Kayla Hodgson

10/04/2021

CSEC 380

Professor Sanders

Homework 3 - Activity 4 Write up

1. Is there certain information about the web server that you can discern based on what files you can access?
    a. Files can help determine what type of webserver is running and the technologies associated with that.
2. Are there any ways to improve the speed of your scanner?
    a. Through the use of HEAD requests, it can significantly improve the speed of the web scanner. Using a HEAD request is better because of the fact we don't actually need to view the content of the website at least for a brute force attack. Additionally, there are common directories you could scan for to get a hit before moving on to the less common ones.
3. How can response codes be used in order to more efficiently search your site?
    a. Through the use of response codes, it's much easier to determine if you need to do any additional receiving of data/information from the site because of the fact that if you have a 301 or 404 error, these can be handled completely differently. With 301, you can parse the redirect and make a request to the new url. With a 404, you don't need to handle anything at all and can drop the request/response. There is no

need to brute force error response codes as they will not return sufficient information that is needed.

4. Are there any common naming patterns that you might expect would yield positive results?
    a. Yes, admin, backup or wordpress can all be potential keywords that would yield positive results. There is a potential for sensitive credentials to be stored in one or more of these naming patterns. But also you can determine what web server may be running if you can find an associated domain like Wordpress or Weebly.