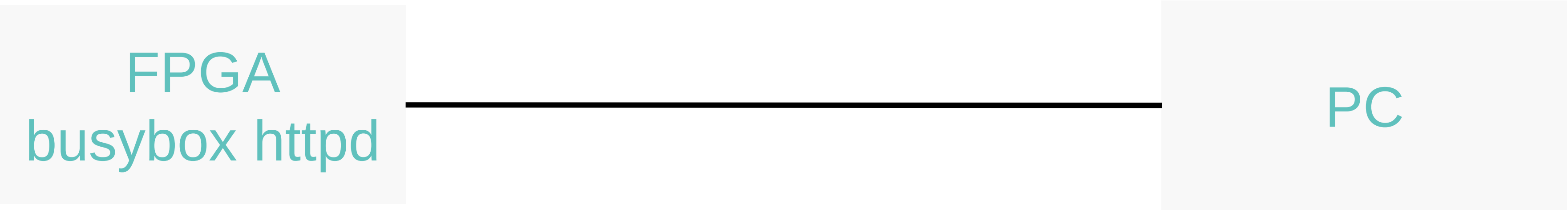
FPGA busybox httpd.

2022 November 04

PUFsecurity

AN eMemory COMPANY

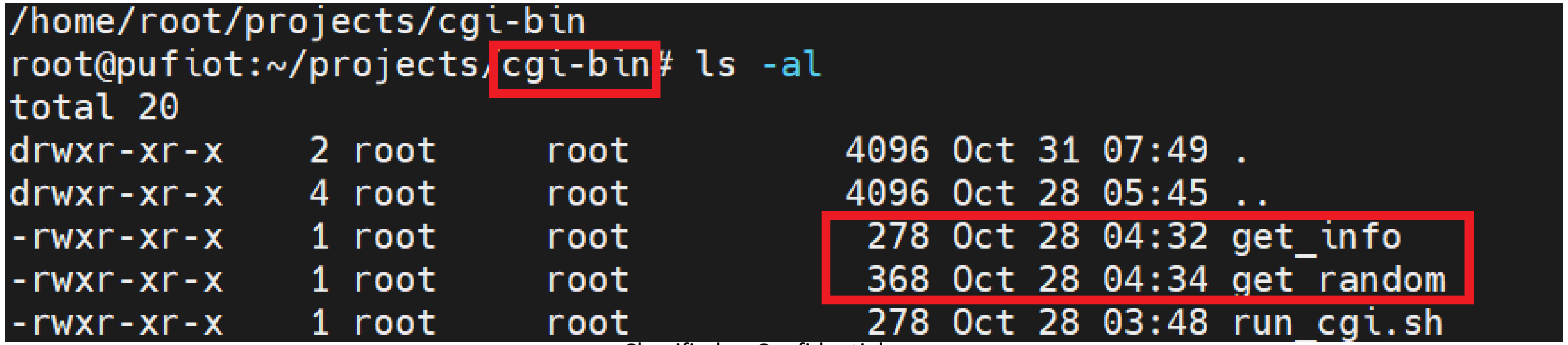
Architecture and Http Services



IP : 172.16.1.91
Home directory: /home/root/projects

http://172.16.1.91:22280/cgi-bin/get_xxx

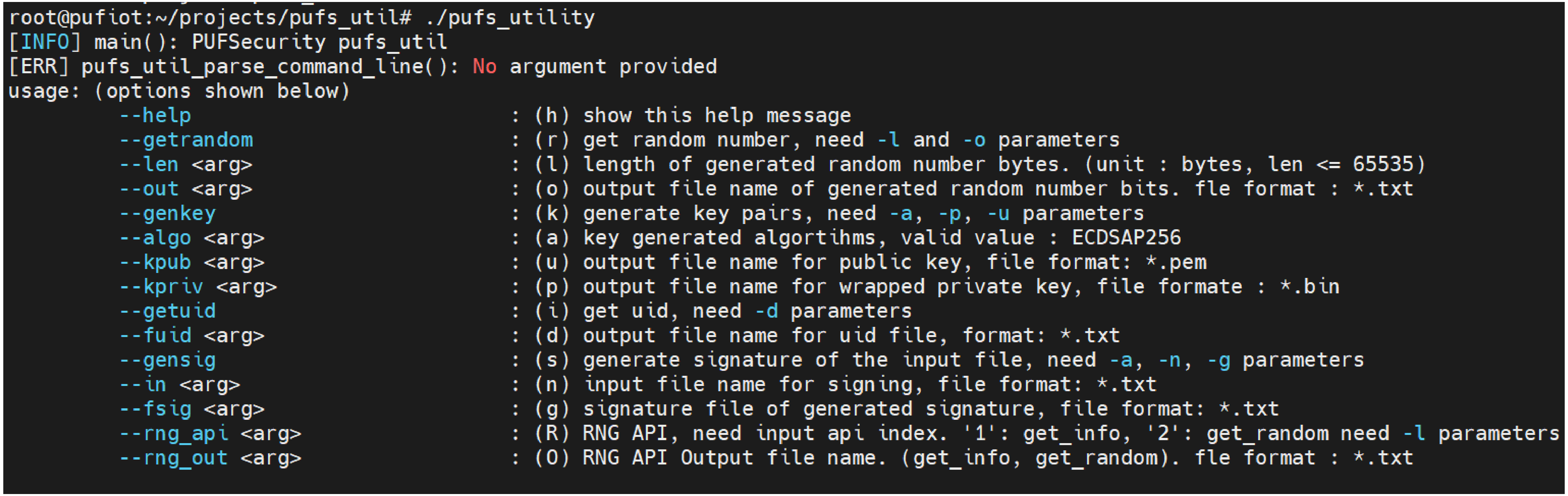
- **Two Http services are provided for RNG :**
  - **Get RNG info: get_info**
  - **Get 8 bytes random number/signature: get_random**
  - **Script location: /home/root/projects/cgi-bin**
  -



```
/home/root/projects/cgi-bin
root@pufiot:~/projects/cgi-bin# ls -al
total 20
drwxr-xr-x    2 root     root          4096 Oct 31 07:49 .
drwxr-xr-x    4 root     root          4096 Oct 28 05:45 ..
-rwxr-xr-x    1 root     root           278 Oct 28 04:32 get_info
-rwxr-xr-x    1 root     root           368 Oct 28 04:34 get_random
-rwxr-xr-x    1 root     root           278 Oct 28 03:48 run_cgi.sh
```

PUFsecurity Utility

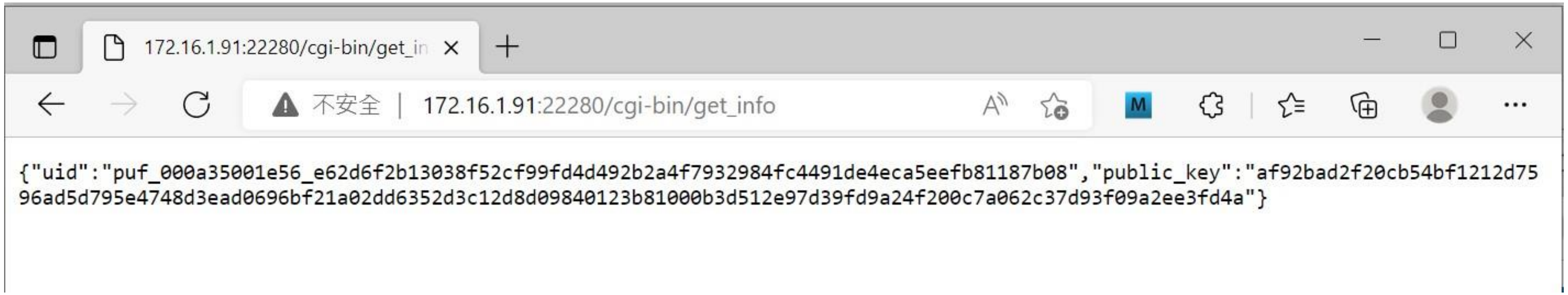
- PUFsecurity Utility
  - location : /home/projects/pufs_util
  - Command line utility



```
root@pufiot:~/projects/pufs_util# ./pufs_utility
[INFO] main(): PUFSecurity pufs_util
[ERR] pufs_util_parse_command_line(): No argument provided
usage: (options shown below)
         --help                          : (h) show this help message
         --getrandom                     : (r) get random number, need -l and -o parameters
         --len <arg>                     : (l) length of generated random number bytes. (unit : bytes, len <= 65535)
         --out <arg>                     : (o) output file name of generated random number bits. fle format : *.txt
         --genkey                        : (k) generate key pairs, need -a, -p, -u parameters
         --algo <arg>                    : (a) key generated algortihms, valid value : ECDSAP256
         --kpub <arg>                    : (u) output file name for public key, file format: *.pem
         --kpriv <arg>                   : (p) output file name for wrapped private key, file formate : *.bin
         --getuid                        : (i) get uid, need -d parameters
         --fuid <arg>                    : (d) output file name for uid file, format: *.txt
         --gensig                        : (s) generate signature of the input file, need -a, -n, -g parameters
         --in <arg>                      : (n) input file name for signing, file format: *.txt
         --fsig <arg>                    : (g) signature file of generated signature, file format: *.txt
         --rng_api <arg>                 : (R) RNG API, need input api index. '1': get_info, '2': get_random need -l parameters
         --rng_out <arg>                 : (O) RNG API Output file name. (get_info, get_random). fle format : *.txt
```

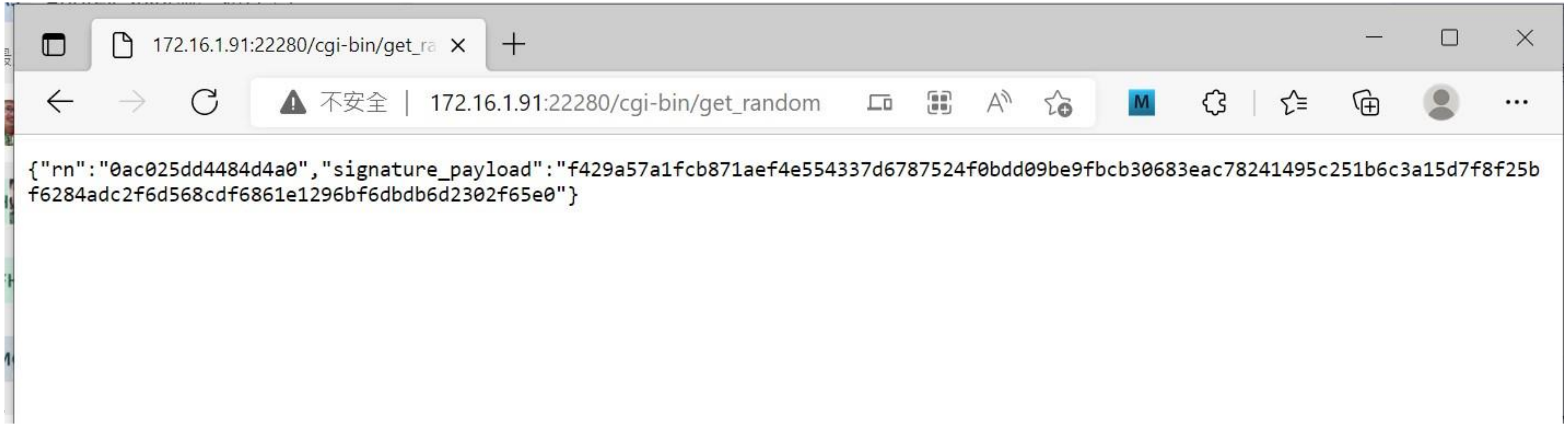
Http – get_info and get_random

- get_info
  - http://172.16.1.91:22280/cgi-bin/get_info


172.16.1.91:22280/cgi-bin/get_in
不安全
172.16.1.91:22280/cgi-bin/get_info

```
{"uid":"puf_000a35001e56_e62d6f2b13038f52cf99fd4d492b2a4f7932984fc4491de4eca5eefb81187b08","public_key":"af92bad2f20cb54bf1212d75
96ad5d795e4748d3ead0696bf21a02dd6352d3c12d8d09840123b81000b3d512e97d39fd9a24f200c7a062c37d93f09a2ee3fd4a"}
```

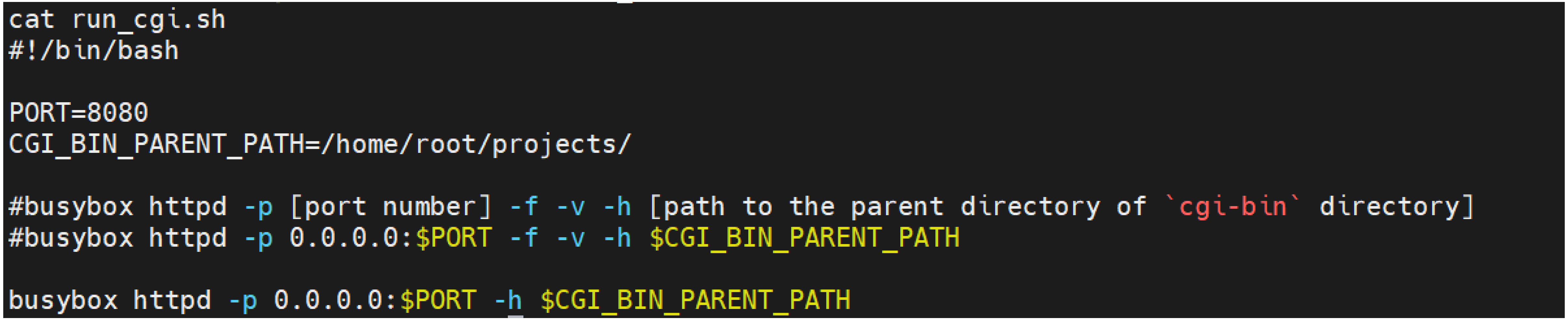
- get_random
  - http://172.16.1.91:22280/cgi-bin/get_random


172.16.1.91:22280/cgi-bin/get_ra
不安全
172.16.1.91:22280/cgi-bin/get_random

```
{"rn":"0ac025dd4484d4a0","signature_payload":"f429a57a1fcb871aef4e554337d6787524f0bdd09be9fbcb30683eac78241495c251b6c3a15d7f8f25b
f6284adc2f6d568cdf6861e1296bf6dbdb6d2302f65e0"}
```

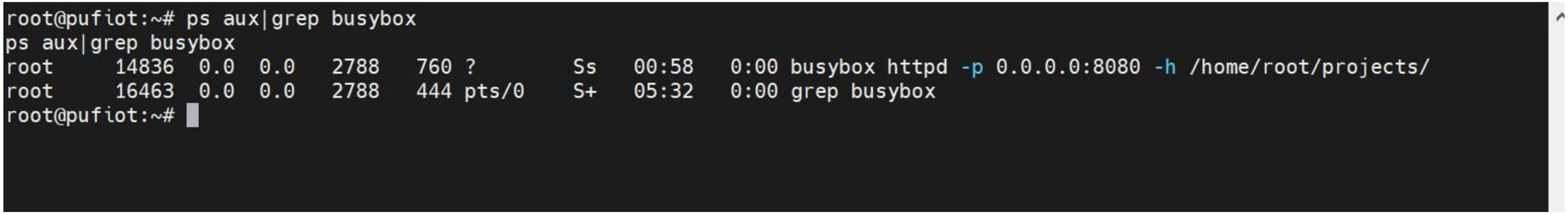
FPGA busybox httpd

- cgi-bin path in fpga: /home/root/project/cgi-bin
- run_cgi.sh to start httpd



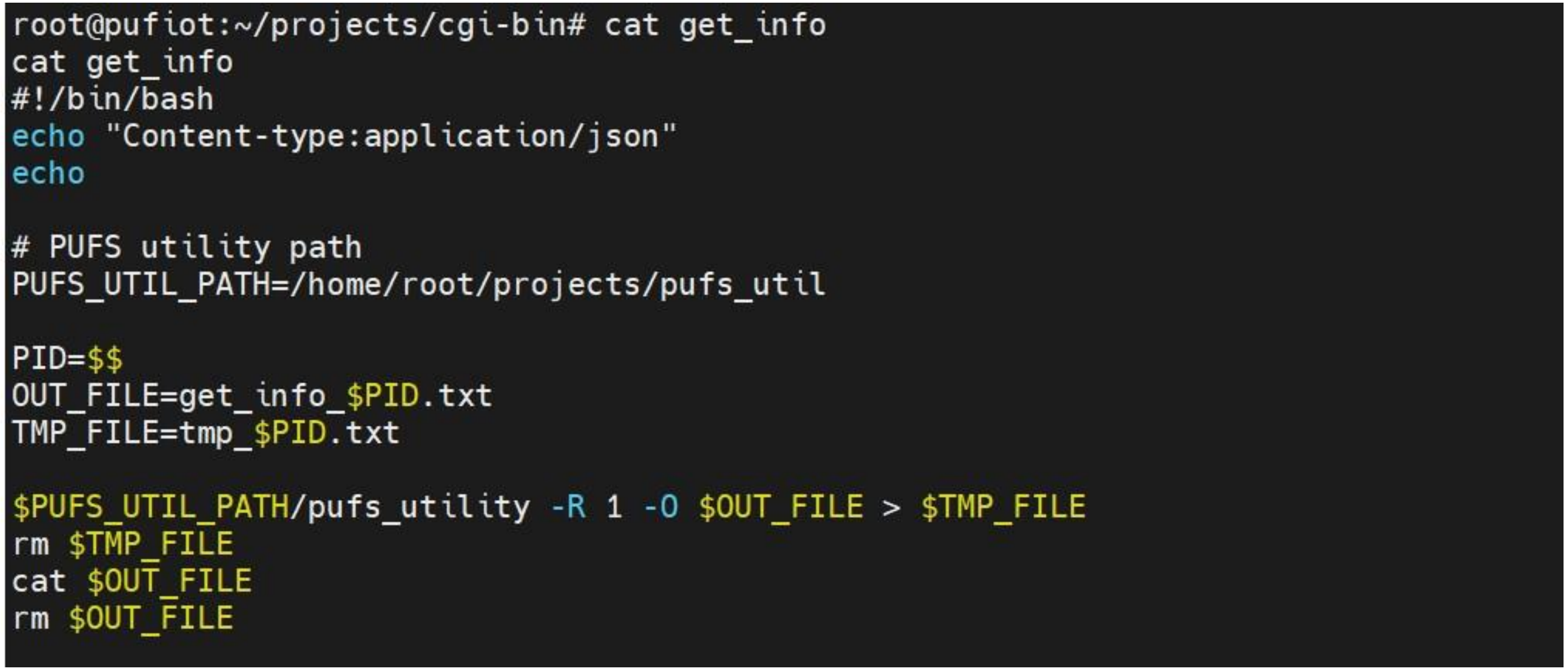
```
cat run_cgi.sh
#!/bin/bash

PORT=8080
CGI_BIN_PARENT_PATH=/home/root/projects/

#busybox httpd -p [port number] -f -v -h [path to the parent directory of `cgi-bin` directory]
#busybox httpd -p 0.0.0.0:$PORT -f -v -h $CGI_BIN_PARENT_PATH

busybox httpd -p 0.0.0.0:$PORT -h $CGI_BIN_PARENT_PATH
```

- busybox httpd started



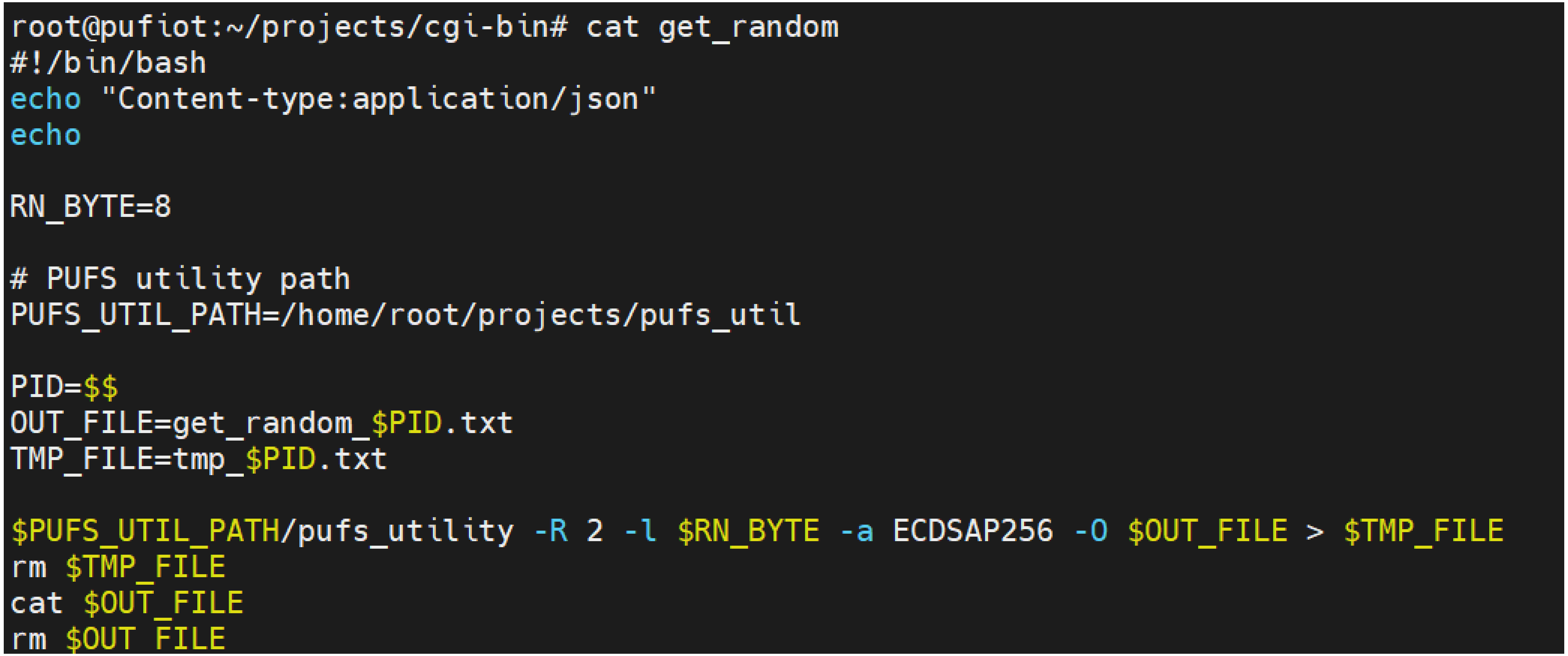
```
root@pufiot:~# ps aux|grep busybox
ps aux|grep busybox
root     14836  0.0  0.0   2788   760 ?        Ss   00:58   0:00 busybox httpd -p 0.0.0.0:8080 -h /home/root/projects/
root     16463  0.0  0.0   2788   444 pts/0    S+   05:32   0:00 grep busybox
root@pufiot:~# 
```

FPGA get_info Bash Script



```
root@pufiot:~/projects/cgi-bin# cat get_info
cat get_info
#!/bin/bash
echo "Content-type:application/json"
echo

# PUFS utility path
PUFS_UTIL_PATH=/home/root/projects/pufs_util

PID=$$
OUT_FILE=get_info_$PID.txt
TMP_FILE=tmp_$PID.txt

$PUFS_UTIL_PATH/pufs_utility -R 1 -O $OUT_FILE > $TMP_FILE
rm $TMP_FILE
cat $OUT_FILE
rm $OUT_FILE
```

FPGA get_random Bash Script



```
root@pufiot:~/projects/cgi-bin# cat get_random
#!/bin/bash
echo "Content-type:application/json"
echo

RN_BYTE=8

# PUFS utility path
PUFS_UTIL_PATH=/home/root/projects/pufs_util

PID=$$
OUT_FILE=get_random_$PID.txt
TMP_FILE=tmp_$PID.txt

$PUFS_UTIL_PATH/pufs_utility -R 2 -l $RN_BYTE -a ECDSAP256 -O $OUT_FILE > $TMP_FILE
rm $TMP_FILE
cat $OUT_FILE
rm $OUT FILE
```

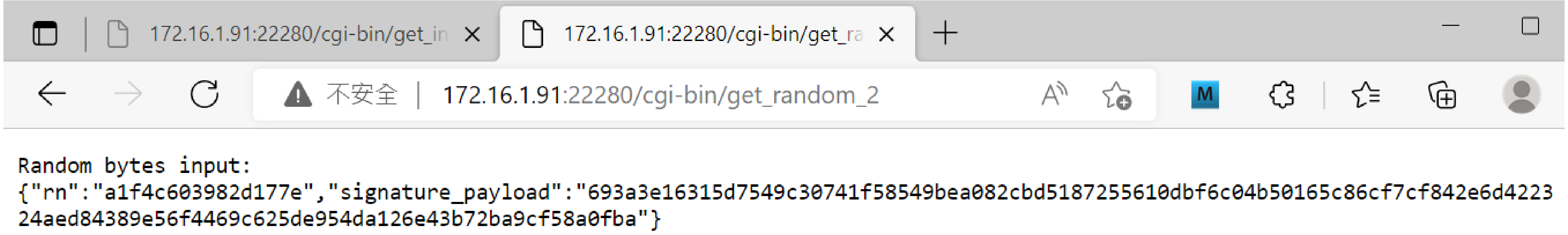
Appendix – get_random_2 with Random Bytes Input

PUFsecurity

AN eMemory COMPANY

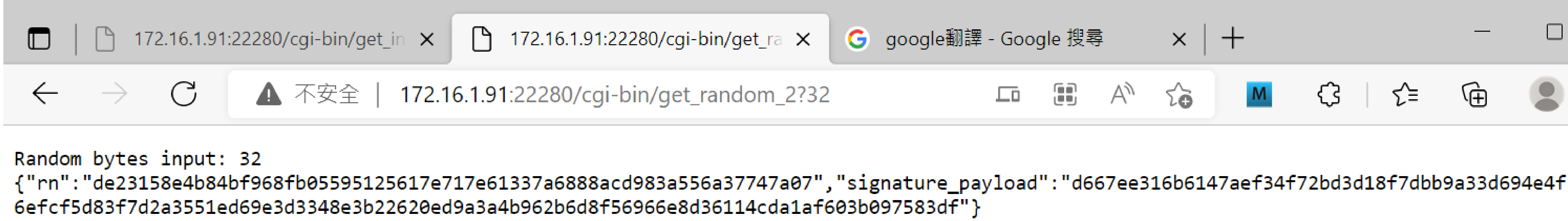
Http – get_random_2 (w/wo Random Bytes Input)

- get_random_2 without random bytes input
  - http://172.16.1.91:22280/cgi-bin/get_random_2


172.16.1.91:22280/cgi-bin/get_in
172.16.1.91:22280/cgi-bin/get_ra
不安全
172.16.1.91:22280/cgi-bin/get_random_2
M

```
Random bytes input:
{"rn":"a1f4c603982d177e","signature_payload":"693a3e16315d7549c30741f58549bea082cbd5187255610dbf6c04b50165c86cf7cf842e6d4223
24aed84389e56f4469c625de954da126e43b72ba9cf58a0fba"}
```

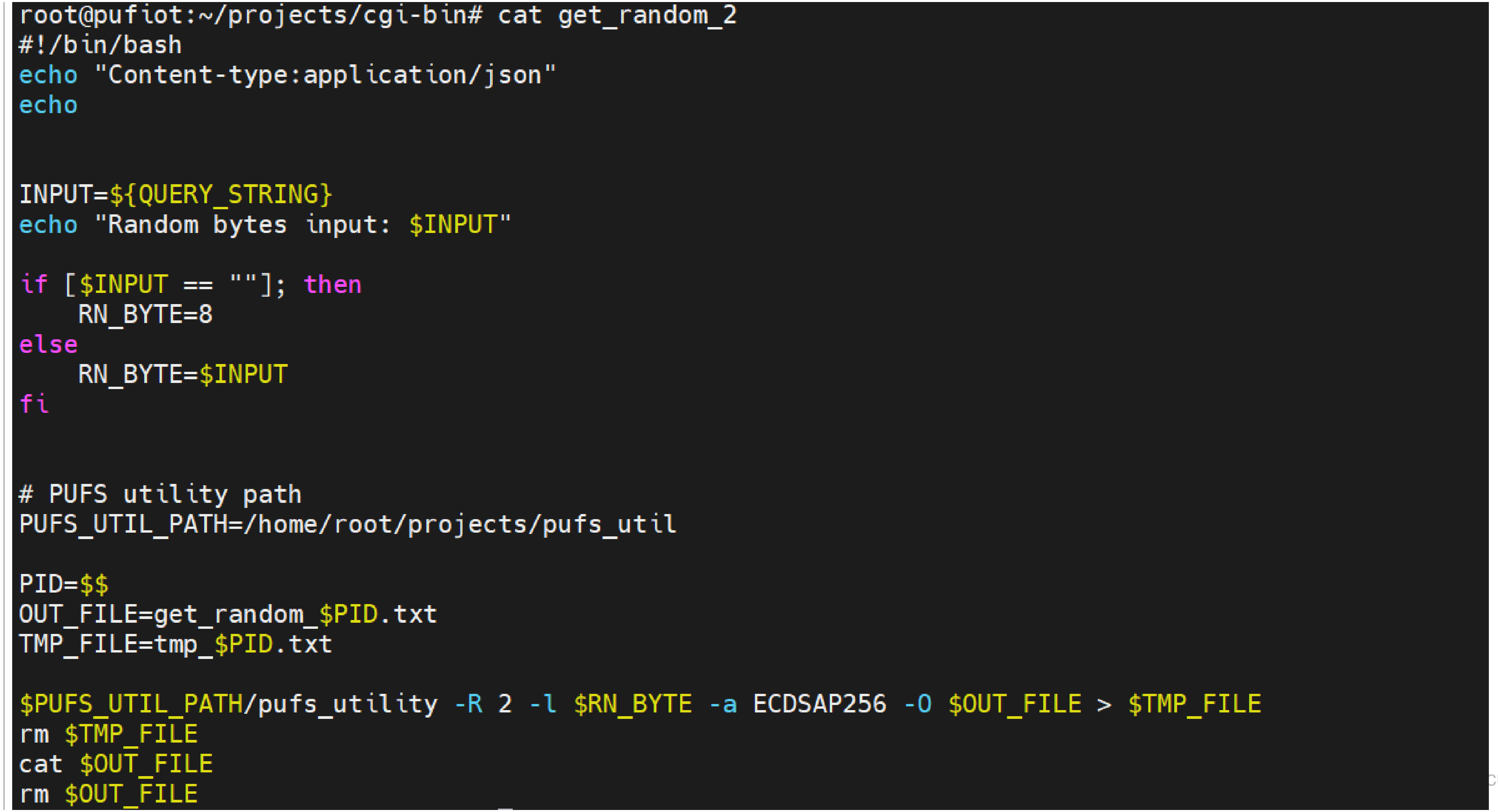
- get_random_2 with 32 random bytes input
  - 172.16.1.91:22280/cgi-bin/get_random_2?32


172.16.1.91:22280/cgi-bin/get_in
172.16.1.91:22280/cgi-bin/get_ra
google翻譯 - Google 搜尋
不安全
172.16.1.91:22280/cgi-bin/get_random_2?32
M

```
Random bytes input: 32
{"rn":"de23158e4b84bf968fb05595125617e717e61337a6888acd983a556a37747a07","signature_payload":"d667ee316b6147aef34f72bd3d18f7dbb9a33d694e4f
6efcf5d83f7d2a3551ed69e3d3348e3b22620ed9a3a4b962b6d8f56966e8d36114cda1af603b097583df"}
```

- Note : max input value : 65535

FPGA Bash Script - get_random_2 with Input Bytes



```
root@pufiot:~/projects/cgi-bin# cat get_random_2
#!/bin/bash
echo "Content-type:application/json"
echo


INPUT=${QUERY_STRING}
echo "Random bytes input: $INPUT"

if [$INPUT == ""]; then
    RN_BYTE=8
else
    RN_BYTE=$INPUT
fi


# PUFS utility path
PUFS_UTIL_PATH=/home/root/projects/pufs_util

PID=$$
OUT_FILE=get_random_$PID.txt
TMP_FILE=tmp_$PID.txt

$PUFS_UTIL_PATH/pufs_utility -R 2 -l $RN_BYTE -a ECDSAP256 -O $OUT_FILE > $TMP_FILE
rm $TMP_FILE
cat $OUT_FILE
rm $OUT_FILE
```