There are a set of sources that provide updated information about security vulnerabilities:

- CVE, Common Vulnerabilities and Exposures
- CWE, Common Weakness Enumeration
- CAPEC, Common Attack Pattern Enumeration and Classification
- ...
CVE is a list of entries—each containing an identification number, a description, and at least one public reference—for **publicly known cybersecurity vulnerabilities**.

CVE Entries are used in numerous cybersecurity products and services from around the world, including the U.S. National Vulnerability Database (NVD).

https://cve.mitre.org/
CWE

- CWE is a community-developed list of common software security weaknesses. It serves as a common language, a measuring stick for software security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.
https://cwe.mitre.org/

CWE - XSS

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Description

The software does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.

Extended Description

Cross-site scripting (XSS) vulnerabilities occur when:

1. Untrusted data enters a web application, typically from a web request.
2. The web application dynamically generates a web page that contains this untrusted data.
3. During page generation, the application does not prevent the data from containing content that is executable by a web browser, such as JavaScript, HTML tags, HTML attributes, mouse events, Flash, ActiveX, etc.
4. A victim visits the generated web page through a web browser, which contains malicious script that was injected using the untrusted data.
5. The malicious script is executed in the context of the web server's domain.
6. The script effectively violates the origin policy, which states that scripts in one domain should not be able to access resources or run code in a different domain.

There are three main kinds of XSS:

- **Type 1: Reflected XSS (or Non-Persistent)** - The server reads data directly from the HTTP request and reflects it back in the HTTP response. Reflected XSS exploits occur when an attacker causes a victim to supply dangerous content to a vulnerable web application, which is then reflected back to the victim and executed by the web browser. The most common mechanism for delivering malicious content is to include it as a parameter in a URL that is posted publicly or e-mailed directly to the victim. URLs constructed in this manner constitute the core of many phishing schemes, whereby an attacker convinces a victim to visit a URL that refers to a vulnerable site. After the site reflects the attacker's content back to the victim,
CAPEC – Common Attack Pattern Enumeration and Classification

- CAPEC helps by providing a comprehensive dictionary of known patterns of attack employed by adversaries to exploit known weaknesses in cyber-enabled capabilities.
- Understanding how the adversary operates is essential to effective cyber security.
- It can be used by analysts, developers, testers, and educators to advance community understanding and enhance defenses.

https://capec.mitre.org/
NIST - National Vulnerabilities Database (VND)

- Collects and classifies the CVE vulnerabilities
- CVEs are related with CWEs and with the products (CPE)
- Metrics are defined to measure the vulnerability dangerousness,
  - each vulnerability is classified in different aspects, see CVSS calculators
    - https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator
- provides machine readable JSON data of vulnerabilities description

NVD - dashboard
www.cvedetails.com provides an easy to use web interface to CVE vulnerability data. You can browse for vendors, products and versions and view CVE entries, vulnerabilities, related to them. You can view statistics about vendors, products and versions of products. CVE vulnerability data are taken from National Vulnerability Database (NVD) XML feeds provided by NIST. Additional data from several sources like exploits from www.exploit-db.com, vendor statements and additional vendor supplied data, Metasploit modules are also published in addition to NVD CVE data. Vulnerabilities are classified by cvedetails.com using keyword matching and CWE numbers if possible, but they are mostly based on keywords. Unless otherwise stated CVSS scores listed on this site are "CVSS Base Scores" provided in NVD feeds. Vulnerability data are updated daily using NVD feeds.
Which are the security measures to be taken when handling payments?  
credit cards information are a very sensitive personal data  
There are some guidelines to be followed  
For example on OWASP  