Listing of Vulnerabilities (as of July 31, 2013)

- SQL Injection
- O/S Command injection
- JSON injection
- HTML injection
- JavaScript Injection
- DOM injection
- Cascading style sheet injection
- Log injection
- Reflected Cross Site Scripting via GET, POST, Cookies, and HTTP Headers
- Stored Cross Site Scripting
- Cross Site Request Forgery
- Authentication Bypass via SQL injection
- Privilege Escalation via Cookie Injection
- Unencrypted database credentials
- Directory Browsing
- JavaScript validation bypass
- Remote File Inclusion
- Frame source injection
- PHPMyAdmin Console
- SSL Stripping
- Application Exception
- Un-validated Redirects and Forwards
- Phishing
- Click-jacking
- CBC bit flipping (latest)
- Brute force "secret admin pages"
- PHP server configuration disclosure
- Application path disclosure
- Platform path disclosure
- Information disclosure via HTML comments
- robots.txt information disclosure
- Parameter addition
- HTTP Parameter Pollution
- Buffer overflow
- Denial of Service
- Loading of any arbitrary file
- Method Tampering
- Forms caching
- Local File Inclusion
- Comments with sensitive data
- Insecure Cookies
- XML External Entity Injection
- Unrestricted File Upload

(Introduction To OWASP Mutillidae (Web Pentest Training Environment).pdf, Appendix A, Page 25-26)