Open eClass - Σφαλματα #119

Ελλειψη addslashes στη διαδικασια εγκαταστασης

12/11/2013 03:21 - Yury Kherimyan

Status:	Επιλυμενο	**Start date:**	12/11/2013
Priority:	Κανονικη	**Due date:**	
Assignee:		**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:		**Spent time:**	0.00 hour

Description

Κατα την διαδικασια εγκαταστασης, δεν γινεται καποιο input sanitization με αποτελεσμα να μπορει να γινει inject καποιο κομματι κωδικα στο αρχειο config.php
Παρατηρηθηκε οταν το ονομα μιας εγκαταστασης περιειχε μια αποστροφο ('), η οποια προκαλουσε php error με blank page. Ισως μετα τη κληση της register_posted_variables()
η και μεσα στην register_posted_variables() να καλουνταν και η addslashes για να εξαλειφοταν αυτος ο κινδυνος.

History

#1 - 14/11/2013 17:25 - Αλεξανδρος Διαμαντιδης

- Status changed from Νεα to Επιλυμενο

- % Done changed from 0 to 100

Σας ευχαριστουμε για την επισημανση του προβληματος! Το θεμα εχει λυθει στην εκδοση 2.8 της πλατφορμας που μολις κυκλοφορησε. Ενημερωτικα, στην υπο αναπτυξη εκδοση 3 δεν υπηρχε το προβλημα αυτο καθως ολες οι ρυθμισεις (εκτος απο τα στοιχεια συνδεσης με τη βαση δεδομενων) αποθηκευονται στη βαση, με το σωστο escaping/sanitization.