

Case study: Heartbleed

- SSL is the main protocol for secure (encrypted) online communication
- Heartbleed was a vulnerability in the most popular SSL server

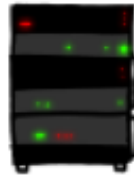


HOW THE HEARTBLEED BUG WORKS:

SERVER, ARE YOU STILL THERE?
IF SO, REPLY "POTATO" (6 LETTERS).



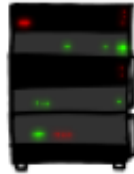
...this pages about "boats". User Erica requests
secure connection using key "4538538374224"
User Meg wants these 6 letters: POTATO. User
Ada wants pages about "irl games". Unlocking
secure records with master key 5130985733435
terrie (chrome user) sends this message: "H



...this pages about "boats". User Erica requests
secure connection using key "4538538374224"
User Meg wants these 6 letters: **POTATO**. User
Ada wants pages about "irl games". Unlocking
secure records with master key 5130985733435
terrie (chrome user) sends this message: "H



POTATO



<https://xkcd.com/1354/>

SERVER, ARE YOU STILL THERE?
IF SO, REPLY "BIRD" (4 LETTERS).



User Olivia from London wants pages about "na
bees in car why". Note: Files for IP 375.381.
283.17 are in /tmp/files-3843. User Meg wants
these 4 letters: BIRD. There are currently 346
connections open. User Brendan uploaded the file
selfie.jpg (contents: 834ba962e2ccb9ff89b43bfff8)



HMM...



User Olivia from London wants pages about "na
bees in car why". Note: Files for IP 375.381.
283.17 are in /tmp/files-3843. User Meg wants
these 4 letters: **BIRD**. There are currently 346
connections open. User Brendan uploaded the file
selfie.jpg (contents: 834ba962e2ccb9ff89b43bfff8)

BIRD



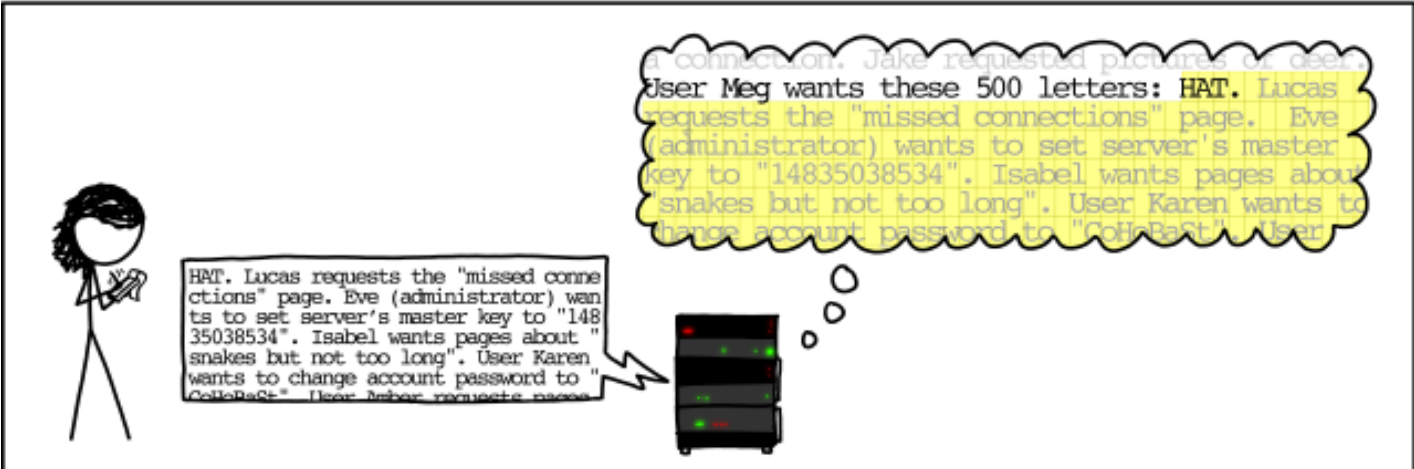
SERVER, ARE YOU STILL THERE?
IF SO, REPLY "HAT" (500 LETTERS).



a connection. Jake requested pictures of deer. User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about snakes but not too long". User Karen wants to change account password to "CoffeeBast". User



Heartbleed: A Closer Look at Buffer Read Overflow



Case study: Heartbleed



- SSL is the main protocol for secure (encrypted) online communication
- Malformed packet allows you to see server memory
 - Passwords, keys, emails, visitor logs
- Fix: Don't let the user tell you how much data to send back!
 - This is a *design* flaw

Heartbleed: A Closer Look at Buffer Read Overflow

- Read Overflow: A bug that permits reading past the end of a buffer.

Read integer
Read message
Echo back
(partial)
message

```
int main() {
    char buf[100], *p;

    while (1) {
        p = fgets(buf, sizeof(buf), stdin);
        len = atoi(p);
        p = fgets(buf, sizeof(buf), stdin);
        for (i=0; i<len; i++) {
            if (!iscntrl(buf[i]))
                putchar(buf[i]);
            else putchar('.');
        }
        printf("\n");
    }
    ...
}
```

***len may exceed
actual message
length!***

Heartbleed: A Closer Look at Buffer Read Overflow

- Sample Output:

```
% ./echo-server
24
every good boy does fine
ECHO: |every good boy does fine|
10
hello there
ECHO: |hello ther|
25
hello
ECHO: |hello..here..y does fine.|
```

OK: input length < buffer size

BAD: length > size !

leaked data