A3 – Cross-Site Scripting (XSS) – XSS (Stored)

- http://localhost/dvwa
- XSS (Stored)
- Do pole „Name *“ zadejte nějaké jméno (např. Petr) a do pole „Message *“ zadejte nějakou
- zprávu (např. „Ahoj!“) a odešlete („Sign Guestbook“).
- To je chtěné chování. Zpráva byla odeslána a zobrazena.

- **Přesměrování na jiný web:**
- Do pole „Name *“ zadejte nějaké jméno (např. Petr) a do pole „Message *“ zadejte řetězec <script>window.location.href="https://silenceplease.cz"</script>
- Nedaří se vám do pole „Message *“ zadat celý řetězec? Řešení je následující:
- Pravým tlačítkem kliknete do pole „Message *“ a vyberte Inspect Element (Q). Následně v *<textarea name="mtxMessage" cols="50" rows="3" maxlength="50"></textarea>* změňte *maxlength="50"* na *maxlength="500"*. Následně klikněte do stránky, znovu zadejte kýžený řetězec do pole "Message *" a zprávu odešlete (Sign Guestbook).
- Během chvíle dojde k přesměrování. Takže do prohlížeče opět musíte zadat: http://localhost/dvwa/
- XSS (Stored)
- Ale zase jste přesměrováni. A to je podstata takových útoku – pokaždé, když uživatel (možná oběť) vstoupí na napadenou stránku, útočný skript se spustí.
- Aby vás něco takového dále neobtěžovalo během experimentování, resetujte databázi:
- http://localhost/dvwa/
- Setup / Reset DB
- Create / Reset Database.

- **Únos hodnoty session** (tato hodnota identifikuje uživatelovo sezení a útočník ji muže použít k přihlášení do uživatelova sezení bez toho, aniž by znal přihlašovací údaje.)
- Do pole "Name *" zadejte nějaké jméno (napr. Petr) a do pole "Message *" zadejte řetězec <script>document.write('')</script>
  Zda se podařilo hodnoty session přenést na jiný server, můžete ověřit na adrese https://www.silenceplease.cz/session.txt.