Αρχικα δημιουργω ενα χρηστη με δικαιωματα ‘secretary’, στο demo μου ο χρηστης αυτος ονομαζεται ‘secretary’ και με password ‘secretary’.

Στη συνεχεια στη καρτελα musicians δημιουργω εναν μουσικο με ονομα ‘θανος’.

Το αποτελεσμα στην παρακατω εικονα ειναι καθως ο secretary αλλαζει το τηλέφωνο του χρηστη Θανου. Ενδεικτικα στο παραδειγμα

χρηστης θανος

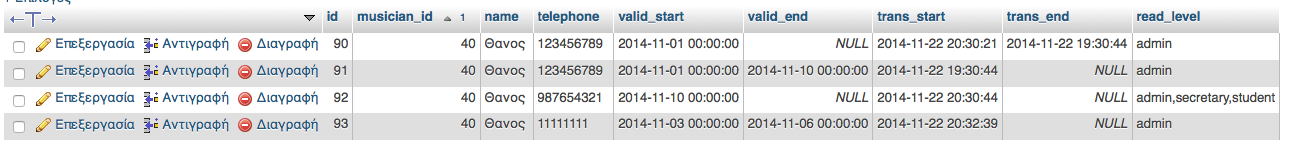
01/11/2014 – 03/11/2014 -> 123456789

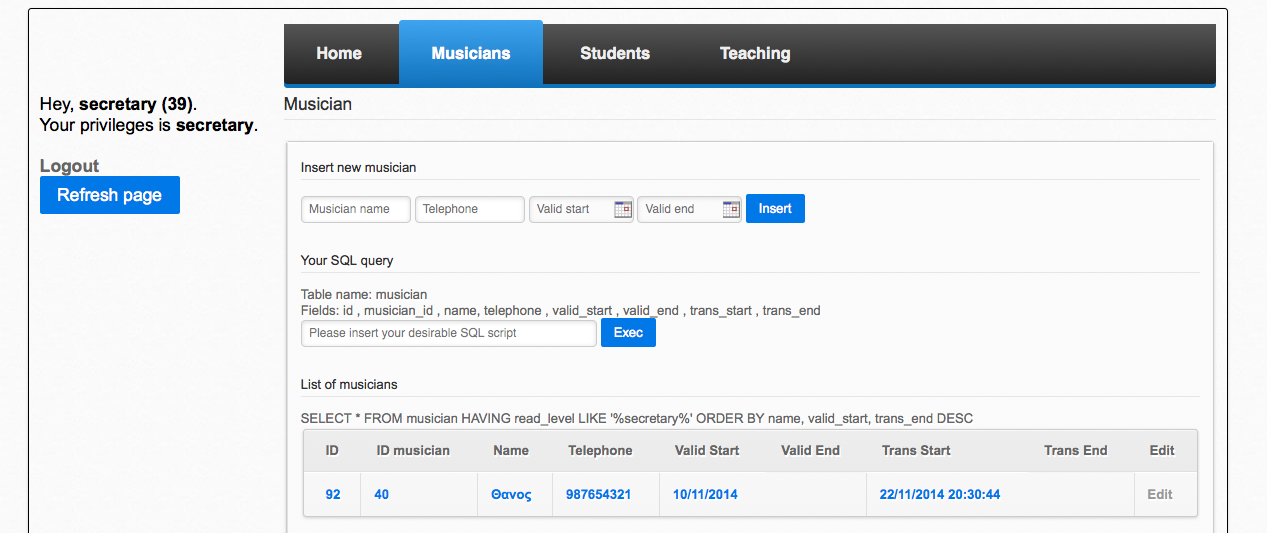
03/11/2014 – 06/11/2014 -> 111111111

06/11/2014 – 10/11/2014 -> 123456789

10/11/2014 – now -> 987654321

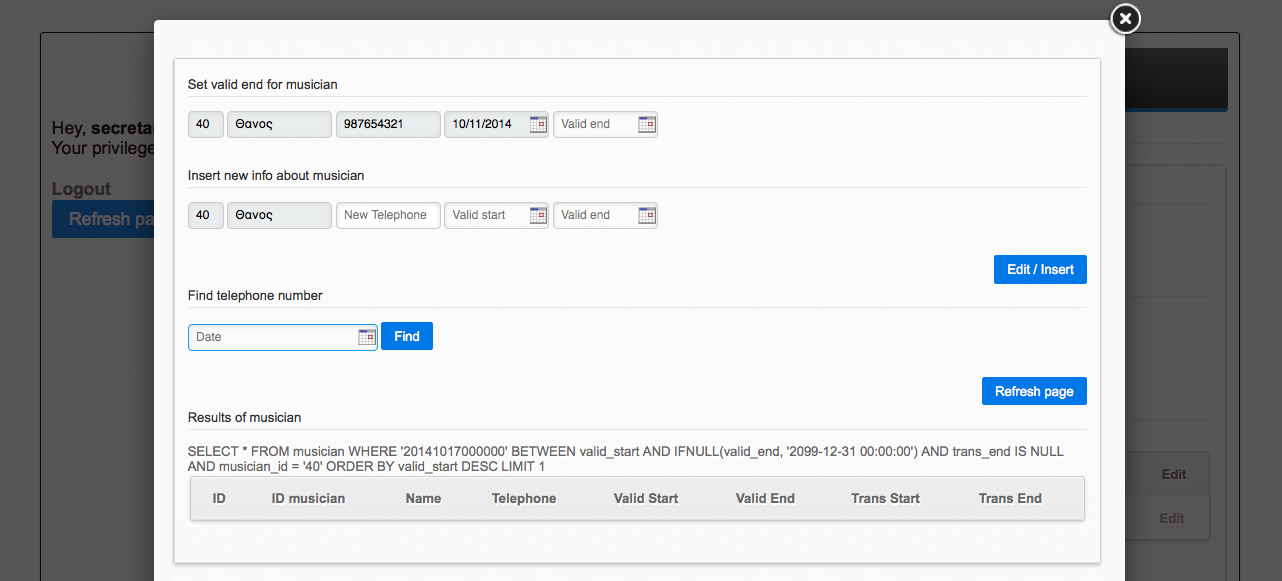
Ετσι οπως φαινεται και απο τους trans χρονους ο αριθμος 111111111 προστεθηκε εμβολημα για καθε ρολους ιστορικου του χρηστη Θανος



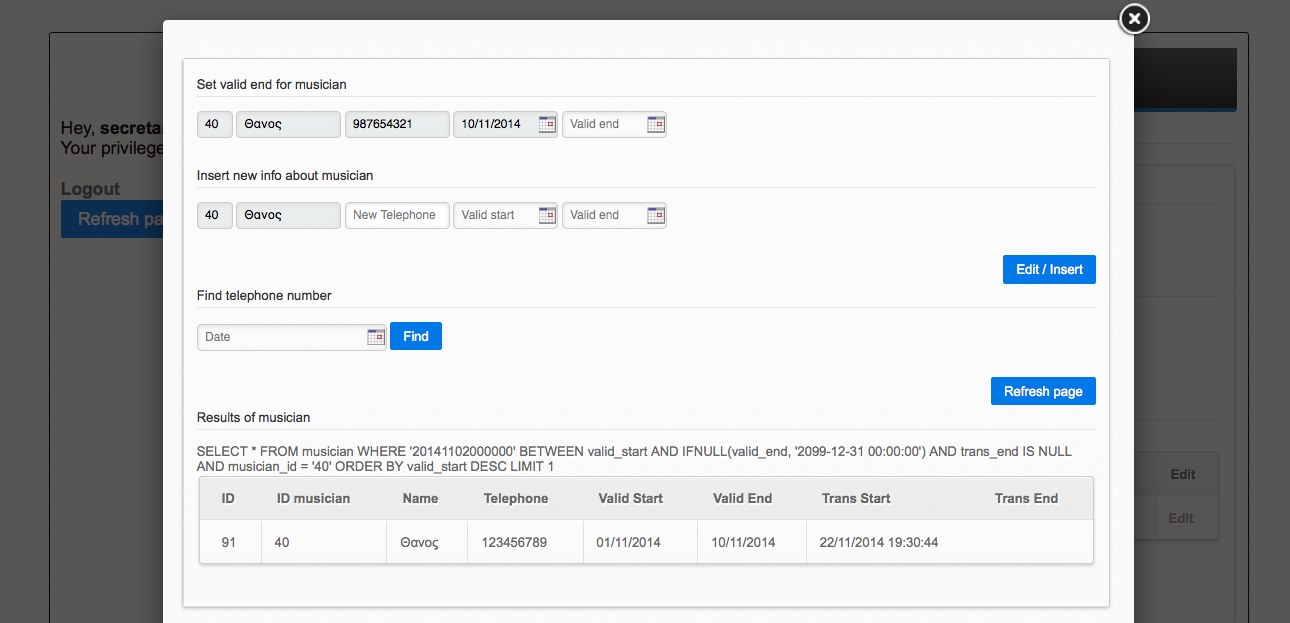
Σαν secretary δικαιωματα ομως ο χρηστης secretary εχει δικαιωμα να δει μονο την τελευταια και ενεργη τιμη τηλεφωνου και οχι το ιστορικο του. 

Για λογους δυνατοτητων ο χρηστης μπορει να κανει αναζητηση στο παρελθον για να δει τι τηλεφωνο ειχε ο χρηστης Θανος στο παρελθον.

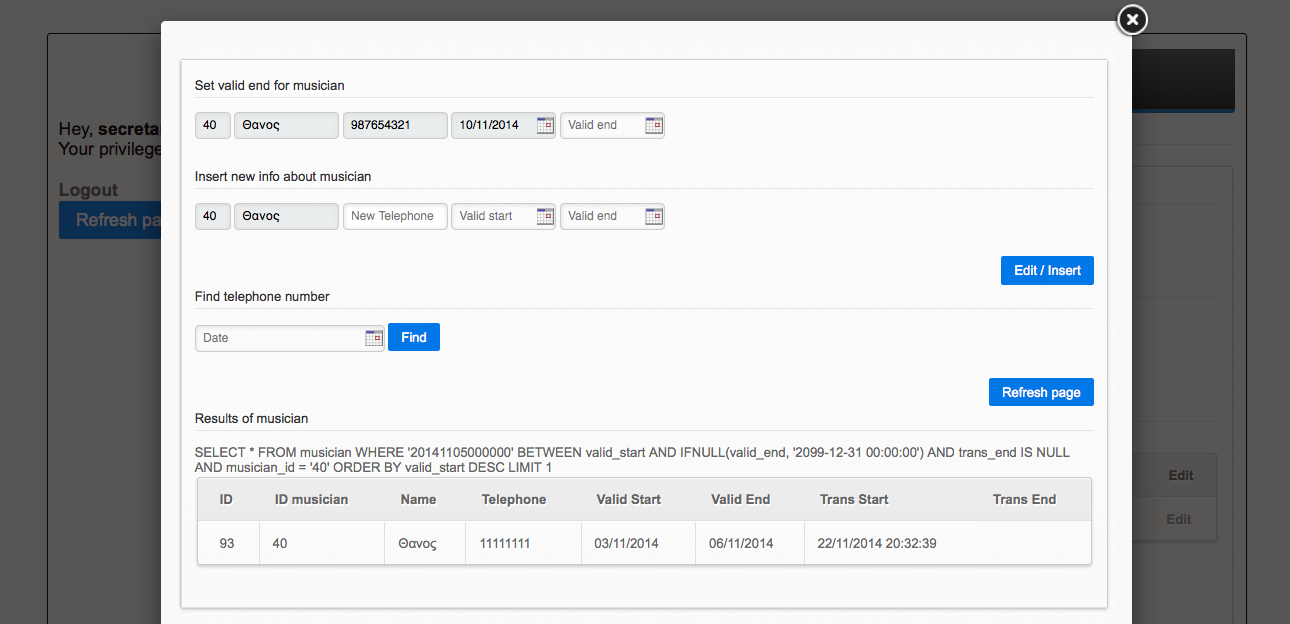
17/10/2014



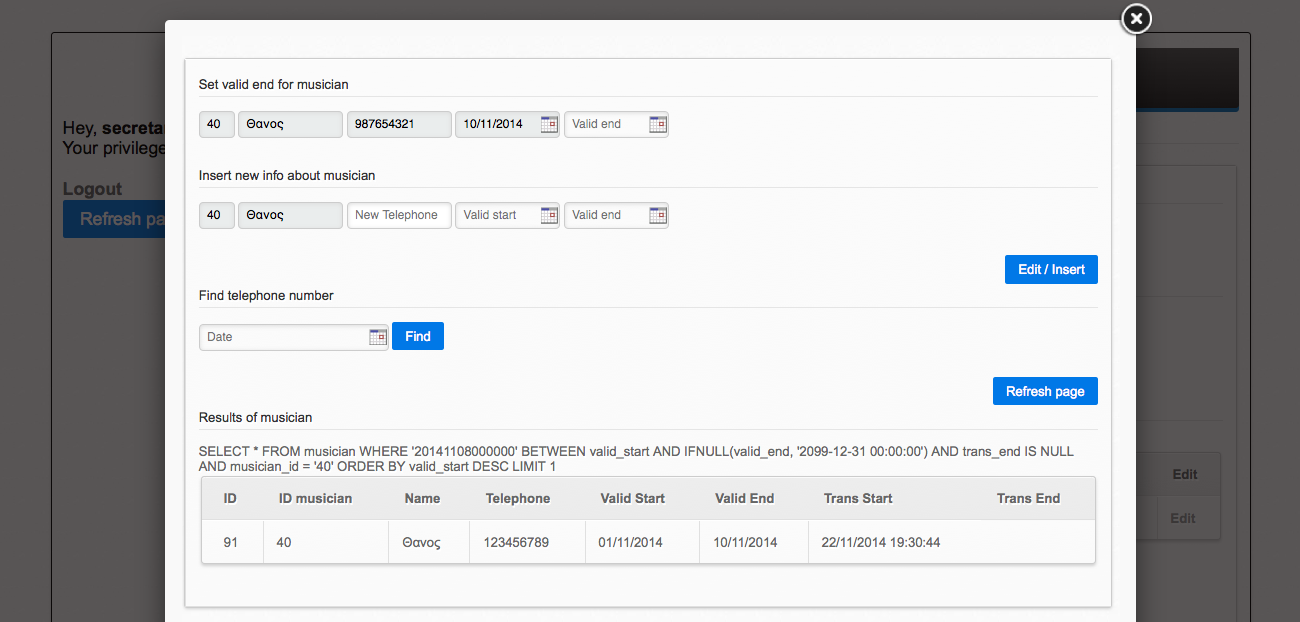
02/11/2014

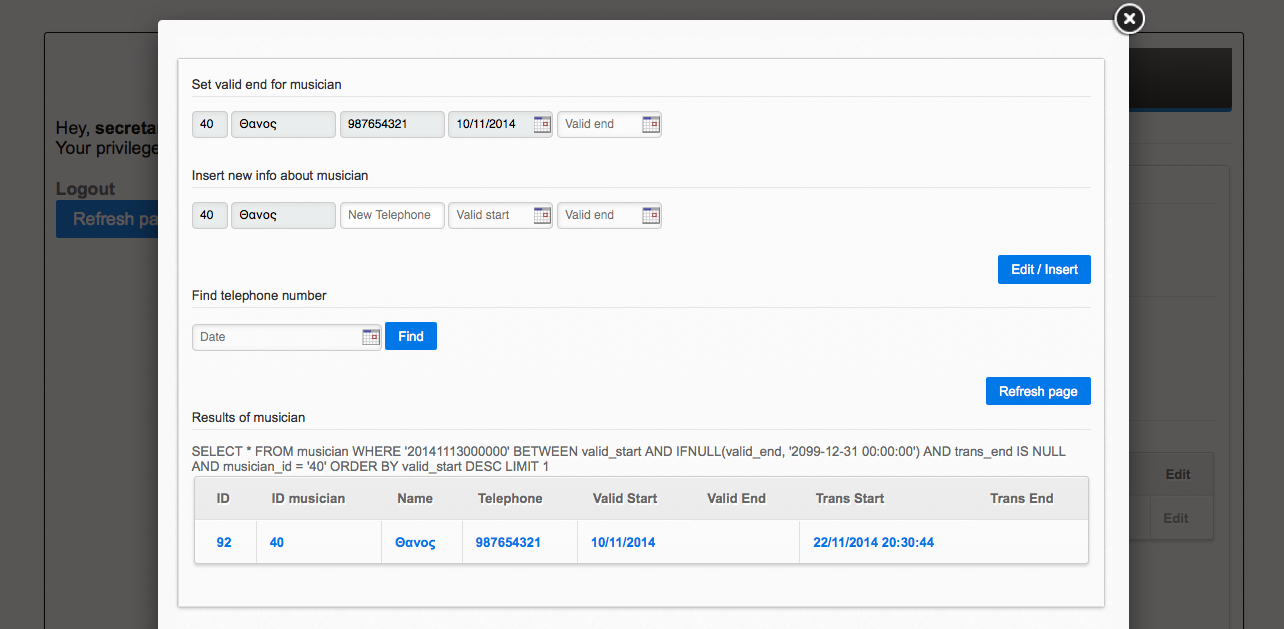


05/11/2014



08/11/2014



30/11/2014

Το ιδιο ισχυει και στην καρτελα students με τις αναλογες αλλαγες στη διευθυνση του καθε μαθητη

Στη συνεχεια προσθετουμε καποιο μουσικο οργανο που θα διδαχθει στο ωδειο. Οσα οργανα εχουν valid end ορισμενοι δε θα εμφανιζονται σαν επιλογη στην καρτελα teaching οπως επισης δε θα εμφανιζονται σε χρηστες με δικαιωματα secretary, musician και student.

Και τελος στην καρτελα teaching μπορουμε να κανουμε την αντιστοιχηση μαθητη, διδασκοντα και μουσικου οργανου με τις ημερομηνιες που θα γινει η παρακολουθηση. Κι εδω η δυνατοτηα πληρης ιστορικης αναφορας γινεται μονο απο admin δικαιωματα.

Απο θεμα ασφαλειας εχω προσθεσει καποιες συναρτησεις για να αποφυγω sql injection οπως

real\_escape\_string()

strip\_tags($variable, ENT\_QUOTES)

επισης χρησιμοποιησα και regular expressions για να αποφυγω τη χρηση καποιων λεξεων οπως select, insert, or

$pattern = '/select|union|insert|delete|or/i';

if(preg\_match($pattern, $variable, $matches, PREG\_OFFSET\_CAPTURE)

Σας επισυναπτω και τα αρχεια απο τα αποτελεσματα του προγραμματος sqlmap πριν και μετα τις προσθηκες ασφαλειας.

Το site ειναι

<http://thanoskeske.zapto.org/biTempMysql/>

Αν δεν μπορειτε να μπειτε τοτε μαλλον ειναwι κλειστος ο υπολογιστης μου. Απλα ενημερωστε με οταν θελετε να το δειτε