

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>

Bypassing Blacklists using PHPx

Blacklist of Disallowed Extensions

```
$notAllowed = array('php');

$splitFileName = explode(".", $_FILES["file"]["name"]);

$fileExtension = end($splitFileName);

if(in_array($fileExtension, $notAllowed))
{
    echo "Please upload a GIF file";
}
else{

    echo "Name: " . $_FILES["file"]["name"];
    echo "<br>Size: " . $_FILES["file"]["size"];
    echo "<br>Temp File: " . $_FILES["file"]["tmp_name"];
    echo "<br>Type: " . $_FILES["file"]["type"];

    move_uploaded_file($_FILES["file"]["tmp_name"], "uploads/" . $_FILES["file"]["name"]);
}
```

php3, php4, php5

- php 3/4/5 are allowed extensions and supported by default

Arbitrary File Upload Vulnerable ISO



securitytube:123321

Download

- <https://sourceforge.net/projects/arbitraryfileuploados>
 - user:pass = securitytube:123321
- created by Ashish Bhangale
- Bugs and Issues:
 - ashish@binarysecuritysolutions.com

Pentester Academy

PentesterAcademy

a SecurityTube.net initiative



TOPICS

PRICING

WHY SUBSCRIBE

MEMBER ACCESS



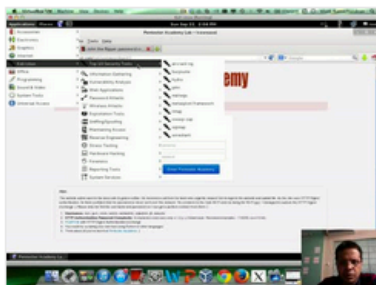
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

Start Learning Today!

Latest Videos

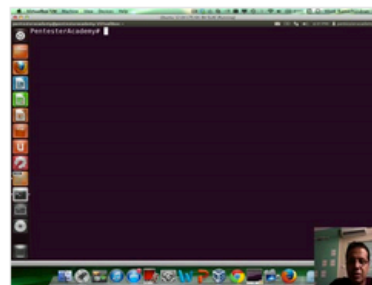
New content added weekly!



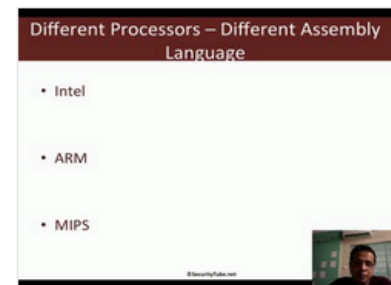
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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