A4 – Nezabezpečený přímý odkaz na objekt

- **Instalační soubory:**
- Správce webu zapomněl odstranit instalační soubor install.php:
- Když do prohlížeče zadáte http://getsimple.silenceplease.cz/admin/xinstall.php (ale nepokračujte v instalaci :-), zřejmě budete mít možnost web přeinstalovat. V tomto případě si někdo myslel, že místo odstranění instalačního souboru install.php jej stačí přejmenovat na xinstall.php.

- **Citlivé informace – PHPINFO:**
- Vývojáři často zapomínají odstranit stránku s citlivými informacemi o nastavení platformy:
- http://localhost/dvwa/phpinfo.php – takové informace velmi usnadňují postup útoku.

- **Citlivé informace – hesla:**
- A vývojář zapomněl také soubor s hesly pod http://getsimple.silenceplease.cz/e107_media/438a1ca919/passwd.txt.
- Ale muže se jednat i o další příklady: databázový klíc jako parametr v URL, který by prý měli znát max. jen administrátoři, ale protože je predikovatelný, zjistí je i uživatel s nižším oprávněním atp.
- **Google hacking** (viz wiki) – do Googlu zkuste zadat například**:**
- p@ssw0rd inurl:pdf site:cz
- inurl:admin.php site:cz
- inurl:intranet site:cz
- atd.