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 Code Execution with LFI and File Upload

©SecurityTube.net

LFI + File Upload to RCE

- Upload Image file with embedded PHP code
  - double extensions disabled
- Use LFI to execute image file

©SecurityTube.net

Vulnerable Code

```
<?php

        $page = $_REQUEST["page"];
        echo "File included: $page<br>";
        echo "<br><br>";
        $local_file =  "html/".$page.".html";
        echo "Local file to be used: ".$local_file;
        echo "<br><br>";

        include $local_file;

?>
```

©SecurityTube.net

Pentester Academy

PentesterAcademy a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

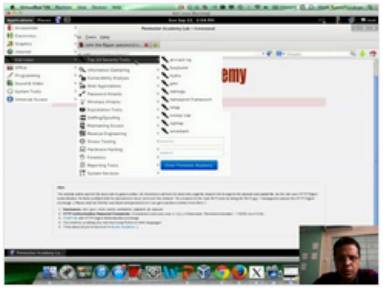
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

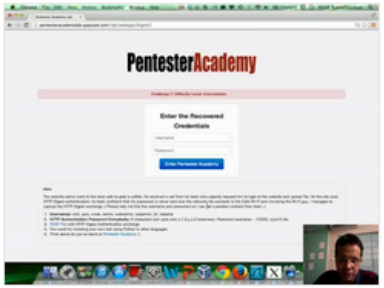
Start Learning Today!

Latest Videos

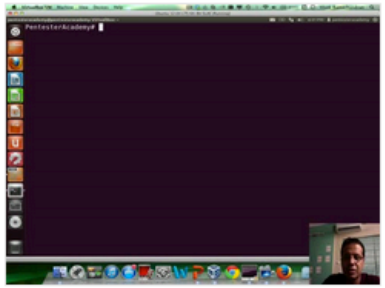
New content added weekly!



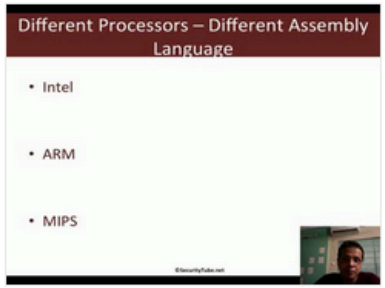
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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