Reporte Final

Primera Parte

José de Jesús Vázquez Gómez

Equipo: Los Vatos de Azcapo

Diego Monroy Fraustro	A01165792
Eduardo Azuri Gaytán Martinez	A01165988
Carlos Alejandro Reyna Gonzalez	A01165824
Diego Galíndez Barreda	A01370815

Descripción de la actividad:

En esta primera entrega se creó un sitio web usando Java, con servlets y jsps. Este sitio es muy simple, solo cuenta con un sistema de login básico (autenticación) y una página que reporta el status del usuario que la acaba de accesar.

Sobre esta se van a revisar varias vulnerabilidades, el primer paso para ello es usando la herramienta Nessus, la cual nos permite escanear vulnerabilidades de diferentes aplicaciones.

Vulnerabilidades:

La herramienta encontró algunas vulnerabilidades muy básicas, pero encontró 3 que podrían ser explotables, a pesa de ser consideradas de baja y media prioridad. Estas consisten en faltas de pruebas de autenticidad por parte del servidor y falta de garantía de privacidad. La principal que se encontró es el envío de credenciales en texto plano.

El envío de credenciales en texto plano (cleartext credentials) se debe a que, en este caso, no estamos encriptando de ninguna manera el password o el nombre de usuario.

Esto permitiría que cualquier tipo de man in the middle suplantara la identidad de cualquiera de nuestros usuarios. Resultaría muy sencillo escuchar la conexión y tomar las credenciales mientras viajan del cliente al servidor.

Controles:

Se pueden usar controles muy simples para cubrir esta vulnerabilidad.

El más sencillo de implementar sería la encripción de la contraseña al enviarla al servidor para ser evaluada. Esto obviamente tiene diferente grado de efectividad según el algoritmo usado para la encripción.

Por lo mismo, es posible (aunque poco probable) que se pueda abusar aun así, ya que todo algoritmo de encripción puede romperse. Idealmente se usaría un algoritmo como RSA, que es computacionalmente seguro.

Otro control, un poco más complejo pero que realmente no tiene mayor dificultad su implementación, sería el uso de una conexión segura (HTTPS) con certificados enviados del servidor al cliente y viceversa.

Esto, en cierto modo, es otro medio de encriptación, ya que el protocolo encripta la conexión. Sin embargo, este encripta toda la información que pasa por la conexión, no solo la contraseña, siendo considerablemente más seguro que solo encriptar la contraseña.

Otra alternativa, que resultaría ideal, sería tener tanto los certificados como la encriptación de la contraseña y el nombre de usuario. Esto da un mayor nivel de seguridad general, ya que aunque se escuche y desencripte la conexión, será necesario desencriptar también las credenciales.

Evidencias:

Se incluye el reporte generado por Nessus como evidencia.