**Introduction**

This document describes the new scope of work and cost estimate for security issue fixing of an existing application MILAAP.

**Scope of Work**

|  |  |  |
| --- | --- | --- |
| 1 | The application is vulnerable to Cross-site request forgery attack | High  https://resources.infosecinstitute.com/topic/fixing-csrf-vulnerability-in-php-application/ |
| 2 | The application does not implement authentication checks for downloads | High |
| 3 | Directory listing is enabled on the server | Medium |
| 9 | Application is vulnerable to Back refresh attack | Medium |
| 6 | The application has auto-complete feature enabled | Medium |
| 4 | The application does not implement required session cookie attribute | Low |
| 7 | Application using vulnerable libraries | Low |
| 8 | Application is vulnerable to Clickjacking | Low |
| 9 | Out-of-date Version (jQuery) | Medium |
| 10 | Missing X-Frame-Options Header | Low |
| 11 | If your website is vulnerable to a Cross-site Scripting attack CSP can prevent successful exploitation of that vulnerability | High |
| 12 | The application will be vulnerable to MIME sniffing. | Medium |
| 13 | An attacker can use this information to get cookie by cross site scripting (XSS) which could lead to session hijacking. | Medium |
| 14 | If the secure flag is not set, then the cookie will be transmitted in clear-text if the user visits any HTTP URLs within the cookie's scope. | Medium |

**Technology Outline**

1. PHP
2. MySql

**Timeline**

10 (Ten Working Days)

**Fees**

INR xx,000.00 (XX XX Only) without tax

**Payment Schedule**

1. Mobilization Advance- 50%
2. Final go live- 50%

**Assumption:**

1. VPN connection will be provided by Magma.
2. Access to Server and Database will be provided.
3. Development instance will be provided.