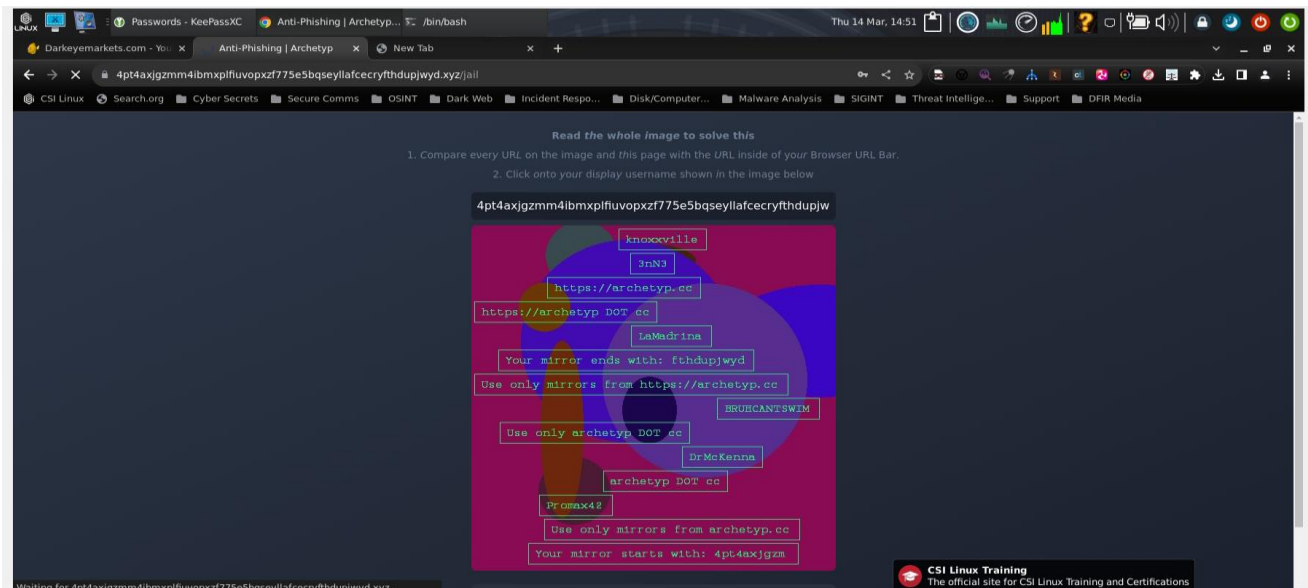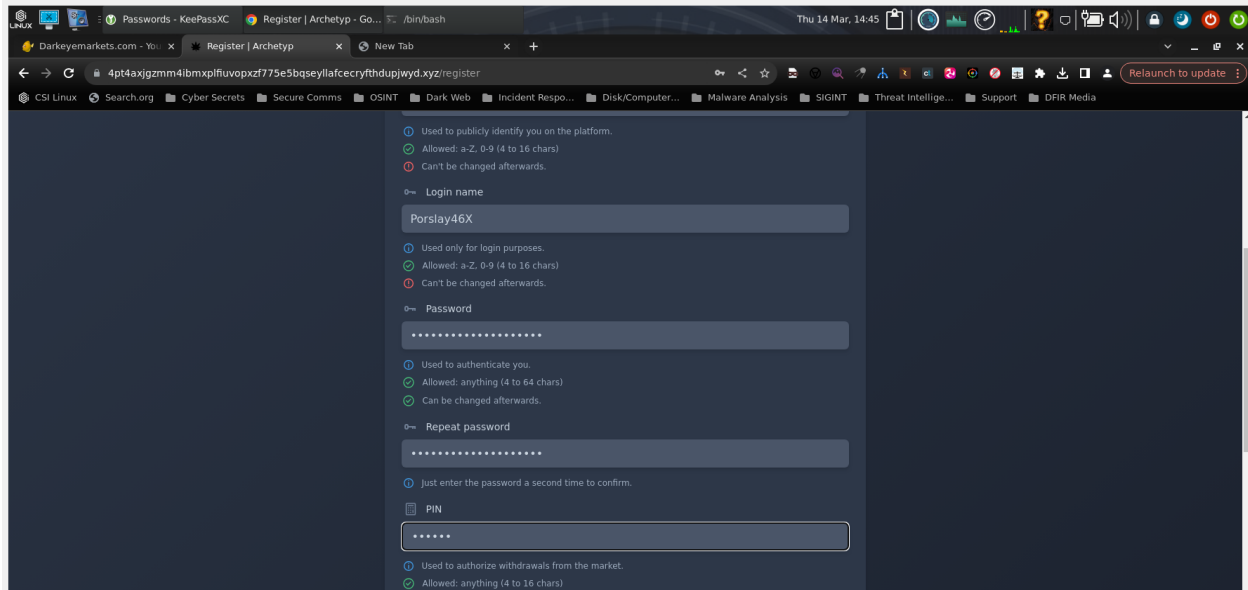# Dark web Exploration Report

The dark web contains many anonymous networks and systems that host illegal and legal content. Due to the anonymity it offers, it stands out as an area where illegal content is abundant and where careful action should be taken. The main pillar here is anonymity, and many different technologies and systems are used to ensure anonymity. The most popular of these technologies is the Onion routing protocol.

The Onion routing protocol divides and encrypts the packets leaving the user and sends them to random servers in the first layer. These servers then decrypt the packets to determine their destinations and send them to the second layer without any IP address information, using an ID that Tor servers can understand. The server in the second layer finally sends them to the exit point in the third layer. Here the packets are combined, decrypted and sent to the destination server. The information from the destination server is then delivered to the user in the opposite direction. The second and third of these layers are randomly determined for each site and change after a certain period of time. Sites with the '.onion' extension can be accessed through this technology. Sites with the '.onion' extension are sites that publish themselves over the onion protocol on condition that they remain anonymous. In this way, anonymity can be achieved up to a point.

One of the striking features of dark web sites is that their links change frequently. With this method, sites can make themselves more hidden. Blockchain-based cryptocurrency systems are used as payment systems. In addition, there are security measures that verify the real personality, especially on trading sites. Sites that take themselves seriously here take strict measures against DDoS attacks.

Due to the risks on the dark web, using onion routing technology alone is not enough. Web browser settings are extremely important. Wrong settings can almost completely expose your identity. For this reason, great care should be taken when adjusting your settings, such as cookie management, tracking blockers, and allowed technologies. You should also pay attention to the security settings of the device you use when logging into this network. Security should be ensured with extra measures such as virtualization, automatic cookie cleaning, disk encryption. When these measures are not paid enough attention, it is inevitable to fall into the hands of malicious people on these networks.

While there are many illegal activities on the dark web, most of the systems are full of deceptive traps such as fraud and identity theft. While surfing the dark web, one can encounter criminals, intelligence officers, security forces, terrorists, scammers, hackers and normal users. In addition to its legal aspects, the dark web is also known to be used by journalists and individuals to ensure their privacy.

In conclusion, the dark web is a deep sea with many dangers. When diving into this sea, it is vital to be sensitive to safety precautions and to act consciously. In this diving adventure, you are faced with a wide range of legal and illegal content. For this reason, you need to act in accordance with ethical principles and know what you are doing.