Agenda

- The Shellshock Vulnerability

The Shellshock Vulnerability

image source: shellshock wikipedia

Class Survey

Before today's class, which one of the following statements describes you correctly?

- A. I have never heard of the Shellshock bug.
- B. I have heard of the Shellshock bug, but that's it. I have no idea what exactly it is or what are the techniques behind this bug.
- C. I have heard of the Shellshock bug, I know it has something to do with the Bash Shell, but I don't know further details.
- D. I know what Shellshock bug is, and I can explain it in a detailed fashion.

Terminology

- CVE Common Vulnerabilities and Exposures. CVE-2014-6271.
- Shell Command-line interpreter in operating systems. Reads commands from the console and execute them.
- Environment Variables A set of named values that affect the way a process behaves.
- CGI Common Gateway Interface. Utilized by web servers to run executable programs that dynamically generate web pages.

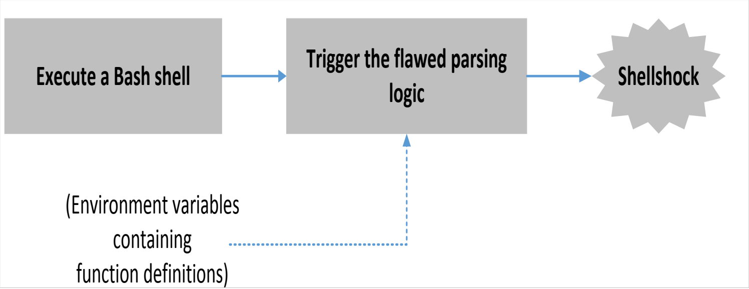
Shellshock

- a security bug in bash (bash shell).
- existing since September 1989.
- discovered in September 2014, announced to public on 24 September 2014.
- bash executes some commands contained in environment variables.

Two Conditions to Trigger Shellshock Vulnerability (Both need to be satisfied)

- invocations of bash
- passing of user data as environment variables

Exploiting the Shellshock Vulnerability



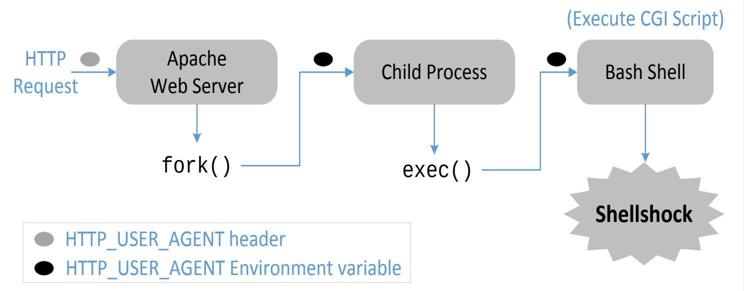
Execute a Bash shell

Trigger the flawed parsing logic

Shellshock

(Environment variables containing function definitions)

Exploiting the Shellshock Vulnerability in CGI programs



References

A large portion of the material is adapted from:

- Computer Security - A Hands-on Approach by Wenliang Du
- The Shellshock Bug In About Four Minutes
  https://www.youtube.com/watch?v=aKShnpOXqn0