Open Bug Bounty Project

Introduction:

The Bug hunting on any target of Open Bug Bounty project aims to enhance the security of websites listed on the Open Bug Bounty platform by identifying and reporting vulnerabilities. This report outlines the findings and actions taken during the Bug hunting process.

Target Selection:

For this Bug hunting assignment, the target selected was a popular e-commerce website listed on the Open Bug Bounty platform. The decision to choose this target was based on its widespread usage and potential impact of any identified vulnerabilities.

Testing Methodology:

1. Reconnaissance: Gathered information about the website’s purpose, technology stack and potential vulnerabilities.
2. Scanning: Utilized automated tools to scan the website for common vulnerabilities such as SQL injection, cross-site scripting, and directory traversal.
3. Manual Testing: Conducted manual testing to identify vulnerabilities not detected by automated tools, focusing on input validation, session management, authentication issues.
4. Fussing: Employed fuzzing tools to test for unexpected behavior or input validation errors.
5. Exploitation: Attempted to exploit identified vulnerabilities to verify their impact and potential risks.
6. Reporting: Document all identified vulnerabilities and reported them to the website owner through the Open Bug Bounty platform, providing detailed descriptions, potential impacts, steps to reduce, along with supporting evidence.
7. Verification: Verified the resolution of reported vulnerabilities by retesting the website or reviewing documentation provided by the website owner.
8. Documentation: Maintained detailed documentation throughout the testing process, including encountered issues, methods used, and outcomes.

Findings:

During the bug hunting process, several vulnerabilities were identified, including:

1. Cross-Site Scripting (XSS) vulnerabilities in the website’s search functionality.
2. SQL Injection vulnerabilities in the login form.
3. Authentication bypass vulnerability allowing unauthorized access to user accounts.
4. Directory Traversal vulnerability enabling access to sensitive system files.

Action Taken:

1. Reported Vulnerabilities: Submitted detailed reports of all identified vulnerabilities to the website owner through the Open Bug Bounty platform, including steps to reproduce and supporting evidence.
2. Followed Up: Regularly checked for updates on the reported vulnerabilities and communicated with the website owner for clarification or additional information if needed.
3. Verification: Verified the resolution of reported vulnerabilities by retesting the website and reviewing documentation provided by website owner.
4. Documentation: Maintained comprehensive documentation of the entire bug hunting process, including methodologies, findings, actions taken, and outcomes.

Conclusion:

The Bug hunting on any target of Open Bug Bounty project is crucial for enhancing the security of websites and preventing potential cyber attacks or breaches. By following a rigorous testing methodology and reporting identified vulnerabilities, security researchers contribute to creating a safer digital environment. Continued collaboration between researchers and website owners is essential for addressing security vulnerabilities effectively and ensuring the protection of user data.