Web Penetration Testing

This cheatsheet is built for Red Teamers and Penetration Testers in order to help them hunt for vulnerabilities. It is designed such that beginners can understand the fundamentals and professionals can brush up their skills with the advanced options. There are multiple ways to perform all the mentioned tasks, so we've performed and compiled this list with our experience. Please share it with your connections and send your queries and feedback directly to Hacking Articles.

Follow us on

1. XXE Injection
2. CSRF
3. Cross-Site Scripting Exploitation
4. Cross-Site Scripting (XSS)
5. Unrestricted File Upload
6. Open Redirect

7. Remote File Inclusion (RFI)
8. HTML Injection
9. Path Traversal
10. Broken Authentication & Session Management
11. OS Command Injection
12. Multiple Ways to Banner Grabbing
13. Local File Inclusion (LFI)
14. Netcat for Pentester
15. WPScan:WordPress Pentesting Framework
16. WordPress Pentest Lab Setup in Multiple Ways
17. Multiple Ways to Crack WordPress login
18. Web Application Pentest Lab Setup on AWS
19. Web Application Lab Setup on Windows
20. Web Application Pentest Lab setup Using Docker
21. Web Shells Penetration Testing
22. SMTP Log Poisoning
23. HTTP Authentication
24. Understanding the HTTP Protocol
25. Broken Authentication & Session Management
26. Apache Log Poisoning through LFI
27. Beginner's Guide to SQL Injection (Part 1)
28. Boolean Based
29. How to Bypass SQL Injection Filter
30. Form Based SQL Injection
31. Dumping Database using Outfile
32. IDOR