**Κουτρουλής Χριστόδουλος**

**AM: ais0056**

Ο ιστότοπος καταχώρησης παραπόνων στον δήμο Πειραιά αποτελείται από 3 php αρχεία, 1 αρχείο css και 5 εικόνες. Το αρχείο **report.php** είναι μια καθαρά html φόρμα χωρίς php κώδικα και είναι η σελίδα η οποία απευθύνεται στον ενδιαφερόμενο χρήστη. Το αρχείο **validate.php** είναι αυτό που περιέχει όλον τον κώδικα σε php που επεξεργάζεται τα δεδομένα της προηγούμενης φόρμας και με ασφαλή τρόπο τα καταχωρεί στην βάση δεδομένων. Το τελευταίο php αρχείο, με όνομα **recaptchalib.php** δίνεται έτοιμο για να υποστηρίξει την λειτουργία re-captcha. Η εφαρμογή συνοδεύεται από ένα αρχείο με όλες τις εντολές sql που χρησιμοποιήθηκαν, το **db\_queries.sql**, από έναν φάκελο με όνομα **SSL keys** που περιέχει τα κλειδιά για πρόσβαση με κρυπτογραφημένη σύνδεση και 2 εικόνες όπου φαίνονται λεπτομέρειες για την κατασκευή του πιστοποιητικού. Τέλος υπάρχει ένας φάκελος με όνομα **Recaptcha** που περιέχει ένα .txt αρχείο με τα κλειδιά για τον έλεγχο reCaptcha.

Όλη η λογική της προστασίας της φόρμας από SQL injection και από XSS βρίσκεται στο αρχείο **validate.php**. Πιο συγκεκριμένα οι άμυνες κατά του **SQL injection** που χρησιμοποιούνται είναι:

α) Εισαγωγή των δεδομένων στην βάση μέσω μιας stored procedure που έχει δημιουργηθεί για τον σκοπό αυτό.

β) Ο λογαριασμός mySQL που χρησιμοποιείται από το σενάριο validate.php έχει δικαίωμα μόνο να καλεί την παραπάνω stored procedure στην συγκεκριμένη βάση και τίποτα περισσότερο.

γ) Όλα τα δεδομένα που πρόκειται να δοθούν σαν ορίσματα στην stored procedure, περνούν επεξεργασία από την συνάρτηση **mysqli\_real\_escape\_string** σαν ένα έξτρα επίπεδο προστασίας.

Οι άμυνες του σεναρίου κατά των επιθέσεων **XSS** περιλαμβάνουν:

α) Τον προκαθορισμό του είδους της αίτησης και τον προκαθορισμό όλων των πεδίων που αναμένεται να περιέχονται σε αυτήν (συγκεκριμένα ονόματα και είδος τιμών στο καθένα).

β) Όπου αναμένεται string, χρησιμοποιείται συνδυασμός φίλτρου απολύμανσης (FILTER\_SANITIZE\_STRING) και ακολουθείται έλεγχος με regular expressions.

γ) Όπου αναμένεται email, χρησιμοποιείται φίλτρο απολύμανσης για email και φίλτρο επικύρωσης για email.

δ) Όπου αναμένεται αριθμός χρησιμοποιούνται συνθήκες επιτρεπόμενου εύρους τιμών και αποκλεισμός κάθε μη αριθμητικού χαρακτήρα με την συνάρτηση ctype\_digit().

Το σενάριο περιέχει και μια συνάρτηση με την οποία ελέγχεται αν ο χρήστης απάντησε σωστά στο τεστ του reCaptcha για τον διαχωρισμό των ανθρώπων από τα προγράμματα.

Ο πρώτος έλεγχος που γίνεται αφορά το αν κάποιος καλεί το σενάριο validate.php απ’ ευθείας **παρακάμπτοντας την φόρμα report.php**. Αυτό γίνεται με την εισαγωγή ενός κρυμμένου στοιχείου στην φόρμα report.php με όνομα **formsubmitted**. Έτσι στην validate.php ελέγχεται αν στην αίτηση περιέχεται αυτό το κρυμμένο στοιχείο και αν έχει την τιμή που του είχε αποδοθεί. Αν η παραπάνω συνθήκη ικανοποιείται, τότε και μόνο τότε το σενάριο θα προβεί σε περεταίρω ελέγχους και επεξεργασία.

Τέλος το ίδιο το σενάριο **validate.php** εμφανίζει στον χρήστη τα μηνύματα σφαλμάτων ή επιτυχίας της καταχώρησης τους.