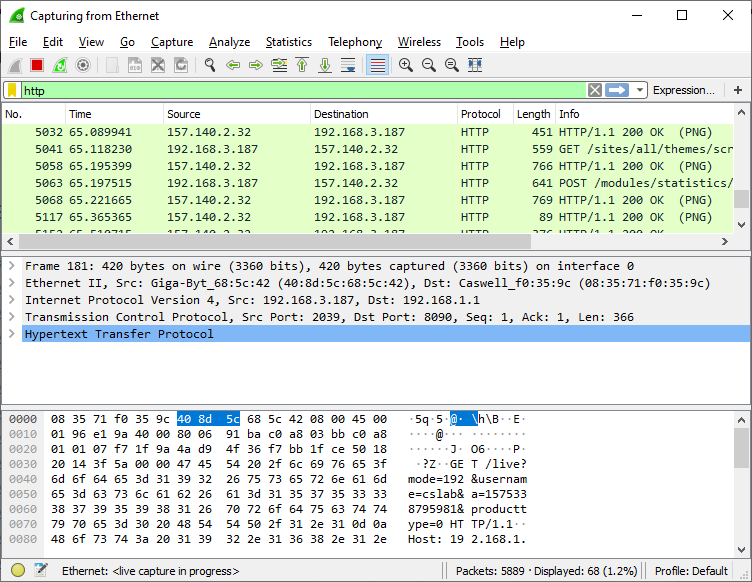
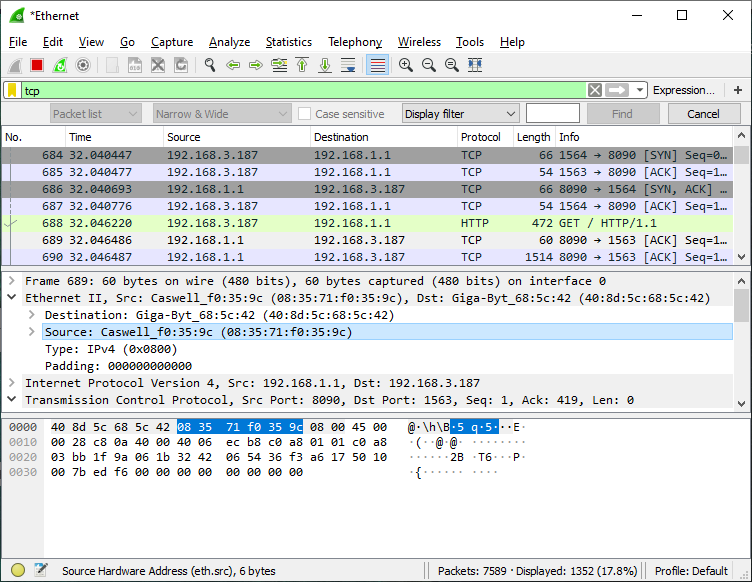
**PRACTICAL NO: 5(a)**

**Aim: Use Wireshark (Sniffer) to capture network traffic and analyse.**

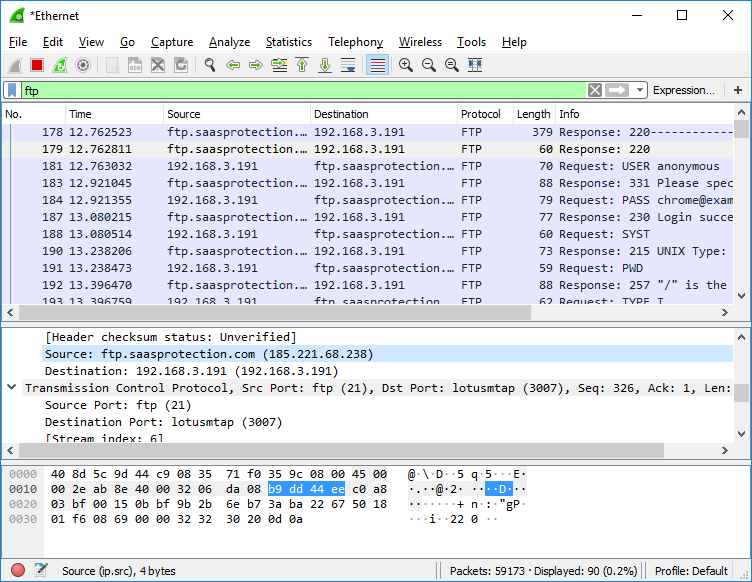
**Capture packet that have http protocol.**



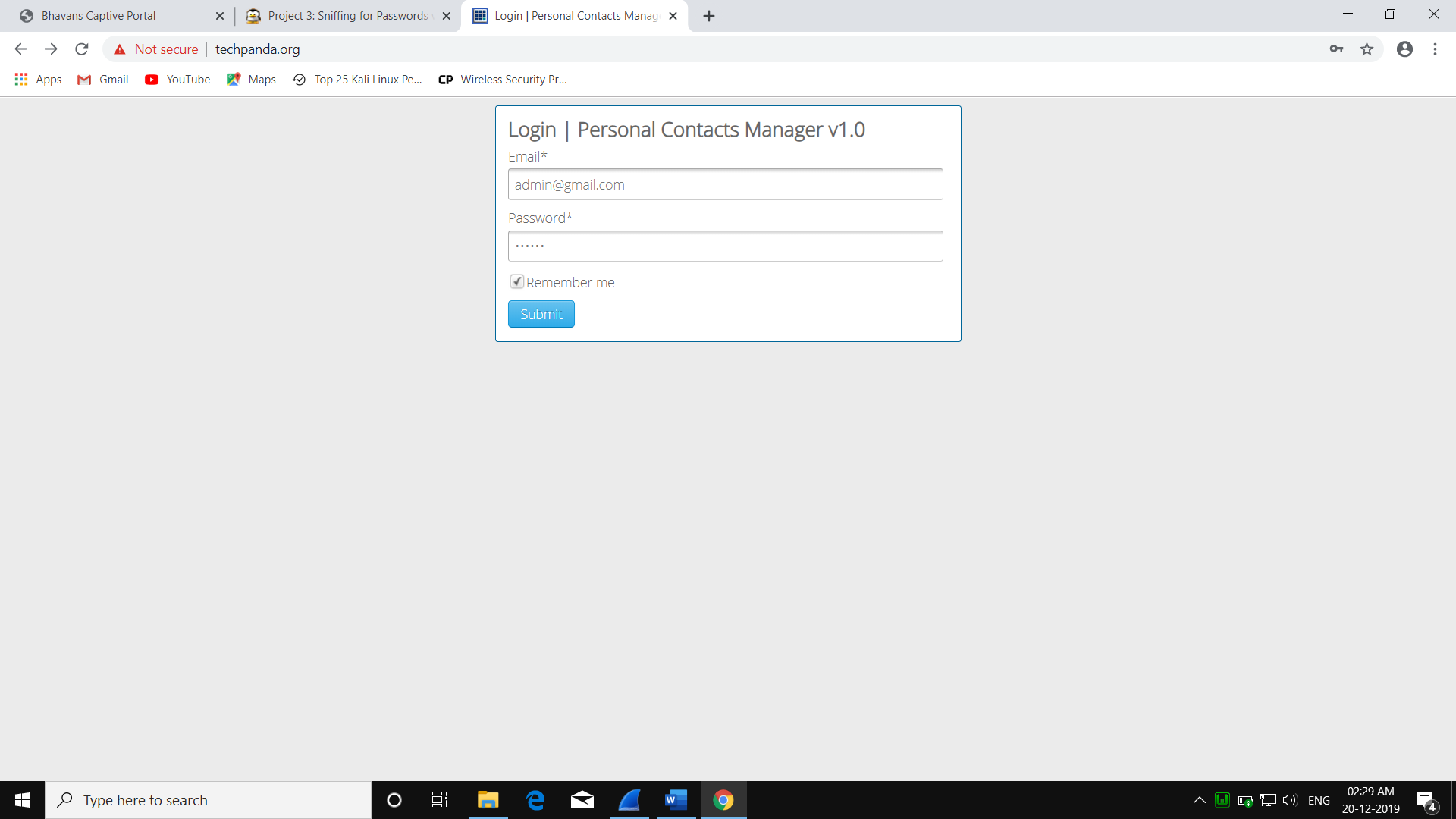
**Capture tcp packet.**



**Capture ftp packet:**

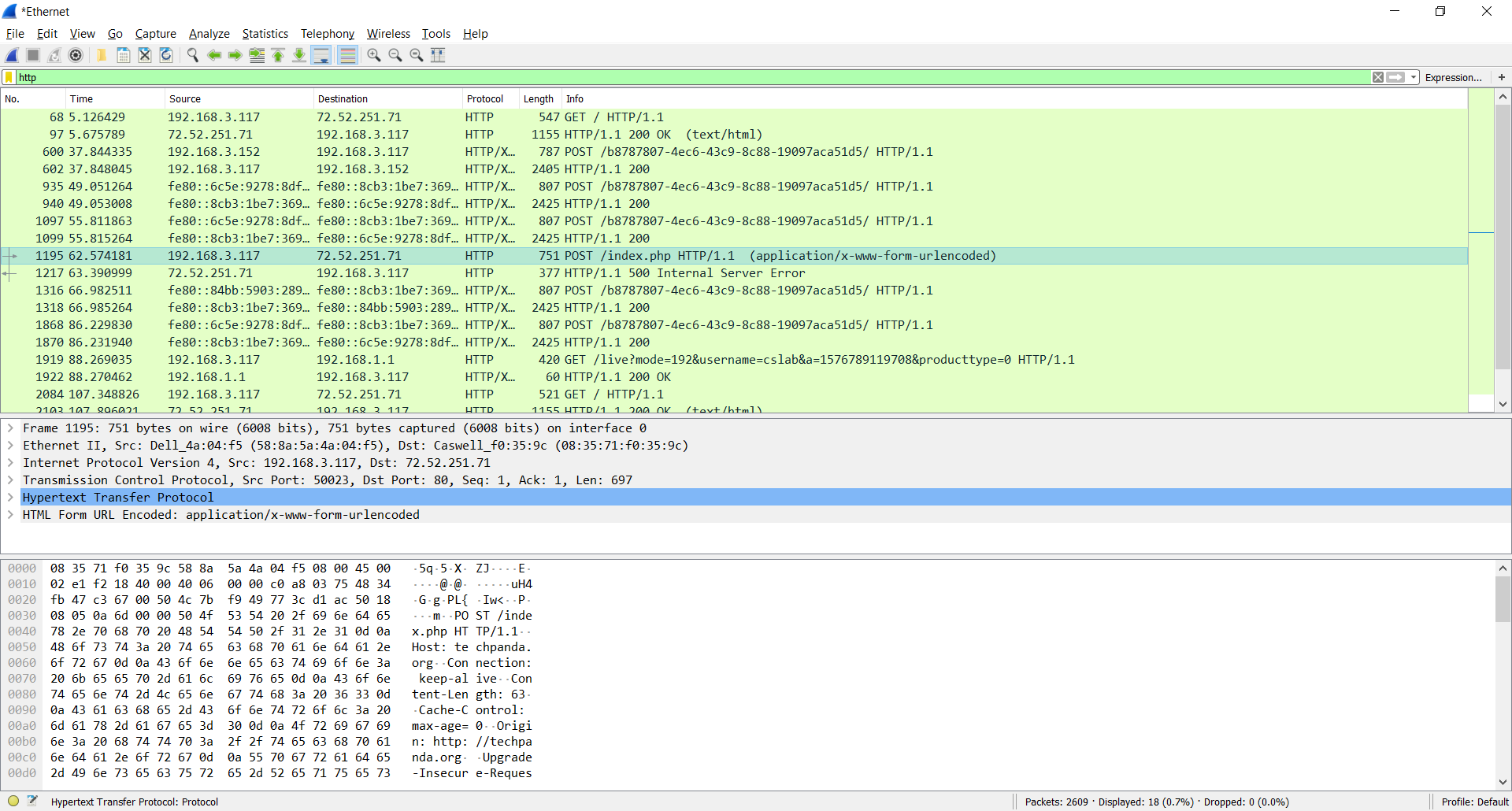


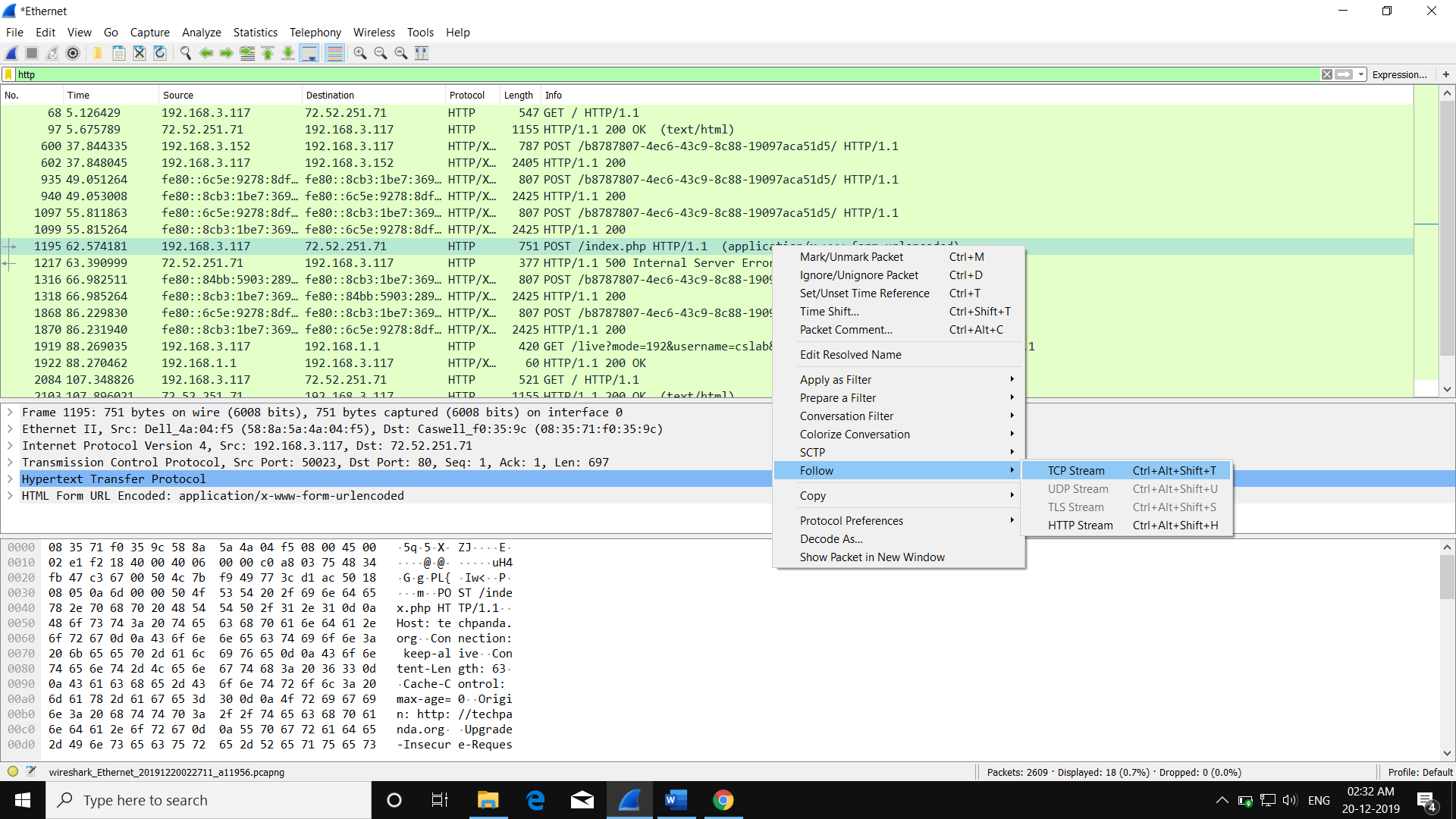
Go to **http://techpanda.org**

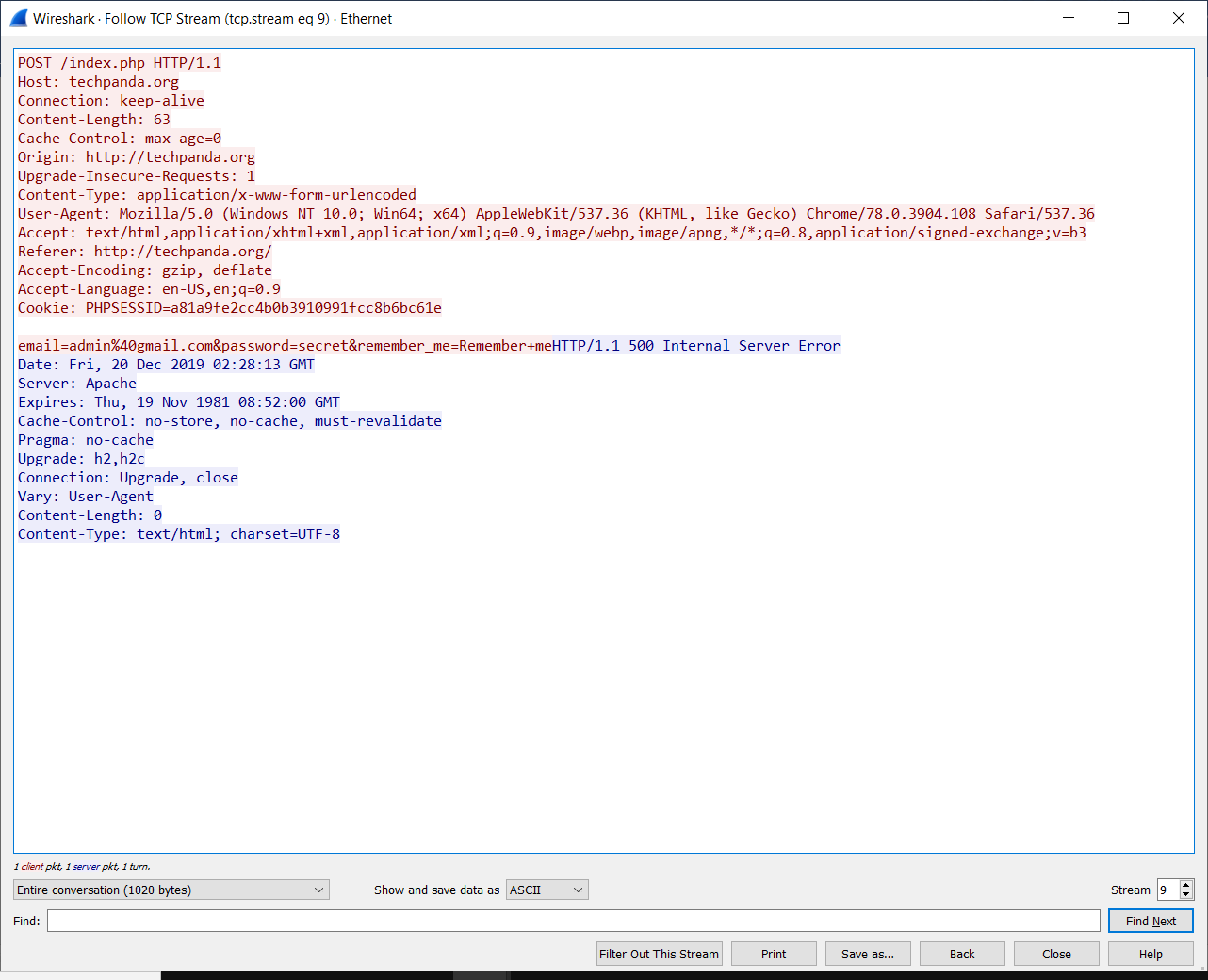


Filter **http** packets:

Right click on packet that has **index.php**

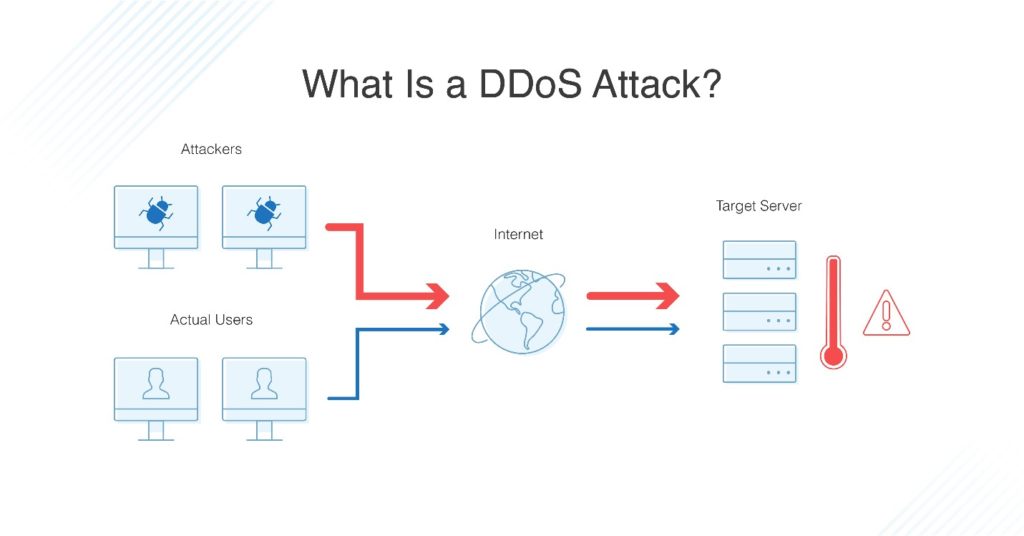




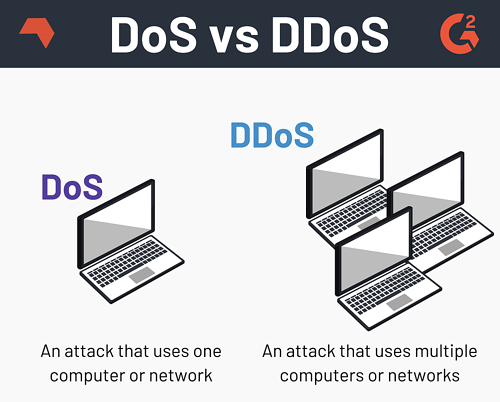


**PRACTICAL NO: 5(b)**

**Aim: launch DoS attack.**



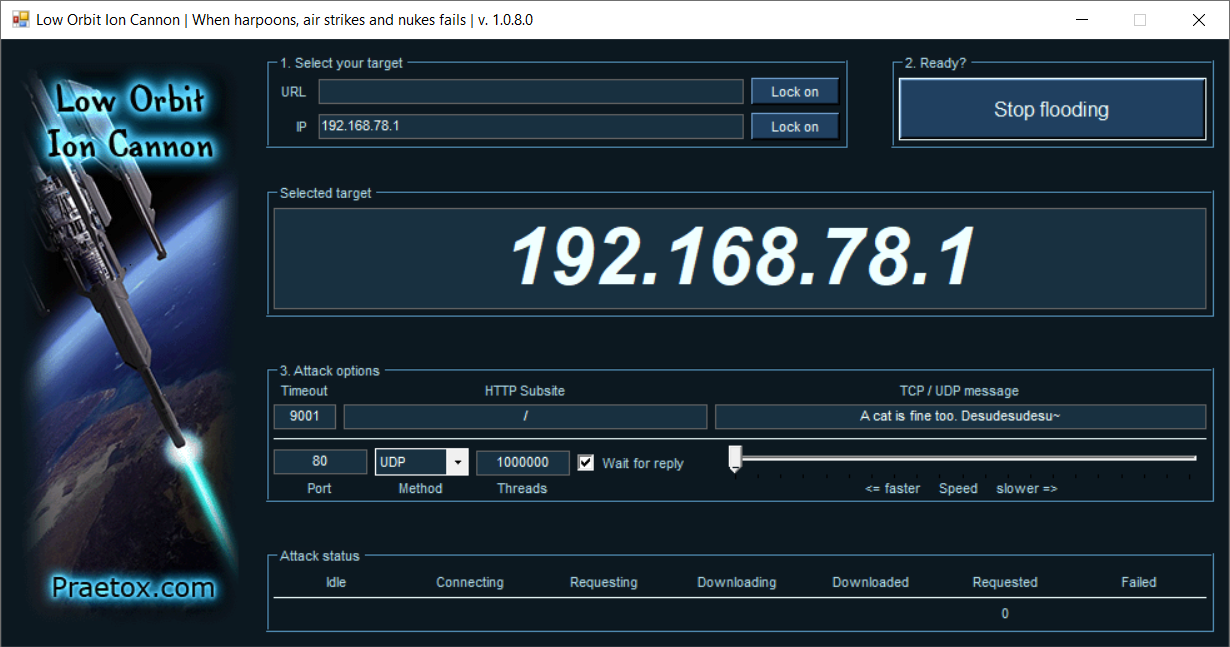
A **DoS attack** is a denial of service **attack** where a computer (or computers) is used to flood a server with TCP **and** UDP packets. A **DDoS attack** is where multiple systems target a single system with a **DoS attack**. The targeted network is then bombarded with packets from multiple locations.



LOIC Tool:

Target IP Address is 192.168.78.1

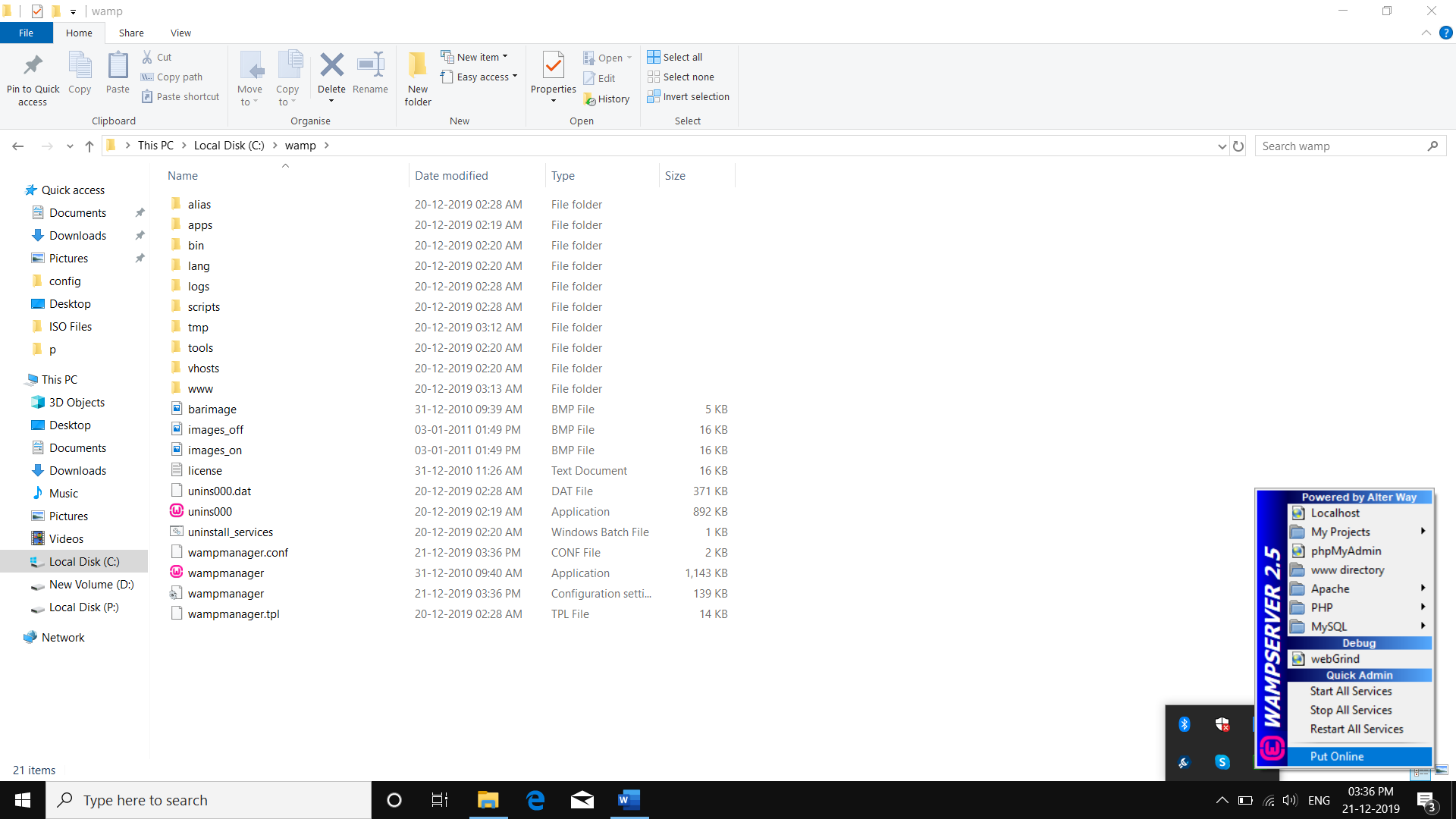
Increase Threads, Select Method, Port and Start Attack:



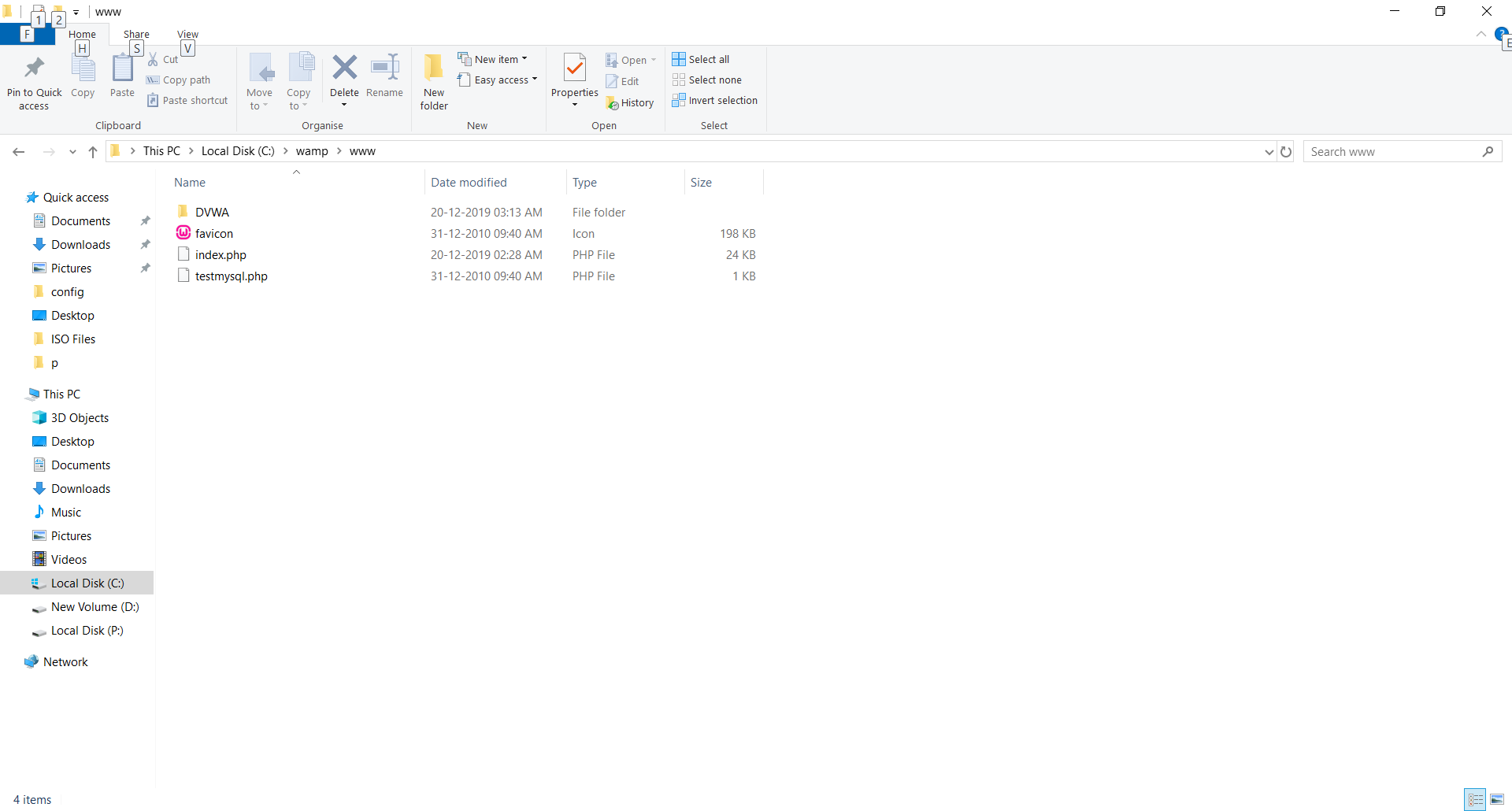
**PRACTICAL NO: 6**

**Aim: Simulate persistent cross-site scripting attack**.

Install WAMP and Start WAMP Server:

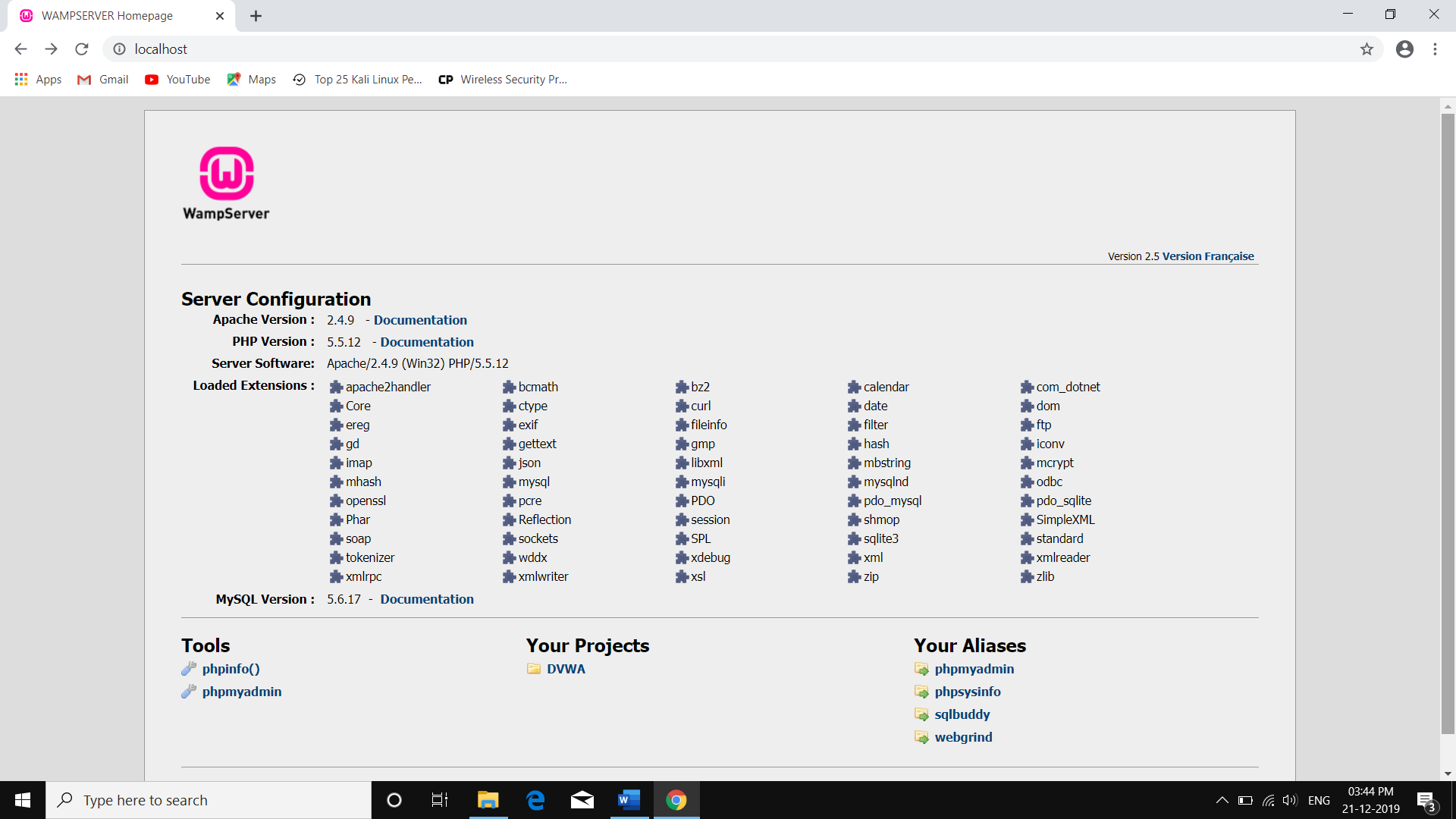


Extract or paste DVWA Folder to C:\wamp\www

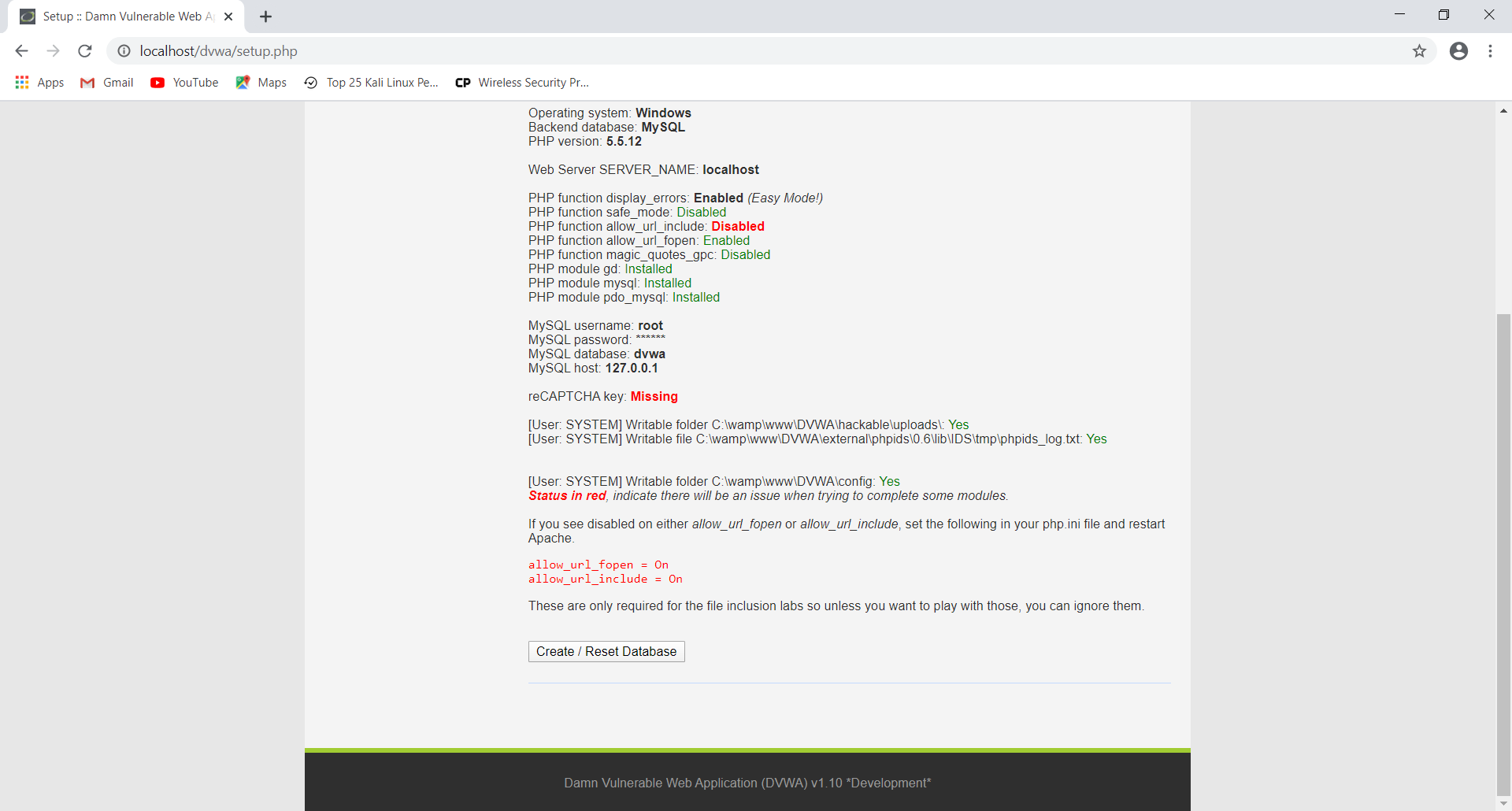


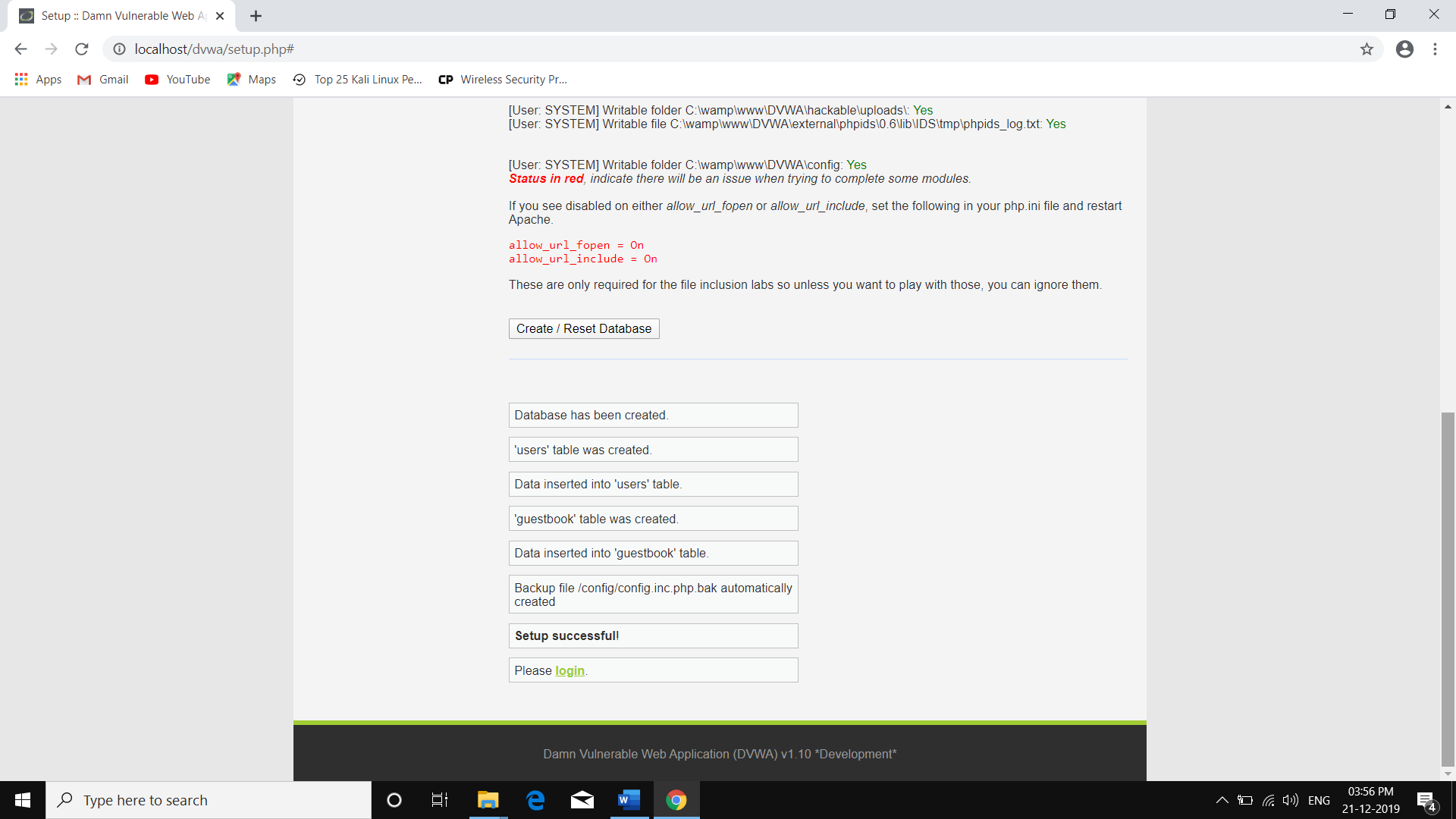
Go to **localhost**

Select **DVWA** From **Your Projects**:

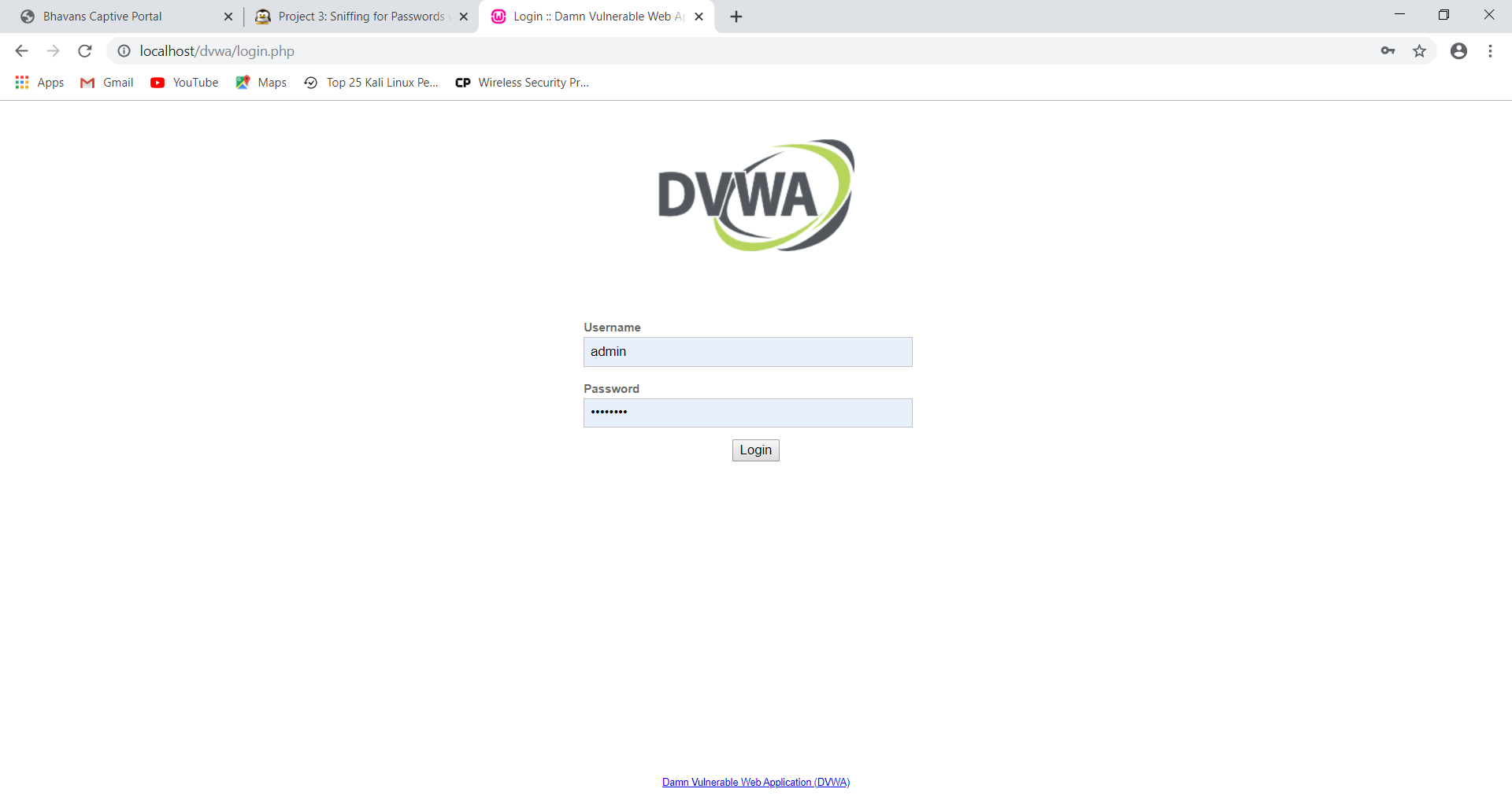


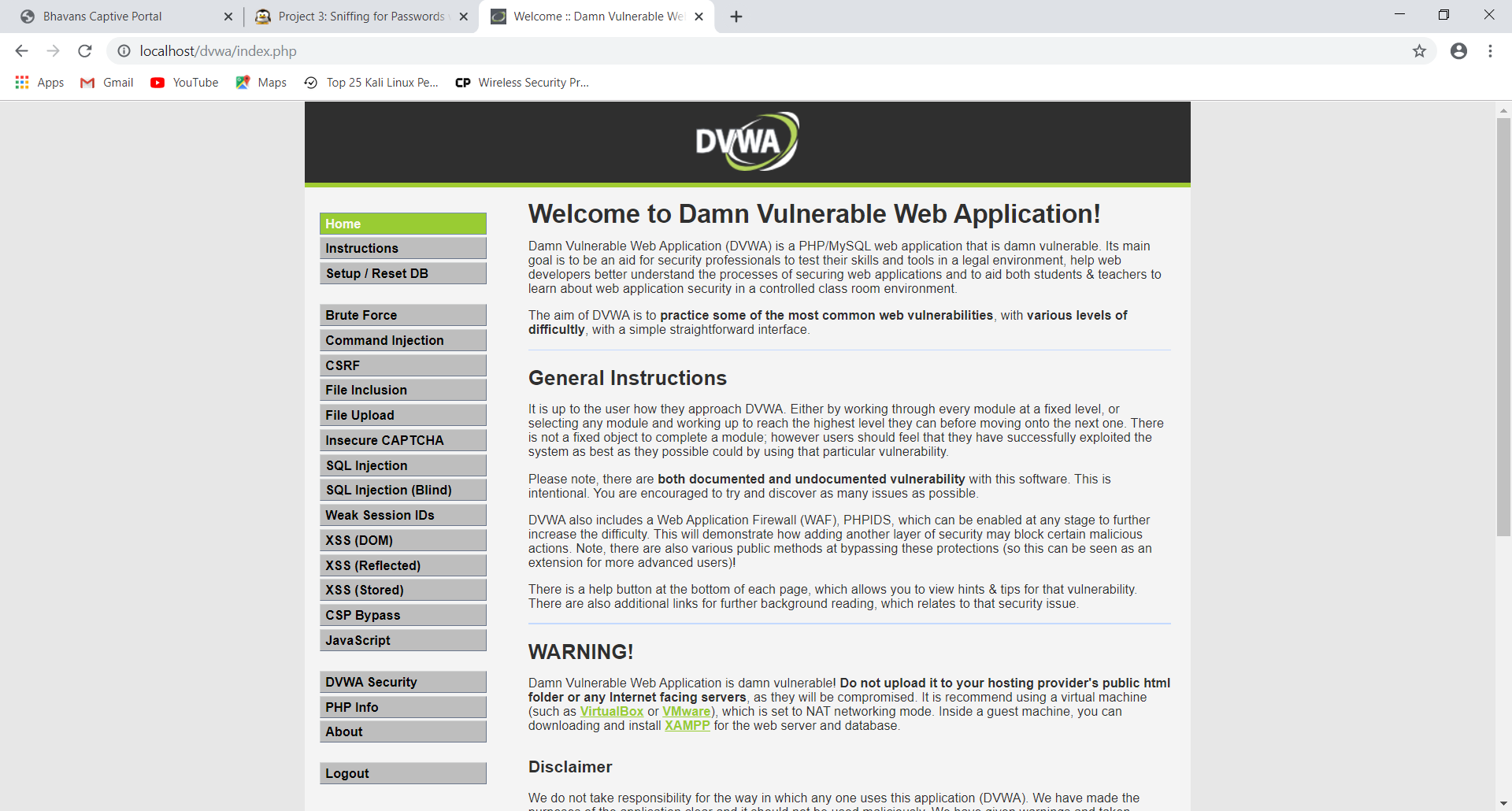
Click on Create/Reset Database:



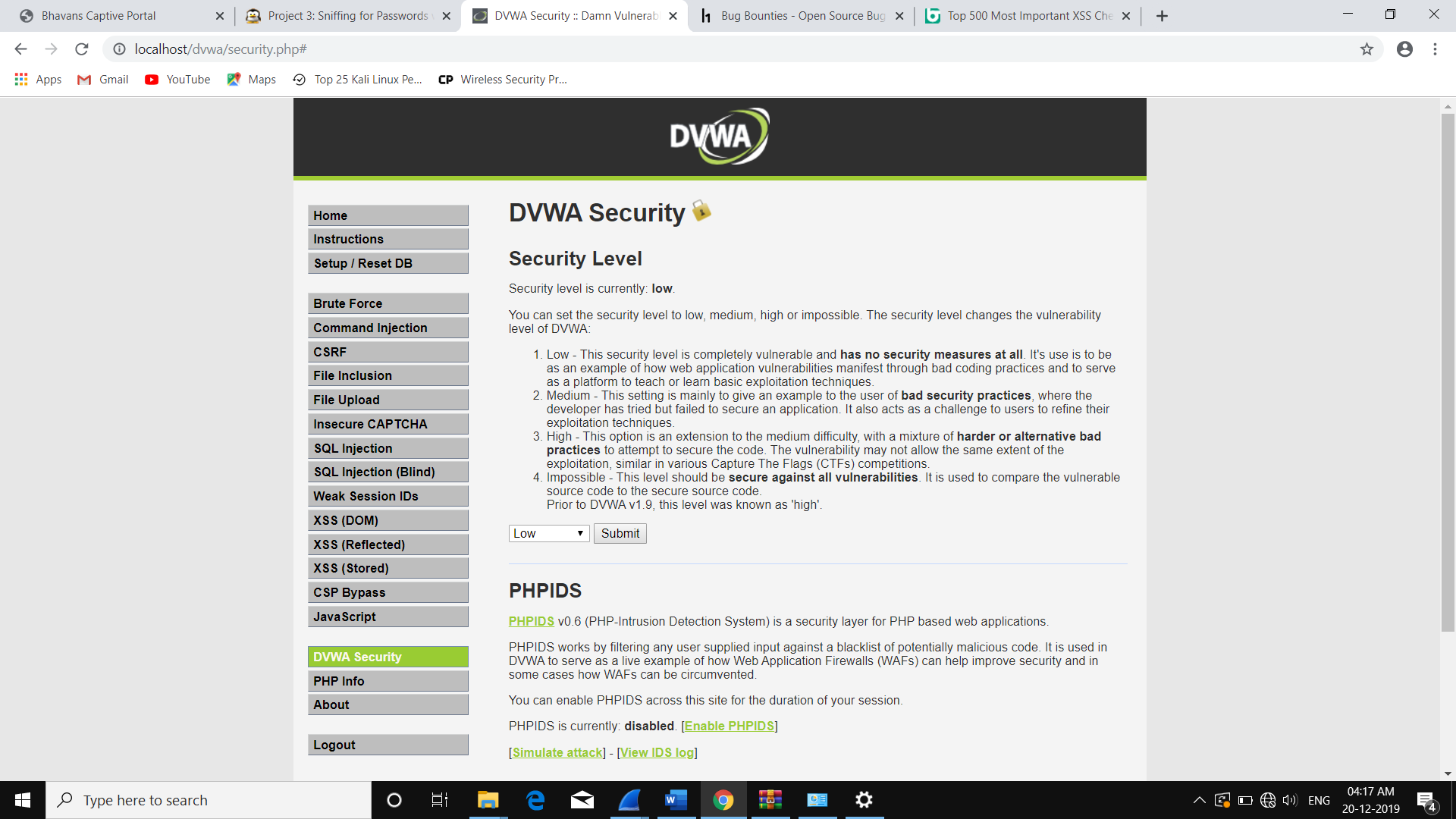


Username: **admin** & Password: **password**

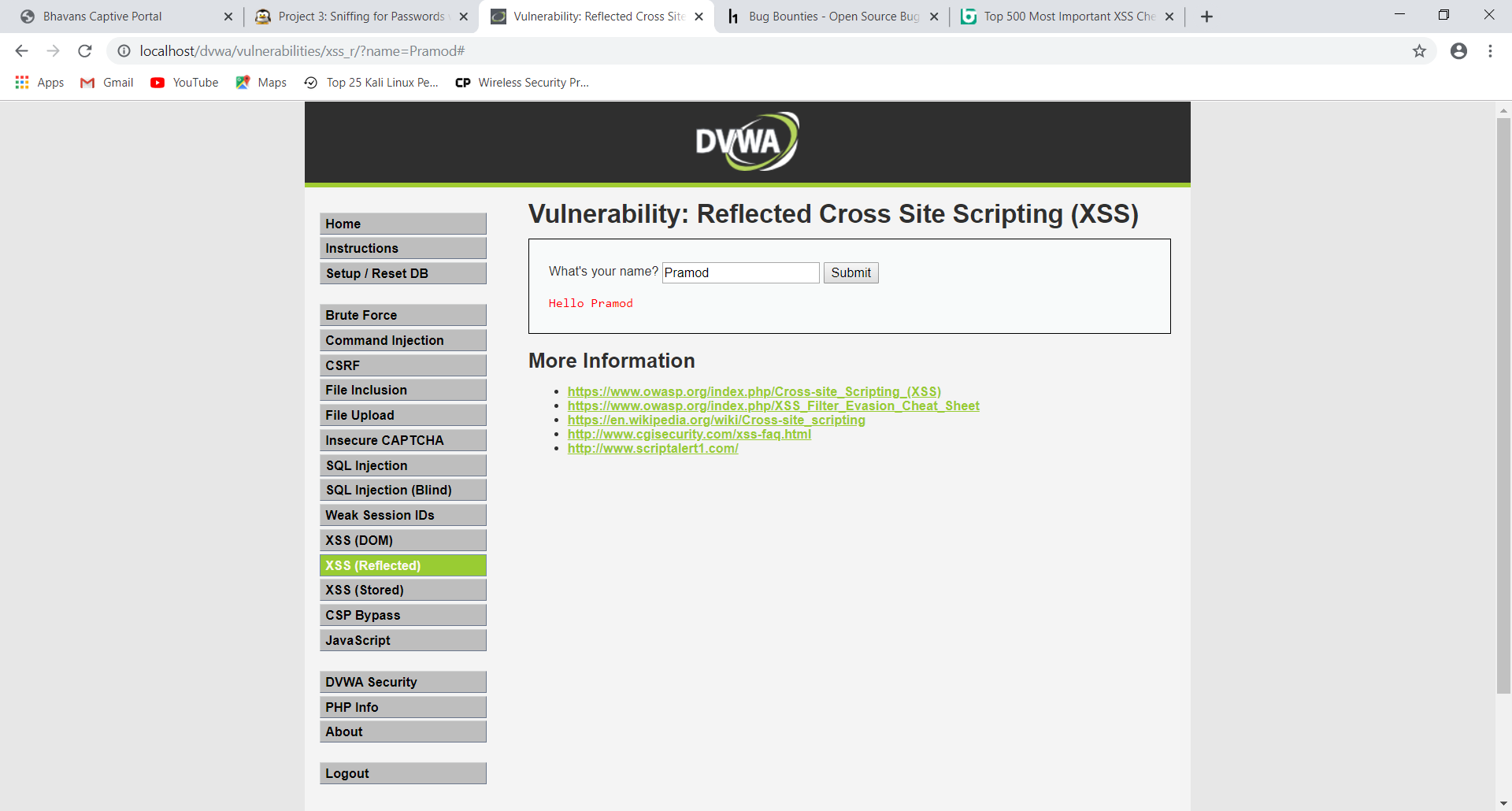




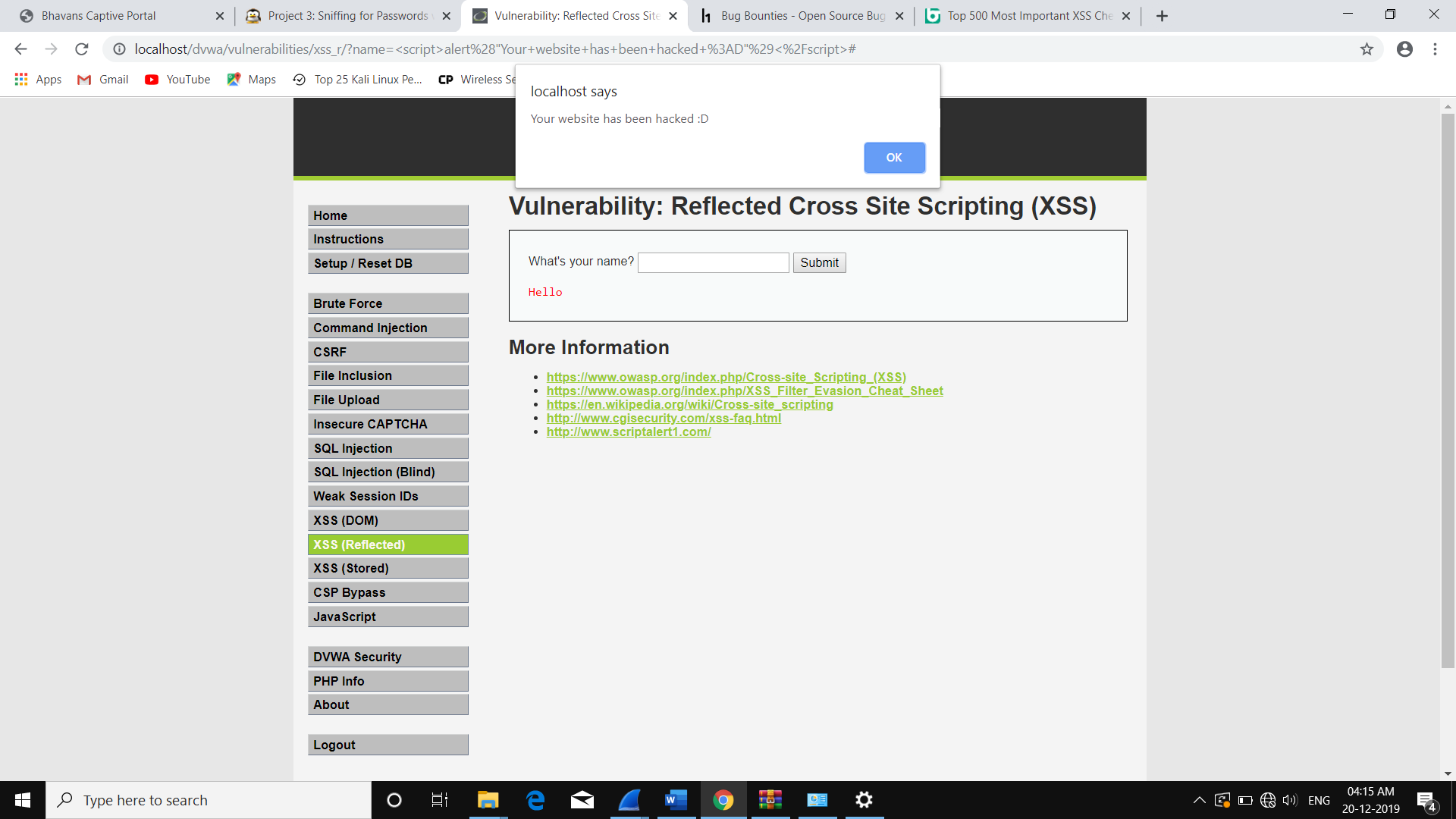
Select DVWA Security & Change Scripting with Security Level : **Low**



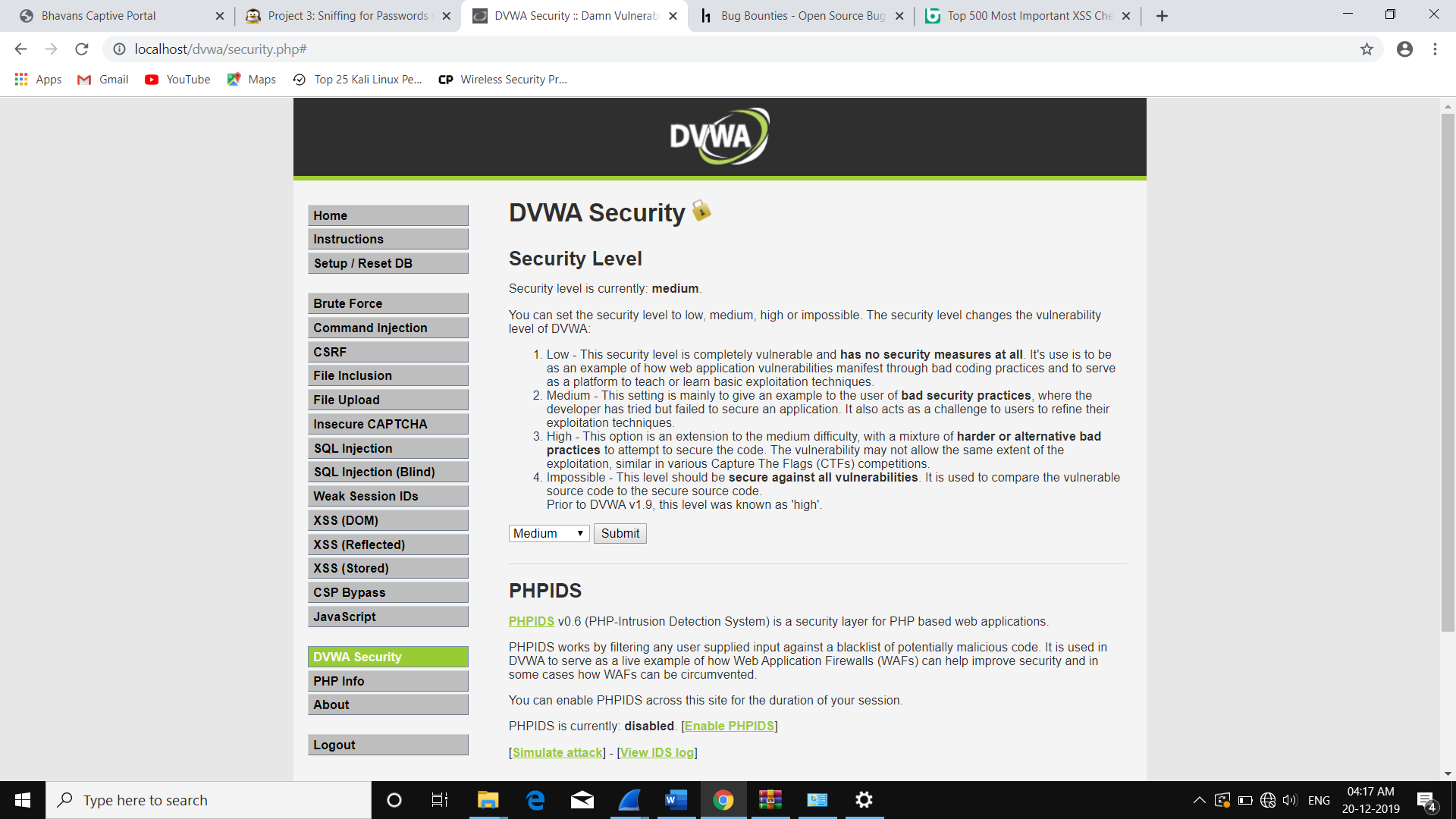
Select XSS(Reflected):



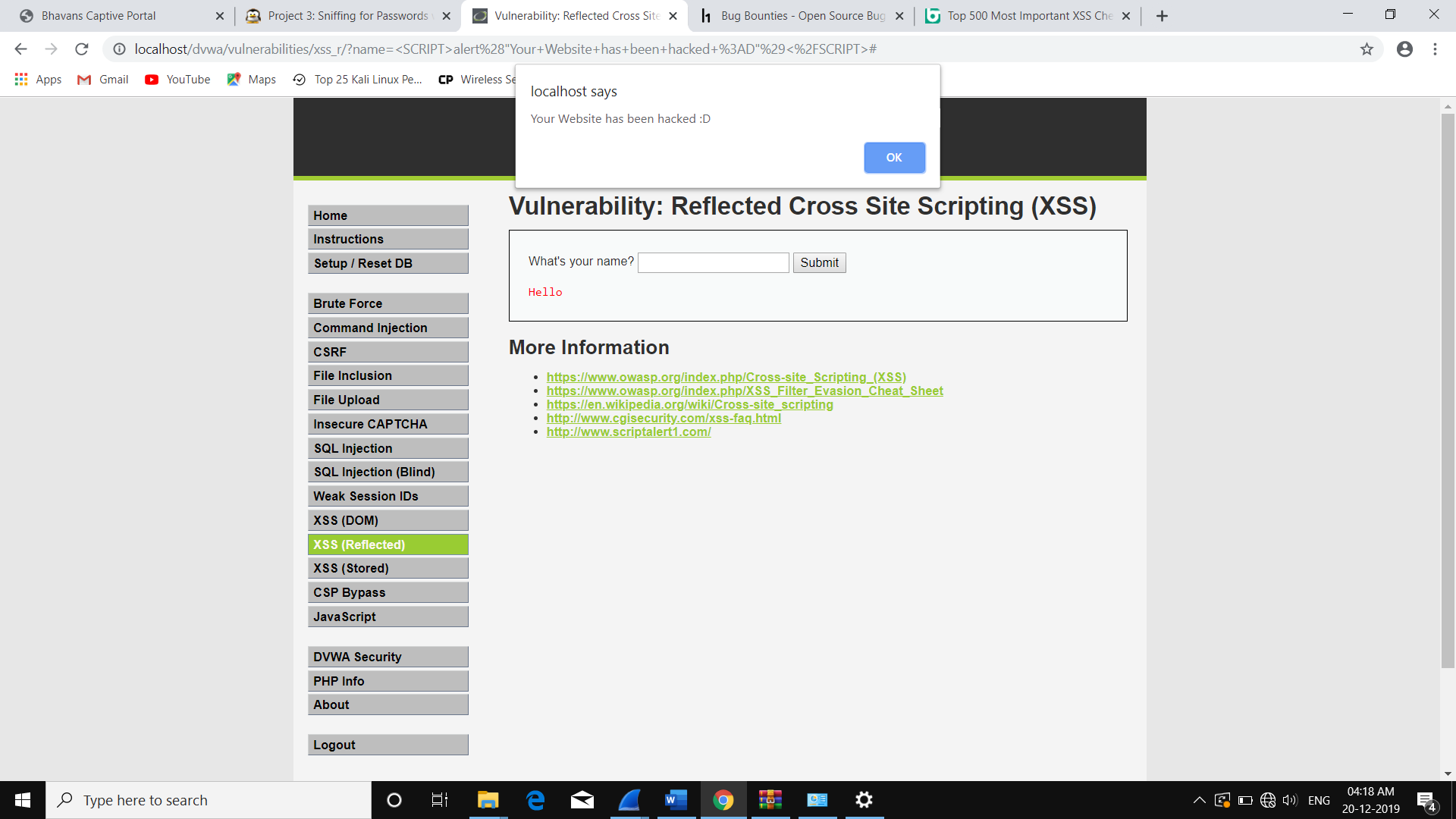
<script>alert("Your Website has been hacked :D")</script>



Scripting with Security Level: **Medium**



<SCRIPT>alert("Your Website has been hacked :D")</SCRIPT>



The **<script>alert(" ")</script>** is not supported in Medium Level Security but it supports Low Level Security. **<SCRIPT>alert(" ")</SCRIPT>** works in Low Level Security as well as Medium Level Security.