|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Target** | **Critical** | **High** | **Medium** | **Low** | **Informational** |
| 127.0.0.1 | 1 | 1 | 1 | 1 | 1 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Sr No.** | **Vulnerability Name** | **Severity** | **CVSS** |
| **1** | Remove prive excalation | **Critical** | 9.3 |
| **2** | local prev escalation | **High** | 7.5 |
| **3** | XSS Injection | **Medium** | 6.5 |
| **4** | Xframe-Options Header missing | **Low** | 3.5 |
| **5** | Right clink not blocked | **Informational** | 0.0 |

|  |  |
| --- | --- |
| ***1*** | ***Vulnerability Name: Remove prive excalation Severity: Critical*** |
| **CVSS** | 9.3-CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H |
| **Organization** | client\_name |
| **Parameter** | PHP v7 |
| **Description** | PHP Remote code execution |
| **Impact** | Remote code execution |
| **Remediation** | Upgra the PHP |
| **PoC** | Step 1:  Step2: |

|  |  |
| --- | --- |
| ***2*** | ***Vulnerability Name: local prev escalation Severity: High*** |
| **CVSS** | 7.5-CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:L |
| **Organization** | client\_name |
| **Parameter** | kernal v12.0.9 |
| **Description** | A standard user can bypass the implemented security mechanism to evlate the privilege and become the admin |
| **Impact** | The threat actor can potentially overtake the system and perform malicious activities. |
| **Remediation** | Upgrade the kernel to the latest version. |
| **PoC** | Step 1:  Step2: |
| ***3*** | ***Vulnerability Name: XSS Injection Severity: Medium*** |
| **CVSS** | 6.5-CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:L |
| **Organization** | client\_name |
| **Parameter** | https://example.com.php?q=123 |
| **Description** | XSS are caused due to improper input sanitization |
| **Impact** | successfulll xss can lead to account take over and credential theft |
| **Remediation** | Sanitize all user inputs |
| **PoC** | Step 1:  Step2: |

|  |  |
| --- | --- |
| ***4*** | ***Vulnerability Name: Xframe-Options Header missing Severity: Low*** |
| **CVSS** | 3.5-CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:L |
| **Organization** | client\_name |
| **Parameter** | https://example.com.php |
| **Description** | Xframe header are used to prevent the websites from XSS injection |
| **Impact** | missing xframe header can lead to successful XSS injection |
| **Remediation** | add xframe-options header in the server header |
| **PoC** | Step 1:  Step2: |

|  |  |
| --- | --- |
| ***5*** | ***Vulnerability Name: Right clink not blocked Severity: Informational*** |
| **CVSS** | 0.0-CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N |
| **Organization** | client\_name |
| **Parameter** | https://example.com.php |
| **Description** | right click enable the users to downlaod the website images and other content |
| **Impact** | an attacker can download the images of the website |
| **Remediation** | block the right click |
| **PoC** | Step 1: |