ΠΑΝΕΠΙΣΤΗΜΙΟ
ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
UNIVERSITY OF WEST ATTICA

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ
ΠΛΗΡΟΦΟΡΙΚΗΣ & ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΑΝΙΧΝΕΥΣΗ ΑΠΟ ΕΠΙΘΕΣΕΙΣ ΤΥΠΟΥ SQL INJECTION

ΠΑΝΑΓΙΩΤΟΠΟΥΛΟΣ ΕΥΑΓΓΕΛΟΣ

ΕΠΙΒΛΕΠΟΥΣΑ ΚΑΘΗΓΗΤΡΙΑ: ΚΑΝΤΖΑΒΕΛΟΥ ΙΩΑΝΝΑ

ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ

01

- Τι είναι μία Βάση Δεδομένων
- Επικοινωνία Βάσης με Ιστότοπο
- Αναφορά σε Διαδικτυακές Επιθέσεις

SQL INJECTION

02

- Τι είναι / Τρόποι Επίθεσης
- Κατηγορίες SQLI

ΠΡΟΣΤΑΣΙΑ ΑΠΟ SQLI

03

- Τρόποι Προστασίας

ΑΝΙΧΝΕΥΣΗ SQLI

04

- Μέθοδοι Ανίχνευσης

ΕΡΓΑΛΕΙΟ ΑΝΙΧΝΕΥΣΗΣ SQLI

05

- Πως Λειτουργεί / Που Εστιάζει

ΣΥΜΠΕΡΑΣΜΑΤΑ

06

- Γιατί είναι τόσο σημαντική η SQLI;

01 ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ

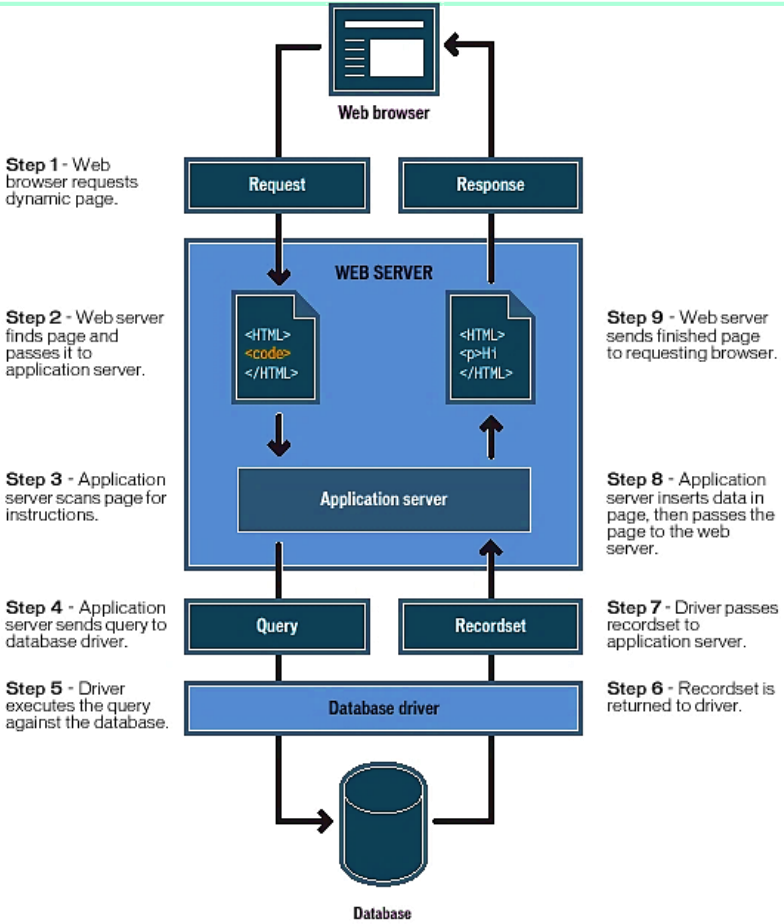
- Τι είναι μία Βάση Δεδομένων SQL
- Επικοινωνία Βάσης με Ιστότοπο
- Αναφορά σε Διαδικτυακές Επιθέσεις

01 ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ

Τι είναι μία Βάση Δεδομένων SQL;

Η SQL (Structured Query Language) :

- Είναι γλώσσα προγραμματισμού υψηλού επιπέδου
- Αποτελείται από δηλωτικά στοιχεία (ερωτήματα)
- Διαχειρίζεται δεδομένα μιας σχεσιακής ΒΔ (RDBMS = Relational Database Management System)
- Επεξεργάζεται την ροή μιας σχεσιακής ΒΔ (RDSMS = Relational Data Stream Management System).



01 ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ

Οι πιο συνηθισμένες επιθέσεις στον κυβερνοχώρο

- **Malware :**
  Κακόβουλο λογισμικό (ιοί, spyware κτλπ)
- **DoS & DDoS:**
  Αμέτρητα αιτήματα -> Εξάντληση πόρων
- **SQL Injection:**
  Κακόβουλος κώδικας -> Απόκτηση ελέγχου ΒΔ
- **Man-in-the-middle:**
  Εισβολή στην επικοινωνία άλλων ατόμων
- **Phishing:**
  Δόλια μηνύματα / Email

02 SQL INJECTION

- Τι είναι
- Τρόποι Επίθεσης
- Κατηγορίες SQLI

02 SQL INJECTION

Τι είναι το SQL Injection;

- Είναι η ευπάθεια που προκύπτει όταν δίνεται η δυνατότητα σε εναν εισβολέα να επηρεάσει τα ερωτήματα SQL προς την βάση δεδομένων.
- Δυνατότητα τροποποίησης δεδομένων.
- Παρακάμπτεται η διαδικασία ταυτοποίησης του χρήστη και αποκτιέται εξουσιοδότηση στην ιστοσελίδα -> Πλήρης έλεγχος της ΒΔ.
- Ο κακόβουλος κώδικας εισάγεται στα πεδία που παρέχονται στον χρήστη.

Υπάρχουν 4 τρόποι επίθεσης SQLI και αυτοί είναι:

Χειραγώγηση της SQL (SQL Manipulation)

Έγχυση κώδικα (Code Injection)

Έγχυση κλήσης συνάρτησης (Function Call Injection)

Υπερχείλιση του Buffer (Buffer Overflow)

02 SQL INJECTION

Κατηγορίες SQL Injection

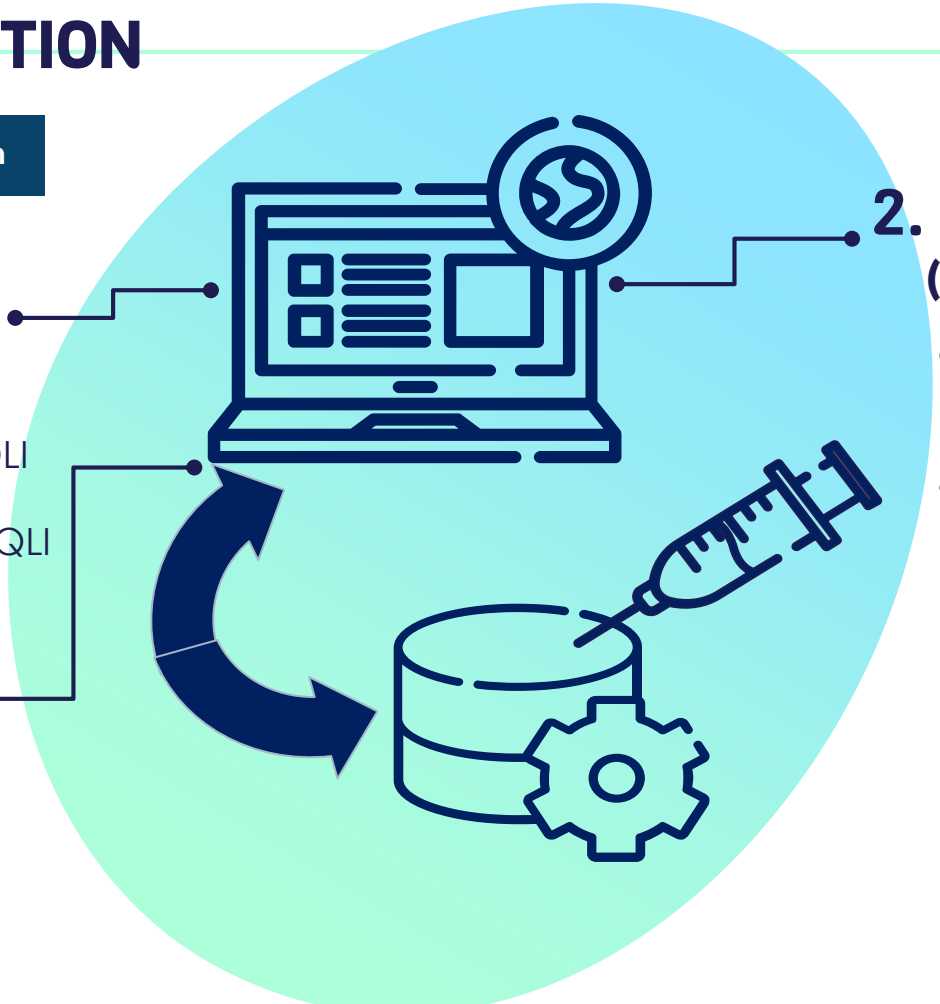
1. In-Band SQLI (Classic SQLI)

- Error-Based SQLI
- Union-Based SQLI

2. Inferential SQLI (Blind SQLI)

- Blind Boolean-based SQLI
- Time-based Blind SQLI

3. Out-Of-Band SQLI



02 SQL INJECTION

Παράδειγμα SQL Injection

127.0.0.1/dvwa/vulnerabilities/sqli/

User ID: 1 Submit

```
ID: 1
First name: admin
Surname: admin
```

127.0.0.1/dvwa/vulnerabilities/sqli/?id=1'&Submit=Submit#

127.0.0.1/dvwa/vulnerabilities/sqli/?id=1' order by 3--+&Submit=Submit#

127.0.0.1/dvwa/vulnerabilities/sqli/?id=1'union select database(),version()--+&Submit=Submit#

```
ID: 1'union select database(),version()--
First name: admin
Surname: admin

ID: 1'union select database(),version()--
First name: dvwa
Surname: 5.7.19-0ubuntu0.16.04.1
```

1 2 3 4 5 6 7 8 ...

```
You have an error in your SQL syntax; check the manual that corresponds
to your MySQL server version for the right syntax to use near ''1''' at line 1
```

127.0.0.1/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#

```
Unknown column '3' in 'order clause'
```

127.0.0.1/dvwa/vulnerabilities/sqli/?id=1'union select 'abc',table_name from information_schema.tables --+&Submit=Submit#

```
ID: 1'union select 'abc',table_name from information_schema.tables --
First name: abc
Surname: guestbook

ID: 1'union select 'abc',table_name from information_schema.tables --
First name: abc
Surname: users

ID: 1'union select 'abc',table_name from information_schema.tables --
First name: abc
Surname: elgg_csrfaccess_collection_membership
```

03

ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΕΠΙΘΕΣΕΙΣ SQLI

- Τρόποι Προστασίας

03 ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΕΠΙΘΕΣΕΙΣ SQLI

01
ΧΡΗΣΗ ΠΑΡΑΜΕΤΡΟΠΟΙΗΜΕΝΩΝ ΕΡΩΤΗΜΑΤΩΝ
(Parameterized Queries)

- Προ-μεταγλώττιση ενός ερωτήματος SQL

02
ΧΡΗΣΗ ΑΠΟΘΗΚΕΥΜΕΝΩΝ ΔΙΑΔΙΚΑΣΙΩΝ
(Stored Procedures)

- Ο κώδικας της καθορίζεται και παραμένει στην ίδια την ΒΔ

03
ΕΠΙΚΥΡΩΣΗ ΤΥΠΟΥ ΔΕΔΟΜΕΝΩΝ ΕΙΣΟΔΟΥ
(Input Data Type Validation)
& ΕΛΕΓΧΟΣ ΜΗΚΟΥΣ ΜΕΤΑΒΛΗΤΩΝ ΕΙΣΟΔΟΥ
(Input Variable Length Checking)

- Ανάθεση τύπου δεδομένων σύμφωνα με τις ανάγκες & περιορισμός μήκους χαρακτήρων

04
ΔΗΜΙΟΥΡΓΙΑ ΛΙΣΤΑΣ ΕΠΙΤΡΕΠΟΜΕΝΩΝ ΜΕΤΑΒΛΗΤΩΝ
(White List Filtering)

- Φιλτράρισμα όλων των πεδίων

05
ΔΗΜΙΟΥΡΓΙΑ ΛΙΣΤΑΣ ΑΠΑΓΟΡΕΥΜΕΝΩΝ ΜΕΤΑΒΛΗΤΩΝ
(Black List Filtering)

- Αποτροπή χρησιμοποίησης συγκεκριμένων εντολών & συμβόλων

06
ΑΠΟΜΟΝΩΣΗ ΔΕΔΟΜΕΝΩΝ ΠΟΥ ΕΙΣΑΓΕΙ Ο ΧΡΗΣΤΗΣ
(Escaping Input)

- Φιλτράρισμα χαρακτήρων

03 ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΕΠΙΘΕΣΕΙΣ SQLI

07
ΑΠΟΦΥΓΗ ΔΙΑΧΕΙΡΙΣΤΙΚΩΝ ΠΡΟΝΟΜΙΩΝ
(Avoiding Administrative Privileges)

- Αποφυγή σύνδεσης Admin στην ΒΔ

08
ΑΡΧΗ ΤΟΥ ΛΙΓΟΤΕΡΟ ΠΡΟΝΟΜΙΟΥΧΟΥ
(Principle of Least Privilege)

- Σωστή κατανομή προνομίων στους χρήστες

09
ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΚΩΔΙΚΩΝ ΠΡΟΣΒΑΣΗΣ
(Password hashing)

- Κρυπτογράφηση κωδικών τύπου SHA-2

10
ΤΕΙΧΟΣ ΠΡΟΣΤΑΣΙΑΣ ΙΣΤΟΣΕΛΙΔΑΣ
(Website Firewall)

- Έλεγχος σε πραγματικό χρόνο

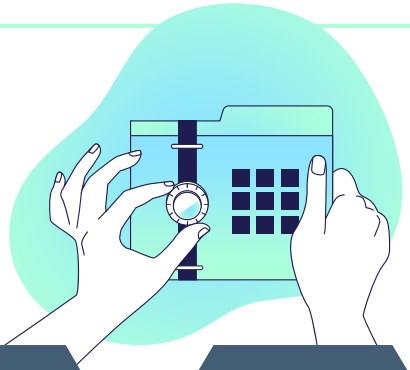
04

ΑΝΙΧΝΕΥΣΗ SQLI

- Μέθοδοι Ανίχνευσης

04 ΑΝΙΧΝΕΥΣΗ SQLI

Μέθοδοι ανίχνευσης



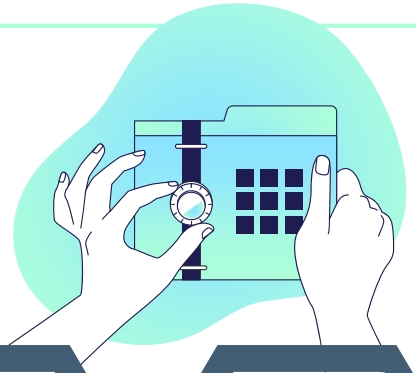
1. Χειροκίνητο **Penetration Test**

- Δημιουργία ερωτημάτων για κάθε είδος επίθεσης
- Εφαρμογή σε όλα τα πεδία που εισάγει πληροφορία ο χρήστης (url, login form)

04 ΑΝΙΧΝΕΥΣΗ SQLI

Μέθοδοι ανίχνευσης

- **SQLMap** (ανοιχτού κώδικα, ανίχνευση όλων των ειδών επιθέσεων)
- **BSQL Hacker** (ειδίκευση σε Blind SQLI)

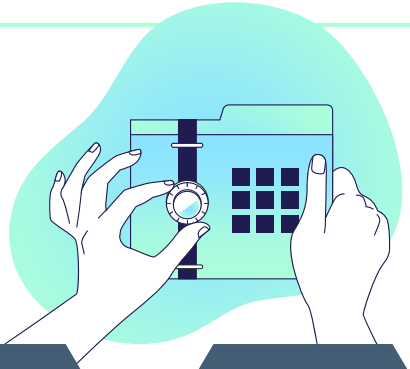


1. Χειροκίνητο **Penetration Test**

2. Αυτοματοποιημένο **Penetration Test**

04 ΑΝΙΧΝΕΥΣΗ SQLI

Μέθοδοι ανίχνευσης

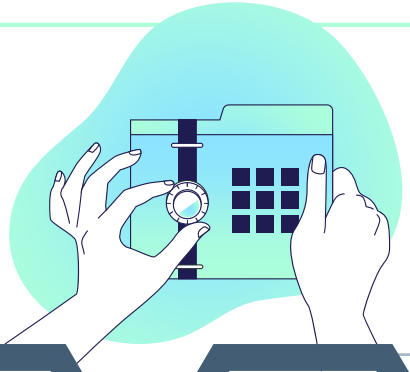


1. Χειροκίνητο **Penetration Test**
2. Αυτοματο-ποιημένο **Penetration Test**
3. Έλεγχος του αρχείου καταγραφέα σφαλμάτων

•Ενεργοποίηση -> extended events (sqlserver.error_reported)
•Ιδιαίτερη προσοχή στα ακόλουθα errors:
> Error 18456 (Αποτυχημένο login)
> Error 245 (Έκδοση Βάσης)
> Error 205 (Union) και άλλα...

04 ΑΝΙΧΝΕΥΣΗ SQLI

Μέθοδοι ανίχνευσης



1. Χειροκίνητο **Penetration Test**
2. Αυτοματο-ποιημένο **Penetration Test**
3. Έλεγχος του αρχείου καταγραφέα σφαλμάτων
4. Επανέλεγχος του πηγαίου κώδικα

- Στατικός
  (Χωρίς την εκτέλεση του κώδικα)
- Δυναμικός
  (Με την εκτέλεση του κώδικα)

Πραγματοποιείται Χειροκίνητα

- Δημιουργία μικρών script –> Τμηματική ανάλυση κώδικα

ή Αυτοματοποιημένα

- Veracode -> Σχεδόν όλες τις γλώσσες προγραμματισμού & Αναλαμβάνει όλη την ανάλυση του κώδικα στατική & δυναμική

05 ΕΡΓΑΛΕΙΟ ΑΝΙΧΝΕΥΣΗΣ SQLI

- Πως Λειτουργεί / Που Εστιάζει

05 ΕΡΓΑΛΕΙΟ ΑΝΙΧΝΕΥΣΗΣ SQLI

Λεπτομέρειες του εργαλείου

ΓΛΩΣΣΑ

Python

Γρήγορη & Αξιόπιστη

In-Band SQLI

Error-based
SQLI

ΚΑΤΗΓΟΡΙΑ

ΕΥΕΛΙΞΙΑ

Προσαρμοστικότητα

Εξωτερικά αρχεία
text

05 ΕΡΓΑΛΕΙΟ ΑΝΙΧΝΕΥΣΗΣ SQLI

Πώς λειτουργεί;

Function 1

Εξαγωγή διαθέσιμων φορμών ιστοσελίδας (login form, search box κτλπ)

Function 2

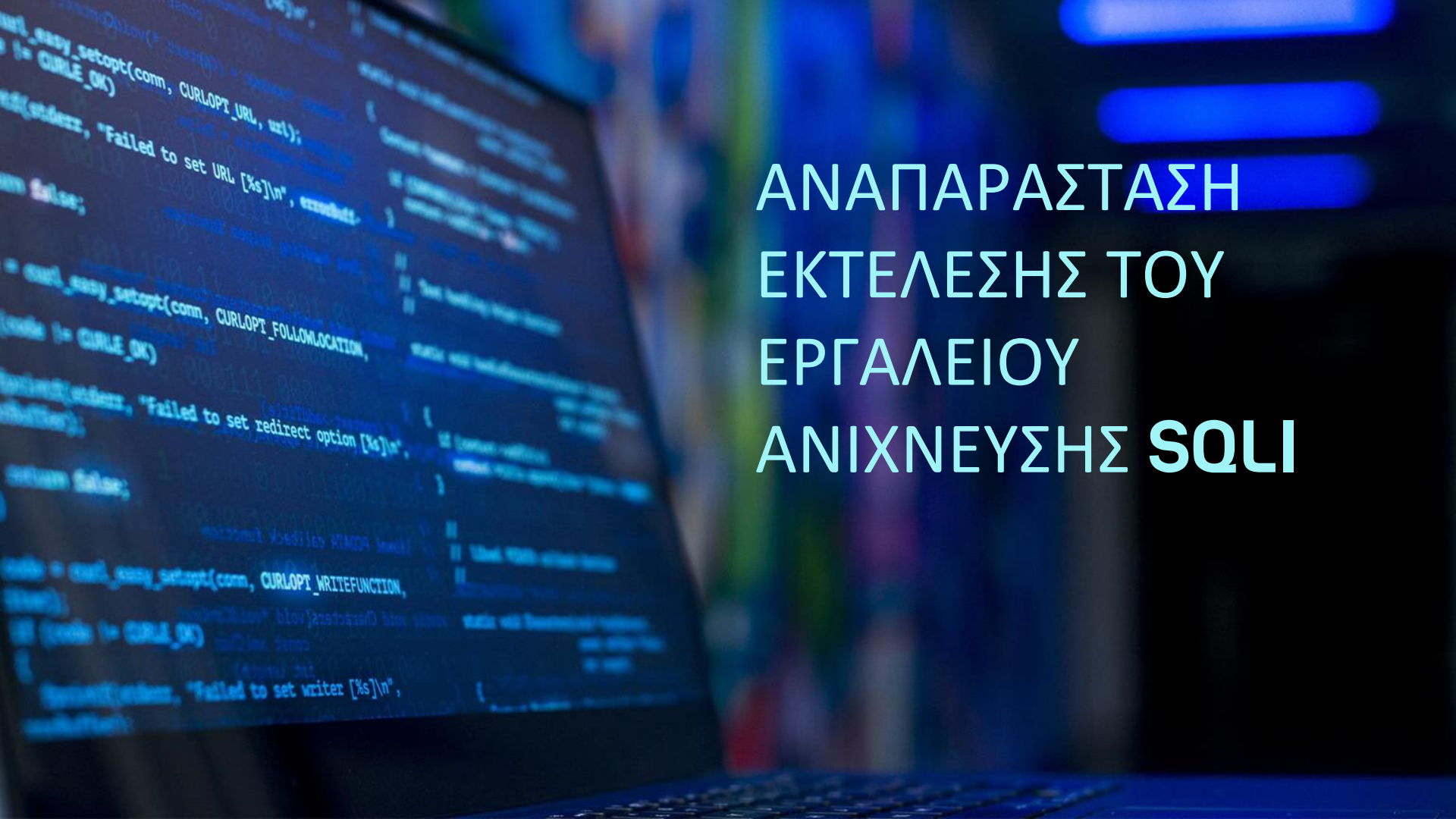
Περαιτέρω πληροφορίες για τις διαθέσιμες φόρμες

Function 3

Έλεγχος ευπάθειας ιστοσελίδας με βάση την ανταπόκρισή της

Συνδυασμός των παραπάνω functions καταλήγοντας σε συμπέρασμα αν η υπό εξέταση ιστοσελίδα είναι ευάλωτη σε SQLI

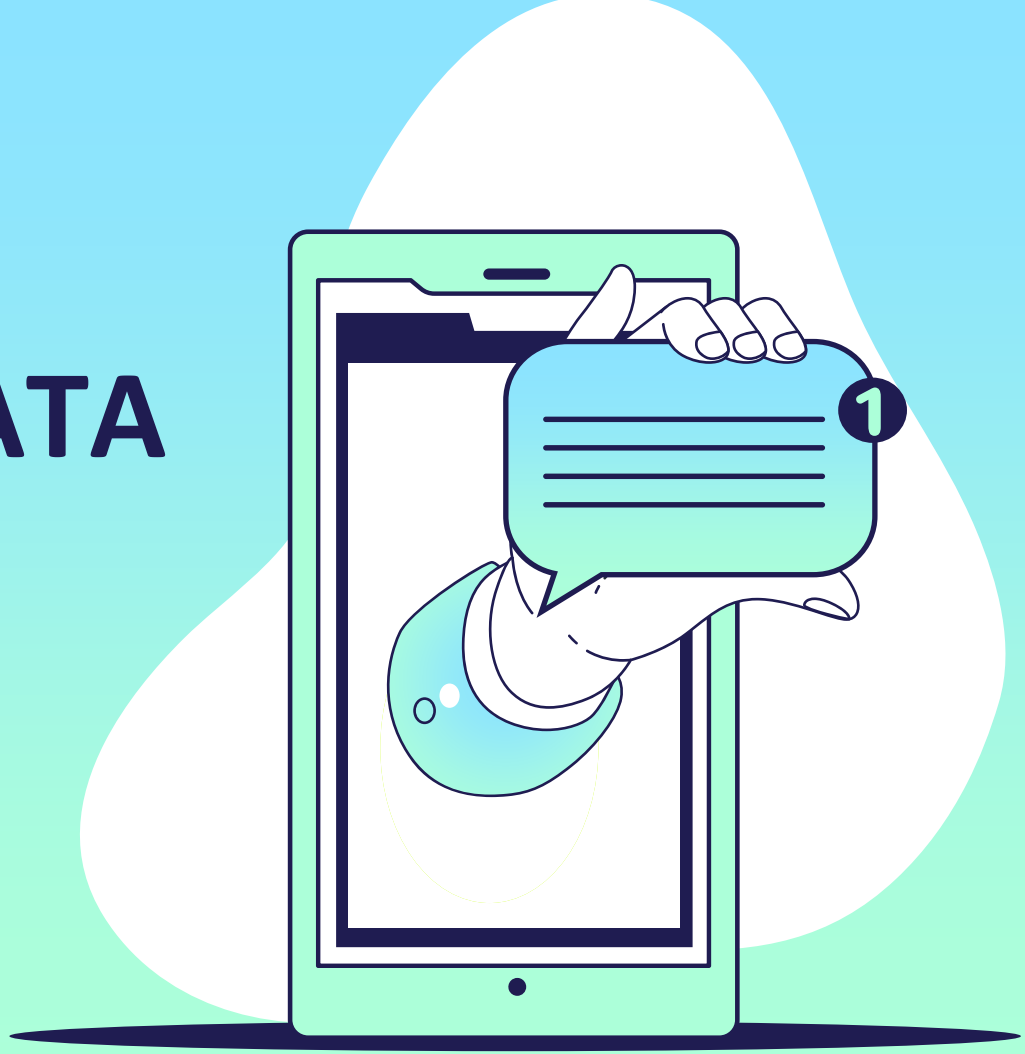
Function 4


ΑΝΑΠΑΡΑΣΤΑΣΗ
ΕΚΤΕΛΕΣΗΣ ΤΟΥ
ΕΡΓΑΛΕΙΟΥ
ΑΝΙΧΝΕΥΣΗΣ SQLI

06

ΣΥΜΠΕΡΑΣΜΑΤΑ

- Γιατί είναι τόσο σημαντική η SQLI;



06 ΣΥΜΠΕΡΑΣΜΑΤΑ

Ενημέρωση προγρ/στών για τους κινδύνους

Ασφαλής ανάπτυξη ιστοσελίδας & Βάσης Δεδομένων

Παρακολού-θηση & συντήρηση Βάσης Δεδομένων

Πολλαπλά επίπεδα προστασίας

06 ΣΥΜΠΕΡΑΣΜΑΤΑ

Γιατί επιλέχθηκε αυτή η επίθεση προς ανάλυση;

Διότι, στατιστικές έρευνες και εταιρείες διαδικτυακής προστασίας την κατατάσσουν στις κορυφαίες επιθέσεις τόσο σε πλήθος όσο και σε κρισιμότητα και επίπεδο επικινδυνότητας. Τα τελευταία χρόνια έχει ανοδική τάση στις επιτυχημένες επιθέσεις

06 ΣΥΜΠΕΡΑΣΜΑΤΑ

Τι διαφέρει το εργαλείο που αναπτύχθηκε στην διπλωματική σε σχέση με τα ήδη υπάρχοντα;

Είναι εύκολο στην χρήση, δεν χρειάζεται πολλούς πόρους οπότε είναι ‘ελαφρύ’, ειδικεύεται σε error-based SQLI αλλά είναι και ευέλικτο να προσαρμοστεί και για τις άλλες κατηγορίες

ΕΥΧΑΡΙΣΤΩ ΠΟΛΥ ΓΙΑ ΤΟΝ ΧΡΟΝΟ ΣΑΣ!