Overview of the Assignment : To find any 10 vulnerabilities of the main website that you have chosen.

Main website : https://www.orchidhomez.com/

1. **Vulnerability name :** Anti-clickjacking X-Frames-Option header is not present
   CWE : CWE-693
   OWASP Category : A6: Security Misconfiguration

   Description : Security misconfiguration is a prevalent web application security risk that occurs when a web application, its server, or associated components are not securely configured. This occurs often due to oversight or a lack of awareness about best practices.

   Business Impact : The absence of protection against clickjacking in a business can have severe consequences. It can lead to fraudulent actions, data breaches, damage to the organization's reputation, potential legal and compliance issues, financial losses, operational disruptions, and the loss of valuable customers. Implementing anti-clickjacking measures is crucial to mitigate these risks and safeguard the business's integrity and success.

2. **Vulnerability name :** X-Content-Type-Options header is not set
   CWE : CWE-16
   OWASP Category : A6: Security Misconfiguration

   Description : In this case, a missing or misconfigured "X-Content-Type-Options" header represents a security misconfiguration that can expose the application to certain risks, including MIME-sniffing attacks. Properly configuring this header is crucial for mitigating such risks.

   Business Impact : The absence of the "X-Content-Type-Options" header, indicative of security misconfigurations, can lead to severe business consequences, including vulnerabilities, data breaches, reputational damage, legal and compliance issues, operational disruptions, and customer attrition, posing a substantial threat to the overall security and success of the organization.

3. **Vulnerability name :** Strict-Transport-Security HTTP Header is not defined
   CWE : CWE-319
   OWASP Category : A3: Cross-Site Scripting (XSS)

   Description : Cross-Site Scripting (XSS) is a prevalent web application security risk where attackers inject malicious scripts into web pages viewed by other users. This can occur when web applications fail to properly validate and sanitize user-provided data or when they don't implement adequate security controls to protect against script injection.

Business Impact : The absence of a properly defined "Strict-Transport-Security" (HSTS) HTTP header can have significant implications for a web application. It can introduce security vulnerabilities, leaving the application susceptible to SSL-stripping and data exposure. Such vulnerabilities can erode user trust and harm the reputation of the website, potentially leading to operational disruptions, additional costs, and financial consequences, including potential legal liabilities.

4. **Vulnerability name :** SSH Weak Algorithms Supported
   CWE : CWE-326
   OWASP Category : A3: Cross-Site Scripting (XSS) (Indirectly)

   Description : XSS is a web application security vulnerability where attackers inject malicious scripts into web pages that are then executed by other users. These scripts can steal user data, session tokens, or perform other malicious actions within the context of the victim's browser.

   Business Impact : If encryption strength is weak, sensitive data exchanged between the client and server might be more easily intercepted and exposed in an XSS attack. An attacker who successfully exploits an XSS vulnerability could potentially target weak encryption to further compromise the confidentiality and integrity of data.This can result in data breaches, exposing sensitive information and leading to legal liabilities and fines. Such security incidents can damage a company's reputation, erode trust, and disrupt operations, causing downtime and additional costs.

5. **Vulnerability name :** Apache Server ETag Header Information Disclosure
   CWE : CWE-200
   OWASP Category : A6: Security Misconfiguration

   Description : The disclosure of sensitive information through the ETag header can be attributed to security misconfiguration, as it can expose server details or file structure information unintentionally. Proper configuration of server headers is essential to prevent such information disclosure vulnerabilities

   Business Impact : It can damage the organization's reputation, eroding trust among customers, partners, and users who may be concerned about the security of their data. Additionally, the competitive disadvantage may arise as customers seek more secure alternatives due to the security incidents. Attackers can exploit the disclosed information to plan targeted attacks, increasing the risk of further security incidents.

6. **Vulnerability name :** SMTP Service Cleartext Login Permitted
   CWE : CWE-319
   OWASP Category : A6: Security Misconfiguration

Description : This category addresses issues related to improper or insecure configurations in web applications, which can include misconfigurations of server services and security settings. Allowing cleartext login for SMTP is a security misconfiguration because it exposes sensitive authentication information to potential interception.

Business Impact : Permitting cleartext login for SMTP (Simple Mail Transfer Protocol) services can have significant implications. Cleartext login means that sensitive data, including usernames and passwords, is transmitted without encryption, leaving it vulnerable to interception. This poses several risks, including potential unauthorized access to email accounts, data breaches, and the loss of user trust due to security incidents. Legal and compliance issues may also arise, leading to potential fines and liabilities.

7. **Vulnerability name :** HTTP Methods Allowed (per directory)
   CWE : CWE-285
   OWASP Category : A5: Broken Access Control

   Description : Broken Access Control refers to vulnerabilities and misconfigurations in web applications where access controls are not effectively enforced. This means that users may be able to access functionalities, data, or perform actions they should not have permission to.

   Business Impact : Allowing inappropriate HTTP methods in a directory may result in unauthorized access, potentially enabling users to perform actions they shouldn't have permission for. Moreover, it can lead to data exposure, risking sensitive information and privacy violations. In cases where write operations like "DELETE" or "PUT" are improperly allowed, data manipulation or deletion by unauthorized users becomes a concern, potentially leading to data loss or tampering.

8. **Vulnerability name :** SSH server CBC mode ciphers enabled
   CWE : CWE-310
   OWASP Category : A6: Security Misconfiguration

   Description : Enabling weak or deprecated Cipher Block Chaining (CBC) mode ciphers in your SSH server configuration can be considered a security misconfiguration. This misconfiguration may result in significant security vulnerabilities and potential risks to your system.

   Business Impact : Enabling weak or deprecated CBC ciphers introduces notable security risks. Such vulnerabilities can be exploited by malicious actors, potentially leading to unauthorized access, data breaches, and significant financial losses. These incidents can also tarnish the organization's reputation, affecting its standing in the eyes of customers and stakeholders.