1. Detailed Observation

## Web Application Security Assessment & Penetration Testing

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | Click jacking | **Risk Rating**: Low |
| **Description** | Click jacking is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages. | |
| **Affected Path(s)** | /(web server) | |
| **Impact** | An attacker can host this domain in other evil site by using iframe and if a user fills the given field it can directly redirect as logs to attacker and after its redirect to your web server. Leading to steal user information too and use that host site as phishing of your site its CSRF and Click jacking. | |
| **Evidence/Proof of Concept**  **Step 1**: Use the click jacking code in the owasp page https://www.owasp.org/index.php/Testing\_for\_Clickjacking\_(OTG-CLIENT-009) By Replacing the URL as shown in below image.  1.png  **Step 2 :**the website is loaded within the frame as shown in below image  **clickjacking.png** | | |
| **Recommendation** | Sites can use X-Frame-Options to avoid click jacking attacks, by ensuring that their content is not embedded into other sites.  It is recommended to perform the following: ? Use the X-FRAME Options in response header set to DENY or Same Origin or ALLOW-FROM a specified URL? X-Frame-Options: This header works with modern browsers and can be used to prevent framing of the page. | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | Technology/Version Disclosure | **Risk Rating**: Low |
| **Description** | The HTTP responses returned by this web application include a header named server and X-Powered by option. The value of this header is used by server to determine which version is in use. It is not necessary for production sites and should be disabled. | |
| **Affected Path(s)** | /(web server) | |
| **Impact** | The HTTP header may disclose sensitive information. This information can be used to launch further attacks | |
| **Evidence/Proof of Concept**  **Step 1**: by capturing the any response from the server we can be able to see the server and technology version as shown in below image  Version disclosure.png | | |
| **Recommendation** |  | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | Stack Trace Error | **Risk Rating**: Low |
| **Description** | The application responds with stack traces that are not managed which could reveal information useful to attackers. Providing debugging information as a result of operations that generate errors is considered a bad practice due to multiple reasons. For example, it may contain information on internal workings of the application such as relative paths of the point where the application is installed or how objects are referenced internally. | |
| **Affected Path(s)** | /(web server) | |
| **Impact** | An attacker can obtain information such as:  • Server version.  • Information about the generated exception and possibly source code, SQL queries, etc.  This information might help an attacker gain more information and potentially focus on the development of further | |
| **Evidence/Proof of Concept**  Step 1: By accessing the some of the web pages the stack trace error is generating as shown in below image  stack trace error.png | | |
| **Recommendation** | Handle all errors properly and do not reveal any sensitive data such as internal path of file.  https://www.owasp.org/index.php/Testing\_for\_Stack\_Traces\_(OTG-ERR-002) | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | Vulnerable JavaScript library | **Risk Rating**: Low |
| **Description** | The application is using multiple vulnerable JavaScript libraries that have the known public exploits. Using these libraries may affect the application’s security. | |
| **Affected Path(s)** | http://code.jquery.com/jquery-latest.min.js | |
| **Impact** | The vulnerabilities caused by the used vulnerable libraries could help the attacker to perform cross site scripting attacks that result in client side attacks that affect the end users. | |
| **Evidence/Proof of Concept**  Step 1:the web application is using the vulnerable jquery version as shown in below mage  outdated jquery version.png | | |
| **Recommendation** | Upgrade to the latest version of the JQuery libraries 3.0 or higher. | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Concurrent Login possible** | **Risk Rating**: [Risk Rating] |
| **Description** | It is the web application design decision to determine if multiple simultaneous logons from the same user are allowed from the same or from different client IP addresses. If the web application does not want to allow simultaneous session logons, it must take effective actions after each new authentication event, implicitly terminating the previously available session, or asking the user (through the old, new or both sessions) about the session that must remain active. | |
| **Affected Path(s)** | http://10.72.5.78:8080/Grievance/Home.jsp | |
| **Impact** | In case the user accessed from the public places and forgot to logout from the system, an attacker who has access to the same system would be able to continue the session and conduct malicious activities. Later, if the user logged in using his laptop from his home, the session being accessed by the attacker will not be terminated which is a serious issue. | |
| **Evidence/Proof of Concept**  Step 1:by using the same user credentials we can able to login in two different accounts as shown in below image  concurrent logins.png | | |
| **Recommendation** | It is recommended for web applications to add user capabilities that allow checking the details of active sessions at any time, monitor and alert the user about concurrent logons, provide user features to remotely terminate sessions manually, and track account activity history (logbook) by recording multiple client details such as IP address, User-Agent, login date and time, idle time, etc  Reference links:  https://www.owasp.org/index.php/Session\_Management\_Cheat\_Sheet#Simultaneous\_Session\_Logons  https://security.stackexchange.com/questions/34880/is-it-safe-to-allow-users-multiple-login-at-different-browsers-computers  https://stackoverflow.com/questions/17515716/only-one-concurrent-login-per-user-in-asp-net  http://geekswithblogs.net/Frez/archive/2010/05/17/preventing-a-user-from-having-multiple-concurrent-sessions.aspx | |
| **Management Comments** |  | |