Selected Vulnerabilities Report

# **Executive Summary**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **S. No** | **Affected Asset i.e. IP/URL/Application etc** | **Observation/ Vulnerability title** | **CVE/CWE** | **Control Objective #** | **Control Name #** | **Audit Requirement #** | **Severity** | **Recommendation** | **Reference** | **New or Repeat observation** |
| 1 | http://10.236.150.124:8000/questions.html | Server Information Disclosure | CVE-2023-29012 / CWE-200 | N/A | N/A | N/A | medium | 1. Configure servers to suppress detailed error messages and limit the information disclosed in HTTP headers. 2. Regularly review and update server configurations to minimize information leakage. 3. Implement security best practices for server hardening. 4. Conduct regular security audits to identify and address information disclosure issues. | https://cwe.mitre.org/data/definitions/200.html | New |
| 2 | http://10.236.150.124:8000/questions.html | Security Headers Missing | CVE-2023-30123 / CWE-16 | N/A | N/A | N/A | medium | 1. Implement and configure all recommended security headers in web applications. 2. Regularly review and update security header configurations to align with best practices. 3. Use automated tools to scan for missing or misconfigured security headers. 4. Conduct regular security audits to ensure compliance with security header policies. | https://cwe.mitre.org/data/definitions/16.html | New |
| 3 | http://10.236.150.124:8000/questions.html | Clickjacking | CVE-2023-36789 / CWE-1021 | N/A | N/A | N/A | low | 1. Implement frame busting techniques to prevent your website from being embedded in iframes. 2. Use the X-Frame-Options HTTP header to restrict framing of your web pages. 3. Conduct regular security testing to identify and address clickjacking vulnerabilities. 4. Educate users about the risks of clickjacking and how to recognize suspicious behavior. | https://cwe.mitre.org/data/definitions/1021.html | New |

# **Vulnerability: Server Information Disclosure**

|  |  |
| --- | --- |
| **Affected Asset:**  http://10.236.150.124:8000/questions.html |  |
| **Vulnerability Title:**  Server Information Disclosure |  |
| **Business Impact:**  Server Information Disclosure can expose sensitive details about the server configuration, software versions, and internal structure. This information can be used by attackers to plan targeted attacks, leading to potential breaches and system compromises. The financial impact includes costs for incident response, system hardening, and potential regulatory fines. |  |
| **Detailed observation:**  This vulnerability occurs when a server inadvertently exposes sensitive information through error messages, HTTP headers, or other means. This information can include software versions, internal IP addresses, or directory structures, which can aid attackers in crafting exploits. |  |
| **CVE/CWE:**  CVE-2023-29012 / CWE-200 |  |
| **Proof of Concept:**    The server information is being Disclosed in the particular image.    Wapplyzer- A Tool to check version usage shows the version of the server and the Python. |  |
| **Vulnerable Points:**  http://10.236.150.124:8000/questions.html |  |
| **Recommendation:**  1. Configure servers to suppress detailed error messages and limit the information disclosed in HTTP headers. 2. Regularly review and update server configurations to minimize information leakage. 3. Implement security best practices for server hardening. 4. Conduct regular security audits to identify and address information disclosure issues. |  |
| **Reference:**  https://cwe.mitre.org/data/definitions/200.html |  |
| **New or Repeat observation:**  New |  |

# **Vulnerability: Security Headers Missing**

|  |  |
| --- | --- |
| **Affected Asset:**  http://10.236.150.124:8000/questions.html |  |
| **Vulnerability Title:**  Security Headers Missing |  |
| **Business Impact:**  Missing security headers can leave applications vulnerable to a variety of attacks, including XSS, clickjacking, and MIME type sniffing. The financial impact includes costs for incident response, potential fines for non-compliance, and reputational damage. |  |
| **Detailed observation:**  Security headers are critical for protecting web applications from common vulnerabilities. Missing headers like Content-Security-Policy, X-Frame-Options, and X-Content-Type-Options can expose applications to XSS attacks, clickjacking, and MIME type sniffing. |  |
| **CVE/CWE:**  CVE-2023-30123 / CWE-16 |  |
| **Proof of Concept:**    Image shows the missing security headers. When we click on inspect, and fo to the network tab in the inspect window, we see the security headers of both request and response. We see that a lot of Security Headers(Content Security Policy, X-Powered-by, X-Content-Type-options)    Shows the missing Response Headers.    Shows the missing requests header. |  |
| **Vulnerable Points:**  http://10.236.150.124:8000/questions.html |  |
| **Recommendation:**  1. Implement and configure all recommended security headers in web applications. 2. Regularly review and update security header configurations to align with best practices. 3. Use automated tools to scan for missing or misconfigured security headers. 4. Conduct regular security audits to ensure compliance with security header policies. |  |
| **Reference:**  https://cwe.mitre.org/data/definitions/16.html |  |
| **New or Repeat observation:**  New |  |

# **Vulnerability: Clickjacking**

|  |  |
| --- | --- |
| **Affected Asset:**  http://10.236.150.124:8000/questions.html |  |
| **Vulnerability Title:**  Clickjacking |  |
| **Business Impact:**  Clickjacking can lead to unauthorized actions performed on behalf of users, compromising data integrity and user accounts. The financial impact includes costs for incident response, potential regulatory fines, and reputational damage. |  |
| **Detailed observation:**  Clickjacking occurs when an attacker tricks a user into clicking on a malicious element disguised as a legitimate interface component. This can lead to unauthorized actions, such as changing account settings or initiating transactions without the user's knowledge. |  |
| **CVE/CWE:**  CVE-2023-36789 / CWE-1021 |  |
| **Proof of Concept:**    Using Burp-Suite as a tool , we see that the page is susceptible to clickjacking. |  |
| **Vulnerable Points:**  http://10.236.150.124:8000/questions.html |  |
| **Recommendation:**  1. Implement frame busting techniques to prevent your website from being embedded in iframes. 2. Use the X-Frame-Options HTTP header to restrict framing of your web pages. 3. Conduct regular security testing to identify and address clickjacking vulnerabilities. 4. Educate users about the risks of clickjacking and how to recognize suspicious behavior. |  |
| **Reference:**  https://cwe.mitre.org/data/definitions/1021.html |  |
| **New or Repeat observation:**  New |  |