Cameron Clark

3/9/2017

**Homework 3 Writeup**

When scanning a web server you can get an idea of what is configured on the back end by the files you can access. For example, if you are able to access a .php file, you can then assume that the php module is enabled on the server. Another example is if you can access a .asp file then you can assume that the server is running an ASP.NET framework.

There are a few different ways to increase the speed of my scanner. Implementing threading throughout the whole application and not just downloading the images would help the spidering aspect. Also using a more efficient search algorithm like Dijkstra's or BFS would allow for a faster scan of each website.

When scanning the website, looking for response codes only within the 200 and 300 range will be much more efficient. Those two status ranges mean that it’s either there or it’s been moved somewhere else, either which way you’re on the right track. Any other status codes can just be ignored as they mean nothings in that specific directory. As a side note however, 500 codes can be considered, as it means you caused something to failed on the servers end, this can be investigated later.

A few naming patterns for directories that are commonly seen in web servers are /images, /admin, /includes, /users, /about. These would normally be found on an traditional web server as they contain common material.