

Forum:[Hack Forums](#)

Thread: [\[TUTORIAL\] Heartbleed Vulnerability](#)

html - April 17, 2020, 2:35 pm

Hi everyone.

Welcome to another Hacking Tutorial by HTML

Recent Threads:

[\[TUTORIAL\] WiFi Cracking Tutorial - Part 1](#)

[\[TUTORIAL\] Basic DoS | DDoS protection](#)

Introduction:

"Heartbleed is a security bug in the open-source OpenSSL cryptography library, which is widely used to implement the Internet's Transport Layer Security (TLS) protocol. This vulnerability, classified as a buffer over-read, results from a missing bound check in the handling of the Transport Layer Security (TLS) heartbeat extension, the heartbeat being behind the bug's name."

A explanation of heartbleed taken from <https://en.wikipedia.org/wiki/Heartbleed>.

In other words, Heartbleed is a vulnerability that pretty much allows you to obtain data being sent allowing you to obtain information like usernames, passwords, emails, etc.

Which Sites Are Vulnerable:

When this exploit first came out (April 3, 2014) every site using SSL was vulnerable to this causing a very big problem for even the biggest of sites. At 1 point sites like google, Tumblr, etc were vulnerable but most big sites have been patched an hour or a day into the discovery.

Due to this being an old exploit it is mostly patched on all SSL sites but can still be abused on 100's of websites.

These SSL versions are at the moment vulnerable and patched:

OpenSSL 1.0.1 through 1.0.1f (inclusive) are vulnerable

OpenSSL 1.0.1g is NOT vulnerable

OpenSSL 1.0.0 branch is NOT vulnerable

OpenSSL 0.9.8 branch is NOT vulnerable

To find a site that is vulnerable download the following plugins on your web browser:

Chrome Bleed: [Chrome Bleed Link](#)

Firefox Heartbleed: [Firefox Heartbleed Vuln Checker](#)

You may also use 1 of these 2 sites:

<http://tif.mcafee.com/heartbleedtest>

<https://filippo.io/Heartbleed/>

To find vulnerable websites try using this dork in a google search:

inurl:https://

If you wanna target a certain type of site just type in a keyword before the dork I provided. For example:

hunting inurl:https://

How To Exploit Sites:

Found a site? Well now let's find out how to exploit it and be rolling in the accounts. First download bleedout. This program allows you to exploit sites. Put this in a folder as it does create many log files.

Open CMD and type in "CD C:\Users\Your Computer Username\Desktop\Bleedout" In other words just do "CD" command and type in the directory bleedout is located in. After type "bleedout" for info on how to use it or just read what I am about to type up. Type in "bleedout -h (domain name without http://)". Then let this run for hours.

After a while check-in the folder there will be a text file that will have all the scraped info. Open the text file then press "CTRL + F" and type in password. It will show you some results just look through them and try the logins out. That's it, you will have a list of accounts soon enough. Ignore the random text that will be generated, this can be used to obtain an SSL private key but either then that they are just replies from the host.

The official site of heartbleed is: <http://heartbleed.com/>

Disclaimers: This is for educational purposes only! I am not responsible for how you decide to use this exploit.

Warning: A VPN is highly recommended, even though it states this does not make any strange connections to the site it still may be risky and better be on the safe side.

??¢??? - April 18, 2020, 1:54 pm

Um , Title is wrong? The thread is about heartbleed.