LU09a - CORS & HTTPS

In diesem Kapitel werden einige praxisrelevanten Stolpersteine erklärt.

CSRF / CORS

CSRF (Cross-Site Request Forgery) ist ein Angriff, bei welchem der Angreifer sensible Informationen oder gar Zugang zu einem Account des Opfers erlangen kann.

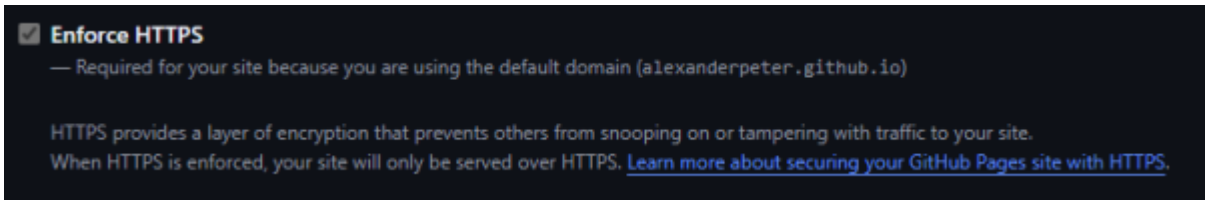
1. Das Opfer ist auf einer validen Webseite eingeloggt und besitzt somit ein Cookie o. Ä. mit der Session.
2. Der Täter bringt das Opfer dazu eine präparierte Webseite aufzurufen (zum Beispiel via Phising Mail o. Ä.).
3. Im Hintergrund wird von der präparierten Webseite eine Anfrage zur validen Webseite geschickt, inklusive der Session aus dem Cookie.
4. Die valide Webseite führt die Aktion aus oder liefert sensible Informationen an die präparierte Seite des Angreifers zurück.

CORS (Cross-Origin Resource Sharing) ist reguliert Webseitenübergreifende Aufrufe und bietet so ein Sicherheitsmechanismus, um CSRF zu verhindern, indem Seitenübergreifende Aufrufe grundsätzlich verhindert werden.

Damit ein Frontend auf ein Backend zugreifen kann, muss die entsprechende Erlaubnis im Backend konfiguriert sein.

Github Pages

Github Pages ermöglicht es statische Webseiten zu hosten. Jedoch ist man mit der Standard-Domain (github.io) gezwungen, HTTPS zu benutzen (Siehe Sceenshot).



Mehr dazu auf
https://docs.github.com/pages/getting-started-with-github-pages/securing-your-github-pages-site-with-https

Dies hat zur Folge, dass sämtliche APIs, welche von einer solchen Webseite aufgerufen werden, ebenfalls HTTPS unterstützen müssen.