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

- http://localhost/dvwa
- XSS (Reflected)
- Do formuláře „What's your name?“ zadejte nějaké jméno, třeba Petr. Správně se zobrazí „Hello Petr“.
- Všimněte si URL http://localhost/dvwa/vulnerabilities/xss_r/?name=Petr
- Zkuste URL doplnit řetězcem <script>alert('XSS1')</script>, tzn. http://localhost/dvwa/vulnerabilities/xss_r/?name=Petr<script>alert('XSS1')</script>
- Jestli se vám zobrazil dialog s nápisem XSS1, objevili jste zranitelnost typu Cross-Site Scripting.
- Pokud vám experiment nefunguje ve Firefoxu mužete zapnout/vypnout filtr JS:
  about:config
  browser.urlbar.filter.javascript
  poklikat

- **Vložení obsahu jiného webu:**
- Nejdříve do formuláře „What's your name?“ vložte
  <iframe src="https://www.silenceplease.cz"></iframe>
- Potom <iframe src="http://cuni.cz"></iframe>
- To, že se obsah prvního nezobrazil a obsah druhého webu zobrazil, je dáno HTTP hlavičkou X-Frame-Options (v případě https://www.silenceplease.cz nastavenou na straně serveru).

  Poznámka: Pomocí hlavičky X-Frame-Options může server prohlížeči sdělit svou představu o chování stránky vložené v rámu (frame, iframe). Server tak může ovlivnit, zda stránka může být vložena všude, jen z jiných stránek téhož serveru nebo nikdy nikam. X-Frame-Options slouží jako ochrana proti clickjackingu (legitimní stránka je natažena ve framu a překryta průhledným obsahem, při kliknutí na místo, kde je v legitimní stránce nějaký prvek je vykonáno kliknutí v záškodnickém průhledném rámu). . X-Frame-Options lze použít také tehdy, když nechceme, aby se stránka zobrazovala jinde vložené v rámu (např. obalené cizím webem, reklamou atp.).

- **Změna velikosti iframu:**
- Do formuláře „What's your name?“ vložte
  <iframe src=" http://cuni.cz /" width="500" height="500"></iframe>
  Mohli bychom do webu vložit například formulář pro zadání přihlašovacích údajů?

- **Přesměrování na jiný web:**
  Do formuláře „What's your name?“ vložte
  <script>window.location.href="https://silenceplease.cz"</script>
- Mohli bychom uživatele přesměrovat na podvodnou stránku?
- Dokázali byste s touto zranitelnosti (XSS- Reflected) zaútočit?