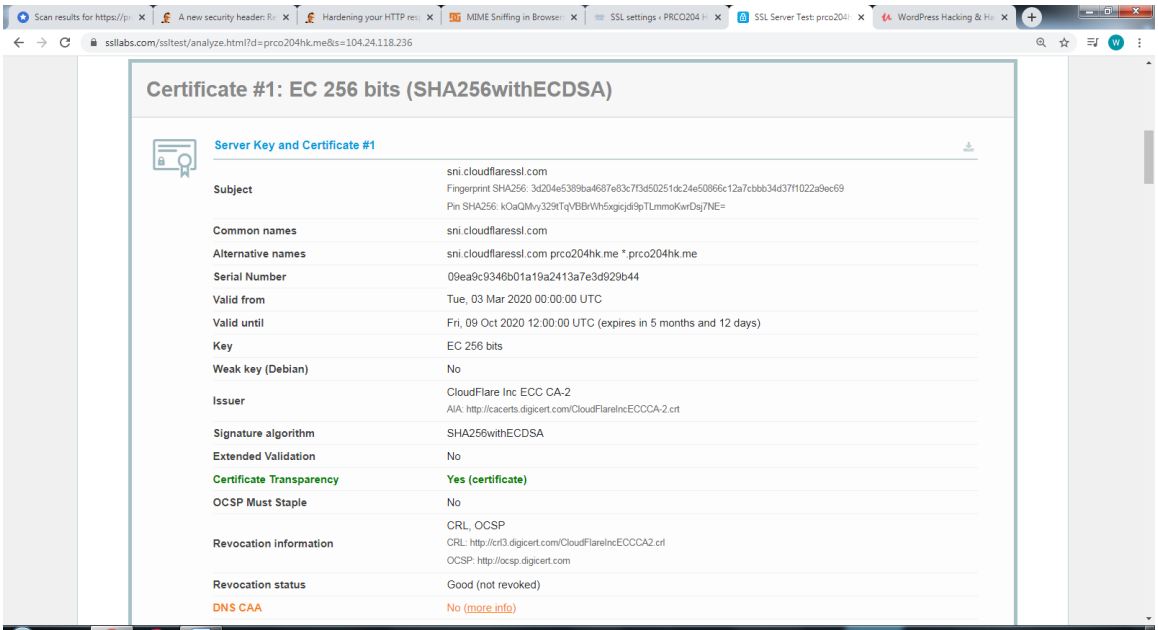
1) Use SFTP/SSH instead of Ftp for web server account

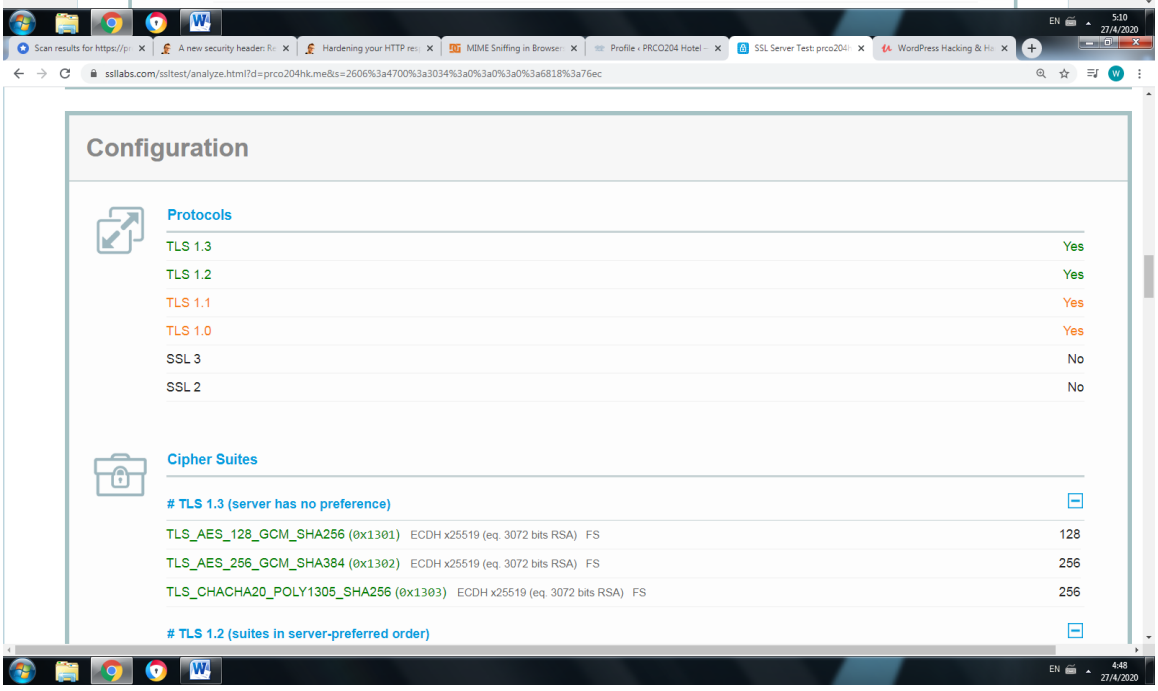
https://www.wpbeginner.com/beginners-guide/reasons-why-wordpress-site-gets-hacked/

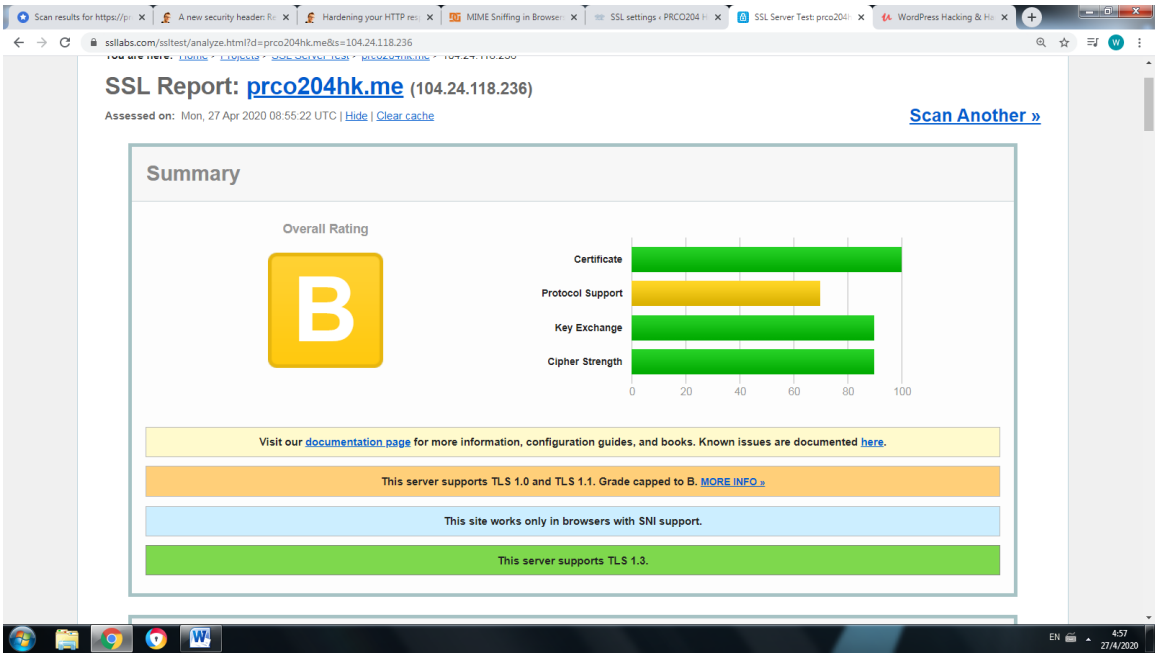
Reason:

When you connect to your site using plain FTP, your password is sent to the server unencrypted.

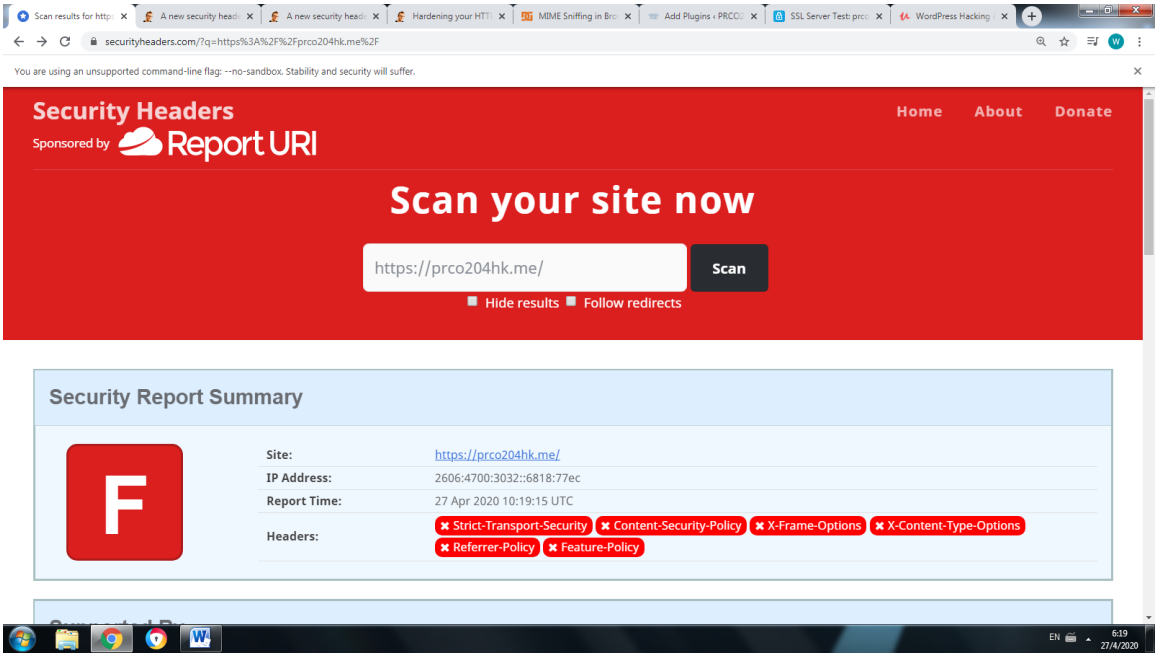
2) TLS scan Result(OK) https://www.ssllabs.com/ssltest/







3) Http Headers Security scan result
https://securityheaders.com/?q=https%3A%2F%2Fprco204hk.me%2F



-HTTP Strict Transport Security is an excellent feature to support on your site and strengthens your implementation of TLS by getting the User Agent to enforce the use of HTTPS. **!!Our Current Https 301 redirection is not strong enough and is susceptible to Man in the Middle Attack.!!**

-Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets**.!! Might disable the site Javascript if not set properly but can choose the source to allow!!**

-X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking. Recommended value "X-Frame-Options: SAMEORIGIN"..

--X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".

Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.

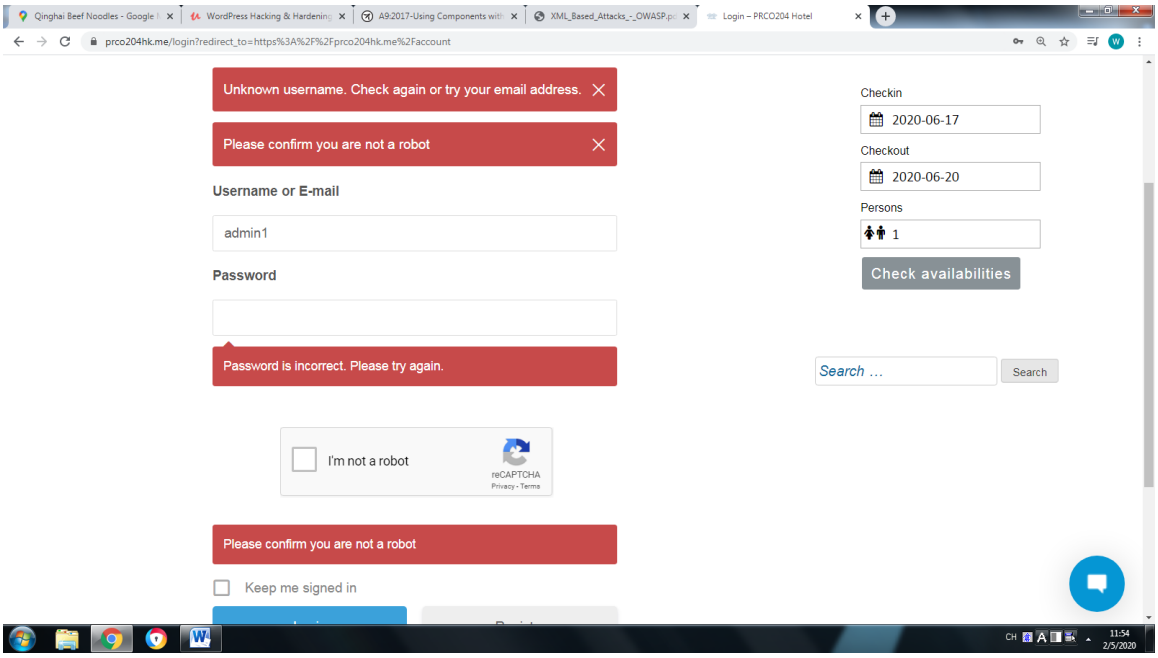
Feature Policy is a new header that allows a site to control which features and APIs can be used in the browser.

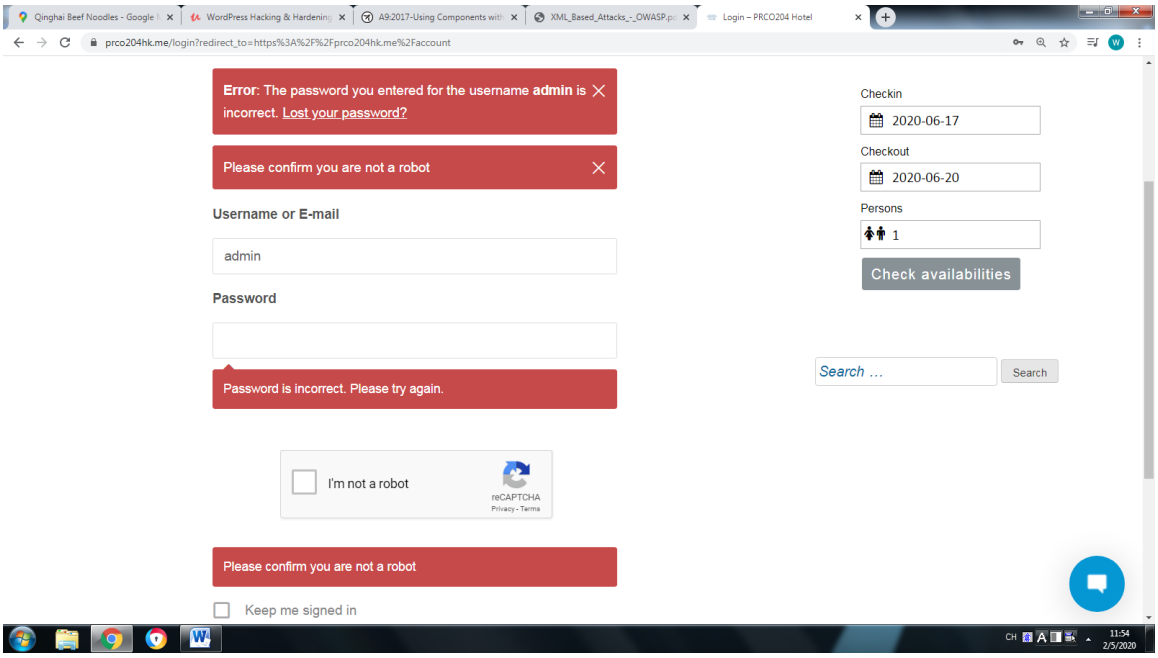
Solution: Can install Http Headers plugin to enable them

4) Changing Wordpress default WP-Admin login page URL, the login page has no captcha so is vulnerable to brute force attack.

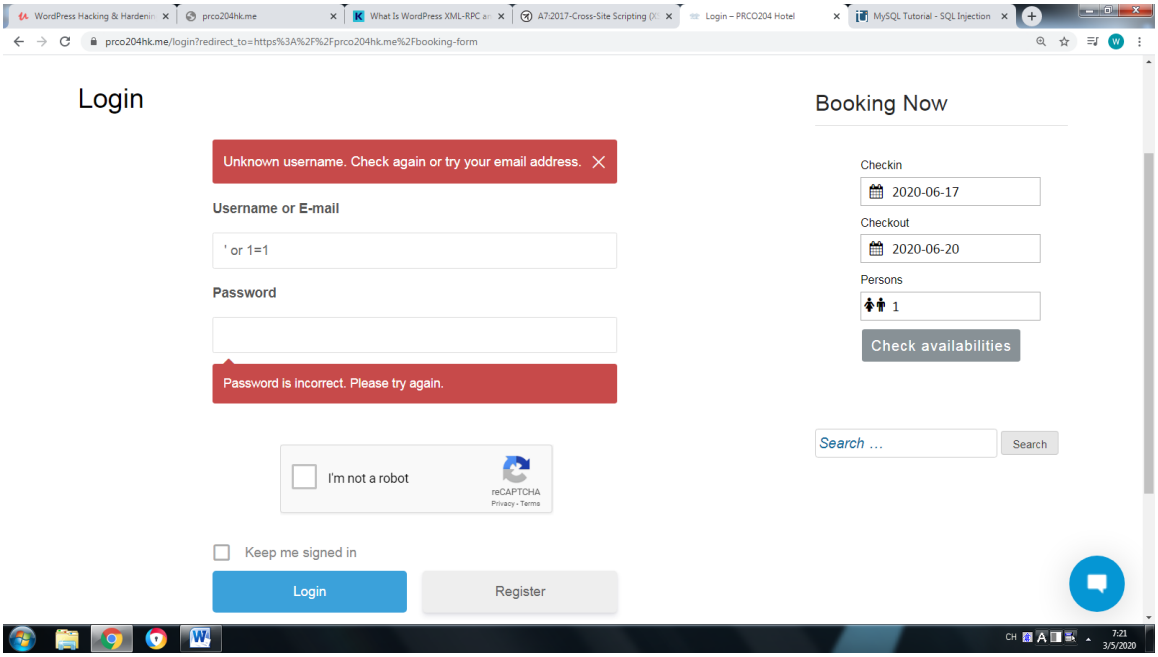
Solution: install “WPS Hide Login” to change the URL

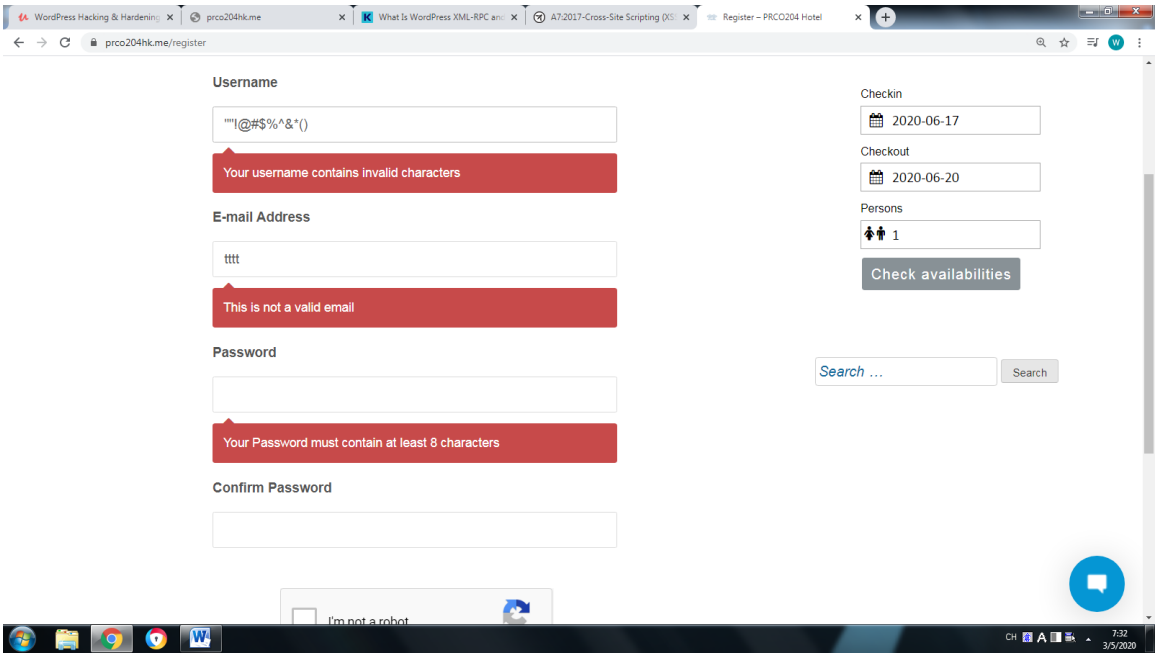
5)Username error message giving hints about the correct username



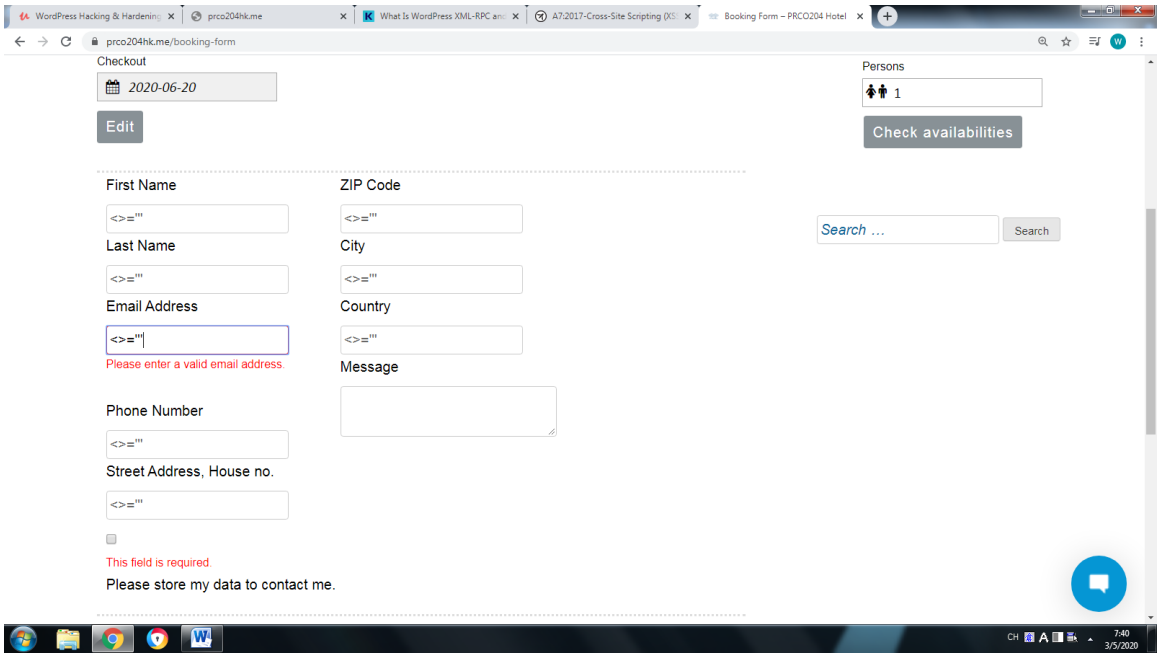


6) SQL injection(Test passed for Login and Register)

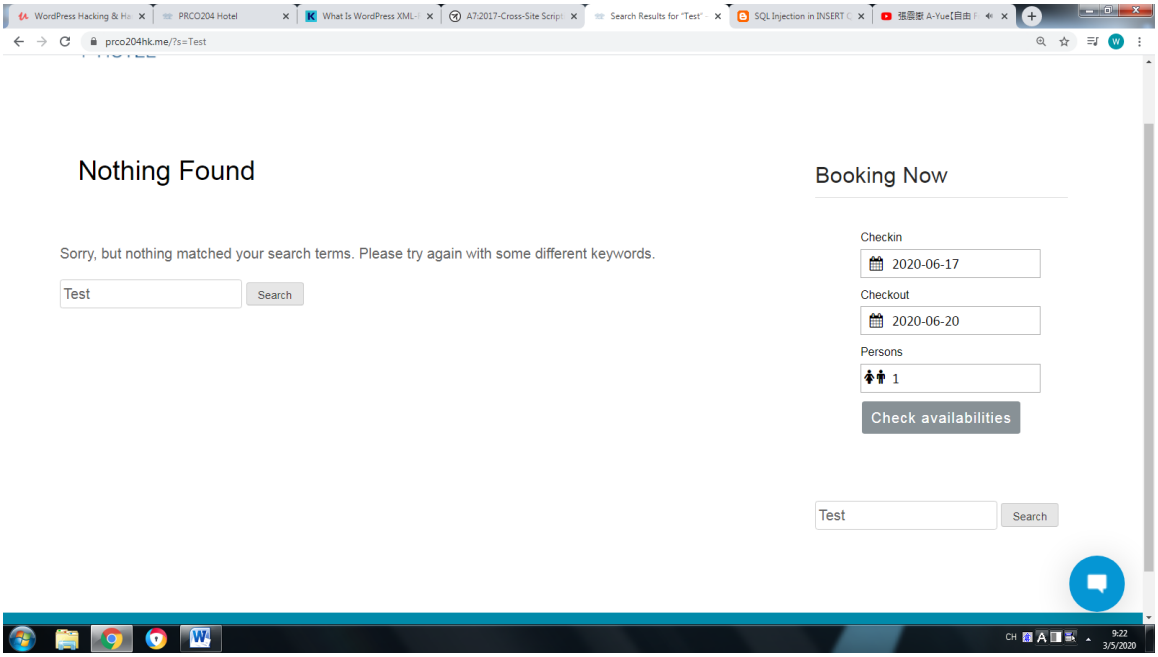




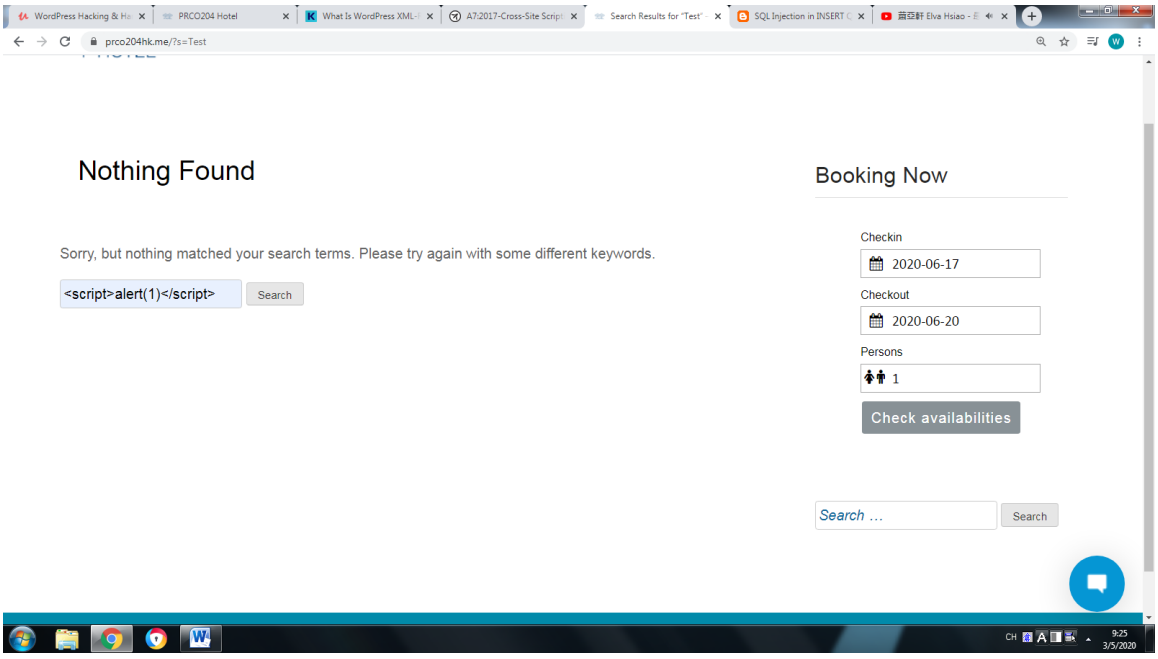
! No data validation (except email) for getting customer info when booking

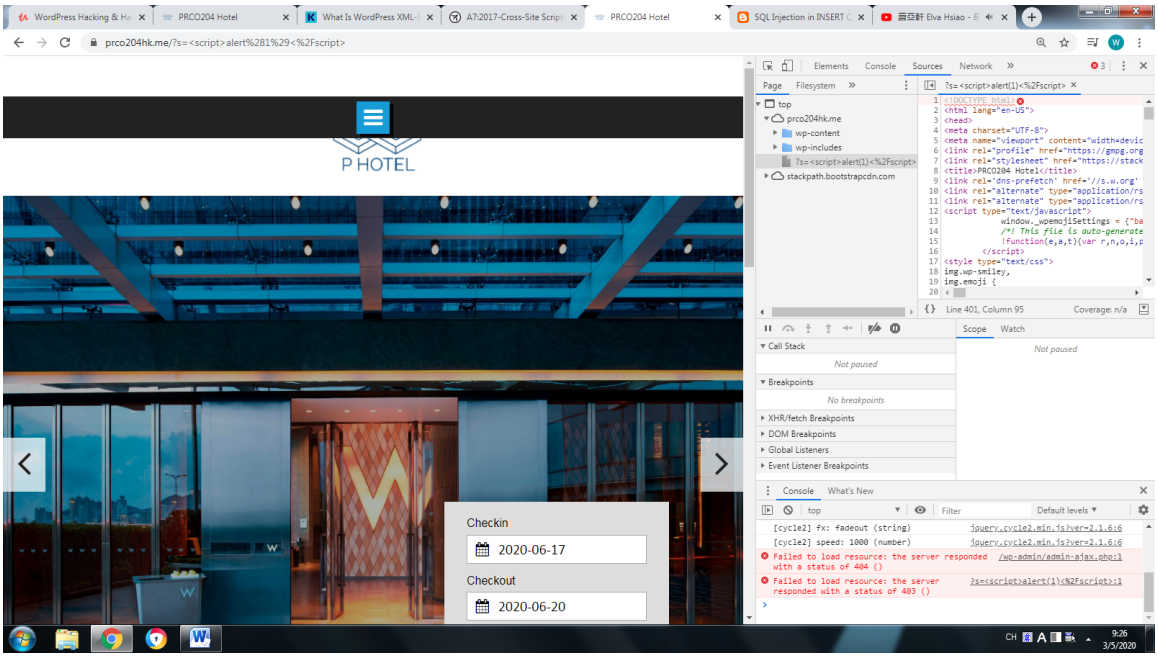


7)XSS(Reflected XSS) test for searchbox



But when trying to input <script> in searchbox instead of Nothing Found will redirect to Home Page

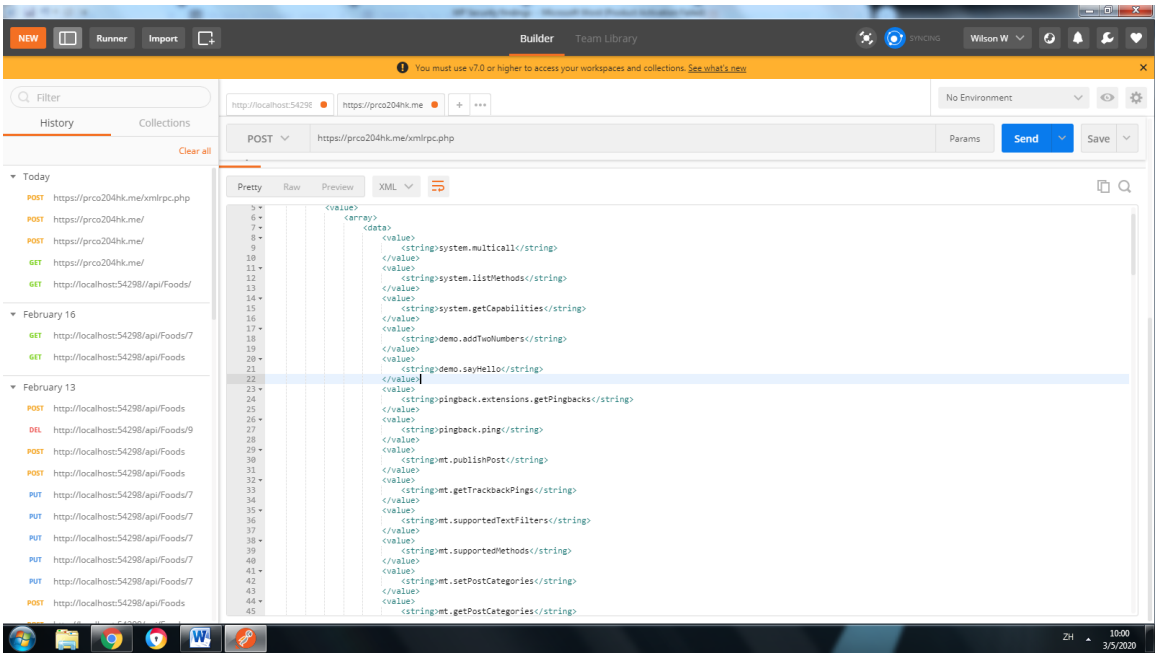




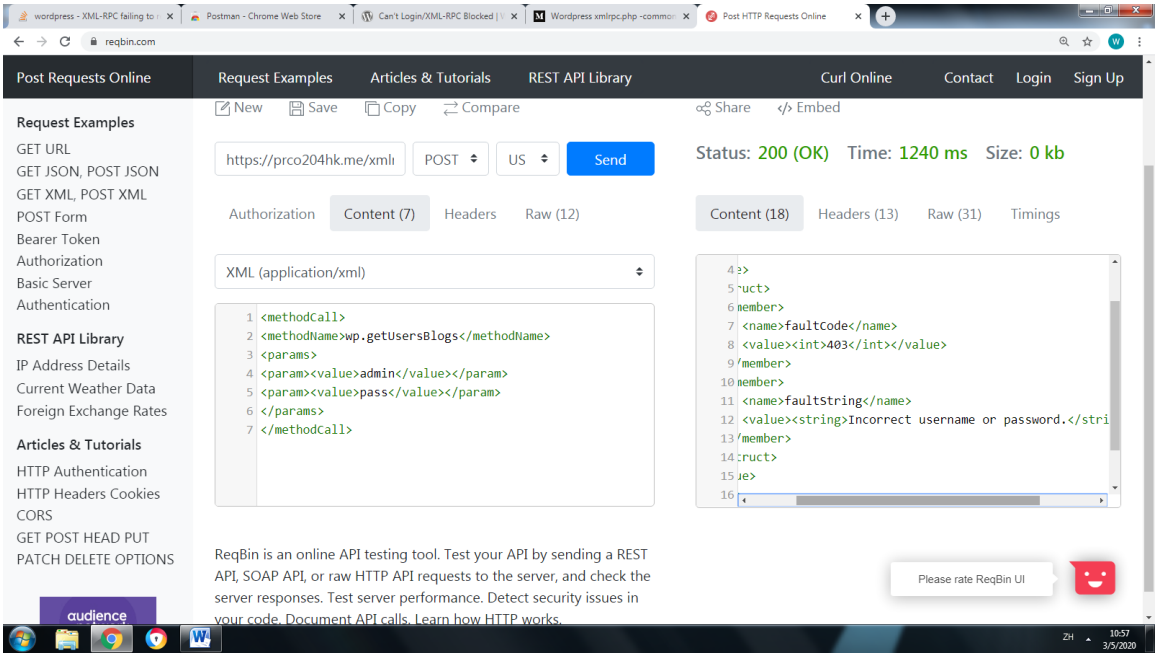
This is not a intended behaviour but is a minor issue as the javascript method didn't execute.

8) XML-RPC in Wordpress is consider a target for brute force attack https://medium.com/@the.bilal.rizwan/wordpress-xmlrpc-php-common-vulnerabilites-how-to-exploit-them-d8d3c8600b32

I just use Postman to send a POST request (https://prco204hk.me/xmlrpc.php)and able to get a list of methods available in XML-RPC



Hackers can use some tools to brute force the username and password replacing admin and pass as shown in the picture and send Post request invoking one of the chosen methods (getUsersBlogs).



Solution: can install the free plugin “Disable XML-RPC” to disable it or modify .htaccess file to deny it from access.

9)(OK) When browser closes, the session is ended . When a user using the site in public computer forgets to click logout instead just closing the browser the account will still logout.