Alec Posthauer

2/16/2024

Burp Suite and OWASP Juice Shop Documentation

Source: https://medium.com/emergent-phenomena/securing-web-applications-using-burp-suite-and-owasp-juice-shop-f7539a1b4268

https://jbcsec.com/owasp-juice-shop/

https://www.101labs.net/comptia-security/lab-38-using-burp-suites-intruder/

https://pwning.owasp-juice.shop/companion-guide/latest/part2/injection.html

SQL Injection payloads: https://github.com/fuzzdb-project/fuzzdb/blob/master/attack/sql-injection/detect/xplatform.txt

https://github.com/rapid7/metasploit-framework/blob/master/data/wordlists/default_pass_for_services_unhash.txt

Solutions: https://help.owasp-juice.shop/appendix/solutions.html

To load an instance of OWASP Juice Shop, access the folder of Juice Shop and type “powershell” into the search bar to open powershell in the library. Then type “npm start” into powershell. Once executed, navigate to http://localhost:3000 .

Introduction to Burp Suite: Burp Suite has 4 essential features to test web application security: Target, Proxy, Repeater, and Intruder. Target sets the target for the penetration testing. Proxy captures the requests/responses, otherwise known as traffic, to and from the web application. Repeater allows you to modify and repeatedly send HTTP requests. Intruder is a tool for automating attacks against the web application.

Task 1: We navigate to the customer feedback page on the Juice Shop and send a POST request to the server. The values can contain anything for this. We then navigate to the Proxy tab and the HTTP history sub-tab in Burp Suite. We can then find our post request of POST /api/Feedbacks/ and right-click to send this to the repeater. Within the repeater, we can manipulate the “rating” to an invalid value such as zero, representing a zero-star review which is not allowed as the value should be between 1 and 5.

Task 2: We will utilize SQL injection on the Intruder tab in Burp Suite to gain access to an authorized account in Juice Shop. Start by entering any credentials into the Juice Shop login page, then find the POST request and send it to intruder by right-clicking on it. In the Intruder tab and the positions sub-tab, highlight over the content in the quotation marks for the credentials, excluding the quotation marks. Then click add$ on the right side of the page. Next, navigate to the payloads sub-tab and copy and paste the SQL injection payload from the link at the top of this documentation. Start the attack. A successful 200 status means you have an authenticated email/username which can be used on the login page.

Alternatively, you can go to the Proxy tab and send the POST request for the original login to the repeater and alter the email to the following within the quotation marks: ‘ or 1=1— . This will read as the OR statement reading as true since 1=1, passing the true to be interpreted as a valid user, then the two dashes will comment out any restrictions for the login because the two dashes are comments for SQL.

Task 3: Navigate to the login page and utilize SQL injection by entering the following within the parentheses (‘ or 1=1 –) for the username and (‘) for the password. This will let you into the admin account. Then you can navigate to the home page or any other and inspect element, use a Chrome extension called Cookie Editor to view the token value of the cookie, and paste the value into https://jwt.io/ . Once you have the JSON from that page, you can grab the password which is MD5 and put it into a MD5 decrypter https://www.md5online.org/md5-decrypt.html . You now have your password (admin123). If logged into any account, you can utilize the cookie editor to find out the password.