gaman.is

Gaman.is tenging fyrir WooCommerce

Öryggi, aðgangsheimildir, meðferð gagna og áhrif á afköst.
Tæknileg lýsing fyrir eigendur verslana og þá sem sjá um vefi þeirra.

Viðbót	Gaman.is tenging (gaman-connect), útgáfa 0.5.1
Dagsetning	Nóvember 2026
Útgefandi	Áfram með Smjörið ehf., kt. 430910-2130, rekstraraðili Gaman.is
Fyrirspurnir	sala@gaman.is

1. Hlutverk viðbótarinnar

Viðbótin tengir WooCommerce-verslun við markaðstorgið Gaman.is og sinnir þremur verkefnum:

- **Vöruupplýsingar.** Gaman.is fær upplýsingar um birtar vörur verslunarinnar: heiti, lýsingu, verð, tilboð, lagerstöðu, myndir, flokka og þyngd.
- **Lagerstaða.** Þegar vara selst á Gaman.is lækkar lagerstaða hennar í versluninni sjálfkrafa, en aðeins eftir að viðbótin hefur staðfest söluna hjá Gaman.is. Sé salan felld niður eða endurgreidd hækkar hún aftur.
- **Pantanir.** Hver staðfest sala á Gaman.is verður að venjulegri pöntun í WooCommerce. Gaman.is er skráð sem kaupandi og greiðslumátinn heitir „Gaman.is“.

Viðbótin breytir ekki greiðsluferli verslunarinnar, stofnar enga notendur í WordPress og sendir engan tölvupóst til viðskiptavina.

> Gaman.is les aðeins birtar vörur, flokka, verð og lager, skráir aðeins pantanir sem gerðar eru á Gaman.is, lækkar lager um það sem selst þar og uppfærir stöðu þeirra pantana. Gaman.is les aldrei viðskiptavini, aðrar pantanir, afsláttarkóða eða stillingar og breytir aldrei verðum eða vörum. Öll samskipti Gaman.is við viðbótina eru undirrituð, og lager er aðeins lækkaður fyrir pantanir sem Gaman.is staðfestir.

2. Auðkenning og undirritun

Tvær leiðir eru tryggðar hvor með sínum hætti, svo lykill sem geymdur er í WordPress dugar aldrei til að þykjast vera Gaman.is.

- **Beiðnir frá Gaman.is til verslunarinnar** eru undirritaðar með einkalykli Gaman.is (Ed25519). Viðbótin geymir aðeins *opinberan* lykil Gaman.is, sem hún sækir sjálf til `https://gaman.is`. Undirskriftin nær yfir aðferð, slóð, fyrirspurn, auðkenni verslunarinnar, tíma, auðkenni beiðnarinnar og SHA-256 tætigildi meginmálsins, svo engu má breyta á leiðinni.
- Köllum sem eru meira en 5 mínútna gömul er hafnað, hvert auðkenni beiðnar gildir aðeins einu sinni (geymt í 10 mínútur) og kalli sem ætlað er annarri verslun er hafnað. Óundirrituð og ógild köll fá villu 401 og eru skráð í Aðgerðaskrá.
- **Beiðnir frá versluninni til Gaman.is** bera lykil viðbótarinnar (`gmn_…`) og eru auk þess undirritaðar með HMAC-SHA256 ásamt tíma og auðkenni beiðnar, svo gömlum og endurteknum köllum er hafnað. Þær fara aðeins á eina fasta slóð, `https://gaman.is`. Viðbótin krefst þess að skilríki netþjónsins séu sannreynd (TLS) og fylgir aldrei áframsendingum (redirect).
- Aðeins vefstjóri (hlutverkið *Administrator*) getur vistað lykil eða skipt um hann. Verslunarstjórar (*Shop manager*) hafa aðgang að öðrum hlutum viðbótarinnar.
- Lykillinn er vistaður í stillingu sem er ekki hlaðin sjálfkrafa (`autoload` af). Hann birtist aldrei í vafra, er aldrei skráður í atvikaskrár og er aldrei sendur út um endapunkta. Á síðunni sjást aðeins fyrstu átta stafir hans. Einnig má skilgreina hann í `wp-config.php`: `define( 'GAMAN_CONNECT_KEY', '…' );`

- Ef Gaman.is hættir að taka við lyklinum slekkur viðbótin á sér sjálf og lokar öllum endapunktum þar til nýr lykill er límdur inn.

3. Endapunktar í versluninni

Viðbótin skráir sex endapunkta í REST API WordPress, undir `/wp-json/gaman/v1`. Þeir krefjast allir undirritunar Gaman.is og viðbótin opnar ekkert annað.

Endapunktur	Aðferð	Hlutverk
`/categories`	GET	Skilar vöruflokkum verslunarinnar ásamt fjölda vara í hverjum flokki, svo para megi þá við flokka Gaman.is.
`/products`	GET	Skilar vörum í síðum, að hámarki 50 á síðu. Hægt er að biðja aðeins um vörur sem hafa breyst frá tilteknum tíma.
`/stock/{vara}`	GET	Skilar lagerstöðu og verði einnar vöru eða afbrigðis. Gaman.is kallar á hann rétt áður en kaupandi greiðir.
`/stock-decrement`	POST	Lækkar lagerstöðu vegna sölu á Gaman.is, aðeins eftir að viðbótin hefur staðfest hjá Gaman.is að pöntunin sé greidd, fyrir þessa verslun og með þessari línu og magni. Aldrei er sett ákveðin lagertala.
`/orders`	POST	Stofnar WooCommerce-pöntun fyrir staðfesta sölu á Gaman.is, byggða á gögnum sem viðbótin sækir sjálf til Gaman.is. Mest 20 nýjar pantanir á klukkustund.
`/order-status`	POST	Uppfærir stöðu pöntunar sem viðbótin stofnaði, og aðeins í stöðu sem Gaman.is staðfestir: sendingarmiði gerður, send, afhent, endurgreidd eða felld niður.

4. Beiðnir verslunarinnar til Gaman.is

Slóð á gaman.is	Hvenær
`/api/public/feed/plugin-config`	Þegar lykill er vistaður og á klukkustundar fresti. Sækir auðkenni verslunarinnar og opinbera undirritunarlykla Gaman.is.
`/api/public/feed/register`	Þegar lykill er vistaður, eftir uppfærslu og við „Athuga tengingu“. Gaman.is fær slóð verslunarinnar og útgáfu viðbótarinnar og prófar tenginguna.
`/api/public/feed/changed`	Um 45 sekúndum eftir að vöru er breytt. Aðeins auðkenni breyttra vara eru send; Gaman.is sækir síðan upplýsingarnar.
`/api/public/feed/status`	Þegar flipinn Yfirlit er opnaður, til að sýna stöðu tengingarinnar. Svarið er geymt í eina mínútu.
`/api/public/feed/session`	Þegar smellt er á „Raða flokkum“, „Opna flokkun á Gaman.is“ eða „Opna sendingar á Gaman.is“. Gaman.is skilar skammlífri slóð á viðkomandi síðu.

`/api/public/feed/orders/{id}`	Áður en lager er lækkaður, pöntun stofnuð eða staða uppfærð. Viðbótin staðfestir pöntunina sjálf hjá Gaman.is.
`/api/public/feed/orders/{id}/delivered`	Þegar verslunin merkir pöntun sem hún afhendir sjálf „Lokið“. Útgreiðslan losnar þá þremur dögum síðar.
`/api/public/feed/alert`	Ef fleiri en 20 nýjar pantanir berast á klukkustund (mest einu sinni á klukkustund).
`/api/public/feed/disconnect`	Þegar smellt er á „Aftengja Gaman.is“. Gaman.is ógildir lykilinn strax.

Liggi Gaman.is niðri hefur það engin áhrif á verslunina. Tilkynningar um breytingar eru reyndar aftur síðar, og Gaman.is samstillir vörur auk þess einu sinni á klukkustund.

5. Gögn sem fara til Gaman.is

Gögn	Nánar
Birtar vörur	Heiti, lýsing, slóð vörusíðu, verð, tilboðsverð og tilboðstímabil, lagerstaða, vörunúmer (SKU), slóðir mynda, flokkar, merki (tags), þyngd, VSK-þrep og virk afbrigði.
Óbirtar vörur	Drög, lokaðar vörur (private), tímasettar vörur og vörur í ruslinu: aðeins auðkenni, heiti og merking um að varan sé ekki til sölu. Lýsing, verð og myndir eru ekki sendar.
Vöruflokkar	Heiti, yfirflokkur og fjöldi vara.
Annað	Slóð verslunarinnar og útgáfunúmer viðbótarinnar. Engar upplýsingar um viðskiptavini verslunarinnar, aðrar pantanir, notendur eða stillingar.

6. Gögn sem koma frá Gaman.is

Hverri Gaman-pöntun fylgja vörulínur með magni og verði, sendingarmáti og þær upplýsingar um kaupandann sem þarf til afhendingar: nafn, símanúmer, netfang og afhendingarstaður. VSK hverrar línu reiknast út frá VSK-þrepi vörunnar í versluninni.

Kaupandinn er skráður sem viðtakandi sendingar, en Gaman.is (Áfram með Smjörið ehf.) sem greiðandi. Netfang kaupandans fer því aldrei í reit sem WooCommerce sendir tölvupóst á. Í pöntuninni kemur einnig fram útgreiðsla til verslunarinnar ásamt þóknun og kortagjaldi, svo uppgjör sé rekjanlegt.

7. Varnir í pöntunum og lagerstöðu

Aðeins staðfestar pantanir

Áður en lager er lækkaður, pöntun stofnuð eða staða uppfærð spyr viðbótin Gaman.is sjálf, á fastri slóð, hvort pöntunin sé til, greidd og fyrir þessa verslun, og hvort línan og magnið passi. Pöntun sem Gaman.is þekkir ekki er hafnað. Pöntunin er stofnuð úr gögnunum sem viðbótin fær í því svari, ekki úr beiðninni sjálfri.

Mest 20 nýjar pantanir á klukkustund

Fleiri nýjum pöntunum er hafnað og Gaman.is látið vita. Endurteknar beiðnir um pöntun sem þegar er til teljast ekki með.

Hver pöntun er aðeins stofnuð einu sinni

Áður en pöntun er stofnuð er auðkenni hennar skráð í töflu viðbótarinnar með einkvæmum lykli (unique key). Endurteknar beiðnir skila sömu pöntun og breyta engu. Berist tvær endurtilraunir á sama tíma heldur aðeins önnur áfram. Mistakist stofnun pöntunar er hún fjarlægð í heild, svo hálfkláraðar pantanir sitja ekki eftir.

Lagerstaða lækkar aðeins einu sinni fyrir hverja línu

Hver lína (pöntun, vara og afbrigði) er skráð með einkvæmum lykli áður en lagerstaðan er lækkuð. Skráð er nákvæmlega hve mikið var tekið af lager, og við endurgreiðslu eða niðurfellingu sem Gaman.is staðfestir er aðeins það magn sett til baka, einu sinni. Auðkenni eru samræmd áður en þau eru notuð, svo „12“, „012“ og „12 “ teljast sama vara.

Aðrar pantanir eru utan seilingar

Stöðubreytingar finna pöntun eingöngu í gegnum tengitöflu viðbótarinnar, svo ekki er hægt að breyta pöntunum sem komu ekki frá Gaman.is. Pöntun sem hefur verið felld niður eða endurgreidd er ekki hægt að færa aftur í vinnslu.

Greiðslumátinn „Gaman.is“

Greiðslumátinn er aðeins notaður á pantanir sem viðbótin stofnar. Hann birtist aldrei í greiðsluferli verslunarinnar og getur ekki tekið við greiðslu.

Tenglar á sendingarmiða og rakningu

Tenglar á sendingarmiða og rakningu sendinga eru aðeins vistaðir ef þeir nota https og vísa á Gaman.is, Dropp eða Póstinn.

8. Stjórnborðið í WordPress

- Síðan er undir WooCommerce → Gaman.is og hefur þrjá flipa: **Yfirlit** (staða tengingarinnar, síðustu 7 dagar og aðgerðir), **Stillingar** (pantanir og tenging) og **Aðgerðaskrá** (allt sem Gaman.is breytir í versluninni og hafnaðar beiðnir).
- Lyklinum er skipt um undir Stillingar → Tenging → „Skipta um lykil“. „Aftengja Gaman.is“ er neðst í sama reit.
- Síðan krefst heimildarinnar `manage_woocommerce`; til að breyta lyklinum þarf `manage_options`. Allar aðgerðir eru varðar með WordPress-nonce gegn fölsuðum beiðnum (CSRF), og allt úttak er varið (escaped) áður en það er birt.
- **Aðgerðaskrá** sýnir tíma, aðgerð, pöntun og niðurstöðu fyrir allt sem Gaman.is breytir og allar hafnaðar beiðnir. Lestur vara birtist sem ein lína á hverja samstillingu ef valið er „Sýna líka lestur“. Skráin er geymd í 90 daga og inniheldur engar persónuupplýsingar.
- Síðurnar Flokkun vara og Sendingar á Gaman.is opnast í nýjum flipa með skammlífri slóð sem Gaman.is gefur aðeins út fyrir viðkomandi verslun. Slóðin virkar einu sinni og innan 10 mínútna.

9. Áhrif á afköst

Vefverslunin sjálf

Viðbótin bætir engum skriftum, stílsniðum eða kóða við síður sem viðskiptavinir sjá: forsíðu, vörusíður, körfu eða greiðsluferli. Eina snerting hennar við greiðsluferlið er greiðslumátinn „Gaman.is“, sem svarar strax að hann sé ekki í boði. Hraði verslunarinnar fyrir viðskiptavini er því sá sami hvort sem viðbótin er virk eða ekki.

Þegar vörum eða lagerstöðu er breytt

Viðbótin skráir aðeins hvaða vara breyttist. Breytingum er safnað saman í 45 sekúndur og þær síðan sendar Gaman.is í einni beiðni, í bakgrunni í gegnum Action Scheduler, sama verkaröðunarkerfi og WooCommerce notar sjálft. Sá sem vistar vöru bíður aldrei eftir svari frá Gaman.is. Svari Gaman.is ekki er reynt aftur fimm mínútum síðar.

Þegar Gaman.is sækir gögn

- Vörur eru sóttar í síðum með að hámarki 50 vörum, og gögn hverrar síðu eru lesin úr gagnagrunninum í einu lagi. Að jafnaði eru aðeins sóttar vörur sem hafa breyst frá síðustu samstillingu.
- Lagerstaða rétt fyrir greiðslu er sótt fyrir eina vöru í senn og er mjög létt beiðni.
- Pantanir kosta álíka mikla vinnslu og venjuleg WooCommerce-pöntun, ein fyrir hverja sölu, auk einnar stuttrar staðfestingar hjá Gaman.is.

Stjórnborðið

Yfirlitið sækir stöðuna til Gaman.is með allt að 8 sekúndna biðtíma og geymir hana í eina mínútu. Eina skiptið sem bíða þarf lengur er þegar lykill er vistaður eða smellt á „Athuga tengingu“. Þá prófar Gaman.is tenginguna, sem tekur yfirleitt nokkrar sekúndur og aldrei meira en 60.

Mjög stórar verslanir

Þegar Gaman.is spyr hvaða vörur hafi breyst fer fyrirspurnin yfir allar vörur verslunarinnar. Í verslunum með nokkur hundruð eða nokkur þúsund vörur tekur það millisekúndur. Í verslunum með tugþúsundir vara er álagið merkjanlegt en lítið. Þeir sem vilja sannreyna þetta geta sett upp ókeypis viðbótina Query Monitor og borið saman síður verslunarinnar með og án viðbótarinnar.

10. Gögn sem viðbótin geymir

Hvar	Hvað
`wp_gaman_orders`	Tenging hverrar Gaman-pöntunar við WooCommerce-pöntun.
`wp_gaman_lines`	Lagerlækkun hverrar pöntunarlínu og hvort hún hafi verið sett til baka.
`wp_gaman_nonces`	Auðkenni undirritaðra beiðna frá Gaman.is síðustu 10 mínútur (vörn gegn endurteknum köllum).
`wp_gaman_log`	Aðgerðaskrá: tími, aðgerð, pöntunarnúmer Gaman.is og niðurstaða. Geymd í 90 daga.
`gaman_connect_settings`	Lykill og stillingar viðbótarinnar, auðkenni verslunarinnar og opinberir lyklar Gaman.is.

`gaman_connect_last_read`	Hvenær Gaman.is las síðast vörur eða flokka (sýnt sem „Síðast samstillt“).
Lýsigögn vara	`_gaman_updated_at` (hvenær vara breyttist síðast) og `_gaman_vat_rate` ef sérstakt VSK-þrep hefur verið valið fyrir Gaman.is.
Lýsigögn pantana	Pöntunarnúmer Gaman.is, útgreiðsla, þóknun, kortagjald, sendingarmáti og upplýsingar um kaupanda vegna afhendingar.

Töfluheitin eru sýnd með sjálfgefnu forskeyti WordPress, `wp_`. Á sumum vefjum er forskeytið annað.

11. Aftenging, óvirkjun og eyðing

- **„Aftengja Gaman.is“ í WordPress.** Viðbótin lætur Gaman.is vita, lokar öllum endapunktum strax og eyðir lyklinum. Vörurnar hverfa af Gaman.is þar til verslunin tengist aftur með nýjum lykli.
- **Óvirkjun.** Viðbótin hættir að eiga samskipti við Gaman.is og áætluð verk hennar eru fjarlægð. Gögn hennar haldast ef hún er virkjuð aftur.
- **Eyðing.** Lykill, stillingar, áætluð verk, töflur viðbótarinnar og lýsigögn hennar á vörum eru fjarlægð. WooCommerce-pantanir og tilvísanir þeirra í Gaman.is haldast, enda þarf bókhaldið á þeim að halda.
- **Aftenging á Gaman.is.** Lykillinn er ógiltur hjá Gaman.is og vörurnar teknar úr sölu þar. Viðbótin slekkur þá á sér sjálf.
- Persónuverndartól WooCommerce (Erase personal data) fjarlægja einnig þær upplýsingar um kaupendur sem viðbótin geymir á Gaman-pöntunum.

12. Breytt vefslóð

Ef tengd verslun skráir sig hjá Gaman.is frá annarri vefslóð en áður breytist ekkert strax. Breytingin bíður þar til bæði eigandi verslunarinnar (með tengli sem sendur er í tölvupósti) og stjórnandi Gaman.is hafa samþykkt hana. Fram að því heldur Gaman.is áfram að nota gömlu slóðina.

13. Ef lykill kæmist í rangar hendur

Lykill viðbótarinnar (gmn_...), t.d. ef WordPress-vefurinn væri brotinn

Lykillinn dugar aðeins í köll frá versluninni til Gaman.is. Með honum væri hægt að láta Gaman.is vita af breytingum (Gaman.is sækir þá gögnin sjálft á skráða slóð verslunarinnar), sjá stöðu verslunarinnar og opna flokkun og sendingarstillingar hennar á Gaman.is.

Með honum væri **ekki** hægt að kalla á endapunkta verslunarinnar, lækka lager, stofna pantanir, lesa viðskiptavini eða pantanir, eða flytja tenginguna á aðra vefslóð án samþykkis eiganda og Gaman.is. Úrræði: búa til nýjan lykil á Gaman.is; sá gamli hættir strax að virka.

Undirritunarlykill Gaman.is, ef brotist væri inn hjá Gaman.is

Með honum væri hægt að lesa birtar vörur, flokka og lager, sömu upplýsingar og verslunin birtir sjálf. Ekki væri hægt að lækka lager eða stofna pantanir nema pöntunin sé til, greidd og fyrir þessa verslun hjá Gaman.is, því viðbótin staðfestir hverja pöntun sjálf á fastri slóð. Aldrei væri hægt að breyta verðum,

vörum eða stillingum, lesa viðskiptavini eða aðrar pantanir, eða stofna fleiri en 20 nýjar pantanir á klukkustund.

Næði árásaraðili bæði undirritunarlyklinum og gagnagrunni Gaman.is gæti hann skráð falsaðar Gaman-pantanir og lækkað lager vegna þeirra, en aldrei fleiri en 20 pantanir á klukkustund. Þær væru alltaf merktar Gaman.is og sjáanlegar í Aðgerðaskrá.

Úrræði: Gaman.is getur skipt um undirritunarlykil og ógilt alla lykla allra verslana strax (neyðarlokun tenginga). Verslunin getur sjálf smellt á „Aftengja Gaman.is“ hvenær sem er.

14. Kóði og uppfærslur

- Viðbótin keyrir engan kóða sem sóttur er af netinu, notar hvorki `eval` né torræðan (obfuscated) kóða, hleður engum skrám niður og hefur ekkert eigið uppfærslukerfi. Nýjasta útgáfan er alltaf á `https://gaman.is/downloads/gaman-connect.zip`.
- Uppfærsla: Viðbætur → Bæta við → Hlaða upp viðbót → veldu nýju skrána → „Skipta út núverandi útgáfu“. Lykillinn og tengingin haldast.
- Í haus viðbótarinnar er skilgreint `Update URI`, svo WordPress býður aldrei upp á aðra viðbót með sama heiti sem uppfærslu.
- Allar fyrirspurnir í gagnagrunn sem innihalda breytur fara í gegnum `$wpdb->prepare()`, og engin skrá viðbótarinnar keyrir ef hún er opnuð beint utan WordPress.
- Í útgáfu 0.5.0 bættust við undirrituð köll, staðfesting pantana, hámark á nýjar pantanir, Aðgerðaskrá og „Aftengja Gaman.is“. Útgáfa 0.5.1 breytir aðeins síðunni í WordPress; öryggi, undirritun og endapunktar eru óbreytt.

15. Kröfur

WordPress 6.2 eða nýrra, PHP 7.4 eða nýrra og WooCommerce 7.0 eða nýrra (prófað með útgáfu 9.4). Viðbótin styður nýju pantanatöflurnar í WooCommerce (HPOS). Verslunin þarf að selja í íslenskum krónum og vefurinn að nota https. Ef Gaman.is nær ekki sambandi: leyfðu beiðnir á `/wp-json/gaman/v1/` í Cloudflare eða öryggisviðbót.

16. Persónuupplýsingar

Verslunin fær aðeins þær upplýsingar um kaupendur á Gaman.is sem þarf til að afgreiða og afhenda pöntun. Gaman.is fær engar upplýsingar um viðskiptavini verslunarinnar sjálfrar. Nánar er fjallað um meðferð persónuupplýsinga á `gaman.is/personuvernd`.

Tilkynningar um öryggisgalla

Telji einhver sig hafa fundið öryggisgalla í viðbótinni eða í tengingunni við Gaman.is biðjum við um að hann sé tilkynntur á sala@gaman.is áður en sagt er frá honum opinberlega. Við svörum innan tveggja virkra daga.

Gaman.is tenging 0.5.1 · Áfram með Smjörið ehf., kt. 430910-2130 · gaman.is