



Cybersecurity

Module 15 Challenge Submission File

Testing Web Applications for Vulnerabilities

Make a copy of this document to work in, and then respond to each question below the prompt. Save and submit this completed file as your Challenge deliverable.

Web Application 1: *Your Wish is My Command Injection*

Provide a screenshot confirming that you successfully completed this exploit:

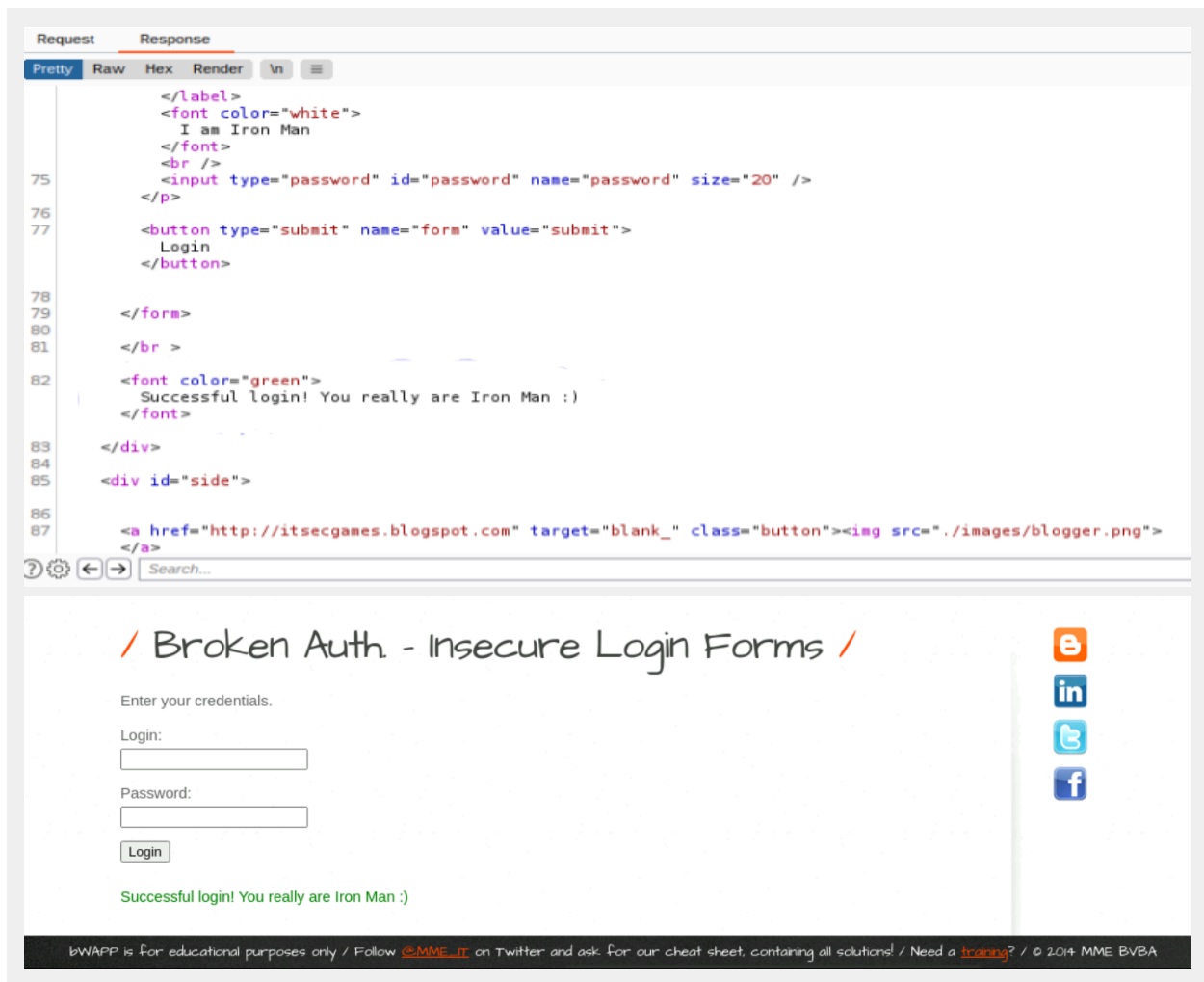
The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The sidebar on the left contains navigation links: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection (highlighted), CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), and CSP Bypass. The main content area is titled 'Vulnerability: Command Injection'. It features a 'Ping a device' section with a form to 'Enter an IP address:' and a 'Submit' button. Below the form, the output of a ping command is displayed in red text: 'PING 127.0.0.1 (127.0.0.1): 56 data bytes', followed by four lines of ping results showing 64 bytes from 127.0.0.1 with various ICMP sequence numbers and times. The output concludes with '4 packets transmitted, 4 packets received, 0% packet loss' and 'round-trip min/avg/max/stddev = 0.037/0.058/0.089/0.000 ms'. Below this, a 'More Information' section lists four links: <http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>, <http://www.ss64.com/bash/>, <http://www.ss64.com/nt/>, and https://www.owasp.org/index.php/Command_Injection.

Write two or three sentences outlining mitigation strategies for this vulnerability:

Using proper coding practices and regularly updating and patching software, can help. Also, conducting thorough security assessments, and employing intrusion detection systems.

Web Application 2: A Brute Force to Be Reckoned With

Provide a screenshot confirming that you successfully completed this exploit:

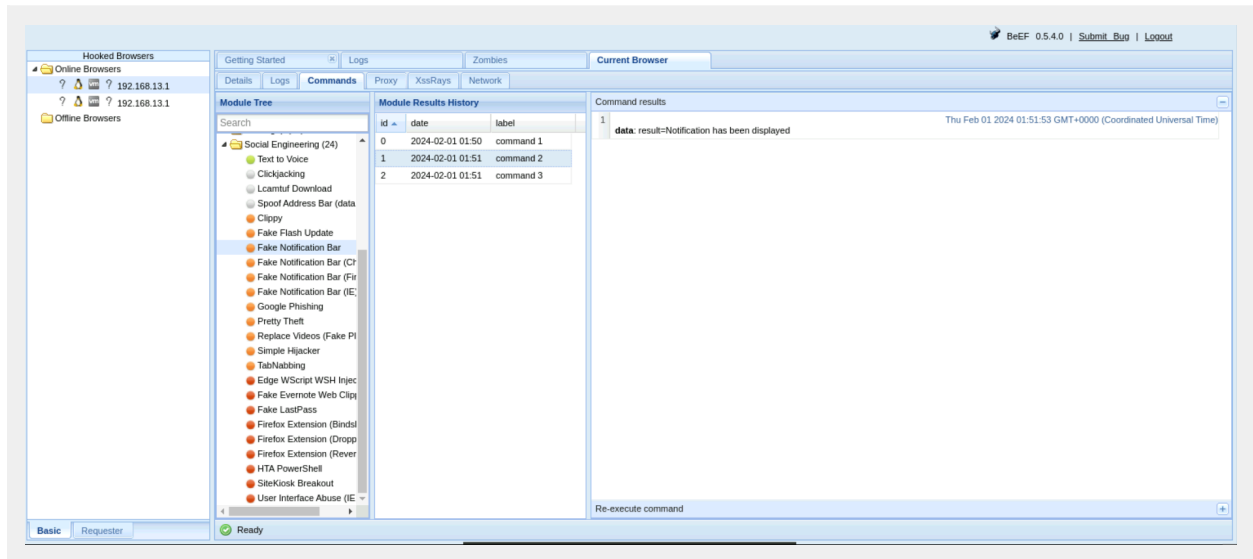


Write two or three sentences outlining mitigation strategies for this vulnerability:

Locking out an account after a certain number of failed attempts, as many websites do. Also, requiring usernames and passwords to be more complex. Also, using multi-factor authentication.

Web Application 3: *Where's the BeEF?*

Provide a screenshot confirming that you successfully completed this exploit:



Write two or three sentences outlining mitigation strategies for this vulnerability:

Regularly updating passwords is a very good way to prevent this vulnerability. Also, performing security tests such as pen testing.