Exploitation: WordPress Configuration and SQL Database

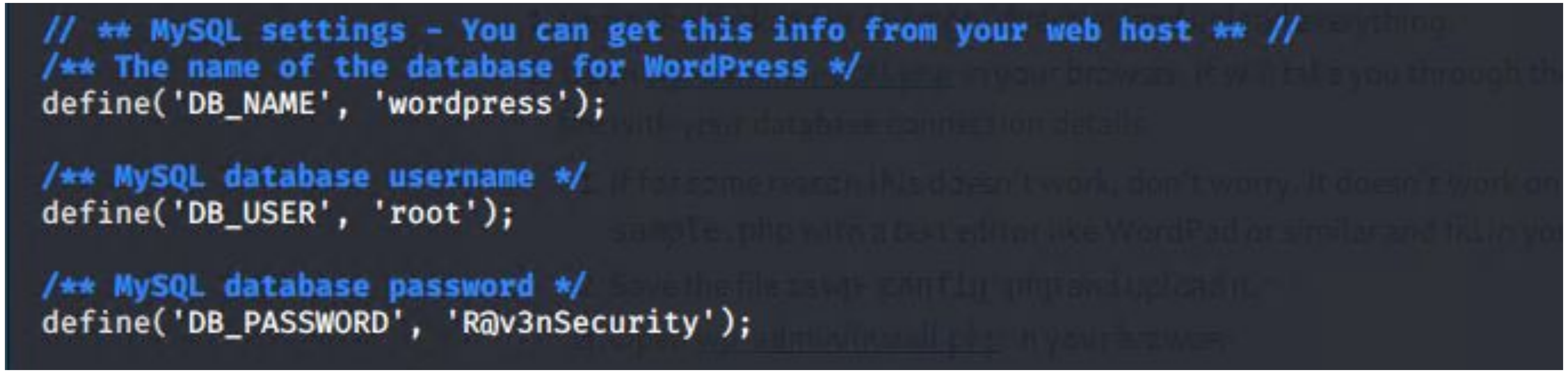
Summarize the following:

How did you exploit the vulnerability?

- The username and password to access the SQL database were in plaintext in the wp-config.php file and not hashed as is best practice, however this is a limitation of wordpress.

What did the exploit achieve?

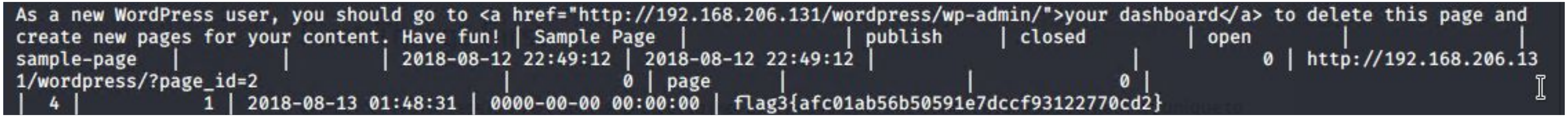
- The exploit granted us mysql access and allowed us to find flag 3. And it also gave the password hash for steven, which meant John could be used to crack the password



```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'R@v3nSecurity');
```



```
As a new WordPress user, you should go to <a href="http://192.168.206.131/wordpress/wp-admin/">your dashboard</a> to delete this page and
create new pages for your content. Have fun! | Sample Page  |                | publish    | closed       | open         |              |
sample-page   |         |        | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 |                        |           0 | http://192.168.206.13
1/wordpress/?page_id=2                   |            0 | page      |              |            0 |
|  4 |            1 | 2018-08-13 01:48:31 | 0000-00-00 00:00:00 | flag3{afc01ab56b50591e7dccf93122770cd2}
```