

**Hardhat Enterprises**

**Fortify**

**Cyber Risk Client Management**

**2022**

|  |  |  |  |
| --- | --- | --- | --- |
| **Client Name** | **Cyber risks** | **Notes** | **Name of Researcher** |
| Cottage by the Sea | * Sensitive Data Exposure: Data that contains minors' private information. * Insufficient monitoring: No one constantly reading logs/monitoring the site. * Security misconfiguration: Using default configurations/passwords that aren't properly configured |  | Emily |
| Ferntree Gully Community Arts Centre | * Sensitive Data Exposure: handling of children and adult information * Broken Access Control: primary communication with clients/volunteers is through an email subscription | Is closely connected to the Knox Council website, as there is no website of its own | Richa |
| Knox Tavern | * Insecure Deserialisation and using component with vulnerabilities: Users are able to upload any type of file into the “Upload your resume” box – no restrictions. * Security Misconfiguration: Site owner has not secured site and provided site URL as “http” not “https”. |  | Michael |
| Australian Rickettsial Reference Lab | * Sensitive Data: Handling of medical records of children and adults including private and personal information. * Broken Access Control: Basic administration staff have full medical record access including edit and create. * Insecure cryptography and network security: No TLS certificate – passwords can be sniffed. Network easily accessible. | Apart of Barwon Health – hacked in 2019. |  |

**How to detect risk based on the** [**OWASP Report**](https://www.superwebpros.com/blog/top-10-critical-security-risks-business-websites/) **-**

*“most prevalent security risks for business websites, and how they relate to the 4 dimensions of security in terms of how easy they are to exploit.”*

*Using this report we can find a risk and use the 4 dimensions to examine potential clients.*

