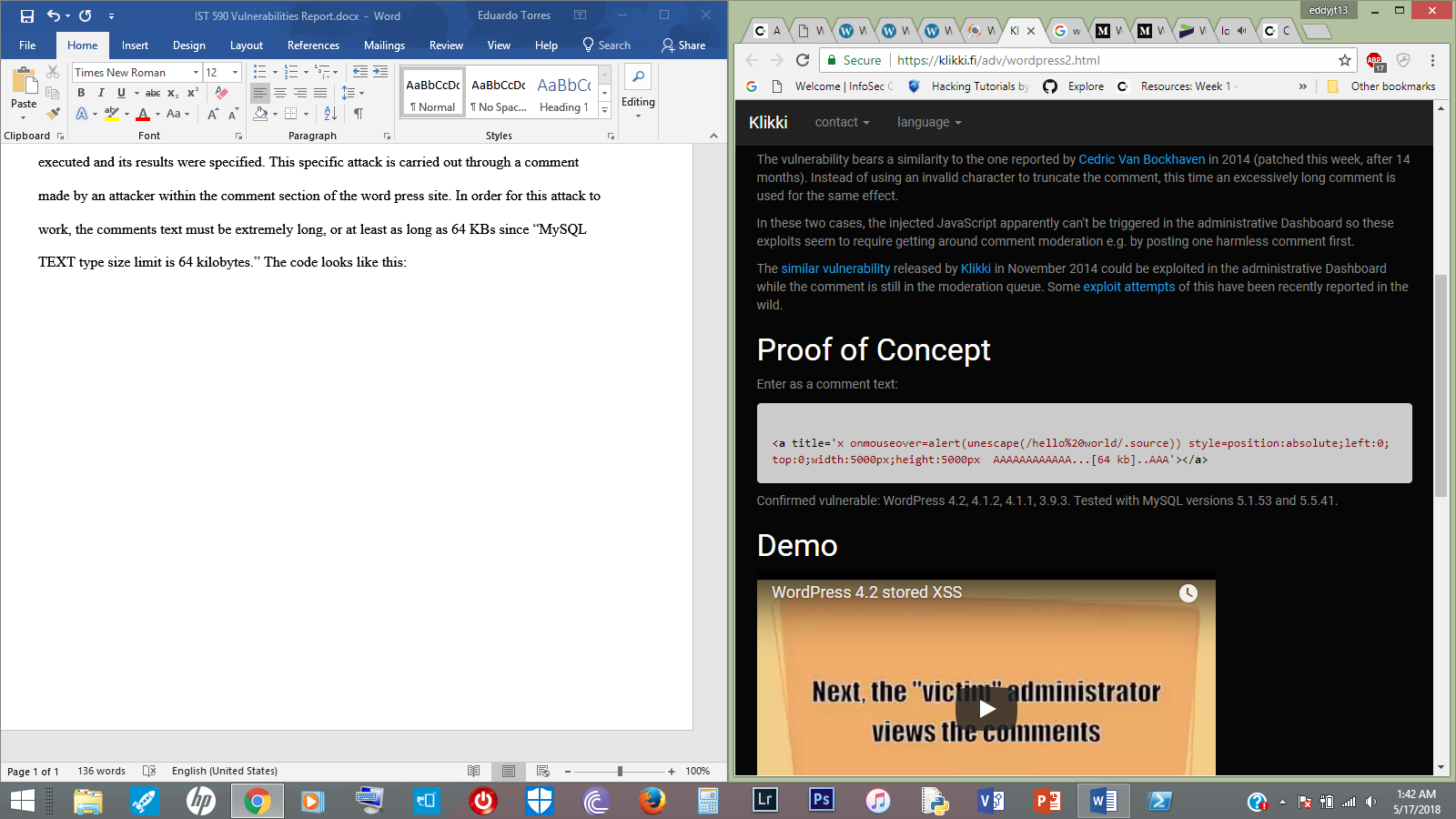
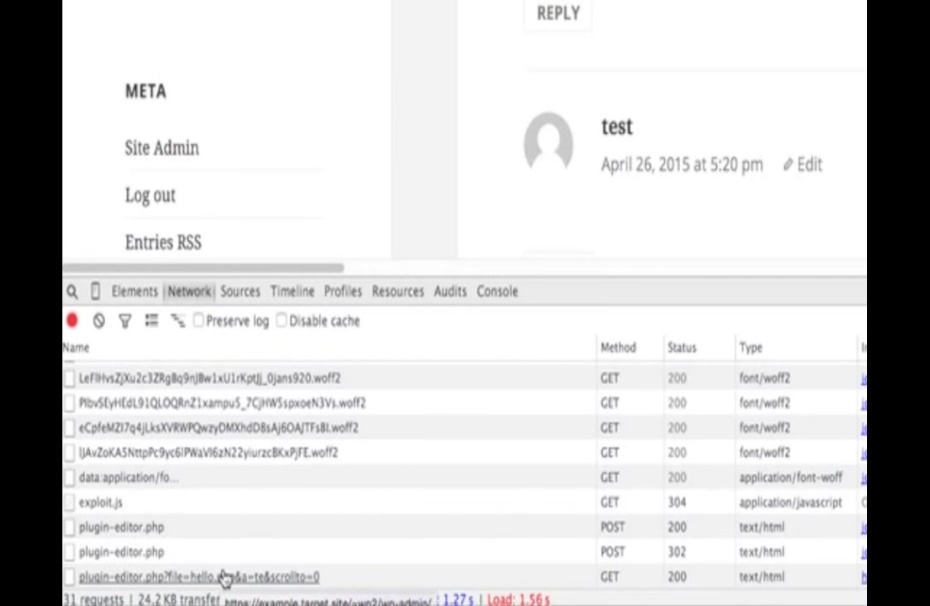
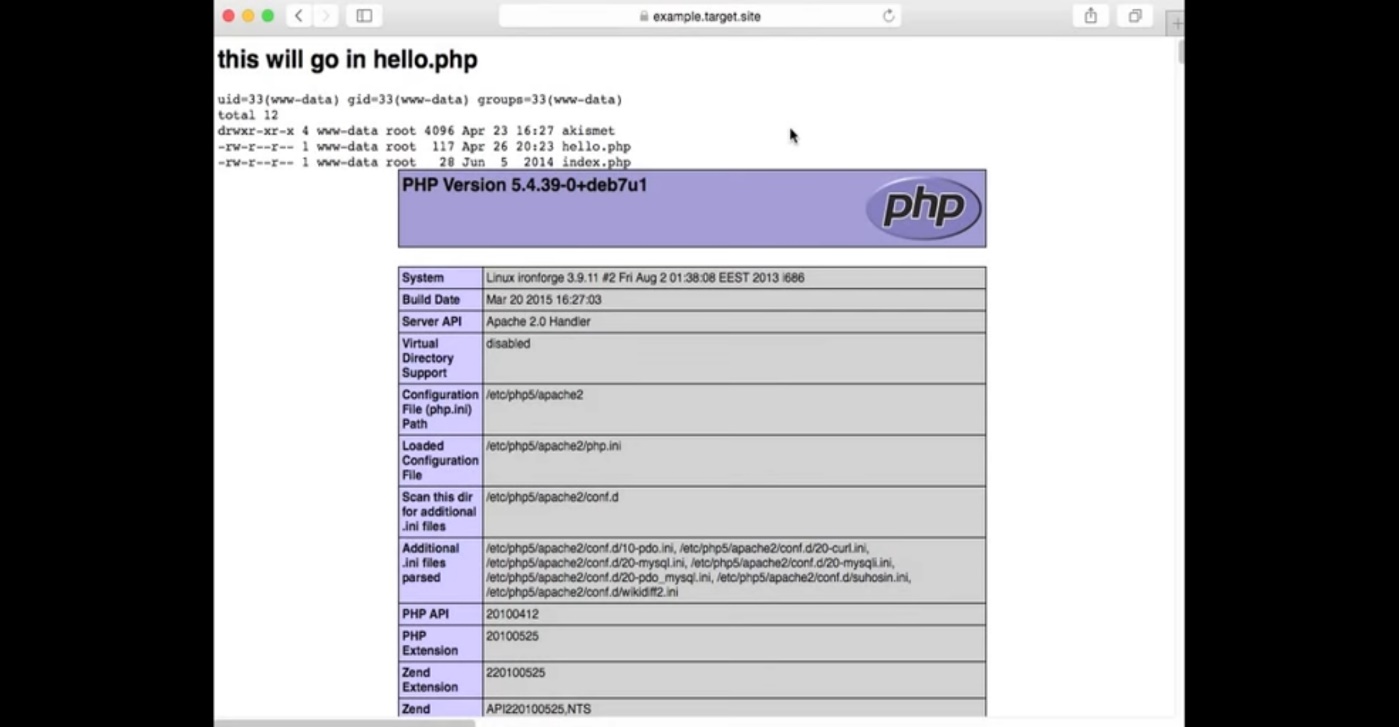
Unauthenticated Stored Cross-Site Scripting (XSS)

A Stored Cross-Site Scripting, or XSS, attack occurs when an attacker injects specially crafted script into a web application. The victim will trigger the attack once they access the stored script. It is not certain how the exploit was found or patched, however. the way how the code was executed and its results were specified. This specific attack is carried out through a comment made by an attacker within the comment section of the word press site. In order for this attack to work, the comments text must be extremely long, or at least as long as 64 KBs since “MySQL TEXT type size limit is 64 kilobytes.” The code looks like this:



Where the code displays “[64 kb]”, is where 64 kb worth of “A’s” will be added. The code will then be placed in the comment section, causing the comment to become truncated once it makes it way to the database. The admin will then check the comment made by the attacker, which will trigger the script



The attacker will be able to access a backdoor through the “hello.php” plugin. Klikki Oy, founder of the exploit, mentioned that the best way to prevent this exploit is by disabling comments and not approving any comment as admin.

References

https://wpvulndb.com/vulnerabilities/7945

<https://klikki.fi/adv/wordpress2.html>