

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/>

The screenshot displays the SSL Labs test results for the domain `sni.cloudflarestl.com`. The test was performed on 27/4/2020 at 5:10. The overall rating is 'Good' (not revoked).

Certificate #1: EC 256 bits (SHA256withECDSA)

Property	Value
Subject	sni.cloudflarestl.com
Common names	sni.cloudflarestl.com
Alternative names	sni.cloudflarestl.com prco204hk.me * prco204hk.me
Serial Number	09ea9c9346b01a19a2413a7e3d929b44
Valid from	Tue, 03 Mar 2020 00:00:00 UTC
Valid until	Fri, 09 Oct 2020 12:00:00 UTC (expires in 5 months and 12 days)
Key	EC 256 bits
Weak key (Debian)	No
Issuer	CloudFlare Inc ECC CA-2 AIA: http://cacerts.digicert.com/CloudFlareIncECCCA-2.crt
Signature algorithm	SHA256withECDSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation Information	CRL, OCSP CRL: http://crl3.digicert.com/CloudFlareIncECCCA2.crl OCSP: http://ocsp.digicert.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)

Configuration

Protocols

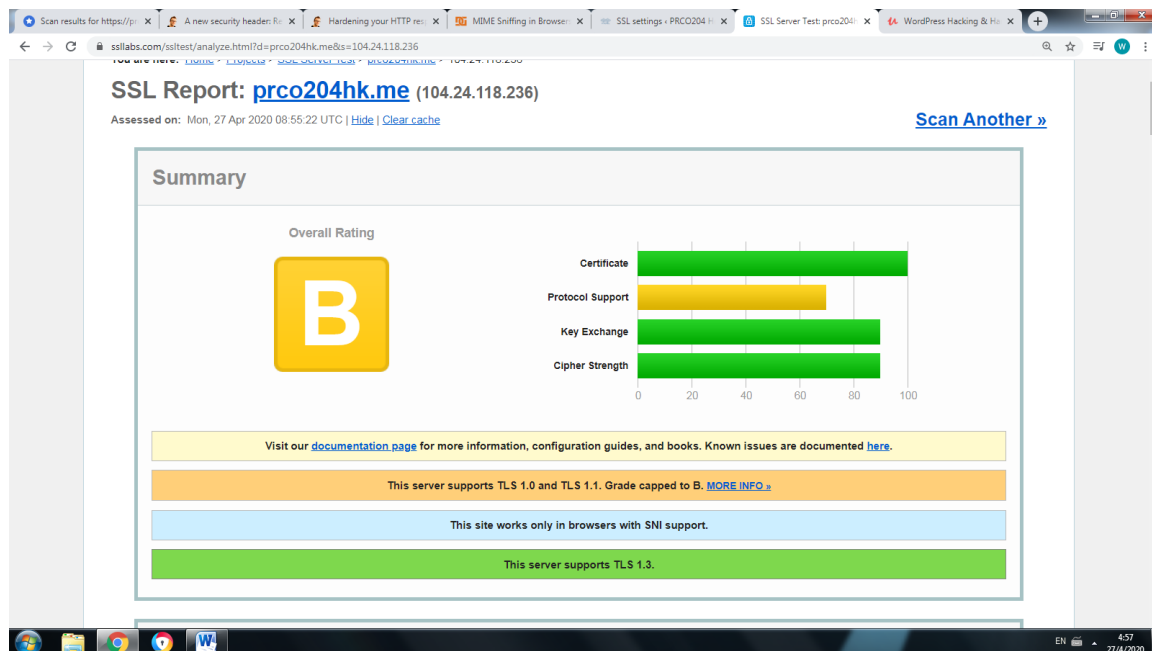
Protocol	Status
TLS 1.3	Yes
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

Cipher Suites

TLS 1.3 (server has no preference)

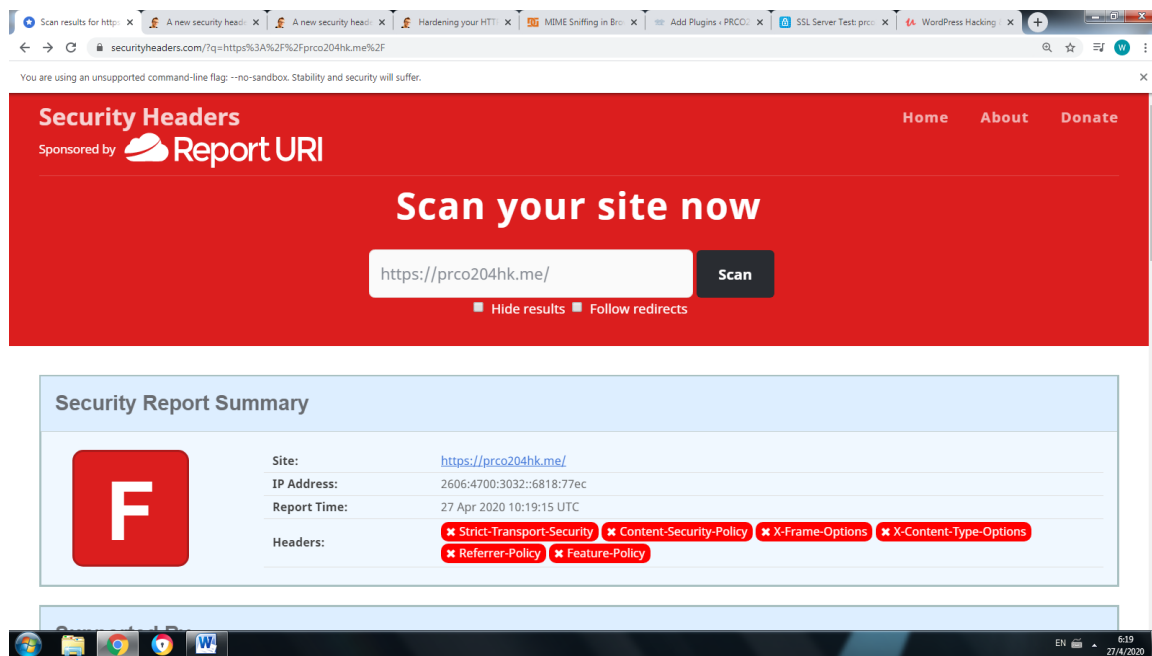
Cipher Suite	Strength
TLS_AES_128_GCM_SHA256 (0x1301) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_AES_256_GCM_SHA384 (0x1302) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303) ECDH x25519 (eq. 3072 bits RSA) FS	256

TLS 1.2 (suites in server-preferred order)



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.

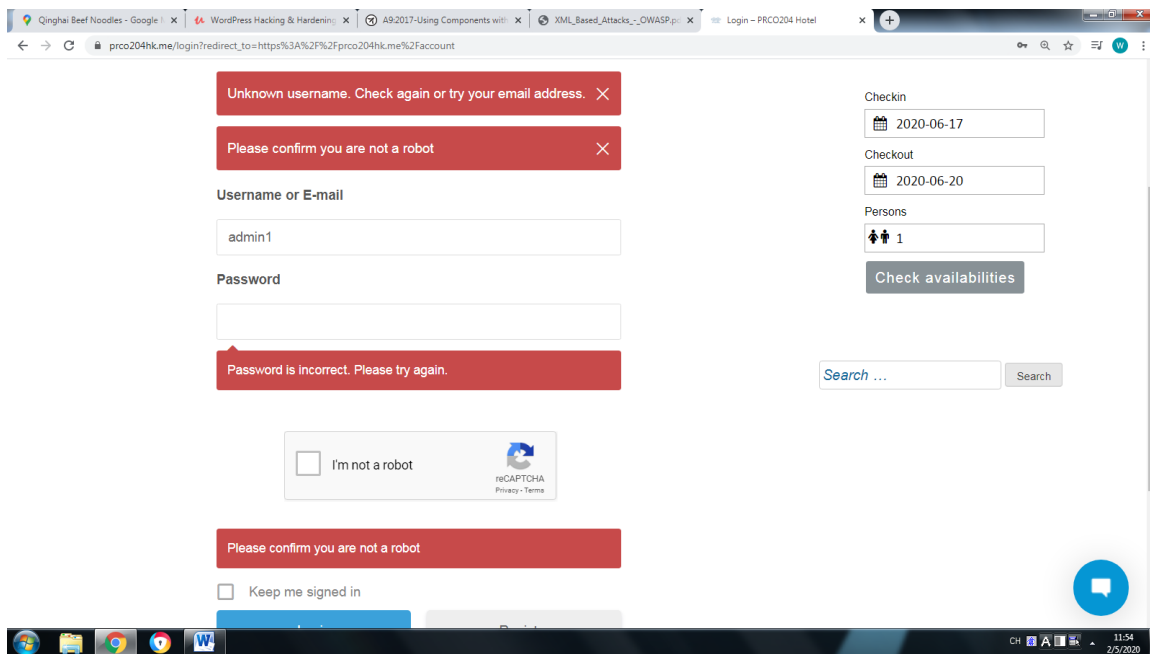
[Feature Policy](#) is a new header that allows a site to control which features and APIs can be used in the browser.

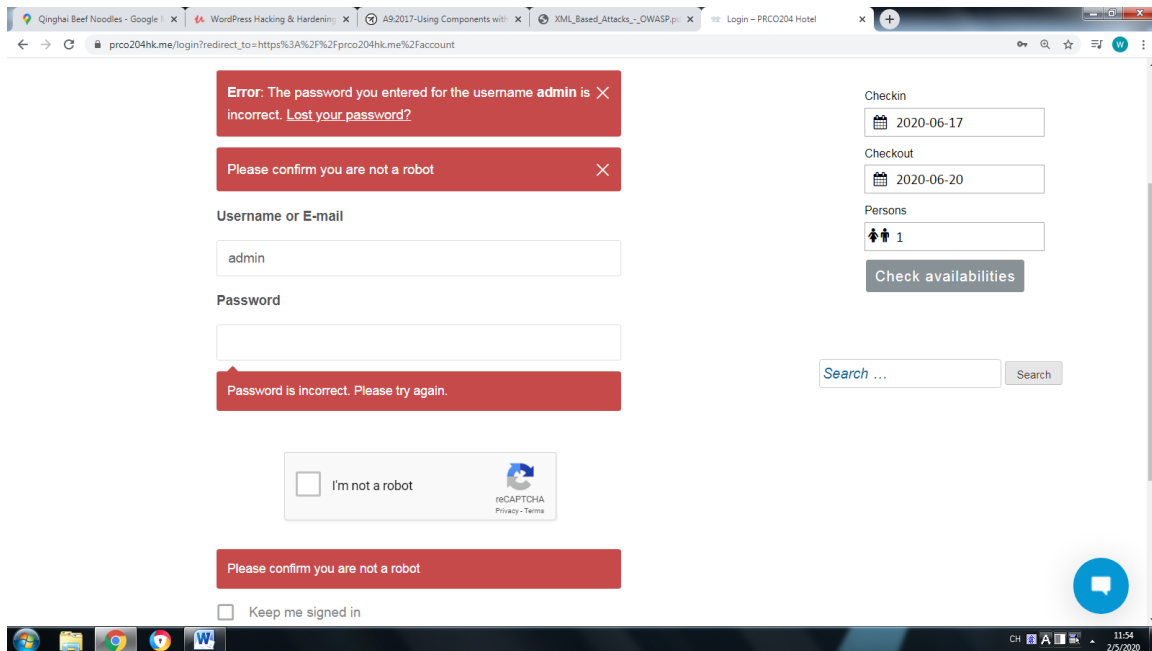
Solution: Can install Http Headers plugin to enable them

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

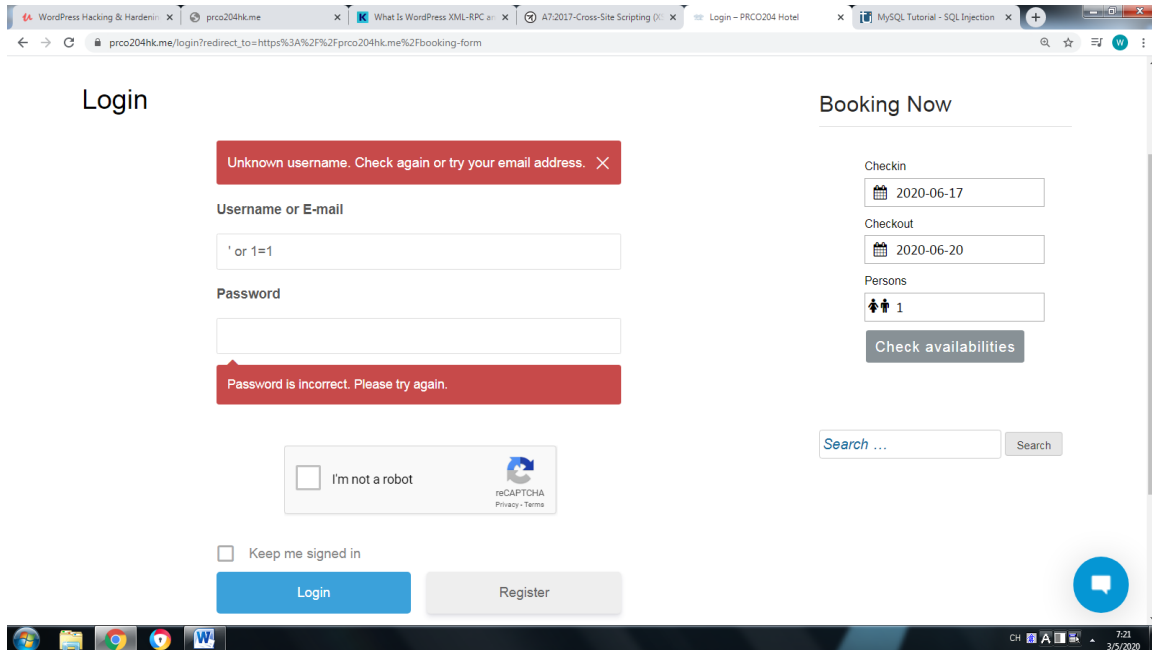
Solution: install "WPS Hide Login" to change the URL

5)Username error message giving hints about the correct username





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



WordPress Hacking & Hardening | prco204hk.me | What Is WordPress XML-RPC an... | A7.2017-Cross-Site Scripting (XSS) | Register - PRCO204 Hotel

prco204hk.me/register

Username

""!@#\$\$%^&*()

Your username contains invalid characters

E-mail Address

tttt

This is not a valid email

Password

Your Password must contain at least 8 characters

Confirm Password

Checkin

2020-06-17

Checkout

2020-06-20

Persons

1

Check availabilities

Search ... Search

I'm not a robot

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

WordPress Hacking & Hardening | prco204hk.me | What Is WordPress XML-RPC an... | A7.2017-Cross-Site Scripting (XSS) | Booking Form - PRCO204 Hotel

prco204hk.me/booking-form

Checkout

2020-06-20

Edit

Persons

1

Check availabilities

Search ... Search

First Name

<>=

Last Name

<>=

Email Address

<>=

Please enter a valid email address.

Phone Number

<>=

Street Address, House no.

<>=

This field is required.
Please store my data to contact me.

ZIP Code

<>=

City

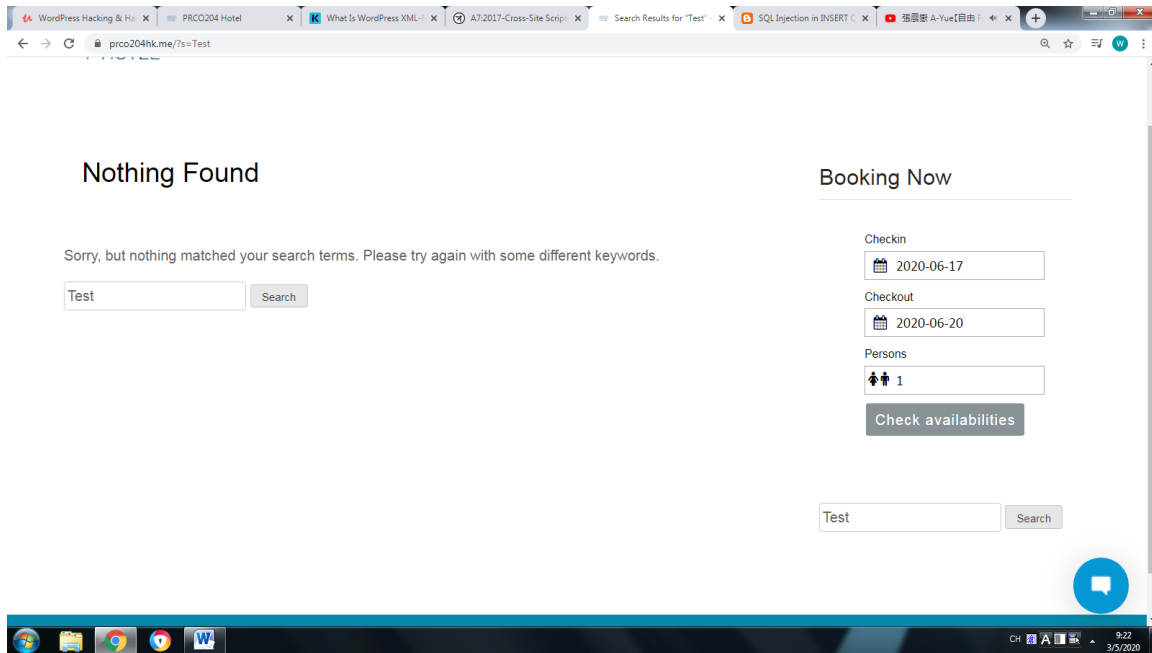
<>=

Country

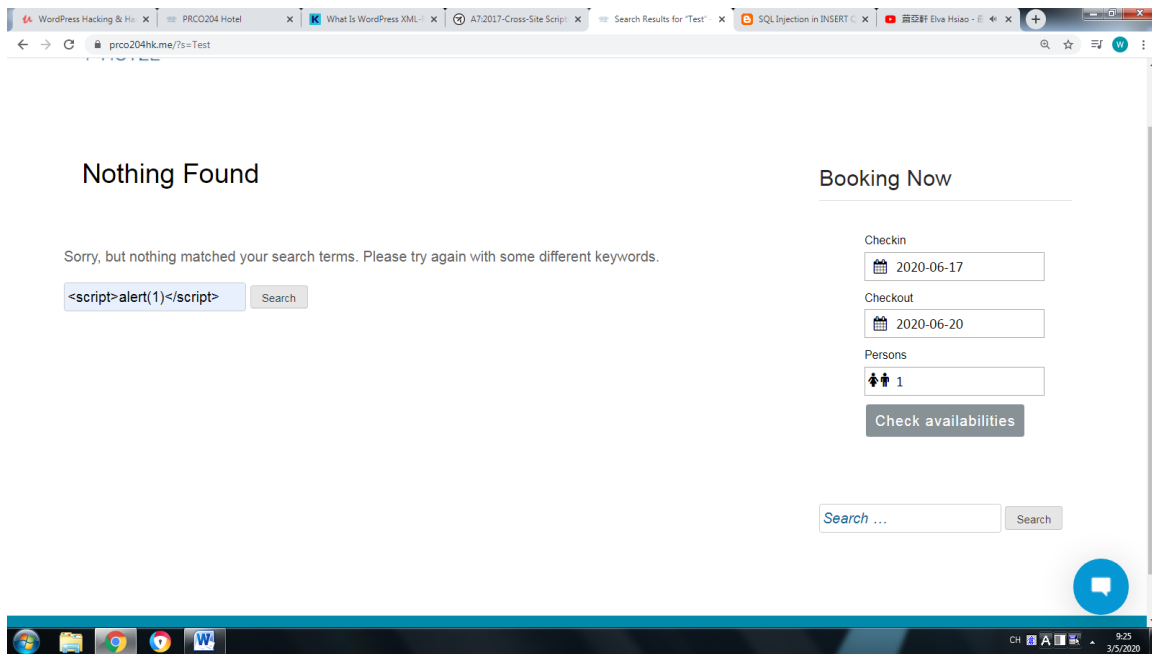
<>=

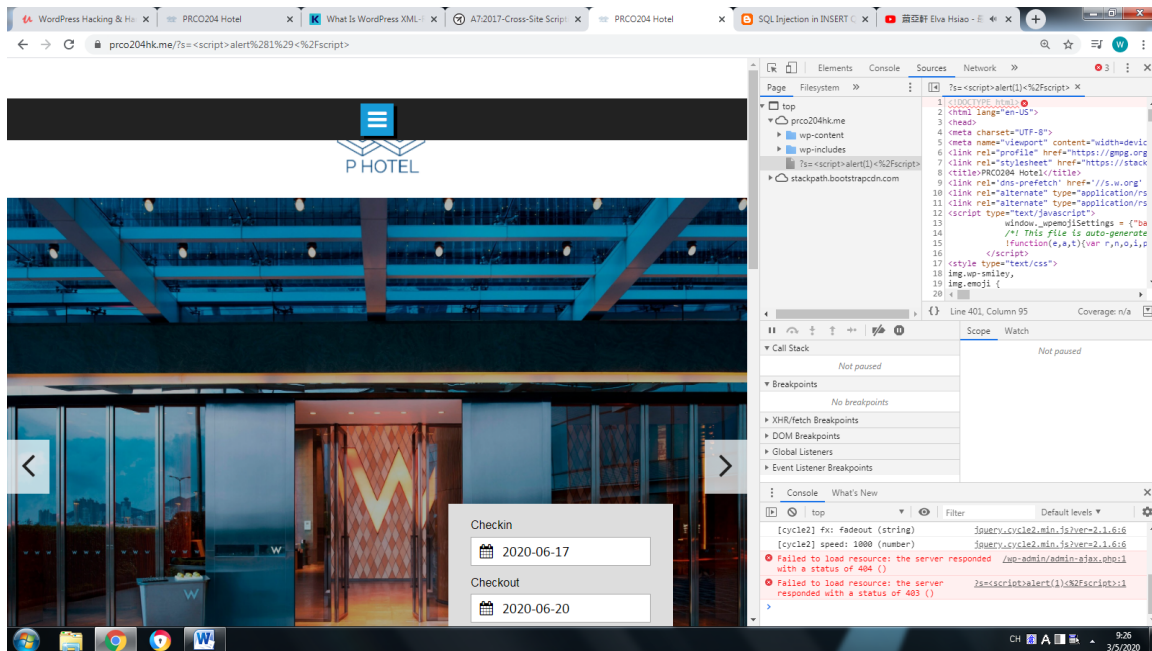
Message

7)XSS(Reflected XSS) test for searchbox



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



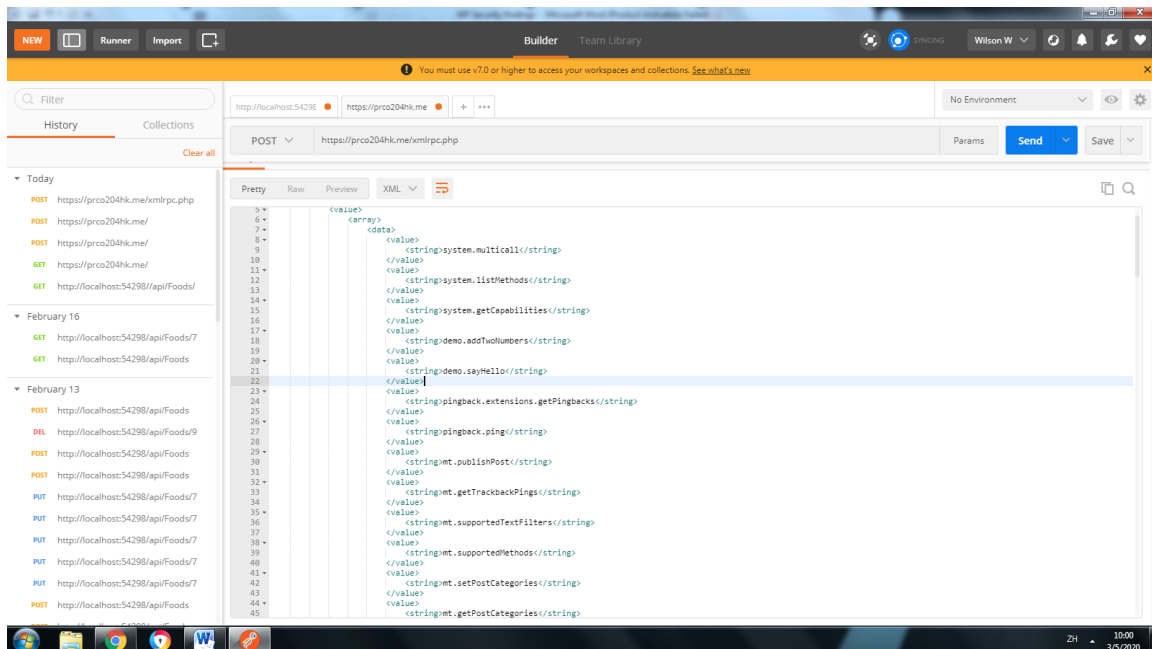


This is not a intended behaviour but is a minor issue as the javascript method didn't execute.

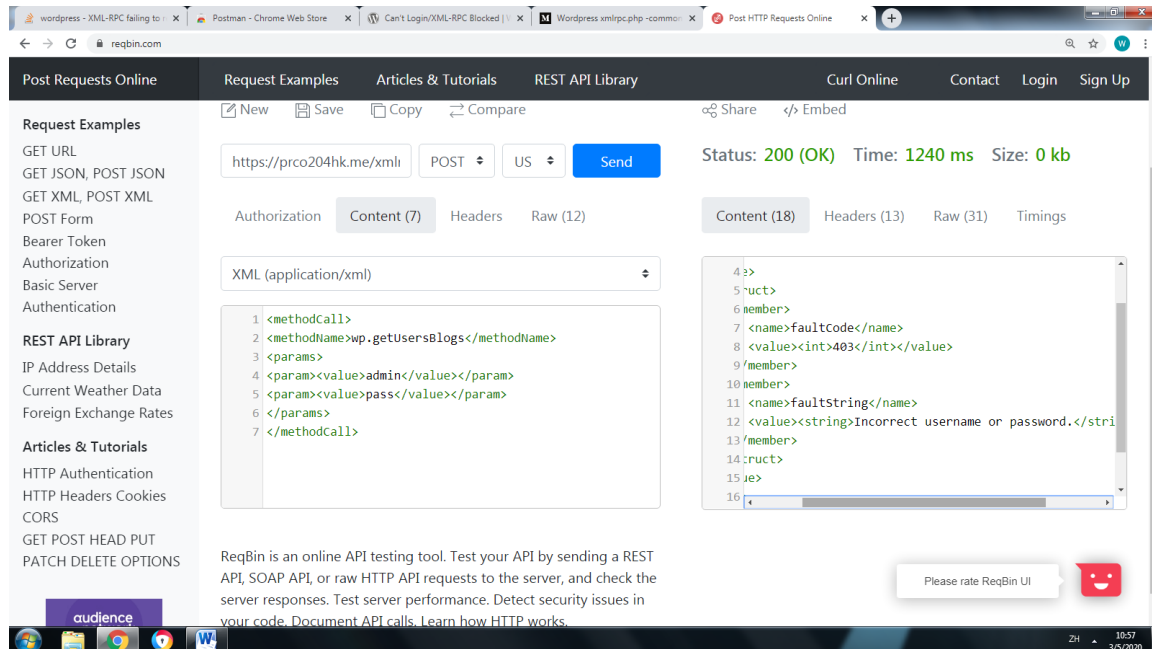
8) XML-RPC in Wordpress is consider a target for brute force attack

<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.