

Infrastructure - Task #3891

review vulnerability to BREACH attacks

2013-08-07 15:01 - Dave Vieglais

Status:	New	Start date:	2013-08-07
Priority:	Normal	Due date:	
Assignee:	Dave Vieglais	% Done:	0%
Category:	Authentication, Authorization	Estimated time:	0.00 hour
Target version:		Story Points:	
Milestone:	None		
Product Version:	*		
Description			
Description at: http://arstechnica.com/security/2013/08/gone-in-30-seconds-new-attack-plucks-secrets-from-https-protected-pages/			
The technique works by exploiting patterns of similarity in compressed HTTPS responses. Turning of gzip compression on the server response avoids the vulnerability at the expense of increased bandwidth.			
Goal of this task is to determine which, if any, services provided by DataONE are vulnerable (i.e. provide interesting information) to an attacker.			