Seguridad y Privacidad en redes 2011

Práctica seguridad de aplicaciones WEB

El objetivo de la presente práctica es manipular distintos tipos de vulnerabilidades WEB para implementar ataques que comprometan la integridad de la aplicación y los datos que esta posee. Es también un objetivo de esta práctica que puedan diferenciar distintos aspectos que inciden en la ejecución de dichas vulnerabilidades (usuarios, aplicaciones, configuraciones del servidor).

Nota: Para realizar esta practica debe usar la aplicación vulnerable DVWA que se encuentra en el LiveCD de la practica. A menos que se indique lo contrario, deberá utilizar el nivel de seguridad **LOW** para la realización de los ejercicios.

1. Cross Site Scripting – Almacenado
   a) Tareas:
      1. Comprobar la existencia de dicha vulnerabilidad en la sección XSS stored de DVWA.
      2. Montar un ataque que permita robar cookies de sesión a usuarios que visitan dicha página o son incitados a hacerlo. Es condición de este ataque que:
         (a) El usuario no sospeche nada respecto del ataque que está sufriendo.
      3. Utilizar la información robada para hacerse pasar por el usuario víctima.
      4. Evalúe el código del nivel medio para esta vulnerabilidad y teniendo en cuenta los controles realizados por la aplicación, adapte el ataque implementado anteriormente para que funcione en dicho nivel.

   b) Preguntas:
      1. En base a lo observado, determine qué medidas podrían ser esenciales en la mitigación de dicho problema:
         (a) Concientización del usuario: SI/NO (en qué temas)
         (b) Concientización del desarrollador: SI/NO (en qué temas)
         (c) Concientización del administrador: SI/NO (en qué temas)

2. Cross Site Scripting – REFLEJADO
   a) Tareas:
      1. Comprobar la existencia de dicha vulnerabilidad en la sección XSS reflected de DVWA.
      2. Montar un ataque que permita distribuir a los usuarios del sistema, mediante ingeniería social, una URL de acceso que ejecute el ataque contra el usuario, permitiendo robarle su cookie de sesión. Es condición de este ataque que:
         (a) El usuario no sospeche nada respecto del ataque que está sufriendo.
         (b) La url esté ofuscada de alguna manera, de modo que no sea posible deducir qué hace por medio de una inspección de la misma.
      3. Utilizar la información robada para hacerse pasar por el usuario víctima.

   b) Preguntas:
      1. En base a lo observado, determine qué medidas podrían ser esenciales en la mitigación de dicho problema:
         (a) Concientización del usuario: SI/NO (en qué temas)
         (b) Concientización del desarrollador: SI/NO (en qué temas)
         (c) Concientización del administrador: SI/NO (en qué temas)

3. Fallas de Inyección – Inyección SQL

   Tareas:

   1. Comprobar la existencia de dicha vulnerabilidad en la sección SQL Injection de DVWA.
   2. Manipular la entrada de datos del usuario para inyectar comandos SQL. A través del presente ataque, deberían poder obtener datos sensibles de la base de datos como los resultantes de la siguiente consulta SQL: *select user,password from dvwa.users;*
   3. Evalúe el código del nivel medio para esta vulnerabilidad y teniendo en cuenta los controles realizados por la aplicación, adapte el ataque implementado anteriormente para que funcione en dicho nivel.

   b) Preguntas:

   1. Dada la información obtenida, se puede decir que la aplicación tiene un problema del tipo “Almacenamiento Criptográfico Inseguro”? SI/NO, ¿por - qué?
   2. En base a lo observado, determine qué medidas podrían ser esenciales en la mitigación de dicho problema:
      (a) Concientización del usuario: SI/NO (en qué temas)
      (b) Concientización del desarrollador: SI/NO (en qué temas)
      (c) Concientización del administrador: SI/NO (en qué temas)

4. Referencia insegura de objetos

   Tareas:

   1. Comprobar la existencia de dicha vulnerabilidad en la sección File inclusion de DVWA. Verifique la posibilidad de revelar el contenido del archivo /etc/passwd.
   2. Montar un ataque que permita ejecutar código PHP arbitrario en el servidor. Es condición de este ataque que:
      (a) El código arbitrario que se ejecuta en el servidor esté alojado en otro servidor web.

   b) Preguntas:

   1. En base a lo observado, determine que medidas podrían ser esenciales en la mitigación de dicho problema:
      (a) Concientización del usuario: SI/NO (en qué temas)
      (b) Concientización del desarrollador: SI/NO (en qué temas)
      (c) Concientización del administrador: SI/NO (en qué temas)

5. Ejecución de archivos maliciosos

   a) Tareas:

   1. Desarrolle un script php que le permita ejecutar comandos pasados por parámetro.
   2. (LOW) Usando el modo de seguridad LOW de DVWA, utilizar la sección “Upload” para subir el archivo antes desarrollado y verificar el correcto funcionamiento del ataque mediante la ejecución de comandos arbitrarios en el servidor mediante la utilización el archivo subido.
   3. (MEDIUM) Evalúe el código del nivel medio para esta vulnerabilidad y teniendo en cuenta los controles realizados por la aplicación, adapte el ataque implementado anteriormente para que funcione en dicho nivel. Verificar el correcto funcionamiento del ataque mediante la ejecución de comandos arbitrarios en el servidor mediante la utilización el archivo subido.
   4. (HIGH uploads /MEDIUM file inclusion) El nivel HIGH de DVWA para la sección upload sólo permite subir archivos con Filetype image/jpeg. El nivel MEDIUM de DVWA para la sección “File Inclusion” sólo permite la referencia de objetos locales.

Realice un ataque que permita la ejecución de comandos en el servidor a través de la combinación de vulnerabilidades anteriores.

b) Preguntas:
   1. En base a lo observado, determine que medidas podrían ser esenciales en la mitigación de dicho problema:
      (a) Concientización del usuario: SI/NO (en qué temas)
      (b) Concientización del desarrollador: SI/NO (en qué temas)
      (c) Concientización del administrador: SI/NO (en qué temas)

6. Cross Site Request Forgery (CSRF)
   a) Tareas:
      1. Comprobar la funcionalidad de la sección CSRF y analice por - qué la misma es suceptible a ataques de CSRF.
      2. Montar una página web en otro servidor a la cual accedan usuarios de DVWA mediante alguna técnica de ingeniería social y como resultado de tal visita se le cambie la contraseña DVWA al usuario atacado. Es condición de este ataque que:
         (a) El usuario no sospeche nada respecto del ataque que está sufriendo.
      3. Evalúe el código del nivel medio para esta vulnerabilidad y teniendo en cuenta los controles realizados por la aplicación, adapte el ataque implementado anteriormente para que funcione en dicho nivel.
   b) Preguntas:
      1. En base a lo observado, determine que medidas podrían ser esenciales en la erradicación de dicho problema:
         (a) Concientización del usuario: SI/NO (en qué temas)
         (b) Concientización del desarrollador: SI/NO (en qué temas)
         (c) Concientización del administrador: SI/NO (en qué temas)

7. Broken Authentication and session management
   a) Tareas:
      1. Analice el manejo de sesiones de la aplicación web y enumere todas las cosas que a su criterio no se manejan adecuadamente.
      2. En cada caso evalúe cómo dichos problemas podrían ser utilizados en la realización de un ataque.
   b) Preguntas:
      1. En base a lo observado, determine que medidas podrían ser esenciales en la mitigación de dicho problema:
         (a) Concientización del usuario: SI/NO (en qué temas)
         (b) Concientización del desarrollador: SI/NO (en qué temas)
         (c) Concientización del administrador: SI/NO (en qué temas)

Otros problemas del OWASP TOP TEN con los que puede experimentar utilizando el DVWA:

8. Information Leakage and Improper Error Handling - Perdida de Información y manejo inadecuado de errores: http://x.x.x.x/algo_que_no_existe.html

9. Falla al restringir el acceso a URLs: http://x.x.x.x/dvwa/setup.php

10. Comunicaciones inseguras: http://x.x.x.x/dvwa/login.php