Hack this site realistic mission 03

This document is written by Adam and is intended for further understanding of the realistic challenges on HackThisSite. The idea behind this document and the ones that follow is that I am explaining what you will need to do, look for and execute. I will also explain why you need to do what I do in these tutorials to create a better understanding of the vulnerabilities, scenario and exploits used.

Link: https://www.hackthissite.org/missions/realistic/3/

Message: I run this website where people can read and submit peace-related poetry. I am doing this out of goodwill towards others, and I don't see why I would be making enemies out of this, but some real ass hole hacked my website posting a bunch of ignorant aggressive propaganda on the front page. And I made that website a while ago, and I no longer have access to it. Do you think you can hack in and change it back? Please? Oh, and bonus points if you message me the name of the bastard who did this!

Vulnerability: Directory Traversal Attack (Path Traversal).

Path traversal allows attackers to read and sometimes write to files on a server. ../ in the URL or input fields allows an attacker to navigate through different directories in the server. ../../../etc/passwd for example.

So first, remember in the last post I spoke about analysing source code, reading comments and scrolling up and down, in and out of web pages looking for hidden clues? We'll use CRTL U to view the webpages source code. As you see the source code is in one long line that is generally unreadable and isn't efficient at all to read, you can either copy and paste the whole thing and use an HTML formatter to make it readable code but in this case, as you can see if you scroll down to the bottom of the pages source code some comments tell us what we need to do.

“<!--Note to the webmaster This website has been hacked, but not totally destroyed. The old website is still up. I simply copied the old index.html file to oldindex.html and remade this one. Sorry about the inconvenience.- >”.

So if you know anything about web servers then you will know about the different directories that a web server has, well in this case we care about two things in the comment, “oldindex.html and index.html”. To put it simply we want “index.html to be the source that viewers see, currently, it’s a defacement however with a directory traversal “attack” you can push to “oldindex.html” to index.html, what this does is it pushes the defacement down and raises the old home page up therefor allowing viewers to see the original source and not the defacement.

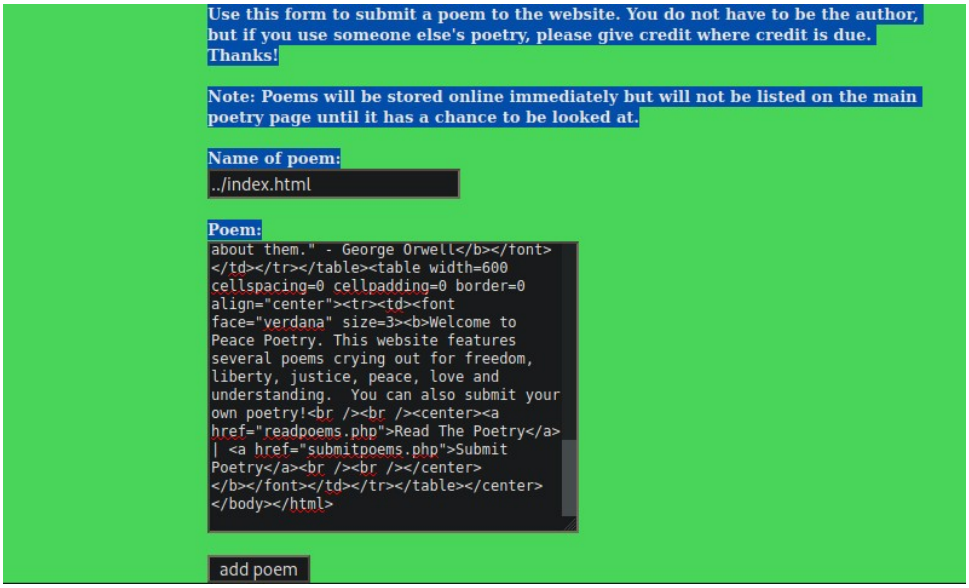
So to do this we’ll need to use a directory traversal technique where ../ corresponds to one directory.

My first thought would be to do an XXS exploit, however after reading “oldindex.html and index.html” it’s clear that we're talking about directories on the webserver so my second thought would be a directory traversal attack exploit.

So now go to the URL and append “oldindex.html” at the end of the current URL. [https://www.hackthissite.org/missions/realistic/3/oldindex.html].

Old site:

From what I can see the site allows users to publish material to the website. There are two links to follow here, one is “Read The Poetry” and the other is “Submit Poetry”. The goal of the CTF challenge is to replace the defacement with the old websites homepage, so to do this view the source of the webpage, copy the source, go to “submit poetry” and in the input field for your poetry copy the webpage source in the field.



From here you need to paste the source of the webpage into the Poem field and then go to the “Name of Poem” which publishes a title for the poem and enter “../index.html” which will push the poem contents to index.html replacing the defacement with the original webpage (home page). Index.html is regarded as the main page or the home page. In a real scenario, the admin will need to delete the defacement, but in this scenario, someone is asking a hacker to help out without admin privileges.

There you have it, you have now completed this CTF challenge.