

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>

Types of XSS

XSS Types

- Persistent
- Non-Persistent
- DOM based

Persistent / Type-1

DVWA

Vulnerability: Stored Cross Site Scripting (XSS)

Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout

Name *
Message *

Name: test
Message: This is a test comment.

More info
<http://hacker.org/xss.html>
http://en.wikipedia.org/wiki/Cross-site_scripting
<http://www.cqisecurity.com/xss-faq.html>

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

<http://www.dvwa.co.uk/>

Non-Persistent / Type II

The screenshot shows a web browser window with the URL `pentesteracademylab.appspot.com/lab/webapp/html/1`. The browser's address bar includes navigation icons and a search box. The page content features the **PentesterAcademy** logo at the top. Below the logo, a pink horizontal bar displays the text "Challenge 16: Difficulty Level: Beginner". The main content area contains a white sign-in form with the heading "Please sign in". The form includes two input fields for "Email address" and "Password", a checkbox for "Remember me", and a blue "Sign in" button. Below the form, a section titled "Objectives:" lists two tasks: "1. Add a Custom Message to the Page" and "2. Replace the existing form with your own". A "Hints:" section below that lists: "1. There is no 'Challenge Cracked' page :)" and "2. Remember what you have learn at [Pentester Academy](#)".

pentesteracademylab.appspot.com/lab/webapp/html/1

ng Started Latest Headlines screen recorder ... Home Learn Pentestin...

PentesterAcademy

Challenge 16: Difficulty Level: Beginner

Please sign in

Email address

Password

Remember me

Sign in

Objectives:

1. Add a Custom Message to the Page
2. Replace the existing form with your own

Hints:

1. There is no "Challenge Cracked" page :)
2. Remember what you have learn at [Pentester Academy](#)

Pentester Academy

PentesterAcademy

a SecurityTube.net initiative



TOPICS

PRICING

WHY SUBSCRIBE

MEMBER ACCESS



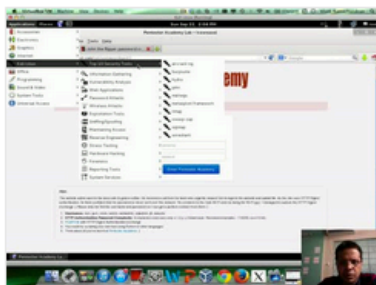
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

Start Learning Today!

Latest Videos

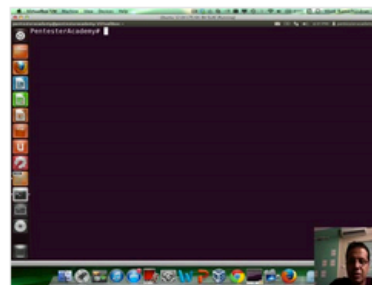
New content added weekly!



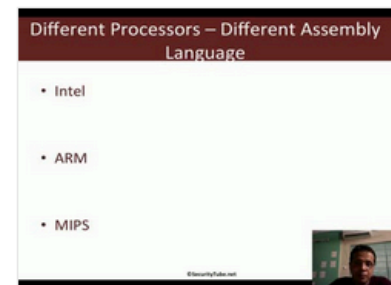
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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