OWASP Juice Shop Security Assessment Documentation

1. Introduction
This document outlines the findings of a security assessment performed on the OWASP Juice Shop application. The assessment included vulnerability scanning, directory enumeration, and manual analysis of exposed functionalities.

---

2. Methodology
Tools Used
- **Nikto v2.5.0**: Web server vulnerability scanner.
- **DIRB v2.22**: Directory brute-forcing tool.
- **Manual Testing**: Review of login functionality and exposed endpoints.

Target
- **URL**: `https://juice-shop.herokuapp.com/`
- **Hostname**: `juice-shop.herokuapp.com`
- **IP Addresses**: `54.220.192.176`, `46.137.15.86`, `54.73.53.134`
- **Port**: `443` (HTTPS)

---

3. Findings

3.1 SQL Injection Vulnerability (Login Page)
- **Evidence**:
  - Login form includes a pre-filled email field with `OR 1=1 --`, a common SQL injection payload (Screenshot 1).
  - Potential bypass of authentication or unauthorized access.
- **Severity**: Critical.

3.2 Exposed Sensitive Directories/Files
- **Nikto/DIRB Scan Results**:
  - `/ftp`: Accessible directory (HTTP 200) (Screenshots 3, 4, 5).
  - `/backup.tar`: Potentially sensitive backup file detected (Screenshots 4, 5).
  - `/robots.txt`: Exposes `/ftp` as a crawlable path (Screenshot 3).
- **Impact**: Unauthorized access to backups or internal files.
- **Severity**: High.

3.3 Missing Security Headers
- **Nikto Findings**:
  - Missing `Strict-Transport-Security` (HSTS) header (Screenshot 3).
  - Uncommon headers (`reporting-endpoints`, `x-recruiting`) detected.

- **Impact**: Risk of protocol downgrade attacks or information leakage.
- **Severity**: Medium.

3.4 Server Misconfigurations
- **DIRB Results**:
  - `/profile` and `/redirect` return HTTP 500 errors, indicating server-side issues (Screenshots 4, 5).
  - `/promotion`, `/video`, and `/snippets` are accessible but unvalidated endpoints.
- **Impact**: Potential denial-of-service or exploitation of unstable endpoints.
- **Severity**: Medium.

3.5 Redundant/Insecure Features
- **Digital Wallet Checkboxes**:
  - Repeated "Search for a new WordPress site" options (Screenshot 2) suggest misconfigured or test features.
- **Impact**: Possible UI confusion or entry points for XSS/CSRF attacks.
- **Severity**: Low.

---

4. Recommendations
1. **Input Validation**: Sanitize login inputs to prevent SQL injection.
2. **Secure Sensitive Paths**:
   - Restrict access to `/ftp` and remove `backup.tar`.
   - Update `robots.txt` to block sensitive directories.
3. **Implement HSTS**: Add `Strict-Transport-Security` header.
4. **Error Handling**: Fix HTTP 500 errors on `/profile` and `/redirect`.
5. **Code Review**: Investigate redundant WordPress-related checkboxes for vulnerabilities.

---

5. Conclusion
The assessment identified critical vulnerabilities (e.g., SQL injection, exposed backups) and misconfigurations requiring immediate remediation. Regular penetration testing and adherence to OWASP guidelines are recommended to maintain security.

Scanned By: Nikto, DIRB, Manual Testing
Date: April 2, 2025
Report Version: 1.0

End of Document