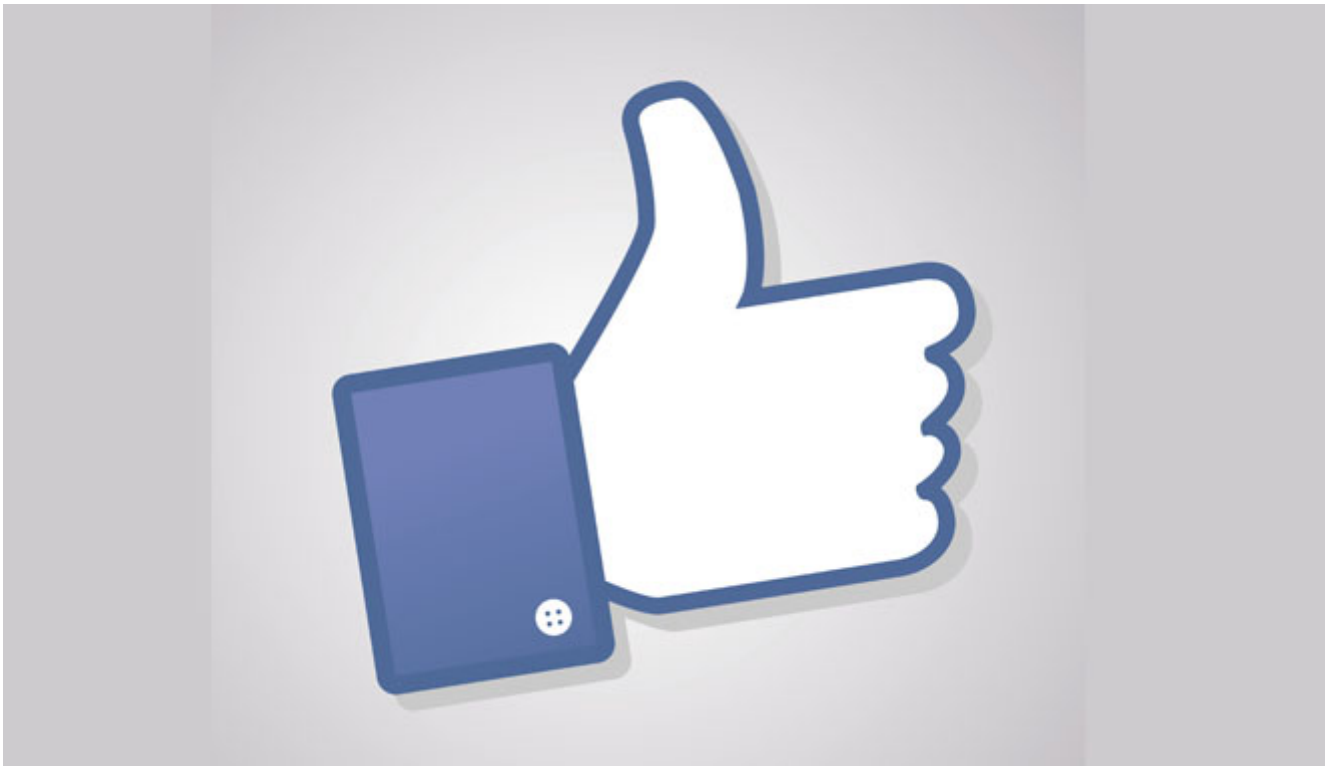
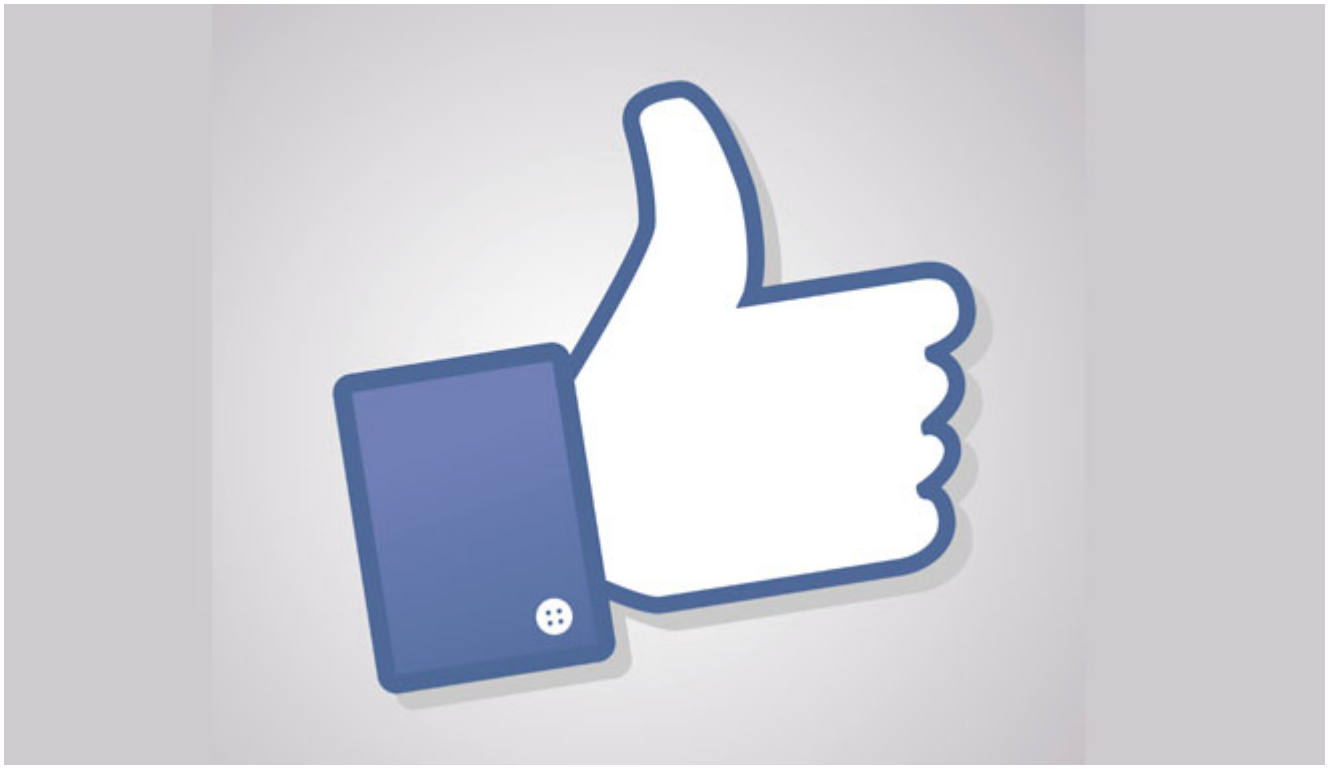
17 Μαρτίου 2016

Facebook: Ποιο ήταν το bug του που σχετιζόταν με την επαναφορά κωδικού;

Επιστήμες / Πληροφορική & Internet





Το Facebook πλήρωσε $15.000 (€ 13.600) σε έναν ανεξάρτητο ερευνητή ασφάλειας, ο οποίος ανακάλυψε έναν απλό τρόπο για την επαναφορά κωδικών πρόσβασης άλλων λογαριασμών, θέτοντας μια νέα συνθηματική

φράση και αποτελεσματικά μπορούσε να πάρει τον έλεγχο άλλων προφίλ.

Ο προγραμματιστής που ανακάλυψε αυτό το ζήτημα και βοήθησε το Facebook να το διορθώσει πριν κακοποιηθεί από κακόβουλους παράγοντες, είναι ο Anand Prakash, ένας ερευνητής ασφάλειας που κατοικεί στην Karnataka, Bangalore στην Ινδία. Όπως ο ίδιος περιγράφει στο blog του, το ζήτημα είναι στην πραγματικότητα μια ασήμαντη επίθεση brute-force στη φόρμα για την ανάκτηση του κωδικού πρόσβασης και όχι στην κεντρική ιστοσελίδα του Facebook, το οποίο προστατεύεται έναντι αυτών των αυτοματοποιημένων τύπων επιθέσεων.

Κάθε φορά που ένας χρήστης ξεχνάει τον κωδικό πρόσβασής του, θα πρέπει να συμπληρώσει μια φόρμα με τη διεύθυνση ηλεκτρονικού ταχυδρομείου του ή τον αριθμό τηλεφώνου, που σχετίζεται με το λογαριασμό του στο Facebook. Μετά την είσοδο ενός από αυτά τα δύο στοιχεία, στέλνεται στον χρήστη ένας εξαψήφιος κωδικός μέσω SMS, τον οποίο θα πρέπει να εισάγει στη φόρμα επαναφοράς κωδικού πρόσβασης για να του επιτραπεί η πρόσβαση σε μια σελίδα όπου μπορεί να αλλάξει τον κωδικό πρόσβασης του λογαριασμού του. Αν κάποιος προσπαθήσει ποτέ να μαντέψει αυτόν τον εξαψήφιο κωδικό για το κεντρικό site του Facebook (facebook.com), θα μπλοκαριστεί από αυτή τη σελίδα μετά από 10 έως 12 άκυρες προσπάθειες.

Ο κύριος Prakash ανακάλυψε ότι αυτό το brute-force όριο προστασίας δεν είναι ενεργό στην beta πλατφόρμα του Facebook, προσβάσιμο στην διεύθυνση beta.facebook.com. Σ’ αυτή την πλατφόρμα δοκιμάζονται, προτού κυκλοφορήσουν στην κύρια πλατφόρμα, τα περισσότερα από τα χαρακτηριστικά του Facebook και η εν λόγω σελίδα την προσφέρει στους χρήστες του, για όποιους επιθυμούν να έχουν πρόσβαση σε περισσότερες νέες λειτουργίες της εταιρείας.

Χρησιμοποιώντας ένα απλό εργαλείο brute-force, ο κύριος Prakash ήταν σε θέση να καταφέρει να εισέλθει στην οθόνη επαναφοράς του κωδικού πρόσβασης όπου χρειάζεται να εισαχθεί ο εξαψήφιος κωδικός.

Μέσω ενός απλού σεναρίου, ο ερευνητής προσπάθησε όλους τους δυνατούς συνδυασμούς μέχρι να μαντέψει το σωστό εξαψήφιο κωδικό. Επειδή η Beta portal του Facebook δεν έχει ρυθμιστεί για να εμποδίσει τους χρήστες οι οποίοι αποτυγχάνουν να εισάγουν τον κατάλληλο κωδικό μετά από 10-12 προσπάθειες, ο ερευνητής ήταν τελικά σε θέση να επαναφέρει τον κωδικό πρόσβασης του δικού του λογαριασμού και θα ήταν και σε θέση να κάνει το ίδιο για οποιονδήποτε άλλο χρήστη. Η μόνη προϋπόθεση θα ήταν για τον εισβολέα να γνωρίζει τον αριθμό τηλεφώνου ή τη διεύθυνση ηλεκτρονικού ταχυδρομείου που σχετίζεται με το λογαριασμό του στόχου.

Ο ερευνητής ανακάλυψε το θέμα στις 22 Φεβρουαρίου, το είπε στο Facebook και η εταιρεία το επιδιόρθωσε την επόμενη ημέρα.

Πηγή: secnews.gr

http://bitly.com/22lBR9S