Web Application Pentesting

Vivek Ramachandran

SWSE, SMFE, SPSE, SISE, SLAE, SGDE Course Instructor

Certifications: http://www.securitytube-training.com

Pentester Academy: http://www.PentesterAcademy.com

Command Injection - Filters

Sanitizing Input

- Replace or Ban arguments with ";"

- Other shell escapes available e.g.
  - &&
  - |
  - …

PHP API for Escaping

escapeshellarg

(PHP 4 >= 4.0.3, PHP 5)

escapeshellarg — Escape a string to be used as a shell argument

Description

string **escapeshellarg** (string *$arg*)

escapeshellarg() adds single quotes around a string and quotes/escapes any existing single quotes allowing you to pass a string directly to a shell function and having it be treated as a single safe argument. This function should be used to escape individual arguments to shell functions coming from user input. The shell functions include exec(), system() and the backtick operator.

http://www.php.net/manual/en/function.escapeshellarg.php

escapeshellcmd

(PHP 4, PHP 5)

escapeshellcmd — Escape shell metacharacters

Description

string **escapeshellcmd** (string *$command*)

escapeshellcmd() escapes any characters in a string that might be used to trick a shell command into executing arbitrary commands. This function should be used to make sure that any data coming from user input is escaped before this data is passed to the exec() or system() functions, or to the backtick operator.

Following characters are preceded by a backslash: ***#&;`|*?~<>^()[]{}$***, ***\x0A*** and ***\xFF***. **'** and **"** are escaped only if they are not paired. In Windows, all these characters plus **%** are replaced by a space instead.

http://www.php.net/manual/en/function.escapeshellcmd.php

You have been warned!

Category: Application (Generic) > PHP

Vendors: PHP Group

PHP escapeshellarg() and escapeshellcmd() Parsing Flaws May Let Remote Users Execute Arbitrary Commands

SecurityTracker Alert ID: 1010410
SecurityTracker URL: http://securitytracker.com/id/1010410
CVE Reference: CAN-2004-0542 *(Links to External Site)*
Updated: Jun 10 2004
Original Entry Date: Jun 7 2004
Impact: Execution of arbitrary code via network, User access via network
Fix Available: Yes **Vendor Confirmed:** Yes
Version(s): 4.3.6 and prior versions
Description: An input validation vulnerability was reported in PHP in the escapeshellarg() and escapeshellcmd() functions. A remote user may be able to bypass the escape function to execute arbitrary commands. Windows-based systems are affected.

Daniel Fabian reported that on Windows platforms, the escapeshellarg() function contains a flaw. A remote user may be able to supply specially crafted input to execute commands on the target system. The specific impact depends on the script that implements the vulnerable function.

The report indicates that the escapeshellcmd() is also affected.

The vendor was reportedly notified on April 4, 2004.

The vendor has confirmed this vulnerability in an announcement, available at:

http://www.php.net/release_4_3_7.php
Impact: A remote user may be able to execute arbitrary commands via a script that implements the vulnerable function.
Solution: The vendor has released a fixed version (4.3.7), available at:

http://www.php.net/downloads.php
Vendor URL: www.php.net/ *(Links to External Site)*
Cause: Input validation error
Underlying OS: Windows (Any)

Message History: None.

http://www.securitytracker.com/id/1010410

Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

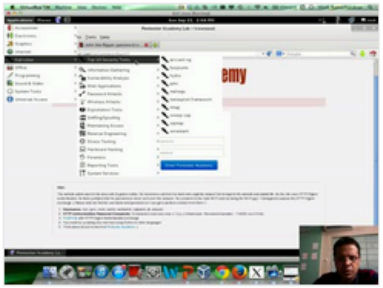
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

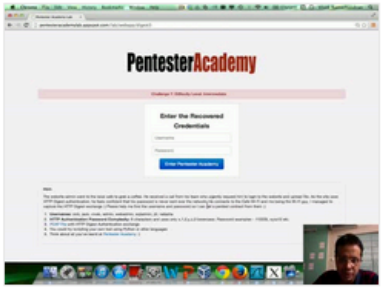
Start Learning Today!

Latest Videos

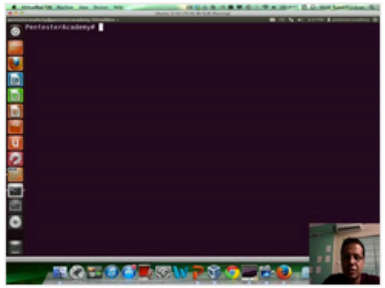
New content added weekly!



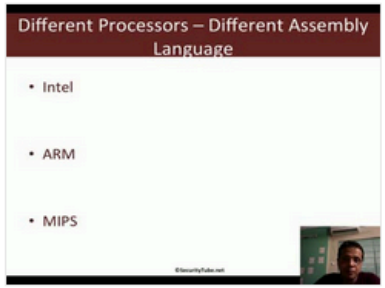
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



Challenge 7: Cracking Digest Authentication in WAP Challenges



Module 1: GDB Test Solution in x86_64 Assembly Language and Shellcoding on Linux



Module 1: CPU Information in x86_64 Assembly Language and Shellcoding on Linux