

---

# Heartbleed

Introduction à la sécurité des systèmes d'informations

---

29 décembre 2016



# Introduction

Nous avons choisi de travailler sur la faille nommée *Heartbleed* qui impacte *OpenSSL* entre les versions 1.0.1 et 1.0.1f.

OpenSSL est une librairie utilisée dans de nombreux sites pour chiffrer et authentifier les échanges, notamment par l'utilisation du protocole SSL/TLS.

Malheureusement, suite à une mise à jour, un bug permet à des attaquants de lire la mémoire du serveur vulnérable, qui peut contenir divers éléments tels que mots de passe, logins, clés, cookies de session...

*Les détails techniques (lancement de l'image Docker, exploitation avec Metasploit) sont dans le fichier README.md contenu dans l'archive. Ce rapport ne présente que l'analyse de la vulnérabilité.*

## Des détails sur la faille

### Quelles sont les victimes de cette faille

Les victimes sont les utilisateurs dont l'authenticité et la confidentialité des données n'est plus garantie lors de leurs échanges avec un serveur vulnérable. Les mots de passe pour l'authentification HTTP Basic et les cookies des utilisateurs peuvent être lus depuis la mémoire du serveur par une tierce partie. De plus, si la clé privée associée au certificat a été compromise, des attaques de type Man in the Middle deviennent possibles, l'attaquant pouvant s'authentifier en tant que serveur légitime pour l'échange SSL/TLS. Il peut ainsi écouter tous les échanges entre l'utilisateur et le véritable serveur.

### Fonctionnement de la faille

TLS implémente une fonctionnalité nommée *Heartbeat* qui permet de savoir si un pair est toujours en vie en envoyant un payload. Si le pair est encore en vie, il doit renvoyer ce même payload grâce au code page 2.

L'instruction `n2s` ligne 3 permet de mettre la taille du message (2 octets, donc jusqu'à 65535) dans la variable `payload`. Ensuite, ligne 17, on alloue de la mémoire à `buffer` dépendant de `payload` et donc de la taille du message pour pouvoir ligne 21 copier `payload` octets du message dans la réponse `bp`. Le problème est que le message est contrôlé par l'attaquant et qu'il peut donc très bien envoyer un message de 1 octet en mentant sur sa taille (par exemple le maximum 65535). Ainsi `memcpy` va renvoyer de la mémoire locale récemment libérée pouvant contenir des informations confidentielles.

### Quel type de machine est affecté

Tout serveur utilisant une version d'OpenSSL vulnérable pour des échanges SSL/TLS.

```

1  /* Read type and payload length first */
2  hbtype = *p++;
3  n2s(p, payload);
4  pl = p;
5  if (s->msg_callback)
6      s->msg_callback(0, s->version, TLS1_RT_HEARTBEAT,
7                      &s->s3->rrec.data[0], s->s3->rrec.length,
8                      s, s->msg_callback_arg);
9  if (hbtype == TLS1_HB_REQUEST)
10     {
11         unsigned char *buffer, *bp;
12         int r;
13         /* Allocate memory for the response, size is 1 bytes
14          * message type, plus 2 bytes payload length, plus
15          * payload, plus padding
16          */
17         buffer = OPENSSL_malloc(1 + 2 + payload + padding);
18         bp = buffer;
19         /* Enter response type, length and copy payload */
20         *bp++ = TLS1_HB_RESPONSE;
21         s2n(payload, bp);
22         memcpy(bp, pl, payload);
23         bp += payload;

```

**Listing 1** – Code où se trouve la faille

Le problème a été résolu grâce au code suivant où l'on vérifie la taille du message donné avec la taille réelle.

```

1  hbtype = *p++;
2  n2s(p, payload);
3  if (1 + 2 + payload + 16 > s->s3->rrec.length)
4      return 0; /* silently discard per RFC 6520 sec. 4 */
5  pl = p;

```

**Listing 2** – Correctif du problème

## Résultats de l'exploitation de la faille

Grâce à l'exploitation de la faille, nous arrivons à trouver la clé privée mais qui n'est pas exactement la même que celle donnée à **nginx** comme vous pouvez le voir sur la figure 3. Ceci est dû au fait que les entiers premiers *p* et *q* sont inversés donnant une autre version de la même clé comme nous pouvons le voir dans la figure 2.

Il nous est aussi arrivé de trouver (pas systématiquement) le login et mot de passe lors du **dump** de la mémoire du serveur.

```
~/Projects/3A/CysecHeartBleed/cysec-heartbleed (master x) ● ● > cat /home
172940 default 172.17.0.2 openssl.heartble_264934.txt
-----BEGIN RSA PRIVATE KEY-----
MIIeOwIBAAKCAQEAxKlon5vL3nruCy1SRlKDXP2VU89jFCZYaBV+y23Mq8JlRv
0MoR0KAYlvsAxNS1miqcz/GSV03j7W1UqtLPjP/t5Q3m48dZL9Y3LGIVfeXnpqP4
YCRi3e0GM7bJlGDhYtj0ZVAD2XEewUdgt15oRaXVArzsGentNXek8MciRqGy7C
0oRXVzb8QnJrd+IggVrP0tyKl8nQ2auttHuAoG8KqWq/X7+nSLh3td90XnwiMhL
pFu0+eNI1xF2J0REIY9Zn3lHBsjhKCTWG3vpXa1Pe6LEvcuxYwFwjCVUI29xzCRK
B2AcVgIic029nAWZqTzVL6l+oA8HFmkM6IEewIDAQABAoIBABYcps1EY9h0H+B0
9CNEeE0Z5sPxwd8PM12DwFqb0aL0rVotMYymUpXLM6pZtzHR2IYCGXu3/Mw1WY7J
I9Yj+7zo0XfUfr2Wf+KEfrkrftEURHGnIdHmILwHCvRgWYsyWAILd4mLHwfs02
ZAHf2sAz0dnnSr2bqkBCSVNM9HPzfHNBn8n5EviTmZGFAfoV2mZA42r88f7Z5g2
nc5WPkc0AM9jok49CeJf8R0ZELfYQ82Pmhx2Q0aXBGg3kCEMrTTOHZNriNvyjgy
qnyQAOV60nsEGY4soS3G2ynuFwLiFncqfYnBq8srdAyp0RVXvEU+0V2P5SV90Mv
5TqCzTECgYEA4cEz0FP0AJZb0/NqDYCUSMnytf6JveN4XAMkXlTm3xUQ/6N2G/Em
4RU/dyWG/y1X3F8vmd8jKsgL/bXkfrUfB6C9ZikfS05CjYhsQu26WJ2BWIhoT
s02c/bnq7lRy1jZqLtgFSNfeaijLpa4K0ktBFxGcKf2sPp5omsL+NMCGYEA3WJ+
k/UBpGPum2Q49kP4E4Yj+o3L2cY0UFak5QZI+y3pC+6LCP8t5bFzHpbVe+SftWm
iJVNmtJCGfV0tecIhzBZRV/wKBZ0UMPjvpUQ5E+GW0dQF2M2g5Ute4aPM0hX
1c7UBaqPEJ000aUrVG2WZs0CrgPYwprVpDumurkCgYBueLLwbbpTL0GmrRCRWmM2
094T0mWWD+0u47rAjzWmN/qz0B0Ev5cPP56EgxD1f/MnVfzdgKJtJUj4+DLBI7z
ztq34rTVyCDAoVyyVvxy3UUEILZT551mn1CDn6jwWOK8onGqo+9HoNk9a8jQpcIjg
Zgcpw6Vsxz+rxUnbsuFEQKBgAG7GZyH79Q3lJlCQwHd4v04MMW4KNG5G+XRRKt+b
OP6bPhNyTHf5r9g/rv8rJB3/b1hf8ladPb7Yq1R48iwPEHuUcnWsM4cUZCRsFgy
sZ6AYvLgTc3T5N8fiwP9gt3EMKNPib6r8VoVW4tw4AGN2aylAJflsvmDYgDnHmR
EezRAoGBAKpxJbVNXvRDeLVVR82tLAzN4rmFNAX6+eXX5H0Uo0d3DCbd9kI1cGey
qJEtS0JAL0W2JaRE7y5+HoW+1L0huc3T+auPLUshMIK7BhLxjHHdRiQ5S3sR0LDF
jWFPttU52n4+VABY9PY1cc0A5i12FWT223SuxsVB51Tvm4LESB3
-----END RSA PRIVATE KEY-----

~/Projects/3A/CysecHeartBleed/cysec-heartbleed (master x) ● ● > cat cert.key
-----BEGIN PRIVATE KEY-----
MIIeVQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDEqWiFm8veeu4L
LwrlGUoPE/ZVTz0l8JlJNoFX7LbcyrwmVG/Qyiv0oDKW+wDE1LWakPzP8ZJXTePt
bV5q0s+M/+3lDebJx1kv1jcsY1995eemo/hgJGL4MYztsmUY0Fi2PRUAPZcQTC
5R2C63VKhFpdUBH0wZ6e0ld6TwxYJGoblTw6hFXNvxcm234iCBWs863IqYhDZ
q620e4Cgbwqpar9fv6dIuHe1305efCIyEukW7T540ixEXYnRF4j1k3eUcGy0G0
JNYbe+nFrU97os59y7FjAXCMJVQjb3HMJEoHYBxWA1zTb2cBZmpNm8vqX6gdwcW
aQzoQh57AgMBAAECggEAHlKmZUTL2HQf4HT0I0R4TRLKw/FZ3w8zXYPAPvRos6t
Wi0xjKZ5Lcszqlm3MdHYhgIze7f8zDVZjskjiP7v0g5d9R9HZZ/4or+uSt+0R5s
cach0eZugvAcK9EbB1zJYAgT3iYseLb+zTZkAd/awDPR2edkvZuqEJJU0z0c/N8
c1s3yfk5+J0ZkYUB9qi/aZkDjavzx/tmDadzlY+Rwx4Az20iJt0J4L/xE7MQT/J
DzY+aHHZDRpcEaDeQI0ytNM4dmeuI2/K0DKqfJAA5XrSewQZijyhLcbbkE4XCWIW
dyp9gluryyt0DKk5FVeBRT7RXY9JJVXZgy/L0oLNMOKBgQDhwrNR8/QALLs782oN
gJRIyfk1/om943hcAyReV0bfFRD/o3Yb85bhfT8PJYb/LVfcUDy+YPyMqyAv9tER
9FR8HoL1kiQVLRiKkNiGxC7bplYnYFYiGh0w7Z29ueruWZHLWNmqW0YVI195qKMu
LrgR5S0EXEZWp/aw+nmiaWv40wKBgQ0fAnT9QgK9Y5BzDj2g/QThiP6jEXzXjRQ
VqTLBk7LekL7osKny2/LsXMeLTV75IWlaaILU2aa0KIZ9U615wiHMFfX/AoFnR
Qw+0+LRDkT4ZBR1AXYzapPm5C17ho8ozSFFvzt0Fqo8QlDQ5p5tUzBzmQKukZha
mtU926a6uQKBgG56WXBtUlmVQaatEJFbAzY73hNCZZYP467jusCPPAyf+pmgHQ5/
lw8/noSEDPV/8ydv/Q00Aom0lSPj4MsEjvP02rfitNXIIMChXJVXHLdRR4gtlPLL
WaeUI0fQPB4ryicaqj70eg2TlryNCLwi08mByndHPwzHP6vF5duy4URAOgADsZl
iHv1DeUnUtxDAd3i87gxbg0rkb5dFEp5s4/ps+E3JMD/mv2D+u/yskHf9vWF/z
Vp09tPtirVhYjLA80e5RydwzHxRlX6wWDXnoBi8uBNZdPk3x+LA/2C3c0y00+J
sjqvxWhVbi3DgAY3ZrKUAL+Wy+YNIAM2GER7NECgYEAqnEt1tUe8NF6VVHza0s
DM3iuYU0Dhr55dfkFRSg53cMJt32qjVwZ7KokS1JCMaVbRlPYETLn4ehb7Us6G5
zdP5q4+V5yEwgrsG6EvGmCd1GjBLEzFE6UMWNYU+21Tnafj5UAFj09jYxygDmLVKv
ZPbbdK7GxUHNv098ziURIHc=
-----END PRIVATE KEY-----
```

**FIGURE 1** – Clé privée trouvée grâce à heartbleed à gauche et clé donnée en paramètre à **nginx** à droite

Nous avons les caractéristiques des clés sur la figure page 4 avec à gauche celles de la clé renvoyée par l'*exploit* et à droite celles de la clé donnée en paramètre de **nginx**. On peut donc voir que les paramètres sont les mêmes et que donc la clé qui a été dump est la bonne : avec cette clé, plus aucune donnée n'est protégée.

```

privateExponent:
  1c:82:a6:cd:44:cb:d8:74:1f:e0:74:f4:23:44:78:
  4d:19:4a:c3:f1:59:df:0f:33:5d:83:c0:5a:9b:d1:
  a2:ce:ad:5a:2d:31:8c:a6:52:95:cb:33:aa:59:b7:
  31:d1:d8:86:02:19:7b:b7:fc:cc:35:59:8e:c9:23:
  d6:23:fb:bc:e8:39:77:d4:7d:1d:96:7f:e2:84:7e:
  b9:2b:7e:d1:14:ac:71:a7:21:d1:e6:54:82:f0:1c:
  2b:d1:1b:06:2c:c9:60:08:2d:de:26:2c:78:b0:7e:
  cd:36:64:01:df:da:c0:33:d1:d9:e7:4a:bd:9b:aa:
  40:42:49:53:4c:f4:73:f3:7c:73:5b:37:c9:f9:12:
  f8:93:99:91:85:01:f6:a8:bf:69:99:03:8d:ab:f3:
  c7:fb:67:98:36:9d:ce:56:3e:47:1c:38:03:3d:8e:
  89:38:f4:27:89:7f:c4:4e:cc:42:df:c9:0f:36:3e:
  68:71:d9:0d:1a:5c:11:a0:de:40:84:32:b4:d3:38:
  76:67:ae:23:6f:ca:38:32:aa:7c:90:00:e5:7a:d2:
  7b:04:19:8e:2c:a1:2d:c6:db:29:ee:17:09:62:16:
  77:2a:7d:83:5b:ab:cb:2b:74:0c:a9:39:15:57:bc:
  45:3e:d1:5d:8f:49:25:55:f6:83:2f:e5:3a:82:cd:
  31
prime1:
  00:e1:c1:19:d1:f3:f4:00:96:5b:3b:f3:6a:0d:80:
  94:48:c9:f2:b5:fe:89:bd:e3:78:5c:03:24:5e:54:
  e6:df:15:10:ff:a3:76:1b:f1:26:e1:15:3f:0f:25:
  86:ff:2d:57:dc:50:3c:be:60:fc:8c:ab:20:2f:f6:
  d7:91:f4:54:7c:1e:82:f5:92:24:15:2d:12:24:28:
  d8:86:c4:2e:db:a6:56:27:60:56:22:1a:13:b0:ed:
  9c:fd:b9:ea:ee:59:91:cb:58:d9:aa:5b:46:15:23:
  5f:79:a8:a3:2e:96:b8:2b:49:2d:04:5c:46:70:a7:
  f6:b0:fa:79:a2:6b:0b:f8:d3
prime2:
  00:df:02:7e:93:f5:01:a4:63:d4:9b:64:38:f6:43:
  f8:13:86:23:fa:8d:e5:d9:c6:34:50:56:a4:e5:06:
  48:fb:2d:e9:0b:ee:8b:0a:9f:2d:bf:96:c5:cc:7a:
  5b:55:ef:92:16:d5:a6:88:95:4d:9a:6b:49:08:67:
  d5:3a:d7:9c:22:1c:c1:65:15:7f:c0:a0:59:d1:43:
  0f:8e:fa:54:43:91:3e:19:6d:1d:40:5d:8c:da:a4:
  f9:b9:0b:5e:e1:a3:ca:33:48:57:d5:ce:d4:05:aa:
  8f:10:94:34:39:a5:2b:54:6d:96:66:cd:02:ae:91:
  98:5a:9a:d5:3d:db:a6:ba:b9
exponent1:
  6e:7a:59:70:6d:ba:53:2f:41:a6:ad:10:91:5b:03:
  36:3b:de:13:42:65:96:0f:e3:ae:e3:ba:c0:8f:3c:
  0c:9f:fa:99:a0:1d:04:bf:97:0f:3f:9e:84:83:10:
  f5:7f:f3:27:55:fc:e4:0e:02:89:b4:95:23:e3:e0:
  cb:04:8e:f3:ce:da:b7:e2:b4:d5:c8:20:c0:a1:5c:
  95:57:1c:b7:51:47:88:2d:94:f9:4b:59:a7:94:20:
  e7:ea:3c:16:38:af:28:9c:6a:a8:fb:d1:e8:36:4f:
  5a:f2:34:29:70:88:e0:66:07:29:c3:1e:95:b3:1c:
  fe:af:15:27:6e:cb:85:11
exponent2:
  0e:c6:65:88:7b:f5:0d:e5:27:52:dc:43:01:dd:e2:
  f3:b8:31:6e:0a:34:ae:46:f9:74:51:29:3f:9b:38:
  fe:9b:3e:13:72:4c:77:f9:af:d8:3f:ae:ff:2b:24:
  1d:ff:6f:58:5f:f3:56:9d:3d:b4:fb:62:ad:51:e3:
  c8:b0:3c:41:ee:51:c9:d6:b0:ce:1c:51:97:11:b0:
  58:32:b1:9e:80:62:f2:e0:4d:cd:d3:e4:df:1f:8b:
  03:fd:82:dd:c4:32:43:4f:89:b2:3a:af:c5:68:55:
  6e:2d:c3:80:06:37:66:b2:94:02:5f:96:cb:e6:0d:
  88:03:36:19:91:11:ec:d1

```

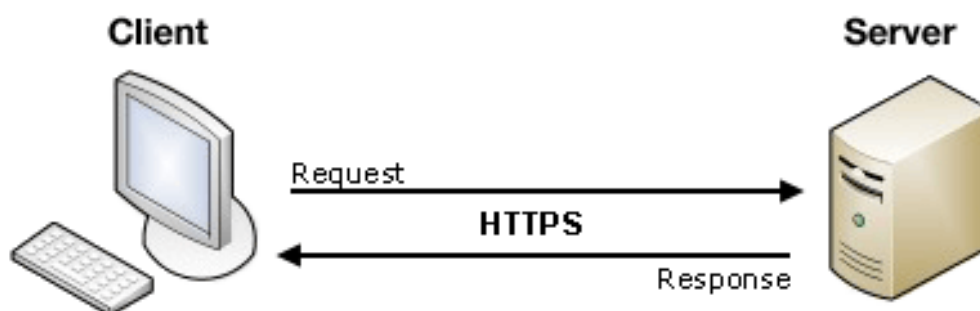
```

privateExponent:
  1c:82:a6:cd:44:cb:d8:74:1f:e0:74:f4:23:44:78:
  4d:19:4a:c3:f1:59:df:0f:33:5d:83:c0:5a:9b:d1:
  a2:ce:ad:5a:2d:31:8c:a6:52:95:cb:33:aa:59:b7:
  31:d1:d8:86:02:19:7b:b7:fc:cc:35:59:8e:c9:23:
  d6:23:fb:bc:e8:39:77:d4:7d:1d:96:7f:e2:84:7e:
  b9:2b:7e:d1:14:ac:71:a7:21:d1:e6:54:82:f0:1c:
  2b:d1:1b:06:2c:c9:60:08:2d:de:26:2c:78:b0:7e:
  cd:36:64:01:df:da:c0:33:d1:d9:e7:4a:bd:9b:aa:
  40:42:49:53:4c:f4:73:f3:7c:73:5b:37:c9:f9:12:
  f8:93:99:91:85:01:f6:a8:bf:69:99:03:8d:ab:f3:
  c7:fb:67:98:36:9d:ce:56:3e:47:1c:38:03:3d:8e:
  89:38:f4:27:89:7f:c4:4e:cc:42:df:c9:0f:36:3e:
  68:71:d9:0d:1a:5c:11:a0:de:40:84:32:b4:d3:38:
  76:67:ae:23:6f:ca:38:32:aa:7c:90:00:e5:7a:d2:
  7b:04:19:8e:2c:a1:2d:c6:db:29:ee:17:09:62:16:
  77:2a:7d:83:5b:ab:cb:2b:74:0c:a9:39:15:57:bc:
  45:3e:d1:5d:8f:49:25:55:f6:83:2f:e5:3a:82:cd:
  31
prime1:
  00:e1:c1:19:d1:f3:f4:00:96:5b:3b:f3:6a:0d:80:
  94:48:c9:f2:b5:fe:89:bd:e3:78:5c:03:24:5e:54:
  e6:df:15:10:ff:a3:76:1b:f1:26:e1:15:3f:0f:25:
  86:ff:2d:57:dc:50:3c:be:60:fc:8c:ab:20:2f:f6:
  d7:91:f4:54:7c:1e:82:f5:92:24:15:2d:12:24:28:
  d8:86:c4:2e:db:a6:56:27:60:56:22:1a:13:b0:ed:
  9c:fd:b9:ea:ee:59:91:cb:58:d9:aa:5b:46:15:23:
  5f:79:a8:a3:2e:96:b8:2b:49:2d:04:5c:46:70:a7:
  f6:b0:fa:79:a2:6b:0b:f8:d3
prime2:
  00:df:02:7e:93:f5:01:a4:63:d4:9b:64:38:f6:43:
  f8:13:86:23:fa:8d:e5:d9:c6:34:50:56:a4:e5:06:
  48:fb:2d:e9:0b:ee:8b:0a:9f:2d:bf:96:c5:cc:7a:
  5b:55:ef:92:16:d5:a6:88:95:4d:9a:6b:49:08:67:
  d5:3a:d7:9c:22:1c:c1:65:15:7f:c0:a0:59:d1:43:
  0f:8e:fa:54:43:91:3e:19:6d:1d:40:5d:8c:da:a4:
  f9:b9:0b:5e:e1:a3:ca:33:48:57:d5:ce:d4:05:aa:
  8f:10:94:34:39:a5:2b:54:6d:96:66:cd:02:ae:91:
  98:5a:9a:d5:3d:db:a6:ba:b9
exponent1:
  6e:7a:59:70:6d:ba:53:2f:41:a6:ad:10:91:5b:03:
  36:3b:de:13:42:65:96:0f:e3:ae:e3:ba:c0:8f:3c:
  0c:9f:fa:99:a0:1d:04:bf:97:0f:3f:9e:84:83:10:
  f5:7f:f3:27:55:fc:e4:0e:02:89:b4:95:23:e3:e0:
  cb:04:8e:f3:ce:da:b7:e2:b4:d5:c8:20:c0:a1:5c:
  95:57:1c:b7:51:47:88:2d:94:f9:4b:59:a7:94:20:
  e7:ea:3c:16:38:af:28:9c:6a:a8:fb:d1:e8:36:4f:
  5a:f2:34:29:70:88:e0:66:07:29:c3:1e:95:b3:1c:
  fe:af:15:27:6e:cb:85:11
exponent2:
  0e:c6:65:88:7b:f5:0d:e5:27:52:dc:43:01:dd:e2:
  f3:b8:31:6e:0a:34:ae:46:f9:74:51:29:3f:9b:38:
  fe:9b:3e:13:72:4c:77:f9:af:d8:3f:ae:ff:2b:24:
  1d:ff:6f:58:5f:f3:56:9d:3d:b4:fb:62:ad:51:e3:
  c8:b0:3c:41:ee:51:c9:d6:b0:ce:1c:51:97:11:b0:
  58:32:b1:9e:80:62:f2:e0:4d:cd:d3:e4:df:1f:8b:
  03:fd:82:dd:c4:32:43:4f:89:b2:3a:af:c5:68:55:
  6e:2d:c3:80:06:37:66:b2:94:02:5f:96:cb:e6:0d:
  88:03:36:19:91:11:ec:d1

```

FIGURE 2 – Caractéristiques des clés privées

## Architecture typique du système information permettant l'exploit



**FIGURE 3** – Modèle client-serveur

Pour exploiter cette faille, il n'y a pas besoin d'avoir une architecture très complexe : un simple client peut être l'attaquant et peut dumper la mémoire du serveur contenant les informations confidentielles. C'est en partie pour cela que la faille est dangereuse. En effet, n'importe qui pouvait en quelques secondes recueillir des mots de passe anonymement sans s'introduire dans le réseau de quelqu'un ou du serveur et sans pouvoir se rendre compte de l'attaque.

### Mesures de sécurité

Il est donc important de mettre à jour *OpenSSL* pour bénéficier des correctifs de la faille. Il existe aussi des scripts qui permettent de voir si son site est vulnérable à ce type de faille. En revanche, il n'existe pas de moyen de "limiter les dégâts" si la version utilisée d'*OpenSSL* est atteinte par le bug.

## HOW THE HEARTBLEED BUG WORKS:

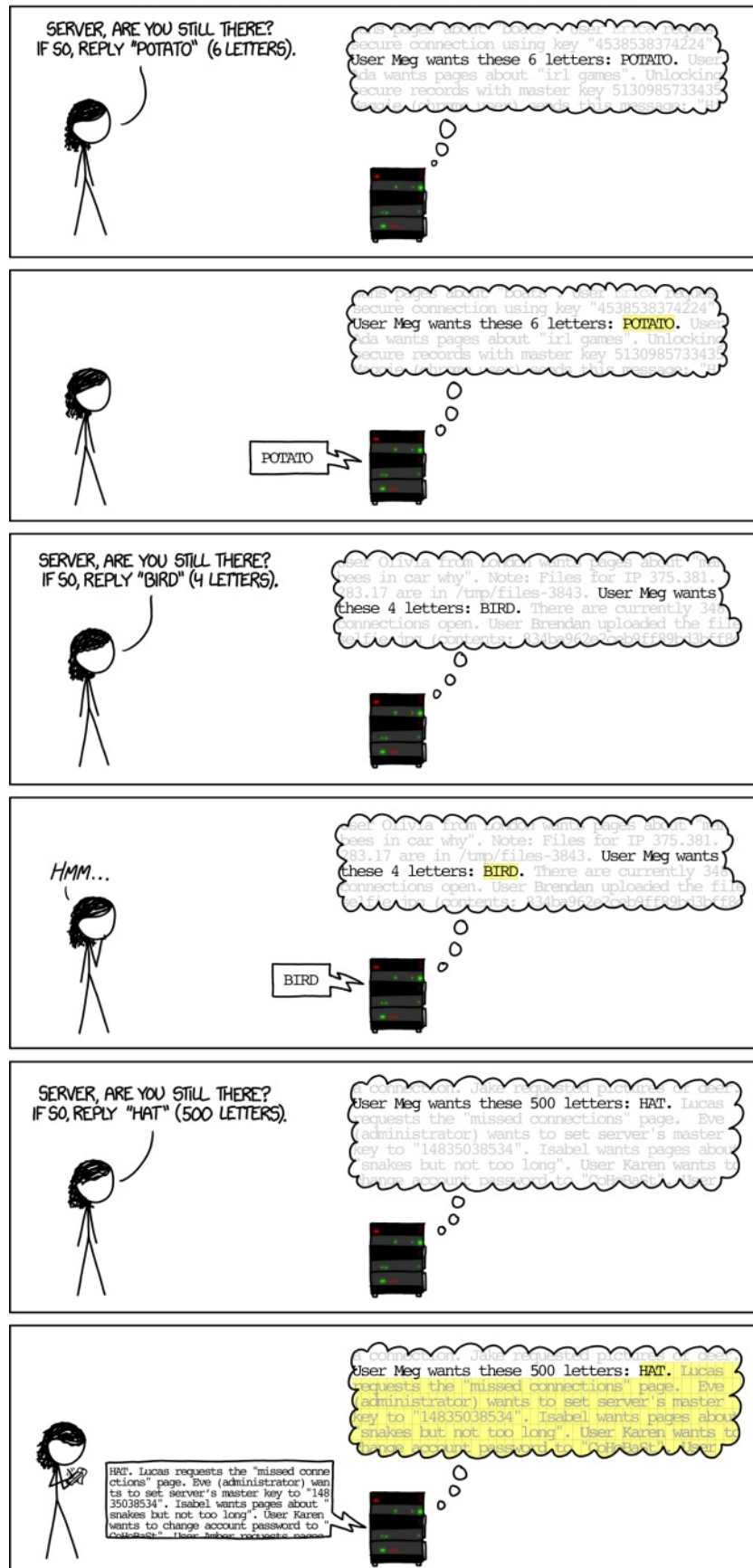


FIGURE 4 – Explication de la faille Hearbleed – XKCD