COGNITO COMMON PITFALLS

¿QUIENES SOMOS?

- @RoloMijan

Application Security Engineer - Doyensec

https://whateversec.com

- @WhoIsSecure

Security Analyst - Wise Security Global

https://whoissecure.xyz

NUESTROS PROPÓSITOS

- Comprender que es Cognito y sus bases.
- Entender como funciona Cognito y su sistema de autenticación.
- Aprender fallos de seguridad comunes en aplicaciones cuyo sistema de autenticación se basa en Cognito.

¿QUÉ ES COGNITO?

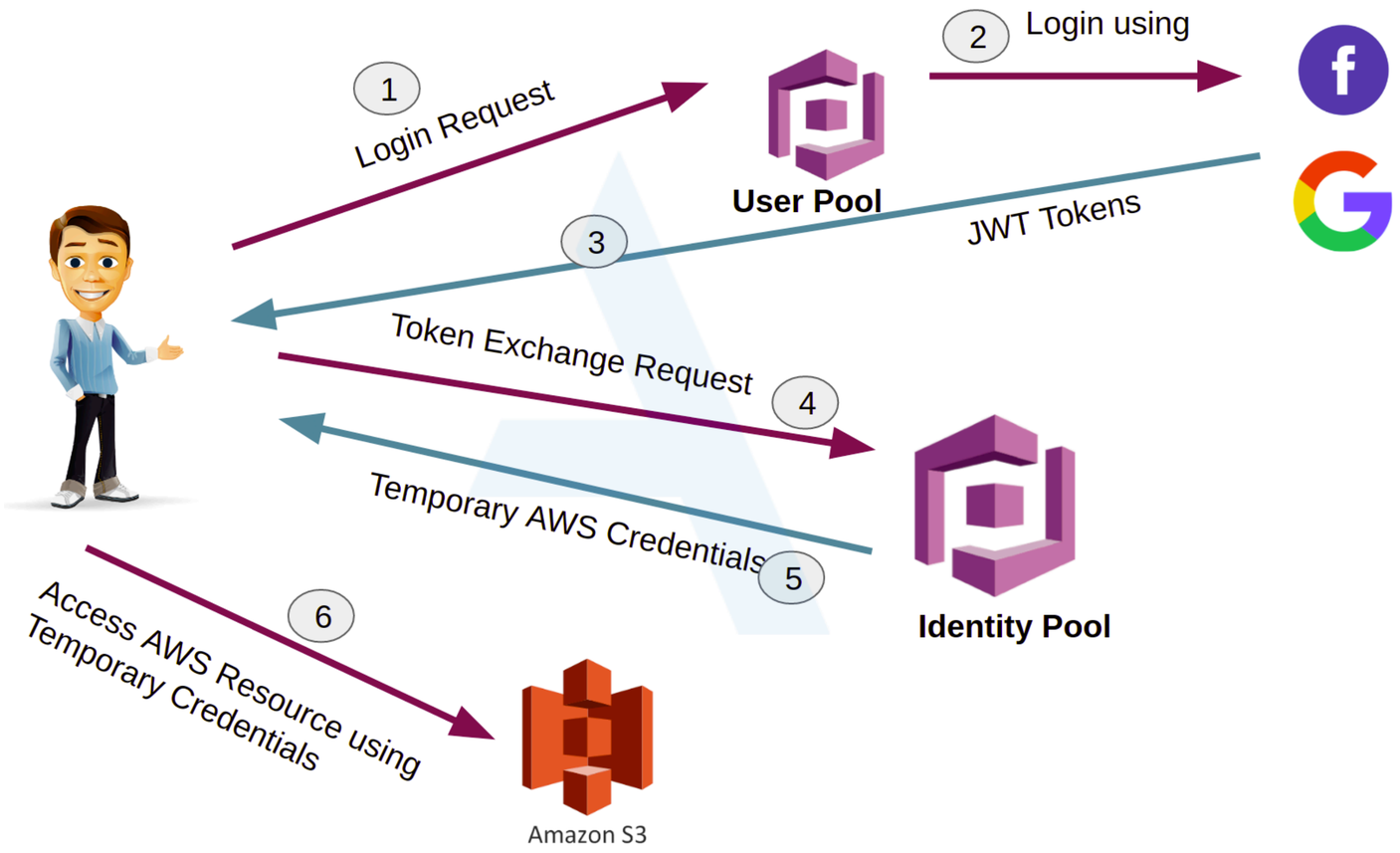
amazon

- Cognito es un sistema de autenticación, autorización y administración de usuarios ofrecido por Amazon.
- Cognito permite delegar dichos sistemas de autenticación, este sistema guarda y sincroniza los datos del usuario final.

LOS GRUPOS

- Grupo de Usuarios: Es un directorio de usuarios en Amazon Cognito. Con él, los usuarios pueden iniciar sesión y registrarse dentro de las aplicaciones Web/ Móvil.
- Grupos de Identidades: Permiten a los usuarios obtener credenciales temporales de AWS para acceder a sus recursos.

¿COMO FUNCIONA LA AUTENTICACIÓN?



ATRIBUTOS DEL GRUPO DE USUARIOS

- Los atributos de un grupo de usuarios es información que se almacena sobre dichos usuarios dentro de Cognito:

    1. Atributos Estandar: Atributos predefinidos por Amazon Cognito (ej. Email).
    2. Atributos Custom: Atributos especificados por los desarrolladores de la aplicación (ej. isAdmin).

POC-1 VULNERABILITY

- Haciendo uso del Token obtenido gracias al Grupo de Identidades, es posible modificar los atributos de nuestro usuario en caso de que no se encuentren correctamente configurados. ¡Incluso si los desarrolladores no han incluido esta funcionalidad específicamente!

POC-1 VULNERABLE CODE

```
@app.route("/secret")
def protected():
    verify_jwt_in_request()
    if get_jwt_identity():
        connection = sqlite3.connect('app.db')
        cursor = connection.cursor()
        messages = cursor.execute('select * from messages where to_email=?', [session['email'].lower()]).fetchall()
        connection.close()
        return render_template("secret.html", messages=messages)
    else:
        return redirect(aws_auth.get_sign_in_url())
```

POC-1 VULNERABILITY FIX

- No confiar en los atributos de los usuarios:

Los atributos de Cognito pueden ser modificados a través de la CLI de AWS, por lo que deben ser tratados al igual que se trata un input en una aplicación Web.

POC-2 VULNERABILITY

- Los Atributos Custom son especialmente sensibles ya que a menudo afectan a la lógica interna de la aplicación.

Comando: aws cognito-idp get-user --region <region> --access-token <Acces_Token>

POC-2 VULNERABLE CODE

```
@app.route("/loggedin", methods=["GET"])
def logged_in():
    access_token = aws_auth.get_access_token(request.args)
    session['isAdmin'] = aws_auth.get_user_info(access_token).get('custom:isAdmin')
    session['email'] = aws_auth.get_user_info(access_token).get('email')
    resp = make_response(redirect(url_for("index")))
    set_access_cookies(resp, access_token, max_age=30 * 60)
    return resp
```

POC-2 VULNERABILITY FIX

- Principio del Mínimo Privilegio:

Se debe garantizar que los usuarios dentro de Cognito no contengan ningún privilegio de modificación de atributos más allá de los necesarios.

POC-3 VULNERABILITY

- El “Access_Key_ID” y el “Secret_Access_Key” nos permiten autenticarnos en AWS como un usuario legítimo. Vamos a buscarlas en:

    1. A través de un Path Traversal.
    2. En el código JavaScript de la aplicación.
    3. En los diferentes repositorios.

Ruta: ~/.aws/credentials

POC-3 VULNERABLE CODE

```python
@app.route("/files")
def files():
    if 'file' in request.args:
        file = request.args.get('file')
    else:
        return "No file provided"

    try:
        content = open(file).read()
    except Exception as e:
        content = e

    return render_template("files.html", content=content)
```

POC-3 VULNERABILITY FIX

- Utilizar variables de entorno para almacenar claves privadas:

Esto impedirá que se pueda acceder a ellas a través de vulnerabilidades como Path Trasversal o que queden expuestas dentro de repositorios públicos.

NOS VEMOS EN LAS BIRRAS

- Es tu momento:
    1. Dudas.
    2. Opiniones.
    3. Criticas.