Common Vulnerabilities and Exposures

Big CVEs in the last 5 years.

CVE-2014-0160 - Heartbleed

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

CVE-2014-6271 - Shellshock

Shellshock, also known as Bashdoor is a family of security bug in the widely used Unix Bash shell, the first of which was disclosed on 24 September 2014. Many Internet-facing services, such as some web server deployments, use Bash to process certain requests, allowing an attacker to cause vulnerable versions of Bash to execute arbitrary commands. This can allow an attacker to gain unauthorized access to a computer system.

CVE-2017-5638 - Apache Struts 2

On March 6th, a new remote code execution (RCE) vulnerability in Apache Struts 2 was made public. This recent vulnerability, CVE-2017-5638, allows a remote attacker to inject operating system commands into a web application through the “Content-Type” header.

Thanks to

- http://heartbleed.com (http://heartbleed.com)
- https://en.wikipedia.org/wiki/Shellshock_(software_bug (https://en.wikipedia.org/wiki/Shellshock_(software_bug))
- Imperva Apache Struts analysis (https://www.imperva.com/blog/2017/03/cve-2017-5638-new-remote-code-execution-rce-vulnerability-in-apache-struts-2/)