**LAB 01 – WEEK 01**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Course:** | KF-5007 Security Case Project | | **Activity No.** | LA/5007/W126012023 | | **Week:** | 01 | | **Duration:** | 03 hours (approx.) | | **Submission:** | Blackboard | | **Assessment Marks:** | Contributed towards workshop participation marks | |
| **After completing this lab, you will be able to:**   * Configure a vulnerable web application using Security Kit. * Execute Brute Force attacks on different security levels. * Build your research and critical analysis activities. |
|  |
| **Essential Reading, Lectures and Tasks:**   1. Listen to Week 5 lecture explaining web architecture and attacks 2. Read research articles available under Week 5 to complete tasks. 3. Watch this video if you wish to configure and install DVWA on your machines using Kali Linux ([watch](https://youtu.be/j16iQwva5xo)).   **Important:**   1. It is your responsibility to contact the loans department to loan the security kit and return the kit back to the loans department right after the lab. One security kit can be connected to four terminals; therefore, only one person should loan the device per group of four students from the loans department. 2. You are **strictly** required to execute these labs within the configured security kits and follow the instructions mentioned in the usage guidance available on the Blackboard. 3. The lab/workshop activity will be made available at the start of the workshop session every week. The lab/workshop activity must be completed during the specified lab/workshop timing. 4. Please report any typos/errors in the lab at [Zeeshan.siddiqui@northumbria.ac.uk](mailto:Zeeshan.siddiqui@northumbria.ac.uk) |
|  |

**Task 01: Brute Force Attack (Low Security)**

In this tutorial, we will perform the Brute Force attack using different security levels, i.e., Low, Medium or High.

* 1. Follow the ‘How to Setup the Security Lab Kit’ tutorial to set up and log in to DVWA.
  2. Choose **DVWA Security** from the left menu and choose **Security Level** to **Low.**
  3. Click on ‘Brute Force’ from the left menu. You will see the login screen again. Let’s assume that we are unaware of the user’s ‘admin’ credentials. We will be using Burp Suit to perform the Brute Force attack.
  4. Access and open *Burp Suit* already available under Applications (Kali Linux).
  5. Click *Proxy > Options* and add *127.0.0.1:8080* to your proxy.
  6. Load Firefox and change your proxy settings to the above address
  7. Head to the target page, [*http://localhost/DVWA/vulnerabilities/brute/*](http://localhost/DVWA/vulnerabilities/brute/)
  8. In Burp suit click *intercept > intercept is on.* With intercept ON, you can monitor, modify or intercept any packet/request.
  9. Without entering any credentials in your browser, hit Login button and take a look at the request in Burp Suit.
  10. You will observe some key information such as GET request, login parameters, cookie information etc.
  11. Click on the first **GET** request and you will see two split windows underneath with the titles **Request** and **Response**. Observe the GET request having variables ‘username’ and ‘password’. Insert the output screenshot in the checkpoint and add any comments (if any).

|  |
| --- |
| **Checkpoint** |
|  |
| **Comments/Discussion:** |

* 1. You should be able to identify the actual password written in plaintext in front of these variables.
  2. In case these variables are randomized/sanitised, there is another (longer) way of extracting the password using any password list.
  3. Click on Actions and choose ‘Send to Intruder’. Go to the Intruder tab and check out the Positions tab. Under the ‘Attack Types’ you will see different types of attacks, such as Sniper, Cluster bomb etc. Select ‘Sniper’ from the list.
  4. The Sniper go through the variables which were sent to the intruder and then loops through a different list. Click on the ‘Payloads’ tab where you can set Payloads, such as 1 which would work for the admin user. In this field, we are only looking to do is Brute force the passwords.
  5. Click the ‘Clear’ button on the right and select the Password variable.
  6. Go back to the ‘Payloads’ tab and choose 1 in ‘Payload Set’. Click ‘Payload type’, where you can choose various types of payloads. For example, ‘Numbers’. We use this type so we can detect values such as user IDs or sets of Numbers.
  7. Choose ‘Simple List’ from the ‘Payload type’ as we are looking for Passwords using a pre-loaded Passwords List. Click on ‘Load’ and it will show the default passwords folder containing various files with the password lists (txt files). You can also create your password list and use that as a Payload.
  8. You can choose ‘darkweb2017.top100.txt’.
  9. Click on the ‘Start attack’ button on the left once the list is loaded.
  10. You will see a process window displaying different passwords with their occurrence values, status or length which can be used to identify which password is correct. Click on the ‘Options’ tab and you can set various strings under the ‘Grep-Match’ to look for passwords using pre-identified strings, messages or errors. Provide a screenshot with any additional comments.

|  |
| --- |
| **Checkpoint** |
|  |
| **Comments/Discussion:** |

* 1. Click on ‘Intercept’ and turn it off. On the Brute force login window, enter any wrong password for the admin user and click Login.
  2. You will see an error message saying, ‘Username and/or Password is incorrect’. Copy this string (make sure there are no spaces copied at the beginning and at the end of the string), go back to ‘Intruder’ and then ‘Options’ > Grep-Match paste the string and click the ‘Add’ button to add.
  3. Choose ‘Exclude Http headers’ because we are only looking into the contents. Sometimes when we receive such error messages, they are sanitized using a Token number. You can use the ‘Grep-Extract’ function to set additional matches and complex macros.
  4. Go back to ‘Target’ and click ‘Start attack’ again.
  5. You should see the same window appearing in Step 21 with an added column of the string you have added with a number of blue ticks and some empty boxes (without blue ticks). These blue ticks will identify incorrect passwords based on the string which was detected during the attack.
  6. The correct password shouldn’t have a blue tick and you will be able to identify it easily. Provide the output and any comments.

|  |
| --- |
| **Checkpoint** |
|  |
| **Comments/Discussion:** |

* 1. If you wish to check if the string is working correctly and identifying the correct password, then try adding the string that appears when you enter the correct username/password. The result will be exactly the opposite of Step 27.
  2. Let’s try another way of Brute force. Try entering the correct credentials and press the login on the Brute force vulnerability login page.
  3. You will see a Welcome message and a picture. Right-click the image and choose view image. The image is going to open in the browser and the complete directory path should be visible in the URL, for example, 127.0.0.1/dvwa/hackable/users/admin.jpg.
  4. Take out the image name in the URL and press Enter. You should be able to see a web directory containing a list of JPG files (and some folders) with a link anchor to go back to the parent directory.
  5. If you observe the filenames, you will be able to understand that these file names are the actual user images associated with legit users, such as ‘admin.jpg’. Therefore, you should be able to see user images like *1337.jpg, gordonb.jpg, pablo.jpg* etc. Provide screenshot and any comments (if any).

|  |
| --- |
| **Checkpoint** |
|  |
| **Comments/Discussion:** |

* 1. Let’s populate a list from this directory and store it in a text file. Open Terminal and type ‘subl users.txt’ to create and open a text file with the name ‘users’.
  2. Enter all the names (only without their extensions) in a separate line and save the file.
  3. We will be using Hydra for this. Open the terminal and type in ‘man hydra’ to make sure that Hydra is installed and working. You can explore different commands, syntax and its usage to try different things. Hydra supports all sorts of scanning using HTTP/HTTPS requests, GET/Post requests and you can also enter usernames or a list of usernames using the -l or -L command. We can also generate passwords if we do not have a password list to work from. You can try ‘hydra -h’ to see other available options as well with supported examples.
  4. Let’s try the following command.

‘hydra -L users.txt -P ~/seclists/Passwords/portable-v2-top1575.txt 127.0.0.1 http-get “/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:incorrect” -V’.

* 1. The -L is used for the user list, -P is for the password list which we have provided ‘~/seclists ..’. The colon separates different parameters. As we need to use the parameters in the URL, therefore, we copied the parameters from the URL and replace the username ‘admin’ and password ‘password’ with our custom parameters USER and PASS. This helps if the values are encrypted or sanitized. The word ‘incorrect’ is from the string we get whenever user enters an incorrect password. Therefore, the hydra is going to identify that particular string and -V is for Verbos.
  2. Once executed, there should be a list of passwords appearing on the terminal showing a number of tries with each password. The actual password should appear in green. If this is not the case then we have to try something else. Provide the screenshot and any comments.

|  |
| --- |
| **Checkpoint** |
|  |
| **Comments/Discussion:** |

* 1. Edit the command mentioned in Step 36,

‘hydra -L users.txt -P ~/seclists/Passwords/portable-v2-top1575.txt 127.0.0.1 http-post-form “/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:incorrect” -V -I’

The -i at the end is to avoid any restore file it has created because of any terminated session. This should give a number of passwords in green. Note that, we have used POST instead of GET.

* 1. Let’s try another command line utility called WFUZZ that comes with Kali Linux. Type ‘man wfuzz’ and it will give you several options to explore similar to hydra, such as -H, -L etc. In your terminal type ‘wfuzz -h’ to explore different parameters. We will be using the PHPSESSID to explore passwords. The token can be extracted using Burp suit as discussed in Step 11.
  2. In the terminal window type

“wfuzz -c -w ~/seclists/Passwords/portable-v2-top1575.txt -b ‘security=low; PHPSESSID= ENTER-YOUR-SESSION-ID’. <http://127.0.0.1/dvwa/vulnerabilities/brute/index.php?username=admin&password=FUZZ&Login=Login>’ ”.

You will see an output with the response code 200 in red which is the correct response code. Observe the changes in the *Ch* (character) values. The correct *Ch* value should stand out from the others. Such as 4280 Ch, whereas others should have a different value e.g., 4237 Ch. Provide the screenshot and comments (if any)

|  |
| --- |
| **Checkpoint** |
|  |
| **Comments/Discussion:** |

* 1. To make it clearer, we can filter out using either character count or words. Let’s filter using the word count of 248 for the identified password ‘password’. Let’s alter the previous command,

“wfuzz - - sw 248 -c -w ~/seclists/Passwords/portable-v2-top1575.txt -b ‘security=low; PHPSESSID= ENTER-YOUR-SESSION-ID’. <http://127.0.0.1/dvwa/vulnerabilities/brute/index.php?username=admin&password=FUZZ&Login=Login>’ ”.

This should bring only one correct record of the actual identified password.

* 1. You can also filter with the incorrect password string if you are not sure about the word/character counts. Enter

“wfuzz - -hz “incorrect” -c -w ~/seclists/Passwords/portable-v2-top1575.txt -b ‘security=low; PHPSESSID= ENTER-YOUR-SESSION-ID’. <http://127.0.0.1/dvwa/vulnerabilities/brute/index.php?username=admin&password=FUZZ&Login=Login>’ ”.

* 1. Let’s try it with the users.txt file we created earlier with the assumption that we are unaware of the username and passwords. Enter the following at the terminal window.

“wfuzz -c -z file.users.txt -z file./home/zeeshan/seclists/Passwords/portable-v2-top1575.txt -b ‘security=low; PHPSESSID= ENTER-YOUR-SESSION-ID’. <http://127.0.0.1/dvwa/vulnerabilities/brute/index.php?username=FUZZ&password=FUZ2Z&Login=Login>’ ”.

|  |
| --- |
| **Checkpoint** |
|  |
| **Comments/Discussion:** |

The -z is used to specify a file and unlike hydra, WFUZZ requires a full path. We will be using FUZZ and FUZ2Z variables for first and second attempts as mentioned in the syntax, please see Step 40. This should bring in only the correct usernames and passwords list. **Please note** the filename should be the correct file path on the kit with a different home location other than /home/Zeeshan ….

**Task 02: Brute Force Attack (Medium Security)**

* 1. Let’s change the difficulty level to Medium. Go back to the DVWA Security and change it to Medium. Go back to the Brute force login screen and hit F12. Make sure that the cookie setting under Storage is also changed to medium security.
  2. Use the same command again with some slight changes.

“wfuzz -c -z file.users.txt -z file./home/zeeshan/seclists/Passwords/portable-v2-top1575.txt -b ‘security=medium; PHPSESSID= ENTER-YOUR-SESSION-ID’. <http://127.0.0.1/dvwa/vulnerabilities/brute/index.php?username=FUZZ&password=FUZ2Z&Login=Login>’ ”.

You will receive the same screen, the only difference is in the speed of the result. The brute force is taking longer than the last attempt in low security.

* 1. Go back to the Brute force login screen and try to log in. You will see that the login screen is going to take much longer than expected. In normal circumstances, when you try to brute force any website, it disallows any attempts after a couple of unsuccessful attempts. As a result, your account can be blocked and it can be reported for further investigation.

**Task 03: Brute Force Attack (High Security)**

* 1. Let’s try this with a High-security level by selecting High from the DVWA Security tab and submitting. Follow Step 45 and check if the cookie session has also been changed to high.
  2. Make sure that Burp suit is still running and intercepting. Try login in from the Brute force screen with a successful password and another attempt with an unsuccessful one. Observe the GET parameters and the change in those parameters as compared to the Request when the security settings were set to Low.
  3. On the Response window (right side), scroll down until you see and observe the incorrect password message.
  4. Under Actions, choose ‘Send to Repeater’. Under Request change the password to an incorrect password ‘test2’. Click Send and click ‘Follow redirection’.
  5. Go to the Response window again and scroll until you see ‘CSRF token is incorrect’. This explains the behavior and use of the token in case of an incorrect attempt. The CSRF stands for Cross Site Request Forgery and the CSRF token prevents the application from such attacks. At every request the token is updated and to perform a Brute force, a correct token is essential.
  6. Hit F12, and in Search HTML, search for ‘user\_token’ and it will bring up an HTML input tag having a type = “hidden”. Clear the type and the token will appear on the webpage next to the Login button.
  7. Refresh the page and copy the newly generated token. Go to the terminal and bring up the command we used in **Step 46**. Edit the command as follows.

“wfuzz -c -z file.users.txt -z file./home/zeeshan/seclists/Passwords/portable-v2-top1575.txt -b ‘security=high; PHPSESSID= ENTER-YOUR-SESSION-ID’. <http://127.0.0.1/dvwa/vulnerabilities/brute/index.php?username=FUZZ&password=FUZ2Z&Login=Login>’ ”.

Press enter and it will bring the 302 codes which were expected. Provide screenshots with comments (if any).

|  |
| --- |
| **Checkpoint** |
|  |
| **Comments/Discussion:** |

* 1. Alter the command as follow and enter the user\_token information.

“wfuzz -c -z file.users.txt -z file./home/zeeshan/seclists/Passwords/portable-v2-top1575.txt -b ‘security=medium; PHPSESSID= ENTER-YOUR-SESSION-ID’. <http://127.0.0.1/dvwa/vulnerabilities/brute/index.php?username=FUZZ&password=FUZ2Z&Login=Login>&user\_token=ENTER-USER-TOKEN’ ”.

This should bring the 200 response code which shows the correct credential in addition to 302 codes.

|  |
| --- |
| **Checkpoint** |
|  |
| **Comments/Discussion:** |

**Task 04: Critical Reading and Analysis**

* + - 1. This task is to help you build critical reading and critical analysis and help you to work on various research-based approaches by giving you a topic to research and discuss within your group. This task is going to help you build your research capabilities to use in your final year project while conducting background study and literature review.

You should discuss and research to answer the following question in your project group and/or individual.

**“How Bruteforce is being used to exploit machine learning approaches?”**

* + - 1. Visit Google Scholar and try to search and read relevant research articles.
      2. You can use your university credentials to login and download any research article which is not available freely/opensource.