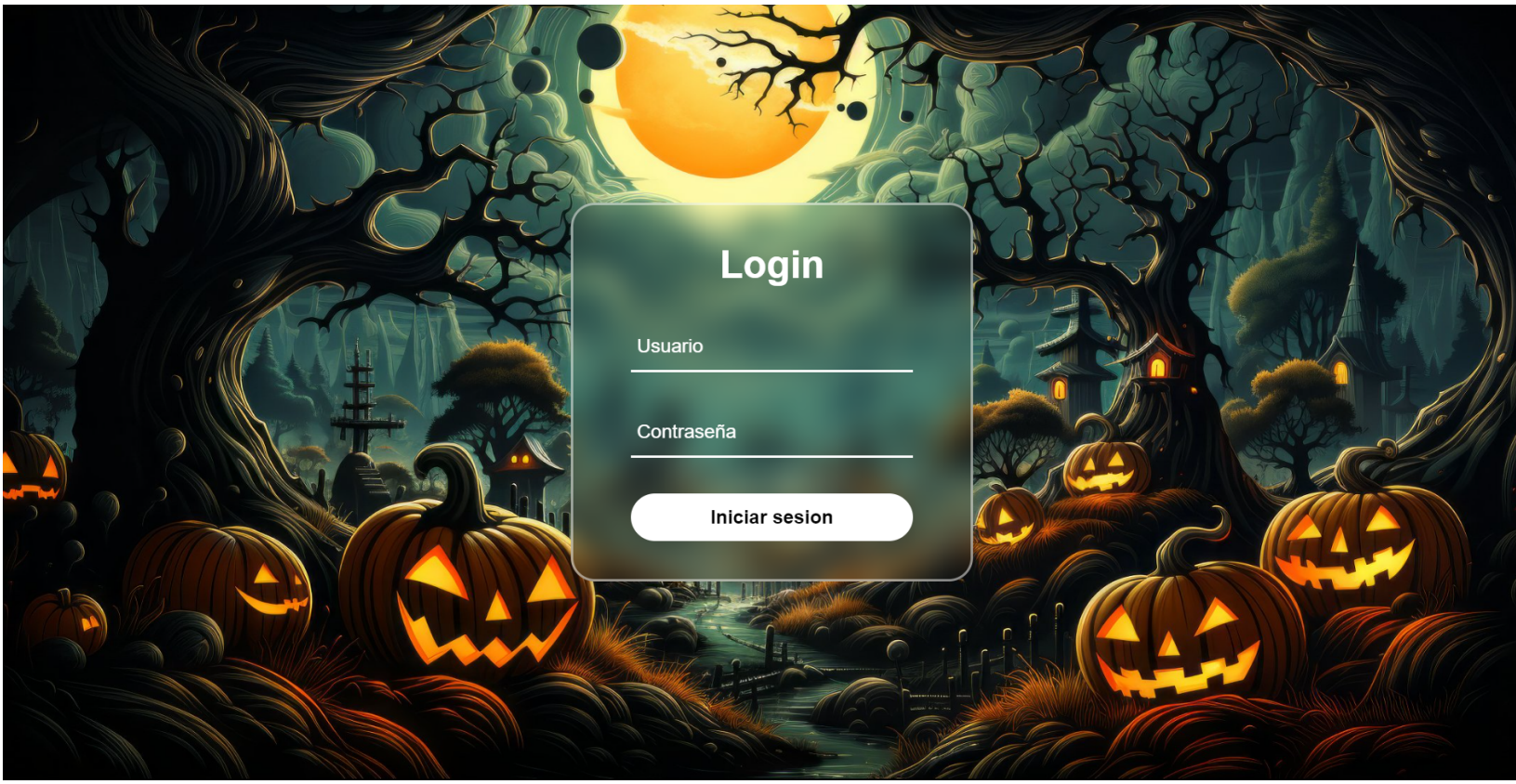
Puesta en producción segura

14 de noviembre de 2023

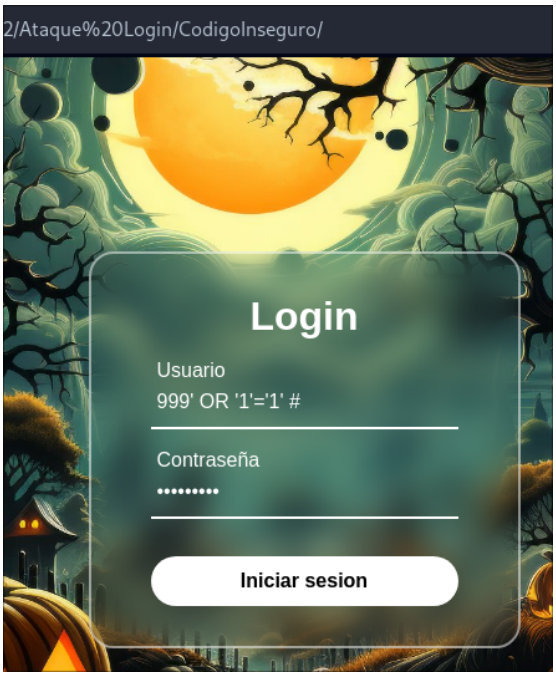
Practica 2.1: Ataque en Login



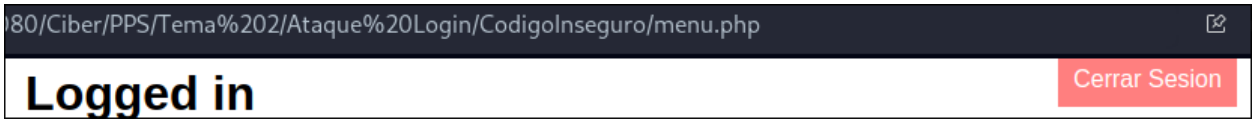
Jose Almirón Lopez

El método de ataque implica realizar una inyección SQL en un formulario de inicio de sesión para obtener acceso no autorizado. En este ejemplo, utilizaremos la siguiente inyección: “**999' or '1' = '1' #”**. Esta técnica, conocida como 'siempre verdadero', aprovecha la falta de seguridad en los datos del formulario de inicio de sesión. Mediante esta simple inyección, podemos conseguir acceder a una aplicación que no ha asegurado adecuadamente su sistema de autenticación.

En el archivo adjunto encontrarás dos códigos: uno inseguro, que ilustra cómo explotar esta vulnerabilidad, y otro asegurado. En el ejemplo del código vulnerable, al utilizar la inyección, somos redirigidos a 'menu.php', logrando así un acceso no autorizado exitoso.



La contraseña que utilicemos carece de importancia, ya que con el símbolo "#" en la inyección indicamos que todo lo que le siga será tratado como un comentario. En consecuencia, lo que introducimos como contraseña se vuelve irrelevante en este contexto.



Para prevenir inyecciones SQL, implementé un condicional que verifica la coincidencia de los datos extraídos de la consulta de usuario y contraseña para el inicio de sesión con los datos recopilados mediante POST desde el formulario. De esta manera, incluso si se intenta realizar una inyección de siempre verdadero, no tendrá éxito, ya que el condicional verificará que no hay ningún usuario en la base de datos que coincida con la información recopilada a través de POST.

```php
if (isset($user) && isset($password)) {
    if ($user == $datos['user'] && $password == $datos['password']) {
        $_SESSION['user'] = $datos;
        header("location:menu.php");
    } else {
        header("location: index.php?error=incorrect");
    }
}
```

Así, al intentar realizar la inyección SQL, el sistema mostrará un mensaje indicando que el usuario o la contraseña son incorrectos, impidiendo así el acceso no autorizado.