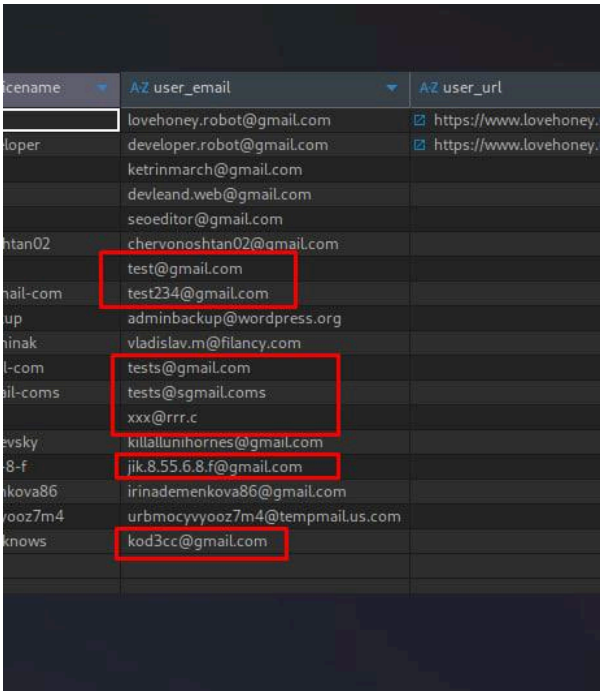
16_09_2025

1. К сожалению Access логов за июнь/июль/август их нет. Только за сентябрь начиная с 7 числа. Так что к сожалению точку входа (загрузку плагина wp-compat) невозможно определить.
2. Но есть debug.log начиная с 27 мая, на котором видно что 06.07 начал вызывать ошибки вредоносный плагин wp-compat

```
[06-Jul-2025 06:25:46 UTC] PHP Notice:  Trying to access array offset on value of type null in /home3/lovehon5/public_html/wp-content/plugins/wp-compat/wp-compat.php on line 25
```

   Так как есть информация, что переезд на другой сервер был после этого числа, скорее всего вредоносные плагины притащили на новый сервер

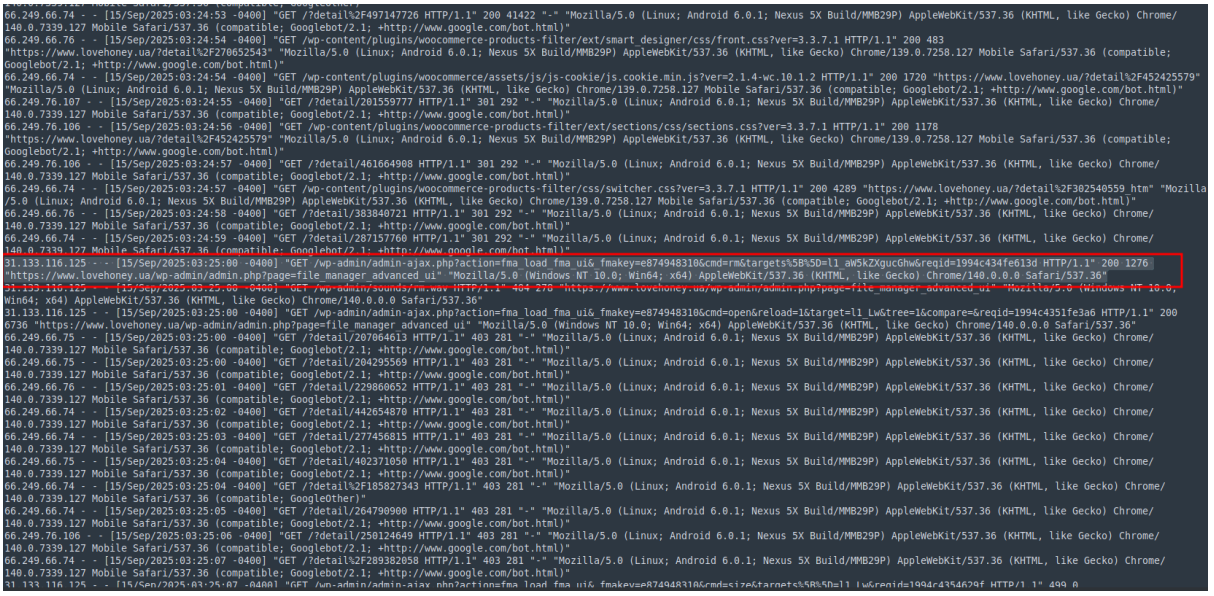
3. Удалили юзеров в БД
   Тут в скриншоте еще не отмечен юзер adminbackup@wordpress.org - Тоже удалили



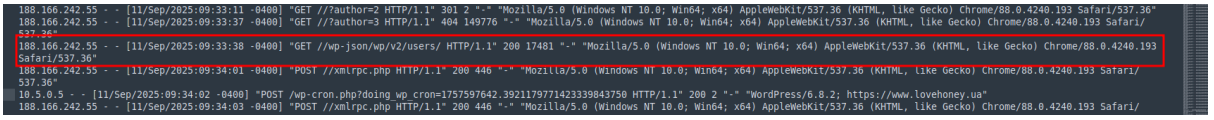
4. 

   видны уже признаки заражения, тут странные запросы, хоть IP принадлежат и **Googlebot** все равно какой-то мусорный контент которые уже индексируются
5. Удалили вредоносный файл `wp-confiig.php` был создан 12 числа. Удалили wp-compact-1 - вредоносный плагин. Восстановили index.php в корне сайта

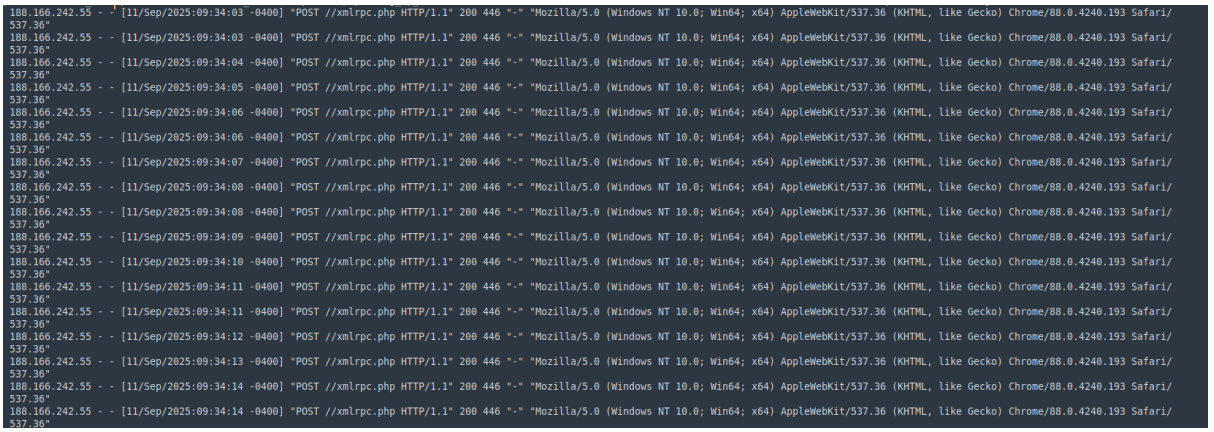
6. 15 сентября в 03:25 был удален файл index.php через GET запрос плагина File-Manager-Advanced



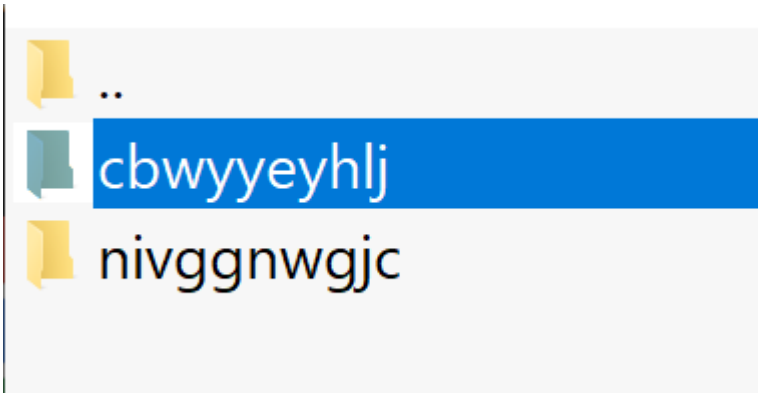
7. 11 сентября в 09:34 судя по логам получили список юзеров вордпресс



После этого предположительно начали перебор паролей через xmlrpc.php

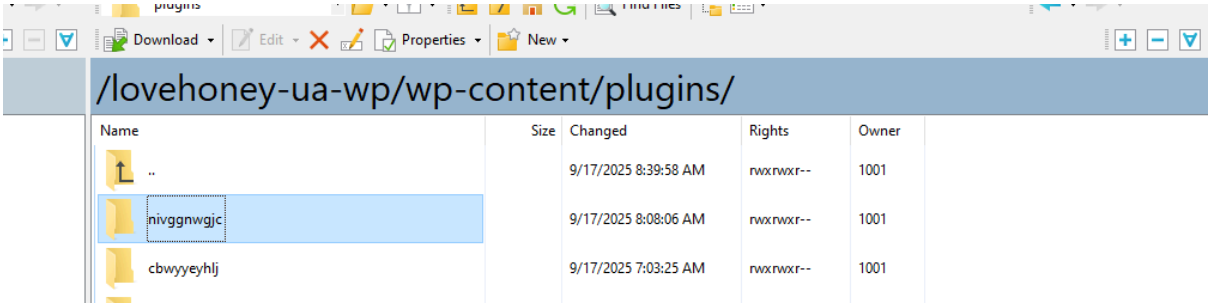


17_09_2025



———————

Удалили вредоносные плагины

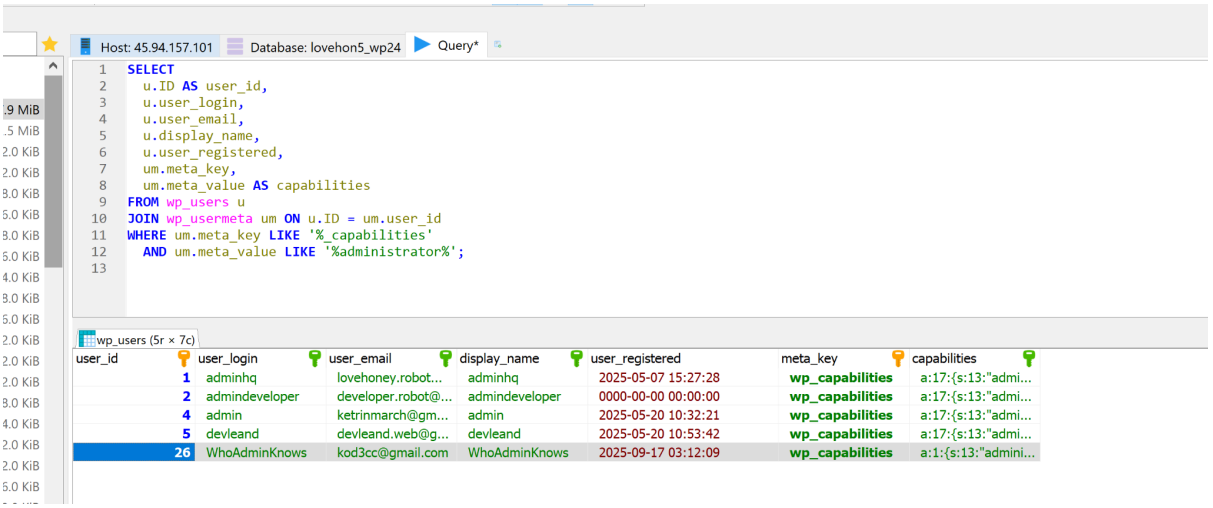


sudo rm -rf /var/www/lovehoney-ua-wp/wp-content/plugins/cbwyyyeyhlj /var/www/lovehoney-ua-wp/wp-content/plugins/nivggnwgjc

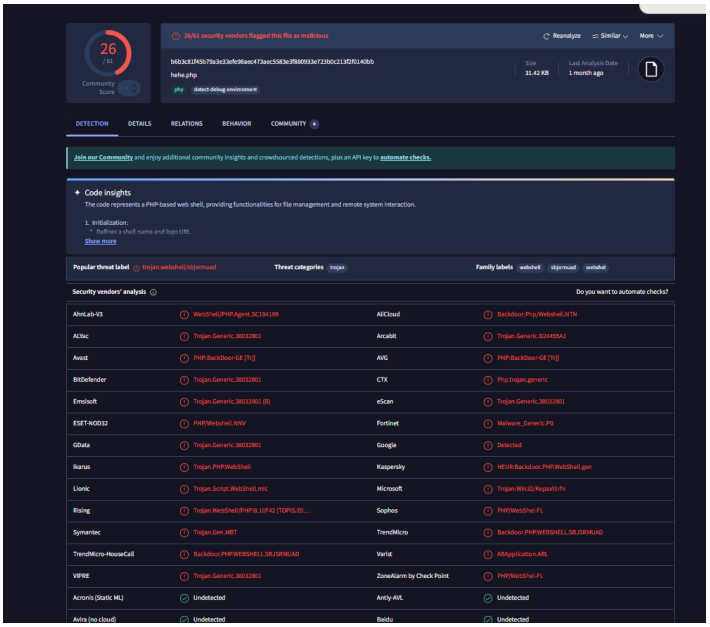
```
[root@hqua0244839 plugins]# ls -la
total 148
drwxr-xr-x 35 deploy wpdev 4096 Sep 17 07:08 .
drwxr-xr-x 10 deploy wpdev 4096 Sep 17 06:12 ..
drwxr-xr-x  5 deploy wpdev 4096 Sep 17 06:12 acf-extended
drwxr-xr-x  7 deploy wpdev 4096 Sep 17 06:12 acfml
drwxr-xr-x  7 deploy wpdev 4096 Sep 17 06:12 advanced-custom-fields
drwxr-xr-x  8 deploy wpdev 4096 Sep 17 06:12 advanced-custom-fields-pro-main
drwxr-xr-x  4 deploy wpdev 4096 Sep 16 10:40 akismet
drwxr-xr-x  2 deploy wpdev 4096 Sep 17 06:12 cbwyyyeyhlj
drwxr-xr-x  9 deploy wpdev 4096 Sep 17 06:12 chaty
drwxr-xr-x  4 deploy wpdev 4096 Sep 17 06:12 classic-editor
drwxr-xr-x  7 deploy wpdev 4096 Sep 17 06:12 cyrlitera
-r--r--r--  1 deploy wpdev  127 Sep 17 06:12 .htaccess
-rwxrwxr--  1 deploy wpdev   28 Sep 16 10:40 index.php
drwxr-xr-x  5 deploy wpdev 4096 Sep 17 06:12 index-wp-mysql-for-speed
drwxr-xr-x  7 deploy wpdev 4096 Sep 17 06:12 loco-translate
drwxr-xr-x 11 deploy wpdev 4096 Sep 17 06:12 members
drwxr-xr-x  6 deploy wpdev 4096 Sep 17 06:12 miniorange-login-openid
drwxr-xr-x  7 deploy wpdev 4096 Sep 17 06:12 mrkv-liqpay-extended
drwxr-xr-x  2 deploy wpdev 4096 Sep 17 06:12 nivggnwgjc
drwxr-xr-x 10 deploy wpdev 4096 Sep 17 06:12 post-thumbnail-editor-master
drwxr-xr-x 10 deploy wpdev 4096 Sep 17 06:12 query-monitor
drwxr-xr-x  6 deploy wpdev 4096 Sep 17 06:12 redux-framework
drwxr-xr-x  6 deploy wpdev 4096 Sep 17 06:12 regenerate-thumbnails
drwxr-xr-x  4 deploy wpdev 4096 Sep 17 06:12 simple-custom-post-order
drwxr-xr-x 16 deploy wpdev 4096 Sep 17 06:12 sitepress-multilingual-cms
drwxr-xr-x 11 deploy wpdev 4096 Sep 17 06:12 svg-support
drwxr-xr-x  7 deploy wpdev 4096 Sep 17 06:12 taxonomy-terms-order
drwxr-xr-x 11 deploy wpdev 4096 Sep 17 06:12 ti-woocommerce-wishlist
drwxr-xr-x  5 deploy wpdev 4096 Sep 17 06:12 upload-svg
drwxr-xr-x  7 deploy wpdev 4096 Sep 17 06:12 woo-checkout-field-editor-pro
drwxr-xr-x 12 deploy wpdev 4096 Sep 17 06:12 woocommerce
drwxr-xr-x 11 deploy wpdev 4096 Sep 17 06:12 woocommerce-multilingual
drwxr-xr-x 12 deploy wpdev 4096 Sep 17 06:12 woocommerce-products-filter
drwxr-xr-x  7 deploy wpdev 4096 Sep 17 06:12 woo-product-gallery-slider
drwxr-xr-x  6 deploy wpdev 4096 Sep 17 06:12 woo-variation-swatches
drwxr-xr-x 13 deploy wpdev 4096 Sep 17 06:12 wordpress-seo
drwxr-xr-x 11 deploy wpdev 4096 Sep 17 06:12 wpml-string-translation
[root@hqua0244839 plugins]#  rm -rf /var/www/lovehoney-ua-wp/wp-content/plugins/cbwyyyeyhlj /var/www/lovehoney-ua-wp/wp-content/plugins/nivggnwgjc
```

удалили плагины 2шт .(cbwyyyeyhlj и nivggnwgjc) руками физически

БД удалили вредоносного пользователя (Админа) из БД

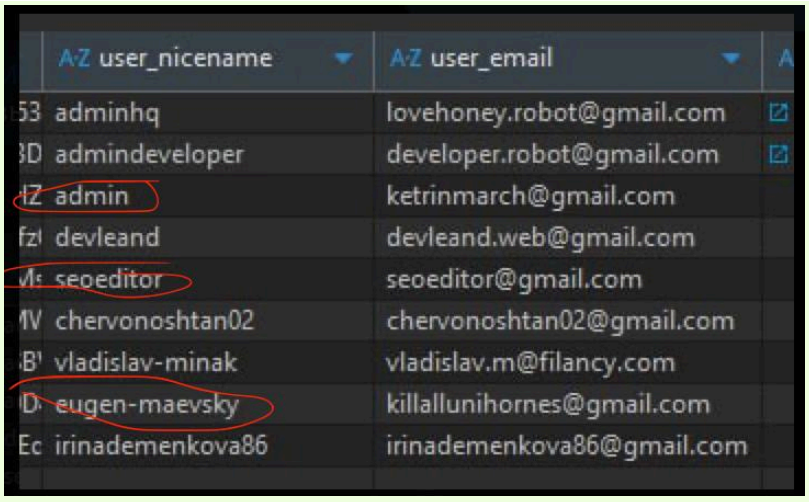


короткое описание кода плагинов: PHP веб-оболочка (web shell), предназначенная для удалённого управления сервером. Поддерживает функции навигации по файлам, загрузки/удаления/создания/редактирования файлов и их прав, выполнения системных команд, обхода отключённых функций PHP, получения информации о системе и пользователях. Использует обфускацию через шестнадцатеричное кодирование имен функций. Имеет веб-интерфейс. Также реализована возможность скачивания файлов и скачивания из внешних серверов и их запуском.



https://www.virustotal.com/gui/file/b6b3c81f45b79a3e33efe98aec473aec5583e3f880933e723b0c213f2f0140bb/detection

спросили по поводу пользывателей и оставили только нужных



user_nicename	user_email
adminhq	lovehoney.robot@gmail.com
admindeveloper	developer.robot@gmail.com
admin	ketrinmarch@gmail.com
devleand	devleand.web@gmail.com
seoeditor	seoeditor@gmail.com
chervonoshtan02	chervonoshtan02@gmail.com
vladislav-minak	vladislav.m@filancy.com
eugen-maevsky	killallunihornes@gmail.com
irinademenkova86	irinademenkova86@gmail.com

Было

```
SELECT
  u.ID,
  u.user_login,
  u.user_registered,
  CASE
    WHEN um.meta_value LIKE '%administrator%' THEN 'admin'
    ELSE 'not admin'
  END AS role_status
FROM lovehon5_wp24.wp_users u
LEFT JOIN lovehon5_wp24.wp_usermeta um
  ON u.ID = um.user_id
  AND um.meta_key = 'wp_capabilities';
```

wp_users (9r × 4c)

ID	user_login	user_registered	role_status
2	admindeveloper	0000-00-00 00:00:00	admin
1	adminhq	2025-05-07 15:27:28	admin
4	admin	2025-05-20 10:32:21	admin
5	devleand	2025-05-20 10:53:42	admin
6	SeoEditor	2025-06-02 10:38:16	not admin
13	chervonoshtan02	2025-06-16 12:48:03	not admin
17	Vladislav-Minak	2025-08-20 09:57:26	not admin
21	Eugen-Maevsky	2025-08-27 06:36:58	not admin
23	irinademenkova86	2025-09-05 04:58:25	not admin

Оставили только пользователей

15

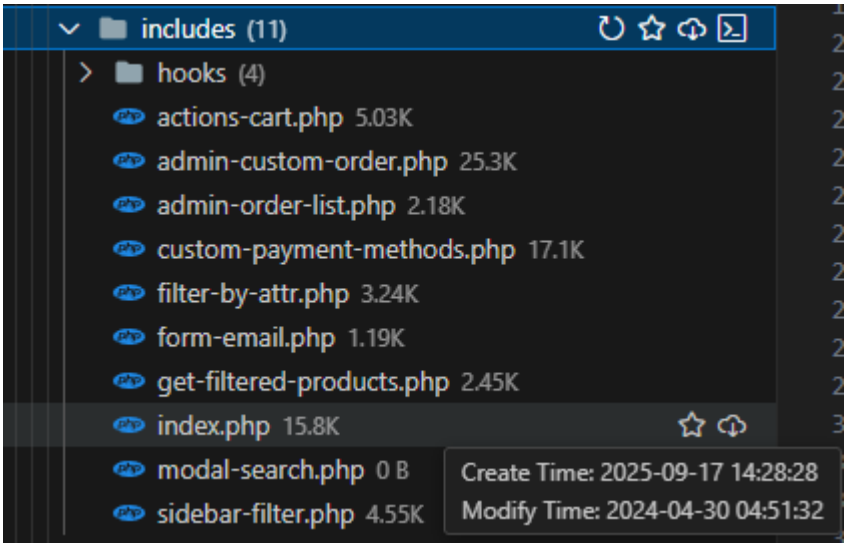
wp_users (4r × 4c)

ID	user_login	user_registered	role_status
2	admindeveloper	0000-00-00 00:00...	admin
4	admin	2025-05-20 10:32...	admin
6	SeoEditor	2025-06-02 10:38...	not admin
21	Eugen-Maevsky	2025-08-27 06:36...	not admin

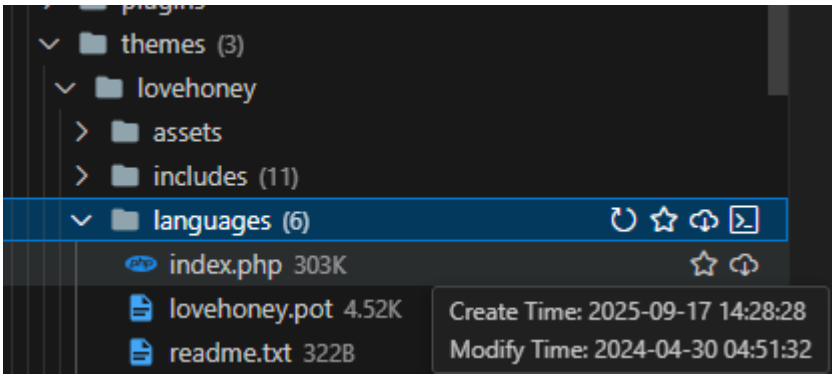
удалили пользователей и их метаданные
DELETE FROM lovehon5_wp24.wp_usermeta
WHERE user_id NOT IN (2, 21, 6, 4);

```
DELETE FROM lovehon5_wp24.wp_users
WHERE ID NOT IN (2, 21, 6, 4);
```

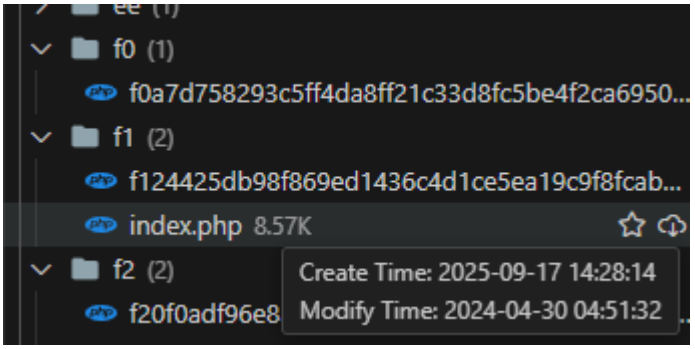
1. /lovehoney-ua-wp/wp-content/themes/lovehoney/includes



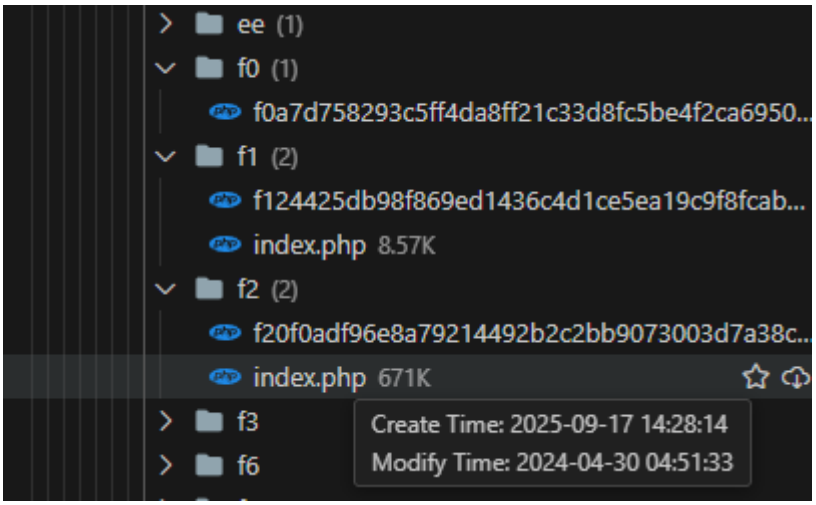
2. /lovehoney-ua-wp/wp-content/themes/lovehoney/languages



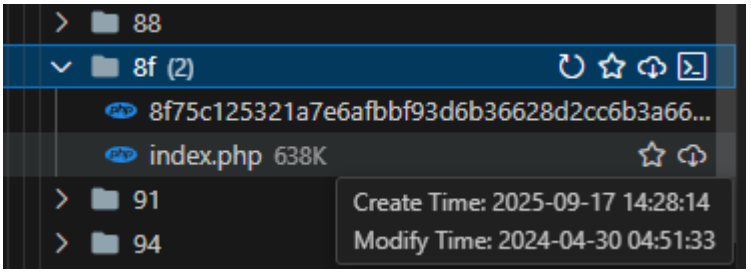
3. /lovehoney-ua-wp/wp-content/uploads/cache/wpml/twig/f1



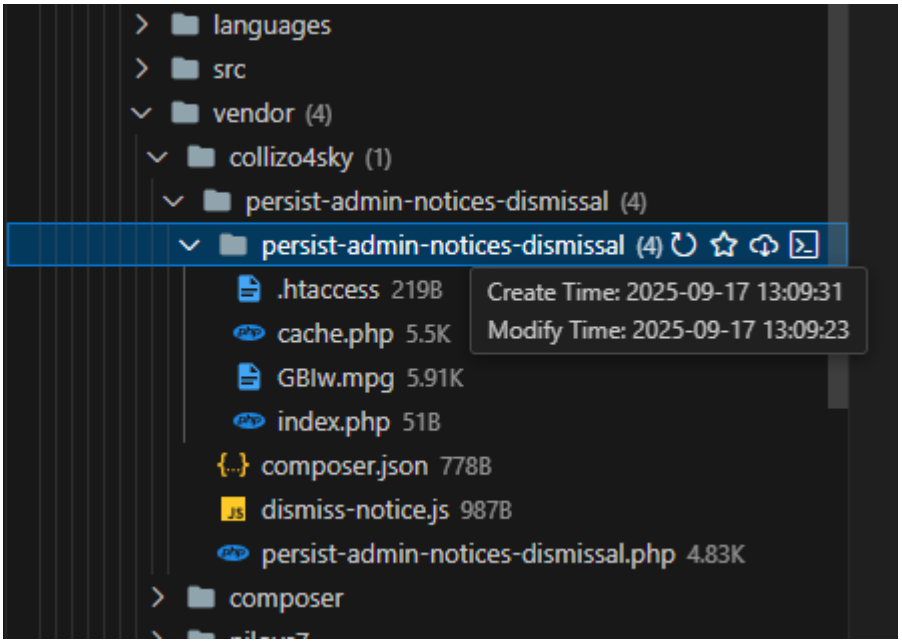
4. /lovehoney-ua-wp/wp-content/uploads/cache/wpml/twig/f2



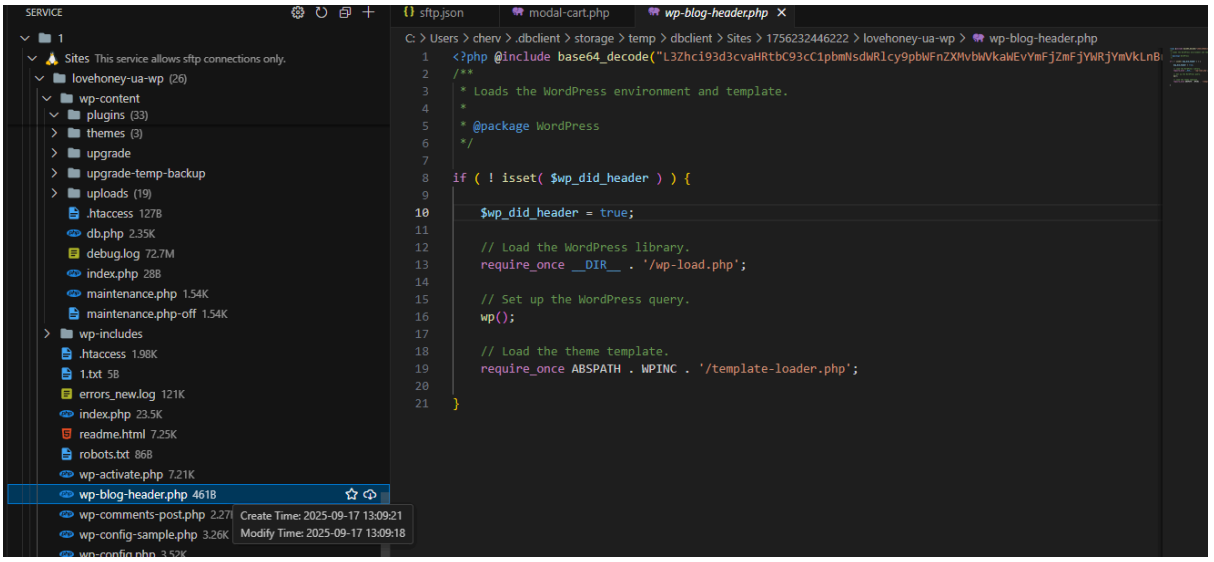
5. /lovehoney-ua-wp/wp-content/uploads/cache/wpml/twig/8f



6. /lovehoney-ua-wp/wp-content/plugins/woo-product-gallery-slider/vendor/collizo4sky/persist-admin-notices-dismissal/persist-admin-notices-dismissal

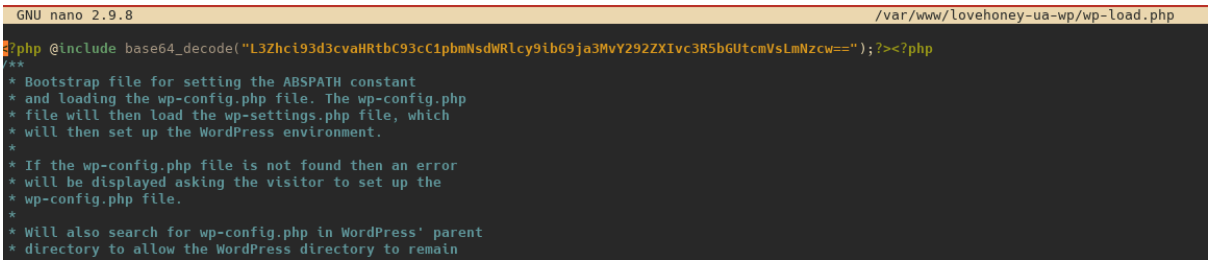


7. /lovehoney-ua-wp/wp-blog-header.php



8. очищен файл /lovehoney-ua-wp/index.php

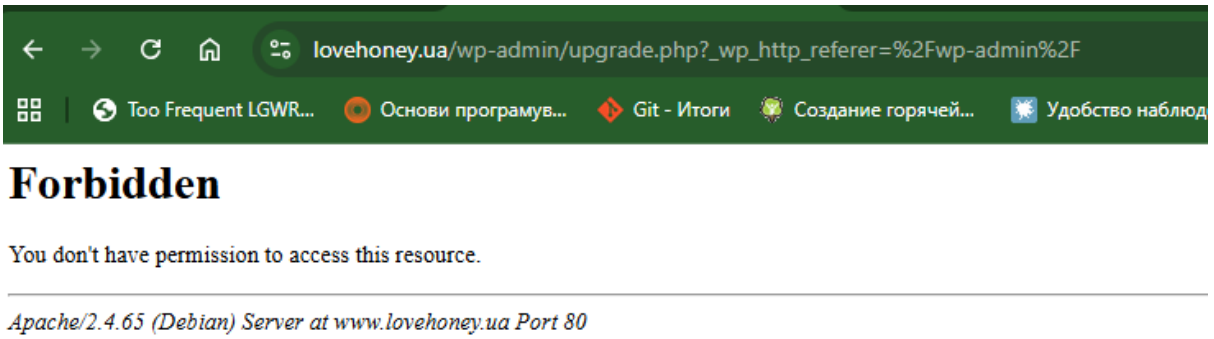
9. очищен файл /lovehoney-ua-wp/wp-load.php



10. wp-admin
    (no teg ?>)

Warning: Cannot modify header information - headers already sent by (output started at /var/www/html/wp-content/themes/lovehoney/includes/admin-order-list.php:59) in /var/www/html/wp-includes/pluggable.php on line 1450 Warning: Cannot modify header information - headers already sent by (output started at /var/www/html/wp-content/themes/lovehoney/includes/admin-order-list.php:59) in /var/www/html/wp-includes/pluggable.php on line 1453

11)



Файл upgrade.php существует и валиден
Ошибка 403 идёт от nginx/Apache
Блокировка идёт из .htaccess
Решение: добавить upgrade.php в белый список

—-

—-

```
[root@hqua0244839 ~]# sudo systemctl reload apache2
Failed to reload apache2.service: Unit apache2.service not found.
[root@hqua0244839 ~]# ps aux | grep nginx
root       51816  0.0  0.0 129564  1300 ?        Ss   Aug27   0:00 nginx: master process /usr/sbin/nginx
nginx      51817  0.0  0.3 164236 18088 ?        S    Aug27   8:46 nginx: worker process
nginx      51818  0.0  0.2 163500 14576 ?        S    Aug27   0:01 nginx: worker process
nginx      51819  0.0  0.2 163228 17468 ?        S    Aug27   0:06 nginx: worker process
root      523615  0.0  0.0 221928  1152 pts/4    S+   15:33   0:00 grep --color=auto nginx
[root@hqua0244839 ~]# ps aux | grep apache
root      422522  0.0  0.7 264812 42496 ?        Ss   09:37   0:01 apache2 -DFOREGROUND
deploy    422565  0.0  1.1 344752 68620 ?        S    09:37   0:07 apache2 -DFOREGROUND
deploy    422566  0.0  1.1 343432 68092 ?        S    09:37   0:08 apache2 -DFOREGROUND
deploy    422567  0.0  1.4 355600 88308 ?        S    09:37   0:08 apache2 -DFOREGROUND
deploy    422568  0.0  1.1 344648 69004 ?        S    09:37   0:07 apache2 -DFOREGROUND
deploy    422569  0.0  1.2 344632 71628 ?        S    09:37   0:08 apache2 -DFOREGROUND
deploy    422571  0.0  1.1 344628 68380 ?        S    09:37   0:07 apache2 -DFOREGROUND
deploy    422889  0.0  1.1 344688 69732 ?        S    09:46   0:07 apache2 -DFOREGROUND
deploy    425551  0.0  1.4 356056 86196 ?        S    10:54   0:06 apache2 -DFOREGROUND
root      523617  0.0  0.0 221928  1152 pts/4    S+   15:33   0:00 grep --color=auto apache
[root@hqua0244839 ~]# sudo systemctl status httpd
Unit httpd.service could not be found.
[root@hqua0244839 ~]# docker ps
CONTAINER ID   IMAGE                          COMMAND                  CREATED       STATUS       PORTS
   NAMES
911ee08afa38   lovehoney-ua-wp-deploy-app   "docker-entrypoint.s…"   6 hours ago   Up 6 hours   127.0.0.1:8000->80/tcp
   lovehoney-ua-wp-deploy-app-1
[root@hqua0244839 ~]#
```

———

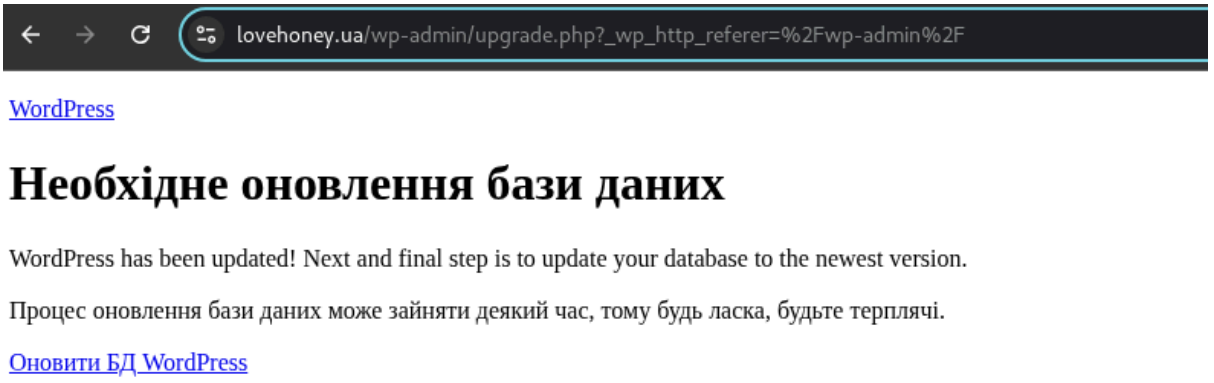
```
[root@hqua0244839 ~]# docker ps
CONTAINER ID   IMAGE                          COMMAND                  CREATED       STATUS       PORTS
   NAMES
911ee08afa38   lovehoney-ua-wp-deploy-app   "docker-entrypoint.s…"   6 hours ago   Up 6 hours   127.0.0.1:8000->80/tcp
   lovehoney-ua-wp-deploy-app-1
[root@hqua0244839 ~]# docker exec -it lovehoney-ua-wp-deploy-app-1 bash
root@911ee08afa38:/var/www/html# ps aux | grep apache
root           1  0.0  0.7 264812 42496 ?        Ss   13:37   0:01 apache2 -DFOREGROUND
www-data      19  0.0  1.1 344752 68620 ?        S    13:37   0:07 apache2 -DFOREGROUND
www-data      20  0.0  1.1 345480 70140 ?        S    13:37   0:08 apache2 -DFOREGROUND
www-data      21  0.0  1.4 355600 88308 ?        S    13:37   0:08 apache2 -DFOREGROUND
www-data      22  0.0  1.1 344648 69004 ?        S    13:37   0:07 apache2 -DFOREGROUND
www-data      23  0.0  1.2 344632 71628 ?        S    13:37   0:08 apache2 -DFOREGROUND
www-data      25  0.0  1.1 344628 68380 ?        S    13:37   0:07 apache2 -DFOREGROUND
www-data     193  0.0  1.1 344688 69732 ?        S    13:46   0:07 apache2 -DFOREGROUND
www-data    1552  0.0  1.4 356056 86196 ?        S    14:54   0:06 apache2 -DFOREGROUND
root        7034  0.0  0.0   3508  1716 pts/0    S+   19:37   0:00 grep apache
root@911ee08afa38:/var/www/html# ps aux | grep httpd
root        7036  0.0  0.0   3508  1708 pts/0    S+   19:37   0:00 grep httpd
root@911ee08afa38:/var/www/html# apache2ctl -k restart
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 10.5.0.5. Set the 'Serv
erName' directive globally to suppress this message
[root@hqua0244839 ~]# curl -I http://localhost
HTTP/1.1 200 OK
Server: nginx/1.14.1
Date: Wed, 17 Sep 2025 19:38:53 GMT
Content-Type: text/html
Content-Length: 4057
Last-Modified: Mon, 07 Oct 2019 21:16:24 GMT
Connection: keep-alive
ETag: "5d9bab28-fd9"
Accept-Ranges: bytes
```

```
[root@hqua0244839 ~]# curl -I http://127.0.0.1:8000
HTTP/1.1 200 OK
Date: Wed, 17 Sep 2025 19:40:29 GMT
Server: Apache/2.4.65 (Debian)
X-Powered-By: PHP/8.1.33
Content-Type: text/html; charset=UTF-8
```

[root@hqua0244839 ~]# sudo nginx -s reload

Исправили ошибку правкой .htaccess

Стало так



WordPress

Помилка бази даних WordPress: [Multiple primary key defined]
`ALTER TABLE wp_usermeta ADD PRIMARY KEY (`umeta_id`)`

Помилка бази даних WordPress: [Duplicate key name 'meta_key']
`ALTER TABLE wp_usermeta ADD KEY `meta_key` (`meta_key`(191))`

Помилка бази даних WordPress: [Multiple primary key defined]
`ALTER TABLE wp_termmeta ADD PRIMARY KEY (`meta_id`)`

Помилка бази даних WordPress: [Duplicate key name 'meta_key']
`ALTER TABLE wp_termmeta ADD KEY `meta_key` (`meta_key`(191))`

Помилка бази даних WordPress: [Multiple primary key defined]
`ALTER TABLE wp_commentmeta ADD PRIMARY KEY (`meta_id`)`

Помилка бази даних WordPress: [Duplicate key name 'comment_id']
`ALTER TABLE wp_commentmeta ADD KEY `comment_id` (`comment_id`)`

Помилка бази даних WordPress: [Multiple primary key defined]
`ALTER TABLE wp_comments ADD PRIMARY KEY (`comment_ID`)`

Помилка бази даних WordPress: [Duplicate key name 'comment_approved_date_gmt']
`ALTER TABLE wp_comments ADD KEY `comment_approved_date_gmt` (`comment_approved`,`comment_date_gmt`)`

Помилка бази даних WordPress: [Duplicate key name 'comment_date_gmt']
`ALTER TABLE wp_comments ADD KEY `comment_date_gmt` (`comment_date_gmt`)`

Помилка бази даних WordPress: [Duplicate key name 'comment_parent']
`ALTER TABLE wp_comments ADD KEY `comment_parent` (`comment_parent`)`

Помилка бази даних WordPress: [Duplicate key name 'comment_author_email']
`ALTER TABLE wp_comments ADD KEY `comment_author_email` (`comment_author_email`(10))`

Помилка бази даних WordPress: [Multiple primary key defined]
`ALTER TABLE wp_options ADD PRIMARY KEY (`option_id`)`

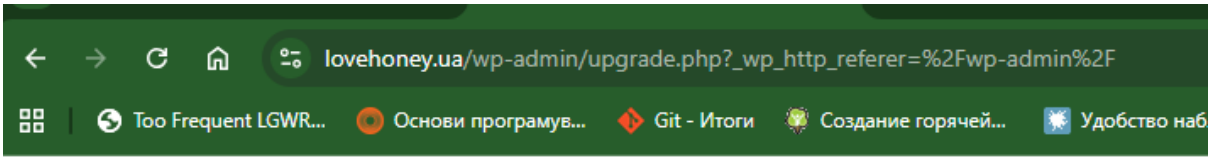
Помилка бази даних WordPress: [Multiple primary key defined]
`ALTER TABLE wp_postmeta ADD PRIMARY KEY (`meta_id`)`

Помилка бази даних WordPress: [Duplicate key name 'meta_key']
`ALTER TABLE wp_postmeta ADD KEY `meta_key` (`meta_key`(191))`

Помилка бази даних WordPress: [Duplicate key name 'type_status_date']
`ALTER TABLE wp_posts ADD KEY `type_status_date` (`post_type`,`post_status`,`post_date`,`ID`)`

Помилка бази даних WordPress: [Duplicate key name 'post_parent']
`ALTER TABLE wp_posts ADD KEY `post_parent` (`post_parent`)`

Помилка бази даних WordPress: [Duplicate key name 'post_author']
`ALTER TABLE wp_posts ADD KEY `post_author` (`post_author`)`

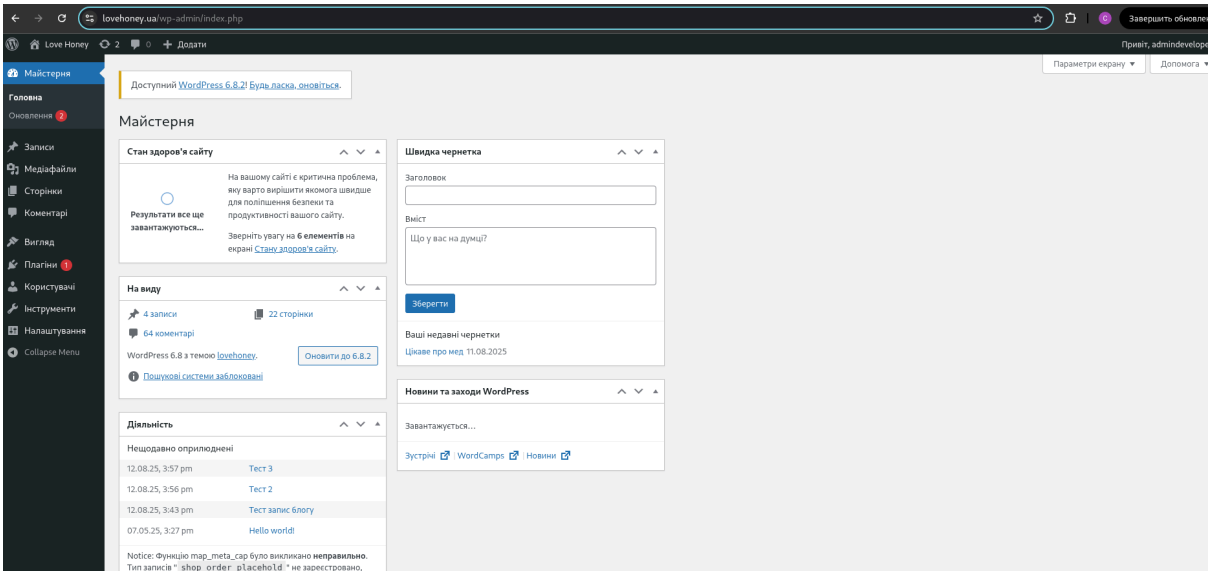


WordPress

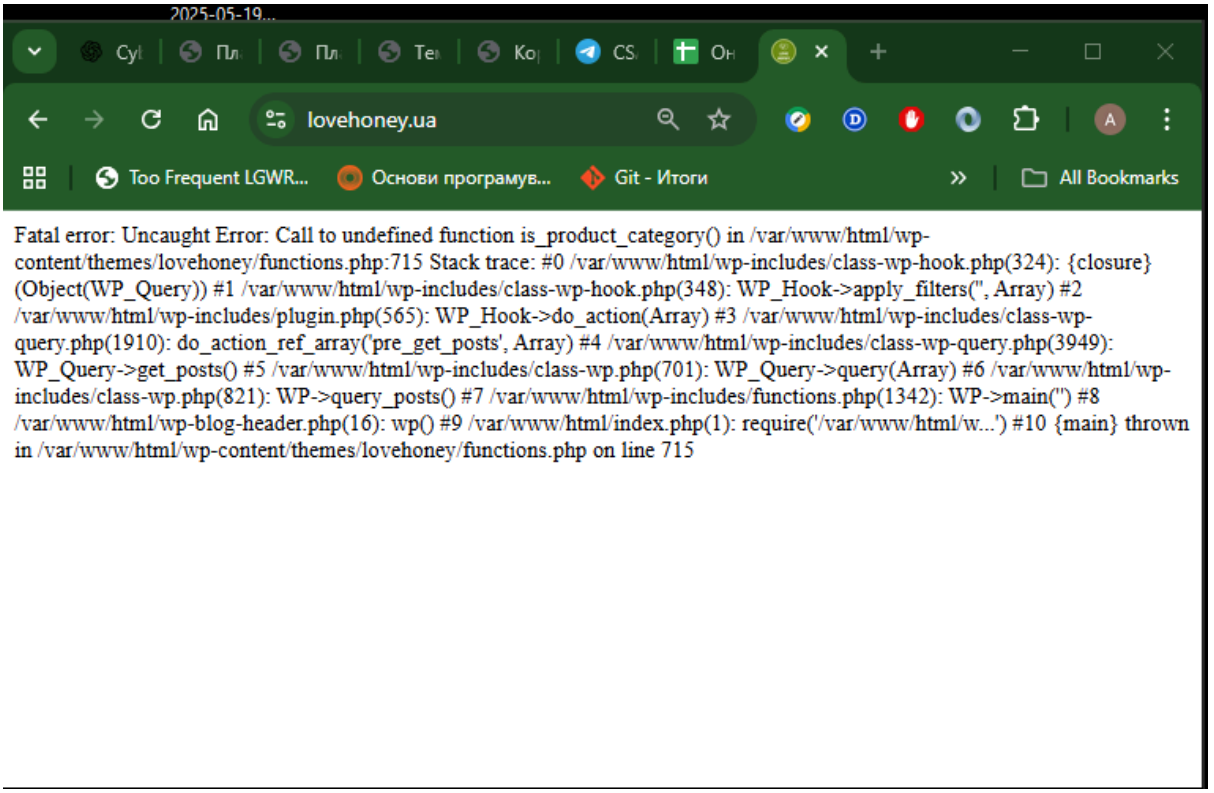
Не потребує оновлень

Ваша база даних WordPress вже оновлена!

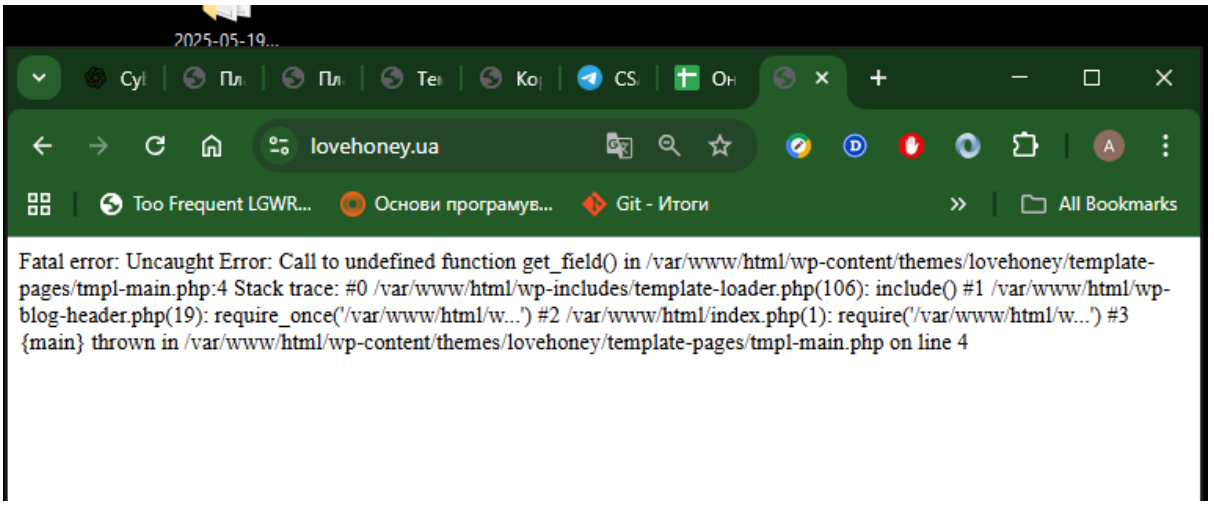
Продовжити



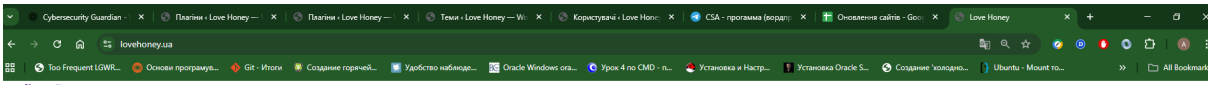
12)



исправляем
Fatal error: Uncaught Error: Call to undefined function is_product_category() in /var/www/html/wp-content/themes/lovehoney/functions.php:715
Функция is_product_category() вызывается, но она определяется только при активном плагине WooCommerce.
активируем плагин



Fatal error: Uncaught Error: Call to undefined function get_field()
Функция get_field() - это часть плагина Advanced Custom Fields (ACF). Ошибка говорит о том, что плагин не подключён или ещё не загружен, когда вызывается get_field().
активируем плагин



Warning: foreach() argument must be of type array|object, string given in /var/www/html/wp-content/themes/lovehoney/template-pages/tmpl-main.php on line 37
Warning: foreach() argument must be of type array|object, string given in /var/www/html/wp-content/themes/lovehoney/template-pages/tmpl-main.php on line 52

LOVE HONEY - СМАЧНІ, КОРИСНІ ТА КОХАНІ

shape hero shape hero lines

категорії товарів

Подарункові набори

Всі товари

LOVE HONEY- це велика сімейна пасіка, яка вироловж багатьох років займається виробництвом натуральних продуктів бджільництва

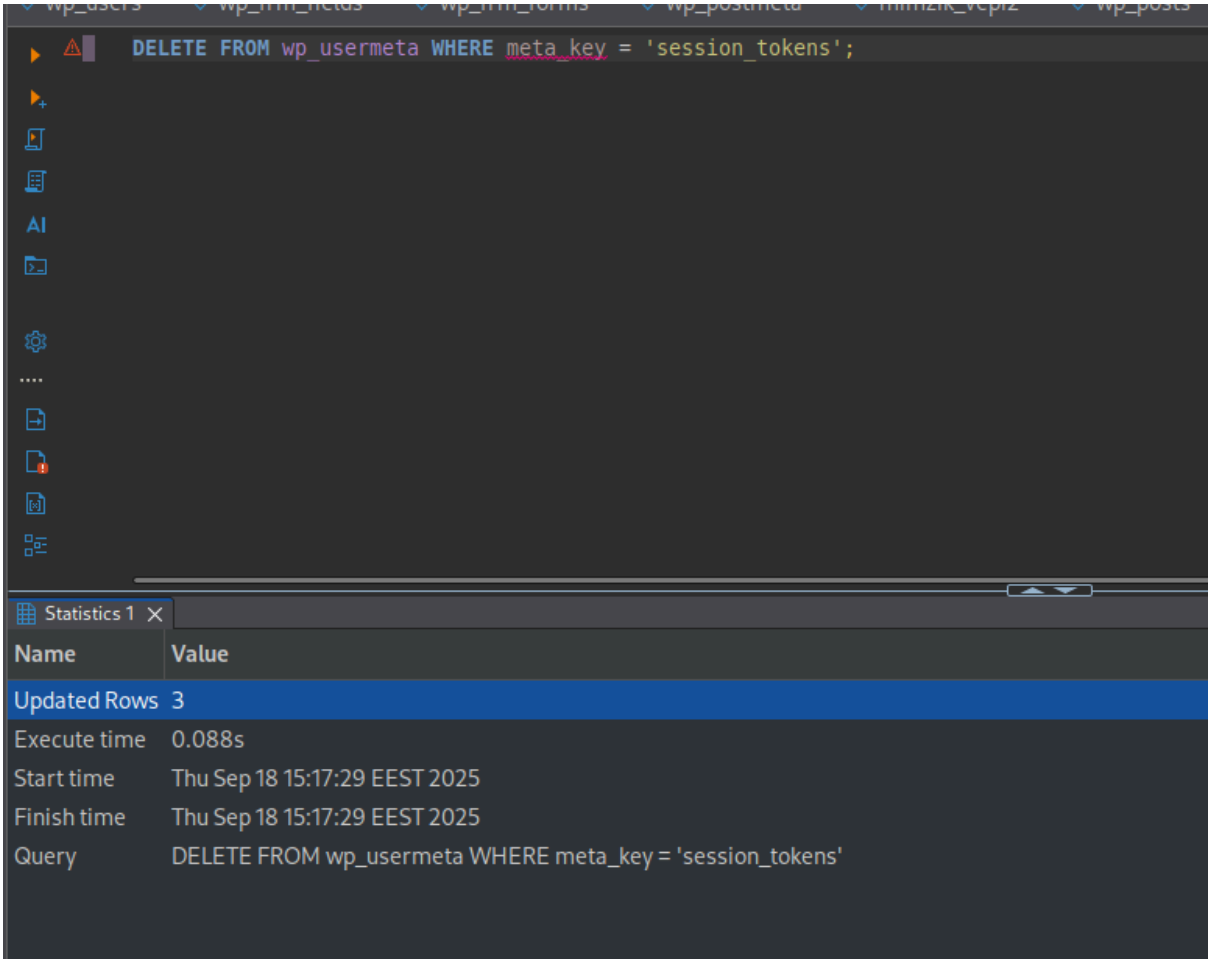
18_19_2025

1.Поправили доступа к файлам стилей, которые не подгружались

```
[root@hqua0244839 lovehoney-ua-wp]# find /var/www/lovehoney-ua-wp -type d -exec chmod 755 {} \;
[root@hqua0244839 lovehoney-ua-wp]# find /var/www/lovehoney-ua-wp -type f -exec chmod 644 {} \;
```

2.Поменяли пароли пользователей вордпресс

3.Очистили токены сессий



4.Очищены лишние файлы в uploads

```
[root@hqua0244839 uploads]# find ./ -type f -name "*.php"
./redux/custom-fonts/custom/index.php
./redux/custom-fonts/index.php
./redux/color-schemes/index.php
./redux/slides.php
./redux/media.php
./redux/index.php
./redux/social-profiles/index.php
./backup/2025/05/index.php
./backup/2025/07/index.php
./backup/2025/06/index.php
./backup/2025/index.php
./backup/index.php
./alm_templates/default.php
./sirsc-logs/index.php
[root@hqua0244839 uploads]# find . -type f \( -name "*.php" -o -name "*.phtml" -o -name "*.pl" -o -name "*.sh" \) -exec rm -f {} +
[root@hqua0244839 uploads]# find ./ -type f -name "*.php"
[root@hqua0244839 uploads]#
```

5.запрет на исполнение файловые системы поддерживают

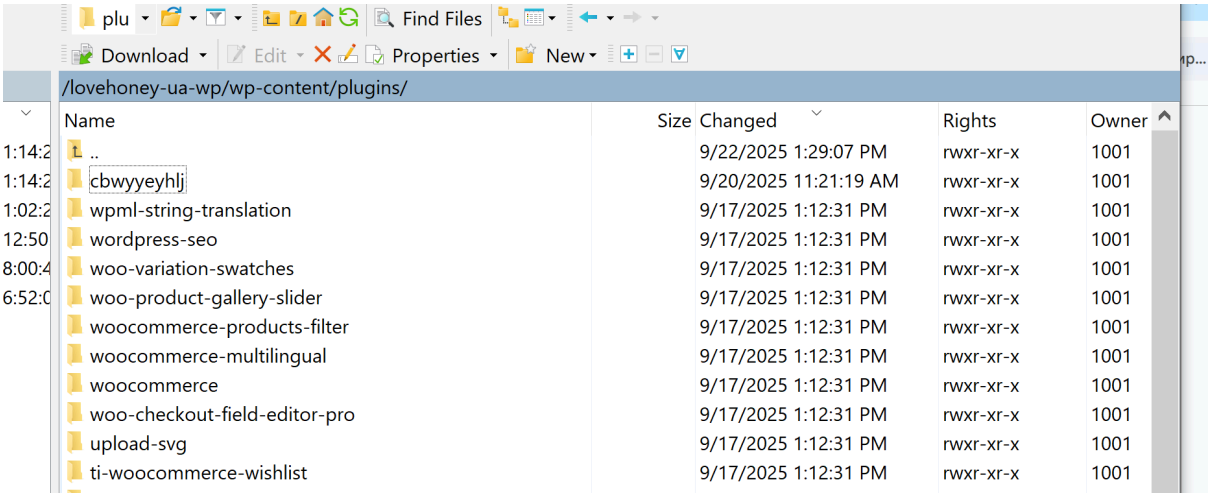
find /var/www/lovehoney-ua-wp/wp-content/uploads -type f -exec chmod a-x {} \;

```
[root@hqua0244839 uploads]# find /var/www/lovehoney-ua-wp/wp-content/uploads -type f -exec chmod a-x {} \;
```

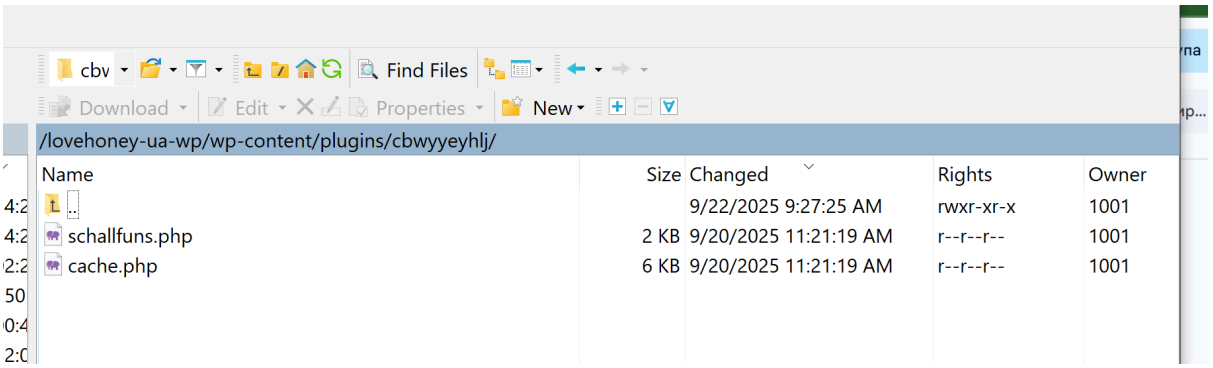
6. поменяли права на wp-config.php (640)

```
chmod: cannot access 'wp-config.php': No such file or directory
[root@hqua0244839 ~]# chmod 640 /var/www/lovehoney-ua-wp/wp-config.php
[root@hqua0244839 ~]#
```

22_09_2025



/wp-content/plugins/cbwyyeyhlj/




```
[root@hqua0244839 wp-content]# ls
db.php      index.php  maintenance      maintenance.php-off  plugins  upgrade              uploads
debug.log   languages  maintenance.php  mu-plugins           themes   upgrade-temp-backup
[root@hqua0244839 wp-content]# ls -la
total 74564
drwxr-xr-x 10 deploy wpdev     4096 Sep 22 06:41 .
drwxr-xr-x  8 deploy wpdev     4096 Sep 20 04:24 ..
-rw-r--r--  1 deploy wpdev     2403 Aug  4 06:47 db.php
-rw-r--r--  1 deploy wpdev 76201834 Sep 17 15:49 debug.log
-r--r--r--  1 deploy wpdev      127 Sep 20 04:23 .htaccess
-rw-r--r--  1 deploy wpdev       28 Sep 16 10:40 index.php
drwxr-xr-x  6 deploy wpdev    12288 Sep 17 06:12 languages
drwxr-xr-x  2 deploy wpdev     4096 Sep 17 06:12 maintenance
-rw-r--r--  1 deploy wpdev     1580 Jul 16 03:16 maintenance.php
-rw-r--r--  1 deploy wpdev     1580 May  7 12:28 maintenance.php-off
drwxr-xr-x  2 deploy wpdev     4096 Sep 18 07:33 mu-plugins
drwxr-xr-x 34 deploy wpdev     4096 Sep 22 02:27 plugins
drwxr-xr-x  3 deploy wpdev     4096 Sep 18 07:46 themes
drwxr-xr-x  2 deploy wpdev     4096 Sep 22 02:27 upgrade
drwxr-xr-x  2 deploy wpdev     4096 Sep 20 04:23 upgrade-temp-backup
drwxr-xr-x 12 deploy wpdev     4096 Sep 18 08:24 uploads
[root@hqua0244839 wp-content]# cd plugins/
```

```
[root@hqua0244839 plugins]# ls -la
total 144
drwxr-xr-x 34 deploy wpdev 4096 Sep 22 02:27 .
drwxr-xr-x 10 deploy wpdev 4096 Sep 22 06:41 ..
drwxr-xr-x  5 deploy wpdev 4096 Sep 17 06:12 acf-extended
drwxr-xr-x  7 deploy wpdev 4096 Sep 17 06:12 acfml
drwxr-xr-x  7 deploy wpdev 4096 Sep 17 06:12 advanced-custom-fields
drwxr-xr-x  8 deploy wpdev 4096 Sep 17 06:12 advanced-custom-fields-pro-main
drwxr-xr-x  4 deploy wpdev 4096 Sep 16 10:40 akismet
drwxr-xr-x  2 deploy wpdev 4096 Sep 20 04:21 cbwyyeyhlj
drwxr-xr-x  9 deploy wpdev 4096 Sep 17 06:12 chaty
drwxr-xr-x  4 deploy wpdev 4096 Sep 17 06:12 classic-editor
drwxr-xr-x  7 deploy wpdev 4096 Sep 17 06:12 cyrlitera
-r--r--r--  1 deploy wpdev  127 Sep 20 04:23 .htaccess
-rw-r--r--  1 deploy wpdev   28 Sep 16 10:40 index.php
drwxr-xr-x  5 deploy wpdev 4096 Sep 17 06:12 index-wp-mysql-for-speed
drwxr-xr-x  7 deploy wpdev 4096 Sep 17 06:12 loco-translate
drwxr-xr-x 11 deploy wpdev 4096 Sep 17 06:12 members
drwxr-xr-x  6 deploy wpdev 4096 Sep 17 06:12 miniorange-login-openid
drwxr-xr-x  7 deploy wpdev 4096 Sep 17 06:12 mrkv-liqpay-extended
drwxr-xr-x 10 deploy wpdev 4096 Sep 17 06:12 post-thumbnail-editor-master
drwxr-xr-x 10 deploy wpdev 4096 Sep 17 06:12 query-monitor
drwxr-xr-x  6 deploy wpdev 4096 Sep 17 06:12 redux-framework
drwxr-xr-x  6 deploy wpdev 4096 Sep 17 06:12 regenerate-thumbnails
drwxr-xr-x  4 deploy wpdev 4096 Sep 17 06:12 simple-custom-post-order
drwxr-xr-x 16 deploy wpdev 4096 Sep 17 06:12 sitepress-multilingual-cms
drwxr-xr-x 11 deploy wpdev 4096 Sep 17 06:12 svg-support
drwxr-xr-x  7 deploy wpdev 4096 Sep 17 06:12 taxonomy-terms-order
drwxr-xr-x 11 deploy wpdev 4096 Sep 17 06:12 ti-woocommerce-wishlist
drwxr-xr-x  5 deploy wpdev 4096 Sep 17 06:12 upload-svg
drwxr-xr-x  7 deploy wpdev 4096 Sep 17 06:12 woo-checkout-field-editor-pro
drwxr-xr-x 12 deploy wpdev 4096 Sep 17 06:12 woocommerce
drwxr-xr-x 11 deploy wpdev 4096 Sep 17 06:12 woocommerce-multilingual
drwxr-xr-x 12 deploy wpdev 4096 Sep 17 06:12 woocommerce-products-filter
drwxr-xr-x  7 deploy wpdev 4096 Sep 17 06:12 woo-product-gallery-slider
drwxr-xr-x  6 deploy wpdev 4096 Sep 17 06:12 woo-variation-swatches
drwxr-xr-x 13 deploy wpdev 4096 Sep 17 06:12 wordpress-seo
drwxr-xr-x 11 deploy wpdev 4096 Sep 17 06:12 wpml-string-translation
[root@hqua0244839 plugins]#
```

```
drwxr-xr-x 34 deploy wpdev 4096 Sep 22 02:27 .
drwxr-xr-x 10 deploy wpdev 4096 Sep 22 06:41 ..
drwxr-xr-x  5 deploy wpdev 4096 Sep 17 06:12 acf-extended
drwxr-xr-x  7 deploy wpdev 4096 Sep 17 06:12 acfml
drwxr-xr-x  7 deploy wpdev 4096 Sep 17 06:12 advanced-custom-fields
drwxr-xr-x  8 deploy wpdev 4096 Sep 17 06:12 advanced-custom-fields-pro-main
drwxr-xr-x  4 deploy wpdev 4096 Sep 16 10:40 akismet
drwxr-xr-x  2 deploy wpdev 4096 Sep 20 04:21 cbwyyeyhlj
drwxr-xr-x  9 deploy wpdev 4096 Sep 17 06:12 chaty
drwxr-xr-x  4 deploy wpdev 4096 Sep 17 06:12 classic-editor
drwxr-xr-x  7 deploy wpdev 4096 Sep 17 06:12 cyrlitera
-r--r--r--  1 deploy wpdev  127 Sep 20 04:23 .htaccess
-rw-r--r--  1 deploy wpdev   28 Sep 16 10:40 index.php
drwxr-xr-x  5 deploy wpdev 4096 Sep 17 06:12 index-wp-mysql-for-speed
drwxr-xr-x  7 deploy wpdev 4096 Sep 17 06:12 loco-translate
drwxr-xr-x 11 deploy wpdev 4096 Sep 17 06:12 members
drwxr-xr-x  6 deploy wpdev 4096 Sep 17 06:12 miniorange-login-openid
drwxr-xr-x  7 deploy wpdev 4096 Sep 17 06:12 mrkv-liqpay-extended
drwxr-xr-x 10 deploy wpdev 4096 Sep 17 06:12 post-thumbnail-editor-master
drwxr-xr-x 10 deploy wpdev 4096 Sep 17 06:12 query-monitor
drwxr-xr-x  6 deploy wpdev 4096 Sep 17 06:12 redux-framework
drwxr-xr-x  6 deploy wpdev 4096 Sep 17 06:12 regenerate-thumbnails
drwxr-xr-x  4 deploy wpdev 4096 Sep 17 06:12 simple-custom-post-order
drwxr-xr-x 16 deploy wpdev 4096 Sep 17 06:12 sitepress-multilingual-cms
drwxr-xr-x 11 deploy wpdev 4096 Sep 17 06:12 svg-support
drwxr-xr-x  7 deploy wpdev 4096 Sep 17 06:12 taxonomy-terms-order
drwxr-xr-x 11 deploy wpdev 4096 Sep 17 06:12 ti-woocommerce-wishlist
drwxr-xr-x  5 deploy wpdev 4096 Sep 17 06:12 upload-svg
drwxr-xr-x  7 deploy wpdev 4096 Sep 17 06:12 woo-checkout-field-editor-pro
drwxr-xr-x 12 deploy wpdev 4096 Sep 17 06:12 woocommerce
drwxr-xr-x 11 deploy wpdev 4096 Sep 17 06:12 woocommerce-multilingual
drwxr-xr-x 12 deploy wpdev 4096 Sep 17 06:12 woocommerce-products-filter
drwxr-xr-x  7 deploy wpdev 4096 Sep 17 06:12 woo-product-gallery-slider
drwxr-xr-x  6 deploy wpdev 4096 Sep 17 06:12 woo-variation-swatches
drwxr-xr-x 13 deploy wpdev 4096 Sep 17 06:12 wordpress-seo
drwxr-xr-x 11 deploy wpdev 4096 Sep 17 06:12 wpml-string-translation
[root@hqua0244839 plugins]# ls -la cbwyyeyhlj/
total 24
drwxr-xr-x  2 deploy wpdev 4096 Sep 20 04:21 .
drwxr-xr-x 34 deploy wpdev 4096 Sep 22 02:27 ..
-r--r--r--  1 deploy wpdev 5620 Sep 20 04:21 cache.php
-r--r--r--  1 deploy wpdev  219 Sep 20 04:21 .htaccess
-r--r--r--  1 deploy wpdev 1915 Sep 20 04:21 schallfuns.php
```

```
-r--r--r--  1 deploy wpdev 1915 Sep 20 04:21 schallfuns.php
[root@hqua0244839 plugins]# rm -rf cbwyyeyhlj
[root@hqua0244839 plugins]# ls -la
total 140
drwxr-xr-x 33 deploy wpdev 4096 Sep 22 06:44
```

Рекомендации

1. Закрыть файл xmlrpc.php
2. Установить fail2ban, так как есть много моментов сканирования и попыток “взломать” сайт из одного или нескольких IP

3. Поменять права на файлах на 444
4. Установить CloudFlare
5. 2FA при заходе в админку, к примеру каждые 2 недели заново перезаходим в админку
6. Docker-рекомендации
7. Linux-рекомендации

Итоги

По серверным логам видно, что есть информация только за сентябрь начиная от 7 числа. Также имеется debug.log но он показал только ошибки в коде, но по ним нельзя судить что происходило на сервере - (он ведется с 27 мая)

Первое вмешательство было 6 июля, сайт перенесли в середине августа. За 6 число видны только ошибки вредоносного плагина wp-compact по файлу debug.log, но к сожалению нет access.log за то время, чтобы понять кто стучался к сайту.

Заметили что 15 сентября был удален важный файл в корне сайта index.php в 3:25 UTC, удален был файл index.php через GET запрос плагина File-Manager-Advanced

В общем и целом все устранили то что могли, почистили/удалили, также индексация закрытая, возможен тот факт, что ее (индексацию) злоумышленники открывали через тот “вирус” , тут проверить не можем. Все что смогли сделать в краткие сроки - то сделали. Все файлы которые не подпадали под структуру проекта или же видно взаимодействие с ними по дате изменения файлов и логам были проверены и/или удалены.

В идеале, чтобы быть полностью уверенными в отсутствии вредоносного кода, стоит просмотреть каждый файл на проекте - на это может уйти достаточно много времени , от нескольких дней - до недель.

Рекомендуем заказать эту услугу у тех, кто занимается чисткой сайтов (кибербезопасностью), но это остаётся на Ваше усмотрение.
Это отдельная услуга, она не входит в услуги разработки сайта.

Ми відповідаємо за розробку, а питання безпеки хостингу та сайту залишаються на стороні клієнта
Якщо б з Вашого боку було налаштоване відповідне моніторинг чи сповіщення, можна було б оперативніше зреагувати

Наразі почистили сайт, наступні питання з безпеки до вашого сисадміна

У файлику є рекомендації, будь ласка дотримуйтесь вказівок

docker-рекомендации

Ваш **docker-compose.yml**

```
services:
   app:
      build: .
      restart: unless-stopped
      working_dir: /var/www/html
      ports:
         - "127.0.0.1:8000:80"
      extra_hosts:
         - "host.docker.internal:host-gateway"
      volumes:
         - ${APP_ROOT_PATH}:/var/www/html
         - ./data/apache2-logs:/var/log/apache2
      networks:
         main:
            ipv4_address: 10.5.0.5

networks:
   main:
      driver: bridge
      ipam:
         config:
            - subnet: 10.5.0.0/16
              gateway: 10.5.0.1
```

---------- рекомендации по улучшению

1) добавить user: от которого запускать контейнер
контейнер не должен работать от root-пользователя

2) добавить
security_opt:
    - no-new-privileges:true
не даст процессам внутри контейнера повышать себе права

3) Volume с APP_ROOT_PATH даёт полный доступ к коду приложения внутри контейнера
- ${APP_ROOT_PATH}:/var/www/html
Риск: если APP_ROOT_PATH указывает на хостовую директорию с доступом на запись - уязвимость на уровне RCE, LFI, или компрометации через плагины.
- ${APP_ROOT_PATH}:/var/www/html:ro - я б писала с доступом на чтение или без wp-config.php и остальных важных файлов

4) Отсутствуют mem_limit, cpus, pids_limit - WordPress может съесть все ресурсы хоста

5) read_only root-файловой системы -
надо добавлять
read_only: true

tmpfs:
  - /tmp
  - /var/tmp

6) restart: unless-stopped - это хорошо , но если упадет из-за бага будет бесконечный перезапуск ,
я б добавила проверку на healthcheck, чтобы Docker понимал когда контейнер сломан
healthcheck:
    test: ["CMD", "curl", "-f", "http://localhost"]
    interval: 30s
    timeout: 10s
    retries: 3

linux-рекомендации

Обязательное обновление ядра и пакетов сервера
Обязательное обновления Docker

SSH
Запретить root-логин по SSH (PermitRootLogin no).
Отключить пароли - только SSH-ключи (PasswordAuthentication no)
Разрешить доступ только определённым пользователям/IP

Порты: если открыто больше сервисов чем нужно закрыть порты

FTP открыт (порт 21) - vsftpd и активно слушает. FTP передаёт пароли в открытом виде. Это небезопасно, особенно если доступ извне.
ограничить доступ через firewall
firewall-cmd --zone=public --remove-port=**21/tcp** --permanent
firewall-cmd --reload

MariaDB (MySQL) доступна извне (**3306/tcp**)
Это не рекомендуется, если нет серьёзной нужды.
Разрешить доступ только с localhost:
bind-address = 127.0.0.1 # в /etc/my.cnf
Или ограничить через firewall:
firewall-cmd --remove-port=3306/tcp --permanent
firewall-cmd --reload

Firewall активен - настроен хорошо, но лучше убрать лишние:
firewall-cmd --remove-service=cockpit --permanent
firewall-cmd --reload
docker зона - все соединения разрешены (в т.ч. между контейнерами) это несет потенциальные риски связанные с безопасностью

Анализ iptables
INPUT цепочка по умолчанию ACCEPT - это небезопасно
 нет фильтрации на INPUT - нет базовых правил
добавить разрешения только на нужные порты

var/lib/docker/overlay2/*/merged/usr/bin/ -это значит, что **контейнеры** запускаются с root-файлами, которые имеют SUID, и если контейнер будет скомпрометирован или выйдет из sandbox (например, через --privileged режим), это путь к LPE на хосте. Если контейнеры запущены с привилегиями, это прямой путь к Root на всей системе.

Мониторинг и защита
auditd - логировать системные вызовы
fail2ban - блокировка брутфорса по ssh, sftp, apache и т.д.
Алерты и оповещения (Telegram/мессенджеры) для моментально реагировать на инциденты (брутфорс-атаки, изменение критичных конфигураций, отключение служб, перезагрузка сервер, изменения в /var/www, wp-config.php , добавления новых пользователей и т.д.)

Если **xmlrpc.php** не используется в сайте, его надо закрыть, так как это распространенный вектор для атаки подбора паролей пользователей .

Наличие регулярного и проверенного резервного копирования - критически важно для обеспечения устойчивости и безопасности сервера. Резервные копии должны лежать на удаленном сервере. (сервер, база, контейнер, сайт и т.д.)

Как часть комплексной защиты WordPress-сервера рекомендую установить антивирусное решение. Несмотря на то, что Linux редко подвергается заражению, WordPress остаётся одной из самых частых целей атак: через уязвимости в плагинах и темах обычно загружают вредоносные скрипты и веб-шеллы. Антивирус позволит сканировать загружаемые файлы, выявлять опасные PHP-скрипты, фильтровать почтовые вложения и формировать отчёты об угрозах.