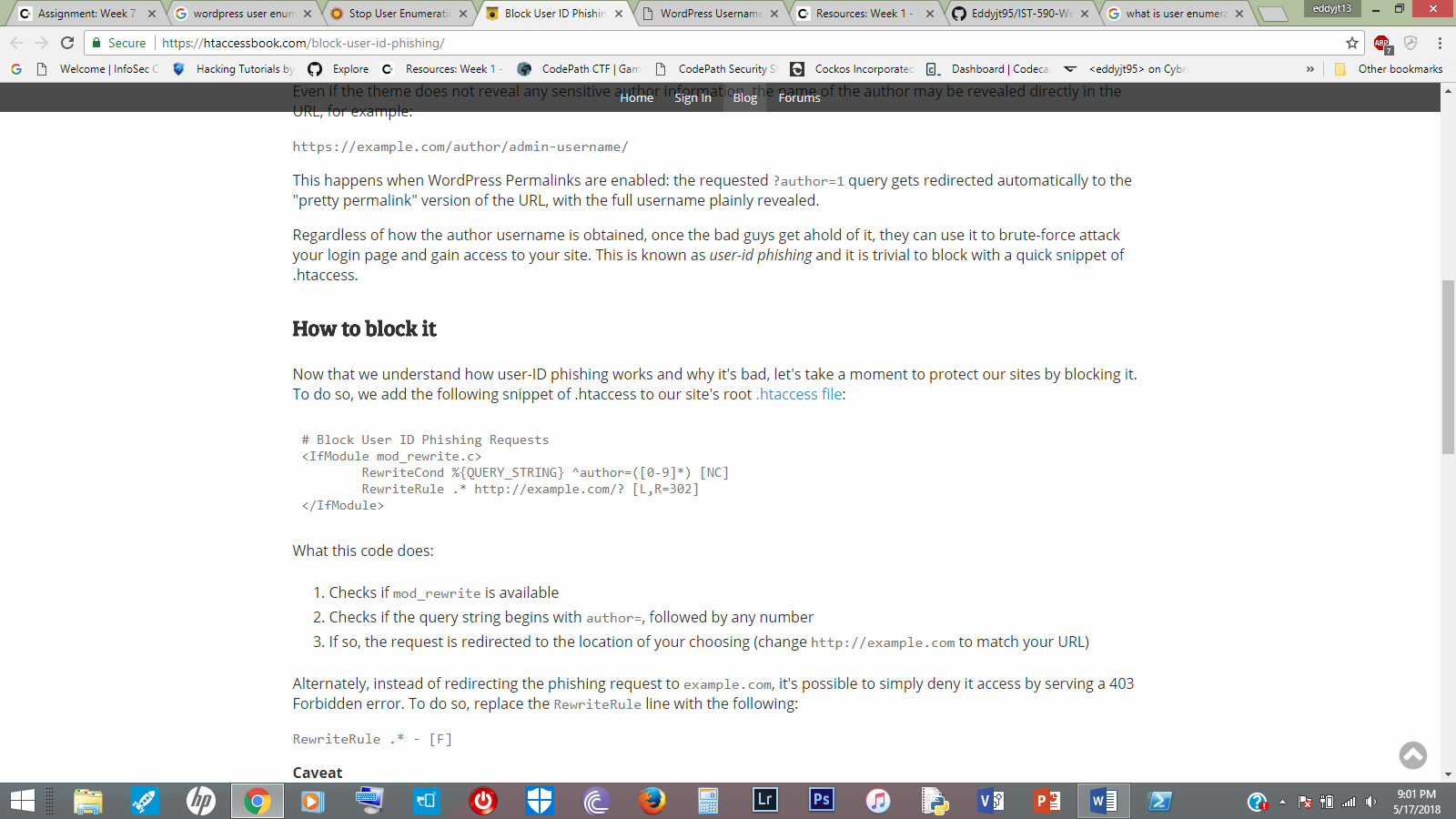
User Enumeration: user-ID phishing

User Enumeration is the process of guessing a combination of usernames and passwords to determine a legitimate user. Normally, the attacker would be able to locate the usernames first since they are easily accessible, leaving the password to be dealt with; Word Press contains this flaw. According to Jeff Star, a blogger for Ht Access Book, explains that a Word Press site can be scanned for user IDs by submitting a URL request like the following: <https://example.com/?author=1> (Starr 2017). He furthers explains that “?author=1” would reveal the full username. User Enumeration, or user-ID phishing, is dangerous because obtaining a username is half the battle, the next step is to solve the password, which can be bruteforced. Starr proceeds to describe how to effectively prevent a username scan from happening with some code he provided:

Starr broke down the code for easy comprehensibility. Firstly, the code checks whether “mod\_rewrite” is available; secondly, the code determines whether the request contains a “author=()” string, where a number is available in place of the paretheses; thirdly, if both conditions are true then the request will send the malicious user to another section of the website (2017). Alternatively, Starr mentions that malicious users can be sent to a 403 Forbidden error page by replacing the “RewriteRule” line with “RewriteRule .\* - [F]”

References

Starr, Jeff. “Block User ID Phishing Requests.” .Htaccess Made Easy, Htaccessbook, 19 Mar. 2017, htaccessbook.com/block-user-id-phishing/.