Práctica 2
Vulnerabilidades de Seguridad – Primavera 2019

	¿Lo he hecho?
Se tiene que entregar la solución en único archivo en formato pdf. No se admite ningún otro formato (doc, docx, odt, zip, rar, tar.gz, ...).	☐
Todas las páginas deben estar numeradas y deben contener nombre y apellidos.	☐
La fecha límite de entrega es el **8 de mayo de 2019 (a las 24 horas UTC / GMT +1 horas).**	☐
Esta actividad se puede resolver, con la nota máxima, de forma relativamente breve. En ningún caso la extensión de la solución debe superar las **10 páginas** con fuente tamaño mínimo 10pt (incluido el texto en las figuras) con interlineado simple. Por favor limitad el uso de capturas de pantalla a cuando sean estrictamente necesarias y mirad que no ocupen demasiado espacio en las páginas.	☐
Razonad la respuesta en todos los ejercicios, indicando todos los pasos que habéis realizado para obtener la solución. Las respuestas sin justificación, que sean una copia de una fuente de información y/o que no contengan las referencias utilizadas, no recibirán ninguna puntuación.	☐

© Este documento tiene copyright. Por favor, absteneos de difundirlo a terceras personas sin una autorización por escrito.

Contexto:

Nos encontramos con una aplicación de “scouting” de deportistas de la empresa ACME. En esta aplicación, los diferentes usuarios pueden añadir deportistas que les resulten interesantes a la base de datos, y anexar a cada uno de estos los comentarios que sean oportunos sobre la idoneidad de su contratación. Como curiosidad, los comentarios no pueden ser editados, pero los deportistas sí (por si cambian de equipo).

Después de que los alumnos de esta asignatura encontraran y explotaran diversas vulnerabilidades, los desarrolladores han decidido lanzar una nueva versión, que se estudia a continuación.

Disponéis de un usuario de nombre «luis» con password «1234» para acceder a esta aplicación.

Configuración:

La web sobre la que trata este ejercicio se puede encontrar al archivo "web.tar.gz" que os podéis descargar del enlace http://deic.uab.cat/~mistic/web.tar.gz . Para hacerla funcionar se puede usar un servidor web apache con php y sqlite3. En Debian/Ubuntu los paquetes a instalar son: sqlite3, php5-sqlite, php5, y apache2. Por Windows u OSX, es recomienda usar XAMPP, en este caso, hay que activar la extensión SQLLite3 modificando el archivo xampp/php/php.ini. En general, un error habitual a la hora de ponerla en funcionamiento es no dar al archivo de base de datos los permisos necesarios.

Alternativamente, a partir de la versión 5.4.0 de php, este incluye un servidor web integrado con el que se puede poner en ejecución de forma rápida (http://php.net/manual/en/features.commandline.webserver.php).

Los archivos dentro de "web.tar.gz" están separados entre los que son accesibles a través del servidor web y los que no lo son (todos son accesibles para el servidor web, pero no todos los sirve en Internet). Se entiende que los archivos de la carpeta “web” están situados en un servidor cualquiera (por ejemplo, http://localhost:80). Los archivos que hay en la raíz son accesibles y los que están en la carpeta “private” no lo son, por lo tanto, **ninguna solución puede basarse en información que se haya obtenido a partir de los archivos de la carpeta “private” excepto que el enunciado lo pida explícitamente**.

Podéis comprobar que efectivamente el fichero que os habéis descargado corresponde con el del enunciado de esta práctica validando el hash SHA256:

29de3416a9fdc358436533c071dc88fce04fada3f2820615ba294b294319c79f

© Este documento tiene copyright. Por favor, absteneos de difundirlo a terceras personas sin una autorización por escrito.

Pregunta 1 *(3 puntos)*

Sabéis que, en la versión inicial, tanto la página principal de esta aplicación web como la página de consulta de comentarios sobre un jugador era vulnerable a inyecciones XSS a través de los campos «Team Name» y «Player Name». Por lo tanto, lo primero que haremos es estudiar si esto ha sido correctamente resuelto por parte de los desarrolladores.

Contestad les siguientes preguntas justificando las respuestas:

1. ¿La página principal («index.php») continua presentando esta vulnerabilidad? ¿Como lo habéis comprobado?

2. ¿La página de consulta de comentarios («show_comments.php») continua presentando aquesta vulnerabilidad? ¿Como lo habéis comprobado?

3. ¿Respecto a las vulnerabilidades que hayan sido resueltas: cómo lo han hecho los desarrolladores?

4. ¿En caso que alguna vulnerabilidad aún no haya sido resuelta: qué error han cometido los desarrolladores? ¿Con qué código se puede explotar?

Pregunta 2 *(7 puntos)*

Por otro lado, os habéis enterado de que se ha localizado una nueva vulnerabilidad en esta aplicación. La única información que os ha llegado es que se trata de una vulnerabilidad similar a la CVE-2008-5804.

Contestad les siguientes preguntas justificando las respuestas:

1. ¿En qué consiste la vulnerabilidad CVE-2008-5804?

2. ¿Qué vulnerabilidad de la aplicación de scouting se le parece? ¿Cómo la habéis encontrado?

Ahora que ya habéis localizado esta vulnerabilidad, decidís aprovecharla para obtener toda la información posible sobre las bases de datos de la aplicación.

Contestad les siguientes preguntas justificando las respuestas:

3. ¿Cómo es el ataque que hay que realizar para descubrir los nombres de todas las tablas de las bases de datos, así como todos los nombres de todos sus campos?

4. ¿Utilizando la información obtenida en el punto anterior, cómo es el ataque que obtiene todos los números de las tarjetas de crédito?

Una vez realizado este ataque, decidís contactar con la empresa ACME para informar del problema, y como ellos no son capaces de solucionarlo, os hacen llegar el código fuente de la aplicación (**para contestar la siguiente pregunta sí que puedes consultar el código fuente de la aplicación**), y os piden ayuda.

5. ¿Qué cambios haríais en el código para conseguir que la aplicación dejara de ser vulnerable a estos ataques? Tened en cuenta también las vulnerabilidades de la pregunta 1 (XSS).

© Este documento tiene copyright. Por favor, absteneos de difundirlo a terceras personas sin una autorización por escrito.

Nota: **Propiedad intelectual**

A menudo es inevitable hacer uso de recursos creados por terceras personas. Es por tanto comprensible hacerlo en el marco de una práctica, siempre que esto se documente claramente y no suponga plagio en la práctica.

Por lo tanto, al presentar una práctica que haga uso de recursos ajenos, se presentará junto con ella un documento en el que se detallen todos ellos, especificando el nombre de cada recurso, su autor, el lugar donde se obtuvo y el su estatus legal: si la obra está protegida por copyright o se acoge a alguna otra licencia de uso (Creative Commons, licencia GNU, GPL ...). El estudiante deberá asegurarse de que la licencia que sea no impide específicamente su uso en el marco de la práctica. En caso de no encontrar la información correspondiente deberá asumir que la obra está protegida por copyright.

Nota: esto se refiere al copyright del documento que entregáis en el registro de evaluación continua y no al copyright de las herramientas que podáis haber usado. Por ejemplo, al usar una imagen en la respuesta de un ejercicio debéis seguir lo aquí indicado, pero por el contrario, si usáis el sistema operativo Debian para resolver el enunciado, entonces no es necesario.

© Este documento tiene copyright. Por favor, absteneos de difundirlo a terceras personas sin una autorización por escrito.