|  |  |
| --- | --- |
| **Vulnerability 9** | **Findings** |
| **Title** | Sensitive data exposure |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | Low |
| **Description** | While the robots.txt file itself does not present a security vulnerability, it can provide awareness of the directories and files within an application's database. If the application relies on the robots.txt file to protect access to these areas and does not enforce proper access controls, this can create a serious vulnerability. During the review, hidden directories and files were discovered. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | It is important to not rely on the robots.txt file to provide protection against unauthorized access. Sensitive information should not be disclosed within these files. Instead, proper access controls and authentication measures should be implemented to protect against unauthorized access to sensitive areas of an application or system. |

|  |  |
| --- | --- |
| **Vulnerability 10** | **Findings** |
| **Title** | Command Injection |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | Critical |
| **Description** | By accessing the networking.php page through the disclaimer.php page, it was possible to execute commands in the tab intended for DNS checks and interact with the databases. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | It is important to ensure that access controls and authentication measures are in place to prevent unauthorized access to sensitive areas of an application or system. It is also important to properly validate and sanitize user input to prevent against potential vulnerabilities, such as command injection attacks. |

|  |  |
| --- | --- |
| **Vulnerability 11** | **Findings** |
| **Title** | Advanced Command Injection |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | critical |
| **Description** | An advanced command injection attack was detected from the networking.php page, allowing the attacker to execute advanced commands in the tab intended for MX record checking. The attack was able to bypass input validation strips. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | An advanced command injection attack was detected that allowed the attacker to execute advanced commands and bypass input validation measures. To address this issue, it is important to implement proper input validation and sanitization measures, as well as access controls and authentication measures to prevent unauthorized access to sensitive areas of the system. Regular review and updates to security measures and user education can also help to secure the system and protect against potential vulnerabilities. |

|  |  |
| --- | --- |
| **Vulnerability 12** | **Findings** |
| **Title** | Authentication/Brute force attack |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | critical |
| **Description** | A brute force attack was successful in accessing the administrator login tabs on the login page. The attacker utilized a previously identified vulnerability to access the **/etc/passwd** file, allowing them to accurately guess the administrator credentials and gain login access. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Implement robust brute-force protection or multi-factor authentication. |

|  |  |
| --- | --- |
| **Vulnerability 13** | **Findings** |
| **Title** | File Path Traversal/ PHP injection |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | critical |
| **Description** | An attacker was able to access hidden information by requesting the **souvenirs.php** page through the URL and utilizing path traversal/PHP injection techniques. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | To remediate the issue of an attacker accessing hidden information through the **souvenirs.php** page using path traversal/PHP injection techniques. You should verify the existence of the vulnerability, identify the root cause, implement a fix, test the fix to ensure it is effective, deploy the fix to the production environment, and monitor the production environment. For any further attempts to access hidden information or other vulnerabilities. |

|  |  |
| --- | --- |
| **Vulnerability 14** | **Findings** |
| **Title** | Session Management |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | critical |
| **Description** | A session management attack was conducted using Burp to identify and exploit a secret session ID in the URL. The attacker used the Intruder tab in Burp suite to find the correct session ID and gain access to pages that were previously only accessible due to a previously identified vulnerability. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | To remediate the issue of an attacker accessing pages via manipulated or leaked session IDs. You should identify the root cause of the vulnerability, implement measures to ensure that session IDs are secure and cannot be easily manipulated, test the implemented measures to ensure they are effective, deploy the measures to the production environment, and monitor the production environment. For any further attempts to access pages via manipulated or leaked session IDs. |

|  |  |
| --- | --- |
| **Vulnerability 15** | **Findings** |
| **Title** | Directory Traversal |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | critical |
| **Description** | Previously identified web vulnerabilities disclosed unknown paths. Allowing an attacker to request files from the URL and retrieve them from the server's file system, due to the lack of defenses against directory traversal attacks. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20, Port 110 |
| **Remediation** | Upgrade SLMail or mitigate risk by restricting access to the service. |

|  |  |
| --- | --- |
| **Vulnerability 16** | **Findings** |
| **Title** | Apache Tomcat JSP Upload bypass RCE (CVE-2017-12617) |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | critical |
| **Description** | An exploited vulnerability (CVE-2017-12617) was discovered on the host, allowing an attacker to use Metasploit to achieve Remote Code Execution (RCE) and gain root access. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.10 |
| **Remediation** | To remediate the issue of an attacker achieving Remote Code Execution (RCE) on the host, you should update Tomcat to the latest version where the exploited vulnerability (CVE-2017-12617) has been fixed, and set the **readonly** init-param to **true** to prevent malicious code from being executed by the Tomcat servlet. Additional measures, such as input validation and regular security assessments, may also be necessary to fully secure the host against RCE attacks. |