ARQUTECTURA DE SOFTWARE

TRABAJO ATRIBUTO NO FUNCIONAL SEGURIDAD

PRESENTADO POR:

CRISTIAN DAVID LOPEZ AREVALO

DOCENTE: Diego Prieto

BOGOTÁ DISTRITO CAPITAL

22/11/2019

Introducción

En este trabajo se busca explicar que procesos de seguridad se pueden implementar en la aplicación capture the flag, con ayuda del trabajo de un red team, los cuales se encargan ver y comprender la aplicación y que formas pueden realizar para vulnerarla para que se aplique un control sobre estas y asegurar este criterio.

Seguridad

Ciber inteligencia

Nos habla de los mecanismos de recolección de información que se podría tener desde aplicaciones open source, donde se puede sacar datos los cuales las personas publican en internet. Lo cual si no se maneja bien el control de datos y se llegara a publicar la cuenta como usuario y contraseña en algún sitio donde pudiera estar al alcance de herramientas de búsqueda se llegaría a comprometer la información de los usuarios o de los mismos desarrolladores de la aplicación.

Acceso físico

Como no se tiene un lugar donde se pueda acceder y comprometer los datos, no se aplica mucho para nuestra aplicación, teniendo este punto asegurado.

Redes

Al ser una aplicación la cual funciona por medio de internet, los usuarios pueden sufir un ataque por el cual el atacante puede suplantar la red wifi a la cual están conectados, y de esta forma también sacarles datos como la contraseña y cuenta de la red real a la cual están conectados.

Red team Tácticas de explotación

Según con las medidas de red team que se plantaron, la cual nos dan un control para evitar la inyección de código como sql, la cual nos es poner restricciones en los campos donde se pide información para que el usuario no pueda meter código que pueda ser ejecutado por el servicio.

En el caso de capture the flag no se ha implementado un control en la parte de login de la aplicación, donde el usuario podría cometer una inyección sql, permitiéndole entrar sin autorización o permisos.

También tener en cuenta como se pasa la información ante la red, ya que se puede capturar y leerla utilizando aplicaciones como burp suite, de este modo buscar la forma en la cual se pueda aprovechar, por ejemplo si al momento de login no se manda la petición de una forma cifrada si no en texto plano dejándole ver la contraseña y cuenta a aquel que capture la información.

Conclusiones

Con la información planteada, se puede ver la importancia de la seguridad en las aplicaciones, y de qué forma podemos hacer para garantizarla lo mejor posible, para ofrecerles una confiabilidad a los usuarios que la utilizan, ya que un error de estos puede dejar en mala reputación y poner en peligro los datos de las personas, donde el atacante podría hacer algo que perjudique a las personas.