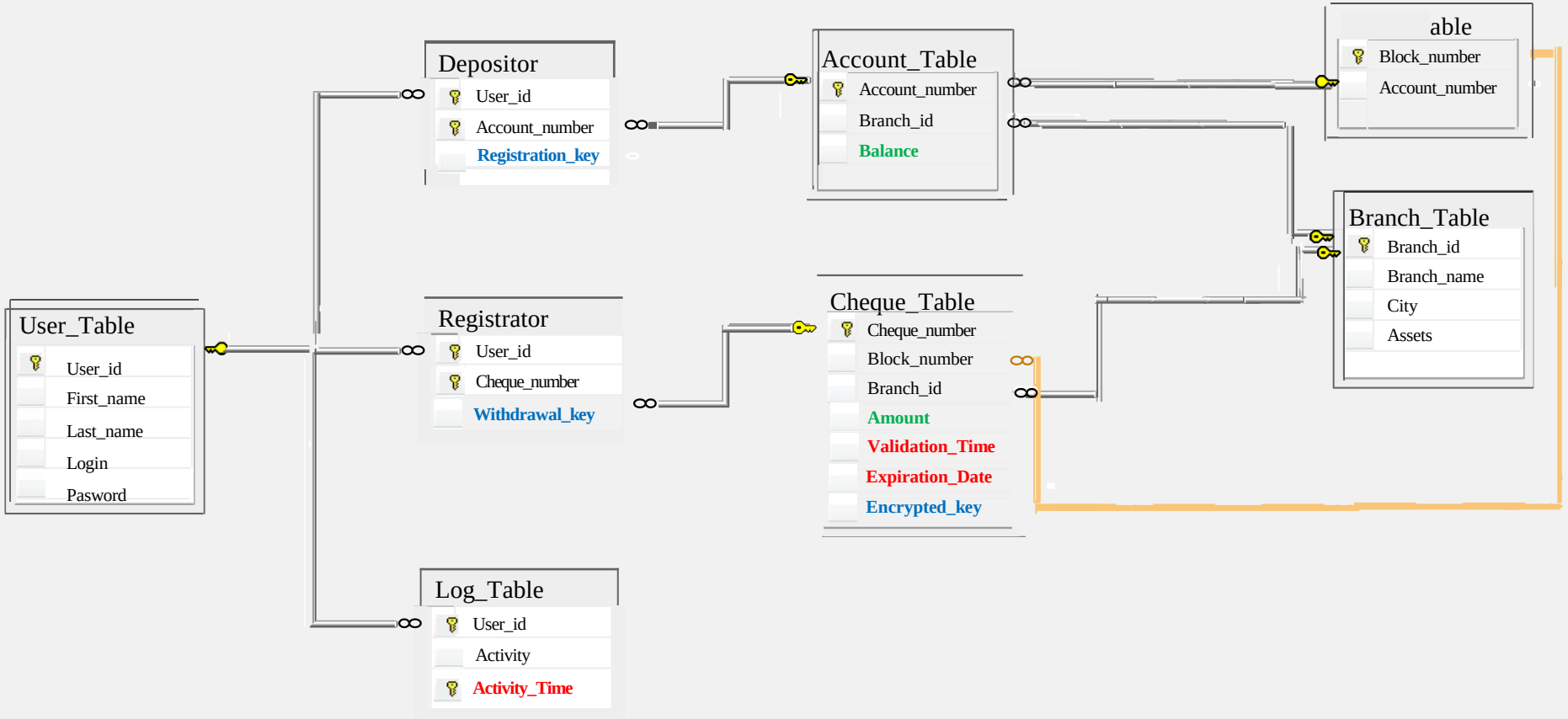
NBG i-bank
#fintech2
crowdhackathon
#NBG #ibank #fintech

StudentVision Team

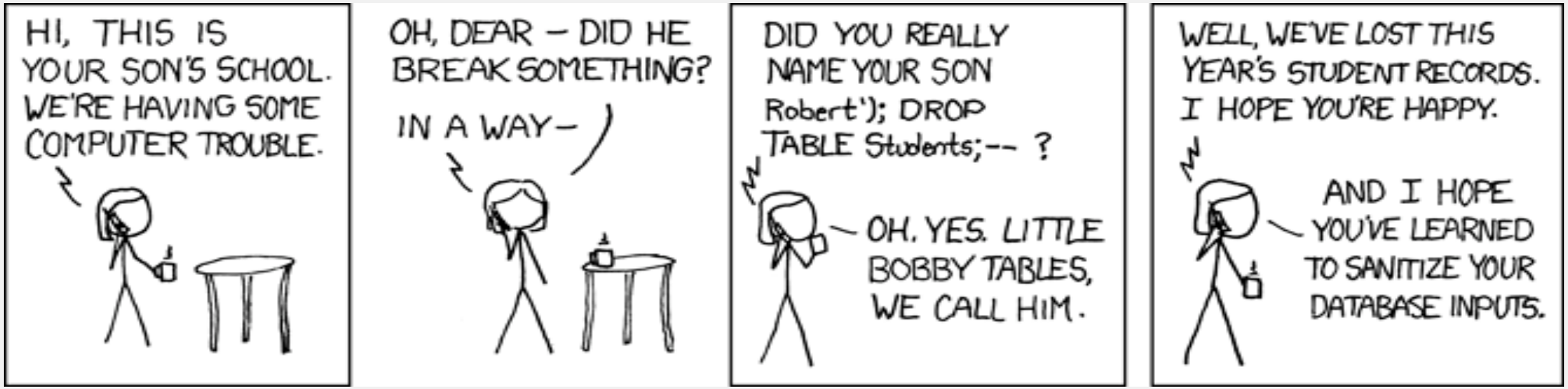
2Ο TEAM MENTORING

ΕΠΙΣΚΟΠΗΣΗ ΛΟΓΙΚΟΥ ΣΧΗΜΑΤΟΣ



ΕΝΕΣΕΙΣ 2 ΕΠΙΠΕΔΩΝ: SQL INJECTION

Ο επιτιθέμενος, ως χρήστης της σελίδας, διαμορφώνει τα δεδομένα που εισάγει με τέτοιο τρόπο ώστε ο διερμηνέας της SQL να τα αντιμετωπίζει ως μέρος της εντολής επερώτησης.



ΕΝΕΣΕΙΣ 2 ΕΠΙΠΕΔΩΝ: SQL INJECTION

- Μια δήλωση Prepare είναι ένα χαρακτηριστικό που χρησιμοποιείται για την εκτέλεση ίδιων (ή παρόμοιων) δηλώσεων SQL επανειλημμένα με υψηλή απόδοση.
- Βήματα:
  1. Δημιουργείται ένα **template SQL statement** και αποστέλλεται στη βάση δεδομένων. Ορισμένες τιμές παραμένουν **απροσδιόριστες**, ονομάζονται παραμέτροι (με την ένδειξη "?"). Παράδειγμα: INSERT INTO table1 VALUES(?, ?, ?).
  2. Η βάση δεδομένων αναλύει, μεταγλωττίζει και εκτελεί βελτιστοποίηση ερωτημάτων στο πρότυπο εντολών SQL και αποθηκεύει το απότέλεσμα χωρίς να το εκτελέσει.
  3. Σε μεταγενέστερο χρόνο, η εφαρμογή δεσμεύει τις τιμές στις παραμέτρους και η βάση δεδομένων εκτελεί τη δήλωση. Η εφαρμογή μπορεί να εκτελέσει τη δήλωση όσες φορές θέλει με διαφορετικές τιμές.

ΕΝΕΣΕΙΣ 2 ΕΠΙΠΕΔΩΝ: SQL INJECTION

Οι προετοιμασμένες δηλώσεις έχουν τρία βασικά πλεονεκτήματα:

1. Οι προετοιμασμένες δηλώσεις **μειώνουν τον χρόνο ανάλυσης** καθώς η προετοιμασία για το ερώτημα γίνεται μόνο μία φορά (αν και η δήλωση εκτελείται πολλές φορές)
2. Οι δεσμευμένες παραμέτρους **ελαχιστοποιούν το εύρος ζώνης στο διακομιστή όπως χρειάζεται**, στέλνουν μόνο τις παραμέτρους κάθε φορά και όχι ολόκληρο το ερώτημα.
3. Οι προετοιμασμένες δηλώσεις **είναι πολύ χρήσιμες σε ενέσεις SQL**, επειδή οι τιμές των παραμέτρων, οι οποίες μεταδίδονται αργότερα χρησιμοποιώντας διαφορετικό πρωτόκολλο, δεν χρειάζεται να διαφεύγουν σωστά. Εάν το αρχικό πρότυπο δήλωσης δεν προέρχεται από εξωτερική είσοδο, δεν είναι δυνατή η εισαγωγή SQL.

ΕΝΕΣΕΙΣ 2 ΕΠΙΠΕΔΩΝ: HTML INJECTION

Έστω η φόρμα "test_form.php".

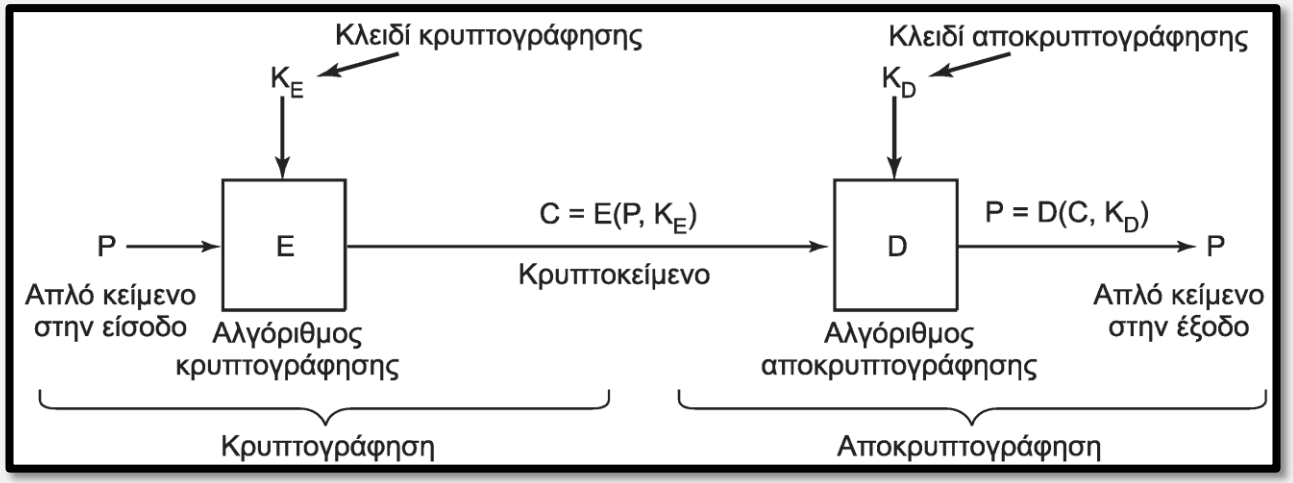
<form method="post" action="<?php echo $_SERVER["PHP_SELF"];?>">

και θεωρήστε ότι ένας χρήστης εισάγει την ακόλουθη διεύθυνσηστη γραμμή διευθύνσεων:
http://www.example.com/test_form.php/%22%3E%3Cscript%3Ealert('hacked')%3C/script%3E, ο παραπάνω κώδικας θα μεταφραστεί ως **<form method="post" action="test_form.php/">**<script>alert('You've been hacked')</script>**.**

ΕΝΕΣΕΙΣ 2 ΕΠΙΠΕΔΩΝ: HTML INJECTION

- Η συνάρτηση **htmlspecialchars ()** μετατρέπει ειδικούς χαρακτήρες σε οντότητες HTML. Αυτό σημαίνει ότι θα αντικαταστήσει χαρακτήρες HTML όπως < *and* > *with < and >*. Αυτό εμποδίζει τους επιτιθέμενους να εκμεταλλευτούν τον κώδικα εισάγοντας κώδικα HTML ή Javascript (επιθέσεις διαδικτυακών σεναρίων) σε φόρμες.
- Στη συνέχεια διαγράφουμε τους περιττούς χαρακτήρες (επιπλέον χώρο, καρτέλα, νέα γραμμή) από τα δεδομένα εισόδου του χρήστη (με τη συνάρτηση της PHP **trim ()**) και αφαιρούμε τα backslashes (\) από τα δεδομένα εισόδου (με τη μέθοδο της PHP **stripslashes ()**). Θα ομαδοποιήσουμε αυτά και θα ονομάσουμε τη λειτουργία **test_input ().**
- ***Goals:*** Επικύρωση δεδομένων εισόδου (validation), sanitization αυτών και escape χαρακτήρων με χρήση των functions **htmlspecialchars()** ή **htmlentities(),** Regular Expressions, Template engine ή frameworks που υποστηρίζουν αυτόματο escape χαρακτήρων κειμένου.

ΒΑΣΙΚΟ ΜΟΝΤΕΛΟ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ



Δομή συστημάτων κρυπτογραφίας

- Έστω με βάση το σχήμα P το απλό κείμενο και C το κρυπτοκείμενο, E/D οι αλγόριθμοι (απο)κρυπτογράφησης, K_E/K_D τα κλειδιά (απο)κρυπτογράφησης.
- Ισχύουν οι εξαρτήσεις: $C=E(P,K_E)$ και $P=D(C,K_D)$

ΥΛΟΠΟΙΗΣΗ ΚΩΔΙΚΑ: GITHUB ACCOUNT

```php
if (!isset($_POST["passwd"])) {
    $loginErr = "Απαιτείται κωδικός.";
} else {
    $login = test_input($_POST["passwd"]);
    // check if name only contains letters and whitespace
    if (!preg_match("/^[a-zA-Z ]*$/",$login)) /* regular expression*/{
        $nameErr = "Only letters and white space allowed";
    }
}

if (!isset($_POST["passwd_1"])) {
    $passErr = "Απαιτείται μυστικός κωδικός.";
} else {
    $pass = test_input($_POST["passwd_1"]);
}

function test_input($data) {
    $data = trim($data);
    $data = stripslashes($data);
    $data = htmlspecialchars($data);
    return $data;
}
```

```php
// sql to identify user
$stmt = $conn->prepare("SELECT User_id FROM User_Table WHERE User_id LIKE ? AND Pasword LIKE ?");
$stmt->bind_param("ss", $login, $pass);
$stmt->execute();
$stmt->bind_result($user);
```

ANY (SQL) QUERIES?

StudentVision

Team

Αθήνα, 21 Οκτωβρίου 2017