|  |  |
| --- | --- |
| Title: Hidden File Found | |
| Description: | |
| Phpinfo.php page Detection, it includes admin detail and other installed and supported software information. | |
| Affected Resources | Severity |
| [phpinfo() (aristopharma.co.in)](http://lms.aristopharma.co.in/phpinfo.php) | **Critical** |
| Impact | |
| By accessing such a file, a remote attacker can discover a large amount of information about the remote web server, including:-   - The root directory of the web server.  - Configuration information about the remote PHP installation. | |
| Recommendation | |
| Remove the affected file | |
| Tool Used | References |
| Nessus | https://www.php.net/manual/en/function.phpinfo.php |
| POC | |
|  | |

|  |  |
| --- | --- |
| Title: Insure Communication | |
| Description: | |
| Insecure Communication over http request leads to packet capturing and reveal the information over network. | |
| Affected Resources | Severity |
| http://lms.aristopharma.co.in/ | **High** |
| Impact | |
| The attacker can get victim passwords , can do MITM attacks. | |
| Recommendation | |
| Do not allow the website open in http request ,use SSL Certificate | |
| Tool Used | References |
| WireShark | [M3: Insecure Communication | OWASP Foundation](https://owasp.org/www-project-mobile-top-10/2016-risks/m3-insecure-communication) |
| POC | |
|  | |

|  |  |
| --- | --- |
| Title: Found Open Ports | |
| Description: | |
| Open Ports are revealing the Service Version that the server is running On. | |
| Affected Resources | Severity |
| http://lms.aristopharma.co.in/ | **High** |
| Impact | |
| The attacker can use this version for finding exploits (pentesting using Metasploit) | |
| Recommendation | |
| Please the in Production that the relevant ports are required, keep the server up to date | |
| Tool Used | References |
| NMAP | [WSTG - Latest | OWASP Foundation](https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/01-Information_Gathering/04-Enumerate_Applications_on_Webserver) |
| POC | |
|  | |

|  |  |
| --- | --- |
| Title: Absence of Anti-CSRF Tokens | |
| Description: | |
| No Anti-CSRF tokens were found in a HTML submission form. | |
| Affected Resources | Severity |
| http://lms.aristopharma.co.in/ | **MEDIUM** |
| Impact | |
| A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. | |
| Recommendation | |
| Use anti-CSRF packages such as the OWASP CSRFGuard. | |
| Tool Used | References |
| ZAP PROXY | https://cwe.mitre.org/data/definitions/352.html |
| POC | |
|  | |

|  |  |
| --- | --- |
| Title: Vulnerable JS Library | |
| Description: | |
| jQuery JavaScript Library v1.6.1 | |
| Affected Resources | Severity |
| http://lms.aristopharma.co.in/aristo\_pharma/include/loadfirst.js | **MEDIUM** |
| Impact | |
| The identified library jquery, version 1.6.1 is vulnerable. | |
| Recommendation | |
| Use up to Date JS version | |
| Tool Used | References |
| ZAP PROXY | http://research.insecurelabs.org/jquery/test/ |
| POC | |
|  | |

|  |  |
| --- | --- |
| Title: Missing Anti-clickjacking Header | |
| Description: | |
| The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks. | |
| Affected Resources | Severity |
| http://lms.aristopharma.co.in/aristo\_pharma/login.php | **MEDIUM** |
| Impact | |
| Website page loading in an anonymous website using iFrame. | |
| Recommendation | |
| Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. | |
| Tool Used | References |
| ZAP PROXY | https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options |
| POC | |
|  | |

|  |  |
| --- | --- |
| Title: Content Security Policy (CSP) Header Not Set | |
| Description: | |
| Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks | |
| Affected Resources | Severity |
| http://lms.aristopharma.co.in/aristo\_pharma/login.php | **MEDIUM** |
| Impact | |
| These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files. | |
| Recommendation | |
| Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header. | |
| Tool Used | References |
| ZAP PROXY | https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing\_Content\_Security\_Policy |
| POC | |
|  | |