What threats would act on (exploit) the following vulnerabilities:

Vulnerabilities	Threats
Zero-Day Vulnerability	
Poor Data Sanitization	
Unpatched Software	
Poorly managed Access permissions	
Misconfiguration	
Vulnerable APIs	
Single factor Authentication	
Exploitable & Unaware Personnel	

Vulnerabilities

1. **Zero-Day Vulnerability:** A zero-day vulnerability is one that is discovered by cybercriminals and exploited before a patch is available.
2. **Poor Data Sanitization:** A failure to properly validate data before processing that leaves applications vulnerable to attack.
3. **Unpatched Software:** A failure to properly patch out-of-date software leaves it vulnerable to exploitation.
4. **Poorly managed Access permissions:** Assigning employees and contractors more access and privileges than they need. These additional permissions create security risks if an employee abuses their access or their account is compromised by an attacker.
5. **Misconfiguration:** A failure to configure applications securely is a common problem, especially in cloud environments.
6. **Vulnerable APIs:** APIs properly secured against unauthorized access or exploitation.
7. **Single factor Authentication:** Using only one method to authenticate users. An attacker with access to a legitimate user's credentials can easily gain access to an organization and its systems.
8. **Exploitable & Unaware Personnel:** Some members of staff that have certain financial problems or are unaware of cybersecurity hygiene may be targeted and exploited

Threats

1. **Malware:** Malicious software is any program or code that is created with the intent to do harm to a computer, network or server. Malware is the most common type of cyberattack, mostly because this term encompasses many subsets such as ransomware, trojans, spyware, viruses, worms, keyloggers etc

2. **Denial-of-Service (DoS):** a malicious, targeted attack that floods a network with false requests in order to disrupt business operations. This results in legitimate users being unable to perform routine and necessary tasks, such as accessing email, websites, online accounts or other resources that are operated by a compromised computer or network.
3. **Phishing:** A type of cyberattack that uses email, SMS, phone, social media, and social engineering techniques to entice a victim to share sensitive information — such as passwords or account numbers — or to download a malicious file that will install viruses on their computer or phone.
4. **Spoofing:** Spoofing is a technique through which a cybercriminal disguises themselves as a known or trusted source. In so doing, the adversary is able to engage with the target and access their systems or devices with the ultimate goal of stealing information, extorting money or installing malware or other harmful software on the device.
5. **Identity-Based Attacks:** When a valid user's credentials have been compromised and an adversary is masquerading as that user, it is often very difficult to differentiate between the user's typical behavior and that of the hacker
6. **Code Injection:** Code injection attacks consist of an attacker injecting malicious code into a vulnerable computer or network to change its course of action.
7. **Insider Threat:** Compromised members of staff that
8. **Zero-day attack:** Any attack to a system or software, usually discovered first by cybercriminals and exploited before a patch was made available.