# WDA Project - Hotel - v3.2

## Τίτλος

Web εφαρμογή αναζήτησης καταλυμάτων

## Περιγραφή

Το παρόν έγγραφο περιγράφει τις λειτουργικές απαιτήσεις για την αναβάθμιση του [Hotel Project v3.1](https://docs.google.com/document/d/10GnBmNQaxS4YdByGoOQwxB2dbuoDumuPr59_hWmOLQk/edit#) που αναπτύχθηκε με σκοπό την θωράκιση της εφαρμογής εναντίων γνωστές επιθέσεις.

Το έγγραφο χωρίζεται στις εξής ενότητες:

* Λειτουργικές απαιτήσεις

## Λειτουργικές Απαιτήσεις

Οι λειτουργικές απαιτήσεις που αναφέρονται σε αυτό το έγγραφο είναι επέκταση των απαιτήσεων που είχαν οριστεί στο v3.1.

### Γενικές Απαιτήσεις

#### CSRF Protection

Σύμφωνα με το [CSRF](https://owasp.org/www-community/attacks/csrf) θα πρέπει η εφαρμογή να προστατεύεται από requests που μπορεί να πραγματοποιηθούν από άλλα sites, εκμεταλλευόμενη τα cookies που αποθηκεύονται.

Η συγκεκριμένη προστασία θα πρέπει να εφαρμόζεται σε κάθε φόρμα που κατά το submit πραγματοποιεί ένα POST request.

#### XSS Protection

Σύμφωνα με το [XSS](https://owasp.org/www-community/attacks/xss/) θα πρέπει η εφαρμογή να προστατεύεται από περιεχόμενο το οποίο μπορεί να προέρχεται από τον χρήστη, π.χ. κριτικές χρηστών.

Η συγκεκριμένη προστασία θα πρέπει να εφαρμόζεται σε όλα τα σημεία στα οποία προβάλλεται πληροφορία που προέρχεται από user input.

#### SQL Injection

Σύμφωνα με το [SQL Injection](https://owasp.org/www-community/attacks/SQL_Injection) θα πρέπει η εφαρμογή να προστατεύεται από κακόβουλα δεδομένα κατά την επικοινωνία με την βάση δεδομένων.

Η συγκεκριμένη προστασία θα πρέπει να εφαρμόζεται σε όλα τα σημεία στα οποία γίνεται επικοινωνία με την βάση δεδομένων, με την χρήση παραμέτρων.

### Ανά Σελίδα

Οι παρακάτω λειτουργικές απαιτήσεις χωρίζονται ανά σελίδα.

#### Αναζήτηση δωματίου

* Κατά την αναζήτηση του δωματίου δεν χρειάζεται κάποια προστασία ενάντια στο CSRF καθώς η συγκεκριμένη φόρμα θα είναι GET

#### Πληροφορίες Δωματίου

* Κατά την εμφάνιση των αξιολογήσεων δωματίου, θα πρέπει να γίνεται έλεγχος ενάντια στις επιθέσεις XSS ως προς το κείμενο της αξιολόγησης