Basic Browser Automation for Security Testing

Submitted by:

Ravinshu

Cyber Security Student

Internship: Penetration Testing Internship

Organization: Deltaware Solutions

Date of Submission: September 2025

1. Objective

The objective of this project is to create a simple browser automation script using Python and Selenium that can:
- Open a target website.
- Detect and test a login form with dummy credentials.
- Capture a screenshot as proof of execution.

This simulates a basic penetration testing task where an analyst checks for weak credentials and documents the test.

2. Tools & Technologies Used

- Python 3
- Selenium (for browser automation)
- Google Chrome + ChromeDriver

3. Methodology / Steps

Step 1: Setup
- Installed Python and Selenium.
- Downloaded ChromeDriver to run automated tests.

Step 2: Script Development
- Wrote a Python script that:
1. Opens the target website.
2. Searches for a login form.
3. Attempts login with test credentials (admin : 1234).
4. Saves a screenshot for documentation.

Step 3: Execution
- Ran the script on the demo site http://testphp.vulnweb.com.
- The script successfully opened the site and captured results.

4. Output

Terminal Output Example:
[+] Opened website: http://testphp.vulnweb.com
[-] No login form found on this page
[+] Screenshot saved as result.png

Generated Screenshot:
- File saved as result.png.
- Shows the page after test execution.

5. Results & Findings

- The script can successfully interact with a website.
- If a login form exists, it can attempt basic login testing.
- The screenshot confirms successful browser automation.

6. Conclusion

This project demonstrates a beginner-friendly penetration testing automation using Selenium. It proves how tasks like login testing and evidence collection can be automated, making the job of a penetration tester more efficient.

The project is intentionally simple to show the practical use of Python in cybersecurity without being too advanced.