M183 Applikationssicherheit Implementieren # 3

By Jürg Nietlispach

Recap # 2?

Recap # 2

Passwords!

1. Persistent XSS Attack
2. Reflected XSS Attack
3. DOM Based XSS Attack

4. Email-Phishing with Clickjacking (UI redress attack) (Iframe / 1:1)

Übung «XSS in Practice»

Implementierung Keylogger-Login fertigstellen

Übung «XSS in Practice»

Implementierung Fake-Login-Snippet (Plain Javascript)

1. index.html-File erstellen
2. <script></script> - Tag vor dem </body> - Tags
3. «DOM» für Fake-Login erstellen (Input-Felder & Formular)
4. «Formular-Submit» Event erstellen
5. «AJAX» Routine vorbereiten, welche dann die «Credentials» an einen Endpunkt (noch zu definieren) sendet.

Übung «XSS in Practice»

Fragen / Konzeptuelle Gedanken zum Fake-Login-Snippet

- Was ist beim Endpunkt für den Push der Fake-Login-Daten zu beachten (Hintergrund: Persistente XSS Attacke)?

- Was ist bei der Wahl des Zeitpunkts des Datenpushes zu beachten?

- Bei welchen Webseiten funktioniert das Snippet (10’ Max)

Übung
«Iframe -Clickjacking»

1. index.html File erstellen, welches z.B. digitec.ch, fleurope.ch etc. via Iframe einbindet.
2. Loginform in Iframe erstellen, welches das original Formular überblendet.
3. Submit des Logins abfangen und zum senden an Endpunkt vorbereiten