



Cybersecurity

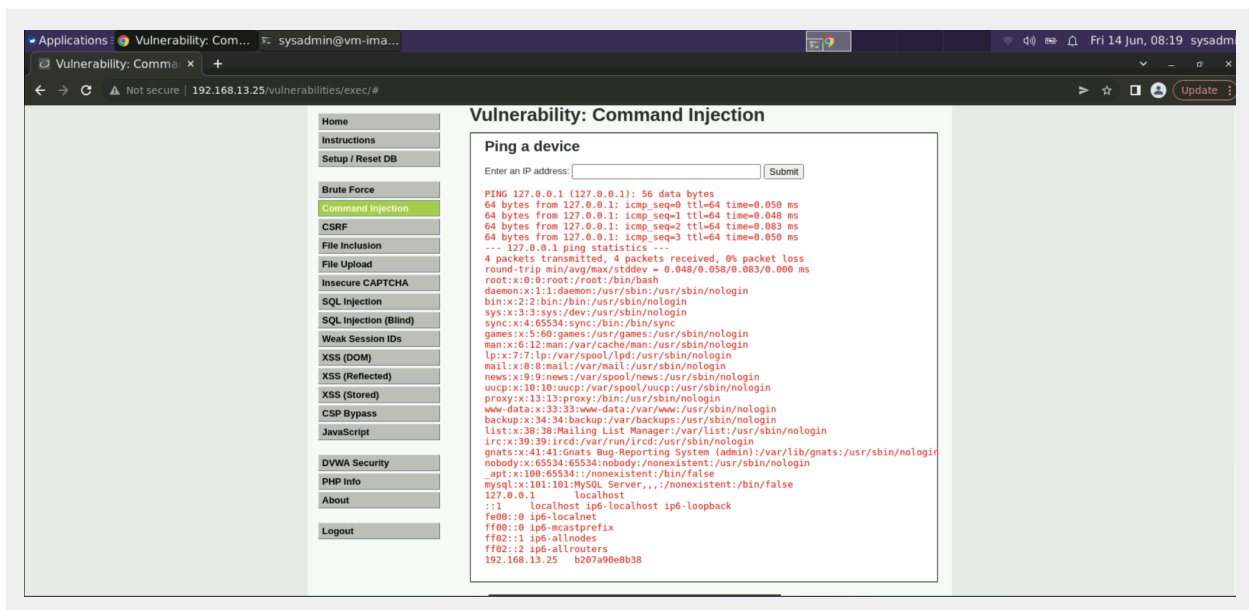
Module 15 Challenge Submission File

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:

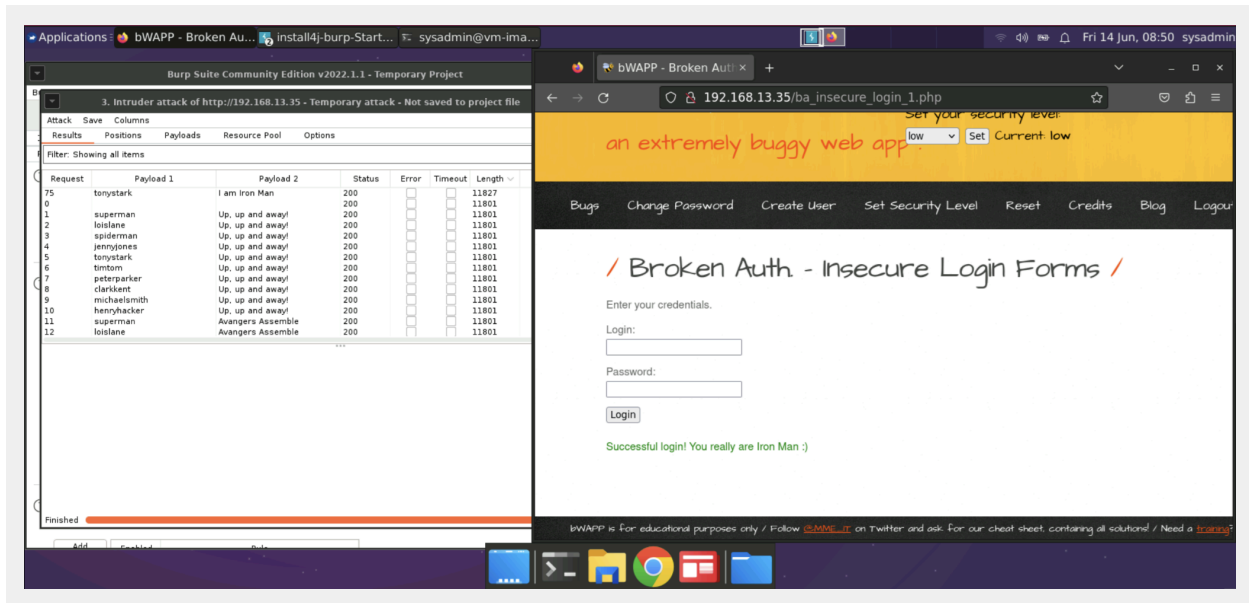


Write two or three sentences outlining mitigation strategies for this vulnerability:

Restrict web server permissions when accessing confidential data and files. Restrict web input to disallow the use of special characters to be inputted into the search functions. Implementing server-side validation will also help to mitigate against such attacks.

Web Application 2: A Brute Force to Be Reckoned With

Provide a screenshot confirming that you successfully completed this exploit:

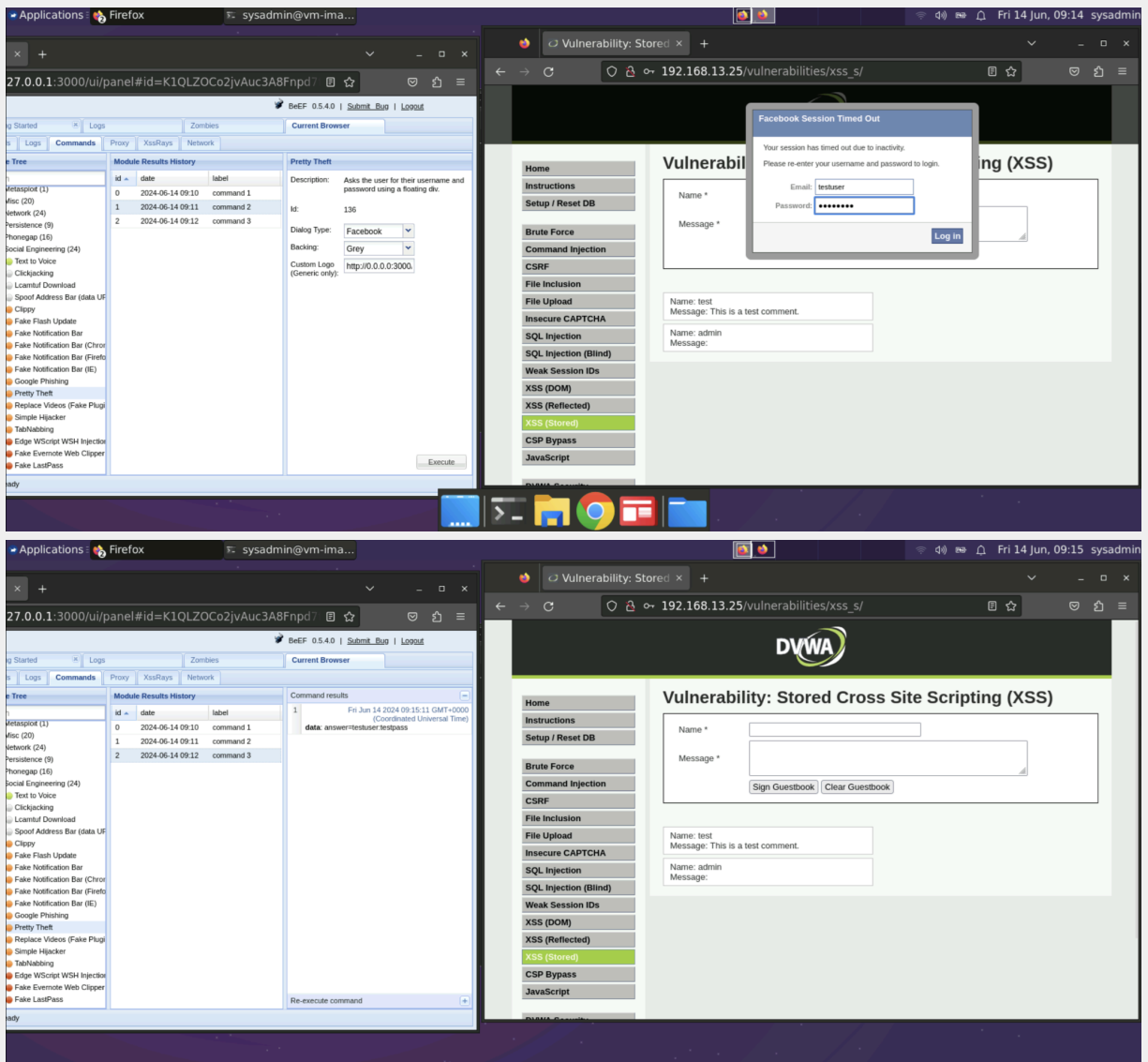


Write two or three sentences outlining mitigation strategies for this vulnerability:

Enabling multi factor authentication on user devices will help to mitigate against this vulnerability. Implementing a lockout of the login page when user's exceed a certain number of failed login attempts would also aid in protecting against this vulnerability.

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:

Deny malicious scripts as inputs through the use of adding server-side input validation. You can also use HTTP response headers that mitigate against the insertion of malicious scripts.