Server

A. Name: Apache 2.0. 39 Win32 directory traversal

CVE #: CVE-2002-0661

CVSS base: 7.5

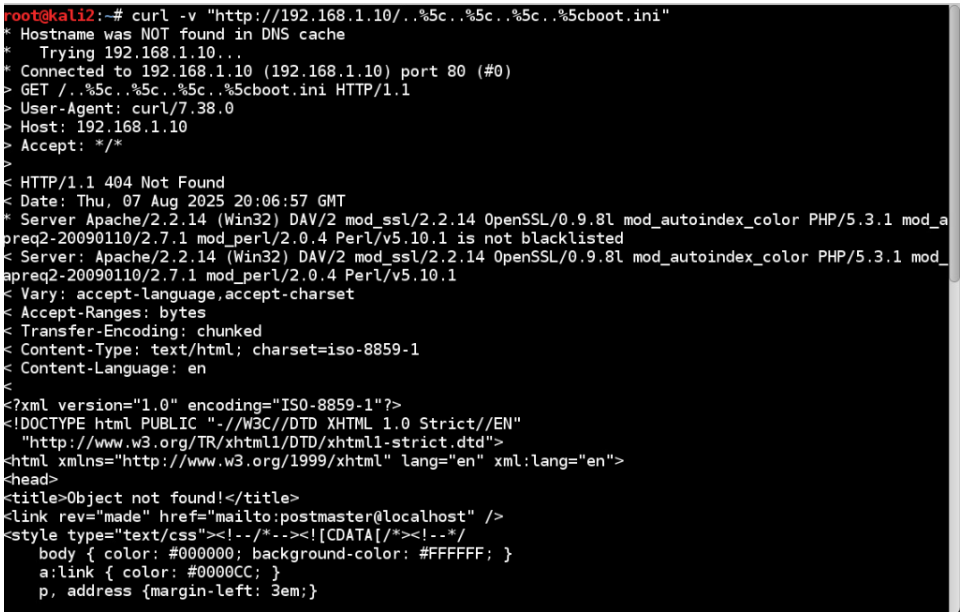
Description: Apache versions 2.0 through 2.0.39 have a flaw that lets attackers use “dot dot” (..) with backslashes in a request to break out of the web folder. This means they could open files they shouldn’t have access to or even run commands on the server, putting sensitive data and the system at risk.

B. In 2002, a vulnerability in Apache 2.0 through 2.0.39 allowed attackers to exploit directory traversal using crafted .. (dot dot) and \ (backslash) sequences to access any file on the system or even execute commands, especially on Windows, OS/2, and Netware setups. Apache reacted quickly by releasing a fix in version 2.0.40. (Debian Security Team, 2002).

C. Evidence of Remediation:

I tried running a directory traversal exploit to grab the boot.ini file from the Windows Server. Instead of giving me the file, the server returned an HTTP 404 Not Found. This means that the file couldn’t be accessed, and since the server is running Apache 2.2.14 instead of the vulnerable 2.0.39, the issue has been fixed.

(Image)



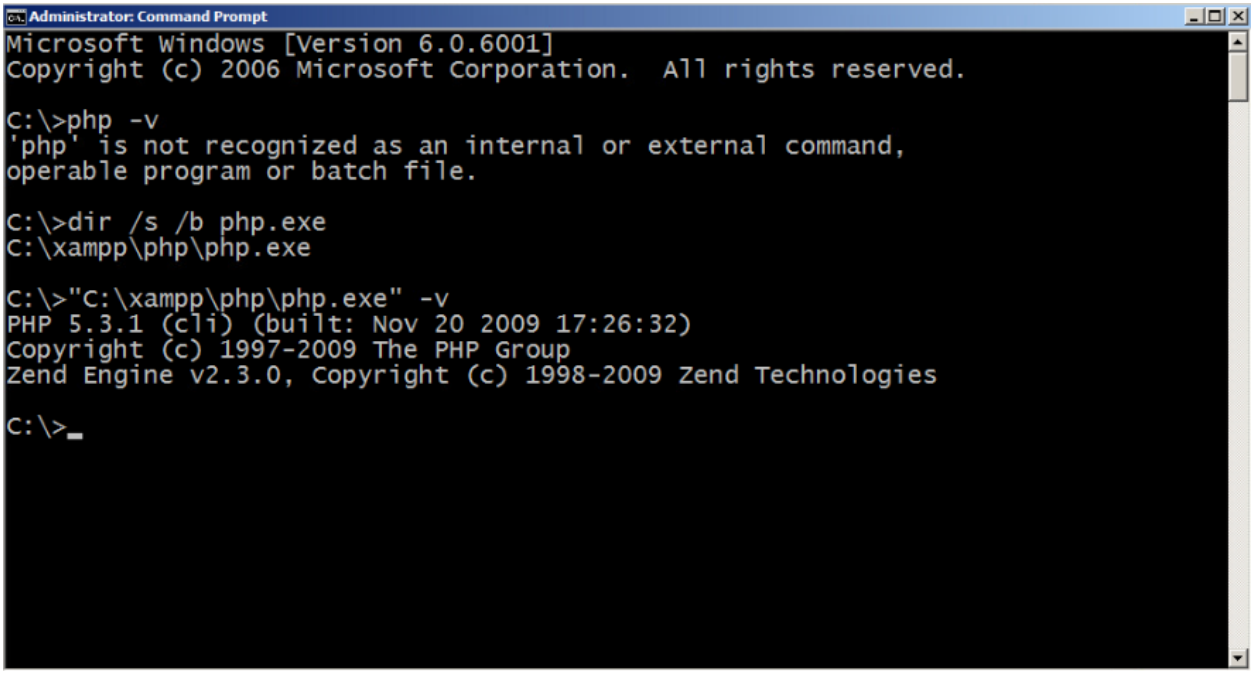
Non-server-related vulnerability

A. **Name: PHP Denial of Service Vulnerability – Aug17 (Windows)**
CVSS: 7.5
CVE: CVE-2017-11362

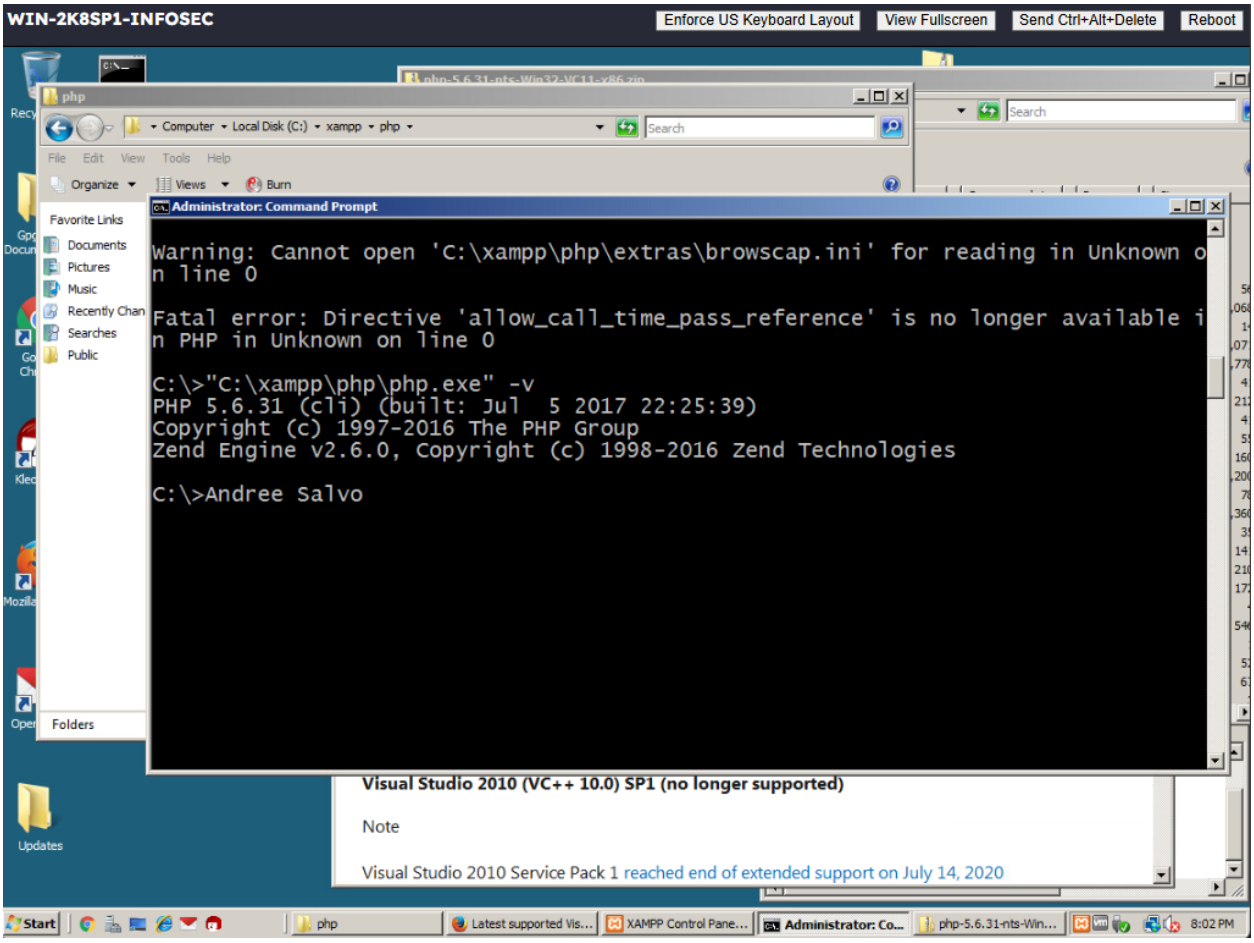
Description: The vulnerability exists because older versions of PHP fail to properly handle very long form variable names in the main/php_variables.c script. A remote attacker can easily exploit this by sending specially crafted requests with extremely long variable names, making the PHP to consume excessive CPU/memory resources and leading to a **Denial of Service (DoS) attacks**.

B. Cybercriminals took advantage of the PHP flaw to incapacitate websites. They did this by dispatching requests that contained form variable names of tremendous length—much longer than typical.

C. **Before Upgrade:** The system was running PHP version 5.3.1, verified using the php -v command from the XAMPP installation directory. This version falls within the vulnerable range identified in the PHP Denial of Service Vulnerability (before 5.6.31), making it susceptible to exploitation.



After Upgrade: PHP was successfully upgraded to version 5.6.31, confirmed using the php -v command from the updated XAMPP installation directory. This version is outside the vulnerable range, addressing the identified Denial of Service vulnerability.



References:

Debian Security Team. (2002, August 18). *Apache directory traversal vulnerability in versions 2.0 through 2.0.39*. Debian Security Mailing List. https://lists.debian.org/debian-security/2002/08/msg00243.html

National Institute of Standards and Technology. (2017, July 17). *CVE-2017-11362 details*. In *National Vulnerability Database*. https://nvd.nist.gov/vuln/detail/CVE-2017-11362