***Trabajo Práctico 2° Cuatrimestre 2017***

***Cátedra Seguridad Informática***

***Investigación de vulnerabilidades y contramedidas***

***Docente:****Ing. Matias Mevied*

***Jefe de Cátedra:****Lic. Juan Carlos Tirante*

Índice

[Introducción 3](#_1fob9te)

[1° Entrega – Selección de la aplicación 3](#_3znysh7)

[2° Entrega – Selección de la vulnerabilidad 3](#_2et92p0)

[3° Entrega – Preparación del entorno de trabajo 4](#_tyjcwt)

[4° Entrega – Investigación de la vulnerabilidad y su contramedida 4](#_3dy6vkm)

[5° Entrega – Desarrollo del Exploit y sus contramedidas 4](#_1t3h5sf)

[Exposición del trabajo práctico 4](#_2s8eyo1)

# Introducción

El trabajo práctico consiste en la investigación y armado de una prueba de concepto sobre una vulnerabilidad que forma parte del top 10 de OWASP (Open Web Application Security Project) y el desarrollo de una contramedida. La aplicación donde se realice la investigación queda a elección del grupo y está sujeta a la aprobación delos docentes. La aprobación del trabajo práctico se compone de la aprobación parcial de cada entrega, la entrega final y la exposición del trabajo realizado.

Cada grupo tienen un margen de 1 día por cada entrega que puede ser administrado como cada grupo quiera, un total de 5 días de margen durante todo el trabajo. Si el grupo tiene más de esos días de demora en la entrega del trabajo se considera reprobado.

Todas las entregas parciales deben ser enviadas por mail al docente asignado y en copia el resto del cuerpo docente para la corrección del trabajo. La entrega final debe ser entregada impresa el día de la exposición, el 28 de Octubre del 2017.

# 1° Entrega – Selección de la aplicación

**Fecha límite de entrega vía mail:** 2 de Septiembre 2017

**Descripción**: Se debe seleccionar una aplicación para poder realizar la investigación sobre una vulnerabilidad existente y de conocimiento público. En esta etapa se debe tener en cuenta que la aplicación seleccionada tenga diversas vulnerabilidades y que las vulnerabilidades tengan asignados CVE (Common Vulnerabilities and Exposures).

Se necesita en esta entrega informar a los docentes la aplicación seleccionada que estará sujeta a la aprobación del cuerpo docente.

# 2° Entrega – Selección de la vulnerabilidad

**Fecha límite de entrega vía mail:** 9 de Septiembre 2017

**Descripción**: Se debe redactar undocumento que contenga como mínimo los siguientes apartados:

* Introducción: Indicar cuál es la vulnerabilidad elegida y su contramedida
* Escenario: Se debe indicar sobre que plataforma aplica la vulnerabilidad y el detalle necesario para entender su funcionamiento
* Arquitectura: Graficar como es la infraestructura donde aplica la vulnerabilidad indicando y explicando los componentes afectados.

# 3° Entrega – Preparación del entorno de trabajo

**Fecha límite de entrega vía mail:** 23 de Septiembre 2017

**Descripción:** En esta entrega se debe tener listo el entorno de trabajo donde se va a explotar la vulnerabilidad y aplicar su contramedida. Para demostrar el cumplimiento de esta entrega se solicitarán capturas de pantalla del entorno conformado y la explicación de cada una de las capturas.

# 4° Entrega – Investigación de la vulnerabilidad y su contramedida

**Fecha límite de entrega vía mail:** 7 de Octubre 2017

**Descripción:** Se debe realizar una investigación exhaustiva de la vulnerabilidad elegida y hacer un informe técnico detallado de dicha vulnerabilidad. Por otra parte analizar alternativas de contramedidas para proteger o mitigar la explotación de la vulnerabilidad seleccionada.

# 5° Entrega – Desarrollo del Exploit y sus contramedidas

**Fecha límite de entrega vía mail:** 21 de Octubre 2017

**Descripción:** Se debe desarrollar en el lenguaje que se desee el Exploit de la vulnerabilidad seleccionada y también se pueden utilizar herramientas ya existentes para la explotación. Además se deben desarrollar contramedidas para intentar evitar o mitigar la explotación de la vulnerabilidad.

**Entrega Final  
Fecha de entrega impresa:** 28 de Octubre 2017

**Descripción:** La entrega final debe contener:

* Todas las entregas parciales
* Reporte ejecutivo
* Conclusión
* Bibliografía

# Exposición del trabajo práctico

En conjunto con la entrega final se debe entregar la presentación que van a realizar el día de la exposición. En caso que el grupo decida no armar una presentación de manera digital, los docentes deben estar informados y aprobar el cambio.