PenTest Lab Exercise Ex120 – Brian's Project

Goal

Uncover remote code execution in a web site.

Tasks

1. Tina Tester is back from Asia now. (Apparently Tina was not cut out for a life of contemplation on the mysteries of the universe without the trappings of big city life one finds in a metropolis like Hoggetowne.) Looking over some packet captures they found there was traffic going to `http://www.artstailor.com/brian`. Tina found that Brian Oppenheimer's TikTok Bio has a link to this web page. In one of his recent videos, Brian talks about his first PHP web project, so he's likely to have made at least a mistake or two. Hank Hacker wants you to take a look at the website and see how far down the rabbit hole you can climb.

2. Tools that you might want to use include `nikto`, `burpsuite` or `tamper chrome`, and perhaps `php-reverse-shell.php` (which can be found in `usr/share/webshells/php`) to achieve the outcome you desire. Using a php reverse shell (which must connect to a listener on a specific host and port) or a php shell (like `Laudanum`'s shell) that requires user credentials, is much preferable to using an unauthenticated back-door to get access to a machine.

3. You'll see that there is an administrative page on this server, but it seems to be password protected. You should be able to find a way to exfiltrate htpasswd credentials from that server. Credentials that provide web content modification often allow you to gain greater access.

4. Find a way to access sensitive data (credentials that provide access as the
tt www-data user) from the host (provide evidence of this in your report).

5. Write a report discussing your method of access and identifying any vulnerabilities you identified. Explain what files you can exfiltrate from the host. Identify what kind of protections or policies might be instituted to prevent the sorts of vulnerabilities you found.

6. You should easily be able to information of value to you if you can exploit a vulnerability in th PHP application.