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

Exploiting RFI with forced extensions

Typical Vulnerable File

```
<?php

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

?>
```

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
```

Beating forced extensions

- Make the extension useless and append any of the following
  - ?
  - %23 (#)
  - ?%26as= (?&as=)
- Attacker can rename file to whatever extension is needed
  - e.g. simple-backdoor.php.html

Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

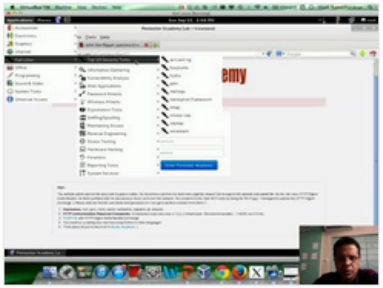
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

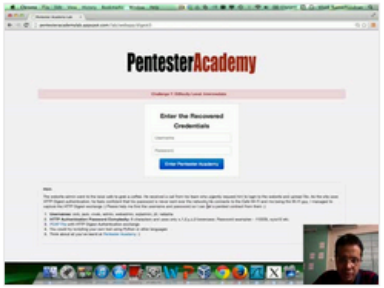
Start Learning Today!

Latest Videos

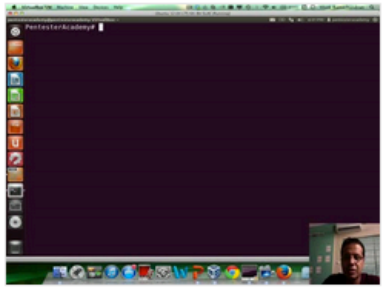
New content added weekly!



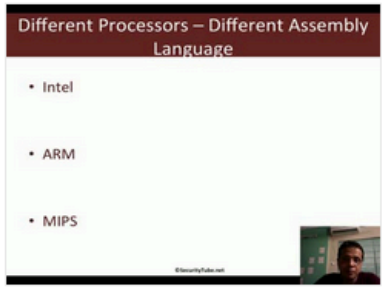
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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