**FIND THE VULNERABILITY**

**TEAM MEMBERS :-**

* **PARTH SARTHI -**
* **CHETNA TAPARIA -**

**WHAT IS VULNERABILITY ?**

A weakness of an asset or group of assets that can be exploited by one or more [cyber threats](https://www.upguard.com/blog/cyber-threat) where an asset is anything that has value to the organization, its business operations and their continuity, including information resources that support the organization's mission.

**WHY WE DO VULNERABILITY TEST OVER A WEBSITE ?**

Vulnerability Testing will provide a picture on unnecessarily open ports, ensuring updates of any outdated software/services, etc. Sometimes, major services will require separate servers, which will also be visible through this procedure.

**HOW TO KEEP CHECK ON VULNERABILITY ?**

Vulnerability management involves several steps ranging from vulnerability scanning to taking other aspects such as risk acceptance, mitigation, and remediation.

* ****Identify assets:**** The first step in vulnerability management is identifying assets in your company. For example, if a database stores the sensitive information of customers, it needs to be well protected.
* ****Scan vulnerabilities****: Once you have identified critical assets, scan them for vulnerabilities. You can do this via regular network scanning, penetration testing, or using an automated tool like a vulnerability scanner.
* ****Identify vulnerabilities****: Once the network is scanned for vulnerabilities, the pen test results, or vulnerability scan results are analyzed to determine anomalies that suggest risks or potential malicious threats that could take advantage of a security vulnerability or could exploit a vulnerability in the future.
* ****Determine the severity of vulnerabilities****: In this step, vulnerabilities are classified on the basis of their severity, the level of risk they represent, and their impact on applications, networks, and servers on the system.
* ****Address vulnerabilities****: After determining the severity of vulnerabilities, it is time to accept, transfer, or mitigate these vulnerabilities.

**WHICH PLATFORM WE USED TO DO THE VULNERABILITY CHECK ?**

<https://hostedscan.com/>

**ABOUT THE PLATFORM WE USED TO DO THE VULNERABILITY CHECK ?**

founded in seattle, washington in 2019, hostedscan, llc. is dedicated to making continuous vulnerability scanning and risk management much more easily accessible to more businesses.

the hostedscan team includes former amazon web services engineers, security researchers and consultants, and enterprise software executives. we are always looking to hire smart and motivated engineers who care deeply about security.

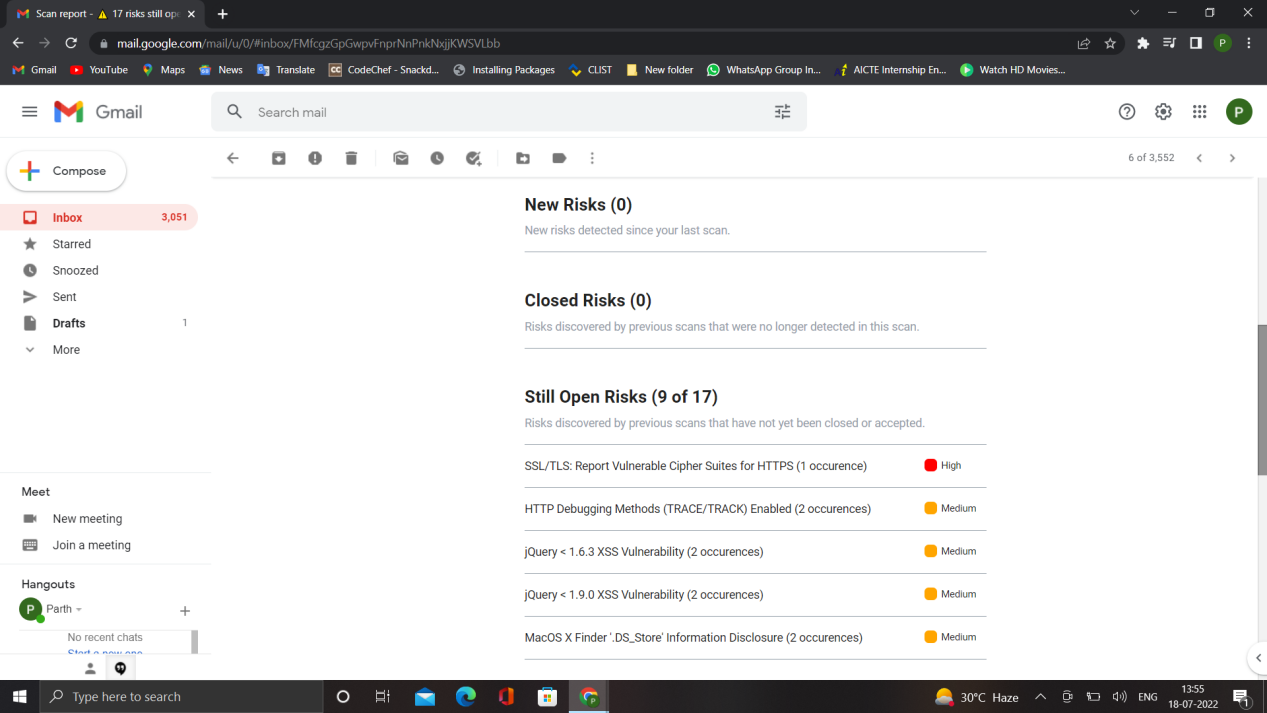
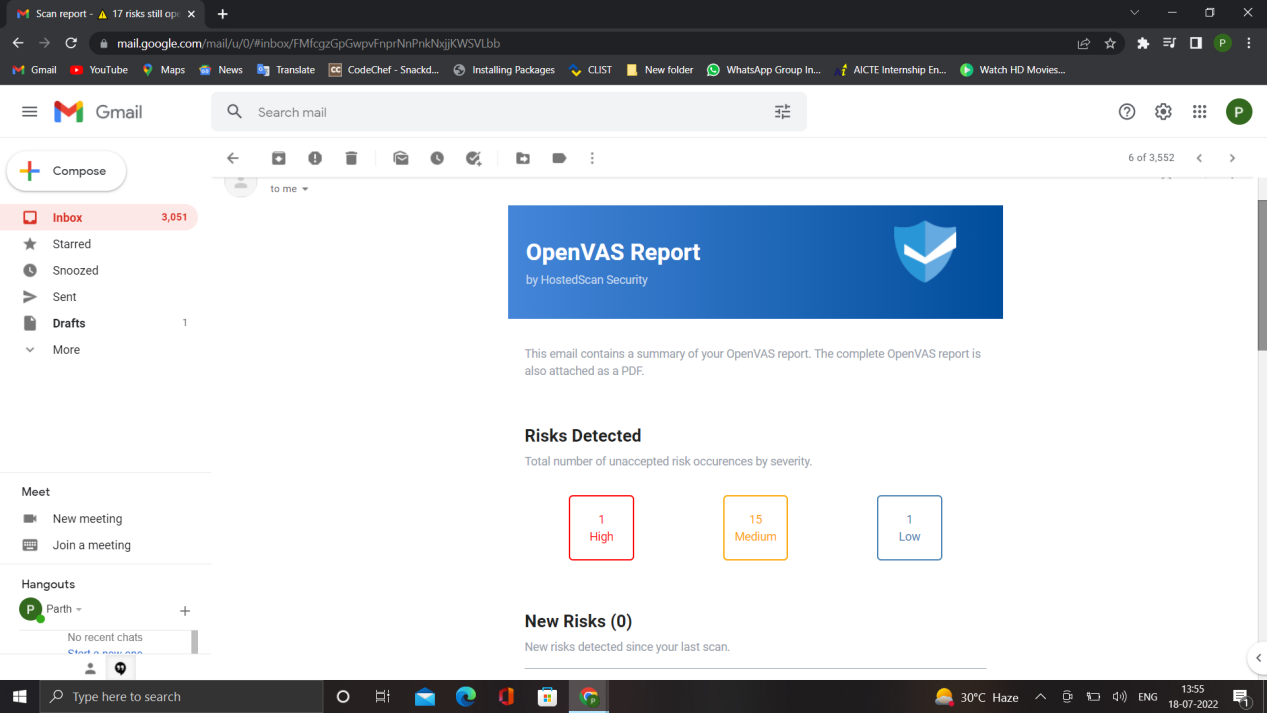
**HOW HOSTEDSCAN DO VULNERABILITY TEST ?**

first it take the url of the website on which we have to do the vulnerability test then it ask for the mail id on which we will get the vulnerability test report of that website

**ON WHICH WEBSITE WE DID THE VULNERABILITY TEST ?**

<http://cs.nits.ac.in/>

**OUR RESULT ?**

****

**TO GO THROUGH THE PDF OF OUR VULNERABILITY TEST RESULT ?**

<https://drive.google.com/file/d/1maRtK22Exv4Ejdv9fJSV4bMPIKvuNjCI/view?usp=sharing>

<https://drive.google.com/file/d/1Yg-t13owjVf5IpUiDfLv1aOmn1irkeSE/view?usp=sharing>

<https://drive.google.com/file/d/1wH1CQJW66hXk7WNvuaDo-yobKwcE1-XE/view?usp=sharing>

**RESOURCES**

<https://www.upguard.com/blog/vulnerability>

<https://www.getastra.com/blog/security-audit/website-vulnerability-testing/#:~:text=Vulnerability%20Testing%20will%20provide%20a,be%20visible%20through%20this%20procedure.>

<https://www.cypressdatadefense.com/blog/vulnerability-management-best-practices/>