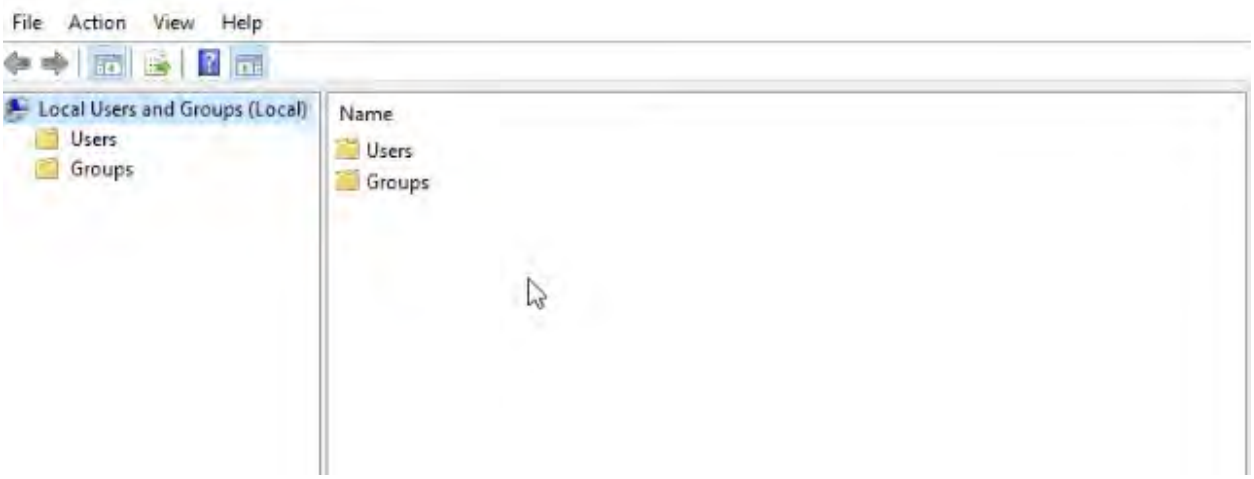
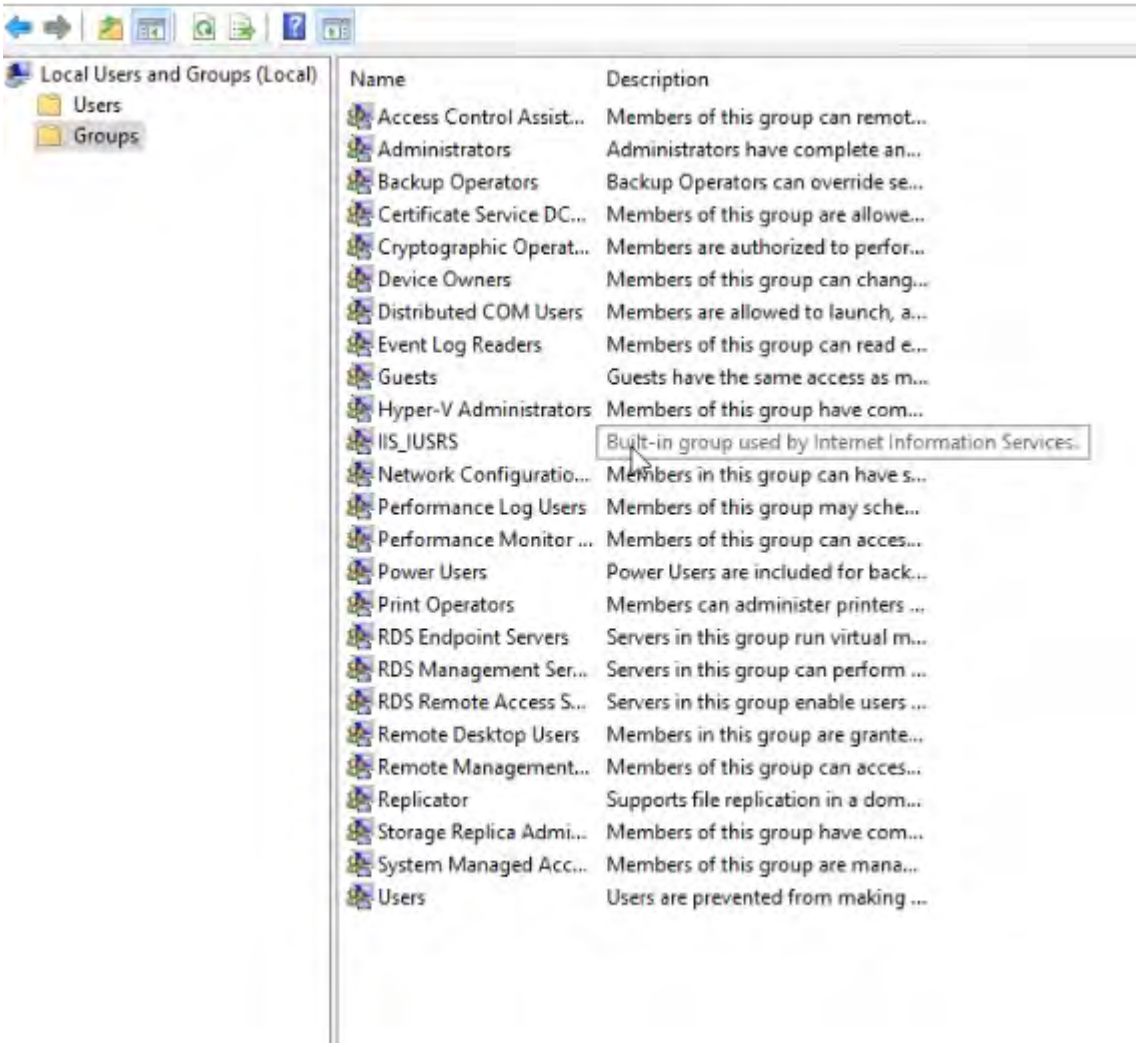
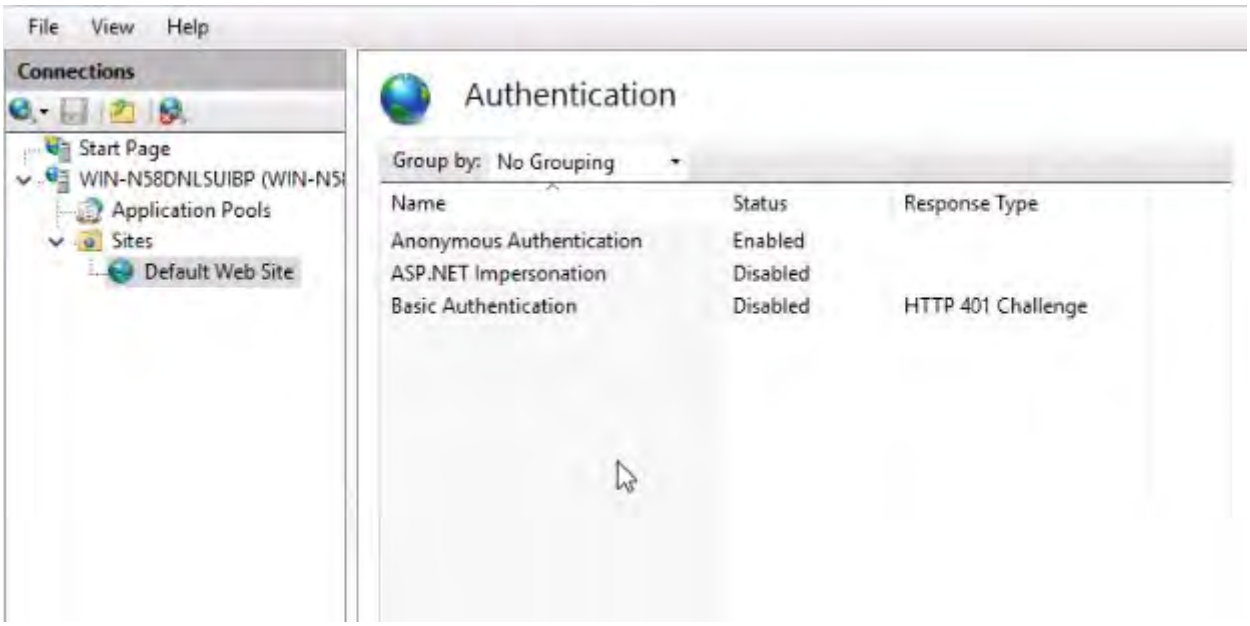
• Administración de sesiones y perfiles web

Crear y configurar usuarios y grupos de usuarios en el servidor para controlas los accesos y privilegios que cada usuario o grupo tendrán.



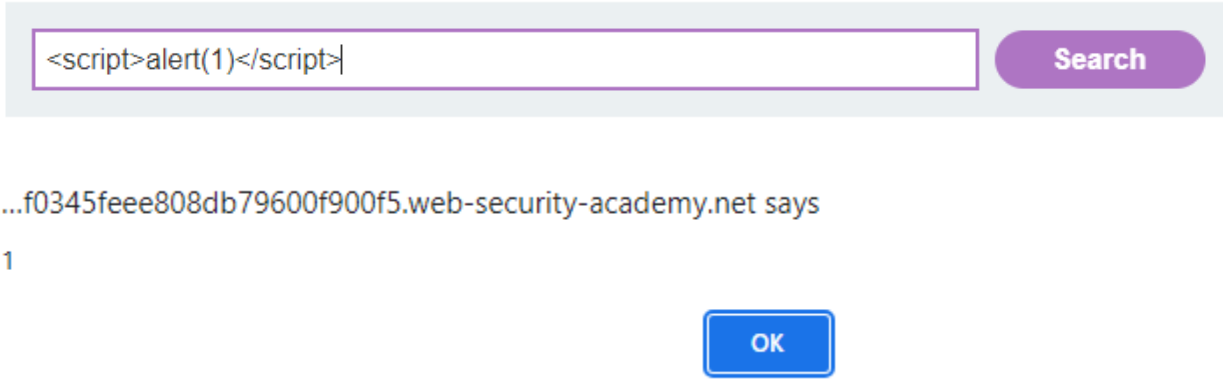


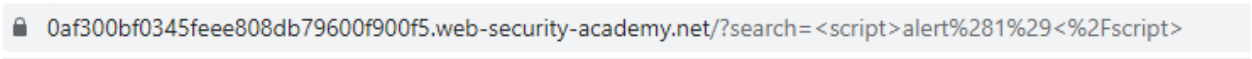


• Atacar por inyecciones y vulnerabilidades XSS

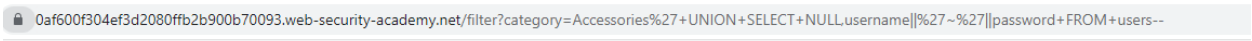
A través de vulnerabilidades en el código como en los ejemplos de portswigger podemos insertar o inyectar líneas de código SQL que modifiquen el comportamiento del url o búsqueda y nos muestren información que no debería estar disponible:

Ej 1:

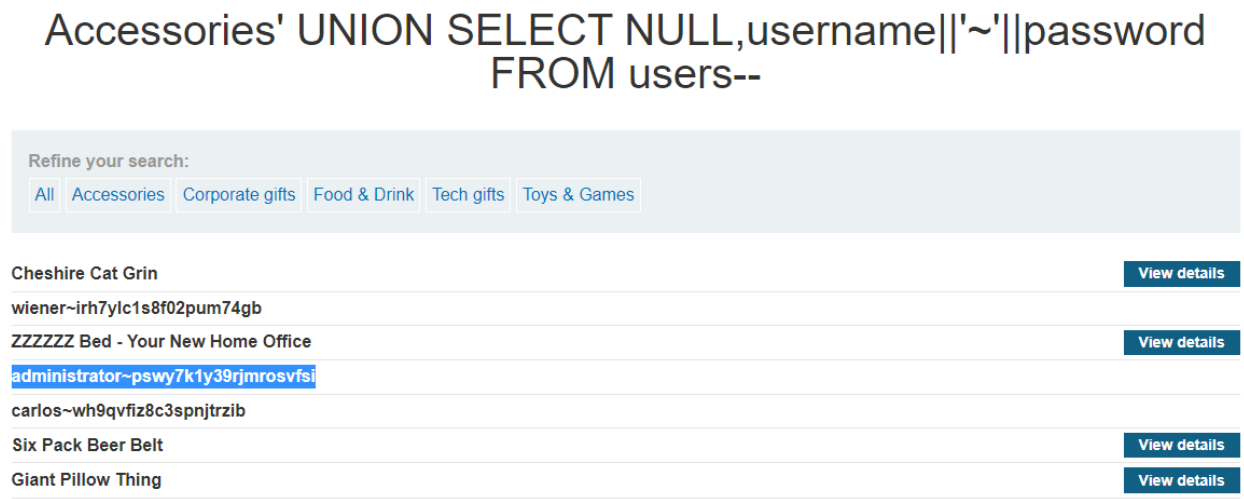




Ej 2:



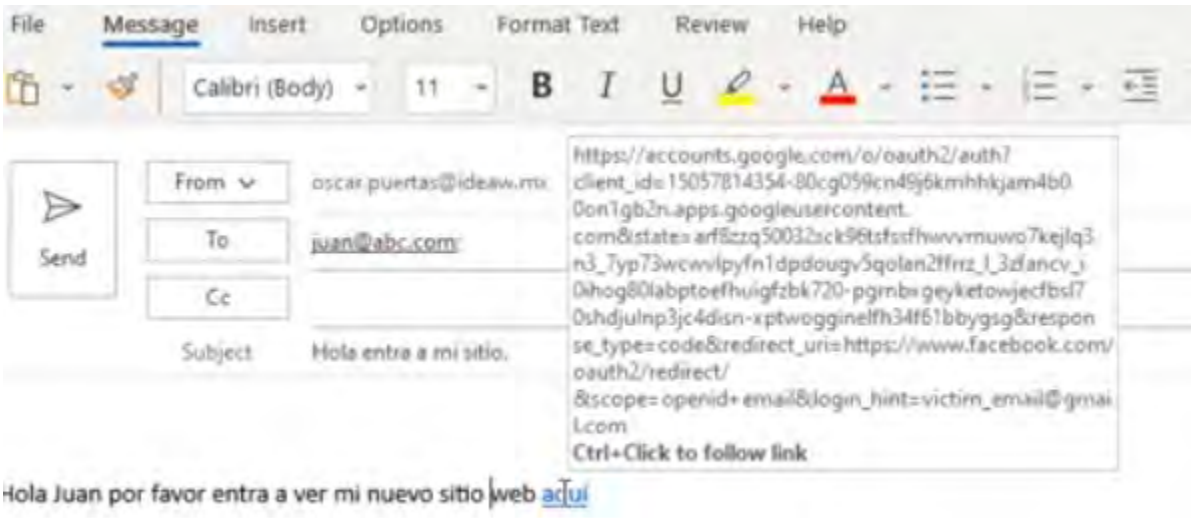
En este ejemplo, modificando el url podemos obtener la base de datos de usuarios junto con sus passwords, incluyendo el de admin:



• Falsificar la identidad y explotar solicitudes entre sitios

Ejemplo:

Cuando recibimos un correo con urls que nos llevan a sitios con engaños, implementados con la intención de capturar nuestros datos como usuario y contraseña.



Y en muchas ocasiones utilizan url shorteners para esconder el url real:

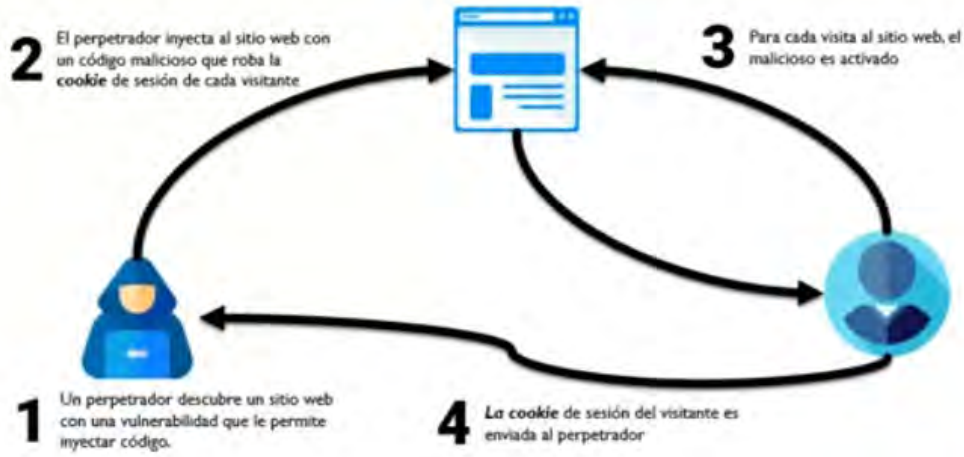
https://tinyurl.com/5y9mdwsu

https://accounts.google.com/o/oauth2/auth?client_id=15057814354-80cg059cn49j6kmhhkjam4b00on1gb2n.apps.googleusercontent.com&state=ARf8Zzq50032sck96TSFssFhWVvMUWO7KEJlq3n3_7Yp73WcWvlpyFn1dpdoUGv5QOLAn2ffrRZ_L_3ZfAncV_I0Ihog80LabpToEfHUIgfzBK720-pGRNbXGeYkETOwjeCfbsl70shdjuLnp3jC4dIsn-xPTwoggineLFh34F61bbYGsg&response_type=code&redirect_uri=https%3A%2F%2Fwww.facebook.com%2Foauth2%2Fredirect%2F&scope=openid+email&login_hint=victim_email@gmail.com

Ejemplo de email falso que parece verdadero:

Estos son algunos ejemplos de ataques cross site scripting:

XSS REFLEJADO



XSS ALMACENADO