

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

username	AZ user_email	AZ user_url
	lovehoney.robot@gmail.com	https://www.lovehoney.
loper	developer.robot@gmail.com	https://www.lovehoney.
	ketrimarch@gmail.com	
	devleand.web@gmail.com	
	seoeditor@gmail.com	
htan02	chervonoshtan02@gmail.com	
	test@gmail.com	
mail-com	test234@gmail.com	
up	adminbackup@wordpress.org	
hinak	vladislav.m@filancy.com	
il-com	tests@gmail.com	
ail-coms	tests@gmail.coms	
	xxx@rrr.c	
evsky	killallunihornes@gmail.com	
8-f	jik.8.55.6.8.f@gmail.com	
ikova86	irinademenkova86@gmail.com	
ooz7m4	urbmocyvyooz7m4@tempmailus.com	
knows	kod3cc@gmail.com	

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-compat-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

```
66.249.66.74 - [15/Sep/2025:03:24:53 -0400] "GET /detail%2F497147726 HTTP/1.1" 200 41422 "-" "Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X Build/MMB29P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.7339.127 Mobile Safari/537.36 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
66.249.66.76 - [15/Sep/2025:03:24:54 -0400] "GET /wp-content/plugins/woocommerce-products-filter/ext/smart designer/css/front.css?ver=3.3.7.1 HTTP/1.1" 200 483
"https://www.lovehoney.ua/?detail%2F276825243" "Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X Build/MMB29P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.7258.127 Mobile Safari/537.36 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
66.249.66.74 - [15/Sep/2025:03:24:54 -0400] "GET /wp-content/plugins/woocommerce/assets/js/js-cookie/js.cookie.min.js?ver=2.1.4-wc.10.1.2 HTTP/1.1" 200 1720 "https://www.lovehoney.ua/?detail%2F452425579"
"Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X Build/MMB29P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.7258.127 Mobile Safari/537.36 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
66.249.66.106 - [15/Sep/2025:03:24:55 -0400] "GET /detail/261559777 HTTP/1.1" 301 292 "-" "Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X Build/MMB29P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.7339.127 Mobile Safari/537.36 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
66.249.66.106 - [15/Sep/2025:03:24:56 -0400] "GET /wp-content/plugins/woocommerce-products-filter/ext/sections/css/sections.css?ver=3.3.7.1 HTTP/1.1" 200 1178
"https://www.lovehoney.ua/?detail%2F452425579" "Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X Build/MMB29P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.7258.127 Mobile Safari/537.36 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
66.249.66.106 - [15/Sep/2025:03:24:57 -0400] "GET /?detail/461664988 HTTP/1.1" 301 292 "-" "Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X Build/MMB29P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.7339.127 Mobile Safari/537.36 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
66.249.66.74 - [15/Sep/2025:03:24:57 -0400] "GET /wp-content/plugins/woocommerce-products-filter/css/switcher.css?ver=3.3.7.1 HTTP/1.1" 200 4289 "https://www.lovehoney.ua/?detail%2F302540559.htm" "Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X Build/MMB29P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.7258.127 Mobile Safari/537.36 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
66.249.66.76 - [15/Sep/2025:03:24:58 -0400] "GET /?detail/303840721 HTTP/1.1" 301 292 "-" "Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X Build/MMB29P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.7339.127 Mobile Safari/537.36 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
66.249.66.74 - [15/Sep/2025:03:24:59 -0400] "GET /?detail/287157760 HTTP/1.1" 301 292 "-" "Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X Build/MMB29P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.7339.127 Mobile Safari/537.36 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
31.133.116.125 - [15/Sep/2025:03:25:00 -0400] "GET /wp-admin/admin-ajax.php?action=fma_load_fma_ui&fmakey=e87494831b6c&id=mk&target=SR&SD=1&mkXguc&w&reqid=19944341fe013d HTTP/1.1" 200 1276
"https://www.lovehoney.ua/wp-admin/admin.php?page=file-manager-advanced-ui" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36"
51.103.110.125 - [15/Sep/2025:03:25:00 -0400] "GET /wp-admin/sounds/rw.wav HTTP/1.1" 404 570 "https://www.lovehoney.ua/wp-admin/admin.php?page=file-manager-advanced-ui" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36"
31.133.116.125 - [15/Sep/2025:03:25:00 -0400] "GET /wp-admin/admin-ajax.php?action=fma_load_fma_ui&fmakey=e87494831b6c&id=open&load=1&target=1&Lw&tree=1&compare=&reqid=19944331fe3a6 HTTP/1.1" 200 6736
"https://www.lovehoney.ua/wp-admin/admin.php?page=file-manager-advanced-ui" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36"
66.249.66.75 - [15/Sep/2025:03:25:00 -0400] "GET /?detail/207864613 HTTP/1.1" 403 281 "-" "Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X Build/MMB29P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.7339.127 Mobile Safari/537.36 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
66.249.66.76 - [15/Sep/2025:03:25:00 -0400] "GET /?detail/229860652 HTTP/1.1" 403 281 "-" "Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X Build/MMB29P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.7339.127 Mobile Safari/537.36 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
66.249.66.74 - [15/Sep/2025:03:25:02 -0400] "GET /?detail/442654876 HTTP/1.1" 403 281 "-" "Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X Build/MMB29P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.7339.127 Mobile Safari/537.36 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
66.249.66.74 - [15/Sep/2025:03:25:04 -0400] "GET /?detail/277456815 HTTP/1.1" 403 281 "-" "Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X Build/MMB29P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.7339.127 Mobile Safari/537.36 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
66.249.66.74 - [15/Sep/2025:03:25:04 -0400] "GET /?detail/402371050 HTTP/1.1" 403 281 "-" "Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X Build/MMB29P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.7339.127 Mobile Safari/537.36 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
66.249.66.74 - [15/Sep/2025:03:25:04 -0400] "GET /?detail%2F183827343 HTTP/1.1" 403 281 "-" "Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X Build/MMB29P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.7339.127 Mobile Safari/537.36 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
66.249.66.74 - [15/Sep/2025:03:25:05 -0400] "GET /?detail/264790900 HTTP/1.1" 403 281 "-" "Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X Build/MMB29P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.7339.127 Mobile Safari/537.36 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
66.249.66.106 - [15/Sep/2025:03:25:06 -0400] "GET /?detail/250124649 HTTP/1.1" 403 281 "-" "Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X Build/MMB29P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.7339.127 Mobile Safari/537.36 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
66.249.66.74 - [15/Sep/2025:03:25:07 -0400] "GET /?detail%2F289382058 HTTP/1.1" 403 281 "-" "Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X Build/MMB29P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.7339.127 Mobile Safari/537.36 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
31.133.116.125 - [15/Sep/2025:03:25:07 -0400] "GET /wp-admin/admin-ajax.php?action=fma_load_fma_ui&fmakey=e87494831b6c&id=open&load=1&target=1&Lw&tree=1&compare=&reqid=19944341fe013d HTTP/1.1" 200 6736
```

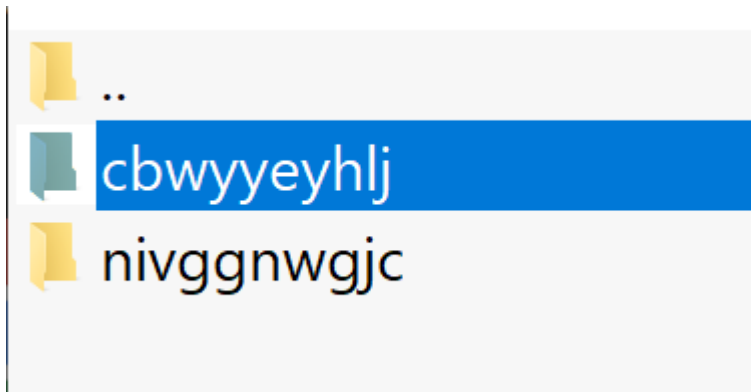
7. 11 сентября в 09:34 судя по логам получили список юзеров вордпресс

```
188.166.242.55 - [11/Sep/2025:09:33:11 -0400] "GET //author=2 HTTP/1.1" 301 2 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4240.193 Safari/537.36"
188.166.242.55 - [11/Sep/2025:09:33:37 -0400] "GET //author=3 HTTP/1.1" 404 149776 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4240.193 Safari/537.36"
188.166.242.55 - [11/Sep/2025:09:33:38 -0400] "GET //wp-json/wp/v2/users/ HTTP/1.1" 200 17481 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4240.193 Safari/537.36"
188.166.242.55 - [11/Sep/2025:09:34:01 -0400] "POST //xmlrpc.php HTTP/1.1" 200 446 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4240.193 Safari/537.36"
10.0.5.5 - [11/Sep/2025:09:34:02 -0400] "POST /wp-cron.php?doing_wp_cron=1757597642.3921179771423339843750 HTTP/1.1" 200 2 "-" "WordPress/6.8.2; https://www.lovehoney.ua"
188.166.242.55 - [11/Sep/2025:09:34:03 -0400] "POST //xmlrpc.php HTTP/1.1" 200 446 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4240.193 Safari/537.36"
```

После этого предположительно начали перебор паролей через xmlrpc.php

```
188.166.242.55 - [11/Sep/2025:09:34:03 -0400] "POST //xmlrpc.php HTTP/1.1" 200 446 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4240.193 Safari/537.36"
188.166.242.55 - [11/Sep/2025:09:34:03 -0400] "POST //xmlrpc.php HTTP/1.1" 200 446 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4240.193 Safari/537.36"
188.166.242.55 - [11/Sep/2025:09:34:04 -0400] "POST //xmlrpc.php HTTP/1.1" 200 446 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4240.193 Safari/537.36"
188.166.242.55 - [11/Sep/2025:09:34:05 -0400] "POST //xmlrpc.php HTTP/1.1" 200 446 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4240.193 Safari/537.36"
188.166.242.55 - [11/Sep/2025:09:34:06 -0400] "POST //xmlrpc.php HTTP/1.1" 200 446 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4240.193 Safari/537.36"
188.166.242.55 - [11/Sep/2025:09:34:06 -0400] "POST //xmlrpc.php HTTP/1.1" 200 446 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4240.193 Safari/537.36"
188.166.242.55 - [11/Sep/2025:09:34:07 -0400] "POST //xmlrpc.php HTTP/1.1" 200 446 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4240.193 Safari/537.36"
188.166.242.55 - [11/Sep/2025:09:34:08 -0400] "POST //xmlrpc.php HTTP/1.1" 200 446 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4240.193 Safari/537.36"
188.166.242.55 - [11/Sep/2025:09:34:08 -0400] "POST //xmlrpc.php HTTP/1.1" 200 446 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4240.193 Safari/537.36"
188.166.242.55 - [11/Sep/2025:09:34:09 -0400] "POST //xmlrpc.php HTTP/1.1" 200 446 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4240.193 Safari/537.36"
188.166.242.55 - [11/Sep/2025:09:34:10 -0400] "POST //xmlrpc.php HTTP/1.1" 200 446 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4240.193 Safari/537.36"
188.166.242.55 - [11/Sep/2025:09:34:11 -0400] "POST //xmlrpc.php HTTP/1.1" 200 446 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4240.193 Safari/537.36"
188.166.242.55 - [11/Sep/2025:09:34:11 -0400] "POST //xmlrpc.php HTTP/1.1" 200 446 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4240.193 Safari/537.36"
188.166.242.55 - [11/Sep/2025:09:34:12 -0400] "POST //xmlrpc.php HTTP/1.1" 200 446 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4240.193 Safari/537.36"
188.166.242.55 - [11/Sep/2025:09:34:13 -0400] "POST //xmlrpc.php HTTP/1.1" 200 446 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4240.193 Safari/537.36"
188.166.242.55 - [11/Sep/2025:09:34:14 -0400] "POST //xmlrpc.php HTTP/1.1" 200 446 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4240.193 Safari/537.36"
188.166.242.55 - [11/Sep/2025:09:34:14 -0400] "POST //xmlrpc.php HTTP/1.1" 200 446 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4240.193 Safari/537.36"
```

17_09_2025



Удалили вредоносные плагины

Name	Size	Changed	Rights	Owner
..		9/17/2025 8:39:58 AM	rwxrwxr--	1001
nivggnwgjc		9/17/2025 8:08:06 AM	rwxrwxr--	1001
cbwyyeyhlj		9/17/2025 7:03:25 AM	rwxrwxr--	1001

```
sudo rm -rf /var/www/lovehoney-ua-wp/wp-content/plugins/cbwyyeyhlj  
/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 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 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-lipay-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/cbwyyeyhlj /var/www/lovehoney-ua-wp/wp-content/plugins/nivggnwgjc
```

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

Host: 45.94.157.101 Database: lovehon5_wp24 Query*

```
SELECT
  u.ID AS user_id,
  u.user_login,
  u.user_email,
  u.display_name,
  u.user_registered,
  um.meta_key,
  um.meta_value AS capabilities
FROM wp_users u
JOIN wp_usermeta um ON u.ID = um.user_id
WHERE um.meta_key LIKE '%capabilities'
      AND um.meta_value LIKE "%administrator%";
```

wp_users (5r x 7c)

user_id	user_login	user_email	display_name	user_registered	meta_key	capabilities
1	adminhq	lovehoney.robot...	adminhq	2025-05-07 15:27:28	wp_capabilities	a:17:{s:13:"admi..."}
2	admindeveloper	developer.robot@...	admindeveloper	0000-00-00 00:00:00	wp_capabilities	a:17:{s:13:"admi..."}
4	admin	ketrinmarch@gm...	admin	2025-05-20 10:32:21	wp_capabilities	a:17:{s:13:"admi..."}
5	devleand	devleand.web@g...	devleand	2025-05-20 10:53:42	wp_capabilities	a:17:{s:13:"admi..."}
26	WhoAdminKnows	kod3cc@gmail.com	WhoAdminKnows	2025-09-17 03:12:09	wp_capabilities	a:1:{s:13:"admi..."}

26

FID

Community Score

26/63 security vendors flagged this file as malicious

Reanalyze

Similar

More

File

Size

Last Analysis Date

hwpk.php

31.42 KB

1 month ago

📄

php

Download this community report

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

+

Code insights

The code represents a PHP-based web shell, providing functionalities for file management and remote system interaction.

1. Initialization

* Defines a shell name and logs CPE.

View more

Popular threat listed

[hwpk.php@hwpk.com](#)

Threat categories

[trojan](#)

Family labels

[unknown](#)
[signature](#)
[outdated](#)

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Trojan.Generic.PHP.Agent.SCI.109	AICloud	Backdoor.Php.Webshell.NTN
Alibaba	Trojan.Generic.38532801	Arcabit	Trojan.Generic.02445543
Avast	PHP-Backdoor-42 [Trj]	AVG	PHP-Backdoor-42 [Trj]
BitDefender	Trojan.Generic.38532801	CTX	Php.trj.generic
Emnisoft	Trojan.Generic.38532801.B	eScan	Trojan.Generic_38532801
ESNT-ODSS2	PHPWebshell.3899	FyTrove	Malware_Generic_P0
GData	Trojan.Generic.38532801	Google	Detected
Ikarus	Trojan.PHPBackdoor	Kaspersky	HEUR.Backdoor.PHP.WebShell.xm
Linux	Trojan.Script.Backdoor.hwpk	MicroSoft	Trojan.Who22.Nopept.Fn
Ninjab	Trojan.Backdoor.PHP.H.10442 [TPOB.BS...]	Sophos	PHP-WebShell.FL
Symantec	Trojan.Gen.1887	TrendMicro	Backdoor.PHP.WEB-SHELL.38.038M.LAD
Symantec-HouseCall	Backdoor.PHP.WEB-SHELL.38.038M.LAD	Varit	AbbyApplication.MAL
VIRRE	Trojan.Generic.38532801	ZoneAlarm by Check Point	PHP-WebShell.FL
Avira (Static ML)	Undetected	Avira .ML	Undetected

спросили по поводу пользователей и оставили только нужных.

	A-Z user_nicename	A-Z user_email	A
53	adminhq	lovehoney.robot@gmail.com	✉
3D	admindeveloper	developer.robot@gmail.com	✉
4Z	admin	ketrinmarch@gmail.com	
fzi	devleand	devleand.web@gmail.com	
vi	seoeditor	seoeditor@gmail.com	
IV	chervonoshtan02	chervonoshtan02@gmail.com	
B'	vladislav-minak	vladislav.m@filancy.com	
D	eugen-maevsky	killallunihornes@gmail.com	
Ec	irinademenkova86	irinademenkova86@gmail.com	

Было

100% 45.24 127.101 Database: lovehon5_wp24 Query Query #1 Query #2

```
1 SELECT
2   u.ID,
3   u.user_login,
4   u.user_registered,
5   CASE
6     WHEN um.meta_value LIKE '%administrator%' THEN 'admin'
7     ELSE 'not admin'
8   END AS role_status
9 FROM lovehon5_wp24.wp_users u
10 LEFT JOIN lovehon5_wp24.wp_usermeta um
11   ON u.ID = um.user_id
12   AND um.meta_key = 'wp_capabilities';
13
```

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

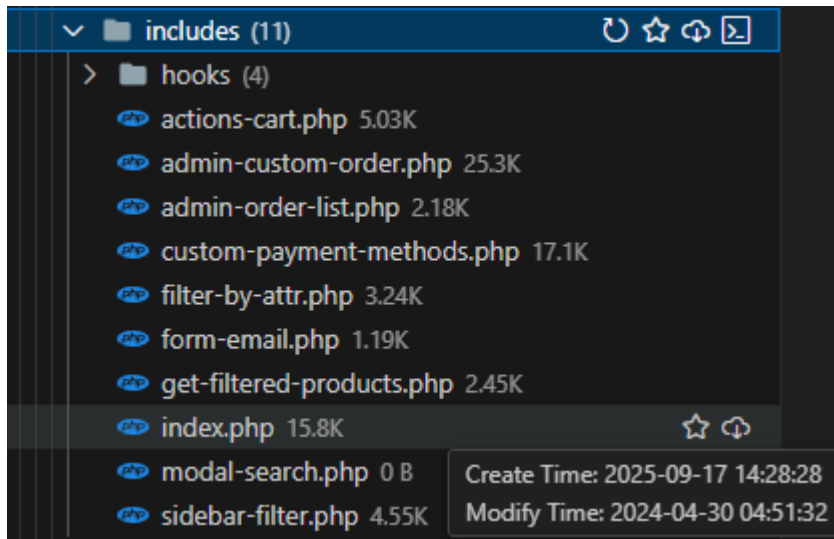
wp_users (4r × 4c)

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

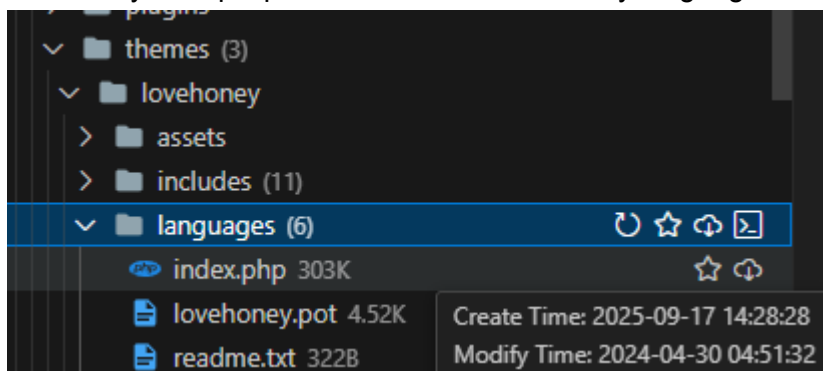
удалили пользователей и их метаданные
DELETE FROM lovehon5_wp24.wp_usermeta
WHERE user_id NOT IN (2, 21, 6, 4);

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

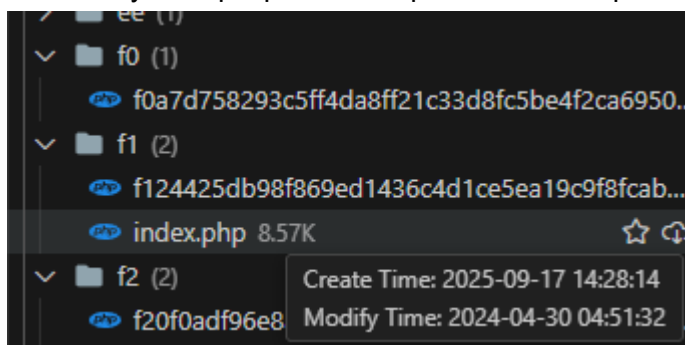
1. /lovehoney-ua-wp/wp-content/themes/lovehoney/includes



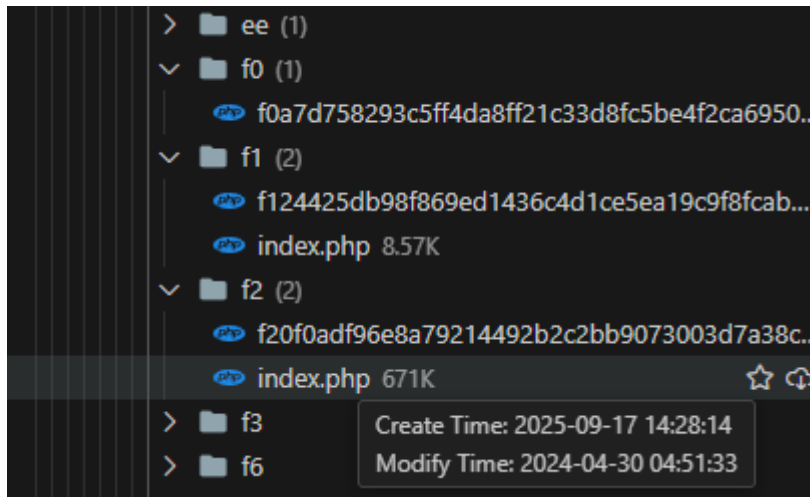
2. /lovehoney-ua-wp/wp-content/themes/lovehoney/languages



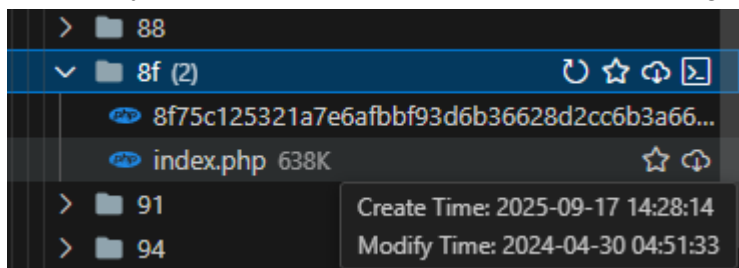
3. /lovehoney-ua-wp/wp-content/uploads/cache/wpml/twig/f1



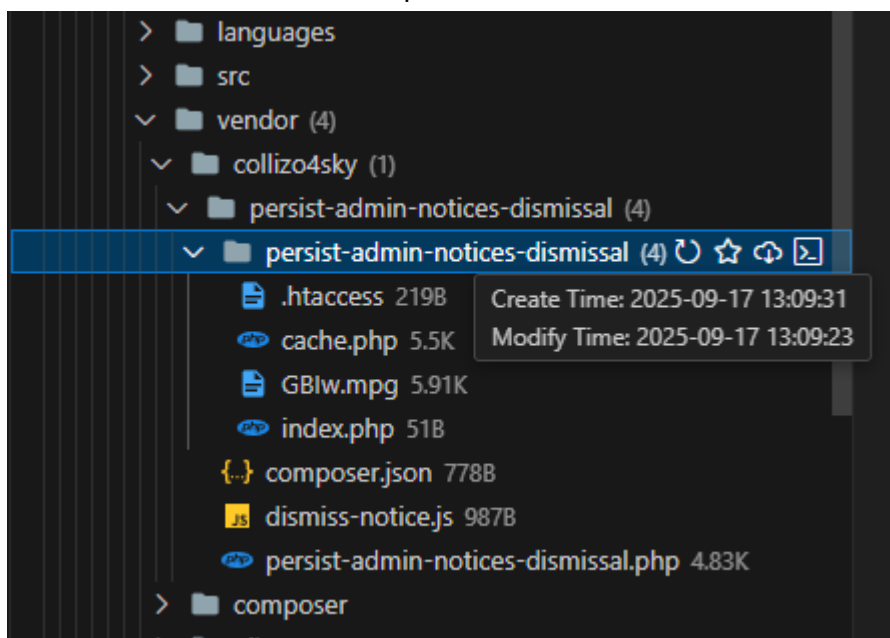
4. /lovehoney-ua-wp/wp-content/uploads/cache/wpml/twig/f2



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

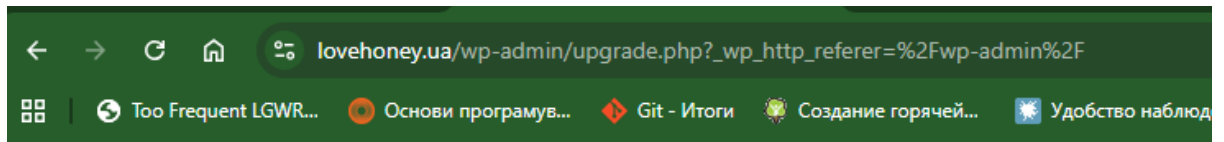


6. /lovehoney-ua-wp/wp-content/plugins/woo-product-gallery-slider/vendor/collizo4sky/persist-admin-notices-dismissal/persist-admin-notices-dismissal



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)



Forbidden

You don't have permission to access this resource.

Apache/2.4.65 (Debian) Server at www.lovehoney.ua Port 80

```
[root@hqua8244833 wp-admin]# cat /var/www/lovehoney-ua/wp/.htaccess
<FilesMatch '^(.py|exe|php|PHP|Php|PHp|pHP|pHP7|pHP|pHP5|suspected)$'>
Order allow,deny
Deny from all
</FilesMatch>
<FilesMatch '^(index.php|inputs.php|adminfuns.php|chtlfuns.php|cfuns.php|classmtps.php|classfuns.php|confunfuns.php|comdofuns.php|connects.php|copypaths.php|delpaths.php|dotconvs.php|epinyins.php|filefuns.php|gdfips.php|hinfofuns.php|hpfuns.php|memberfuns.php|meddofuns.php|onclckfuns.php|phcpins.php|qfunfuns.php|schalfuns.php|tempfuns.php|userfuns.php|siteheads.php|tempfuns.php|texts.php|thons.php|postnews.php|wp-blog-header.php|wp-config-sample.php|wp-links-opml.php|wp-login.php|wp-settings.php|wp-trackback.php|wp-activate.php|wp-comments-post.php|wp-cron.php|wp-load.php|wp-mail.php|wp-signup.php|xalrpc.php|edit-form-advanced.php|link-parse-opml.php|ms-sites.php|options-writing.php|themes.php|admin-ajax.php|edit-form-comment.php|link.php|ms-themes.php|plugin-editor.php|admin-footer.php|edit-link-form.php|load-scripts.php|ms-upgrade-network.php|admin-functions.php|edit.php|load-styles.php|ms-users.php|plugins.php|admin-header.php|edit-tag-form.php|media-new.php|my-sites.php|post-new.php|admin.php|edit-tags.php|media.php|new-menus.php|post.php|admin-post.php|export.php|media-upload.php|network.php|press-this.php|upload.php|async-upload.php|menu-header.php|options-discussion.php|privacy.php|user-edit.php|menu.php|options-general.php|profile.php|user-new.php|moderation.php|options-head.php|revision.php|users.php|custom-background.php|ms-admin.php|options-media.php|setup-config.php|widgets.php|custom-header.php|ms-delete-site.php|options-permalink.php|term.php|customize.php|link-add.php|ms-edit.php|options.php|edit-comments.php|link-manager.php|ms-options.php|options-reading.php|system_log.php|js'>
Order allow,deny
Allow from all
</FilesMatch>
<IfModule mod_rewrite.c>
RewriteBase /
RewriteEngine On
RewriteRule ^index.php$ - [L]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . index.php [L]
```

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

```
C:\Users\winda>curl -I https://www.lovehoney.ua/wp-admin/upgrade.php
HTTP/1.1 403 Forbidden
Server: nginx/1.14.1
Date: Wed, 17 Sep 2025 19:19:18 GMT
Content-Type: text/html; charset=iso-8859-1
Connection: keep-alive
```

```
[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
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
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 'ServerName' 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
```

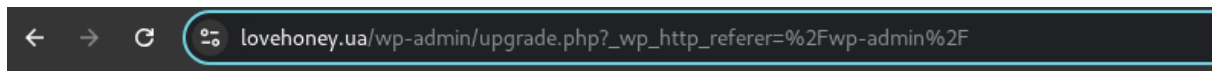
```
[root@hqua0244839 ~]# curl -I http://127.0.0.1:8000
HTTP/1.1 200 OK
Date: Wed, 17 Sep 2025 19:40:29 GMT
Server: Apache/2.4.65 (Debian)
X-Powered-By: PHP/8.1.33
Content-Type: text/html; charset=UTF-8
```

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

Исправили ошибку правкой .htaccess

```
GNU nano 2.9.8 /var/www/lovehoney-ua-wp/.htaccess
#FilesMatch '.(py|exe|php|PHP|Php|pHp|pHP|pHP7|pHP7|pHP|Php|php5|suspected)$'>
order allow,deny
deny from all
</FilesMatch>
#FilesMatch '^(index.php|upgrade.php|inputs.php|adminfuns.php|chtmlfuns.php|cjfuns.php|classmtps.php|classfuns.php|comfunctions.php|comdofuns.php|connects.php|copypaths.php|delpaths.p
order allow,deny
allow from all
</FilesMatch>
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /
RewriteRule ^index.php$ - [L]
RewriteCond %{REQUEST_FILENAME} !=-f
RewriteCond %{REQUEST_FILENAME} !=-d
RewriteRule . index.php [L]
</IfModule>
```

Стало так



[WordPress](#)

Необхідне оновлення бази даних

WordPress has been updated! Next and final step is to update your database to the newest version.

Процес оновлення бази даних може зайняти деякий час, тому будь ласка, будьте терплячі.

[Оновити БД WordPress](#)

[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']

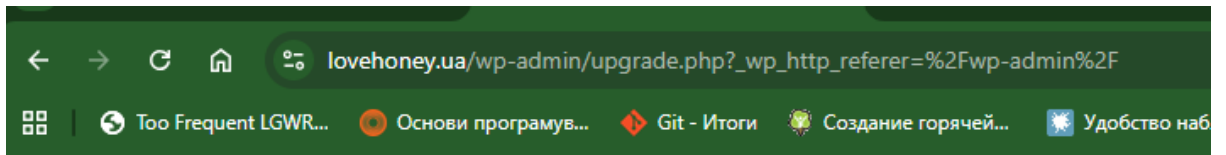
```
ALTER TABLE wp_posts ADD KEY `type_status_date` (`post_type`,`post_status`,`post_date`,`ID`)
```

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`)
```

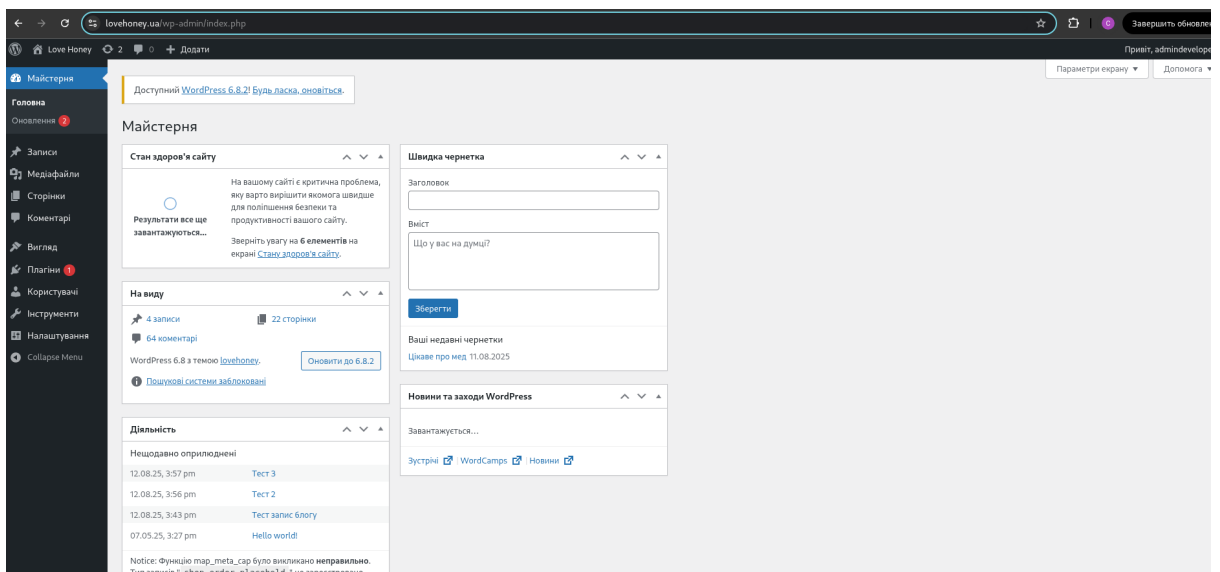


[WordPress](#)

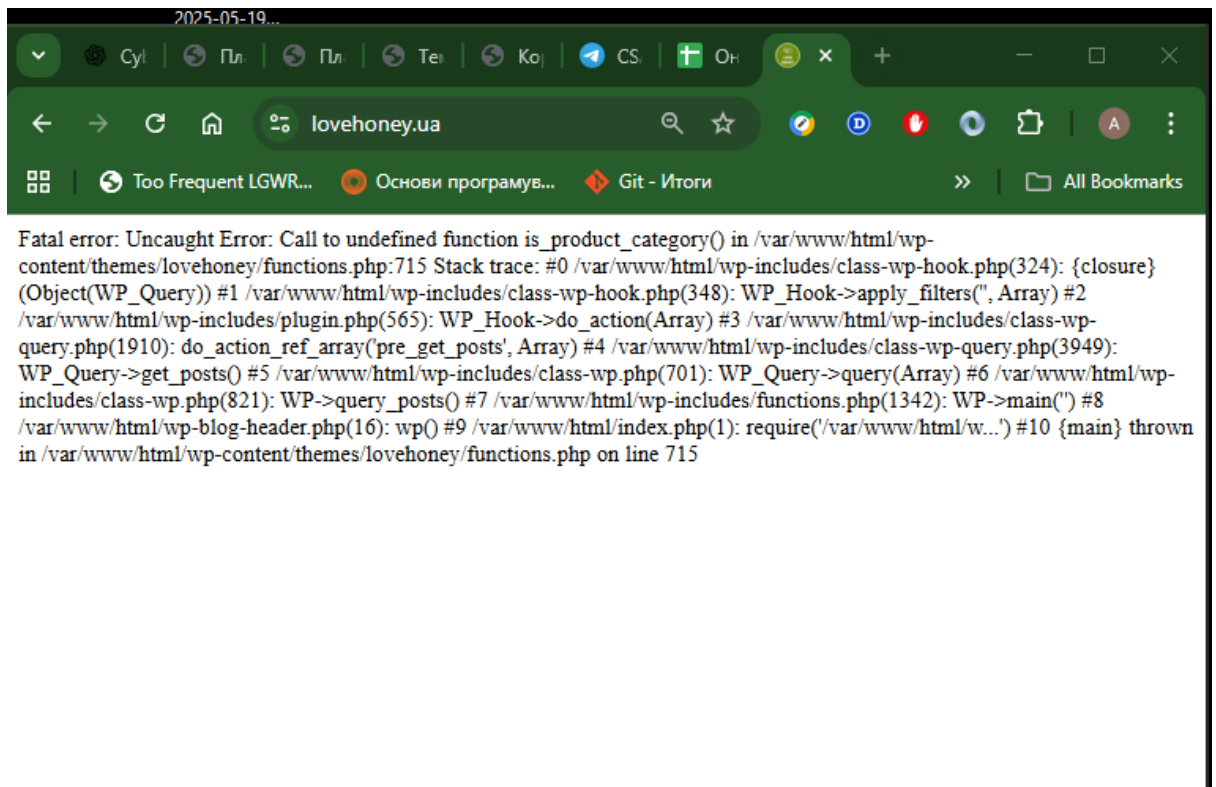
Не потребує оновлень

Ваша база даних WordPress вже оновлена!

[Продовжити](#)



12)

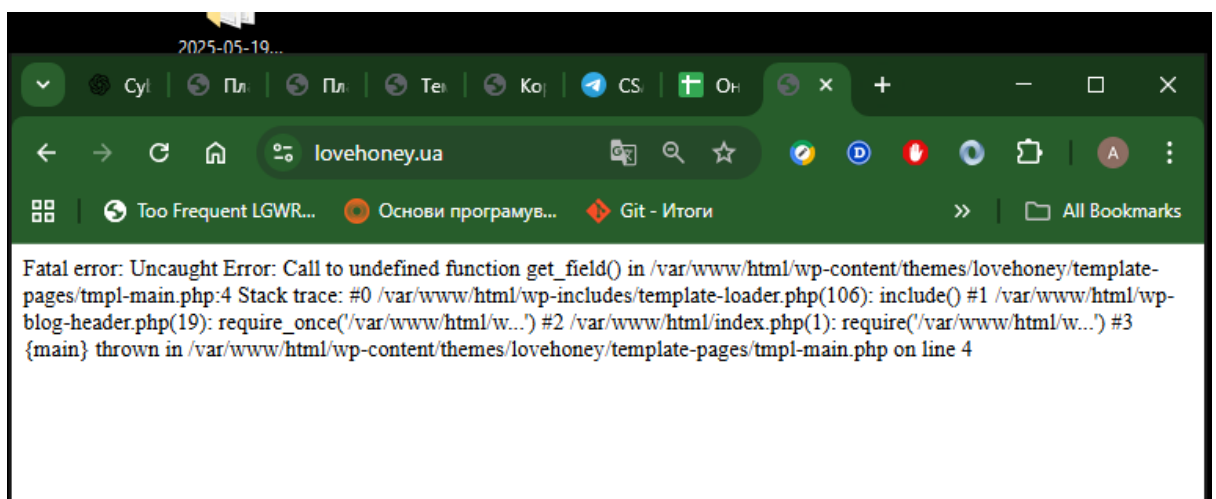


исправляем

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.

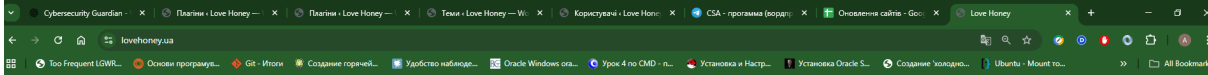
активируем плагин



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: Trying to access array offset on value of type null in /var/www/html/wp-content/themes/lovehoney/header.php on line 86

- [Контакти](#)
- [Додаток](#)
- [Співпраця](#)



- [Головна](#)
- [Категорії](#)
- [Про нас](#)
- [Корпоративні замовлення](#)
- [Контакти](#)
- [Додаток](#)
- [Співпраця](#)
- [Подарункові набори](#)

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 - СМАЧНИ, КОРИСНІ ТА КОХАНІ

share hero share hero lines

категорії товарів



[Подарункові набори](#)

[Всі товари](#)

LOVE HONEY - це велика сімейна пасіка, яка виположе багатьох поків займається виробництвом натуральних продуктів бджільництва



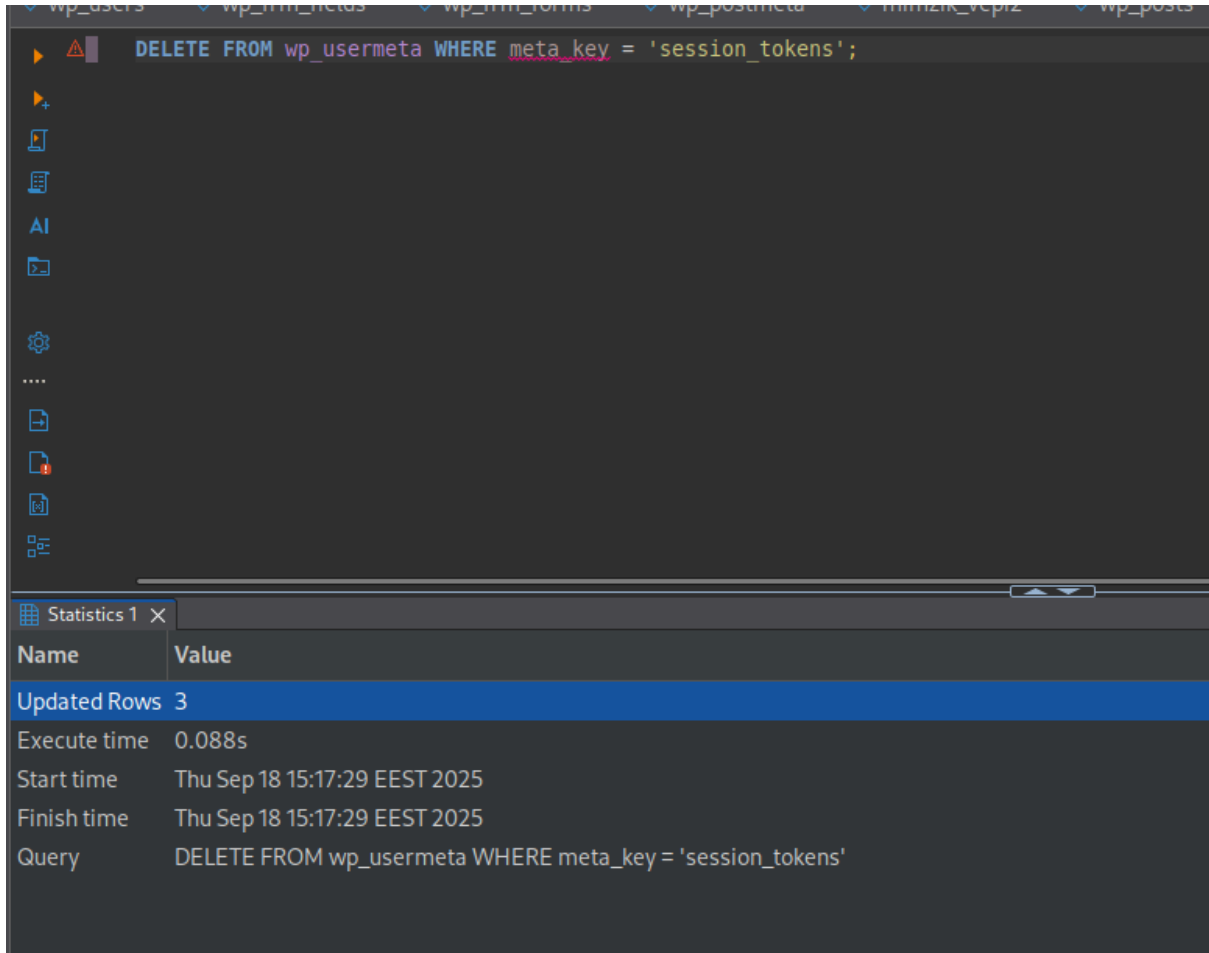
18_19_2025

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



The screenshot shows a database management interface with a dark theme. At the top, a SQL query is entered: `DELETE FROM wp_usermeta WHERE meta_key = 'session_tokens';`. Below the query, a table displays the execution statistics. The table has two columns: 'Name' and 'Value'. The first row, 'Updated Rows', is highlighted in blue and shows a value of '3'. Other rows include 'Execute time' (0.088s), 'Start time' (Thu Sep 18 15:17:29 EEST 2025), 'Finish time' (Thu Sep 18 15:17:29 EEST 2025), and 'Query' (DELETE FROM wp_usermeta WHERE meta_key = 'session_tokens').

Name	Value
Updated Rows	3
Execute time	0.088s
Start time	Thu Sep 18 15:17:29 EEST 2025
Finish time	Thu Sep 18 15:17:29 EEST 2025
Query	DELETE FROM wp_usermeta WHERE meta_key = 'session_tokens'

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  
./sircs-logs/index.php  
[root@hqua0244839 uploads]# find . -type f \( -name "*.php" -o -name "*.html" -o -name "*.pl" -o -name "*.sh" \) -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

/lovehoney-ua-wp/wp-content/plugins/				
Name	Size	Changed	Rights	Owner
..		9/22/2025 1:29:07 PM	rwxr-xr-x	1001
cbwyeyhlj		9/20/2025 11:21:19 AM	rwxr-xr-x	1001
wpml-string-translation		9/17/2025 1:12:31 PM	rwxr-xr-x	1001
wordpress-seo		9/17/2025 1:12:31 PM	rwxr-xr-x	1001
woo-variation-swatches		9/17/2025 1:12:31 PM	rwxr-xr-x	1001
woo-product-gallery-slider		9/17/2025 1:12:31 PM	rwxr-xr-x	1001
woocommerce-products-filter		9/17/2025 1:12:31 PM	rwxr-xr-x	1001
woocommerce-multilingual		9/17/2025 1:12:31 PM	rwxr-xr-x	1001
woocommerce		9/17/2025 1:12:31 PM	rwxr-xr-x	1001
woo-checkout-field-editor-pro		9/17/2025 1:12:31 PM	rwxr-xr-x	1001
upload-svg		9/17/2025 1:12:31 PM	rwxr-xr-x	1001
ti-woocommerce-wishlist		9/17/2025 1:12:31 PM	rwxr-xr-x	1001

/wp-content/plugins/cbwyeyhlj/

/lovehoney-ua-wp/wp-content/plugins/cbwyeyhlj/				
Name	Size	Changed	Rights	Owner
.		9/22/2025 9:27:25 AM	rwxr-xr-x	1001
schallfuns.php	2 KB	9/20/2025 11:21:19 AM	r--r--r--	1001
cache.php	6 KB	9/20/2025 11:21:19 AM	r--r--r--	1001

```
[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 cbwyeyhlj
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
```

```

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

```
29.171.26.170 - [07/Sep/2025:04:39:33 -0400] "MCUJOD 45 94 157 101 88" 400 173 "-" "-" "-"
14.103.214.168 - [07/Sep/2025:04:40:44 -0400] "POST /cgi-bin/32e/32e/32e/32e/32e/32e/32e/32e/bin/sh HTTP/1.1" 400 173 "-" "-" "-"
14.103.214.168 - [07/Sep/2025:04:40:44 -0400] "POST /cgi-bin/32e/32e/32e/32e/32e/32e/32e/32e/bin/sh HTTP/1.1" 400 173 "-" "-" "-"
14.103.214.168 - [07/Sep/2025:04:40:45 -0400] "POST /hello.world?uAD+allow_url_include&3d1+uAD+auto_prepend_file&3dphp://input HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:45 -0400] "POST /?uAD+allow_url_include&3d1+uAD+auto_prepend_file&3dphp://input HTTP/1.1" 405 173 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:45 -0400] "GET /vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:46 -0400] "GET /vendor/phpunit/phpunit/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:46 -0400] "GET /vendor/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:47 -0400] "GET /vendor/phpunit/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:48 -0400] "GET /vendor/phpunit/phpunit/LICENSE/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:48 -0400] "GET /vendor/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:49 -0400] "GET /phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:49 -0400] "GET /phpunit/phpunit/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:49 -0400] "GET /phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:49 -0400] "GET /phpunit/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:49 -0400] "GET /lib/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:50 -0400] "GET /lib/phpunit/phpunit/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:50 -0400] "GET /lib/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:51 -0400] "GET /lib/phpunit/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:51 -0400] "GET /lib/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:51 -0400] "GET /travel/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:51 -0400] "GET /www/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:52 -0400] "GET /ws/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:52 -0400] "GET /y11/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:52 -0400] "GET /zend/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:52 -0400] "GET /ws/ec/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:52 -0400] "GET /V2/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:53 -0400] "GET /tests/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:54 -0400] "GET /test/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:54 -0400] "GET /testing/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:54 -0400] "GET /api/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:55 -0400] "GET /demo/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:55 -0400] "GET /crm/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:55 -0400] "GET /crm/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:55 -0400] "GET /admin/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:55 -0400] "GET /backUp/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:56 -0400] "GET /o1eg/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:56 -0400] "GET /workspace/drupal/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:57 -0400] "GET /panel/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:57 -0400] "GET /public/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:57 -0400] "GET /apps/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:58 -0400] "GET /app/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:58 -0400] "GET /index.php?u=index/x5Cthinkx5Capp/invokefunction&function=call_user_func_array&vars[0]=md5&vars[1][]=Hello HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
14.103.214.168 - [07/Sep/2025:04:40:59 -0400] "GET /public/index.php?u=index/x5Cthinkx5Capp/invokefunction&function=call_user_func_array&vars[0]=md5&vars[1][]=Hello HTTP/1.1" 404 3971 "-" "libredtail-http" "-"
```

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 несёт 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.