ΤΕΧΝΙΚΗ ΑΝΑΦΟΡΑ

Optisleek

Ανάλυση του WordPress plugin για το ziger.gr

Αναλυτική ανάγνωση του κώδικα: τι είναι το plugin, τι ακριβώς κάνει, πώς συνδέεται με την πλατφόρμα Optisleek και πού χρειάζεται προσοχή.

ΕΚΔΟΣΗ PLUGIN	AUTHOR	WORDPRESS	PHP	ΕΞΑΡΤΗΣΗ
1.0.4	FDN Group	≥ 6.7	≥ 7.4	WooCommerce

ΗΜΕΡΟΜΗΝΙΑ

24 Σεπτεμβρίου 2026

Εγκατάσταση αναφοράς: ziger.gr

— Περιεχόμενα

01 **Σύνοψη** — τι είναι σε μία παράγραφο

02 **Αρχιτεκτονική** — αλυσίδα εκκίνησης και χάρτης αρχείων

03 **Tracking** — τα έξι events και πώς ταξιδεύουν

04 **Attribution** — aguid, btaguid, alpguid

05 **Παραγγελίες** — το τριπλό δίχτυ ασφαλείας

06 **Export καταλόγου** — δύο παράλληλα APIs

07 **Ταξινόμηση κατηγοριών** — από το Optisleek στο ORDER BY

08 **Widgets προϊόντων**

09 **Landing Pages**

10 **Περιβάλλον διαχείρισης**

11 **Παράρτημα δεδομένων** — options, hooks, session, cron

12 **Ασφάλεια** — ευρήματα κατά σοβαρότητα

13 **Νεκρός και αδρανής κώδικας**

14 **Γνωστά λειτουργικά όρια**

15 **Συνολική εκτίμηση**

1. Σύνοψη

Το Optisleek είναι ο **συνδετήρας ανάμεσα σε ένα WooCommerce κατάστημα και την εξωτερική πλατφόρμα analytics & βελτιστοποίησης Optisleek**. Δεν εκτελεί το ίδιο καμία ανάλυση και δεν παράγει προτάσεις — λειτουργεί ως καλώδιο δύο κατευθύνσεων.

Κατεύθυνση	Τι μεταφέρει
Προς τα έξω	Συμπεριφορά επισκεπτών (6 τύποι events), ολοκληρωμένες παραγγελίες με απόδοση ανά κανάλι, και ολόκληρος ο κατάλογος προϊόντων με τιμές, αποθέματα και variations.
Προς τα μέσα	Αποφάσεις της πλατφόρμας: σειρά προϊόντων ανά κατηγορία, widgets προτεινόμενων προϊόντων, landing pages.

Χωρίς ενεργό λογαριασμό και server Optisleek το plugin δεν παράγει τίποτα ορατό: είναι client μιας υπηρεσίας, όχι αυτόνομο εργαλείο. Ένας κεντρικός διακόπτης (`optisleek_enabled`) σταματά τα πάντα.

2. Αρχιτεκτονική

Αλυσίδα εκκίνησης

Γραμμική και χωρίς εκπλήξεις. Το κύριο αρχείο φορτώνει την κλάση-ενορχηστρωτή, η οποία με τη σειρά της φορτώνει εννέα modules και τα αρχικοποιεί ανάλογα με το περιβάλλον:

```
optisleek.php                       bootstrap + activation/deactivation hooks
  └─ class-optisleek.php  →  Optisleek::init()
       ├─ require × 9 modules
       ├─ Optisleek_Landing_Pages::init()        (πάντα)
       ├─ Optisleek_Admin_Page::init()           (μόνο is_admin)
       ├─ Optisleek_Tracking_Core::init()        (μόνο front-end)
       ├─ Optisleek_Related_Products_Widget::init()
       ├─ Optisleek_Bought_Together_Widget::init()
       ├─ Optisleek_Sorting::init()
       └─ rest_api_init → Optisleek_REST_API::register_routes()
```

Στην ενεργοποίηση προγραμματίζεται το cron της ταξινόμησης και τίθεται transient που ανακατευθύνει στη σελίδα καλωσορίσματος. Στην απενεργοποίηση το cron αποπρογραμματίζεται. Ο πίνακας της βάσης δημιουργείται τεμπέλικα, με έλεγχο έκδοσης σχήματος.

Χάρτης αρχείων

Αρχείο	Ρόλος
`tracking-pixelV2.php`	Events, attribution, καταγραφή παραγγελιών
`class-admin-page.php`	Έξι σελίδες admin, AJAX handlers, settings registry
`class-product-export.php`	Export καταλόγου (legacy endpoint)
`class-product-widget-base.php`	Κοινή βάση widgets και φόρτωση SDK
`optisleek-landing-pages.php`	Shortcode και alpguid attribution
`class-sorting.php`	Ταξινόμηση κατηγοριών
`class-rest-api.php`	REST API: export και CRUD κανόνων
`class-optisleek.php`	Ενορχηστρωτής
`class-tracking-core.php`	Το επίσημο pixel snippet
`class-related-products-widget.php`	Δηλώσεις ρυθμίσεων widget
`class-bought-together-widget.php`	Δηλώσεις ρυθμίσεων widget
`class-attribute-erp.php`	**Νεκρός κώδικας** — βλ. §13
`assets/js/admin.js`	Dropdowns, φίλτρα κανόνων, μαζικές ενέργειες
`assets/js/optisleek-widget-mock.js`	Τοπικό mock του SDK για δοκιμές

> **ΠΑΡΑΤΗΡΗΣΗ ΓΙΑ ΤΗ ΣΥΝΤΗΡΗΣΗ**
>
> Η αρχιτεκτονική είναι συνεπής: στατικές κλάσεις με `init()`, μηδενικό αντικειμενικό state, όλες οι ρυθμίσεις σε WP options. Μία εξαίρεση ξεχωρίζει — το `tracking-pixelV2.php` είναι procedural, με εκτενές inline JavaScript ενσωματωμένο μέσα σε PHP. Είναι κληρονομιά της αρχικής φάσης και συγκεντρώνει το μεγαλύτερο μέρος του τεχνικού χρέους.

3. Tracking

Υπάρχουν **δύο παράλληλα κανάλια** προς το Optisleek. Το πρώτο είναι το επίσημο pixel snippet (`optisleekpx.js`) που τυπώνεται στο footer από το `class-tracking-core.php` . Το δεύτερο, και πολύ πιο εκτενές, είναι η δική του υλοποίηση events στο `tracking-pixelV2.php` , που χτυπά απευθείας το endpoint `{optisleek_url}/api/event/push` .

Τα έξι events

Event	Πότε ενεργοποιείται	Τι κουβαλά
`product`	Άνοιγμα σελίδας προϊόντος· και ξανά σε κάθε αλλαγή χρώματος ή μεγέθους	product_id, κατηγορίες, επιλεγμένα variation term ids
`add_to_cart`	Επιτυχής προσθήκη στο καλάθι	product_id, ποσότητα, variation
`product_engagement`	60 δευτερόλεπτα παραμονής στη σελίδα προϊόντος	product_id, κατηγορίες, timeSpend
`products_engagement`	60 δευτερόλεπτα χωρίς scroll σε σελίδα λίστας	Batch όλων των ορατών προϊόντων με κατηγορίες και χρώμα
`add_to_favorites`	Κλικ σε κουμπί wishlist	product_id, κατηγορίες, χρώμα
`eshop_order_complete`	Σελίδα ευχαριστίας — με server-side δίχτυ (§5)	Όλες οι γραμμές, τιμές, ποσότητες, απόδοση καναλιού

Πώς ταξιδεύουν τα δεδομένα

Η μεταφορά έχει τρία επίπεδα υποχώρησης, ώστε το event να φύγει ακόμα κι όταν ο χρήστης κλείνει την καρτέλα:

```
navigator.sendBeacon()  →  fetch() POST no-cors, keepalive  →  <img> GET
```

Ένα λεπτό αλλά ουσιαστικό σημείο: αν το τελικό URL ξεπεράσει τους **6.000 χαρακτήρες**, το payload μεταφέρεται στο σώμα του αιτήματος με σημαία `edb=1` . Χωρίς αυτό, ο nginx θα απέρριπτε σιωπηλά το αίτημα με 414 — και το event θα χανόταν χωρίς κανένα ίχνος. Αφορά κυρίως το `products_engagement` σε σελίδες με πολλά ορατά προϊόντα.

Ταυτοποίηση επισκέπτη

Τυχαίο αναγνωριστικό `opt_uid` που παράγεται στον browser και αποθηκεύεται στο localStorage, με fallback σε εφήμερο id αν το localStorage είναι κλειδωμένο. Δεν γίνεται κανένας έλεγχος συγκατάθεσης cookies πριν την έναρξη της καταγραφής.

Ο ρόλος των «watched attributes»

> **Η ΠΙΟ ΚΡΙΣΙΜΗ ΡΥΘΜΙΣΗ ΤΟΥ PLUGIN**
>
> Στις Γενικές Ρυθμίσεις ορίζονται ποιες ιδιότητες WooCommerce είναι «χρώμα» και ποιες «μέγεθος». Η επιλογή αυτή καθορίζει *τρία ανεξάρτητα πράγματα*: ποιες αλλαγές variation πυροδοτούν event, τι μπαίνει στο πεδίο `erp_code` των παραγγελιών, και πώς υπολογίζονται τα `all_choices` / `available_choices` στο export. Λάθος ρύθμιση εδώ αλλοιώνει σιωπηλά και τα τρία.

4. Attribution

Το plugin απαντά στο ερώτημα **«ποιο εργαλείο του Optisleek οδήγησε σε αυτή την πώληση;»** με τρία αναγνωριστικά που φτάνουν ως παράμετροι URL:

Αναγνωριστικό	Προέλευση	Αποθήκευση
`aguid`	Widget σχετικών προϊόντων	WooCommerce session
`btaguid`	Widget «αγοράστηκαν μαζί»	WooCommerce session
`alpguid + alpguidToken`	Landing page	Session, με fallback cookie 7 ημερών

Η ροή, βήμα προς βήμα

1. **Άφιξη.** Ο επισκέπτης φτάνει σε σελίδα προϊόντος με `?aguid=…` · το αναγνωριστικό αποθηκεύεται μαζί με το id του συγκεκριμένου προϊόντος.
2. **Last touch.** Μόλις ένα προϊόν αποδοθεί σε ένα κανάλι, αφαιρείται αυτόματα από τα άλλα δύο. Κάθε προϊόν ανήκει σε ακριβώς ένα κανάλι — το τελευταίο που το «άγγιξε».
3. **Προσθήκη στο καλάθι.** Ένα μόνο AJAX αίτημα με `guid_type=all` προσθέτει το variation id και στα τρία αναγνωριστικά ταυτόχρονα, αντί για τρεις ξεχωριστές κλήσεις.
4. **Checkout.** Όλα αντιγράφονται σε order meta `_optisleek_guids`. Αυτό είναι απαραίτητο: το WP-Cron που εκτελεί το fallback δεν έχει πρόσβαση σε session.
5. **Αποστολή.** Στο event της παραγγελίας, κάθε γραμμή φέρει τα δικά της `aguid` / `btaguid` / `alpguid` flags.

Η αντιστοίχιση γραμμής προς αναγνωριστικό αντέχει και την περίπτωση όπου ο επισκέπτης είδε τον γονέα αλλά αγόρασε variation: ελέγχονται και τα δύο ids, καθώς και ο γονέας κάθε variation.

5. Παραγγελίες — το τριπλό δίχτυ

Το πιο προσεγμένο κομμάτι του plugin. Μια ολοκληρωμένη παραγγελία δεν πρέπει ούτε να χαθεί (ad-blocker, JS σφάλμα, κλείσιμο καρτέλας) ούτε να μετρηθεί δύο φορές.

Μηχανισμός	Λειτουργία
Browser	Στέλνει το event και έπειτα επιβεβαιώνει με AJAX, σημειώνοντας `_optisleek_tracked = yes` στην παραγγελία.
Server-side fallback	Προγραμματισμένο WP-Cron +5 λεπτά. Αν δεν υπάρξει επιβεβαίωση, στέλνει το ίδιο ακριβώς payload server-side με `wp_remote_post`.
Off-site gateways	Επιπλέον hooks σε `processing` και `completed`, γιατί με Viva ή Stripe redirect η σελίδα ευχαριστίας ενδέχεται να μην ανοίξει ποτέ.
Επαναλήψεις	Έως 3 προσπάθειες, μία ανά ώρα, με μετρητή σε order meta.

Τρία order meta συγκρατούν την κατάσταση και αποτρέπουν τη διπλομέτρηση: `_optisleek_tracked`, `_optisleek_js_rendered`, `_optisleek_track_attempts`. Το δεύτερο καλύπτει την περίπτωση όπου ο πελάτης κάνει refresh στη σελίδα ευχαριστίας πριν προλάβει η επιβεβαίωση.

Τι περιέχει το payload μιας παραγγελίας

Μία εγγραφή ανά γραμμή παραγγελίας — με το id του γονικού προϊόντος, όλες τις κατηγορίες σε CSV, ποσότητα, τιμή μονάδας, τα term ids των watched attributes ως `erp_code`, και τα τρία flags απόδοσης — και στο τέλος μία εγγραφή με το συνολικό ποσό της παραγγελίας.

6. Export καταλόγου

Υπάρχουν **δύο παράλληλα APIs** που επιστρέφουν ουσιαστικά τα ίδια δεδομένα.

1. Legacy endpoint (custom rewrite rule)

```
/optisleek/api/?sync=all-json
                    brands
                    categories
                    attributes-templates
                    attributes
                    products
```

2. REST endpoint

```
GET /wp-json/optisleek/products
```

Παράμετροι

Παράμετρος	Λειτουργία
`pg` / `page`	Αριθμός σελίδας — η σελιδοποίηση είναι opt-in
`per_page`	Μέγεθος σελίδας, με ανώτατο όριο 500
`modified_after`	Incremental sync: μόνο όσα άλλαξαν μετά την ημερομηνία

Τι περιέχει η απάντηση

Ενότητα	Πεδία
brands	term id, όνομα, αν έχει δημοσιευμένα προϊόντα
categories	id, όνομα, γονέας, σύνδεσμος, κατάσταση
attributeTemplates	Οι ομάδες ιδιοτήτων του WooCommerce (Χρώμα, Μέγεθος…)
attributes	Κάθε τιμή ιδιότητας, με το template στο οποίο ανήκει
products	Τίτλος, SKU, τιμές, διαθεσιμότητα, κατηγορίες, brand, περιγραφή, εικόνες και πλήρης ανάλυση variations

Το πλουσιότερο κομμάτι είναι τα variations. Πέρα από τιμή και απόθεμα, το plugin υπολογίζει ανά συνδυασμό τα `all_choices` και `available_choices` — δηλαδή «πόσα μεγέθη υπάρχουν συνολικά» και «πόσα από αυτά είναι διαθέσιμα σε αυτό το χρώμα». Ο υπολογισμός γίνεται με cache ανά προϊόν, ώστε να μην εκφυλίζεται σε τετραγωνική πολυπλοκότητα.

> **ΠΡΟΣΟΧΗ**
>
> Και τα δύο endpoints είναι **εντελώς δημόσια**, χωρίς καμία αυθεντικοποίηση. Αναλυτικά στην §12.

7. Ταξινόμηση κατηγοριών

Η πλατφόρμα αποφασίζει τη σειρά με την οποία θα εμφανίζονται τα προϊόντα σε κάθε κατηγορία, και το plugin την επιβάλλει στο κατάστημα.

Αποθήκευση

Δικός του πίνακας στη βάση, `wp_optisleek_sorting` :

Στήλη	Περιεχόμενο
`category_ids`	JSON πίνακας με τα term ids των κατηγοριών του κανόνα
`product_ids`	JSON πίνακας με τα ids των προϊόντων **στη σειρά που τα θέλει το Optisleek**
`enabled`	Αν ο κανόνας εφαρμόζεται
`updated_at`	Χρόνος τελευταίας ενημέρωσης

Δύο δρόμοι εγγραφής

Δρόμος	Ροή
Pull	Το plugin καλεί `POST {optisleek_url}/api/products/sort` με api_token και shop_id. Ενεργοποιείται από WP-Cron δύο φορές την ημέρα, από κουμπί στο admin, ή από εξωτερικό cron μέσω του endpoint `/wp-json/optisleek/cron-sync?cron_token=…` .
Push	Το Optisleek καλεί `POST / PUT / PATCH / DELETE /wp-json/optisleek/sorting` με κεφαλίδα `X-Api-Token` .

Εφαρμογή στο κατάστημα

Προστίθεται η επιλογή «Προτεινόμενα (Optisleek)» στο dropdown ταξινόμησης του WooCommerce και ορίζεται ως προεπιλογή. Οι υπόλοιπες επιλογές του πελάτη (τιμή, δημοφιλία) συνεχίζουν να λειτουργούν κανονικά — η σειρά του Optisleek εφαρμόζεται μόνο όταν είναι ενεργή η δική του επιλογή. Η ίδια η ταξινόμηση γίνεται με απευθείας παρέμβαση στο `ORDER BY` του ερωτήματος:

```
FIELD(ID, <λίστα>) = 0,                 -- πρώτα όσα υπάρχουν στη λίστα
FIELD(ID, <λίστα>) ASC,                 -- με ακριβώς τη σειρά του Optisleek
menu_order ASC, post_date DESC, ID DESC   -- σταθερή σειρά για όλα τα υπόλοιπα
```

Η τρίτη γραμμή δεν είναι διακοσμητική: χωρίς σταθερό tiebreaker η MySQL δεν εγγυάται συνεπή σειρά μεταξύ σελίδων, με αποτέλεσμα προϊόντα να εμφανίζονται δύο φορές ή να χάνονται στο pagination.

Εντοπισμός τρέχουσας κατηγορίας

Τρεις διαδοχικές μέθοδοι, ώστε να δουλεύει και με AJAX φίλτρα τρίτων: το αντικείμενο της σελίδας, έπειτα το `tax_query` του ερωτήματος, και τέλος η παράμετρος `filter_cat`.

Διαχείριση από το admin

Πίνακας κανόνων με αναζήτηση, πολλαπλή επιλογή, μαζική ενεργοποίηση ή διαγραφή, κουμπί άμεσου συγχρονισμού και ιστορικό των τελευταίων 50 συγχρονισμών με αποτέλεσμα, αφορμή και μήνυμα σφάλματος.

8. Widgets προϊόντων

Δύο widgets — σχετικά προϊόντα και «αγοράστηκαν μαζί» — μοιράζονται μία αφηρημένη βάση. Κάθε υποκλάση δηλώνει μόνο έξι πράγματα: τύπο, slug, ετικέτα και τα τρία option keys της. Όλη η λογική φόρτωσης είναι κοινή.

Θέμα	Υλοποίηση
Τοποθέτηση	`woocommerce_after_single_product_summary`, priority 25 και 26
Διαφυγή για page builders	Προαιρετικός custom CSS selector ανά widget, για Divi/Elementor templates που δεν τρέχουν το hook
Φόρτωση SDK	Το `products.js` φορτώνεται **μία φορά** για όλα τα ενεργά widgets
Αρχικοποίηση	Επαναλαμβανόμενη προσπάθεια έως 10 δευτερόλεπτα μέχρι να οριστεί το `OPTAnalytics`
Διάγνωση	Σε αποτυχία τυπώνεται στην κονσόλα ακριβώς τι δεν βρέθηκε — anchor, selector ή SDK

Οι ρυθμίσεις Pixel ID και Base URL των widgets κληρονομούνται πλέον αυτόματα από τις Γενικές Ρυθμίσεις και εμφανίζονται κλειδωμένες, ώστε να μην μένει ποτέ παλιό αντίγραφο που θα υπερίσχυε μετά από αλλαγή στις Γενικές.

9. Landing Pages

Shortcode `[optisleek_landing_page token="…"]` που τοποθετείται σε οποιαδήποτε σελίδα. Τυπώνει έναν container με τα στοιχεία σύνδεσης ως data attributes και φορτώνει έναν JS loader, ο οποίος πρώτα ελέγχει με αίτημα HEAD και χρονικό όριο 3 δευτερολέπτων αν το script υπάρχει, πριν προσπαθήσει να το φορτώσει.

Υποστηρίζεται το preview του Elementor. Από εδώ γεννιέται το `alpguid` της §4, που κλείνει τον κύκλο απόδοσης μέχρι την παραγγελία. URL και Pixel ID κληρονομούνται από τις Γενικές Ρυθμίσεις, ενώ το shortcode μπορεί ακόμα να τα παρακάμψει ανά σελίδα.

10. Περιβάλλον διαχείρισης

Σελίδα	Περιεχόμενο
Γενικές Ρυθμίσεις	Optisleek Code, E-shop API Token, Shop ID, Optisleek URL και η επιλογή των ιδιοτήτων χρώματος/μεγέθους
Widgets Προϊόντων	Ενεργοποίηση των δύο widgets και custom σημεία εισαγωγής· Pixel και URL κλειδωμένα στις Γενικές
Landing Pages	Ενεργοποίηση shortcode και οδηγίες χρήσης· URL και Pixel κλειδωμένα στις Γενικές
Ταξινόμηση	Κανόνες, φίλτρα, μαζικές ενέργειες, χειροκίνητος συγχρονισμός, ιστορικό
Docs	Ό,τι αρχείο τοποθετηθεί στον φάκελο `/docs/` εμφανίζεται αυτόματα, χωρίς αλλαγή κώδικα
Welcome	Κρυφή σελίδα, με αυτόματη ανακατεύθυνση κατά την ενεργοποίηση

Δύο προειδοποιήσεις εμφανίζονται αυτόματα στο admin: όταν λείπουν βασικές ρυθμίσεις ενώ το plugin είναι ενεργό, και όταν έχει μείνει ανοιχτή η δοκιμαστική λειτουργία των widgets.

11. Παράρτημα δεδομένων

Ρυθμίσεις (WP options)

Option	Περιεχόμενο
`optisleek_enabled`	Κεντρικός διακόπτης όλου του plugin
`optisleek_code`	Pixel ID / αναγνωριστικό καταστήματος
`optisleek_url`	Base URL της πλατφόρμας
`api_token`	Token — διπλός ρόλος, βλ. §12
`optisleek_shop_id`	Αναγνωριστικό καταστήματος για τον συγχρονισμό ταξινόμησης
`optisleek_color_attribute[]`	Ιδιότητες που θεωρούνται «χρώμα»
`optisleek_size_attribute[]`	Ιδιότητες που θεωρούνται «μέγεθος»
`relative_products_enabled`	Ενεργοποίηση widget σχετικών προϊόντων
`bought_together_products_enabled`	Ενεργοποίηση widget «αγοράστηκαν μαζί»
`optisleek_*_selector`	Custom CSS σημεία εισαγωγής ανά widget
`optisleek_widgets_test_mode`	Δοκιμαστική λειτουργία (χωρίς UI πλέον)
`optisleek_landing_pages_enabled`	Ενεργοποίηση shortcode landing pages
`optisleek_sorting_enabled`	Ενεργοποίηση ταξινόμησης
`optisleek_sorting_log`	Ιστορικό 50 τελευταίων συγχρονισμών
`optisleek_cron_secret`	Token για το εξωτερικό cron endpoint
`optisleek_sorting_db_ver`	Έκδοση σχήματος του πίνακα
`optisleek_api_rewrite_v1`	Σημαία ότι έγινε flush των rewrite rules

Κλειδιά WooCommerce session

Κλειδί	Περιεχόμενο
`optisleek_aguid`	Αναγνωριστικό καναλιού σχετικών προϊόντων
`optisleek_aguid_product_ids`	Τα προϊόντα που αποδίδονται σε αυτό
`optisleek_btaguid`	Αναγνωριστικό καναλιού «αγοράστηκαν μαζί»
`optisleek_btaguid_product_ids`	Τα προϊόντα που αποδίδονται σε αυτό
`optisleek_alpguid`	Landing page: guid, token και προϊόντα

Order meta

Meta	Περιεχόμενο
`_optisleek_guids`	Στιγμιότυπο των guid του session τη στιγμή του checkout
`_optisleek_tracked`	Η παραγγελία έχει σταλεί — αποτρέπει διπλομέτρηση
`_optisleek_js_rendered`	Το JS τυπώθηκε ήδη μία φορά
`_optisleek_track_attempts`	Μετρητής αποτυχημένων προσπαθειών

Προγραμματισμένες εργασίες

Εργασία	Συχνότητα
`optisleek_sorting_cron_sync`	Δύο φορές την ημέρα — συγχρονισμός κανόνων ταξινόμησης
`tpv2_order_track_fallback`	Μία φορά ανά παραγγελία, +5 λεπτά· επανάληψη ανά ώρα έως 3 φορές

Σημεία εισόδου προς το plugin

Endpoint	Πρόσβαση
`/optisleek/api/?sync=…`	ΔΗΜΟΣΙΟ
`GET /wp-json/optisleek/products`	ΔΗΜΟΣΙΟ
`/wp-json/optisleek/sorting`	X-API-TOKEN
`/wp-json/optisleek/cron-sync`	CRON_TOKEN
`admin-ajax: sorting/docs ενέργειες`	NONCE + ΔΙΚΑΙΩΜΑΤΑ
`admin-ajax: tpv2_products_engagement_prefetch`	ΔΗΜΟΣΙΟ, ΧΩΡΙΣ NONCE

12. Ασφάλεια

Σοβαρά

1 · ΔΗΜΟΣΙΟ EXPORT ΟΛΟΚΛΗΡΟΥ ΤΟΥ ΚΑΤΑΛΟΓΟΥ

Και τα δύο endpoints της §6 είναι ανοιχτά χωρίς καμία αυθεντικοποίηση. Εκτίθενται τιμές αγοράς και έκπτωσης, αποθέματα ανά variation, SKU, περιγραφές και σύνδεσμοι. Οποιοσδήποτε γνωρίζει το URL μπορεί να κατεβάζει τον πλήρη κατάλογο όποτε θέλει. *Γνωστό εύρημα του τεχνικού ελέγχου (#20/#21).*

2 · ΤΟ TOKEN ΤΟΥ LANDING PAGE ΤΥΠΩΝΕΤΑΙ ΣΤΟ HTML

Το shortcode τυπώνει το token ως `data-opt-token` μέσα στη σελίδα, ορατό σε κάθε προβολή πηγής. Αν πρόκειται για το ίδιο `api_token` των Γενικών Ρυθμίσεων, τότε διαρρέει δημόσια το token που προστατεύει τα endpoints της ταξινόμησης.

3 · CREDENTIALS ΜΕΣΑ ΣΤΟΝ ΦΑΚΕΛΟ ΤΟΥ PLUGIN

Το αρχείο `.vscode/sftp.json` περιέχει διεύθυνση server, όνομα χρήστη και **κωδικό σε καθαρό κείμενο**, με `uploadOnSave: true` προς το `/wp-content/plugins/optisleek`. Δηλαδή κάθε αποθήκευση αρχείου ανεβάζει αυτόματα στον live server — και το ίδιο το αρχείο με τον κωδικό ταξιδεύει μαζί. Πρέπει να μπει σε `.gitignore` και να αποκλειστεί ρητά από κάθε πακέτο διανομής.

4 · ΑΠΕΝΕΡΓΟΠΟΙΗΜΕΝΗ ΕΠΑΛΗΘΕΥΣΗ SSL

Η κλήση συγχρονισμού ταξινόμησης χρησιμοποιεί `sslverify => false`. Ακυρώνεται ο έλεγχος πιστοποιητικού στο ακριβώς ίδιο αίτημα που μεταφέρει το api_token.

Μικρότερης σοβαρότητας

Σοβαρότητα	Εύρημα
ΜΕΣΑΙΑ	Το αρχείο `api/analytics_data.json` — πλήρες dump καταλόγου, με brands άλλου καταστήματος — είναι δημόσια προσβάσιμο και δεν το χρησιμοποιεί κανένα σημείο του κώδικα.
ΜΕΣΑΙΑ	Καμία διαχείριση συγκατάθεσης cookies πριν την έναρξη της καταγραφής (GDPR, εύρημα #19).
ΧΑΜΗΛΗ	Το δημόσιο AJAX `tpv2_products_engagement_prefetch` δέχεται αυθαίρετα product ids χωρίς nonce και επιστρέφει κατηγορίες και term ids.
ΧΑΜΗΛΗ	Τα αρχεία του φακέλου `/docs/` είναι δημόσια προσβάσιμα από όποιον γνωρίζει το URL — τεκμηριωμένο στο README του φακέλου, αλλά εύκολο να ξεχαστεί.

Τι είναι σωστά υλοποιημένο

- Σύγκριση tokens με `hash_equals` και στα δύο σημεία — χωρίς διαρροή χρόνου.
- Nonce και έλεγχος `current_user_can` σε όλα τα AJAX του διαχειριστή.

- Προστασία από path traversal με `realpath` στη διαγραφή εγγράφων, με whitelist επεκτάσεων και προστατευμένα ονόματα.
- Συνεπές escaping στην έξοδο (`esc_html`, `esc_attr`, `esc_url`).
- Επαλήθευση κλειδιού παραγγελίας πριν τη σήμανσή της ως καταγεγραμμένης.

13. Νεκρός και αδρανής κώδικας

Στοιχείο	Κατάσταση
`class-attribute-erp.php`	Σκελετός με άδειες μεθόδους. Δεν φορτώνεται καν με `require` και το `add_action` του είναι σχολιασμένο — αν αποσχολιαστεί, προκαλεί fatal error.
Term meta `code`	Διαβάζεται σε δύο σημεία του export, αλλά **δεν το γράφει τίποτα** μέσα στο plugin — αυτή ακριβώς θα ήταν η δουλειά της παραπάνω κλάσης. Πρακτικά πέφτει πάντα στο fallback του term id.
`registration_admins_products_enabled` `b2b_registration_products_enabled`	Registered options χωρίς UI και χωρίς κανέναν αναγνώστη.
Ενότητα «Αυτόματος Συγχρονισμός»	Ολόκληρο το box είναι σχολιασμένο. Το REST endpoint και το token λειτουργούν, αλλά το URL δεν εμφανίζεται πουθενά — και το κουμπί ανανέωσης token είναι κι αυτό μέσα στο σχόλιο, οπότε ο αντίστοιχος handler είναι απρόσιτος.
Δοκιμαστική λειτουργία widgets	Ο μηχανισμός και το mock παραμένουν ενεργά· το UI αφαιρέθηκε πρόσφατα κατόπιν αιτήματος. Αν η ρύθμιση έμεινε ανοιχτή, δεν σβήνει πλέον από τη διεπαφή.
`api/analytics_data.json`	Μεγάλο αρχείο δεδομένων που δεν διαβάζει κανείς. Φουσκώνει το πακέτο διανομής.

> **ΑΣΥΝΕΠΕΙΑ ΠΡΟΣ ΕΠΙΒΕΒΑΙΩΣΗ**
>
> Το legacy `all-json` επιστρέφει το κλειδί `attributeTemplates` σε camelCase, ενώ το REST `optisleek/products` το ίδιο περιεχόμενο ως `attribute_templates` σε snake_case. Αν τα καταναλώνει ο ίδιος server, το ένα από τα δύο πιθανότατα αγνοείται σιωπηλά.

14. Γνωστά λειτουργικά όρια

Θέμα	Περιγραφή
Ανίχνευση wishlist	Το `add_to_favorites` εντοπίζει κουμπιά ψάχνοντας τη λέξη «wish» σε class ή id. Κάθε theme και wishlist plugin χρησιμοποιεί διαφορετική ονοματολογία, οπότε απαιτείται προσαρμογή σε κάθε εγκατάσταση.
Landing pages	Λειτουργούν σωστά, αλλά έχουν δοκιμαστεί μόνο με Elementor.
Μέγεθος καταλόγου	Χωρίς παραμέτρους, το export φορτώνει όλα τα προϊόντα ταυτόχρονα. Σε μεγάλο κατάλογο θα χτυπήσει σε timeout ή όριο μνήμης — η σελιδοποίηση υπάρχει αλλά είναι opt-in.
Χρονισμοί engagement	Τα 60 δευτερόλεπτα είναι σταθερά στον κώδικα, κατόπιν απόφασης· δεν ρυθμίζονται από το admin.
Καταγραφή στην κονσόλα	Κάθε event τυπώνεται με `console.log` και στο production, επίσης κατόπιν απόφασης.

15. Συνολική εκτίμηση

Το plugin κάνει σημαντικά περισσότερα από ένα απλό tracking pixel. Υλοποιεί πλήρη απόδοση καναλιού με last-touch λογική, ανθεκτική καταγραφή παραγγελιών με server-side δίχτυ που αντέχει ad-blockers και off-site πληρωμές, δυναμική ταξινόμηση καταλόγου σε επίπεδο SQL, και export με incremental sync και σελιδοποίηση.

Η ποιότητα του κώδικα είναι άνιση, με τρόπο που αποτυπώνει την ιστορία του έργου. Τα πρόσφατα κομμάτια — widgets, ταξινόμηση, βοηθητικά του admin — είναι καθαρά, σχολιασμένα στα ελληνικά και με ξεκάθαρο διαχωρισμό ευθυνών. Το αρχικό κομμάτι του tracking κουβαλά το βάρος της πρώτης φάσης: procedural δομή και εκτενές inline JavaScript μέσα σε PHP.

Οι δύο πραγματικοί κίνδυνοι για παραγωγή είναι **το δημόσιο export του καταλόγου** και **το token που τυπώνεται στο HTML**. Ακολουθεί, ως θέμα διαδικασίας παρά κώδικα, **το αρχείο credentials με αυτόματο ανέβασμα**. Όλα τα υπόλοιπα ευρήματα είναι θέματα συντήρησης και καθαριότητας, όχι έκθεσης.