, a pane will appear at the bottom of the *Firefox* main window, as seen in *item* **1.** Click the **Cookies** option on the left side of the pane, as seen in *item* **2** to reveal the contents. As you can see, there is one entry that shows the top-level domain name for the page. Click the option **http://192.168.68.12** as seen in *item* **3** to reveal all the cookies loaded for the page, as seen in *item* **4**.
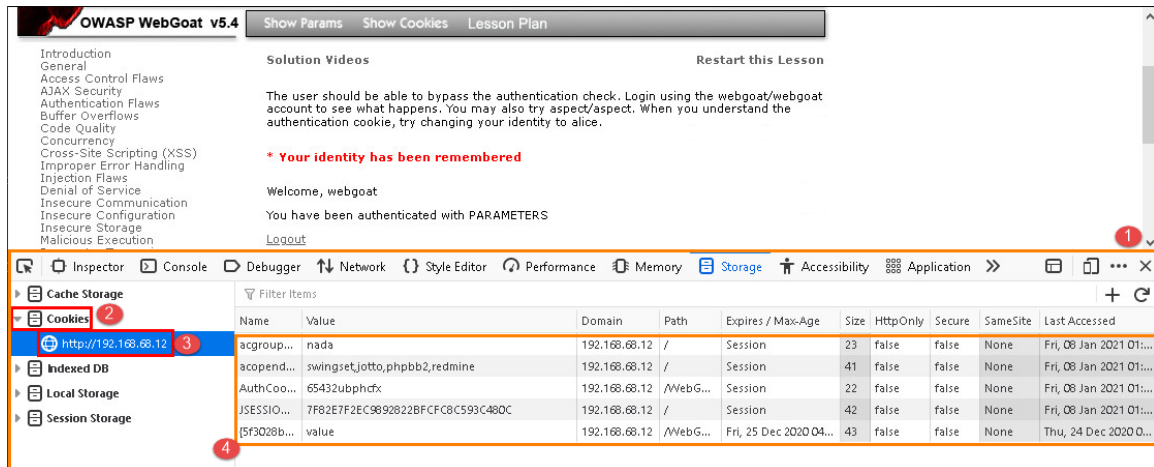
10. As you can see from the list, there are a variety of cookies. The one we are interested in is the one called *AuthCookie.* Click **AuthCookie** to view the contents of the cookie in the *Data* pane on the right, as seen in *items* **1** and **2.**
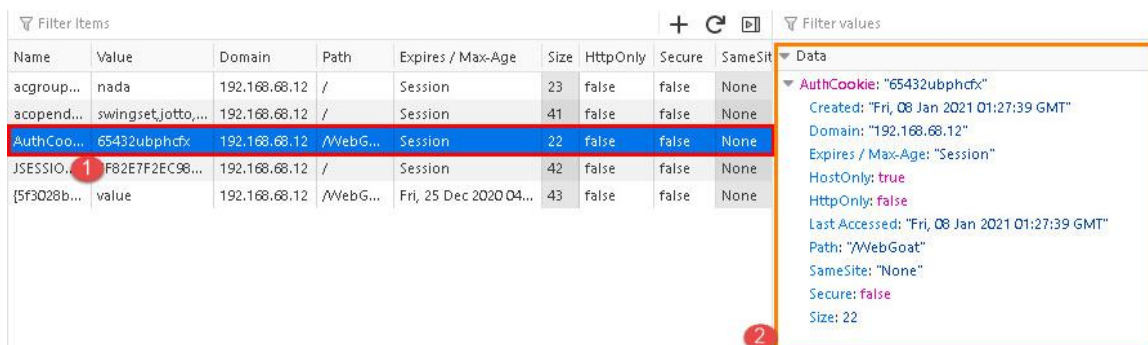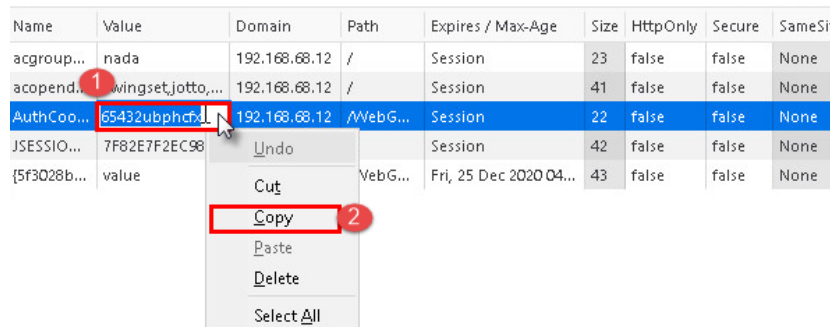
11. The details of the cookie are shown in the *Data* pane, as seen in the following screenshot. The table below the following screenshot provides details about the data within the cookie.

#	Name	Description
1	AuthCookie	contains the value that is used to generate the Session ID
2	Created	the date and time the cookie was generated
3	Domain	the domain name of the web page
4	Expires / Max Age	the length of time the cookie is valid
5	HostOnly	a flag that specifies if the cookie can be accessed by subdomains as well.
6	HttpOnly	a flag included in the cookie that helps to mitigate the risk of client-side scripting.
7	LastAccessed	the last time the cookie was accessed
8	Path	the path the cookie is stored
9	Samesite	a flag that can further restrict the cookie to a specific domain or subdomains.
10	Secure	Determines whether the cookie can be transmitted over less secure protocols like HTTP.
11	Size	The size of the cookie.

12. To continue, we need to copy the value in the *AuthCookie* field. Do this by double-clicking the *Value* field, right-click the highlighted data and select **Copy** from the context menu as seen in *items* **1** and **2** below.
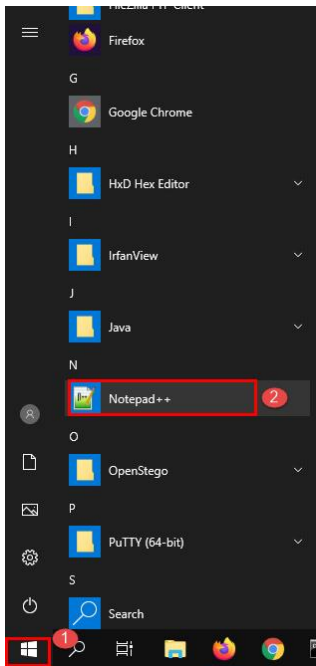
13. Let us open *Notepad++* so we can copy the text there. To do this, click the **Start** button and select **Notepad++** from the *Start Menu,* as seen in *items* **1** and **2.**


14. Once *Notepad++* opens, type the username `webgoat` as seen in *item* **1.** We will paste the copied text beside the username to help us remember what account the value is associated with. To paste the data, right-click in the space beside the word *webgoat* and click **Paste** from the context menu, as seen in *items* **2** and **3.**
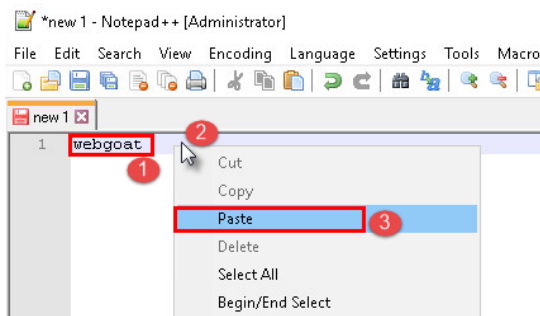

15. Let us save this data before going any further. To do this, navigate to **File > Save** as seen in *items* **1** and **2.**
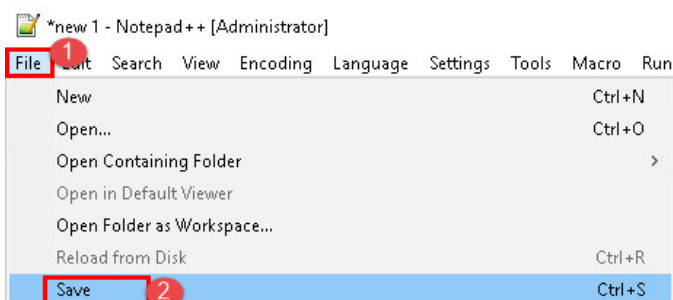
16. The *Save As* window will appear. Navigate to **Documents > Lab 24** as seen in *items* **1** and **2.** Then, type the name `cookie.txt` in the *File name* field and click **Save** as seen in *items* **3** and **4** below.
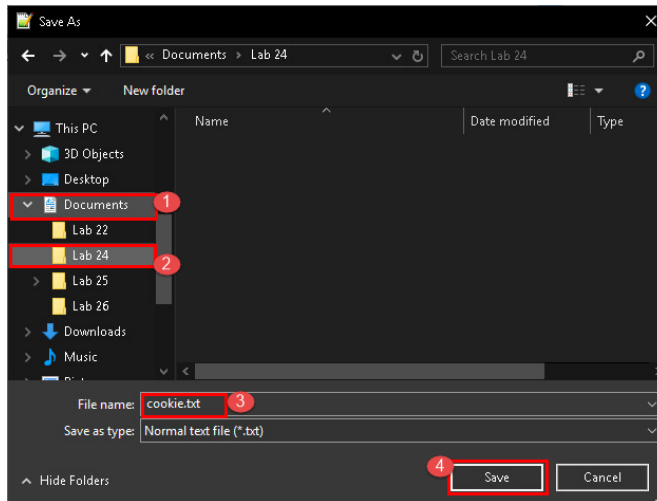
17. Now let us go back to the web browser and continue our exercise. To do this, minimize *Notepad++* by clicking the _ button at the top-right corner of the window, as seen in *item* **1** below.
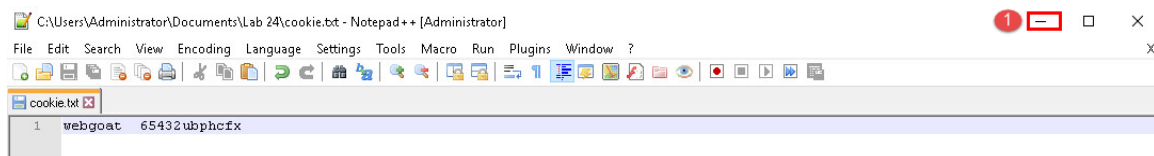

> If the *Firefox* window was minimized, maximize it by clicking the **Firefox** icon on the taskbar.

18. The *Storage Inspector* pane should still be open, click the **X** at the top-right corner of the *Storage Inspector* pane, as seen in *item* **1** below.
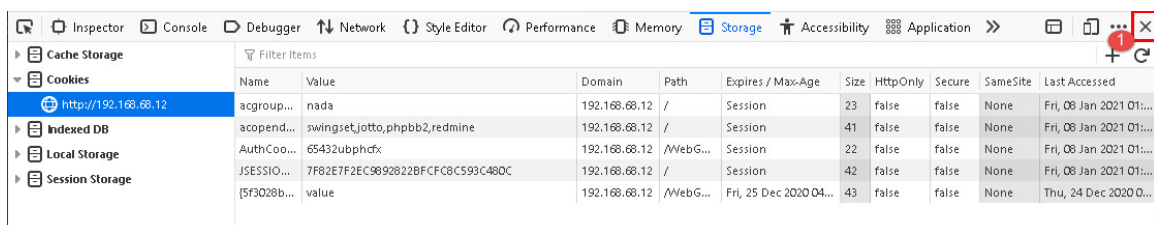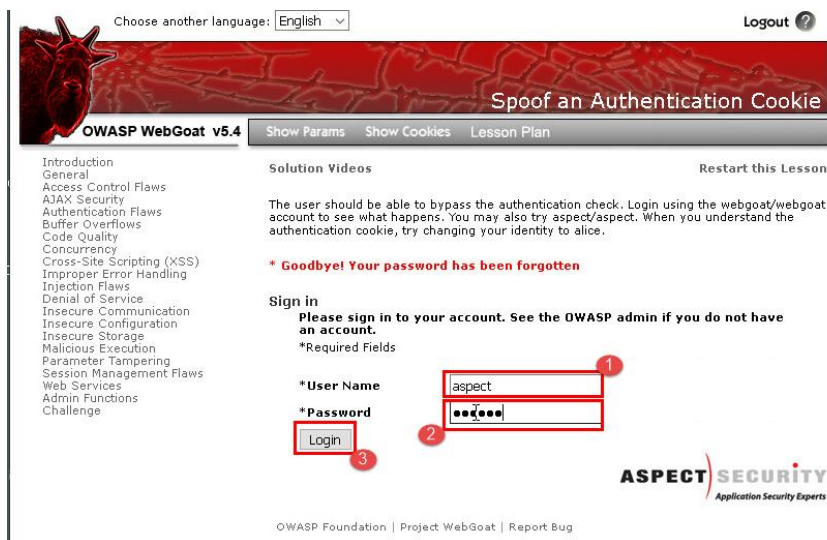
19. We are done with the account called *webgoat* for now, so let us log out and use the next account called aspect to log in. To log out, click the **Logout** option seen in *item* **1.**
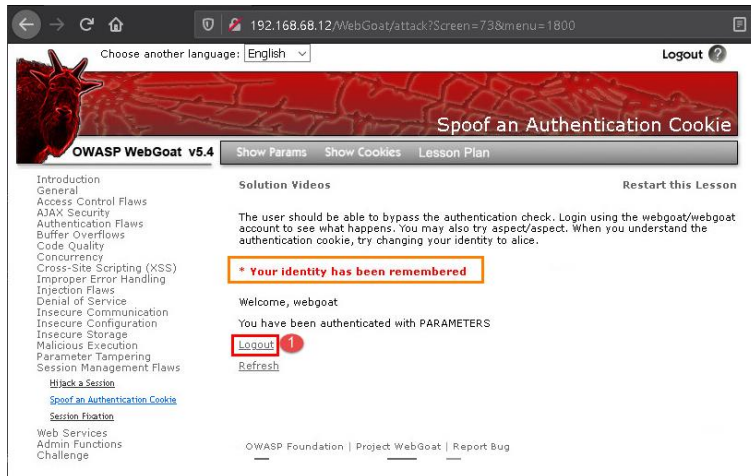

20. You will be taken back to the login screen. Type the word **aspect** in both the *User Name* and *Password* fields and then click **Login** as seen in *items* **1, 2,** and **3** below.

21. Once again you will be authenticated and taken to a private page that displays the message "* *Your identity has been remembered*." Let us look at the authentication cookie for this account as well. To begin, click on the **Open Menu** button at the top-right corner of *Firefox's* main window, as seen in *item* **1**. Next, click the **Web Developer** option from the dropdown menu that appears, as seen in *item* **2**.
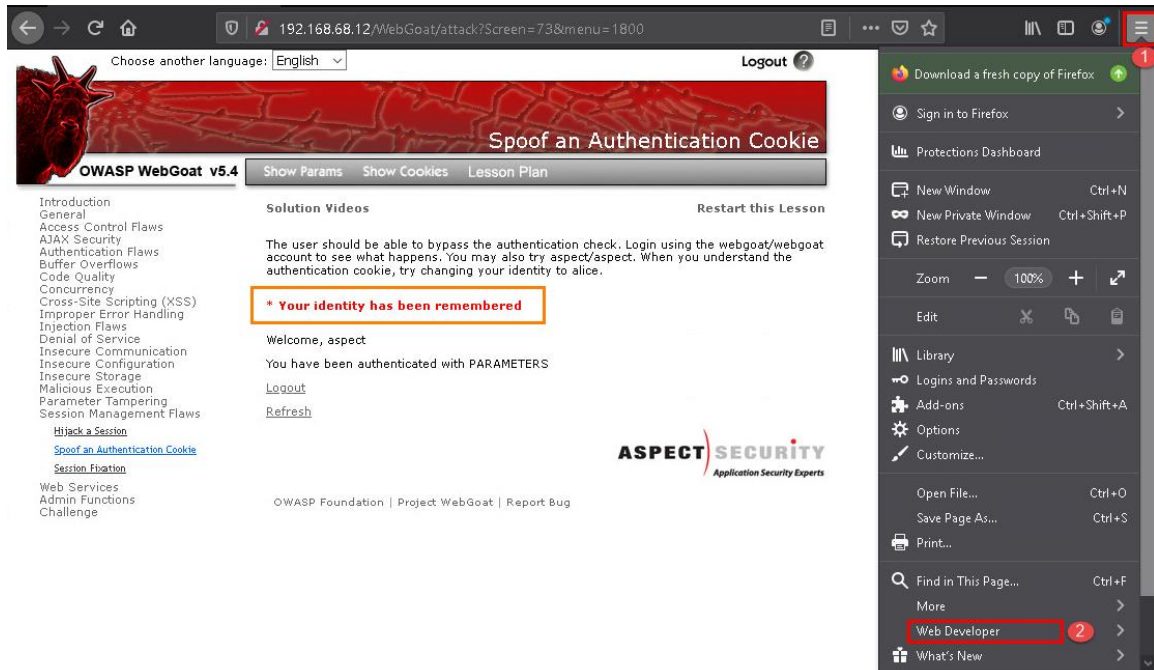

22. The *Web Developer* menu will appear. Click **Storage Inspector** to open it, as seen in *item* **1**.
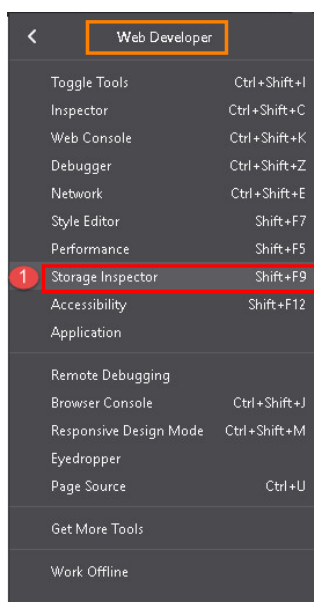
23. Let us copy the value in the *AuthCookie* field as we did before. Do this by double-clicking the *Value* field, as seen in *item* **1.** Now, copy the highlighted data by right-clicking on it and clicking **Copy** from the context menu that appears, as seen in *items* **2** and **3** below.
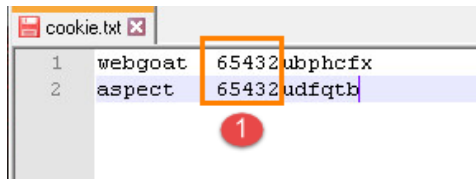

24. Now maximize *Notepad++* by clicking the Notepad++ icon from the taskbar, as seen in *item* **1** below.
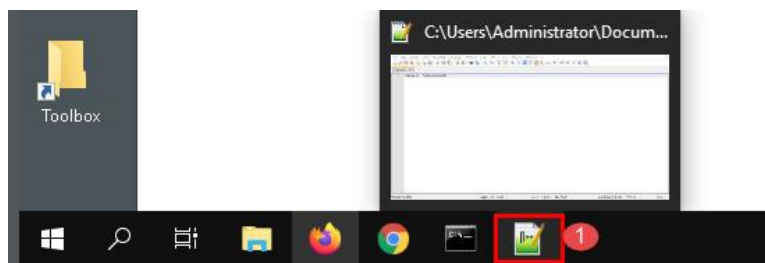
25. Once it is maximized, press the **Enter** key to start a new line and type the word `aspect` as seen in *item* **1.** Now, paste the data we copied from the cookie. To do this, right-click in the space beside the word *aspect* and click **Paste** from the context menu, as seen in *items* **2** and **3.**
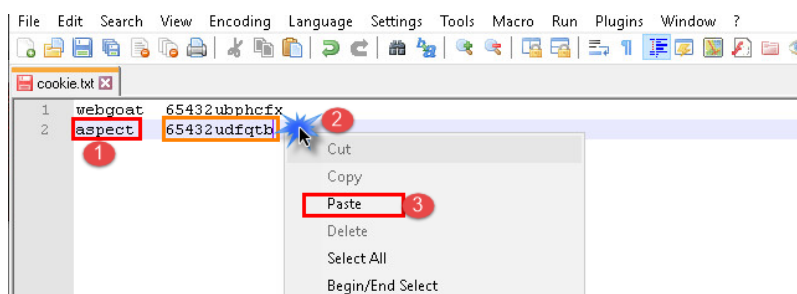
26. If you look at the values for both cookies, you can see that the first 5 characters are similar, *65432* as seen in *item* **1**. This means we just need to learn how to decode the data after *65432*. This data is encoded by reversing the username and then shifting one letter alphabetically. Let us look at the word *webgoat.* First, reverse it and it will become **taogbew.** Now, let us change each letter into the next letter alphabetically: t > **u**, a > **b**, o > **p**, g > **h**, b > **c**, e > **f**, w > **x**. As you can see, the result is **ubphcfx,** which is the same value as the *webgoat* session cookie value. Since we are trying to get into the account called *alice*, we need to reverse and shift the characters for the word *alice*. Do this calculation using the same method as we did before.

```
cookie.txt
   1   webgoat   65432 ubphcfx
   2   aspect    65432 udfqtb
                  1
```
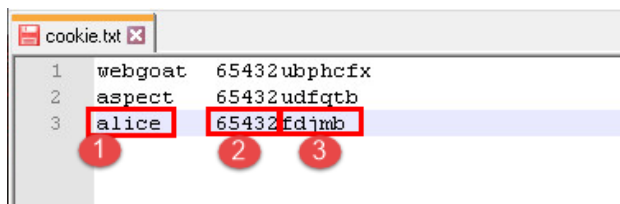
"ecila" e > **f**, c > **d**, i > **j**, l > **m**, a > **b**

27. Since you have the value, press the **Enter** key to go to a new line in *Notepad++* and then type the username `alice` as seen in *items* **1** and **2**. Now, type `65432` and the value you calculated from the username, which is `fdjmb` as seen in *item* **3**.

```
cookie.txt
   1   webgoat   65432ubphcfx
   2   aspect    65432udfqtb
   3   alice     65432fdjmb
        1          2     3
```
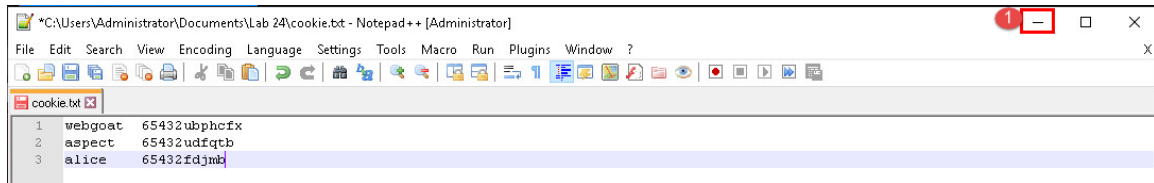
28. Now that we have the session cookie value for the account called *alice,* we can use it to trick the website into giving us access to *alice's* account without the password. First, we must log in using a legitimate account. Let us use the *aspect* account since we are already logged in. For now, minimize *Notepad++* by clicking the _ button at the top-right corner of the window.

29. Firefox should now be in focus. However, if the *Firefox* window was minimized, maximize it by clicking the **Firefox** icon on the taskbar.
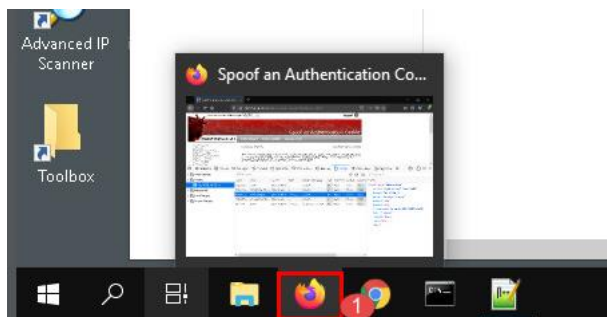
You should still be logged in as *aspect* and the *Storage Inspector* pane should still be open.

30. Let us change the *AuthCookie* value and replace it with *alice's* value. Begin by double-clicking the *AuthCookie* value as seen in *item* **1** below. Once it is highlighted, click the end of the value, and delete the letters and then replace them with `fdjmb` as seen in *items* **2** and **3** below. Once you are done, click in an empty area outside the field or press the **Enter** key to confirm the change.

31. Now that the cookie has been changed, click the **Refresh** option in the webpage area, as seen in *item* **1.**
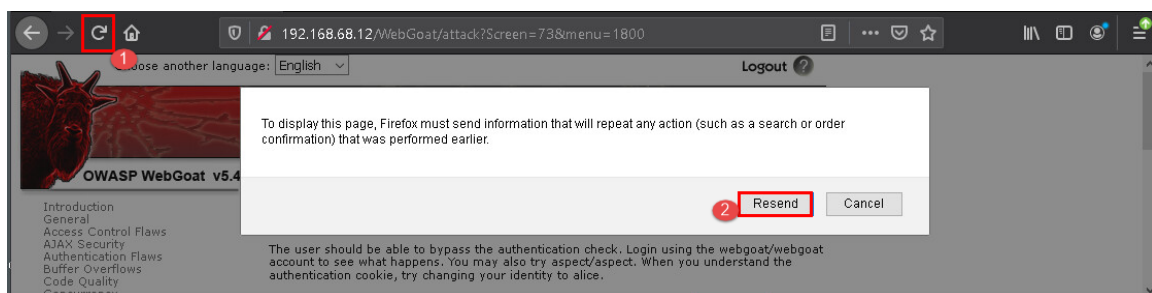
This will reload the web page and send the new cookie we modified. When prompted by the browser, select **Resend** to confirm the action.

32. If everything was done correctly, you will be successfully logged into *alice's* account. Close the *Storage Inspector* pane by clicking the **X** at the top-right corner of the *Storage Inspector* pane to close it and get a better view of the page's contents. As you can see on the web page, there is a congratulatory message that states "** Congratulations. You have successfully completed this lesson.*" You have successfully modified/spoofed a session cookie and got unauthorized access to the user account called *alice*.

33. Close all open windows and applications to complete the lab.