**UNIVERSIDAD TÉCNICA DE AMBATO**

**Facultad de Ingeniería en Sistemas, Electrónica e Industrial**

**Título:**

Ataque XSS almacenado

**Carrera:**

Ingeniería en Sistemas Computacionales e Informáticos

**Área Académica:**

Hardware y Redes

**Línea de Investigación:**

Software

**Ciclo Académico y Paralelo:**

Noveno “A” Sistemas.

**Alumno participante:**

Bonilla Jefersson

Cornejo Edison

Gómez Daniel

Torres Jefferson

**Módulo y Docente:**

Seguridad Informática, Ing. Félix Fernández Peña

**Ataque XSS almacenado**

XSS ocurre cuando un atacante es capaz de inyectar un script, normalmente Javascript, en el output de una aplicación web de forma que se ejecuta en el navegador del cliente. Los ataques se producen principalmente por validar incorrectamente datos de usuario, y se suelen inyectar mediante un formulario web o mediante un enlace alterado.

**Ejemplo de ataque XSS**

Supongamos por ejemplo el siguiente formulario:



En el formulatio hay una caja de texto para datos de entrada y un botón de enviar. Una vez que el formulario es enviado, enviará los datos a post.php para procesarlos. Supongamos que lo único que se hará con los datos en post.php será mostrarlos con un echo:



Sin ningún tipo de filtrado, el atacante puede enviar el siguiente script a través del formulario, lo que generará un popup en el navegador con el mensaje "Hackeado":



El script anterior tan sólo envía un mensaje de alerta, pero con Javascript ya hemos visto que se pueden hacer multitud de cosas que pueden dañar al usuario, especialmente relacionadas con el robo de cookies y sesiones.