|  |  |  |
| --- | --- | --- |
| Τίτλος Έργου | : | TRIAN.GR v1 |
|  | | |
| Υπεύθυνος Έργου | : | Δημήτρης Βαϊνανίδης |
|  | | |
| Υπεύθυνος Ελέγχου | : | Κώστας Τριανταφύλλου |
|  | | |
| Ημερομηνία Ελέγχου | : | 8/1/2024 |
|  | | |
| α/α Ελέγχου | : | 1 |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***A1 – Injection*** | | *Checked?* | | | | | | | | ***X*** |
|  |  |  |  |  | | | |  | | |
|  |  |  | | | |  |  | | |  |
|  |  |  | | | | OK |  | | NOT OK | | |
|  | | | | | | | | | | |
| Δεν γίνεται σύνδεση με κάποια Βάση Δεδομένων. | | | | | | | | | | |
| Δεν εφαρμόζεται / Δεν υπάρχει τέτοιος κίνδυνος. | | | | | | | | | | |
|  | | | | | | | | | | |
|  |  |  |  |  | | | |  | | |
| ***A2 – Broken Authentication and Session Management*** | | | | | *Checked?* | | | | | ***X*** |
|  |  |  |  |  | | | |  | | |
|  |  |  | | | |  |  | | |  |
|  |  |  | | | | OK |  | | NOT OK | | |
|  | | | | | | | | | | |
| Για authentication χρησιμοποιείται η υπηρεσία Firebase Authentication. | | | | | | | | | | |
| Για authorization όπου απαιτείται, γίνεται η επαλήθευση του Firebase Access Token | | | | | | | | | | |
| από το API (back-end). | | | | | | | | | | |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***A3 – Cross-Site Scripting (XSS)*** | | | | | *Checked?* | | | | | ***X*** |
|  |  |  |  |  | | | |  | | |
|  |  |  | | | |  |  | | |  |
|  |  |  | | | | OK |  | | NOT OK | | |
|  | | | | | | | | | | |
| Δεν εφαρμόζεται / Δεν υπάρχει τέτοιος κίνδυνος. Δεν υπάρχει περιεχόμενο σε κάποια σελίδα | | | | | | | | | | |
| του front-end (e-shop), που να προέρχεται από τους χρήστες. | | | | | | | | | | |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***A4 – Insecure Direct Object References*** | | | | | *Checked?* | | | | | ***X*** |
|  |  |  |  |  | | | |  | | |
|  |  |  | | | |  |  | | |  |
|  |  |  | | | | OK |  | | NOT OK | | |
|  | | | | | | | | | | |
| Η επεξεργασία των objects από το API γίνονται σε επίπεδο controller, με ειδική αναφορά για το | | | | | | | | | | |
| κάθε πεδίο ή object property γενικότερα. Δεν υφίστανται επεξεργασία άλλα properties | | | | | | | | | | |
| αυτόματα ή με βάση το input του χρήστη. | | | | | | | | | | |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***A5 – Security Misconfiguration*** | | | | | *Checked?* | | | | | ***X*** |
|  |  |  |  |  | | | |  | | |
|  |  |  | | | |  |  | | |  |
|  |  |  | | | | OK |  | | NOT OK | | |
|  | | | | | | | | | | |
| Αποκλεισμός λεπτομερειακών error messages στο χρήστη, ώστε | | | | | | | | | | |
| να μην είναι δυνατή η έκθεση πηγαίου κώδικα ή σχετικών πληροφοριών. | | | | | | | | | | |
|  | | | | | | | | | | |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***A6 – Sensitive Data Exposure*** | | | | | *Checked?* | | | | | ***X*** |
|  |  |  |  |  | | | |  | | |
|  |  |  | | | |  |  | | |  |
|  |  |  | | | | OK |  | | NOT OK | | |
|  | | | | | | | | | | |
| Δεν γίνεται χρήση password. Το login γίνεται μέσω magic (e-mail) link authentication. | | | | | | | | | | |
| Στη συνέχεια, το session management γίνεται με βάση το token. Δεν είναι δυνατό, | | | | | | | | | | |
| κάποιος χρήστης να δει δεδομένα άλλου χρήστη. Τα δεδομένα που επιστρέφονται από το API | | | | | | | | | | |
| διαμορφώνονται με βάση το Token, και όχι με βάση το τι ζητάει το front-end. | | | | | | | | | | |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***A7 – Missing Function Level Access Control*** | | | | | *Checked?* | | | | | ***X*** |
|  |  |  |  |  | | | |  | | |
|  |  |  | | | |  |  | | |  |
|  |  |  | | | | OK |  | | NOT OK | | |
|  | | | | | | | | | | |
| Δεν υπάρχουν ενέργειες που να εξαρτώνται από το URL. | | | | | | | | | | |
| Για όλα τα προς ενέργεια requests, γίνεται επαλήθευση του Firebase Token. | | | | | | | | | | |
| Δεν υπάρχουν ρόλοι administrator στο API. Μόνος ρόλος είναι του πελάτη (customer). | | | | | | | | | | |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***A8 – Cross-Site Request Forgery*** | | | | | *Checked?* | | | | | ***X*** |
|  |  |  |  |  | | | |  | | |
|  |  |  | | | |  |  | | |  |
|  |  |  | | | | OK |  | | NOT OK | | |
|  | | | | | | | | | | |
| Για την άμυνα εναντίον του CSRF, γίνεται χρήση του Firebase Token. | | | | | | | | | | |
| Κάθε request (που δεν αποτελεί απλή λήψη πληροφοριών για τα προϊόντα), | | | | | | | | | | |
| απαιτεί το Firebase Token για να είναι έγκυρο. | | | | | | | | | | |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***A9 – Using Components with Known Vulnerabilities*** | | | | | *Checked?* | | | | | ***X*** |
|  |  |  |  |  | | | |  | | |
|  |  |  | | | |  |  | | |  |
|  |  |  | | | | OK |  | | NOT OK | | |
|  | | | | | | | | | | |
| Κατά τη διαδικασία ανάπτυξης, δεν υπήρχαν known vulnerabilities. | | | | | | | | | | |
| Επίσης, υπάρχει η δυνατότητα αναβάθμισης σε περίπτωση που παρουσιαστούν τέτοια | | | | | | | | | | |
| στο μέλλον. | | | | | | | | | | |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***A10 – Unvalidated Redirects and Forwards*** | | | | | *Checked?* | | | | | ***X*** |
|  |  |  |  |  | | | |  | | |
|  |  |  | | | |  |  | | |  |
|  |  |  | | | | OK |  | | NOT OK | | |
|  | | | | | | | | | | |
| Δεν υπάρχουν σύνδεσμοι προς εξωτερικές σελίδες. | | | | | | | | | | |
| Κατά τη χρήση του magic link, γίνεται validation του URL. | | | | | | | | | | |
|  | | | | | | | | | | |

|  |
| --- |
| Επόμενες Ενέργειες |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
| Υπογραφή |