OWASP TOP 10 PENTEST REPORT

Website: https://target.com

Author: SK Arif Bin Ekram
Assessment Scope: Identified OWASP Top 10 vulnerabilities

Vulnerability Assessment

1. Injection (OWASP A1:2021)
    - **Affected Component:** Login endpoint **https://target.com/login**
    - **Proof of Concept:** Input **' OR '1'='1** in **username** parameter causes unauthorized access.
    - **Technical Details:** Absence of input validation allows SQL query termination and manipulation.
2. Broken Authentication (OWASP A2:2021)
    - **Affected Component:** Session management **https://target.com/session**
    - **Proof of Concept:** Using whitespace in **username** parameter, e.g., **username=+darren**, bypasses authentication.
    - **Technical Details:** Improper trimming of whitespace leads to authentication bypass.
3. Sensitive Data Exposure (OWASP A3:2021)
    - **Affected Component:** Assets directory **https://target.com/assets**
    - **Proof of Concept:** Directly accessing **https://target.com/assets/webapp.db** reveals sensitive data.
    - **Technical Details:** Misconfigured access controls permit unauthorized retrieval of database files.
4. XML External Entity (XXE) (OWASP A4:2021)
    - **Affected Component:** XML processing endpoint **https://target.com/xml/upload**
    - **Proof of Concept:** Submitting a modified XML document with a crafted entity to read internal files.
    - **Technical Details:** XML parser improperly configured to allow external entity references.
5. Broken Access Control (OWASP A5:2021)
    - **Affected Component:** Note viewing functionality **https://target.com/notes/view**
    - **Proof of Concept:** Altering **note_id** parameter value, **https://target.com/notes/view?note_id=2**, accesses other users' notes.

- **Technical Details:** Parameter manipulation leads to unauthorized access due to IDOR.

6. Security Misconfiguration (OWASP A6:2021)
    - **Affected Component:** Server configuration file exposed at **https://target.com/server/config**
    - **Proof of Concept:** Retrieving **https://target.com/server/config/todo.db** exposes database file.
    - **Technical Details:** Insecure server settings allow unauthorized access to application configuration files.
7. Cross-Site Scripting (XSS) (OWASP A7:2021)
    - **Affected Component:** Search function **https://target.com/search**
    - **Proof of Concept:** Entering **<script>alert(1)</script>** in **search** parameter executes JavaScript.
    - **Technical Details:** Inadequate encoding of user inputs allows scripting attacks.
8. Insecure Deserialization (OWASP A8:2021)
    - **Affected Component:** API endpoint **https://target.com/api/endpoint**
    - **Proof of Concept:** Sending serialized object payload via POST request to **https://target.com/api/endpoint** executes code.
    - **Technical Details:** Application deserializes untrusted data without adequate security checks, leading to RCE.
9. Using Components with Known Vulnerabilities (OWASP A9:2021)
    - **Affected Component:** Third-party bookstore component **https://target.com/bookstore**
    - **Proof of Concept:** Exploiting a known vulnerability in the bookstore component to execute arbitrary code.
    - **Technical Details:** Outdated component with known vulnerabilities lacks necessary updates and patches.
10. Insufficient Logging & Monitoring (OWASP A10:2021)
    - **Affected Component:** Application logs at **https://target.com/logs**
    - **Proof of Concept:** Repeated failed login attempts from the same IP address go unnoticed.
    - **Technical Details:** Logging system fails to capture or alert on potential brute-force attacks, enabling persistent attack attempts without detection.

Conclusion

This security assessment revealed critical vulnerabilities within the web application that align with the OWASP Top 10 risks. Each identified issue has been documented with specific details regarding the

affected components, exploitation methods, and underlying technical weaknesses. Immediate remediation is advised to mitigate these risks and strengthen the application's security posture.

Note: The vulnerabilities outlined in this report are critical and require immediate attention. This assessment was conducted under authorized conditions and complies with standard ethical practices in cybersecurity. The contents of this report are confidential and intended for the security improvement of the web application in question.