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

©SecurityTube.net

Remote File Inclusion Vulnerability Basics

©SecurityTube.net

Remote File Inclusion

- User editable input is used to include other files in execution flow
- Input is not sanitized and can lead to arbitrary files being included by a malicious user
- In PHP, include, include_once, require, require_once are responsible for File Inclusions

©SecurityTube.net

Typical Vulnerable File

```
<?php

        echo "File included: ".$_REQUEST["file"]."<br>";
        echo "<br><br>";
        include $_REQUEST["file"];
        echo "<br><br>";

?>
```

©SecurityTube.net

Required PHP Configuration for RFI

/etc/php5/apache2/php.ini

```
814
815 ; Whether to allow include/require to open URLs (like http:// or ftp://) as files.
816 ; http://php.net/allow-url-include
817 allow_url_include = On
```

©SecurityTube.net

Pentester Academy

PentesterAcademy a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

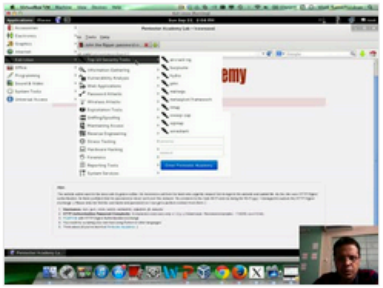
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

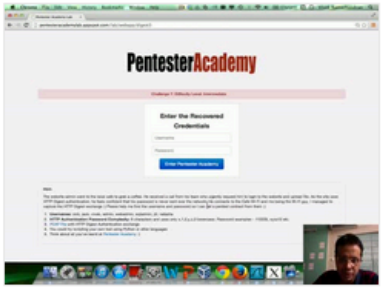
Start Learning Today!

Latest Videos

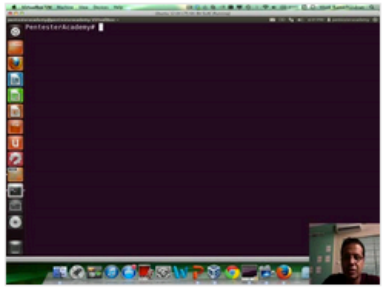
New content added weekly!



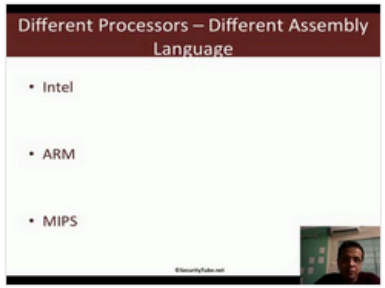
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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

©SecurityTube.net