

Anthony Constantino

HW 9

Heartbleed Bug

The HeartBleed bug was discovered recently that had to deal with passwords and popular websites. Pretty much the problem with it is that tons of user information was at risk of being exposed through an error in the openSSL used on these pages. The vulnerability allowed hackers to get access to 64 kilobytes of server memory that could contain usernames, passwords, and all sorts of information from the server on other users' accounts. This was a serious problem and affected possibly 500 thousand websites when it was found. Millions of people were potentially exposed and needed to change information as soon as they could. I remember when this happened and I learned that it is important to not stick with passwords for very long periods of time without giving thought to change them. Based on the article I read, and the comic which I will include, I wondered how something this crucial could slip out into production on such a wide used scale? In my opinion this was the kind of slip that would put companies out of business so how was it exposed for so long without anyone noticing?


Here are the sources I used.

Article - <https://www.cnet.com/news/heartbleed-bug-what-you-need-to-know-faq/>



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

HOW THE HEARTBLEED BUG WORKS:

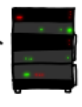
SERVER, ARE YOU STILL THERE?
IF SO, REPLY "POTATO" (6 LETTERS).



...this page from /misc/... User Meg wants these 6 letters: **POTATO**. User da wants pages about "irl games". Unlocking secure records with master key 5130985733435... (about user) sends this message: "8"



POTATO



...this page from /misc/... User Meg wants these 6 letters: **POTATO**. User da wants pages about "irl games". Unlocking secure records with master key 5130985733435... (about user) sends this message: "8"


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



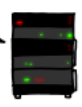
...this page from /misc/... Note: Files for IP 375.381. 83.17 are in /tmp/files-3843. User Meg wants these 4 letters: **BIRD**. There are currently 346 connections open. User Brendan uploaded the file ... (about user) sends this message: "8"



HMM...




BIRD





...this page from /misc/... Note: Files for IP 375.381. 83.17 are in /tmp/files-3843. User Meg wants these 4 letters: **BIRD**. There are currently 346 connections open. User Brendan uploaded the file ... (about user) sends this message: "8"

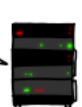
SERVER, ARE YOU STILL THERE?
IF SO, REPLY "HAT" (500 LETTERS).



...connection. User requested page ... 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 ... (about user) sends this message: "8"



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 "P0t0R4c3" (User Andrea requests page ...)



...connection. User requested page ... 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 ... (about user) sends this message: "8"