CSEC-140 Introduction to Cybersecurity: Class Activity 11

Cooper Broll, Kylee Kublin, Kisakye Kirabo

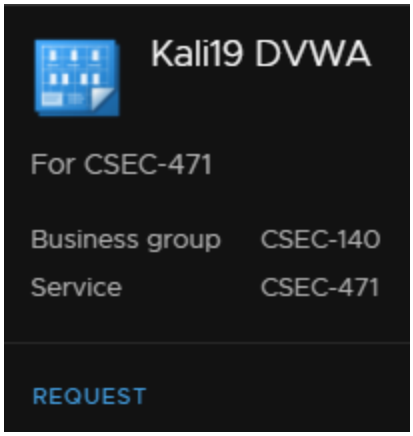
Instructions

1. Follow the instructions in myCourses to duplicate this file in your shared group folder.
2. Complete each section as instructed.

Your participation grade will be determined based on your contributions as indicated by “Track Changes” and by your comments in the document.

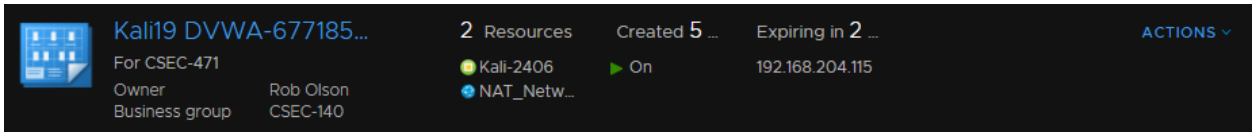
Deploy the VM

1. Navigate to https://rlescloud.rit.edu.
2. Log in with your RIT username and password.
3. Choose Kali19 DVWA, and request a deployment.

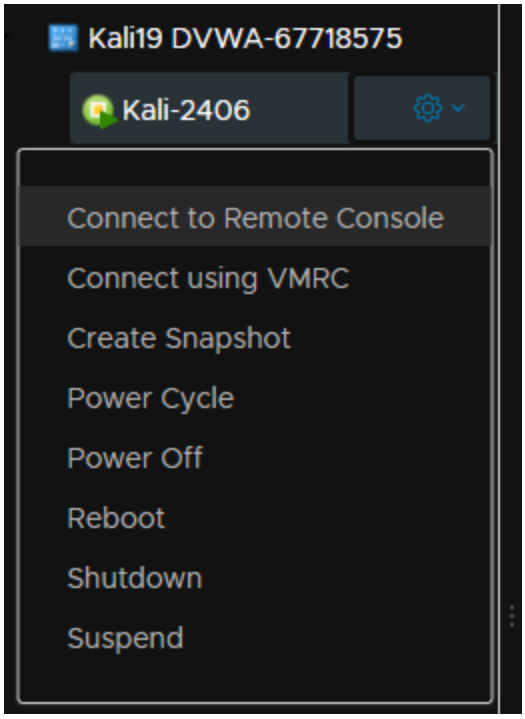


4. A window will open asking you to verify and add additional details. Leave all details unchanged, and press the SUBMIT button.

5. The deployment will start. You will receive an email regarding this step. This may take a while depending on the amount of deployments being processed in RLES at the moment (**on average 5 to 10 minutes**).
6. Wait until your request is complete. You will receive an email when your deployment is complete. You will see your deployment created and powered on under the Deployments tab.



7. Click the VM in the Deployments tab.
8. When the deployment window opens, click the actual VM under the deployment. The settings button (gear icon) will appear next to the VM. Click the settings button, and choose “Connect to Remote Console”.

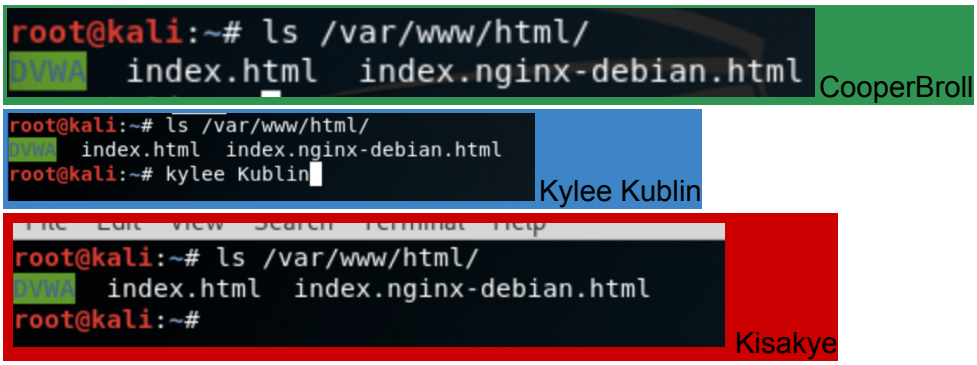


9. A new browser tab or window will open. If a new tab or window does not open, ensure your pop-up blocker is disabled.
10. Log in to the VM.
    - Username **root**
    - Password **toor**
11. Open the Terminal  in the VM.

Web Application Basics

Fundamentally, a web server is a file server. When a user accesses a web site, they are just asking for a web server to send over one or more files. For example, if the user visits http://www.example.com/index.html, they are asking the web server named www.example.com to send them the file index.html. These are just files in the server’s file system.

1. Run the command `ls /var/www/html/` to view the files in the web root. **Each student should insert a screenshot showing their web root directory. Include your name with your screenshot.**



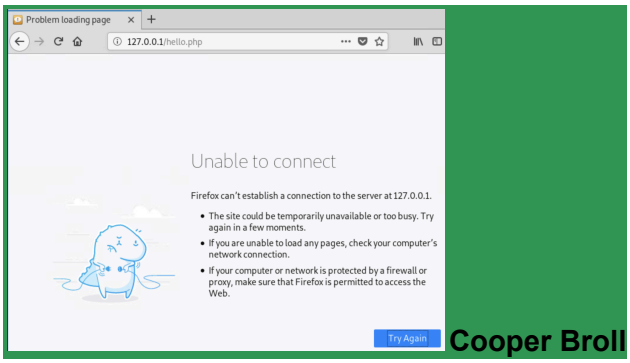
A web application is just code. Sometimes that code executes in the user's browser. A browser knows how to process HTML, CSS, and JavaScript by default, although there is some debate about whether HTML and CSS are technically programming languages. If the files the user requests contain code from these languages, the browser executes that code blindly, without any form of authentication or integrity checking.

Some files contain code that the server will execute before sending the file to the user. This is often written in languages like PHP, NodeJS, or Ruby. The server will execute little segments of these server-side programming languages embedded within the requested file and just send the output of the code to the client instead.

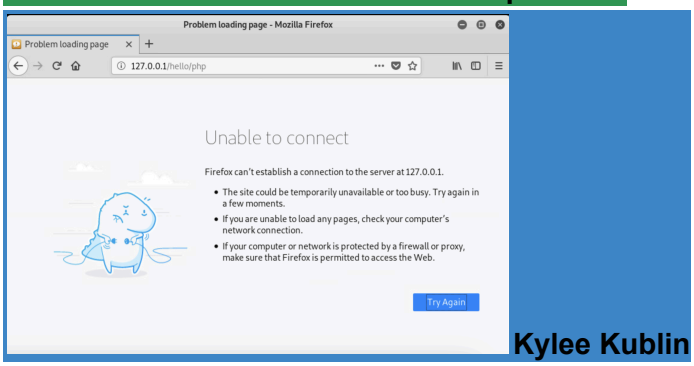
2. Use the following command to open a text editor.
   `leafpad /var/www/html/hello.php`

3. In this file, write the following code, and save your file. You will know your file is saved when the asterisk in the filename disappears.

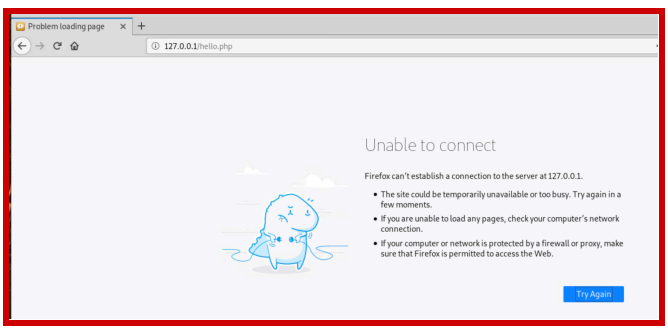
4. Open a web browser, and attempt to access the file that you wrote by visiting `http://127.0.0.1/hello.php`. This should be unsuccessful. **Each student should include a screenshot of their web browser. Include your name with your screenshot.**



Cooper Broll



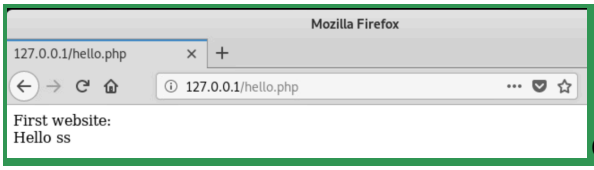
Kylee Kublin



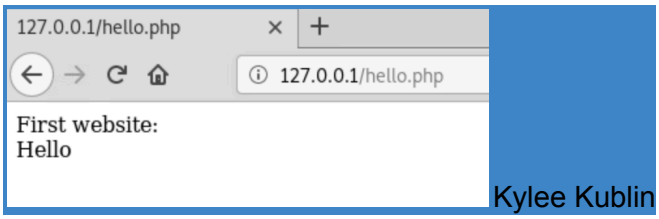
Kisakye Kirabo

5. The reason you could not access the file you created is that the web server is not running. Because the web server is not running, your browser cannot access files on it. **Close your text file**. At the command line, run the following command.
   `service apache2 start`

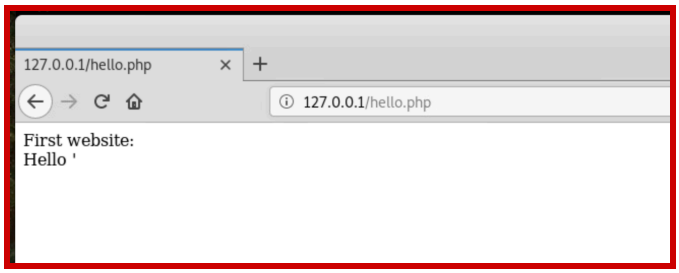
6. Open a web browser, and attempt to access the file that you wrote by visiting `http://127.0.0.1/hello.php`. This should be successful. **Each student should include a screenshot of the page the web server sends them. Include your name with your screenshot.**



Cooper Broll

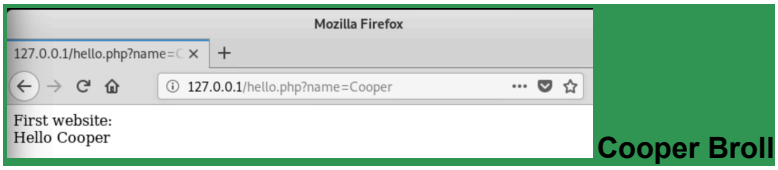


Kylee Kublin

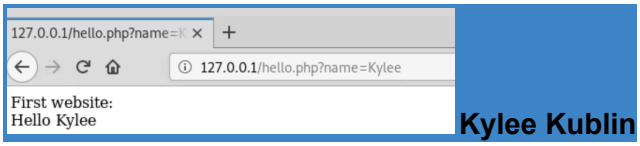


Kisakye Kirabo

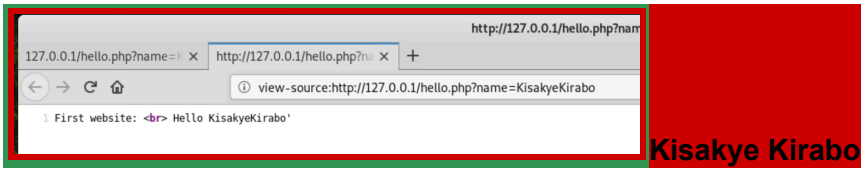
7. Change the URL in your web browser so that it has some data after ".php". It should look like the following: `http://127.0.0.1/hello.php`**`?name=YourNameHere`**. Press the Enter key. After the page loads, right click anywhere on the web page, and click View Page Source. **Each student should include a screenshot of the new window their browser opens. Include your name with your screenshot.**



Cooper Broll



Kylee Kublin



Kisakye Kirabo

8. Review your screenshot in step 7. **Each student should briefly describe, in their own words, what happened when they visited the URL in step 7. Be sure to identify what you think the expected input to this script is.**

9. Change the URL in your web browser to the following, and press the Enter key.
`http://127.0.0.1/hello.php`**`?name=<script>document.location.href="http://www.youtube.com";</script>`**

10. **Each student should briefly describe, in their own words, what happened when they visited the URL in step 9.**

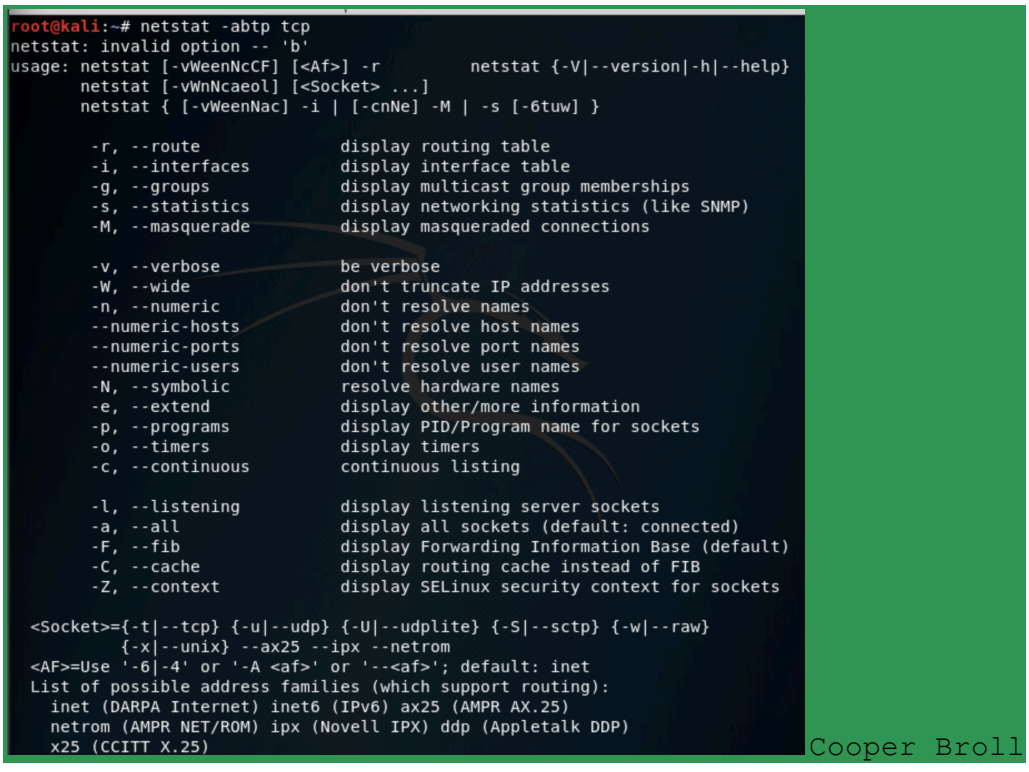
11. **Each student should answer the following question. Should what occurred in step 9 be possible in a well-coded web application?**

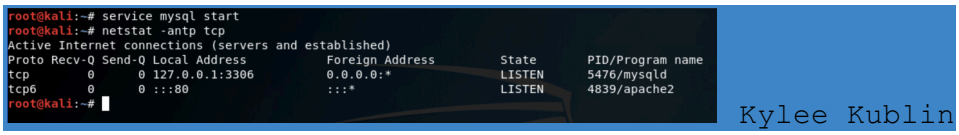
Run DVWA

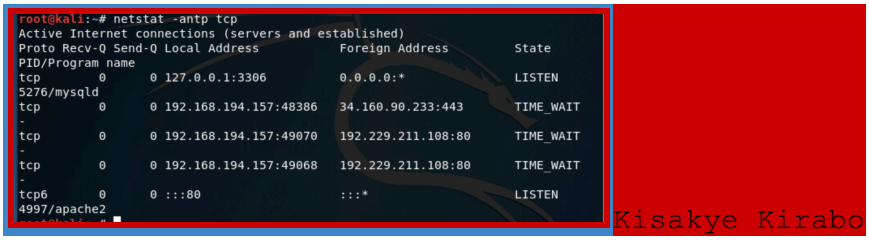
The Damn Vulnerable Web Application (DVWA) is a web site that has been made intentionally vulnerable to web application attacks for educational purposes. It has far more vulnerabilities in it than we will be examining in this activity, so you may wish to retain this virtual machine and explore further.

1. Before we start examining the security posture of this application, we must go through some configuration steps. First, like most web sites, DVWA relies on a database back end to hold data. Your Kali VM already has database software called MySQL installed. Run the following command.
   `service mysql start`

2. It may look like nothing has happened, but the database software should be running in the background. We can verify that this software is running by checking to see if the MySQL network port TCP/3306 is open. Run the following command to view the open network ports on your Kali VM. **Each student should include a screenshot showing that port TCP/3306 is open. Include your name with your screenshot.**
   `netstat -antp tcp`







3. Visit `http://127.0.0.1/DVWA/setup.php` in your web browser. You should be presented with an interface for configuring the DVWA database. Scroll to the bottom, and click 'Create / Reset Database'.

4. In this exercise, you will compromise each other's DVWA instances. This is only legal because these systems are owned by RIT and specifically intended for this activity. Attempting to hack real websites (outside of the strict rules set by bug bounty programs) is illegal. **Each student should explicitly acknowledge that hacks of the kind that are possible in DVWA are easy to detect and that attempting them against real websites can get you into serious trouble. Failure to acknowledge this will result in a 0 on this activity regardless of any work done.**

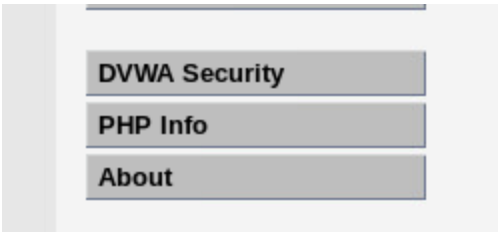
5. Use the command `leafpad /root/secret.txt` to create a file called 'secret.txt'. Put some message in it that only you know. This will be a 'flag' for other students to try and find while hacking your VM.

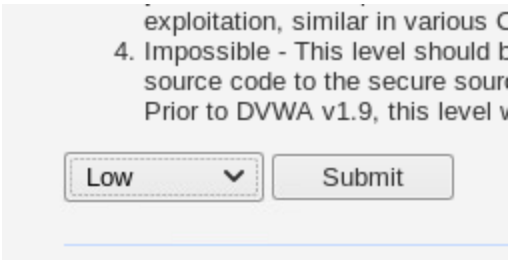
6. Use the command `ifconfig` to identify your VM's IP address, and fill in the following table. Be aware that RLES automatically suspends VMs. Students in asynchronous sections of CSEC 140 or students completing this outside of normal class time may want to coordinate a time to complete the lab with other students in the group. **You Imay target your own system with your instructor's permission.**

Student	Student's IP Address	Target	Target's IP Address
Cooper Broll	193.168.195.250	193.168.195.250	193.168.195.250
Kylee Kublin	192.168.195.228	192.168.195.228	192.168.195.228
Kisakye Kirabo	192.168.194.157	192.168.194.157	192.168.194.157

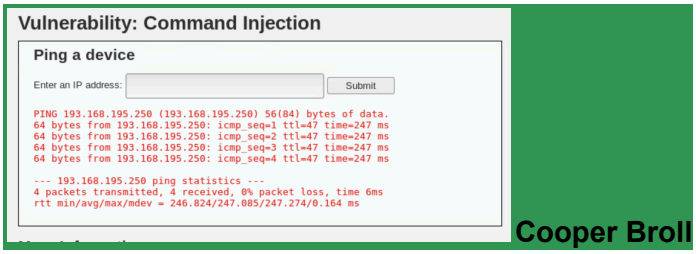
7. Access DVWA on your target's system by visiting `http://InsertTargetIPHere/DVWA`. Log in with the username **admin** and the password **password**.

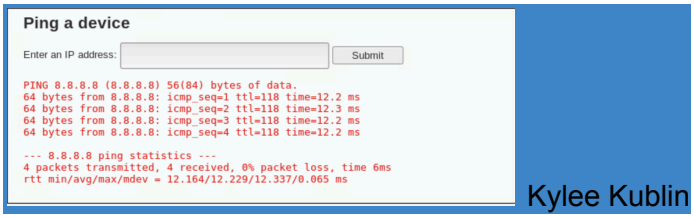
8. On the left side of the screen, you will see a long menu of vulnerabilities and configuration pages. Click on the 'DVWA Security' button towards the bottom. Change the security level to 'low', and click the 'Submit' button.

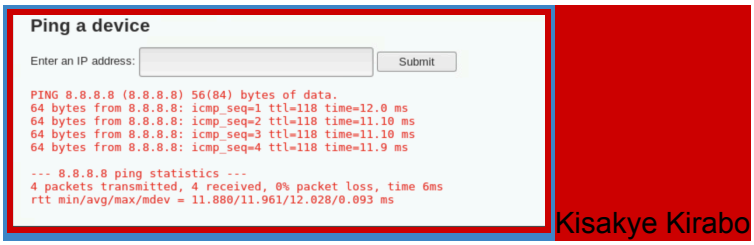




9. Click on 'Command Injection'. You will see an interface titled 'Ping a device'. Input the IP address `8.8.8.8`. Observe that this output is exactly the same as the output that would appear if you ran 'ping' using the Linux command line. **Each student should include a screenshot of your output**. **Include your name with your screenshot.**





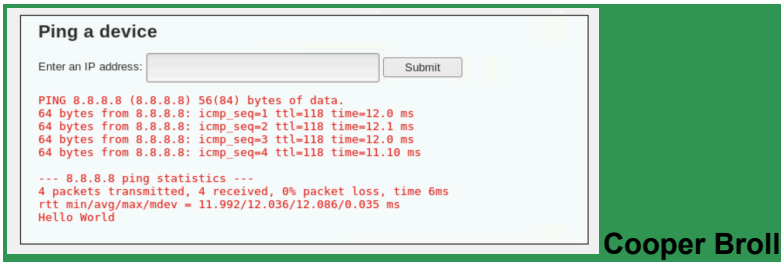


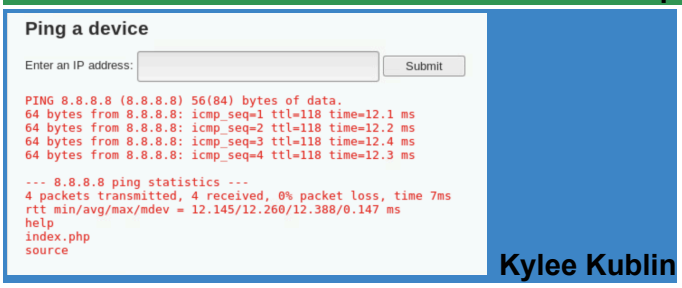
10. Because PHP is passing the input provided in this interface off to the Linux command line, it may be possible to execute other Linux commands. Try typing the following command into the DVWA web interface.

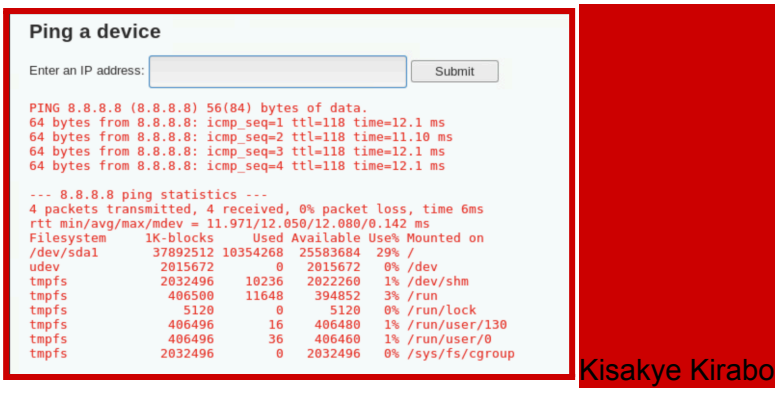
    `8.8.8.8 && pwd`

11. **Each student should describe what happened in step 10.**

12. Replace the Linux command `pwd` with any other Linux command that you've learned in CSEC-140. **Each student should include a screenshot of their command injection attempt. If the command does not appear to work, provide a brief explanation as to why you think that might be.**

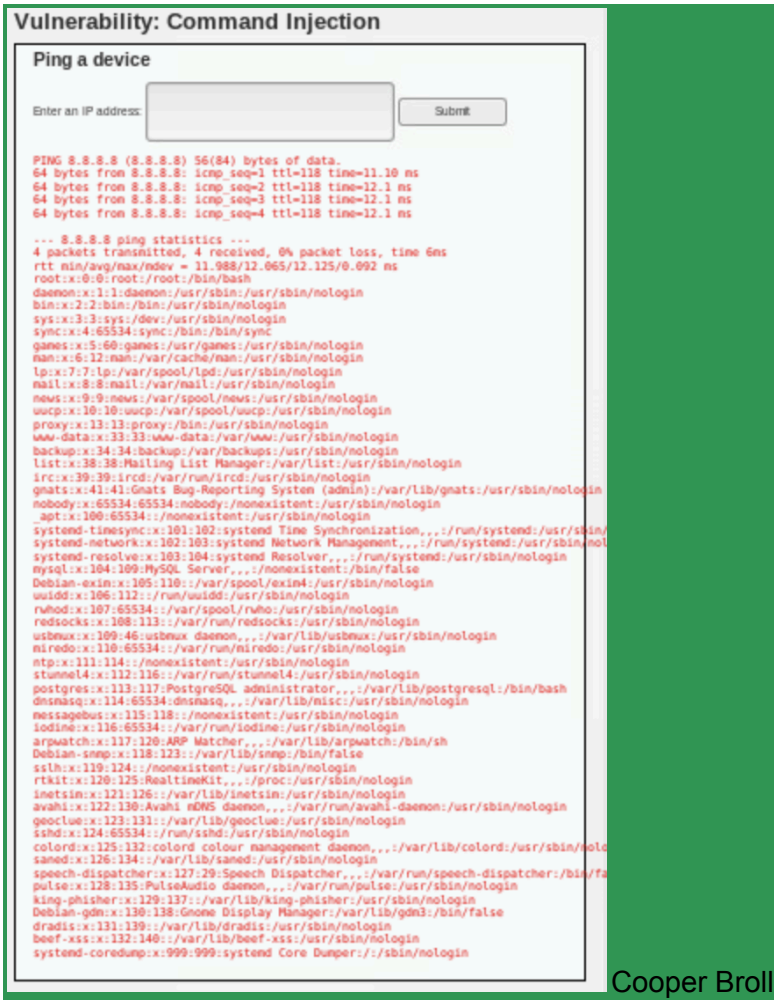






13. The 'cat' command shows the contents of a file at the command line. For example, 'cat /etc/passwd' would show the contents of the Linux passwd file. Conduct an injection

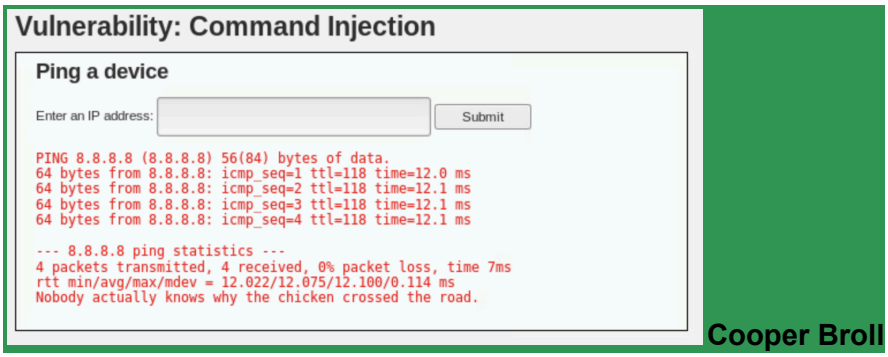
attempt using `8.8.8.8 && cat /etc/passwd`. **Each student should include a screenshot of your output**. **Include your name with your screenshot.**

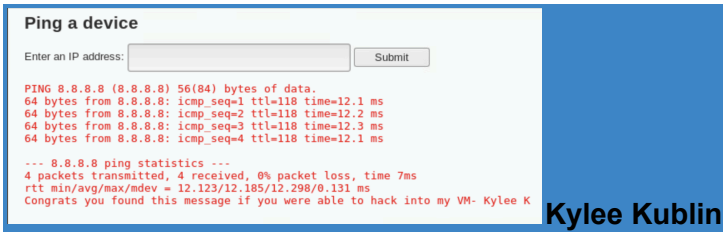


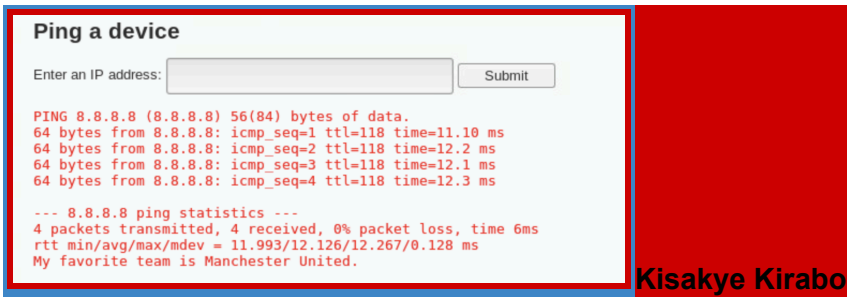
Cooper Broll


Kylee Kublin

14. Use what you have learned in the last several steps to access the secret left for you to find in step 5. **Each student should post a screenshot of an injection attempt displaying the secret. Include your name with your screenshot.**







15. **As a group, identify two ways that an application developer could stop this type of attack.**

If you are interested in learning more about web application security and how DVWA works, you can find walkthroughs describing how to hack DVWA at different levels of security at https://github.com/mrudnitsky/dvwa-guide-2019.