Footprinting of Orchid school

Name:- Binay Chaudhary

Date:- 6th/feb/2023

Time:- 10:00 pm

Website:- https://www.orchidharion.edu.np/

Address: Harion-11,Sarlahi

Email: info@orchidintl.edu.np

Phone: 046-530653

Content page no.

Introduction 3

1. Wappalyzer

Wordpress 4.9.2

NextGen Gallery 2.2.54

jQuery 1.12.4

jQuery UI 1.11.4

contact form 7 5.0.1

ii . Censys.io

1. Nmap Online
2. HackerTarget.com
3. Web crawls
4. Ns lookup.io
5. Criminal Ip

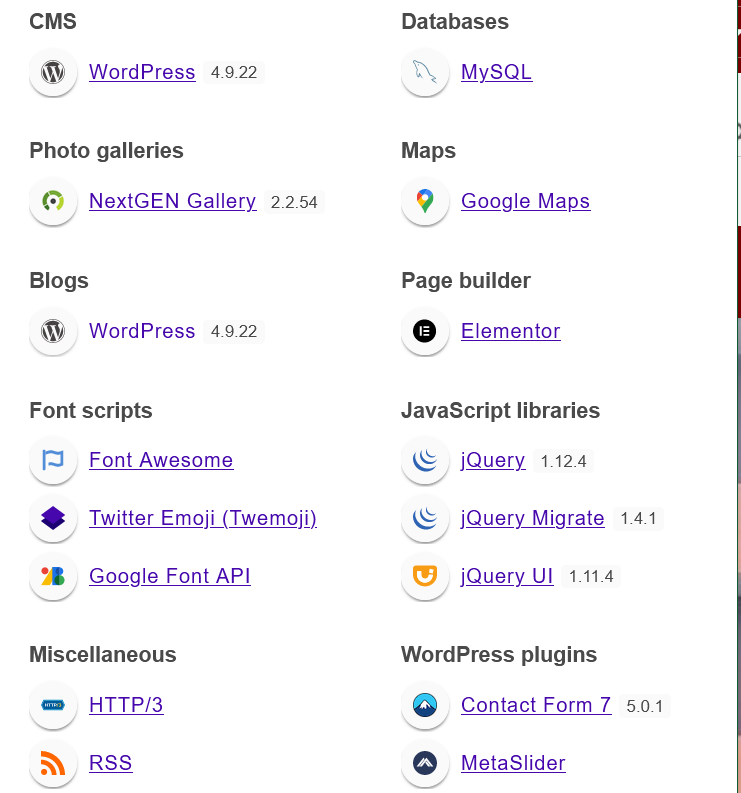
Introduction of Orchid Harion

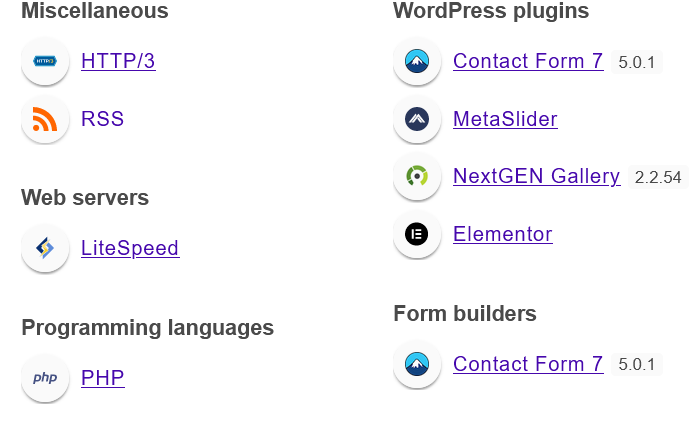
Orchid School recognizes that each child is an individual, that all children are creative; that all children need to succeed. Therefore orchid school respects the individual needs of children; fosters a caring and creative environment and emphasizes the social, emotional, physical, intellectual development of each child.

Our mission is to assist all the students to attain their personal, education and career goals using the latest technology means in the shortest time, affordable fees and the most effective manner.

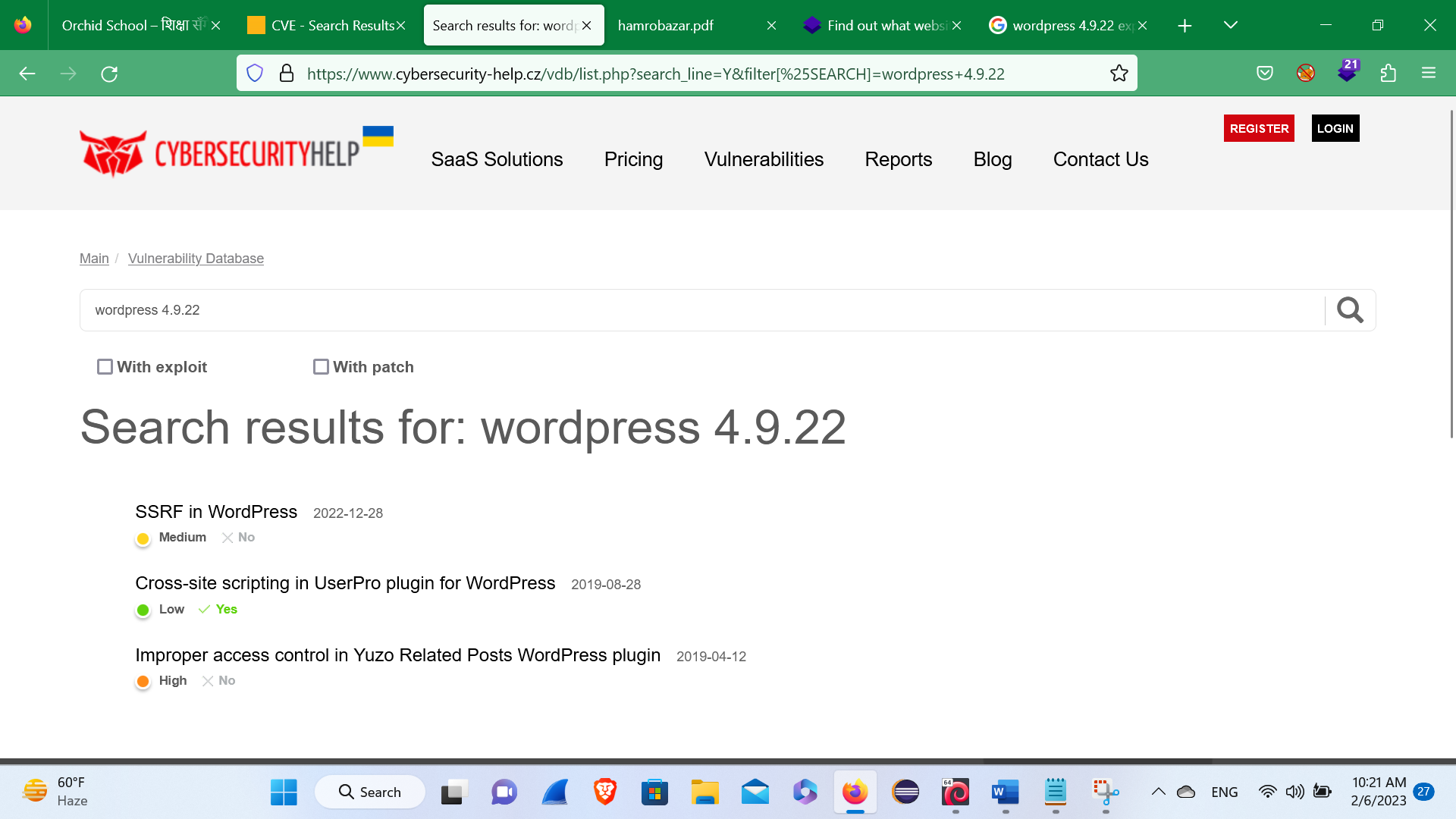
**Wapplyzer**

The Wappalyzer APIs provide instant access to website technology stacks, company and contact details, social media profiles, email verification and more. Track your prospects' technology choices, examine large numbers of websites or enrich your own datasets with technographic insights.



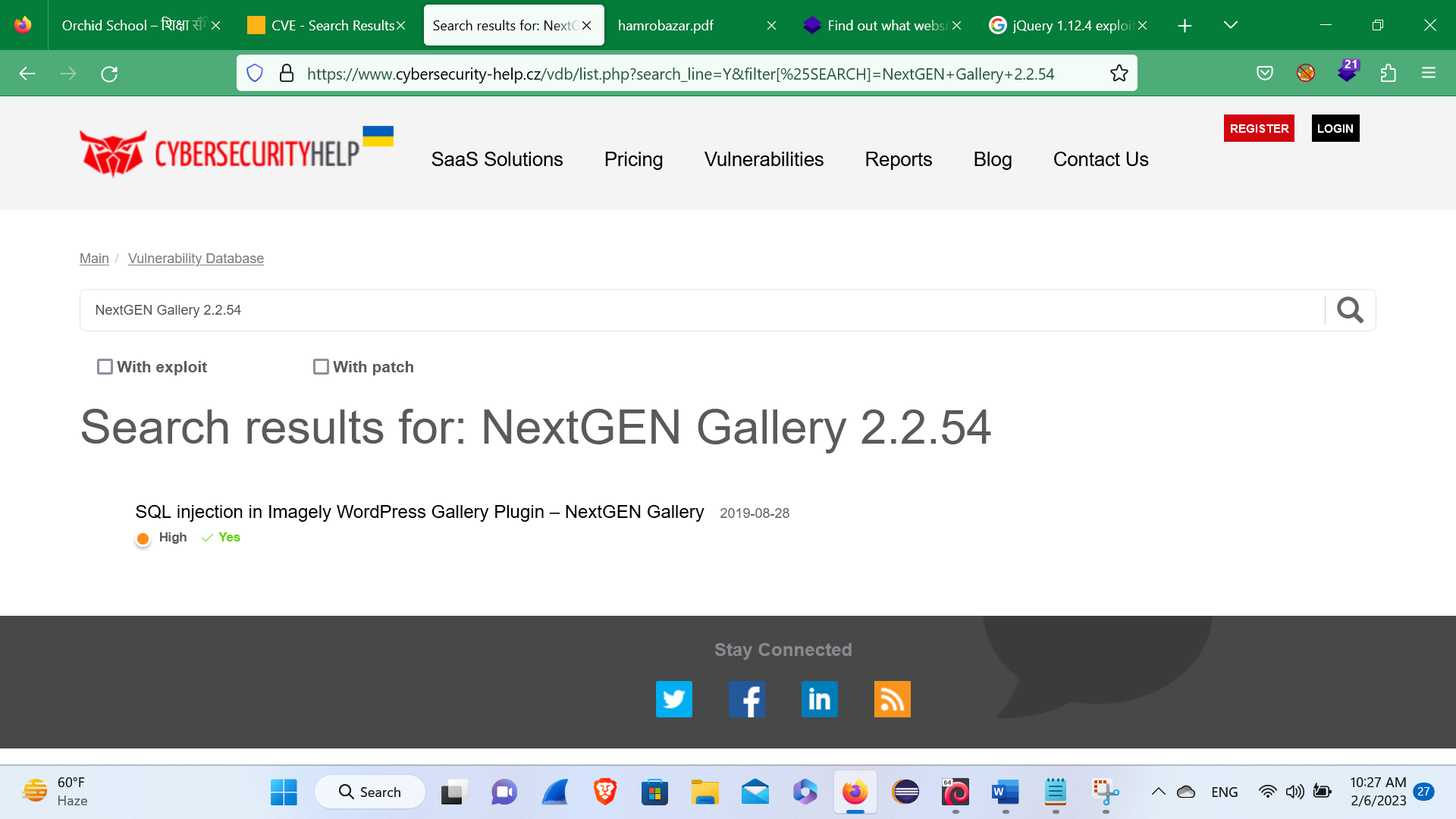


In this above picture I’ve found the version of Technology which is used by Orchid Harion school , let’s go with the version.

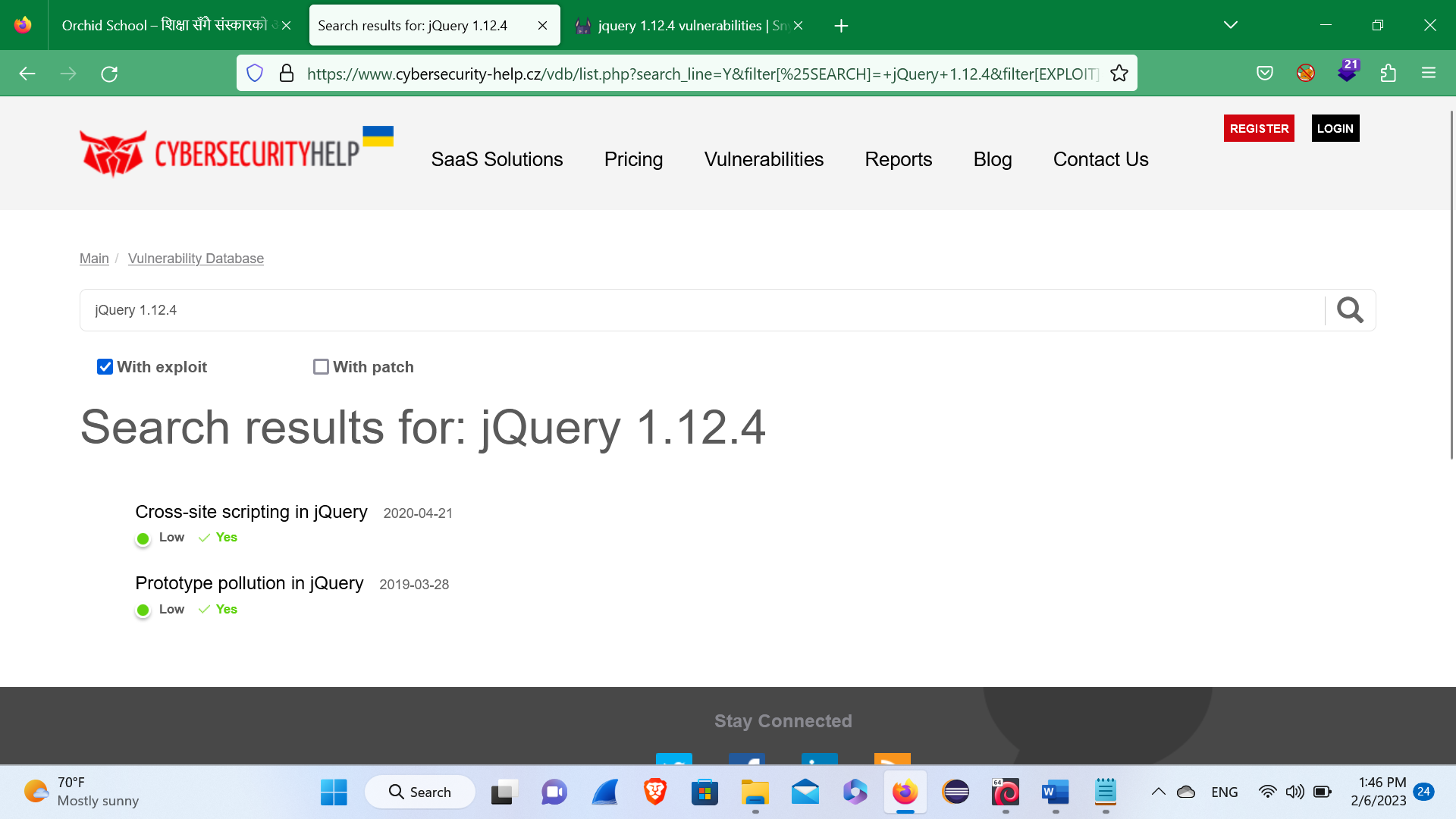
Wordpress 4.9.22

In this version of wordpress 4.9.22 I’ve found the following bugs like SSRF, Cross site scripting, Improper Access control.

**NextGEN Gallery 2.2.54**

****

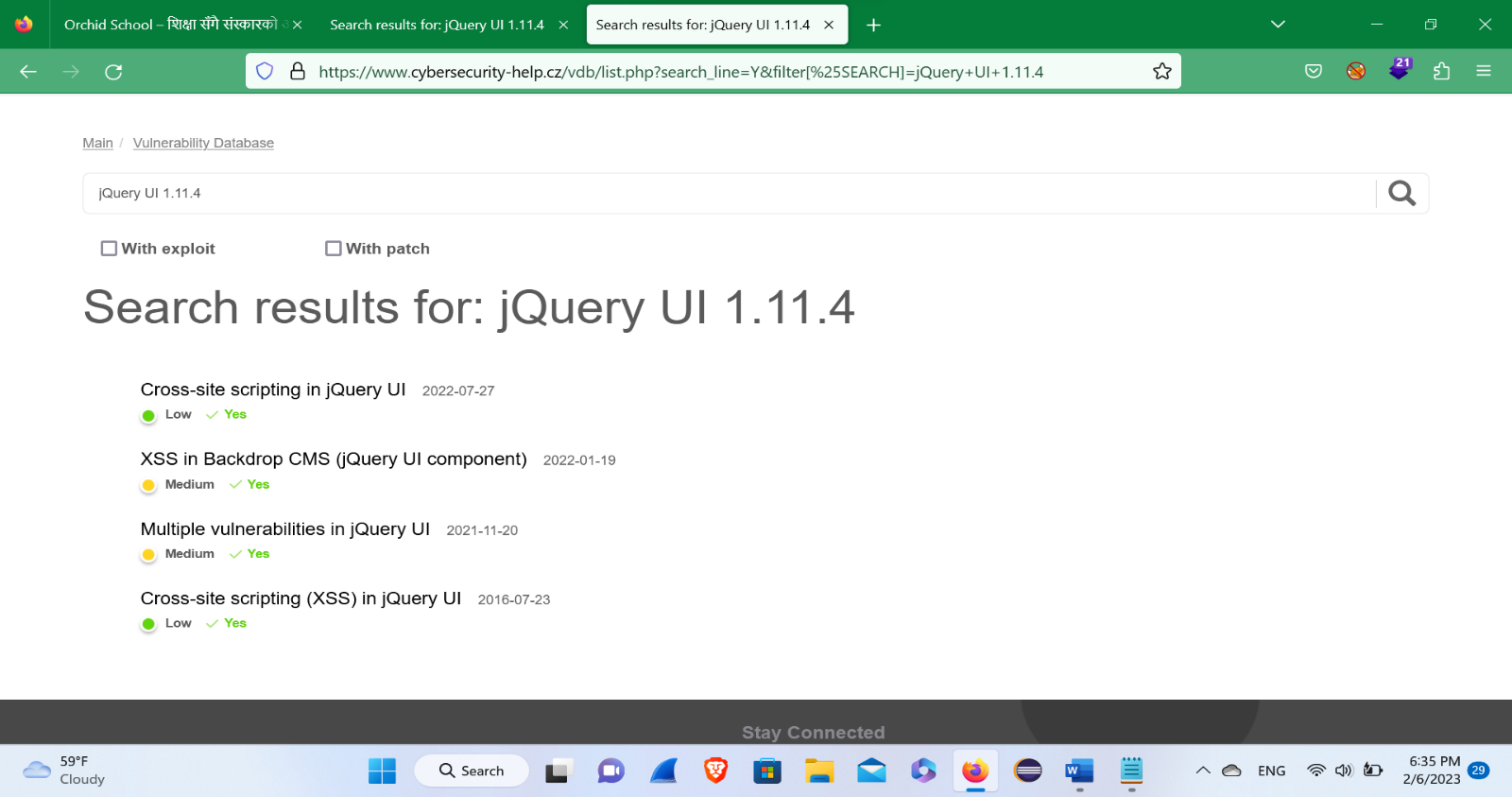
In this, version of NextGEN Gallery 2.2.54 I’ve found the following bug like SQL injection.

**jQuery 1.12.4**

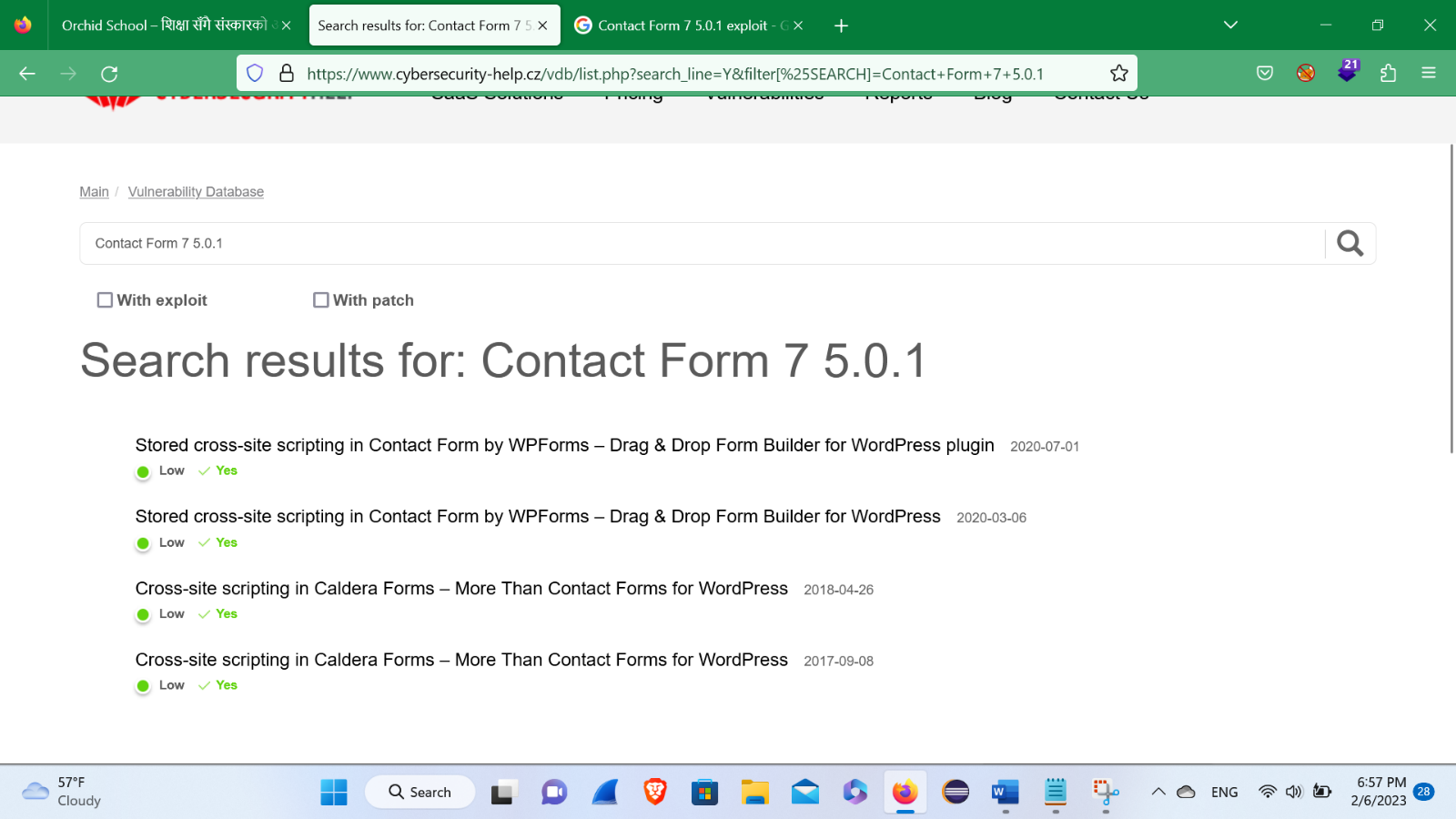
Here, in this version of jQuery 1.12.4, I’ve found the following Bug like

XSS (Cross-site scripting) and prototype pollution.

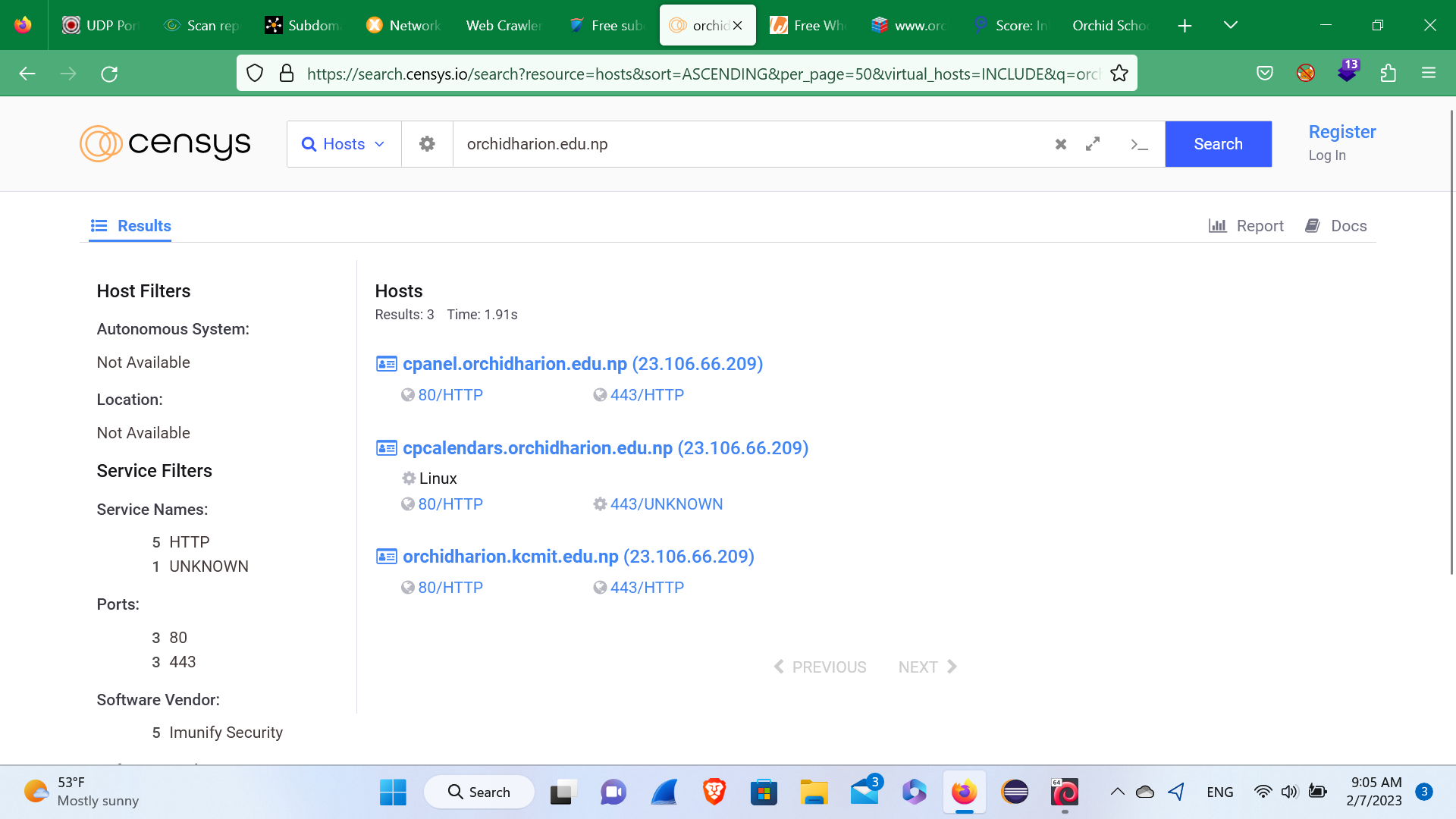
**jQuery UI 1.11.4**



Here, in this version of jQuery UI 1.11.4 I’ve found the following Bug like Cross-site scripting, XSS in backdoor CMS, and Multiple vulnerabilities.

**Contact Form 7 5.0.1**

Here, in this version of Contact Form 7 5.0.1 I’ve found the following Bug like Stored XSS, XSS in caldera forms.

**Censys.io**

Here, In this site of orchidharion.edu.np I’ve found the following Hosts and its open ports like

Cpanel.orchidharion.edu.np (23.106.66.209)

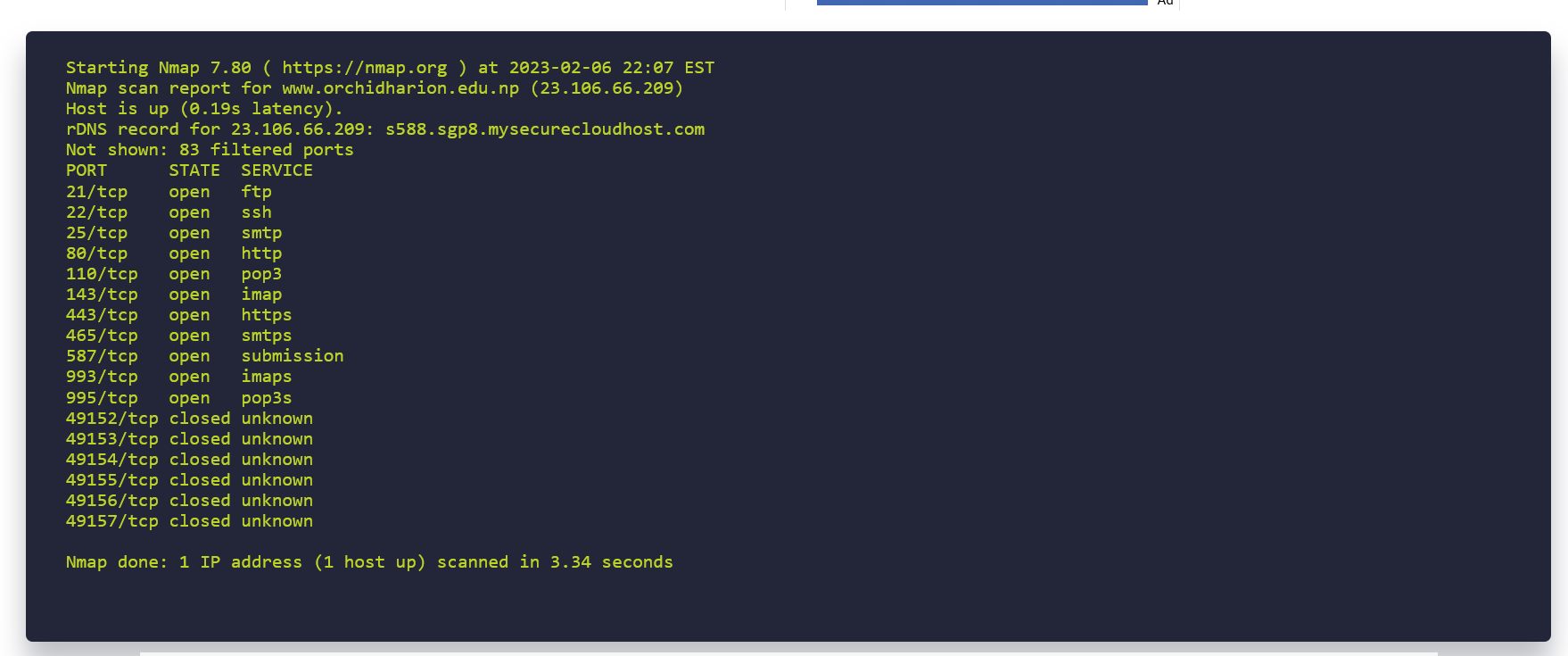
80/HTTP 443/HTTP

Cpcalendars.orchidharion.edu.np

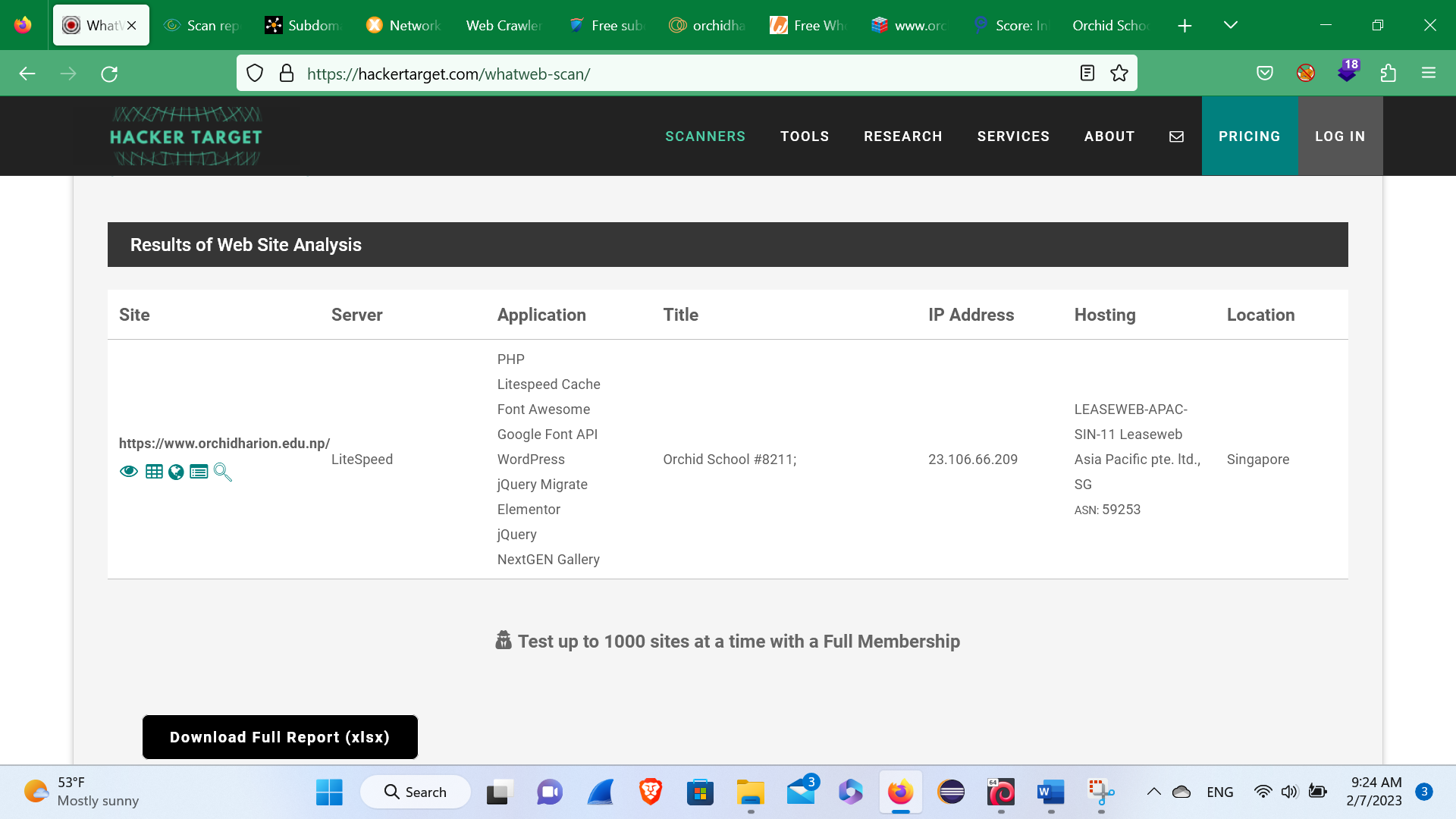
80/HTTP 443/UNKNOWN

Orchidharion.kcmit.edu.np

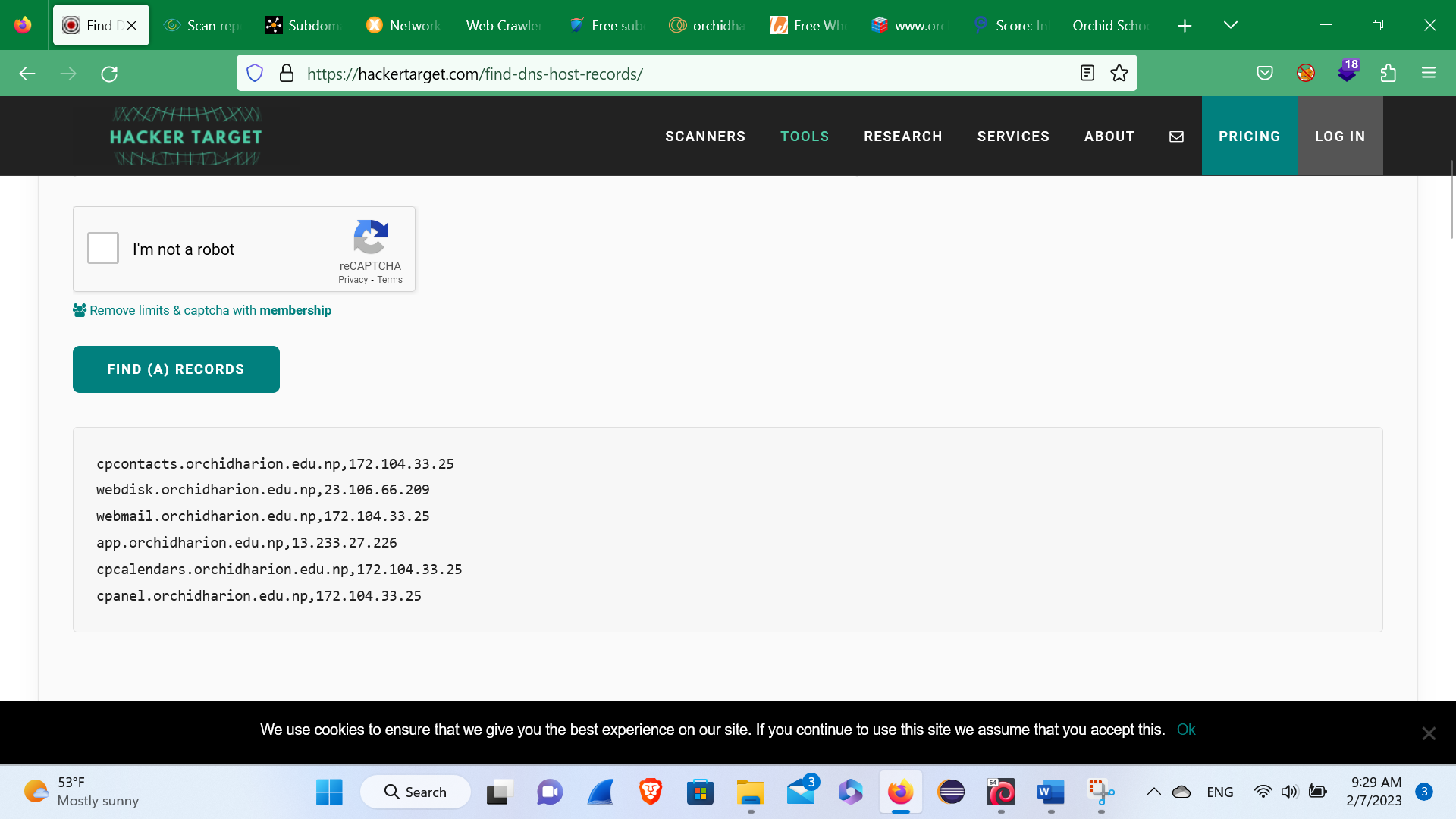
80/HTTP 443/HTTP

**NMAP Online**

Here, In this site of [www.orchidharion.edu.np](http://www.orchidharion.edu.np) (23.106.66.209), I’ve found the following open ports as you can see above in the picture and also found the ip address as mention the above.

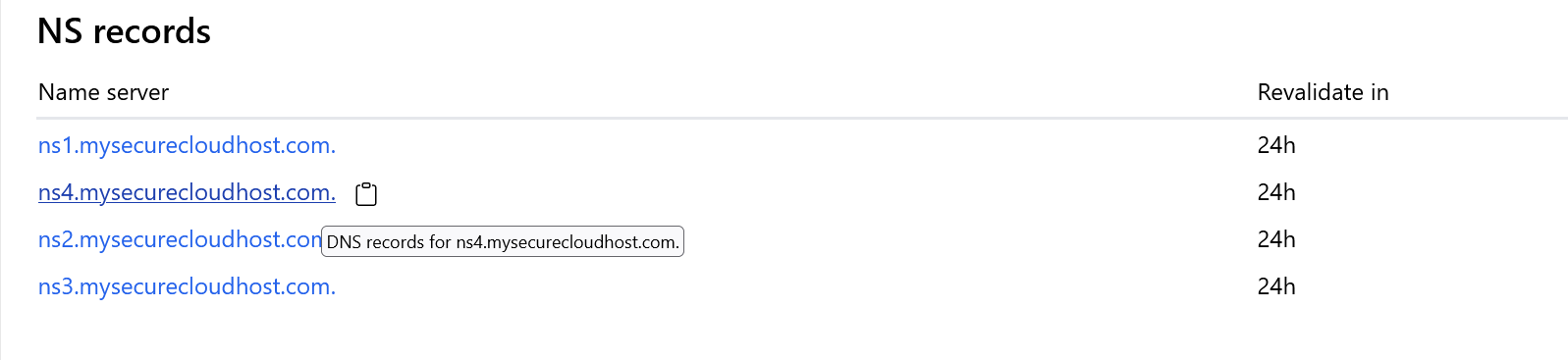
**Hackertarget.com**

Here, in this website of orchid Harion school, I’ve found the site, where is the server, what are the technology they are using, and the title of the website, ip address, From where it is being hosted, and the location of the Company.

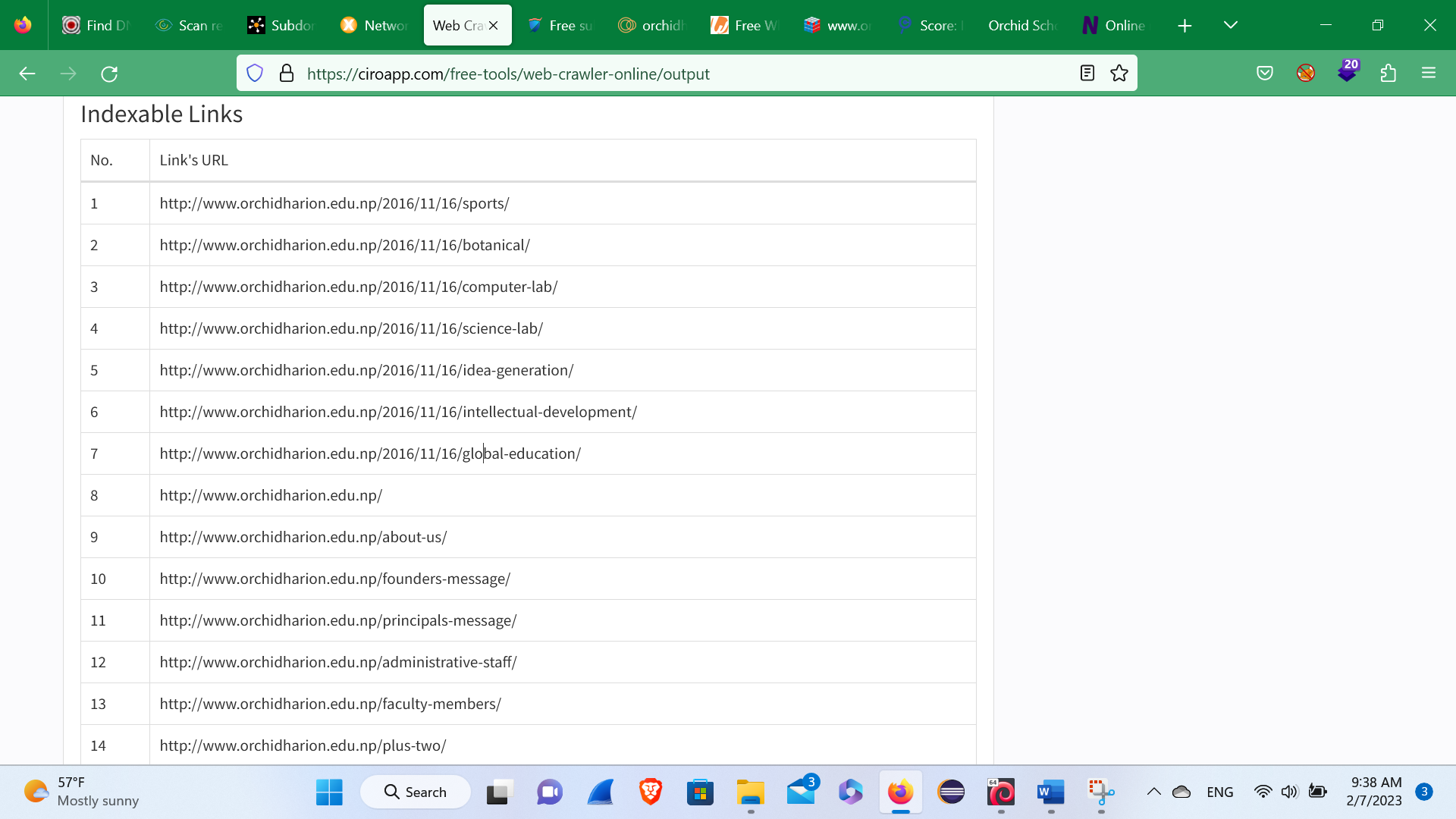


Here, I’ve found the DNS record for the subdomain as you can see in the above figure.

**NSLOOKUP.IO**

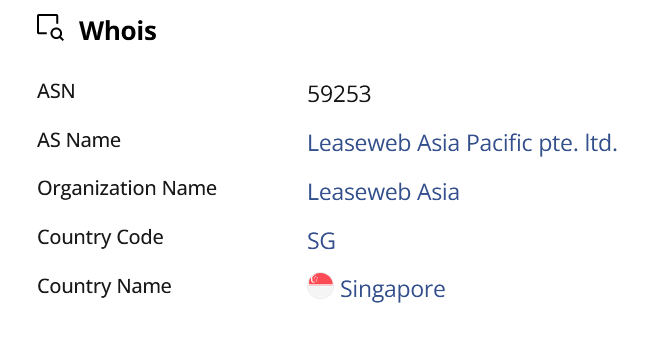
****

Here, in this above picture I’ve found the above Name server request in from the above picture.

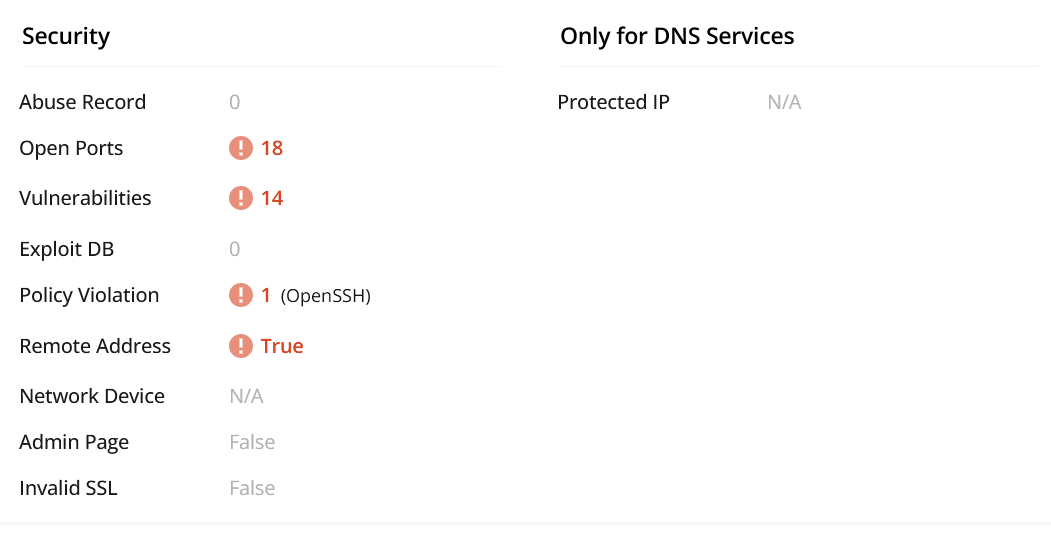
**Crawled Links(web crawls)**

Here, in this site i’ve found the crawled links in the above figure.

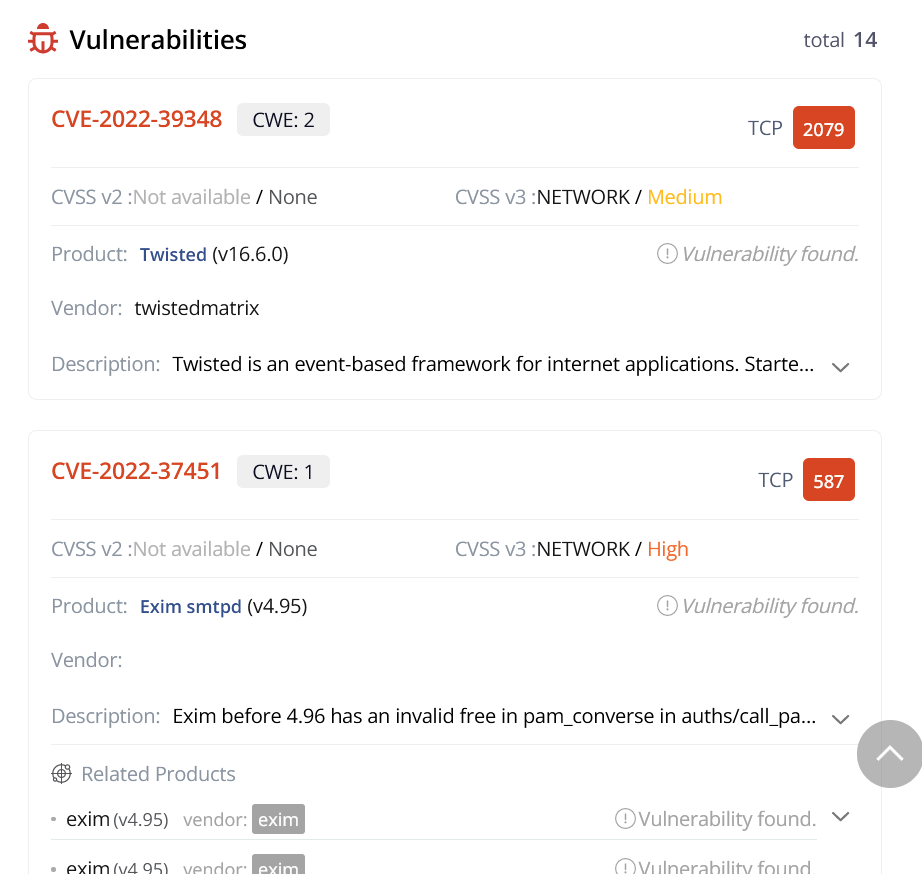
**Criminal Ip**

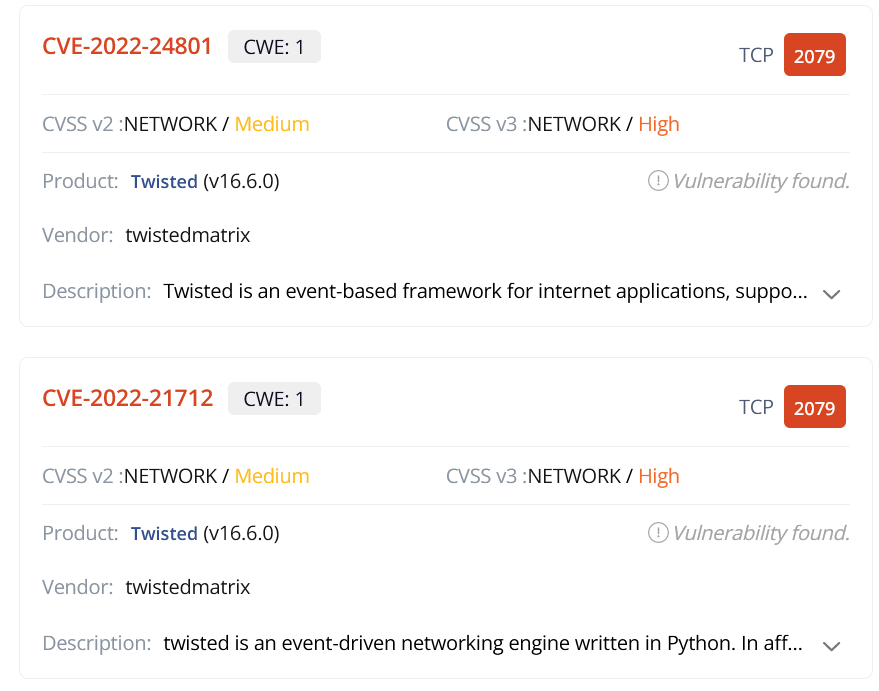
****

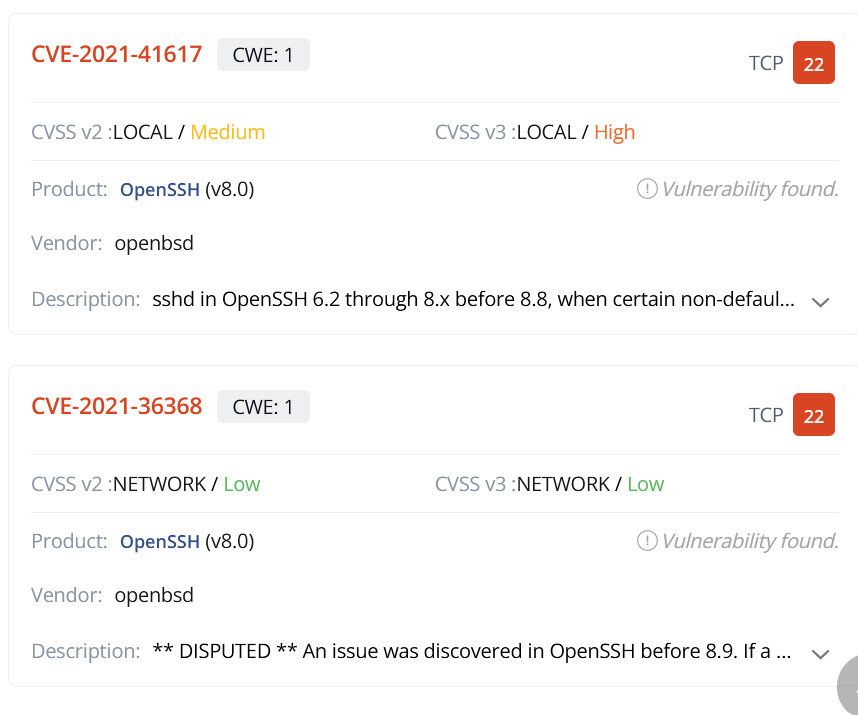
Here, In this figure you can see the whois like ASN number, AS Name, Organization name, country code and the Country Name in the above figure. While doing the criminal ip search I’ve found the following thing as given below in figure:-

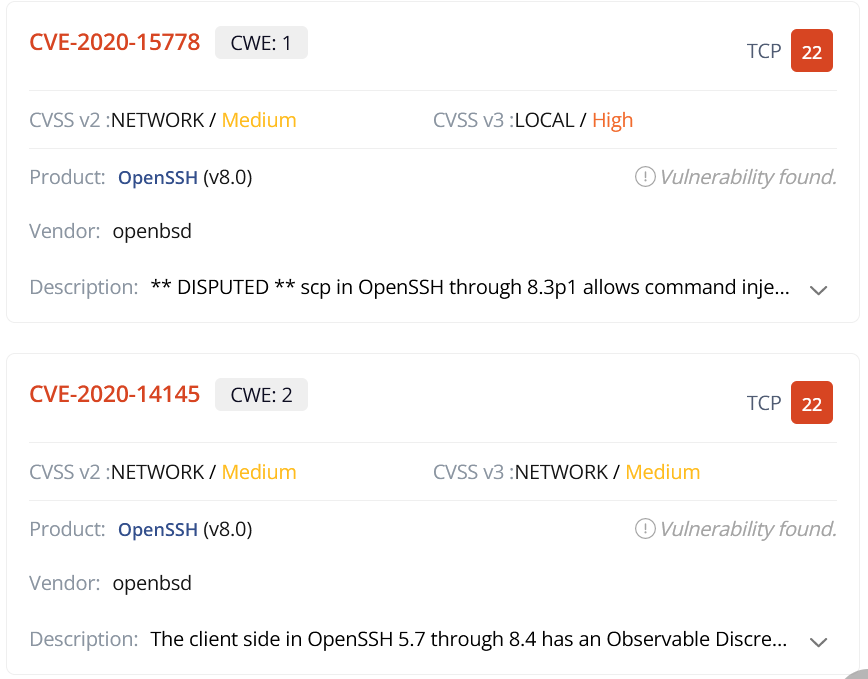


While doing criminal ip I’ve found the Following CVE’S Vulnerability in the given below figure:-

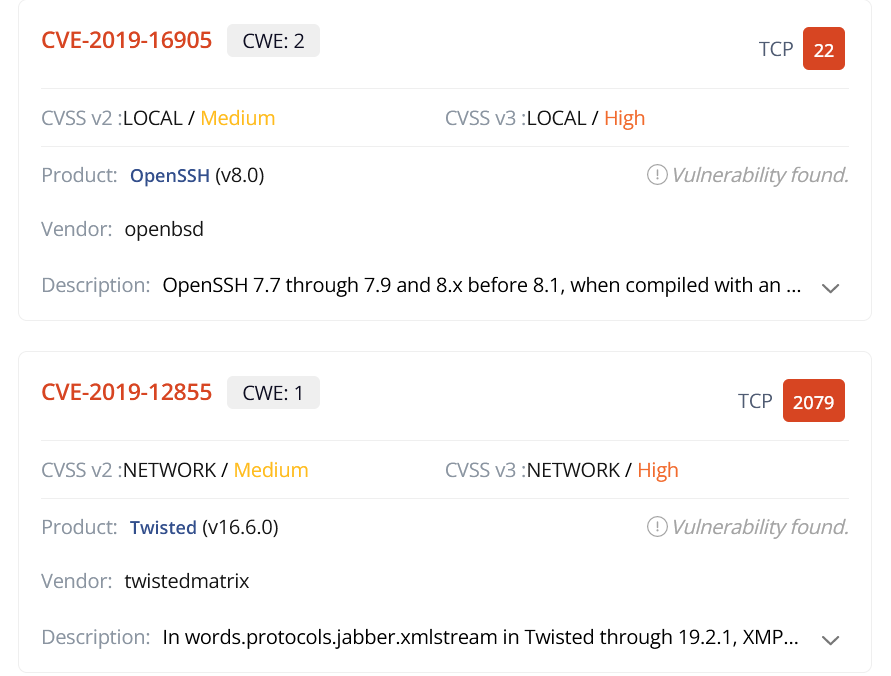


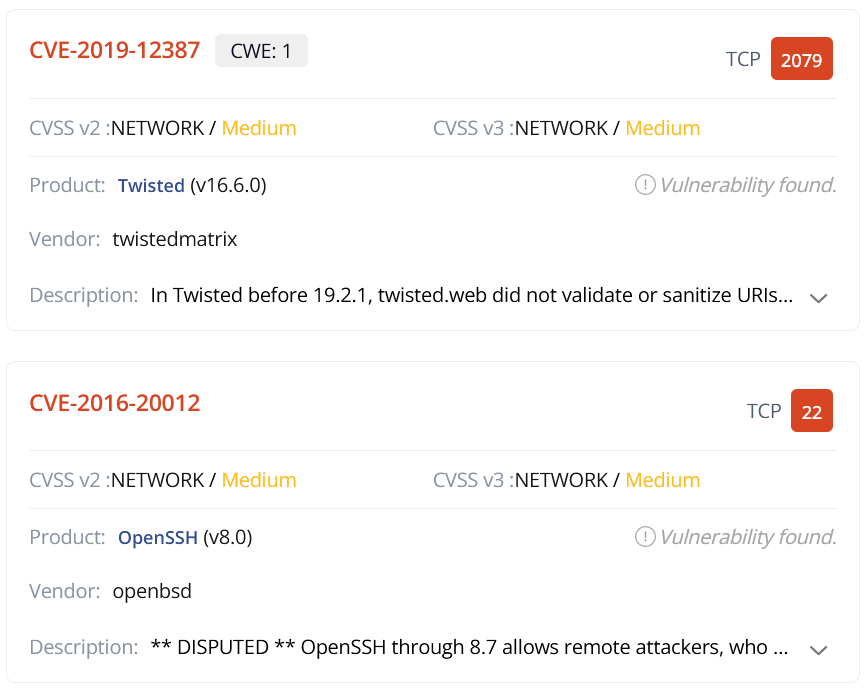


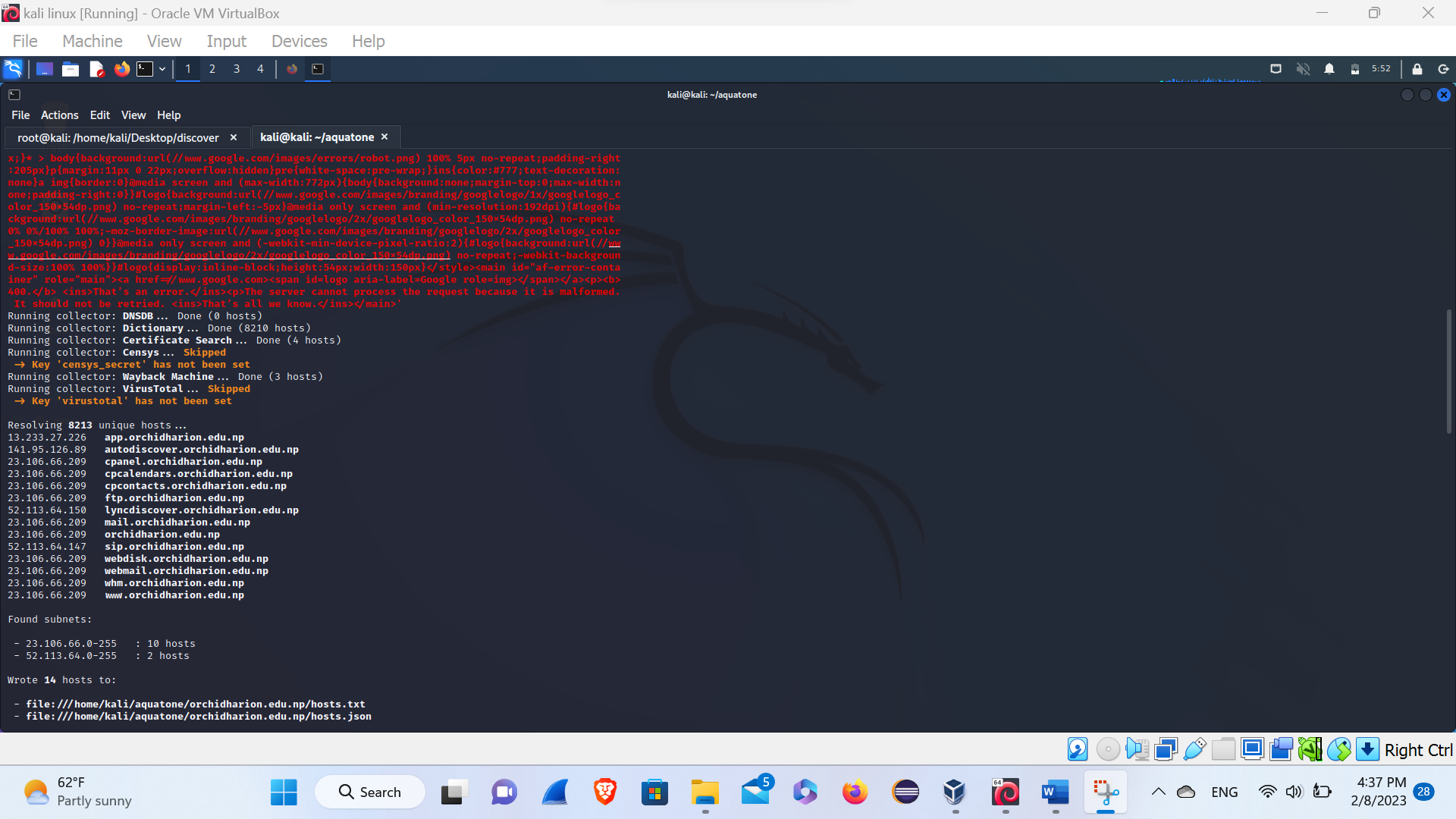




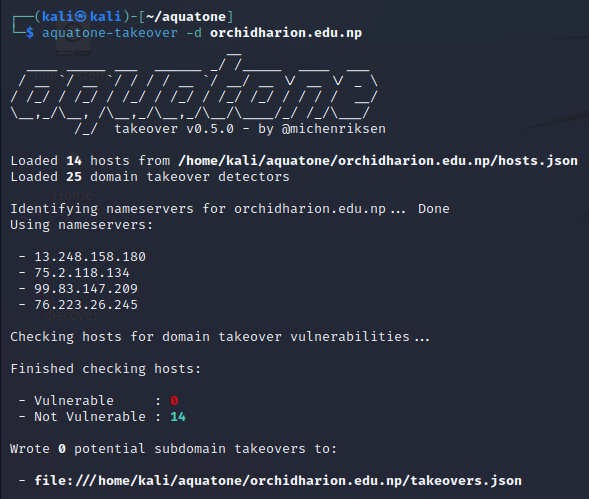




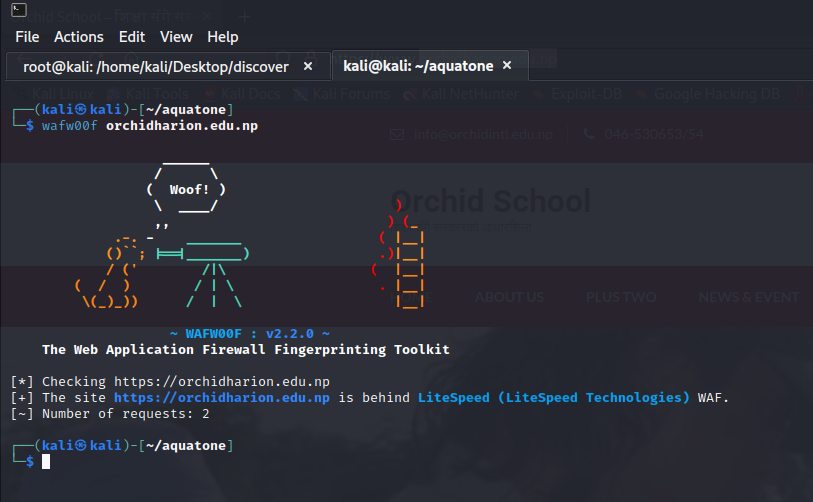


**AQUATONE**

Here in this above figure, I’ve found that there is 8213 unique hosts, among of them I’ve found 10 hosts that can be wulnerable,



**Here**, In this figure I’ve searched for vulnerable domain to take over but there is no any vulnerable.

**Wafw00f**

Here, In the above figure I’ve found the firewall that the company is using.

Conclusion

Here in this site of Orchid Harion school, I’ve found the Bug which may the data will be publicly available which may impact losses of company. If there is a outdated version of a software or Technology they have to up to date the Technology. Here, in this website (<https://www.orchidharion.edu.np/>) I,ve found many critical bugs which may impact the company reputation and may attacker take the advantage of loopholes of this company, so the company need an pentester for doing the pentesting of the company website, and may the company will patch up when the pentester penitest his company. The company have to work for the up to date of the web Technologies that they are using.