

**iGNITE**  
Technologies



# Burpsuite for Pentester: Authorise

Página 1 de 22

[www.hackingarticles.in](http://www.hackingarticles.in)

## Contenido

Burpsuite para Pentester: Autorizar .....	3
Vulnerabilidades comunes detectadas por Autorize .....	3
Comprender el funcionamiento de Autorize.....	4
Instalación y configuración .....	4
Opciones de navegación y configuración.....	7
Demostración práctica de Autorize en acción .....	12
Conclusión .....	22

## Burpsuite para Pentester: Autorizar

Para proteger los activos en línea, las pruebas de seguridad de las aplicaciones web son un elemento esencial para salvaguardarlos. Burp Suite ha sido líder en esta área durante muchos años y todavía lo utilizan profesionales de la seguridad y piratas informáticos éticos. Una de esas extensiones que destaca en la comunidad de pruebas de seguridad web es "Authorize", que viene con una amplia variedad de características adicionales para mejorar sus capacidades. Con esta extensión está disponible un potente conjunto de funciones que simplifican el proceso de prueba de autenticación y autorización.

Autorizar = Autenticar + Autorizar

La autorización incluye cualquier método mediante el cual un sistema otorga o revoca permiso para acceder a datos específicos, datos o acciones. Mientras tanto, la autenticación es un proceso mediante el cual un individuo o un sistema se autentica como quien dice ser.

- Vulnerabilidades comunes detectadas por Authorize
- Comprensión de la funcionalidad
- Instalación y configuración
- Opciones de navegación y configuración
- Demostración práctica de Authorize en acción

## Vulnerabilidades comunes detectadas por Authorize

Se centra principalmente en identificar vulnerabilidades relacionadas con la autorización. Puede ayudar a identificar algunos de los principales tipos de vulnerabilidades, como por ejemplo:

- Control de acceso basado en roles (RBAC) inadecuado: puede descubrir problemas en los que los roles o permisos de los usuarios no se aplican adecuadamente, lo que permite a los usuarios acceder a funciones o datos a los que no deberían tener acceso.
- Controles de acceso rotos: puede identificar casos en los que los controles de acceso no están correctamente implementados, dando lugar a un acceso no autorizado a recursos o acciones.
- Referencias directas a objetos inseguros (IDOR): puede encontrar situaciones en las que los atacantes pueden manipular la entrada para acceder a los datos de otros usuarios o realizar acciones que no deberían poder realizar.
- Navegación forzada: puede ayudar a identificar casos en los que un atacante puede navegar directamente a áreas restringidas de la aplicación manipulando las URL.
- Autorización insuficiente: puede detectar situaciones en las que los roles o permisos del usuario no son aplicados adecuadamente, permitiendo que se realicen acciones no autorizadas.
- Escalada de privilegios horizontal y vertical: puede encontrar vulnerabilidades que permitan a los atacantes escalar sus privilegios dentro de la aplicación, ya sea haciéndose pasar por otros usuarios u obteniendo permisos adicionales.
- Defectos de lógica de negocios: Authorize puede descubrir vulnerabilidades de lógica de negocios, donde los flujos de trabajo de las aplicaciones pueden manipularse de maneras no deseadas, lo que podría conducir a acciones no autorizadas o exposición de datos.

Recuerda que la efectividad de Authorize depende de qué tan bien esté configurado y se realicen tus pruebas.

## Comprender el funcionamiento de Autorize

Entendamos cómo funciona Autorizar. Supongamos, por ejemplo, que una aplicación web implementa roles basados en usuarios y admite autenticación basada en cookies.

Usuario normal: tiene acceso a la funcionalidad general pero no se le permite acceder a las funciones de administración ni a la base de datos (acceso de solo lectura).

Usuario administrador: tiene acceso a todas las funciones (acceso de lectura/escritura).

Capture las cookies de usuario normales y agréguelas a Autorizar. Vuelva a iniciar sesión con el usuario administrador, acceda a todas las funciones de administración y actualice algunos datos en la base de datos.

¿Qué hará Autorize ahora? Autorize captura todas las solicitudes y cambia la cookie del administrador con las cookies de su usuario normal cuando navega por una aplicación y luego las envía al servidor. Vea la respuesta del servidor, si el servidor se comporta de la misma manera que el administrador legítimo (como 200 OK en respuesta) y no se han detectado errores. ¡La solicitud fue resaltada como una derivación roja! Otro

La solicitud se muestra como Green Enforced!.

Por cada solicitud enviada al servidor desde un cliente, realizará una prueba automatizada. Con una aplicación grande, con más de 30 páginas web dinámicas, facilitará nuestro trabajo. Hay muchas URL que debes probar manualmente, por lo que Autorize lo hará por ti.

De manera similar, Autorize también detecta un problema en el punto final de la API de la misma manera. Se debe verificar el método de autenticación para la API. Digamos que una API usa un token JWT, puede controlarlo modificando su encabezado de autorización e identificando los problemas de omisión de autenticación con las API.

## Instalación y configuración

Desde Bapp Store, puede descargar e instalar la extensión. Seleccione Bapp Store en Extensiones. Puede buscar "Autorizar" o simplemente mirar hacia abajo. Haga clic en él, desplácese hacia abajo hasta el lado derecho.

La extensión está integrada en Python, verá que primero es necesario instalar 'Jython'.



Comparer Logger Organizer **Extensions** Learn

Installed **BApp Store** APIs BChecks Extensions settings

Total estimated system impact: **Medium**

### BApp Store

The BApp Store contains Burp extensions that have been written by users of Burp Suite, to extend Burp's capabilities.

Search

Name	Instal...	Rating	Popu...	Last upda...	System ...	Detail
AuthMatrix		☆☆☆		15 Oct 2...	Low	
AuthMatrix		☆☆☆		15 Oct 2...	Low	
Authz		☆☆☆		01 Jul 20...	Low	
Auto-Drop Requests		☆☆☆		10 Feb 2...	Low	
AutoRepeater		☆☆☆		06 Jun 2...	Low	
<b>Authorize</b>		☆☆☆		06 Jun 2...	Low	
Autowasp		☆☆☆		10 Feb 2...	Low	Pro extens...
AWS Security Checks		☆☆☆		18 Jan 2...	Medium	
AWS Signer		☆☆☆		08 Jun 2...	Low	
AWS Sigv4		☆☆☆		03 Aug 2...	Medium	
Backslash Powered ...		☆☆☆		10 Oct 2...	Low	Pro extens...
Backup Finder		☆☆☆		04 Aug 2...	Low	
Batch Scan Report ...		☆☆☆		04 Feb 2...	Low	Pro extens...
BCheck Helper		☆☆☆		02 Nov 2...	Low	Pro extens...
BeanStack - Stack-t...		☆☆☆		04 Feb 2...	Low	Pro extens...
Blazer		☆☆☆		01 Feb 2...	Low	
Blazor Traffic Proce...		☆☆☆		21 Sep 2...	Low	
Bookmarks		☆☆☆		21 May ...	Low	

Refresh list Manual install ...

Memory Low CPU Low Time Low Scanner Low

**Author:** Barak Tawily, AppSec Labs  
**Version:** 1.7  
**Source:** <https://github.com/portswigger/authorize>  
**Updated:** 06 Jun 2023  
**Rating:** ☆☆☆☆☆ Submit rating  
**Popularity:**

**Install**

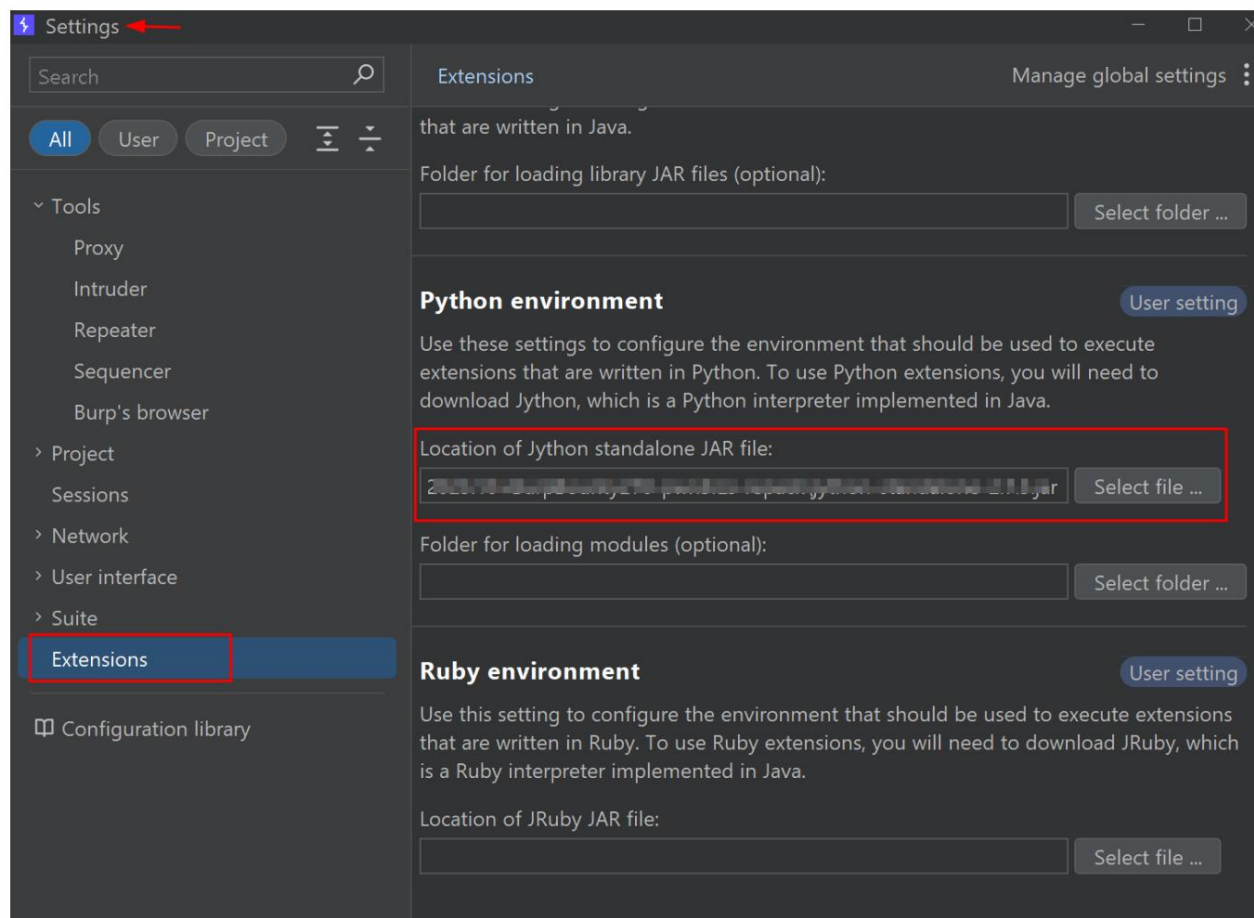
To use Python extensions, you need to download Jython, and configure its location in Burp Extender options.

**Download Jython**

Explore el siguiente enlace y descargue 'Jython Standalone'.

Consulte este enlace: <https://www.jython.org/download.html>

Después de la descarga, vaya a Configuración > Extensión > en el lado derecho del navegador del entorno Python, el archivo Jython. Este entorno se ha configurado correctamente para Jython.



Reinicie el programa Burp y siga esta ruta para instalar Authorize en BApp Store. Notarás que el botón de instalación está resaltado. Puedes hacer clic en él e instalarlo.

## Autorize

Autorize is an extension aimed at helping the penetration tester to detect authorization vulnerabilities. It is sufficient to give to the extension the cookies of a low privileged user and navigate the website with the extension and detects authorization vulnerabilities.


It is also possible to repeat every request without any cookies in order to detect authentication vulnerabilities.





The plugin works without any configuration, but is also highly customizable, allowing configuration of the extension. It is possible to save the state of the plugin and to export a report of the authorization tests in HTML or CSV format.

The reported enforcement statuses are the following:

1. Bypassed! - Red color
2. Enforced! - Green color
3. Is enforced??? (please configure enforcement detector) - Yellow color

## Estimated system impact

Overall: **Low** 

Memory	CPU	Time	Scanner
 Low	 Low	 Low	 Low


**Author:** Barak Tawily, AppSec Labs

**Version:** 1.7

**Source:** <https://github.com/portswigger/authorize>

**Updated:** 06 Jun 2023

**Rating:** 

**Popularity:** 

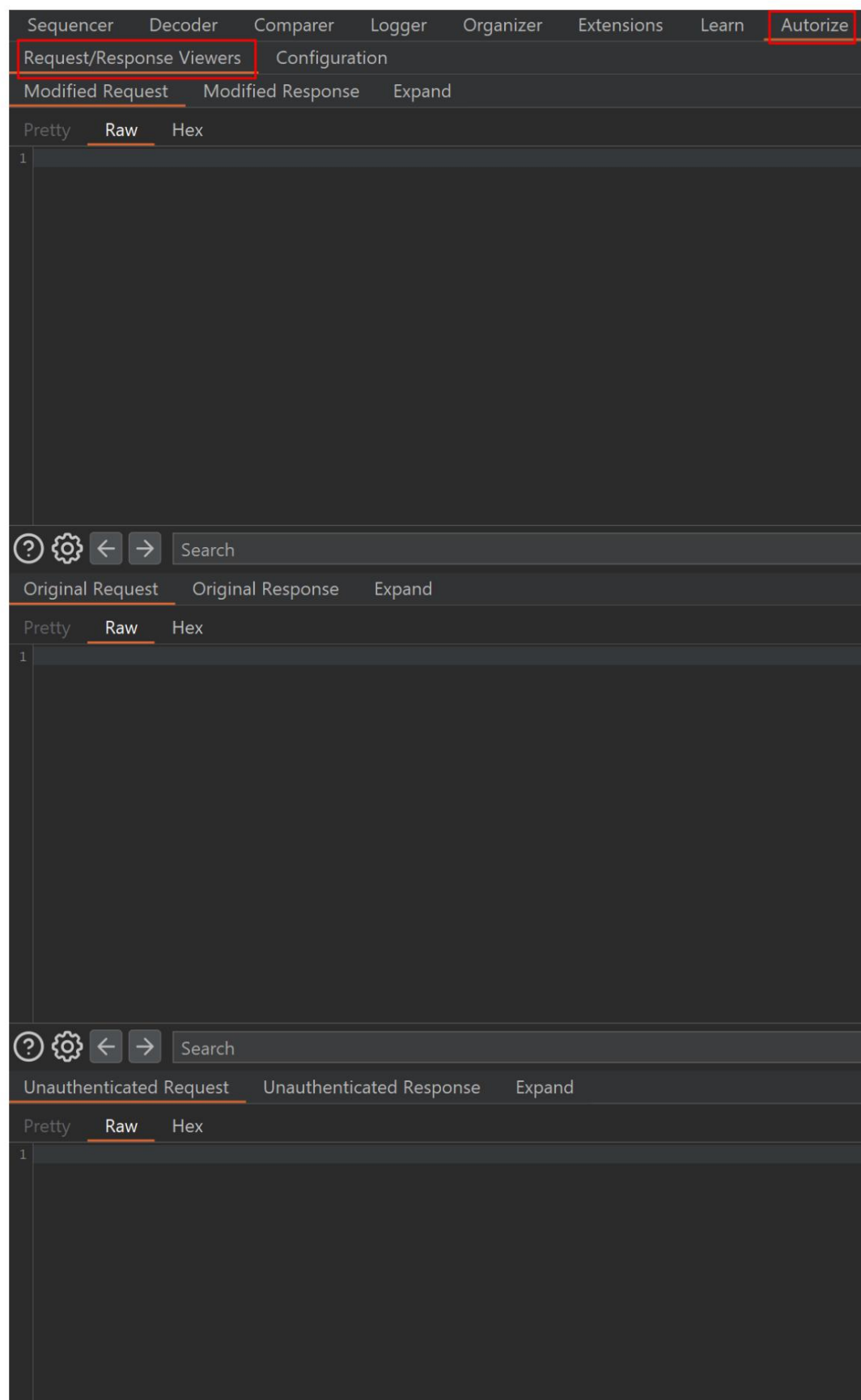
**Install**

La pestaña Autorizar aparecerá en la barra después de una instalación exitosa.

## Opciones de navegación y configuración

Hay dos pestañas en la sección Autorizar, la primera es la pestaña Visores de solicitud/respuesta y la otra es la pestaña Configuración.

Visores de solicitud/respuesta: la pestaña Solicitud/Respuesta mostrará información completa sobre la solicitud particular que capture dentro de Autorizar y elegir. La solicitud manipulada se mostrará en la sección Solicitud modificada, la pestaña Solicitud original mostrará la solicitud original/sin modificar y la solicitud no autenticada mostrará la solicitud sin autenticación.



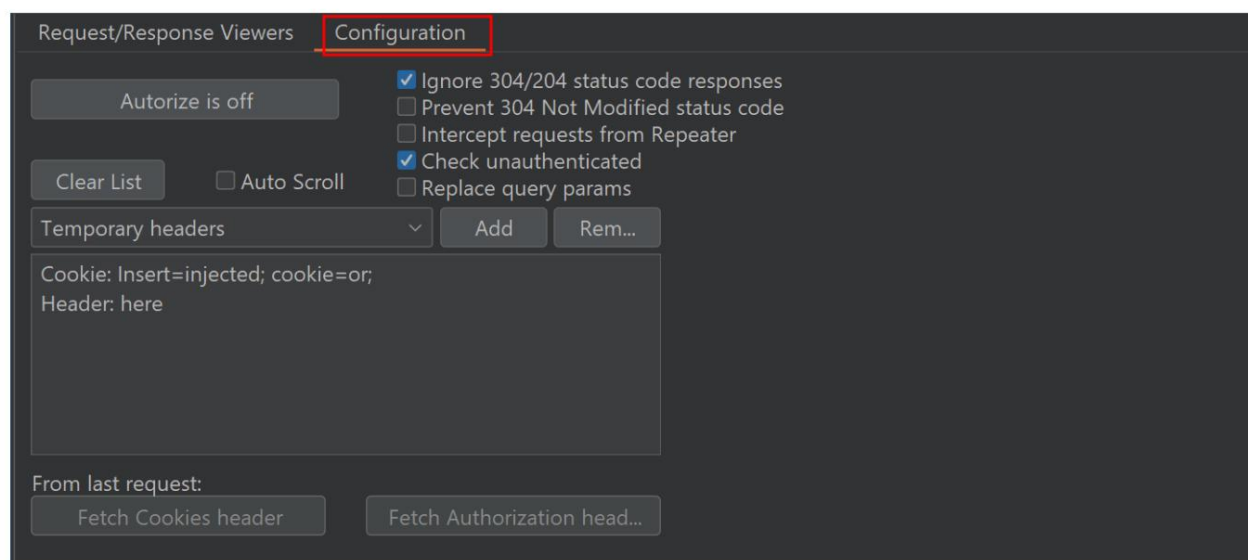


Configuración: en la pestaña de configuración verá que Autorizar está desactivado de forma predeterminada; cuando esté listo para capturar la solicitud, primero active Autorizar. También hay algunas configuraciones para capturar una solicitud y un código de estado del servidor. Dependiendo de tu preferencia, puedes seleccionarlo.

Aquí, debajo del cuadro Encabezado temporal; debe colocar el valor normal del token de usuario/cookies/encabezado que desea reemplazar dentro de la solicitud real, es decir, si alguna aplicación utiliza un token JWT para el mecanismo de autenticación, debe colocar ese valor aquí.

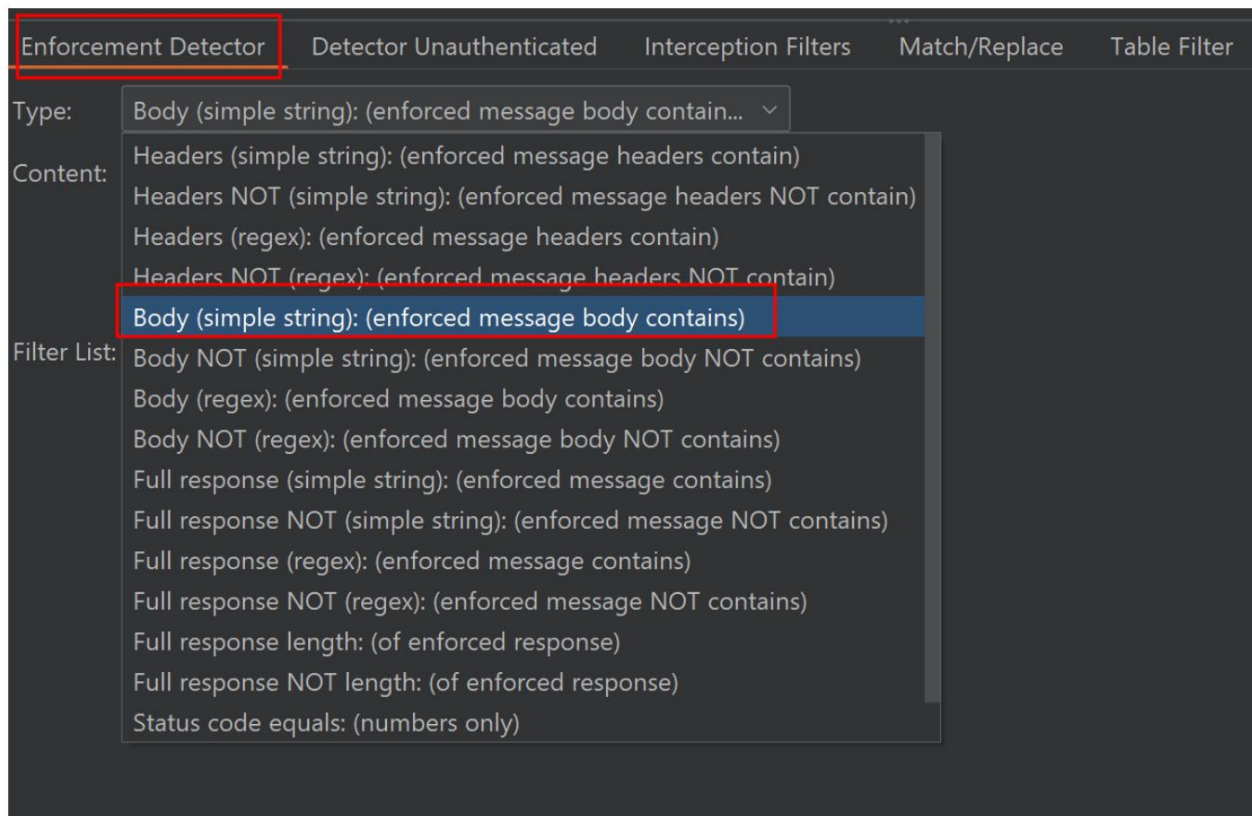
Puede agregar manualmente el valor de autenticación o debajo está la opción para recuperarlo de la última solicitud. Si desea agregar el encabezado de cookies de la última solicitud, haga clic en 'Obtener encabezado de cookies' o si desea agregar encabezado de autorización: haga clic en 'Obtener encabezado de autorización'.

Generalmente, las cookies de sesión se encuentran en el encabezado de cookies y el token de autenticación en el encabezado de autorización.



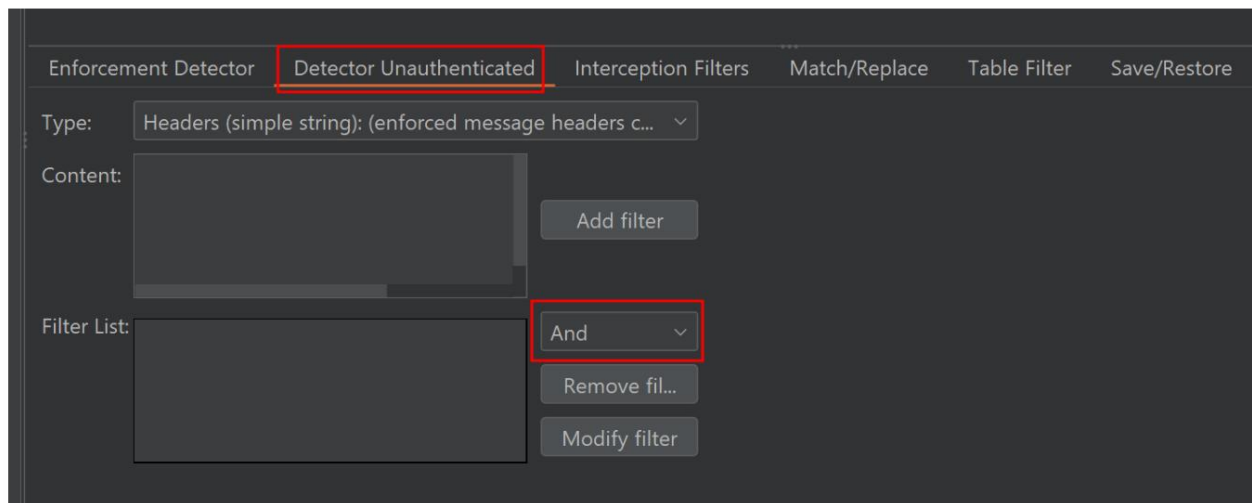
Una vez cargadas las cookies de sesión, es fundamental indicar a Authorize qué solicitudes interceptar y establecer el comportamiento estándar de la aplicación cuando se trata de solicitudes no autorizadas o con permisos insuficientes.

Comenzando con el Detector de cumplimiento, ingrese una característica de la respuesta de la aplicación que se puede anticipar cuando un usuario con privilegios limitados intenta realizar una acción para la que carece de permisos suficientes. En mi práctica, descubrí que utilizar la opción "Cuerpo (cadena simple): el cuerpo del mensaje obligatorio contiene" es la opción más sencilla de configurar y funciona de manera efectiva. Elija el tipo y el contenido que se ajuste a sus necesidades específicas y recuerde hacer clic en el botón "Agregar filtro".

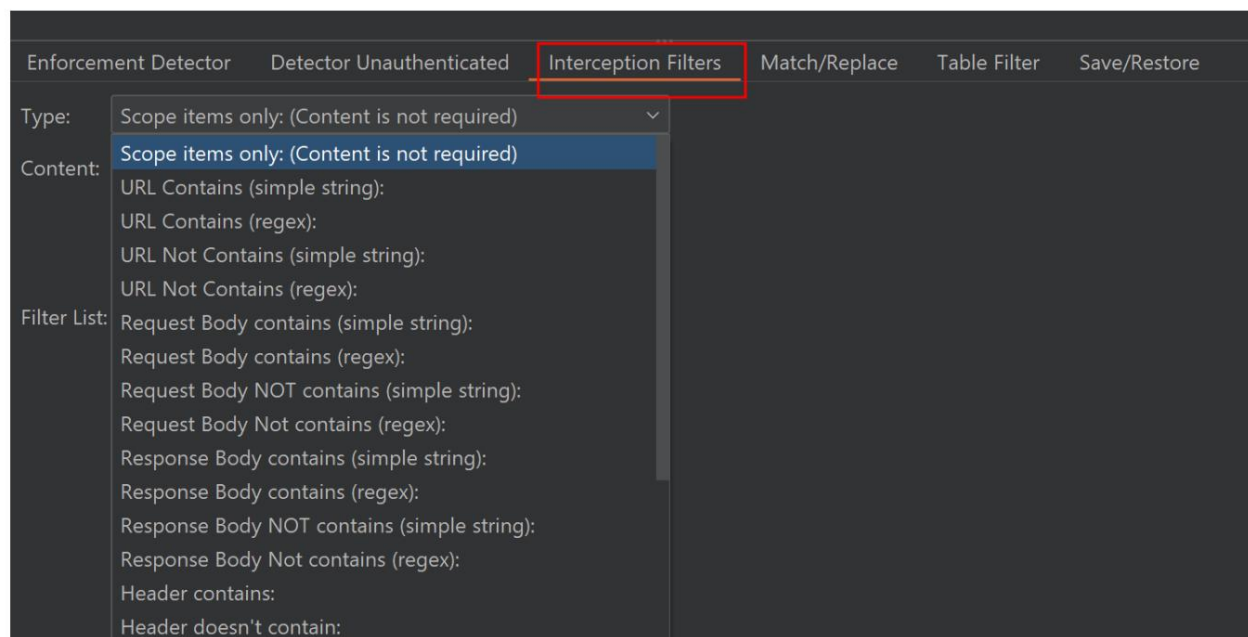


Además, es necesario comprender que establece automáticamente la comparación predeterminada en "Y" al evaluar múltiples filtros. Por lo tanto, si la aplicación genera mensajes de error distintos, como uno al intentar leer un archivo y otro al intentar acceder a funciones administrativas, debe crear un filtro para cada escenario y cambiar "Y" por "O".

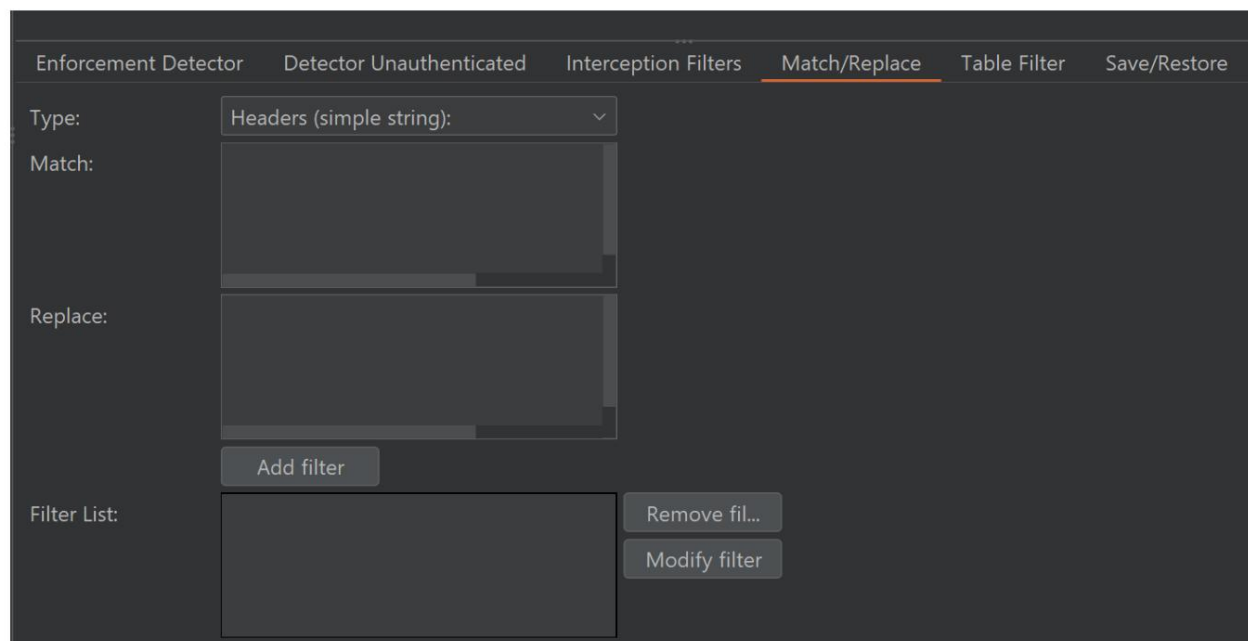
Siga el mismo procedimiento para el detector no autenticado.



El filtro de interceptación interceptará "solo elementos de alcance" independientemente del contenido y, a partir de esas solicitudes, ignorará las solicitudes de araña y las URL que contengan extensiones de imágenes. Puede seleccionar su preferencia y hacer clic en "Agregar filtro" cuando seleccione el tipo.

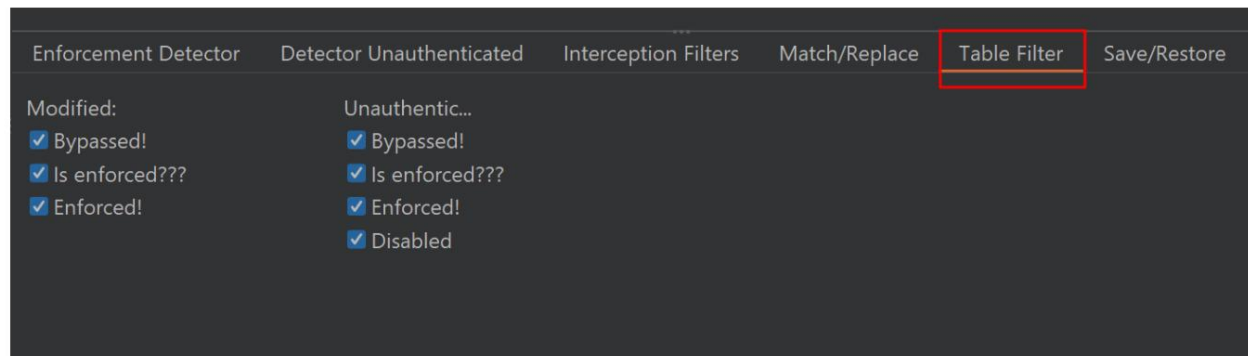


Esta es otra característica adicional de Coincidir/Reemplazar. Puede seleccionarlo desde este sitio si necesita cambiar algún encabezado o parámetro de cuerpo específico en la solicitud de Autorizar. Supongamos que hay un nombre de parámetro 'u.name' en el cuerpo de la solicitud y debe reemplazarse por un EID de administrador, es decir: = "a.name") para evitar el acceso adecuado. Puede informarle a Autorizar agregando aquí.

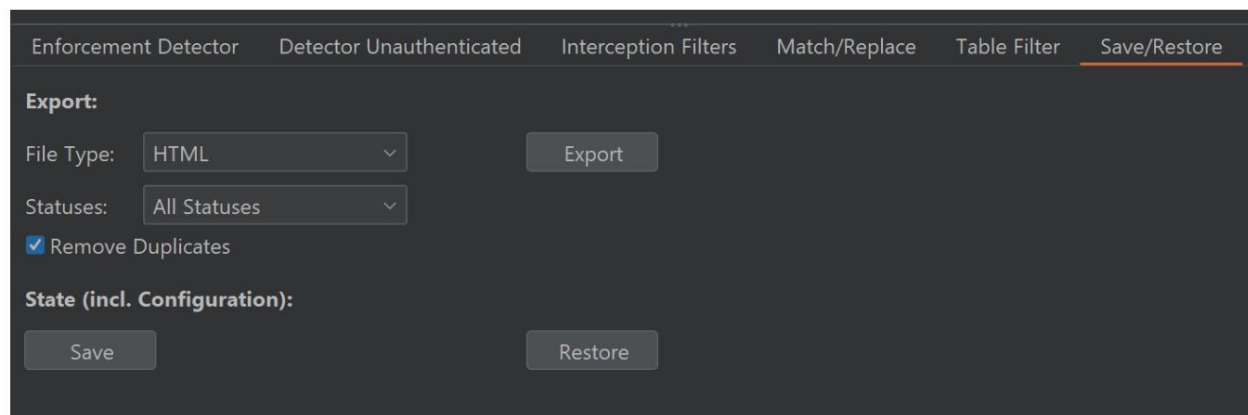


Puede seleccionar el tipo de solicitudes que desea ver en la barra Filtro de tabla,

- ¡omitido!: el punto final puede ser vulnerable a IDOR, • ¡Se aplica!: el punto final parece estar protegido, pero vuelva a verificarlo una vez, • ¡Aplicando!: contra IDOR, el punto final está claramente protegido.



Puede guardar y exportar los datos para su posterior análisis en la pestaña Guardar/Restaurar.



## Demostración práctica de Autorize en acción

Hagamos una demostración rápida para entenderlo de una manera fácil, para realizar esta práctica vamos a utilizar un laboratorio de Port Swigger preconfigurado "El control de acceso basado en métodos se puede eludir". Haga clic en acceder al laboratorio y explore la aplicación.

Esto mostrará una vulnerabilidad de control de acceso roto con dos usuarios que tienen diferentes roles, usuarios con privilegios más altos y más bajos. El mismo concepto se puede aplicar a usuarios del mismo nivel.

The screenshot shows a web browser window with a table of HTTP requests in the background and a web page in the foreground. The table lists several GET requests to various URLs, all with a status code of 200. The web page has a header with 'Home | My account' and a main section titled 'WE LIKE TO SHOP' with a hanger icon. Below this, there are four images: a green leaf, a red flower, a cartoon character, and a silhouette of a person.

Host	Method	URL	Params	Status code	Length	MIME type	Tit
https://0aa000f3040eb...	GET	/academyLabHeader		101	147		
https://0aa000f3040eb...	GET	/		200	10810	HTML	Method-bas
https://0aa000f3040eb...	GET	/resources/images/sho...		200	7258	XML	
https://0aa000f3040eb...	GET	/resources/labheader/i...		200	8852	XML	
https://0aa000f3040eb...	GET	/resources/labheader/i...		200	942	XML	
https://0aa000f3040eb...	GET	/resources/labheader/j...		200	987	script	

Method-based access control ca x +

https://0aa000f3040eb78c86a1cae2004300d4.web-security-academy.net

Home | My account

WE LIKE TO SHOP

Primero, tenemos que capturar las cookies para usuarios con pocos privilegios (usuario normal). Estamos utilizando las credenciales de usuario normales predeterminadas,

viénés: pedro

E inició sesión en la aplicación para capturar la cookie de sesión.



← → ↻ <https://0aa000f3040eb78c86a1cae2004300d4.web-security-academy.net/login>

# Web Security Academy

## Method-based access control can be circumvented

[Back to lab description](#) >>

---

### Login

Username

Password

[Log in](#)

Se actualizaron algunos detalles más.



## Method-based access control can be circumvented

[Back to lab description](#) >>

---

### My Account

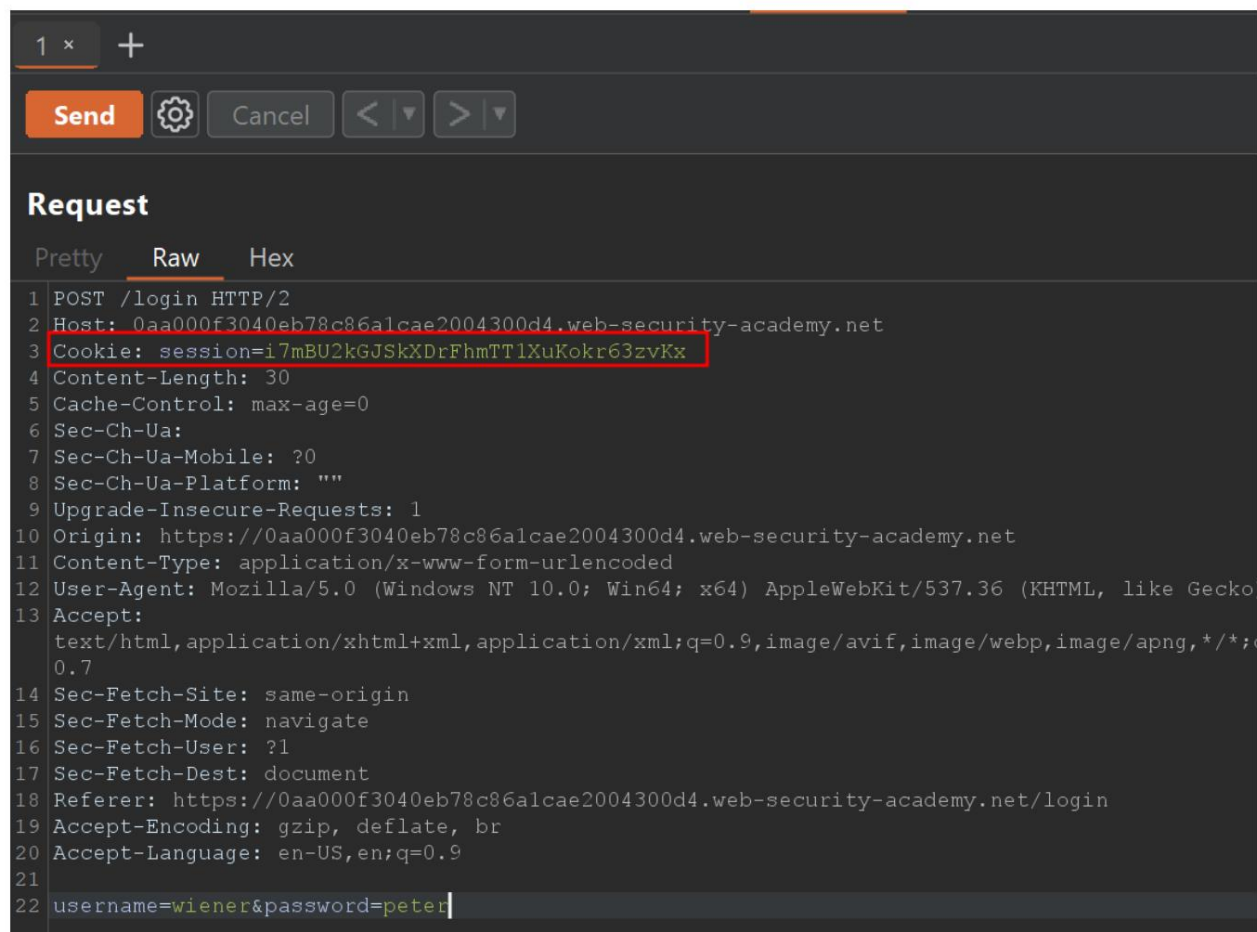
Your username is: wiener

Email

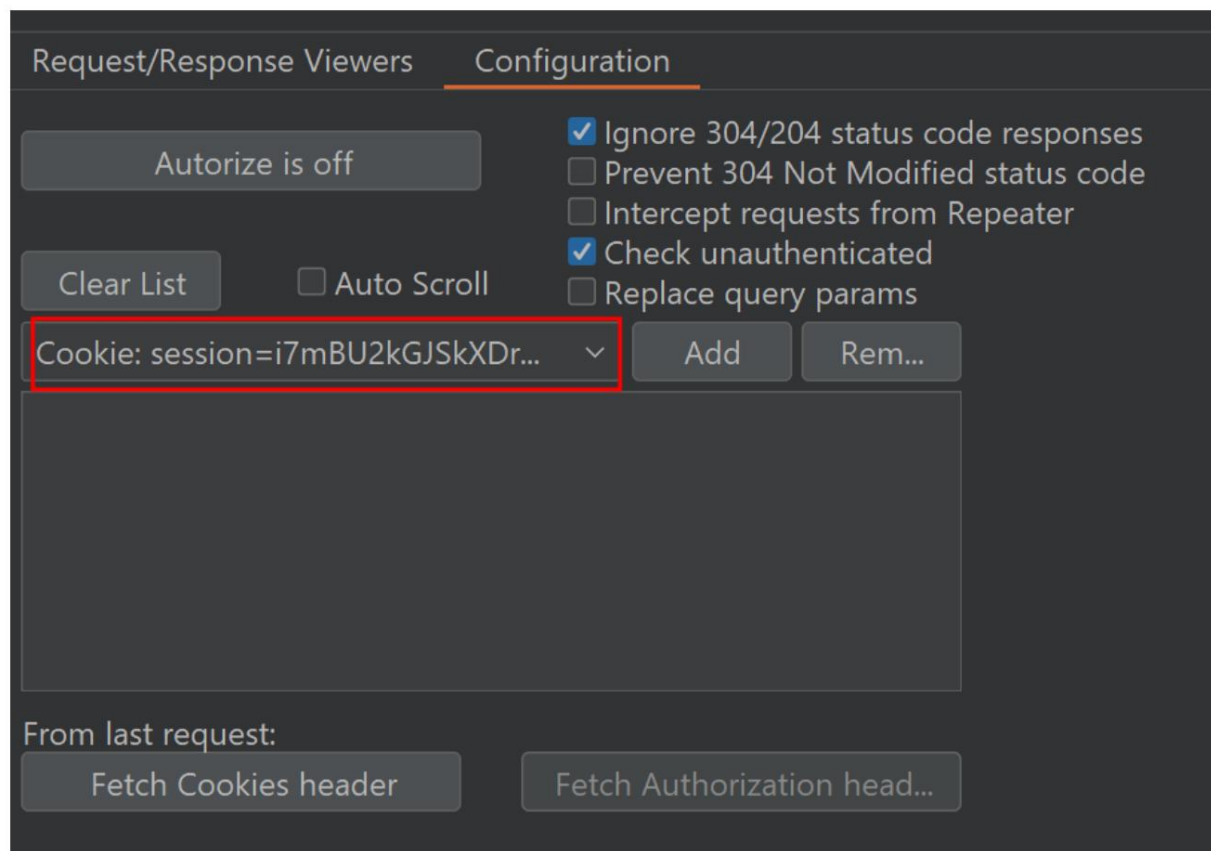
raj@ignitetechnologies.in|

Update email

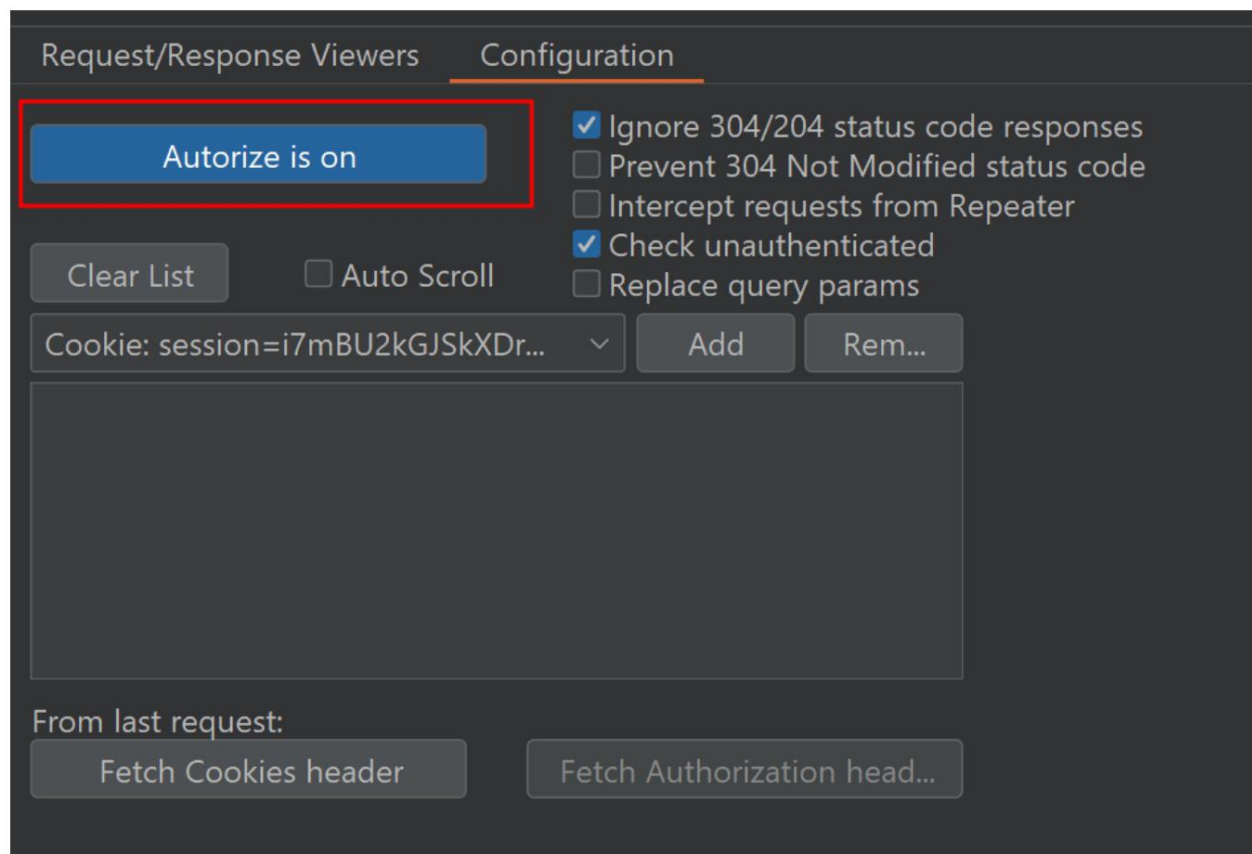
Verá la siguiente cookie de sesión de captura en la solicitud de inicio de sesión. Ahora copie este encabezado de cookie.



Agregue este valor de encabezado de cookie a la pestaña Autorizar como se muestra a continuación,



Y mantén Autorizar activado.



Para verificar la omisión de autenticación, ahora tenemos que iniciar sesión con altos privilegios (usuario administrador). Vaya a la página de inicio de sesión nuevamente y use las credenciales de administrador para iniciar sesión.

Administrador: administrador



 <https://0aa000f3040eb78c86a1cae2004300d4.web-security-academy.net/login>

# Web Security Academy

## Method-based access control can be circumvented

[Back to lab description >>](#)

## Login

Username

Password

Log in

Después de iniciar sesión con éxito y explorar todas las URL exclusivas para administradores. Puede ver en la pestaña Autorizar algunas solicitudes destacadas

La autorización. El estado indica qué puntos finales son accesibles para wiener (usuario normal).

La Unauth. El estado pertenece a usuarios no autorizados, eliminando efectivamente la cookie y todos los encabezados de autorización. Puede optar por desactivar esta función desmarcando la opción "Verificar no autenticado" en la pestaña Autorizar configuración.

Rojo [¡Omitido!] : el punto final podría ser vulnerable a problemas de control de acceso/IDOR.

Naranja [¡Se aplica!] : el punto final parece estar protegido, pero se verifica manualmente reemplazando el valor de las cookies.

Verde [¡Aplicado!] : el punto final está claramente protegido contra problemas de control de acceso/IDOR.

...	...	URL	...	...	...	Authz. Status	Unauth. Status
1	...	https://0aa000f3040eb78c86a1cae2004300d4.web-security-academy.net:443/login	0	0	0	Bypassed!	Bypassed!
2	...	https://0aa000f3040eb78c86a1cae2004300d4.web-security-academy.net:443/my-account?id=administrator	...	...	...	Bypassed!	Bypassed!
3	...	https://0aa000f3040eb78c86a1cae2004300d4.web-security-academy.net:443/academyLabHeader	0	...	...	Enforced!	Enforced!
4	...	https://0aa000f3040eb78c86a1cae2004300d4.web-security-academy.net:443/admin	...	...	...	Bypassed!	Bypassed!
5	...	https://0aa000f3040eb78c86a1cae2004300d4.web-security-academy.net:443/academyLabHeader	0	...	...	Enforced!	Enforced!
6	...	https://0aa000f3040eb78c86a1cae2004300d4.web-security-academy.net:443/admin-roles	0	0	0	Bypassed!	Bypassed!
7	...	https://0aa000f3040eb78c86a1cae2004300d4.web-security-academy.net:443/admin	...	...	...	Bypassed!	Bypassed!
8	...	https://0aa000f3040eb78c86a1cae2004300d4.web-security-academy.net:443/academyLabHeader	0	...	...	Enforced!	Enforced!
9	...	https://0aa000f3040eb78c86a1cae2004300d4.web-security-academy.net:443/admin-roles	0	0	0	Bypassed!	Bypassed!
...	...	https://0aa000f3040eb78c86a1cae2004300d4.web-security-academy.net:443/admin	...	...	...	Bypassed!	Bypassed!
...	...	https://0aa000f3040eb78c86a1cae2004300d4.web-security-academy.net:443/academyLabHeader	0	...	...	Enforced!	Enforced!

Como se ve en la imagen de arriba, las solicitudes 1, 2, 6 y 7 tienen un problema de control de acceso roto.

Tenga en cuenta que no siga ciegamente el resultado de Autorizar. Las solicitudes resaltadas en rojo no significan que todos los puntos finales sean vulnerables o se omitan. Puede haber falsos positivos; Debes hacer una verificación cruzada.

Algunos otros escenarios posibles. Supongamos que está probando problemas de autenticación con dos usuarios del mismo nivel. Como resultado, verá Authz. El estado muestra ¡Omitido! Y Unaut. El estado muestra ¡Aplicado! En ese caso, se puede encontrar una autorización incorrecta en la solicitud que muestra que el 2 puede acceder al punto final específico.

— usuario pero ha implementado correctamente la autorización para cualquier usuario no autorizado.

Al seleccionar cualquier solicitud resaltada, en el lado derecho verá la información detallada sobre Solicitudes y respuestas modificadas, originales y no autenticadas.

Organizer Extensions Learn Authorize

Request/Response Viewers Configuration

Modified Request Modified Response Expand

Pretty Raw ex

```

1 POST /my-account/change-email HTTP/2
2 Host: 0a2000f4041f53818018353200cb00fd.web-security-academy.net
3 Content-Length: 34
4 Cache-Control: max-age=0
5 Sec-Ch-Ua:
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: ""
8 Upgrade-Insecure-Requests: 1
9 Origin: https://0a2000f4041f53818018353200cb00fd.web-security-academy.net
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: https://0a2000f4041f53818018353200cb00fd.web-security-academy.net/my-ac
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Cookie: session=e02BUCQvmsEIqb87XJBCiACSHSdXd9Yf
21

```

? ⚙️ ⬅️ ➡️ Search

Original Request Original Response Expand

Pretty Raw Hex

```

1 POST /my-account/change-email HTTP/2
2 Host: 0a2000f4041f53818018353200cb00fd.web-security-academy.net
3 Cookie: session=dxqZCSrDns2hw10FoRl866ROgo4Gv6Cb
4 Content-Length: 34
5 Cache-Control: max-age=0
6 Sec-Ch-Ua:
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: ""
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0a2000f4041f53818018353200cb00fd.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://0a2000f4041f53818018353200cb00fd.web-security-academy.net/my-ac
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: en-US,en;q=0.9
21

```

? ⚙️ ⬅️ ➡️ Search

Unauthenticated Request Unauthenticated Response Expand

Pretty Raw Hex

```

1 POST /my-account/change-email HTTP/2
2 Host: 0a2000f4041f53818018353200cb00fd.web-security-academy.net
3 Content-Length: 34
4 Cache-Control: max-age=0
5 Sec-Ch-Ua:
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: ""
8 Upgrade-Insecure-Requests: 1
9 Origin: https://0a2000f4041f53818018353200cb00fd.web-security-academy.net
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: https://0a2000f4041f53818018353200cb00fd.web-security-academy.net/my-ac
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20
21 email=rrai340ignitetechnologies.in

```

? ⚙️ ⬅️ ➡️ Search

Eso es todo por ahora. ¡Salud!

## Conclusión

Para realizar revisiones de seguridad integrales, la extensión "Authorize Burp" es una herramienta esencial. Al automatizar la autenticación y permitir la prueba de áreas restringidas, mejora la eficiencia y eficacia de las evaluaciones de seguridad. Esta extensión es una herramienta indispensable para realizar pruebas exhaustivas e identificar posibles vulnerabilidades a las que solo pueden acceder usuarios autenticados.

# ÚNETE A NUESTRO PROGRAMAS DE ENTRENAMIENTO

