1. Αντικείμενο.

Η παρούσα προσφορά αφορά την αναβάθμιση της ιστοσελίδας gnedessas.gov.gr, ώστε να αποκατασταθούν τα ευρήματα του ελέγχου ευπαθειών (Vulnerability Assessment) της Space Hellas της 13/5/2026, ο οποίος έχει αξιολογηθεί ως «No Pass».

Στόχος είναι η ιστοσελίδα να περάσει τον επαναληπτικό έλεγχο, ώστε να καταστεί δυνατή η μετάπτωσή της από τις υποδομές του ΣΥΖΕΥΞΙΣ Ι στις υποδομές του ΣΥΖΕΥΞΙΣ ΙΙ.

Η μετάπτωση και ο επαναληπτικός έλεγχος πραγματοποιούνται από το ΣΥΖΕΥΞΙΣ και δεν περιλαμβάνονται στο αντικείμενο της προσφοράς.

2. Αποκατάσταση ευρημάτων.

Για κάθε εύρημα του report προβλέπονται οι παρακάτω ενέργειες:

Absence of Anti-CSRF Tokens High Προσθήκη anti-CSRF token στις φόρμες του ιστοτόπου, συμπεριλαμβανομένης της φόρμας αναζήτησης, και έλεγχος ότι καμία φόρμα δεν εκτελεί ενέργεια μέσω GET.
Content Security Policy (CSP) Header Not Set
Medium Σχεδιασμός και εφαρμογή πολιτικής CSP προσαρμοσμένης στο theme και στα plugins, ώστε να μην επηρεαστεί η λειτουργία της ιστοσελίδας.
Cookie No HttpOnly Flag Low Ενεργοποίηση HttpOnly στα cookies της εφαρμογής που δεν απαιτούν πρόσβαση από JavaScript.
Cookie without SameSite Attribute Low Ορισμός SameSite=Lax στα cookies της εφαρμογής.
Server Leaks Information via "XPowered-By"
Low Απόκρυψη του header X-Powered-By (έκδοση PHP/Plesk).
Strict-Transport-Security Header Not Set
Low Εφαρμογή HSTS σε όλες τις αποκρίσεις του ιστοτόπου, συμπεριλαμβανομένων των στατικών αρχείων.
X-Content-Type-Options Header Missing
Low Ορισμός X-Content-Type-Options: nosniff.
Ενημερωτικά ευρήματα (Charset Mismatch, Cookie Poisoning, Reexamine Cache-control Directives, User Controllable HTML Element Attribute, Modern Web Application, Session Management Response Identified) Informational
Ενημερωτικά ευρήματα χωρίς βαθμολογία κινδύνου (CVSS 0).
Δεν περιλαμβάνονται στο αντικείμενο της προσφοράς, καθώς δεν αποτελούν ευπάθειες και, σύμφωνα με το report, δεν απαιτούν διορθωτικές ενέργειες.

3. Επιπλέον εργασίες αναβάθμισης.

• Πλήρες αντίγραφο ασφαλείας αρχείων και βάσης δεδομένων πριν από κάθε παρέμβαση.
• Ενημέρωση του WordPress core και των plugins στις τρέχουσες σταθερές εκδόσεις.
• Ενημέρωση του theme στην τρέχουσα έκδοσή του και έλεγχος της ορθής εμφάνισης της ιστοσελίδας.
• Αφαίρεση του plugin WP Hardening (Astra Security), του οποίου η υποστήριξη έχει διακοπεί από τον κατασκευαστή, και μεταφορά των ρυθμίσεων ασφαλείας που εφαρμόζει σήμερα στη διαμόρφωση της ιστοσελίδας, χωρίς χρήση πρόσθετου plugin.
• Δικός μας έλεγχος ευπαθειών με αντίστοιχο εργαλείο πριν από το αίτημα επαναληπτικού ελέγχου προς το ΣΥΖΕΥΞΙΣ.

4. Παραδοτέα.

• Αναβαθμισμένη ιστοσελίδα με αποκατεστημένα τα ευρήματα του report.
• Τεχνική αναφορά με τις ενέργειες ανά εύρημα και τα αποτελέσματα του δικού μας ελέγχου, κατάλληλη για προώθηση στο ΣΥΖΕΥΞΙΣ.
• Οδηγίες προς τον διαχειριστή του server για τις ρυθμίσεις που απαιτούνται σε επίπεδο server, εφόσον χρειαστούν.

5. Χρονοδιάγραμμα

Οι εργασίες θα ολοκληρωθούν εντός ενός (1) μηνός από τη χορήγηση των απαραίτητων προσβάσεων.

1η εβδομάδα: Πρόσβαση, αντίγραφα ασφαλείας, καταγραφή υφιστάμενης κατάστασης
2η εβδομάδα: Ενημερώσεις WordPress, theme, plugins και αφαίρεση WP Hardening
3η εβδομάδα: Αποκατάσταση ευρημάτων (CSRF, CSP, headers, cookies)
4η εβδομάδα: Δικός μας έλεγχος, διορθώσεις, τεχνική αναφορά, ενημέρωση για αίτημα επαναληπτικού.

6. Προϋποθέσεις και όροι

• Πρόσβαση στο Plesk της ιστοσελίδας (αρχεία και βάση δεδομένων) και στο διαχειριστικό του WordPress.
• Οι εργασίες αφορούν την ιστοσελίδα. Ρυθμίσεις σε επίπεδο server θα γίνουν από τον διαχειριστή του server, με βάση τις οδηγίες μας.
• Η προσφορά καλύπτει τα ευρήματα των reports της Space Hellas της 13/5/2026.
Αν κάποιο από αυτά επανεμφανιστεί στον επαναληπτικό έλεγχο, θα το αποκαταστήσουμε **χωρίς επιπλέον χρέωση**.
• Νέα ευρήματα που τυχόν προκύψουν στον επαναληπτικό έλεγχο και δεν περιλαμβάνονται στα αρχικά reports θα κοστολογηθούν χωριστά, μετά από ενημέρωση και έγκρισή σας.
• Οι εργασίες θεωρούνται ολοκληρωμένες με την επίτευξη αξιολόγησης «Pass» στον επαναληπτικό έλεγχο της Space Hellas.
Νέα ευρήματα που τυχόν προκύψουν στον επαναληπτικό έλεγχο και δεν περιλαμβάνονται στα αρχικά reports, καθώς και επιπλέον εργασίες που θα ζητηθούν μετά την επίτευξη «Pass», θα κοστολογηθούν χωριστά, μετά από ενημέρωση και έγκρισή σας.