DERIVACIÓN 2FA

Omitir la autenticación de dos factores

[ ] Lógica de verificación de dos factores defectuosa A veces, la lógica defectuosa en la autenticación de dos factores significa que después de que un usuario ha completado el paso de inicio de sesión inicial, el sitio web no verifica adecuadamente que el mismo usuario esté completando el segundo paso. Por ejemplo, el usuario inicia sesión con sus credenciales normales en el primer paso de la siguiente manera:

```
POST /login-steps/first HTTP/1.1 Host:
sitio-web-vulnerable.com
...
nombre de usuario=carlos&contraseña=qwerty
```

Luego se les asigna una cookie relacionada con su cuenta, antes de pasar al segundo paso del proceso de inicio de sesión:

```
HTTP/1.1 200 correcto
Set-Cookie: cuenta=carlos

OBTENER /pasos-de-iniciar sesión/segundo HTTP/1.1
Cookie: cuenta=carlos
```

Al enviar el código de verificación, la solicitud utiliza esta cookie para determinar a qué cuenta intenta acceder el usuario:

```
POST /login-steps/segundo HTTP/1.1
Host: sitio-web-vulnerable.com
Cookie: cuenta=carlos
...
código de verificación = 123456`
```

En este caso, un atacante podría iniciar sesión con sus propias credenciales pero luego cambiar el valor de la cookie de la cuenta a cualquier nombre de usuario arbitrario al enviar el código de verificación.

```
POST /login-steps/segundo HTTP/1.1
Host: sitio-web-vulnerable.com
Cookie: cuenta=usuario-víctima
...
código de verificación = 123456
```

[] Clickjacking en la función de desactivación 2FA

1. Intente crear un Iframe en la página donde la aplicación permite al usuario desactivar 2FA. 2. Si el Iframe tiene éxito, intente realizar un ataque de ingeniería social para manipular a la víctima.

[] Manipulación de respuesta

1. Verifique la respuesta de la solicitud 2FA.
2. Si observa "Éxito": falso 3. Cambie esto a "Éxito": verdadero y vea si omite la 2FA

[] Manipulación del código de estado

1. Si el código de estado de respuesta es 4XX como 401, 402, etc.
2. Cambie el código de estado de respuesta a "200 OK" y vea si omite la 2FA

[] Reutilización del código 2FA

1. Solicite un código 2FA y úselo . 2.
Ahora, reutilice el código 2FA y, si se usa correctamente, eso es un problema.
3. Además, intente solicitar varios códigos 2FA y vea si los códigos solicitados anteriormente caducan o no . 4. Además,
intente reutilizar el código utilizado anteriormente después de un período prolongado, digamos 1 día o más. Eso

[] CSRF en la función de desactivación 2FA

1. Solicite un código 2FA y úselo . 2.
Ahora, reutilice el código 2FA y, si se usa correctamente, eso es un problema.
3. Además, intente solicitar varios códigos 2FA y vea si los códigos solicitados anteriormente caducan
o no cuando se solicita un nuevo código. 4. Además,
intente reutilizar el código utilizado anteriormente después de un período prolongado, digamos 1 día o más.
Esto será un problema potencial , ya que 1 día es suficiente para descifrar y adivinar un código 2FA de 6
dígitos.

[] Abuso del código de respaldo

Aplique las mismas técnicas utilizadas en 2FA, como manipulación de códigos de respuesta/
estado, fuerza bruta, etc. para omitir códigos de respaldo y deshabilitar/restablecer 2FA

[] Habilitar 2FA no caduca la sesión anterior

1. Inicie sesión en la aplicación en dos navegadores diferentes y habilite 2FA desde la primera sesión.
2. Utilice la segunda sesión y, si no ha caducado , podría ser un problema si no hay un problema de caducidad de sesión
insuficiente. En este escenario, si un atacante secuestra una sesión activa antes de 2FA, es posible llevar a cabo
todas las funciones sin necesidad de 2FA.

[] 2FA Consultar Comprobar Anulación

1. Navegue directamente a la página que viene después de 2FA o cualquier otra página autenticada de
la aplicación.
2. Si no tiene éxito, cambie el encabezado de referencia a la URL de la página 2FA. Esto puede engañar a la
aplicación para que pretenda que la solicitud se produjo después de cumplir la condición 2FA.

[] Fuga de código 2FA en respuesta

1. En la Solicitud de activación de código 2FA, como la función Enviar OTP, capture la solicitud.
2. Ver la Respuesta de esta solicitud y analizar si se filtra el Código 2FA.

[] Análisis de archivos JS

1. mientras activa la solicitud de código 2FA, 2.
analice todos los archivos JS a los que se hace referencia en la respuesta

3. para ver si algún archivo JS contiene información que pueda ayudar a omitir el código 2FA.

[] Falta de protección de fuerza bruta

Esto implica todo tipo de problemas relacionados con una mala configuración de seguridad, como la falta de límite de velocidad, la falta de protección de fuerza bruta, etc.
1. Solicite el código 2FA y capture esta solicitud.
2. Repita esta solicitud entre 100 y 200 veces y, si no hay ninguna limitación establecida, ese es un límite de velocidad . 3. En la página de verificación del código 2FA, intente aplicar fuerza bruta para obtener una 2FA válida y ver si hay algún éxito. 4. También puede intente iniciar, solicitando OTP en un lado y fuerza bruta en el otro. En algún lugar , la OTP coincidirá en el medio y puede brindarle un resultado rápido.

[] Restablecimiento de contraseña/cambio de correo electrónico: 2FA deshabilitado

1. Suponiendo que puede realizar un cambio de correo electrónico o restablecer la contraseña del usuario víctima o hacer que el usuario víctima lo haga por cualquier medio posible.
2. 2FA se desactiva después de cambiar el correo electrónico o restablecer la contraseña. Esto podría ser un problema para algunas organizaciones. Sin embargo, depende de cada caso .

[] Falta la validación de integridad del código 2FA

1. Solicite un código 2FA de la cuenta del atacante.
2. Utilice este código 2FA válido en la solicitud 2FA de la víctima y vea si pasa por alto la protección 2FA.

[ ] Solicitud directa

1. Navegue directamente a la página que viene después de 2FA o cualquier otra página autenticada de la aplicación.
2. Vea si esto pasa por alto las restricciones de 2FA. 3.
Intente cambiar el **encabezado de referencia** como si viniera de la página 2FA.

[] Reutilización del token

1. Tal vez puedas reutilizar un token usado previamente dentro de la cuenta para autenticar.

[] Compartir tokens no utilizados

1. Verifique si puede obtener el token de su cuenta e intente usarlo para evitar la 2FA en una diferencia.

[] Token filtrado

1. ¿Se filtra el token tras una respuesta de la aplicación web?

[] Permiso de sesión

1. Usando la misma sesión, inicie el flujo usando su cuenta y la cuenta de la víctima .
2. Al alcanzar el punto 2FA en ambas cuentas, 3. complete el 2FA con su cuenta pero no acceda a la siguiente parte.

4. En lugar de eso, intenta acceder al siguiente paso con el flujo de cuenta de la víctima .
5. Si el back-end solo establece un booleano dentro de sus sesiones indicando que ha pasado con éxito

[] Función de restablecimiento de contraseña

1. En casi todas las aplicaciones web, la **función de restablecimiento de contraseña inicia sesión automáticamente en el usuario . 2. Verifique si se envía un **correo** con un **enlace** para **restablecer la contraseña** y si puede * *reutilizar**

[] Falta de límite de tarifa

¿Existe algún límite en la cantidad de códigos que puedes probar, por lo que puedes simplemente forzarlos ? ser ca

[] Límite de caudal pero sin límite de caudal

En este caso, hay un límite de caudal (hay que forzarlo muy lentamente: 1 hilo y así

[] Reenviar código y restablecer el límite

Hay un límite de tarifa , pero cuando "reenvía el código" se envía el mismo código y el límite de tarifa es

[] Omisión del límite de tarifa del lado del cliente

{% content-ref url="rate-limit-bypass.md" %} rate-limit-bypass.md {% endcontent-ref %}

[ ] Falta de límite de tarifa en la cuenta del usuario

A veces puedes configurar la 2FA para algunas acciones dentro de tu cuenta (cambiar correo, contraseña...

[ ] Falta de límite de tarifa reenviando el código vía SMS

No podrá eludir la 2FA, pero podrá desperdiciar el dinero de la empresa.

[] Regeneración infinita de OTP

Si puede **generar una nueva OTP infinitas veces**, la** OTP es bastante simple** (4 números), y y

[] Galleta adivinable

Si la función "recordarme" utiliza una nueva cookie con un código adivinable, intente adivinarlo .

[ ] Dirección IP

Si la función "recordarme" está adjunta a su dirección IP, puede intentar averiguar la

[ ] Subdominios

Si puede encontrar algunos subdominios de "prueba" con la funcionalidad de inicio de sesión, podrían estar usando v antiguo.

[] API

Si descubre que 2FA está utilizando una API ubicada en un directorio /v*/ (como "/v3/"), esto probablemente

[ ] Sesiones anteriores

Cuando la 2FA está habilitada, las sesiones anteriores creadas deben finalizar . Esto se debe a que cuando un cliente

[] Control de acceso inadecuado a códigos de respaldo

Los códigos de respaldo se generan inmediatamente después de habilitar 2FA y están disponibles con una sola solicitud

[ ] Divulgación de información

Si nota que aparece información confidencial en la página 2FA que no conocía anteriormente

[] Omitir 2FA con nulo o 000000

[] Las sesiones creadas previamente siguen siendo válidas después de la activación de MFA

1 acceda a la misma cuenta en https://account.grammarly.com en dos dispositivos 2 en el dispositivo 'A' vaya a https://
account.grammarly.com/security > complete todos los pasos para activar el
Ahora la 2FA está activada para esta cuenta.
3 volver al dispositivo 'B' recargar la página La sesión aún está activa

[] Habilitar 2FA sin verificar el correo electrónico. Puedo agregar 2FA a mi cuenta sin verificar mi correo electrónico.

Escenario de ataque:

El atacante se registra con el correo electrónico de la víctima (la verificación por correo electrónico se enviará al correo electrónico de la víctima).
El atacante pudo iniciar sesión sin verificar el correo electrónico.
El atacante agrega 2FA.

[] Contraseña no verificada al deshabilitar 2FA

PoC
1- vaya a su cuenta y active 2FA desde /settings/auth 2- después de activar esta opción, haga clic en
el ícono Desactivado al lado de Autenticación de dos factores. 3- Se abrirá una nueva ventana solicitando autenticación o código de
respaldo - Contraseña para confirmar la desactivación.

4- en el primer cuadro ingrese un código de autenticación o de respaldo válido y en la contraseña ingresada ingrese un 5- la opción se desactivará exitosamente sin verificar la validación de la contraseña.

[] El modo MFA “correo electrónico” permite omitir MFA del dispositivo de la víctima cuando la confianza del dispositivo no ha caducado

Pasos para reproducir:
Nota:
1-Utilice burp suite u otra herramienta para interceptar las solicitudes 2-Encienda
y configure su MFA 3-Inicie sesión con su
correo electrónico y contraseña 4-La página de
MFA aparecerá 5 -Ingrese cualquier número
aleatorio 6-cuando presione el
botón "iniciar sesión de forma segura" intercepta la solicitud POST auth.grammarly.com/v3/a "mode":"sms" by "mode":"email"
"secureLogin":true by "secureLogin":false

7-envía la modificación y comprueba, ¡estás en tu cuenta! No era necesario entrar al pho.

[] Omisión de 2FA enviando un código en blanco

1- Inicie sesión en Glassdoor y navegue hasta https://www.glassdoor.com/member/account/securitySettings_i
2- Habilitar 2FA
3- Cerrar
sesión 4- Inicie sesión nuevamente y observe que
se solicita OTP 5- Ahora, usando la suite Burp, intercepte la solicitud POST enviando un código incorrecto. [No re-enviar]
6- Antes de reenviar la solicitud al servidor, elimine el código y reenvíe 7- Desactive la intercepción
y observe que su solicitud de inicio de sesión se ha cumplido