**Burp Suite Tutorial**

By: Waleed Muhammad and Shabaz Badshah

Tuesday March 17, 2020

CSC427 - Information Security

**Pre-tutorial:**

* vulnerabilities.txt file

**Setup:**

1. Copy VM from [here](https://drive.google.com/open?id=19aqTN8NsbY7xypCBjhNzyUgmh-ude-Z4) onto your laptop
2. Turn the vm on and go to terminal (username/password is kali/kali)
3. Put in the following commands:
   1. sudo service apache2 start (sudo password is kali)
   2. sudo service mysql start
   3. sudo ifconfig (make sure you note down your eth0 inet ip. Looks like 192.168.X.XX)
   4. Go to 192.168.X.XX/DVWA (username/password is admin/password)
      1. If it says the proxy server is refusing connections then your web browser is already on the burp proxy settings and is waiting for the burp proxy to start (DO not need to do Tutorial part 4 if this is the case)
   5. Go to start menu and search for burpsuite professional and open it
   6. Go with the default settings for burp and create a temporary project

**Tutorial:**

In this tutorial, we will be brute forcing login/password pairs by intercepting a request to the server and editing it with new login/password pairs each time to find new pairs that work.

Link for brute-forcing is: [http://192.168.X.XX/DVWA/vulnerabilities/brute/](http://192.168.x.xx/DVWA/vulnerabilities/brute/)

1. Startup a temporary project and use burp defaults on burp suite pro
2. Go to Proxy → Options → proxy listeners, make sure you have a proxy at 127.0.0.1 on port 8080 and it is running
3. Go to Target → Scope → Target scope, add 192.168.X.XX to it
4. To get your browser to use the proxy that burp suite set up:
   1. Go to firefox, preferences, and network settings
   2. Click the manual proxy configuration
      1. Set HTTP proxy to 127.0.0.1 and port 8080
      2. Tick off “Use this proxy server for all protocols”
      3. Hit ok and now refresh the dvwa page for burp to intercept the call
5. Log in to DVWA with username: admin and password: password
6. Make sure the DVWA security level is set to low by going DVWA security → Security level and then set it to low
7. Identify the issue number of the vulnerability from this DVWA [report](https://drive.google.com/file/d/1ktsyYv9GJT9IJVauCCsGpFLR7HzucZHm/view?usp=sharing) that can allow for the brute forcing exploit
8. From the OWASP top 10 lecture slide, what is the number of the vulnerability that we are exploiting (hint it may be in the top 5)
9. Suggest how you can mitigate this brute forcing issue
10. Go to the brute force page on DVWA
11. Click the login button to intercept the call made to login
12. Now use the intruder tool to try and brute-forcing it
    1. HINT #1: this link might be useful: <https://portswigger.net/burp/documentation/desktop/tools/intruder/positions>
    2. HINT #2: a list of potential usernames is provided below (only 5 of them are real users):
       1. admin
       2. test
       3. hackerman
       4. picasso
       5. pablo
       6. escobar
       7. root
       8. 1337
       9. gordonr
       10. gordonb
       11. johndoe
       12. johnsmith
       13. johny
       14. smithy
       15. johndoe
    3. HINT #3: one password is harder than the rest so you might need a better word list that Rocks…
13. Search through the responses and confirm the correct password
14. After finding the username/password pair, go to the DVWA and plug in each pair to receive the 5 secret images

**Submission:**

Files to submit for this tutorial are:

1. usercreds.txt which contains the 5 correct usernames with their corresponding passwords in the format username/password
2. The secret images for each user from DVWA (naming convention will be username.jpg)
3. vulnerabilities.txt from the lecture
4. answers.txt that have answers to the questions 7, 8, 9 (these are the answers to step 7, 8, and 9 from the tutorial)
5. members.txt with yours and your partners names and UTORids

Zip the above files up and submit it on UtorSubmit

**DO NOT SUBMIT ANY OTHER FILES (eg. no vms, no wordlists, etc.)**