**6.3.1 Descripción de la situación**

Una tienda que vende artículos y accesorios para animales de compañía, que se ha constituido recientemente, se encuentra con la situación de que le han llegado rumores de que se han desarrollado ataques cibernéticos en toda la zona en la que se ha ubicado la empresa, además de sus propios compañeros del sector que les informaron de este tipo de actos vandálicos.

Ahora mismo, disponen de una web a modo de tienda virtual (E-commerce), en la que se dedica a vender a todos los usuarios online de manera nacional. Para poder comprar en esta web será necesario registrarse en la aplicación. Por lo que se necesitará almacenar todos los datos personales de dicho usuario como pueden ser: la dirección, teléfono de contacto, DNI o NIF, etc.

Esta página web está desarrollada de una manera sencilla con el lenguaje de programación de C++. Por lo que el propietario de la organización necesita saber los errores o debilidades que tiene en la web así como en el diseño y desarrollo de esta. Y si se da el caso de tener entrometido ya algún virus o archivo remoto.

### **6.3.2 Recomendación de tecnología a utilizar**

|  |  |  |
| --- | --- | --- |
| **Criterios relevantes para la decisión** | **Ventajas tecnología 1 Netsparker** | **Ventajas tecnología 2 Nmap** |
| Criterio A.2: Coste | Coste de 1.195$ | Gratuita. |
| Criterio C.6: Plataformas disponibles | Solo se encuentra disponible para el Sistema Operativo de Windows. | Está disponible para una gran variedad de sistemas como Windows o Linux. |
| Criterio D.1: XSS (Cross-site Scripting) | Detecta la intrusión de scrips ejecutables. | No puede detectar la introducción de código. |
| Criterio D.3: Inclusiones de archivos remotos | Es capaz de detectar la inyección de archivos remotos. | No es capaz de detectar la inyección de archivos remotos. |
| Criterio D.4: Mal uso de los puertos SSL y TSL para los pagos | No puede detectar las vulnerabilidades de los puertos de los protocolos SSL / TLS. | Es capaz de detectar vulnerabilidades en los puertos de los protocolos SSL y TSL. |
| Criterio D.5: Mal uso de los puertos HTTPS | No puede detectar el uso de los puertos de los protocolos de seguridad de HTTPS. | Puede detectar el uso erróneo de los puertos de los protocolos de seguridad de HTTPS. |
| Criterio D.6: Errores de desarrollo | Pueden identificar más detalladamente los errores en el desarrollo de la web. | Pueden detectar los errores en el desarrollo de la web. |
| Criterio D.7: Errores de diseño | Puede identificar de manera más detallada y específica los errores en el diseño de una web. | Es capaz de identificar los errores en el diseño de la web. |

En este caso como Netsparker se centra en el escaneo e investigación del código fuente, detecta la posibilidad de la intrusión de código ejecutable en C++ (lenguaje de programación muy utilizado para actos maliciosos) en la aplicación web así como de detectar posibles secuencias de comandos entre los distintos sitios.

Realizará un análisis de todos los posibles scripts introducidos y ataques de robo de información, así como la suplantación de indentidad en el inicio de sesión, además de detectar la inyección de archivos ejecutables remotos que puedan ejecutar códigos en el servidor o la redirección a otras web que pueden ser hackeadas para redireccionar a sitios maliciosos y muchas cosas más. Pero tiene el problema de que no analiza la seguridad de los puertos de seguridad de los protocolos usados.

Por eso será necesaria la aportación de la herramienta Nmap, ya que esta realizará una investigación exhaustiva de los puertos para ver cuáles son las vulnerabilidades existentes. Para ello se analizará el uso de los puertos de seguridad de los protocolos SSL/TLS (Para la compras de artículos) y HTTPS (Para la navegación segura de los usuarios) además de muchos otros relacionados con el robo de información personal, los datos enviados y recibidos así como el cifrado de los paquetes que se envían y reciben.

Además de ello también será necesario analizar con ambas herramientas los errores existentes en el diseño y desarrollo de la página web.

Por lo tanto, en esta situación recomendamos el uso de ambas herramientas para una correcta y completa investigación, ya que estas dos son complementarias, por lo que se obtendrá un informe muy detallado de todas las posibles vulnerabilidades y debilidades del sitio web, para poder sanarlas a tiempo.