Security Threats:

* **DDOS attack:**

A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. They target a wide variety of important resources, from banks to news websites, and present a major challenge to making sure people can publish and access important information.

More **than 2000 daily DDoS** Attacks are observed worldwide by Arbor Network,   
**one of three (1/3)** of all downtime incidents are attributed to DDOS attacks.

* **Injections**

Injection flaws, such as SQL, NoSQL, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

* **Broken Authentication:**

Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

* **Sensitive Data Exposure:**

Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

* **Cross-site Scripting:**

Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

Security Solutions:

* **Two-factor authentication:**

Two-factor authentication adds a second level of authentication to an account log-in. When you have to enter only your username and one password, that's considered a single-factor authentication. 2FA requires the user to have two out of three types of credentials before being able to access an account. The three types are:

·         Something you know, such as a personal identification number (PIN), password

or a pattern

·         Something you have, such as an ATM card, phone.

·         Something you are, such as a biometric like a fingerprint or voice

·         Something that is generated, such as pseudo-random number

* **Web application filter:**

A web application firewall (WAF) is an [application firewall](https://en.wikipedia.org/wiki/Application_firewall) for HTTP applications. It applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as [cross-site scripting (XSS)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)) and [SQL injection](https://www.owasp.org/index.php/SQL_Injection).