**List of Bookmarks**

This document is an index for all website gathered during PWK labs, this will come in handy during PWK exam as it’s more intuitive as far as search goes compared to KeepNote.

**Windows Privilege Escalation**

<http://www.fuzzysecurity.com/tutorials/16.html>

**Reverse Shell Cheat Sheet**

<http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet>

**MSSQL Injection Cheat Sheet**

<http://pentestmonkey.net/cheat-sheet/sql-injection/mssql-sql-injection-cheat-sheet>

**MySQL SQL Injection Cheat Sheet**

<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

**Postgres SQL Injection Cheat Sheet**

<http://pentestmonkey.net/cheat-sheet/sql-injection/postgres-sql-injection-cheat-sheet>

**Online Password Cracker**

<https://crackstation.net/>

**Linux Privilege Escalation**

<https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/>

<https://www.rebootuser.com/?p=1623>

**Local File Inclusion**

<http://resources.infosecinstitute.com/local-file-inclusion-code-execution/#gref>

<http://www.securityidiots.com/Web-Pentest/LFI/guide-to-lfi.html>

**Web vulnerabilities to gain access to the system - paper**

<https://www.exploit-db.com/papers/13017/>

**Bypassing File Upload Restrictions**

<http://www.securityidiots.com/Web-Pentest/hacking-website-by-shell-uploading.html>

**Basic SQLi**

<http://www.securityidiots.com/Web-Pentest/SQL-Injection/Part-1-Basic-of-SQL-for-SQLi.html>

<http://www.securityidiots.com/Web-Pentest/SQL-Injection/Part-2-Basic-of-SQL-for-SQLi.html>

<http://www.securityidiots.com/Web-Pentest/SQL-Injection/Part-3-Basic-of-SQL-for-SQLi.html>

<http://www.sqlinjection.net/login/>

**Script to compile some known exploit for immediate use**

<https://github.com/codingo/OSCP-1>

**Default Passwords Database**

<https://cirt.net/passwords>

**IIS 6 WebDAV .asp Webshell Upload Guide**

<http://www.r00tsec.com/2011/09/exploiting-microsoft-iis-version-60.html>

**Total OSCP Guide**

<https://sushant747.gitbooks.io/total-oscp-guide/content/>

**Pass the Hash**

<https://github.com/byt3bl33d3r/CrackMapExec>

**PowerSploit**

<https://github.com/PowerShellMafia/PowerSploit#powerup>

**WordPress Shell Plugin**

<https://github.com/leonjza/wordpress-shell>

**LFI Scanner**

<https://github.com/monkeysm8/CTF-Stuff/blob/master/LFI_Scanner.py>

**Shell Escape**

<https://speakerdeck.com/knaps/escape-from-shellcatraz-breaking-out-of-restricted-unix-shells>

<https://pen-testing.sans.org/blog/2012/06/06/escaping-restricted-linux-shells>

<https://netsec.ws/?p=337>

**Spawn TTY Shell**

<https://netsec.ws/?p=337>

**\*NIX Apache Logs Location**

<http://blog.codeasite.com/how-do-i-find-apache-http-server-log-files>