Sample Plan of Action

Identify

- **Web server:** I will reference my network design from the Project 2.1.3 Ecommerce Architecture. I plan to validate that the Bikes, Boards, and Beyond architecture represents a solution that separates public-facing and private information. I can use the Connections folder to log in to each host and then run netstat -an to confirm the host is either listening for web page requests (and is a web server) or is not.

- **Website:** I will visit each page of the website. For any pages that are interactive or use a script, I will try the exploits that I know to see whether they work or they fail and then determine whether the pages are secure.

Detect

Reminder: Students will not actually turn the firewall on, disable directory browsing, change the log file location, nor disable FTP. The only need to recommend these actions.

- **Web server:**
  Hint: Students should test for six server configurations including vulnerabilities. If they don't recall them, direct them to Lesson 2.2 and their own documentation.

  - I will check whether the firewall is running.
  - I will try to perform directory browsing on the website.
  - In a browser, I will check whether the Log file is still the default location (C:\inetpub\logs) and if log files are visible.
  - I will test the FTP service to see whether I can transfer a file to the server over FTP. I can also use netstat -an to see if port 21 is listing.
  - I will use netstat -an to check whether SMTP is running and observe whether port 25 is listening.
  - To test loose-lipped error messages, I will access a non-existing web page.

- **Website:**
  Hint: Students should know to test all four exploits on both web pages. If they don't recall them, direct them to Lesson 2.3 and their own documentation.

  - I will try all of the exploits on both interactive web pages.
    - Command execution
    - SQL Injection
    - XSS reflected
    - XSS stored
  - I will capture screenshots of any web pages that show evidence of exploits.
  - I will capture screenshots of the Wireshark packet showing the test URL. To make packet analysis easier, I can run Wireshark only while I test each page.
  - I will capture screenshots of the Wireshark packet showing the test URL. To make packet analysis easier, I can run Wireshark only while I test each page.

Protect

- **Web server:**
  Hint: If students don't recall how to configure the web server , direct them to Lesson 2.3 and their own documentation.

  - Based on the results of my security checks in the browser, I will use the Server Manager to recommend:
    - Ensure the firewall is enabled.
    - Change the location of the log file.
    - Disable directory browsing, FTP, SMTP, and loose-lipped errors.

- **Website:**
  Hint: If students struggle to identify the correct script to the exploit, remind them they can use the View source feature from the right-click menu on a web page to see the page source code.

  - I will identify the page(s) of their website that can be exploited. I will identify the exploit as one of: command execution, SQL injection, xss reflected, and/or xss stored.

Respond with a Report

Recommendations to secure the server: I will provide screenshots of the Server Manager's new settings for the disabled directory browsing feature, the new log file location, and the disabled FTP service.
Documentation and **evidence:** I will provide screenshots of the exploited web page, the captured Wireshark packets showing the exploited URL, and the recommended software fix (the screenshot of the highly secure code related to this exploit I learned about in Lesson 2.3).