OC Entwicklung - Change #1004

[Security] Bei login über https: Cookies nur über https senden

08/08/2016 16:41 - Rotzbua

Status:	erledigt	**% Done:**	100%
Priority name:	2 mittel	**Estimated time:**	0.00 hour
Assignee:			
Target version:	Version 3.1.1		
Ticket Referenz:		**Kategorien:**	Security

Description

(2) Bei login über https: Cookies nur über https senden
Umsetzung: mittel
Prio: mittel
Angriffsszenario: passive or active MiTM
Hintergrund:
Wird über https eingeloggt so wird ein Cookie gesetzt, welches über jede Verbindung also auch über unsicheres http gesendet wird, gesetzt.
Lösung:
Cookie httpsonly setzen.
Vorschlag:
Cookie mit sensiblen Daten httpsonly setzen. Ein weiteres Cookie setzen welches signalisiert, dass über https eingeloggt wurde und automatisch dann auf https zurückgeleitet wird falls die Seite über http aufgerufen wird.

Usecase:
Login über http:
Session-Cookie ganz normal wie jetzt setzten.
-> http und https funktionieren so wie jetzt

Login über https:
Session-Cookie httpsonly setzen, dann wird dieser Cookie nur über https übertragen (ist eine Cookie Eigenschaft), zweiten "normalen" UmleitenNachHTTPS-Cookie setzen.
-> Aufruf über http: Session-Cookie wird nicht übertragen (MiM kann nicht Session klauen), UmleitenNachHTTPS-Cookie wird übertragen -> Seite erkennt das und leitet auf https um
-> Aufruf über https: alles wie bisher

Associated revisions

Revision 0de94600 - 09/21/2016 00:24 - Rotzbua

change cookie for https; updates #1004

- https only if login was https
- add flag cookie to redirect to https
- on logout destroy redirect flag cookie

History

#1 - 08/15/2016 13:56 - Rotzbua

PR ist draußen, lokal getestet

#2 - 10/25/2016 00:06 - teiling88

- Status changed from neu to erledigt

- % Done changed from 0 to 100