Foreman - Bug #4968

API with SSO access requires some CSRF protection

03/31/2014 01:24 PM - Dominic Cleal

Status:	New		
Priority:	Normal		
Assignee:			
Category:	Security		
Target version:			
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

The API can be accessed with our SSO implementations (e.g. REMOTE_USER, mod_auth_kerb), an existing session (#4776, #4895) or the HTTP basic auth "SSO" impl.

When using SSO impls, we should employ some CSRF protection so a user with say, an active Kerberos ticket, can't be attacked to perform API requests using their active SSO.

See https://github.com/theforeman/foreman/pull/1331#issuecomment-39075332 for some background.

Related issues:

Related to Foreman - Bug #4895: API should check for the presence of a CSRF t...	**Closed**	**03/26/2014**

History

#1 - 03/31/2014 01:25 PM - Dominic Cleal

- Related to Bug #4895: API should check for the presence of a CSRF token when there is a session user added