**Name:** Hemant Jain

**Lab Progress Report Due Date:** 03/29/2021

**Current Week Since Start Date:** Week 10 (03/31/2021– 04/06/2021)

**Reporting Week:** From Mar 23, 2021 to Mar 29, 2021

**Summary about the TestOut Module-10 Learning:**

From the TestOut LabSim, I learnt about Securing Data and Applications. In this week’s module., numerous conventions made within the past were outlined with few to no security controls. An unsecured protocol is one that does not give verification or encryption, or one that employments plaintext for passing authentication data or information. More current conventions with security controls incorporate Secure Attachment Layer (SSL), Transport Layer Security (TLS), Secure Shell (SSH), HyperText Exchange Convention (HTTP), and HyperText Exchange Convention Secure (HTTPs).

In the later module, discussed in brief about IPSec Facts, Protocols, Modes of Operations, Internet Key Exchange(IKE), IPSec facts. Detailing out each layer of the OSI Model and discussing the two IPsec protocols namely Authentication Header(AH), Encapsulating Security Payload(ESP). The transport and tunnel mode in the IPSec and IKE facts was outlined in summary. Discussed about the Data Loss Prevention (DLP), which is a system that attempts to detect and stop breaches of sensitive data within an organization. Various DLP Implementations namely Network DLP, Endpoint DLP, File-level DLP, Cloud DLP were discussed in the further outliners. The two masking algorithms Dynamic data Masking and Static Data Masking working by replacing the sensitive data with the realistic fictional data.

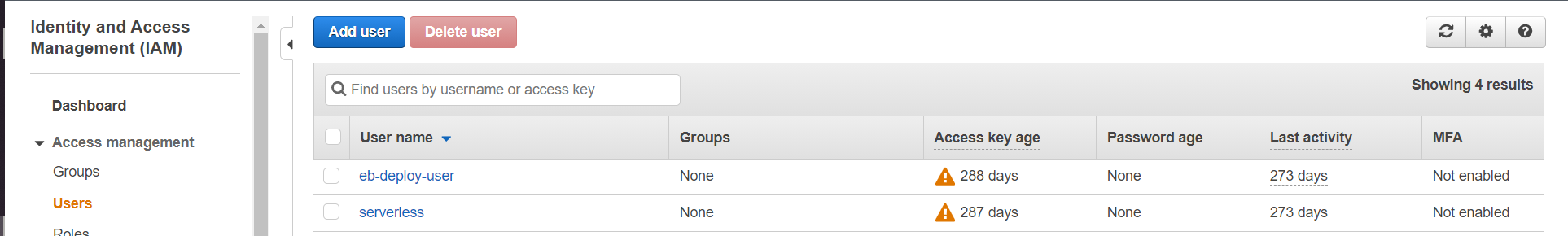
Tokenization which is an effective tool to avoid the data loss and replaces out the actual data with a randomly generated alphanumeric character set called a token and stores original data on a server, protecting data on its server with authentication and authorization protocols allowing the continued control access to the file. Rights management classified in two types : Digital Rights (DRM) and Information Rights(IRM) was discussed.

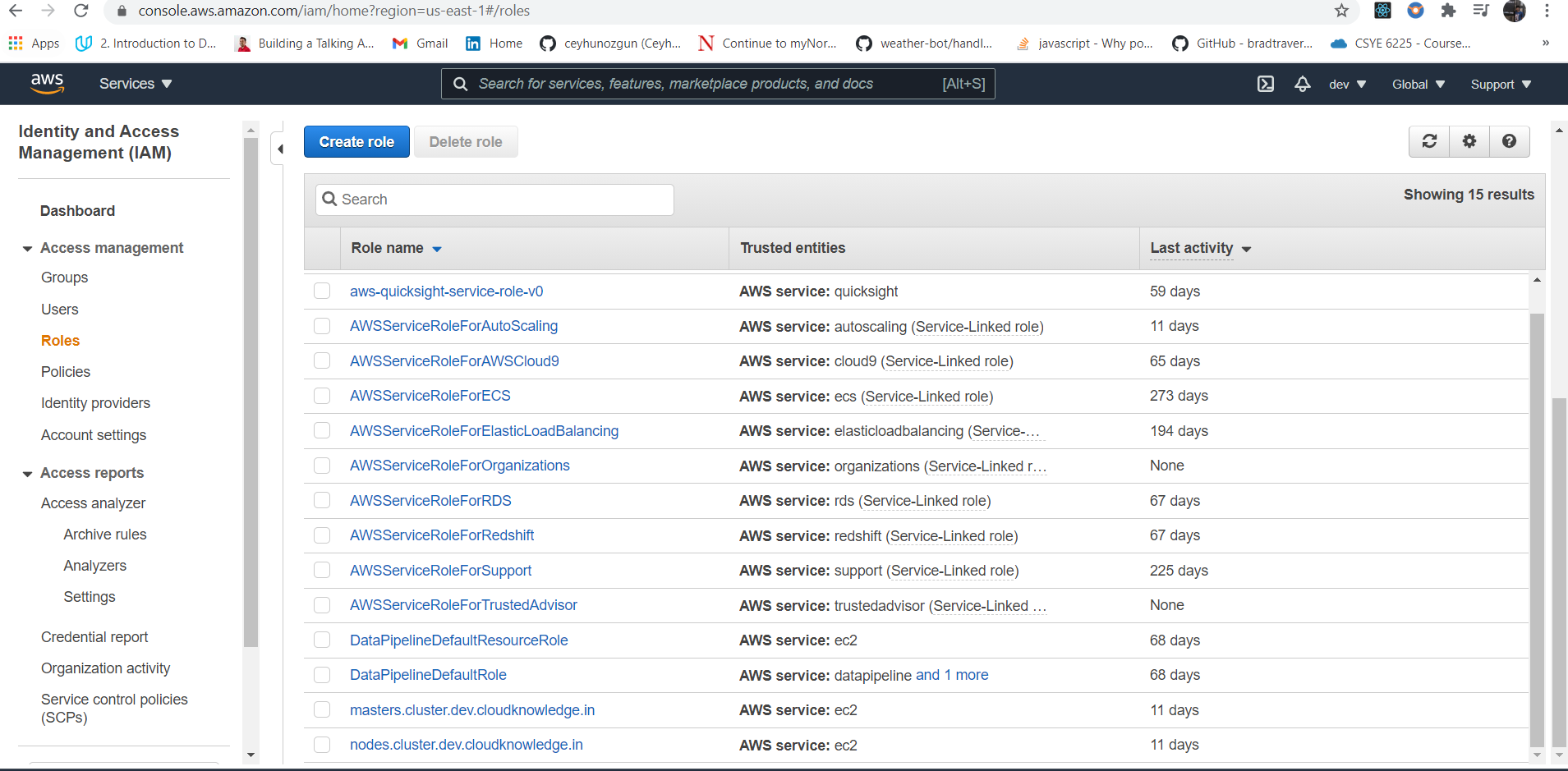
Learnt Techniques for the Enhanced Browser Privacy in the Browser Settings Cookies, Cache, Security, Add-ons, General. In detail description about the various methods attackers use to find the bug/loophole in the web applications and exploit it out namely Privilege Escalation, Pointer Dereference, Buffer Overflows, Resource Exhaustion, Memory Leaks, Race Conditions, Error Handling, Improper Input Handling, replay attacks, Pass the hash, API attacks, SSL Scripting, Driver Manipulations.

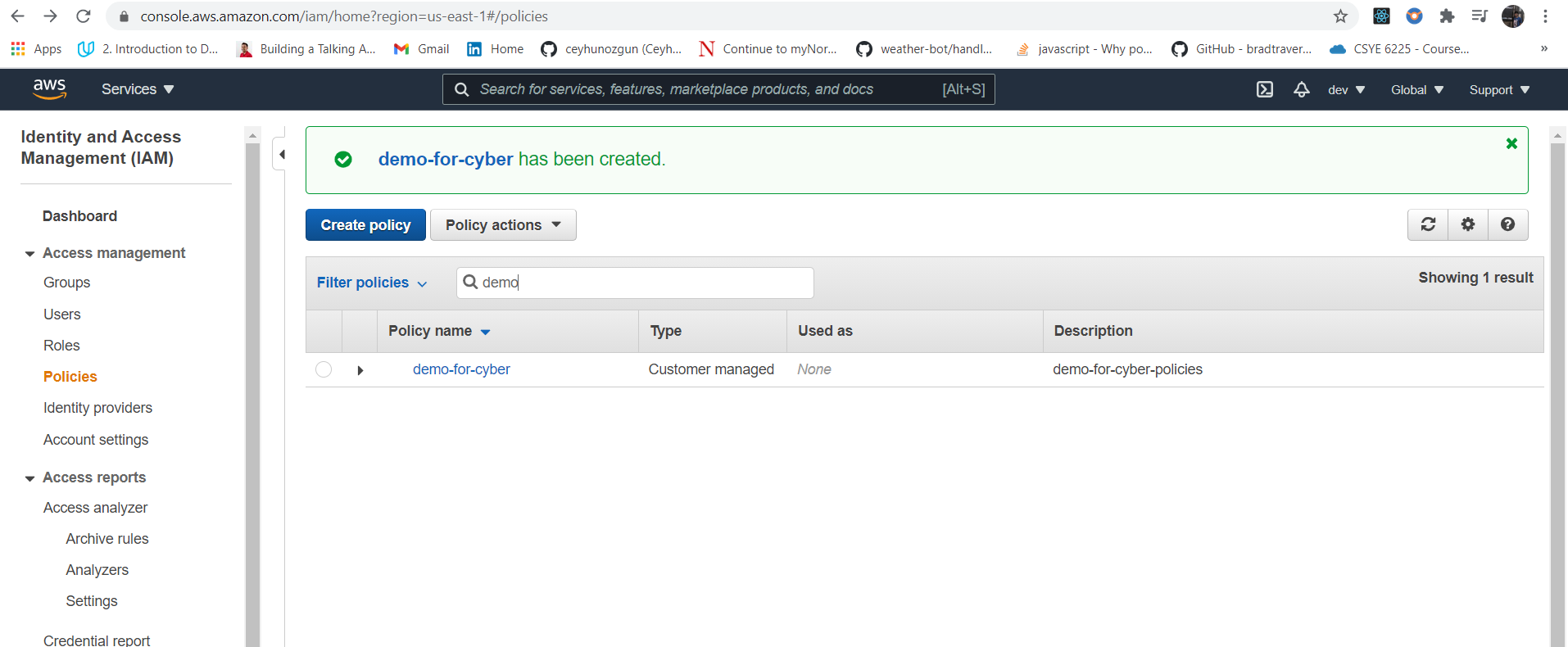
Discussed in summary about the various Life Cycle Models available: Waterfall and agile along the Coding Errors and different types of them with some of Security testing methods like Normalization, Stored Procedures, Code Obfuscation, Code Reuse, Dead Code, Memory Management, Third-party libraries and software development kits(SDKs), Sensitive data exposure, Fuzz testing, Code Signing.

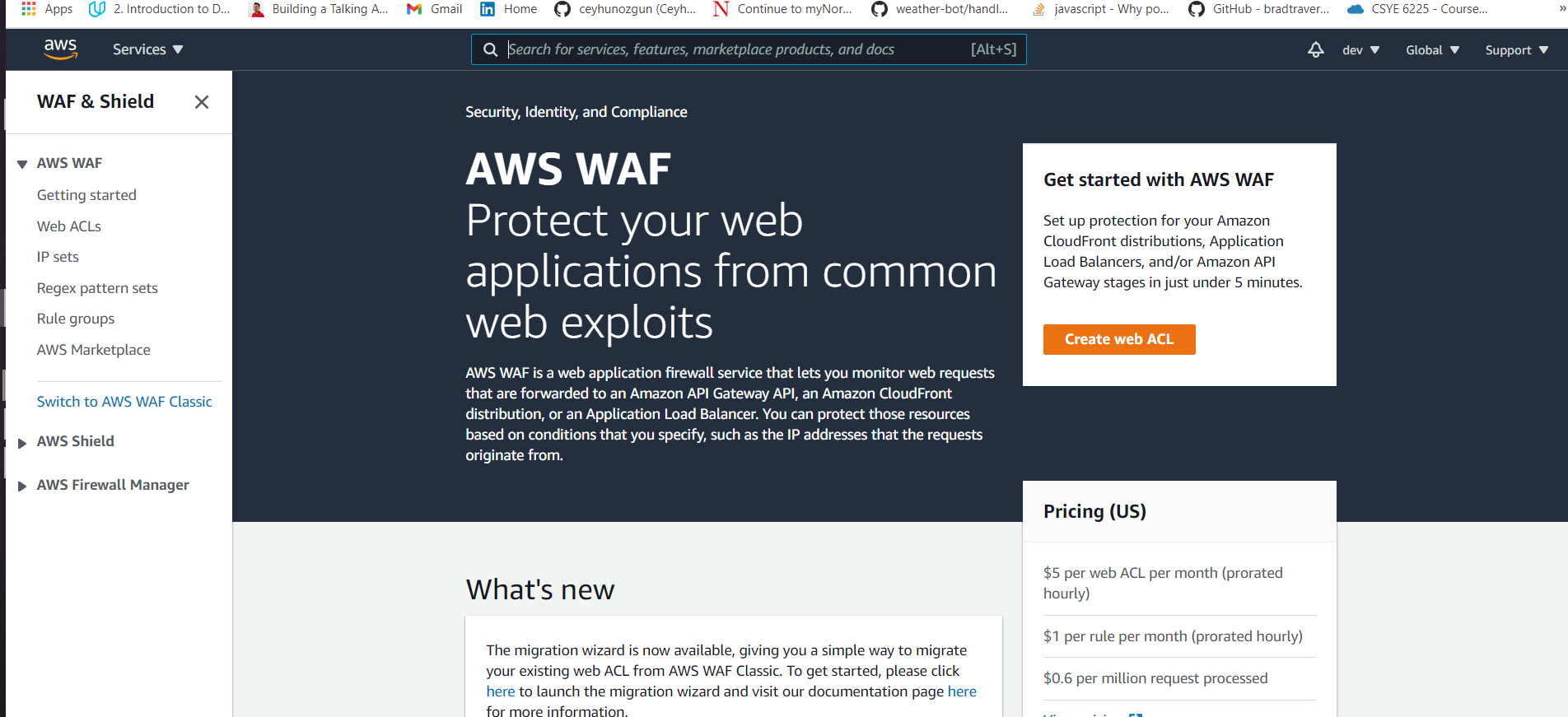
**Class Labs Screenshots:**

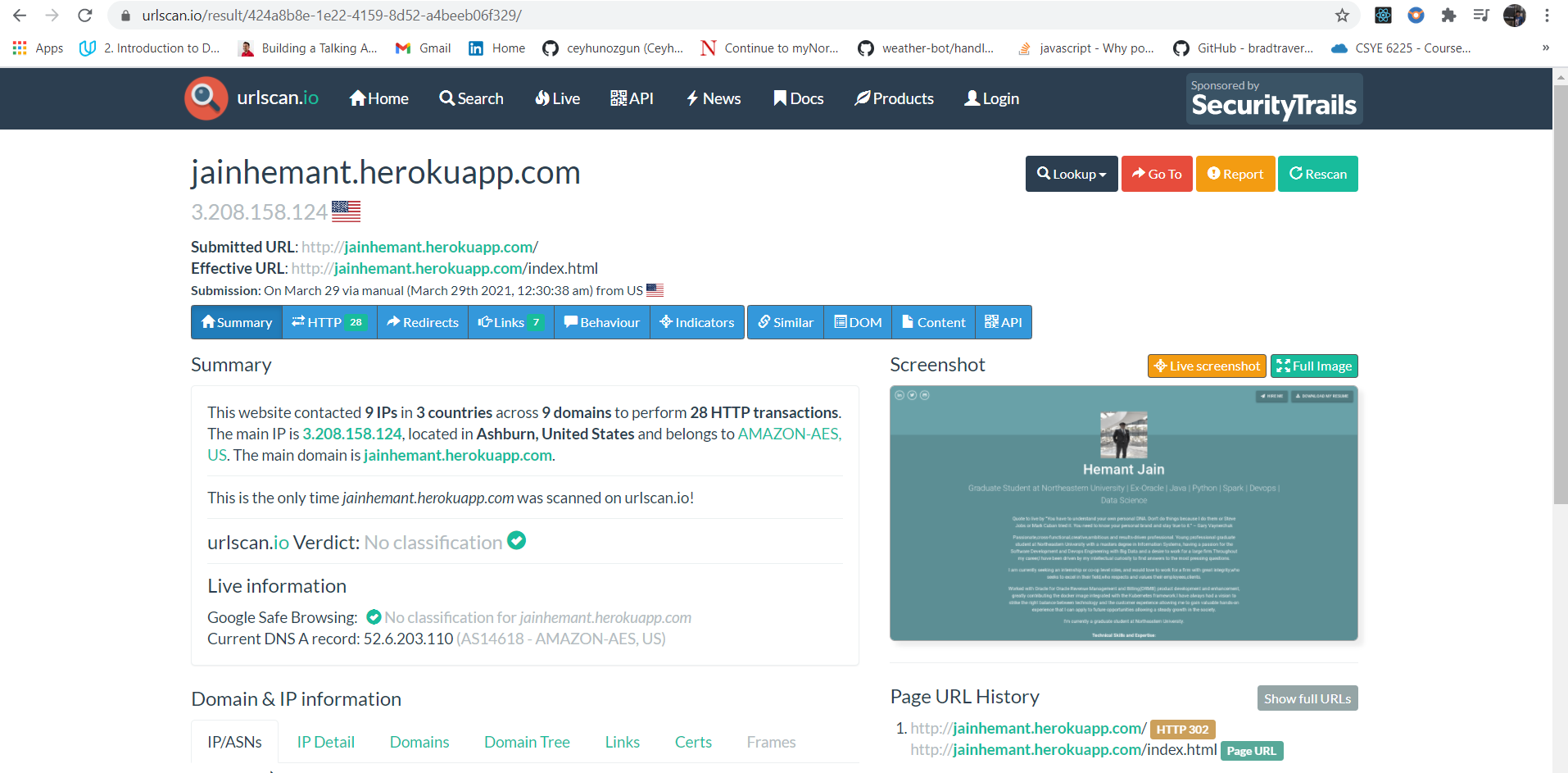
**IAM USER GROUP POLICIES:**



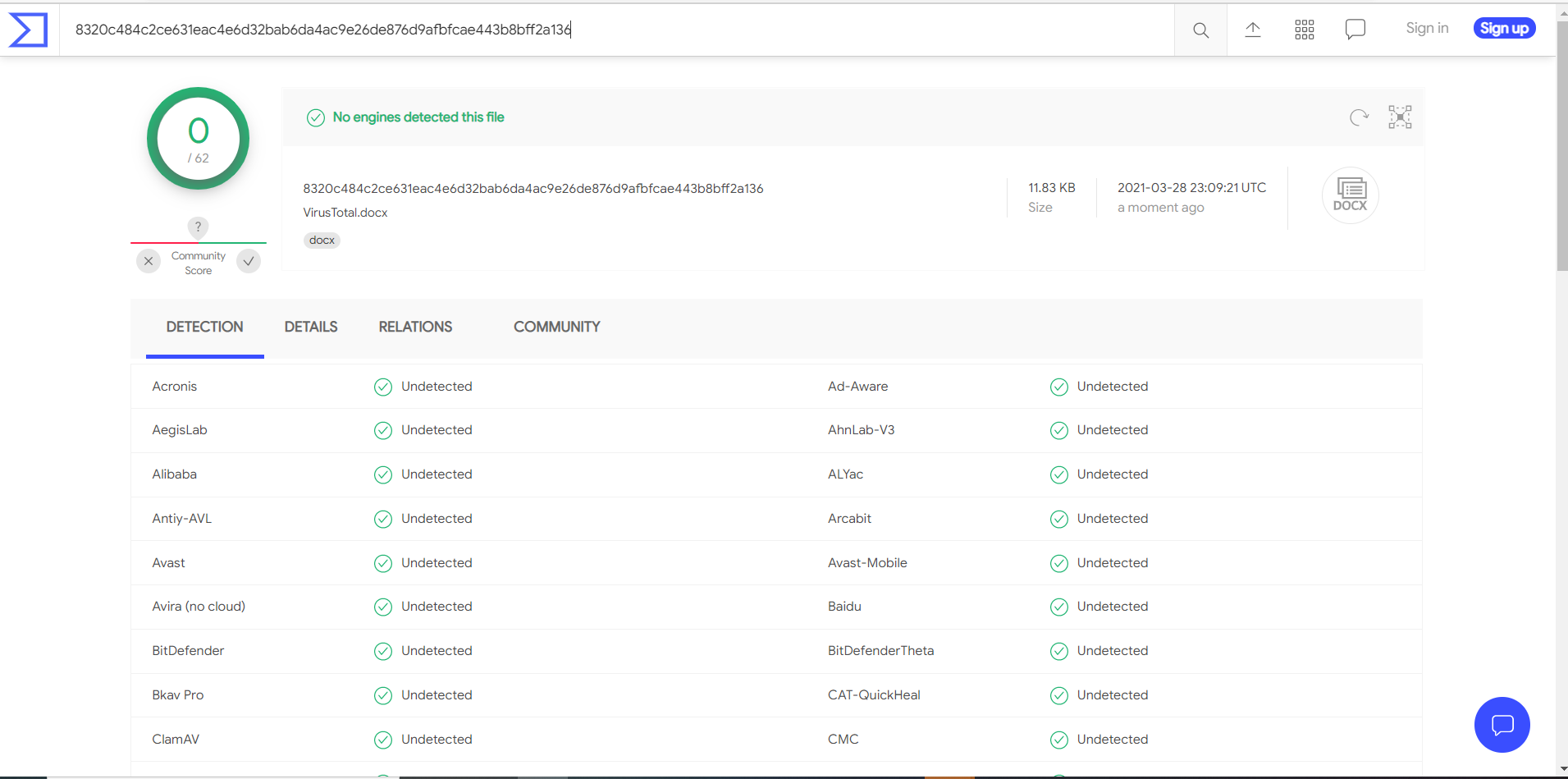


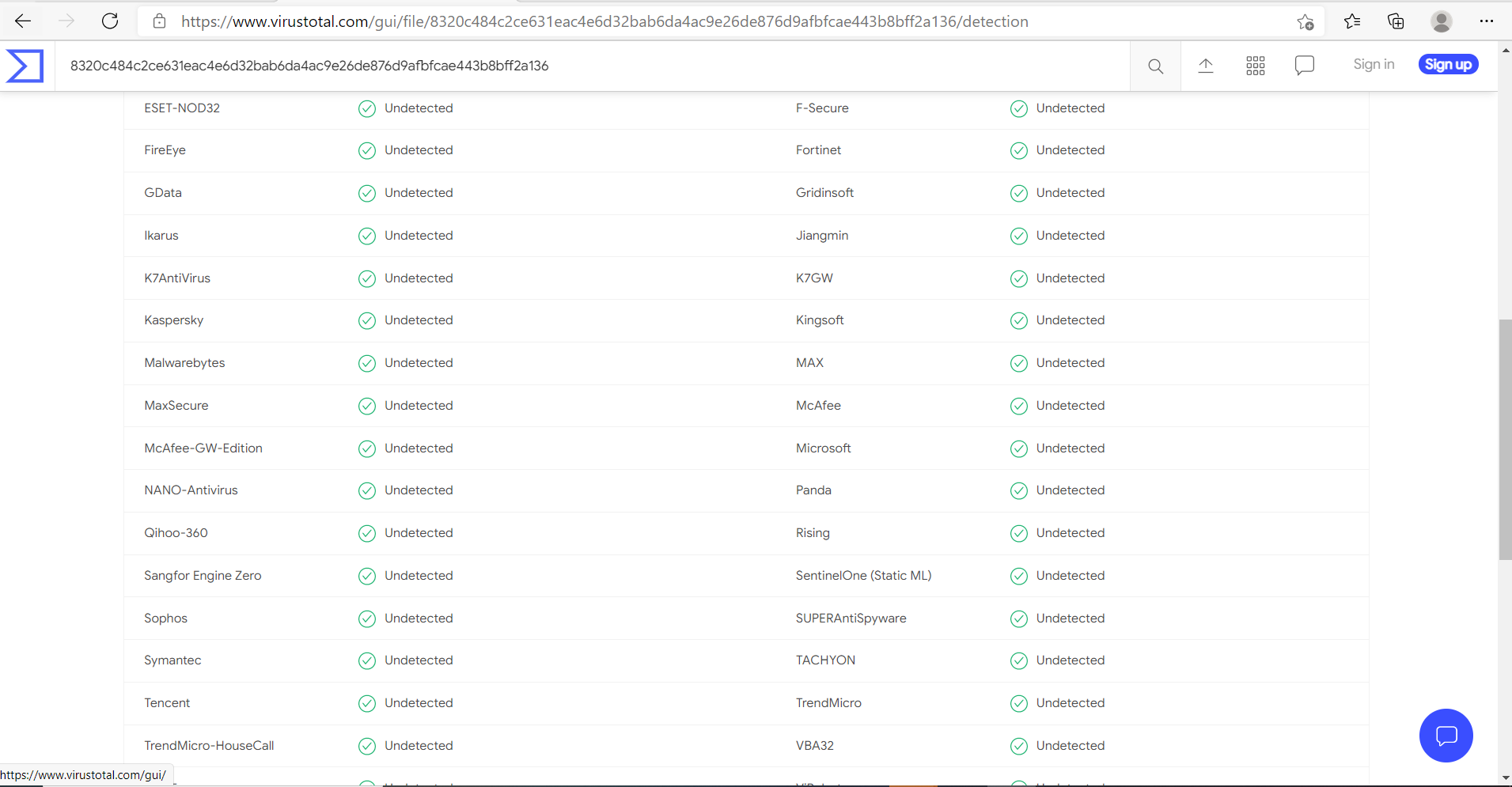


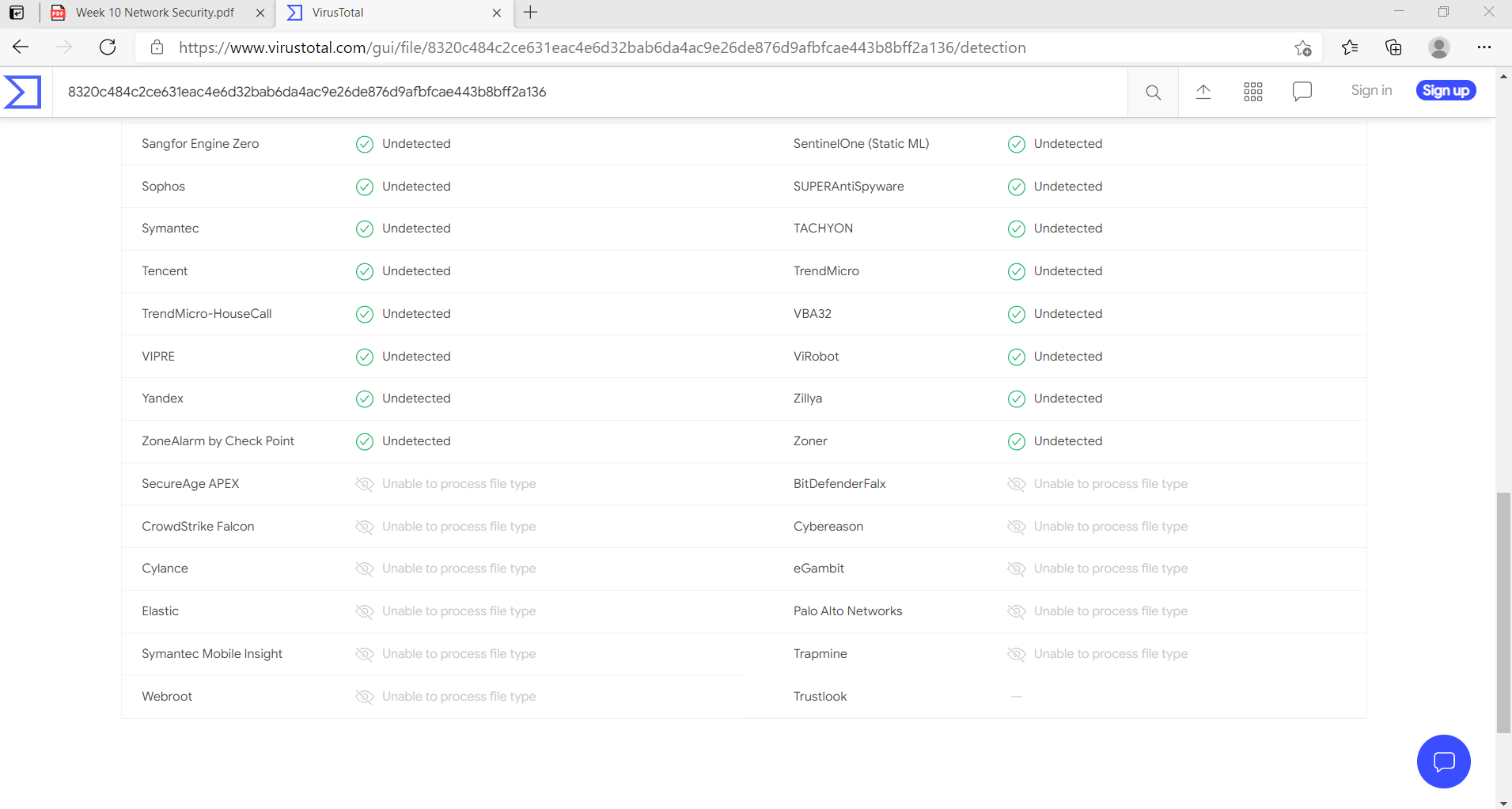




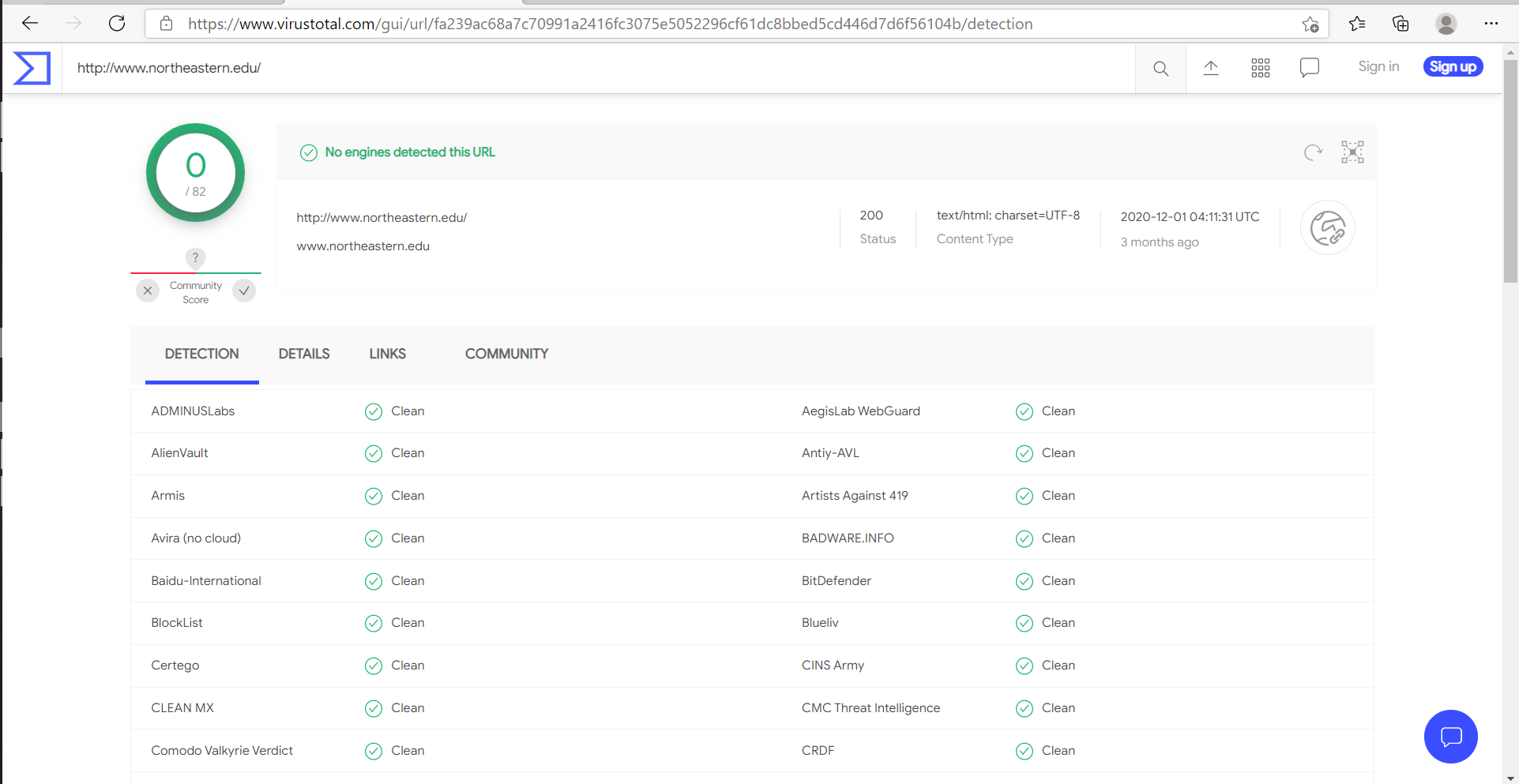
**Project 3-1: Analyze File and URL for File-Based Viruses Using VirusTotal-Part 1**

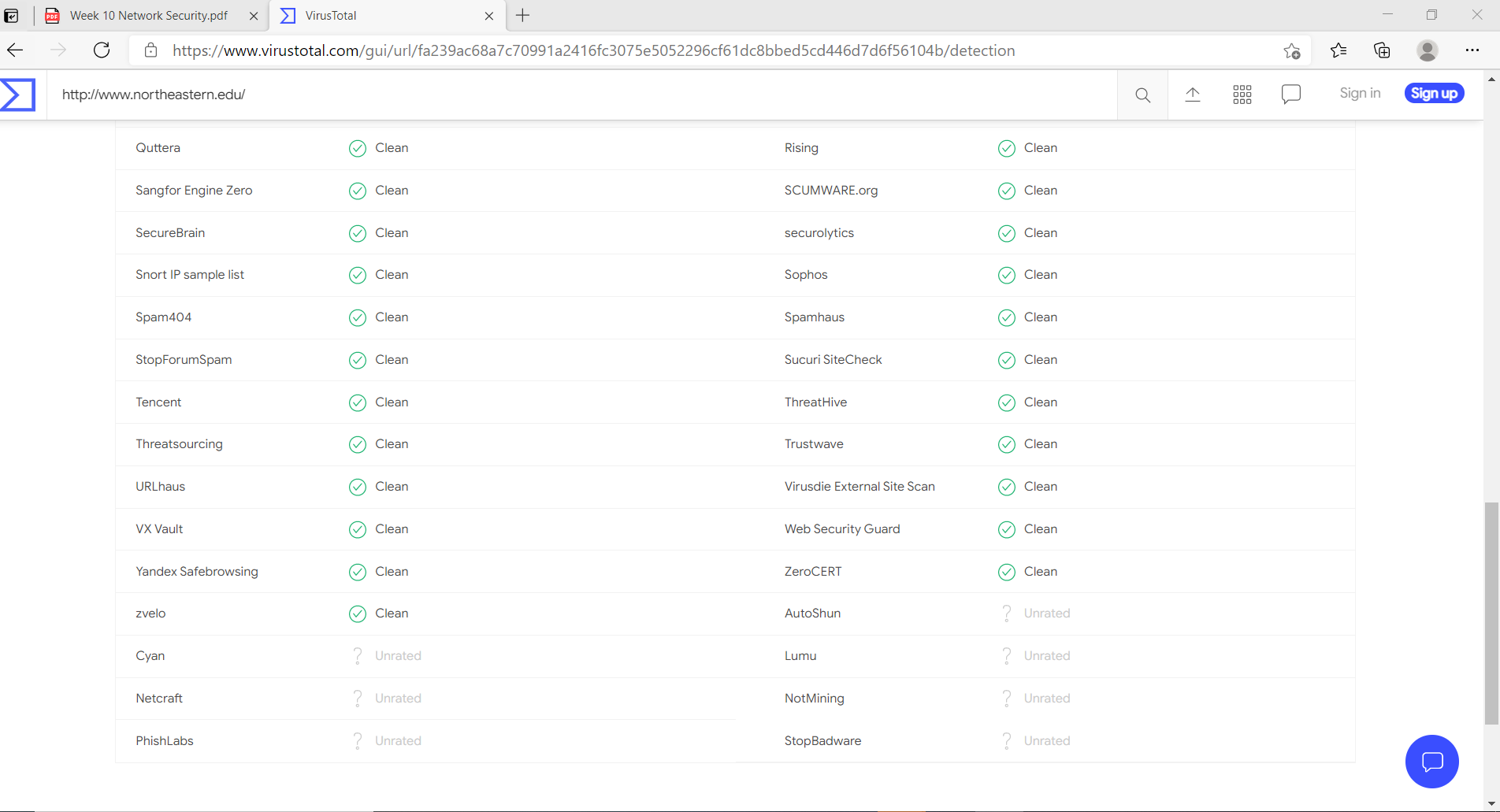






**University Website VirusTotal Screenshots:**





Que: How could VirusTotal be useful to users? How could it be useful to security researchers? Could it also be used by attackers to test their own malware before distributing it to ensure that it does not trigger an AV alert? What should be the protections against this?

Ans: VirusTotal inspects items with over 70 antivirus scanners and URL/domain blacklisting services, in addition to a myriad of tools to extract signals from the studied content. Any user can select a file from their computer using their browser and send it to VirusTotal. VirusTotal offers several file submission methods, including the primary public web interface, desktop uploaders, browser extensions and a programmatic API. The web interface has the highest scanning priority among the publicly available submission methods. Submissions may be scripted in any programming language using the HTTP-based public API.

As with files, URLs can be submitted via several different means including the VirusTotal webpage, browser extensions and the API.

Upon submitting a file or URL basic results are shared with the submitter, and between the examining partners, who use results to improve their own systems. As a result, by submitting files, URLs, domains, etc. to VirusTotal you are contributing to raise the global IT security level.

This core analysis is also the basis for several other features, including the VirusTotal Community: a network that allows users to comment on files and URLs and share notes with each other. VirusTotal can be useful in detecting malicious content and in identifying false positives -- normal and harmless items detected as malicious by one or more scanners.

VirusTotal not only tells you whether a given antivirus solution detected a submitted file as malicious, but also displays each engine's detection label (e.g., I-Worm.Allaple.gen). The same is true for URL scanners, most of which will discriminate between malware sites, phishing sites, suspicious sites, etc. Some engines will provide additional information, stating explicitly whether a given URL belongs to a particular botnet, which brand is targeted by a given phishing site, and so on.

**Project 3-2: Analyze Virus File Using VirusTotal-Part 2**

Was Popped up with the error and was unable to get it inside the Windows Sandbox.

But overall, I understood the concept and looks quite like the above practical inside of uploading the VirusTotal.docx file we were uploading the eicar.com file.

Performed the lab on the SEED Ubuntu machine on the VirtualBox:

Graphical user interface, application

Description automatically generated

**Project 3-3: Explore Ransomware Sites**

**Que:** Read through the Prevention Advice. Do you think it is helpful?

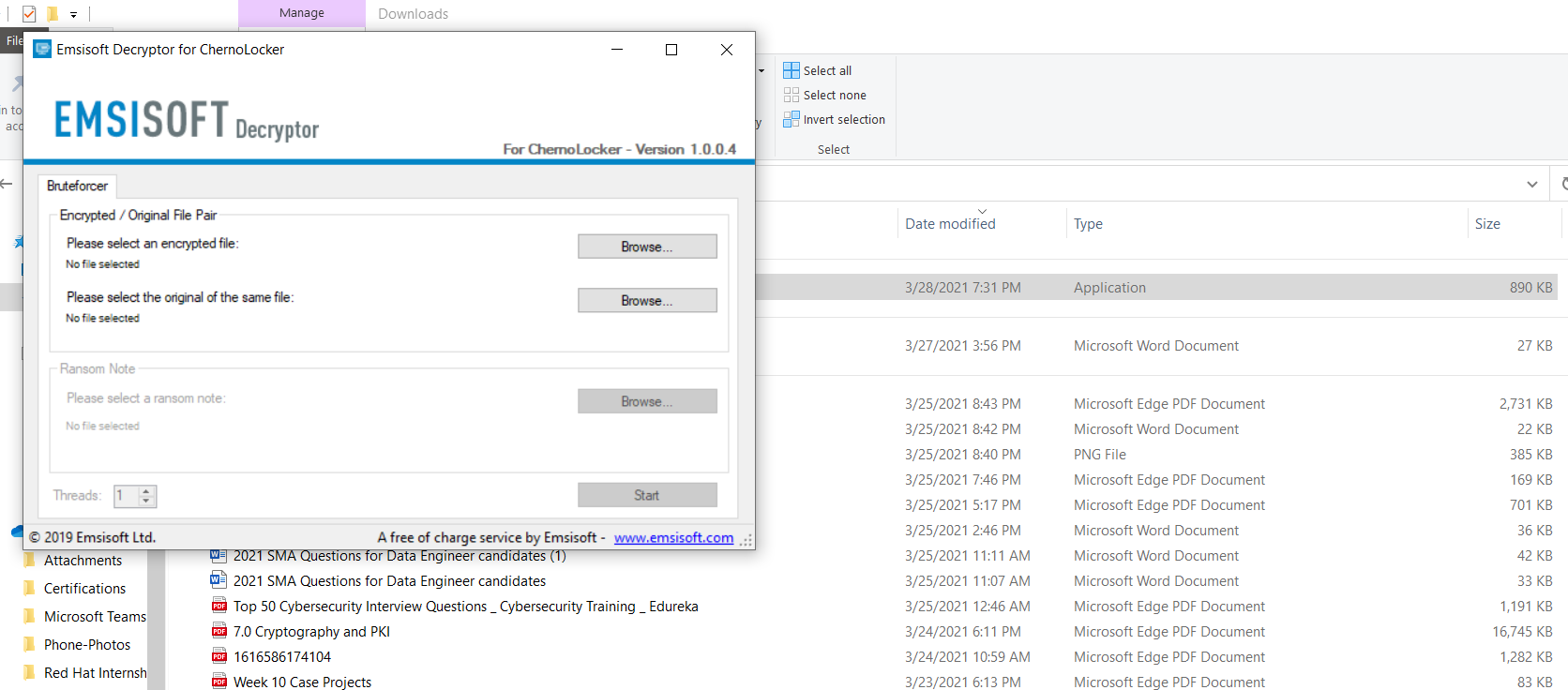
Ans: Yes, it was helpful to get some basic information needed to prevent the ransom attacks like creating Back-up, enabling antivirus software, and updating system software etc.

**Que:** Click Crypto Sheriff. How could this be useful to a user who has suffered a ransomware infection?

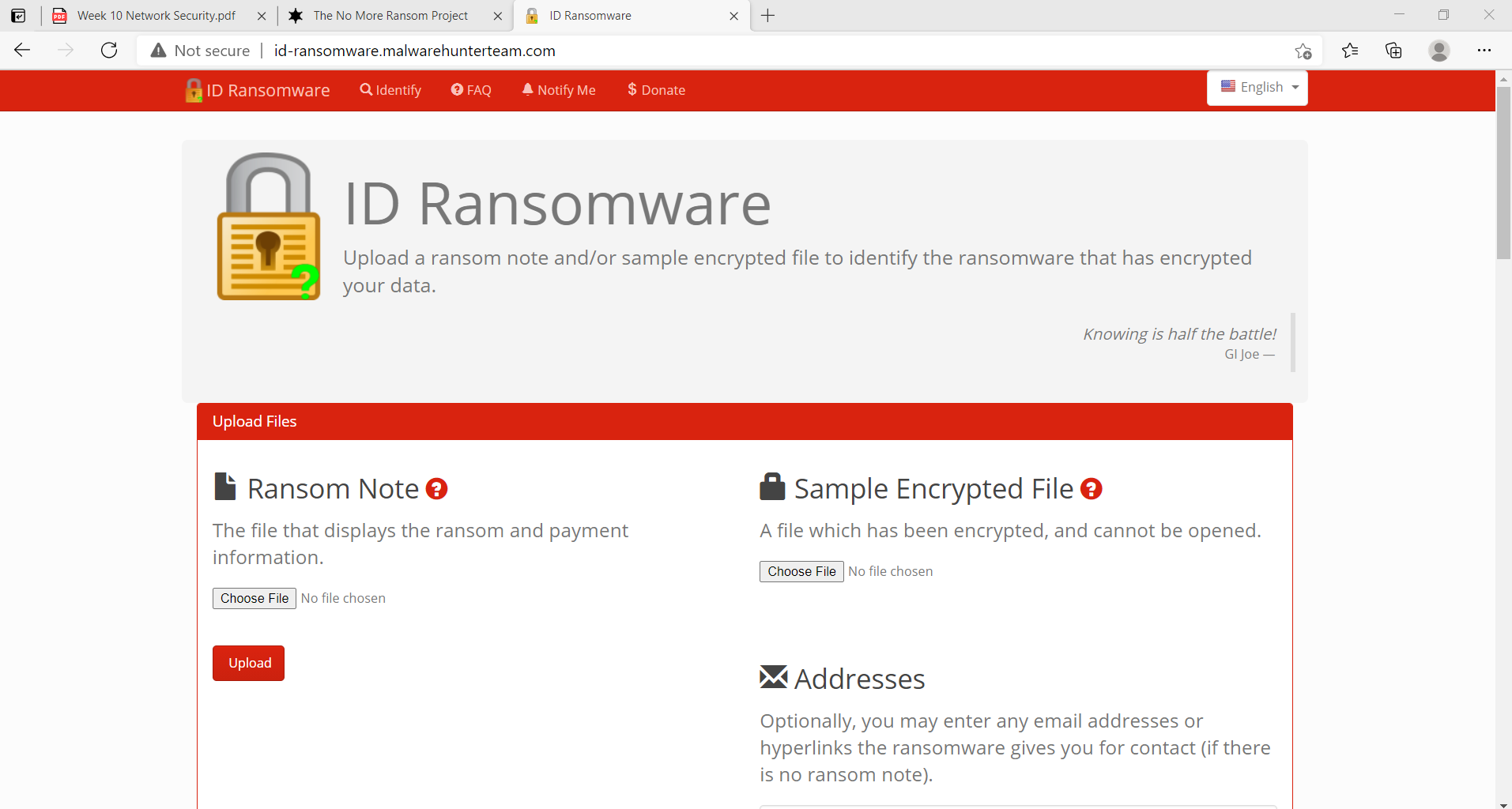
Ans: To help us define the type of ransomware affecting your device, please fill in the form below. This will enable us to check whether there is a solution available. If there is, we will provide you with the link to download the decryption solution.

**Que:** Click Ransomware: Q&A. Read through the information. Which statements would you agree with? Which statements would you disagree with?

Ans: Agree with all statements.



[ID Ransomware (malwarehunterteam.com)](http://id-ransomware.malwarehunterteam.com/)



**Que:** What features does this site provide?

Ans: ID Ransomware is, and always will be, a free service to the public. It is currently a personal project that I have created to help guide victims to reliable information on a ransomware that may have infected their system. Other than direct development and signature additions to the website itself, it is an overall community effort.

**Que: How could the website like ID Ransomware be useful?**

Ans:Everyone can be the target of a ransomware attack. It doesn't discriminate whether you are rich or poor, for as long as your computer is not secured, you can be infected by ransomware. Each one must learn how to identify ransomware in order to know what to do in case you encounter an attack.

Ransomware can be dangerous if it is on your computer. Simply because it locks your computer and sometimes it encrypts your data. You will know that you have been infected when there is a ransom message on your screens. Then it demands you to pay a certain amount, typically in the form of cryptocurrency.

ID ransomware behavior is silent but deadly. It has many ways on how it could enter your computer. If you do not know how to identify ransomware and how it acts, it would be difficult for you to make a solution to the problem it created.

**File Encryption**

One simple way on identify ransomware on your computer is when the file got encrypted. Ransomware has the capability of encrypting all kind of files. It includes photos, videos, office documents and many else.

**File Renaming**

When an id ransomware gets into your computer, it renames your data. This is a better way of identifying ransomware on your computer. This is typical behavior of a ransomware to create confusion on which file is affected.

**File Extension Alteration**

To help you on how to identify ransomware, you can check the extension file of your data. If the extensions were altered and became an unknown character, there is a big possibility of a ransomware infection on your computer.

**Ransom Note on the Screen**

Usually, you will never know when a ransomware gets inside to your computer. It will secretly do what it needs to do, and when it is finished, that is the time it will reveal itself. A good way to know identify ransomware is when you see a ransom message flashed to your screen. It demands you to pay a ransom fee for a certain period. If you fail to pay the criminals, all your files will be deleted.

**Turn your Computer into Botnets**

One of the things that may happen to your computer when you have been infected by a ransomware is to become a bot in a botnet. Although it would be difficult for you how to identify ransomware on your computer if it became a botnet. You will just notice that your PC is running slow and keeps on hanging most of the time.

**Spread in the Network**

Another common way on how to identify Ransomware is when your neighboring computers also gets infected. It is because ransomware can spread the infection into your local network. So, if you are infected, all the computer connected to your network will also be infected by the ransomware.

**Data extraction**

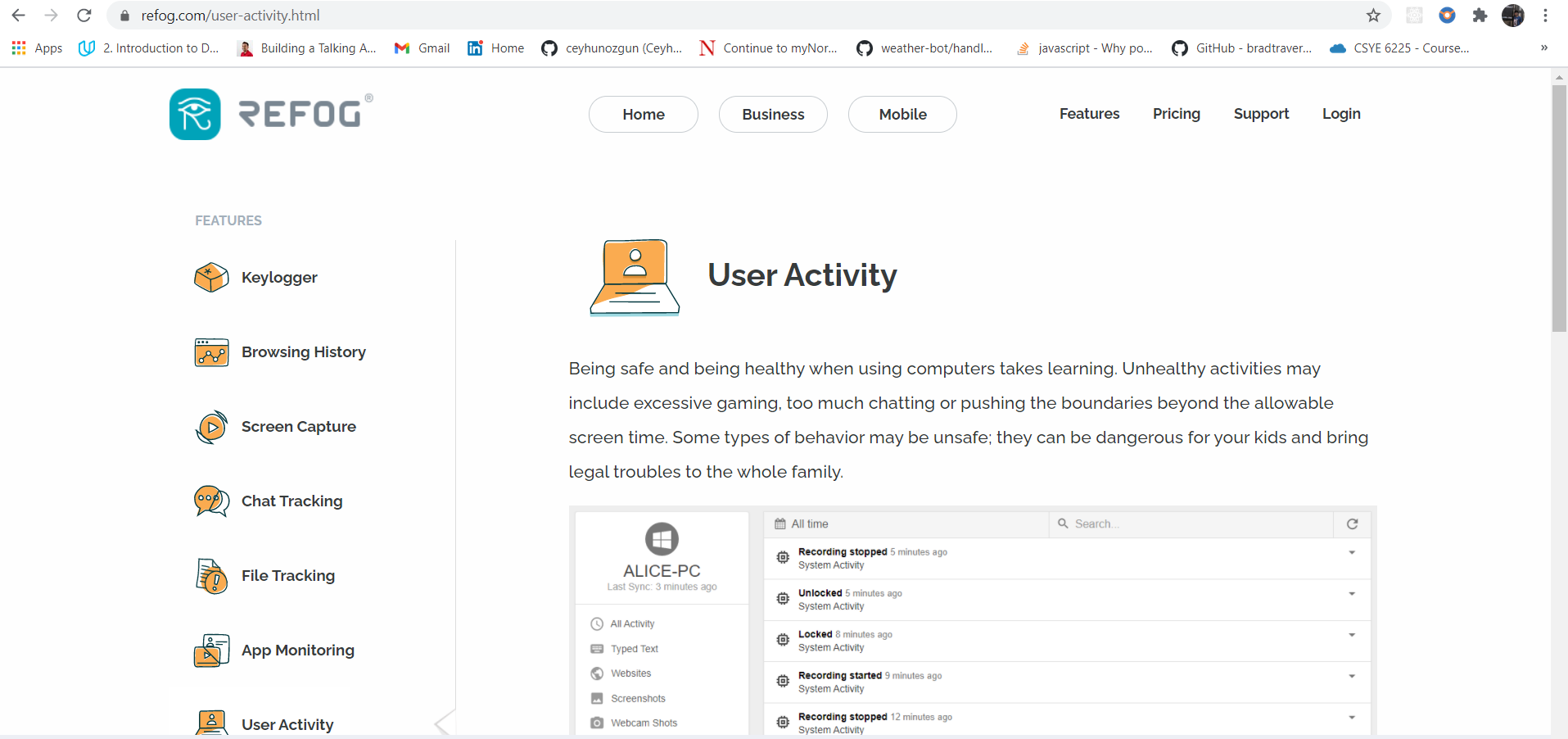
The last option on how to identify ransomware is data extraction. Although this also happens in the background and would be hard to recognize. Once it has extracted your files, you will never know what it will do next. It could upload your file to criminal's server or encrypt them all.

**Sources of Ransomware**

There are many sources on how to identify ransomware on your computer. One typical way is when you visited a compromised website. If the website is infected by a ransomware and you accidentally visited the site, the ransomware script could be transferred to your computer.

Another way is via spam emails. When you received an email coming from an unknown sender and you open the email and click any link that is on that email. There is a big chance of getting infected by a ransomware. The spam emails might also include a malicious attachment that could be carrying a script. If you happen to open the attachments, the malicious script may run to your computer and infect yours with the ransomware.

**Project 3-4: Use a Software Keylogger**



Performed all the key steps and uninstalled the tool immediately.

**Progress Embedded Image of Progress Report from LabSim:**

