

Articles sur le piratage

Le blog de Raj Chandel

Menu

🏠 Maison » Piratage de sites Web » Burpsuite pour Pentester : Autoriser

[Piratage de sites Web](#)

Burpsuite pour Pentester : Autoriser

22 Janvier 2024 Par Raj

Afin de protéger les actifs en ligne, les tests de sécurité des applications Web sont un élément essentiel de leur sauvegarde. Burp Suite est un leader dans ce domaine depuis de nombreuses années et est toujours utilisé par les professionnels de la sécurité ainsi que par les pirates éthiques. L'une de ces extensions qui se démarque dans la communauté des tests de sécurité Web est « Autorize », qui est dotée d'une grande variété de fonctionnalités supplémentaires pour améliorer ses capacités. Un ensemble puissant de fonctionnalités qui simplifient le processus de test d'authentification et d'autorisation est disponible avec cette extension.

Autoriser = Authentifier + Autoriser

L'autorisation inclut toute méthode par laquelle un système accorde ou révoque l'autorisation d'accéder à des données ou à des actions spécifiques. Pendant ce temps, l'authentification est un processus par lequel un individu ou un système s'authentifie comme étant celui qu'il prétend être.

- Vulnérabilités courantes détectées par Autorize
- Comprendre la fonctionnalité
- Installation et configuration
- Options de navigation et de configuration
- Démonstration pratique d'Autorize en action

Vulnérabilités courantes détectées par Autorize



Il se concentre principalement sur l'identification des vulnérabilités liées aux autorisations. Cela peut aider à identifier certains des principaux types de vulnérabilités, tels que :

- **Contrôle d'accès basé sur les rôles inadéquat (RBAC)** : il peut révéler des problèmes dans lesquels les rôles ou les autorisations des utilisateurs ne sont pas correctement appliqués, permettant aux utilisateurs d'accéder à des fonctionnalités ou à des données auxquelles ils ne devraient pas avoir accès.
- **Contrôles d'accès brisés** : il peut identifier les cas où les contrôles d'accès ne sont pas correctement mis en œuvre, conduisant à un accès non autorisé aux ressources ou aux actions.
- **Références d'objet directes non sécurisées (IDOR)** : il peut trouver des situations dans lesquelles les attaquants peuvent manipuler les entrées pour accéder aux données d'autres utilisateurs ou effectuer des actions qu'ils ne devraient pas pouvoir faire.
- **Navigation forcée** : elle peut aider à identifier les cas dans lesquels un attaquant peut accéder directement à des zones restreintes de l'application en manipulant les URL.
- **Autorisation insuffisante** : il peut détecter des situations dans lesquelles les rôles ou les autorisations des utilisateurs ne sont pas correctement appliqués, permettant ainsi l'exécution d'actions non autorisées.
- **Escalade des privilèges horizontaux et verticaux** : il peut détecter des vulnérabilités qui permettent aux attaquants d'élever leurs privilèges au sein de l'application, soit en se faisant passer pour d'autres utilisateurs, soit en obtenant des autorisations supplémentaires.
- **Faibles de logique métier** : Autorize peut découvrir des vulnérabilités de logique métier, où les flux de travail des applications peuvent être manipulés de manière involontaire, conduisant potentiellement à des actions non autorisées ou à une exposition de données.

N'oubliez pas que l'efficacité d'Autorize dépend de la qualité de sa configuration et de la réalisation de vos tests.

Comprendre le fonctionnement d'Autorize

Comprenons comment fonctionne Autorize. Supposons, par exemple, qu'une application Web implémente des rôles basés sur les utilisateurs et prenne en charge l'authentification basée sur les cookies.

Utilisateur normal : a accès aux fonctionnalités générales mais n'est pas autorisé à accéder aux fonctions d'administration et à la base de données (accès en lecture seule).

Utilisateur administrateur : a accès à toutes les fonctionnalités (accès en lecture/écriture)

Capturez les cookies utilisateur normaux et ajoutez-les à Autoriser. Reconnectez-vous avec l'utilisateur administrateur, accédez à toutes les fonctionnalités d'administration et mettez à jour certaines données dans la base de données.

Que va faire Autorize maintenant ? Autorize capture toutes les demandes et remplace le cookie de l'administrateur par les cookies de votre utilisateur normal lorsque vous naviguez dans une application, puis les envoie au serveur. Consultez la réponse du serveur, si le serveur se comporte de la même manière qu'un administrateur légitime (comme 200 OK en réponse) et qu'aucune erreur n'a été détectée. La demande a été mise en évidence comme un contournement rouge ! Une autre demande s'affiche sous la forme d'un Green Enforced !.

Pour chaque requête envoyée au serveur par un client, celui-ci effectuera un test automatisé. Avec une grande application, avec plus de 30+ pages Web dynamiques, cela va faciliter notre travail. Il y a de nombreuses URL que vous devez tester manuellement, donc Autorize le fera pour vous.

De même, Autorize détecte également un problème de point de terminaison d'API de la même manière. La méthode d'authentification doit être vérifiée pour l'API. Supposons qu'une API utilise un jeton JWT, vous pouvez le contrôler en modifiant son en-tête d'autorisation et en identifiant les problèmes de contournement d'authentification avec les API.

Installation et configuration

Depuis le Bapp Store, vous pouvez télécharger et installer l'extension. Sélectionnez Bapp Store dans Extensions. Vous pouvez rechercher « Autoriser » ou simplement regarder vers le bas. Cliquez dessus, faites défiler vers le côté droit.

L'extension est construite en Python, vous verrez que 'Jython' doit d'abord être installé.

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	
Autorize		☆☆☆		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.

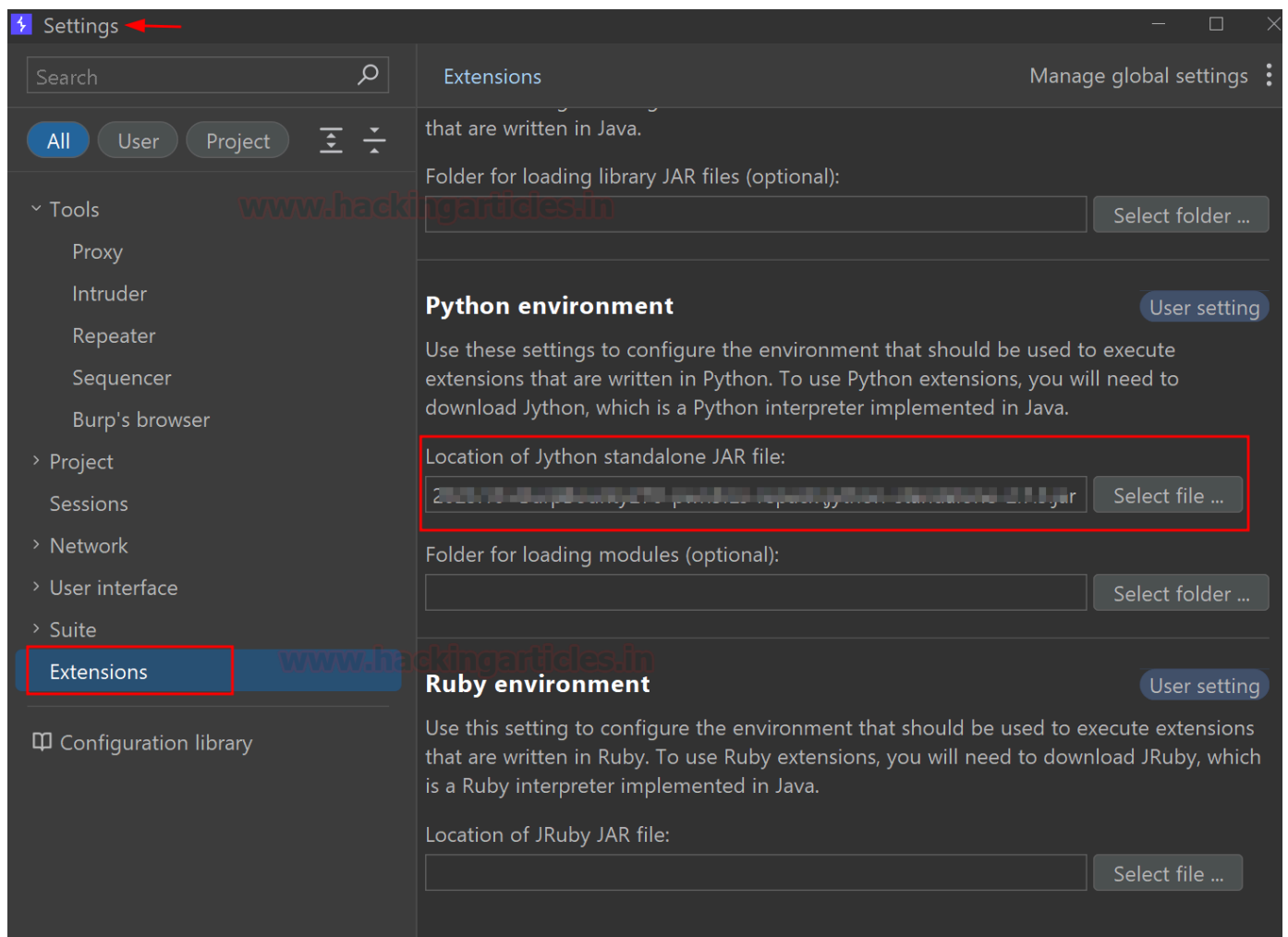
Download Jython

Parcourez le lien ci-dessous et téléchargez « Jython Standalone ».

Référez-vous à ce lien : <https://www.jython.org/download.html>

Après le téléchargement, accédez à Paramètres > Extension > sur le côté droit sous le navigateur de l'environnement Python, le fichier Jython. Cet environnement a été configuré avec succès pour Jython.





Redémarrez le programme Burp et suivez ce chemin pour installer Authorize sur BApp Store. Vous remarquerez que le bouton d'installation est en surbrillance. Vous pouvez cliquer dessus et l'installer.



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 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 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
 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: 

Popularity: 

Install

L'onglet Autoriser apparaîtra dans la barre après une installation réussie.

Options de navigation et de configuration

Il y a deux onglets sous la section Autoriser, le premier est l'onglet Observateurs de requêtes/réponses et l'autre l'onglet Configuration.

Visionneuses de demandes/réponses : l'onglet Demande/Réponse affichera des informations complètes sur la demande particulière que vous capturez dans Autoriser et choisir. La demande manipulée sera affichée sous la section Demande modifiée, l'onglet Demande originale affichera la demande originale/non modifiée et la demande non authentifiée affichera la demande de non-authentification.



SequencerDecoderComparerLoggerOrganizerExtensionsLearnAuthorize

Request/Response ViewersConfiguration

Modified RequestModified ResponseExpand

PrettyRawHex

1

www.hackingarticles.in

?

⚙

⬅

➡

Search

Original RequestOriginal ResponseExpand

PrettyRawHex

1

?

⚙

⬅

➡


Search

Unauthenticated RequestUnauthenticated ResponseExpand

PrettyRawHex

1

⌆

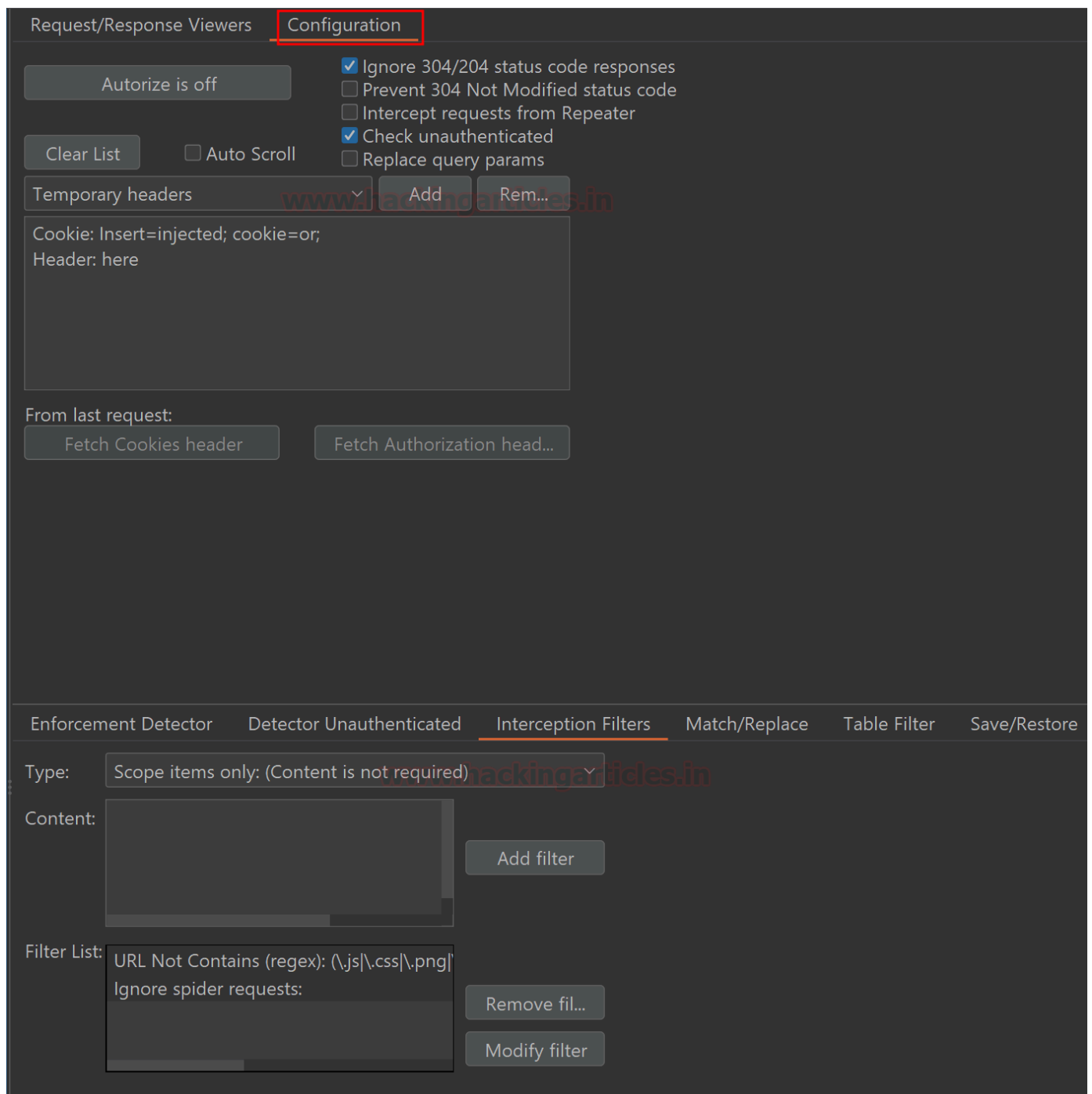


Configuration: Under the configuration tab you will see Authorize is off by default, when you are ready to capture the request first put Authorize on. There are also some configurations for capturing a request and server status code. Depending on your preference, you can select it.

Here, under the Temporary header box; you need to put the normal user token/cookies/header value that you want to replace within the actual request i.e. if any application is using a JWT token for auth mechanism you need to put that value here.

Either you can manually add the auth value or below is the option to fetch it from the last request. If you want to add the cookies header from the last request – click on ‘Fetch Cookies header’ or If you want to add Authorization header – click on ‘Fetch Authorization header’.

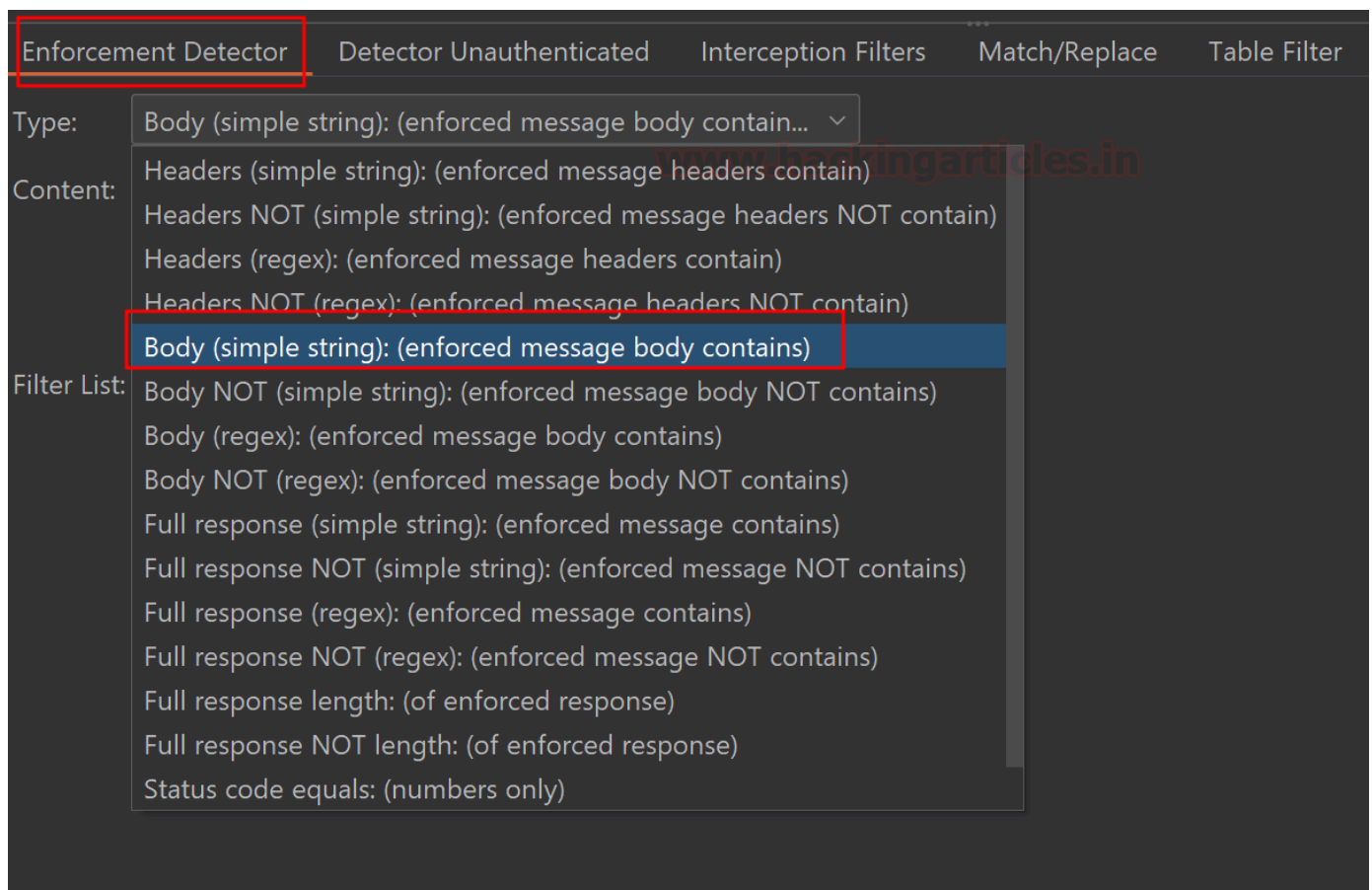
Generally, the session cookies are under Cookies Header and the auth token comes under Authorization Header.



Once the session cookies are loaded, it is essential to instruct Authorize on which requests to intercept and establish the standard behavior for the application when dealing with unauthorized requests or those with insufficient permissions.

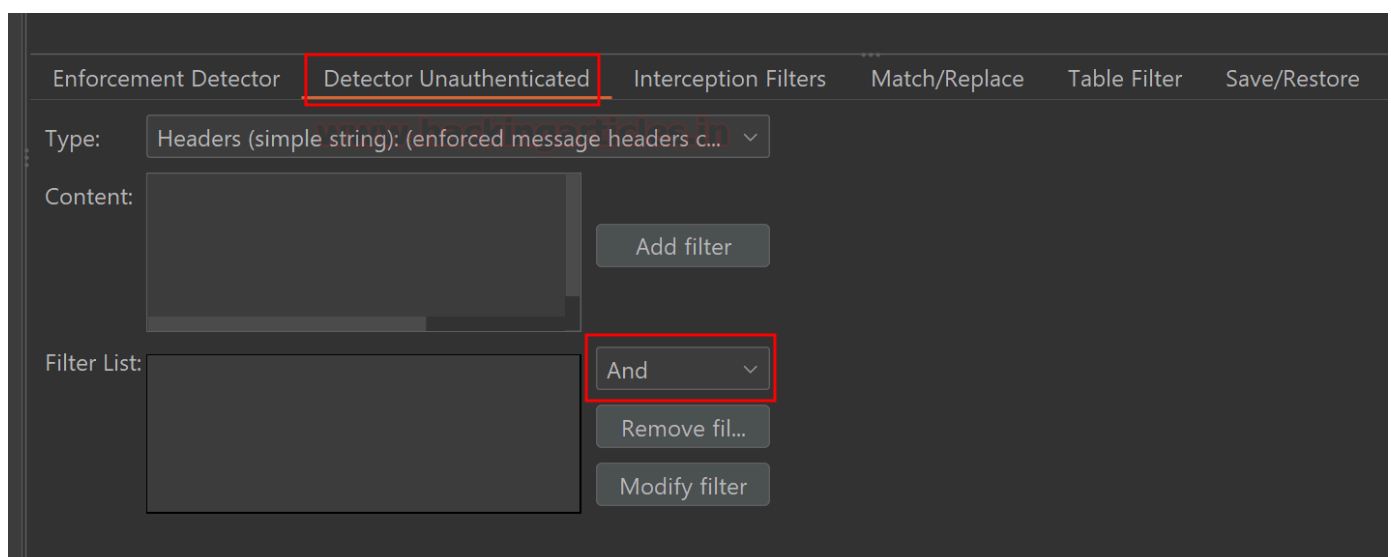
Commencing with the Enforcement Detector, input a characteristic of the application's response that can be anticipated when a user with limited privileges tries to perform an action they lack sufficient permissions. In my practice, I've found that utilizing the "Body (simple string): enforced message body contains" option is the simplest to set up and functions effectively. Choose the type and content that aligns with your specific needs and remember to click the "Add filter" button.





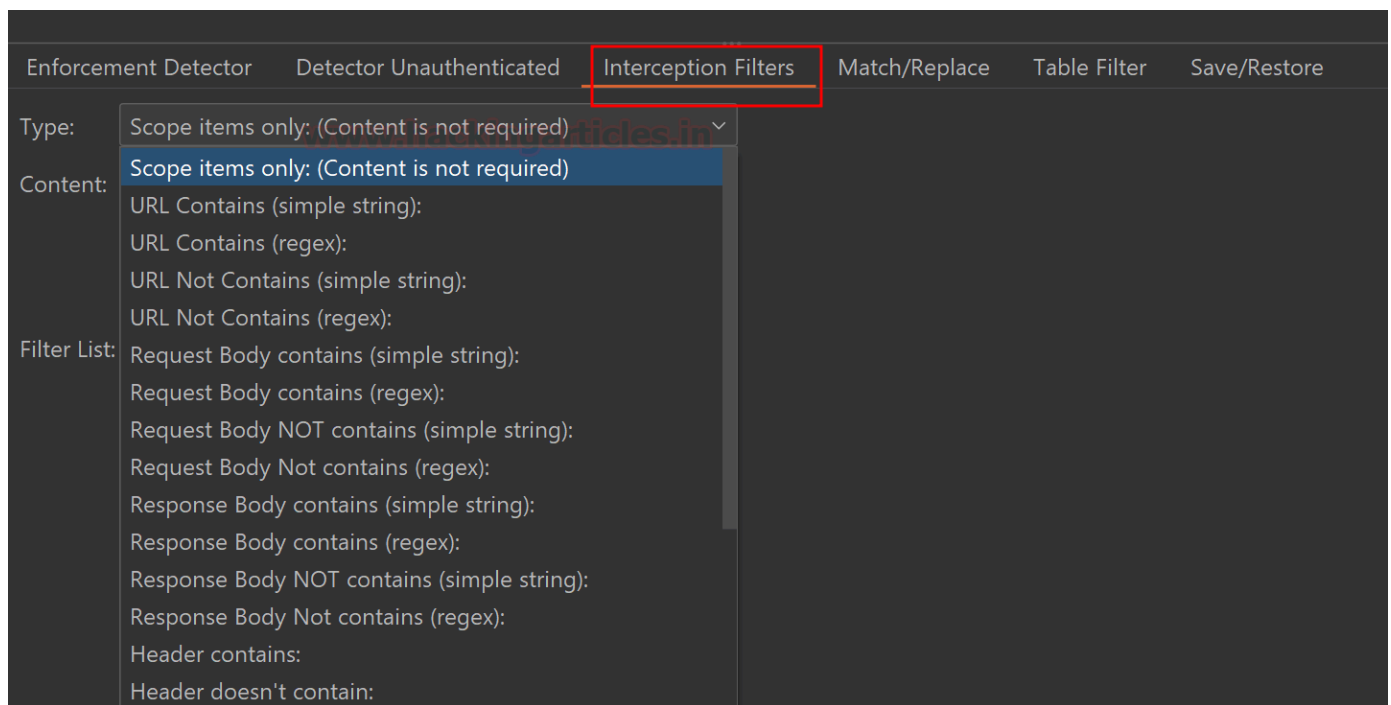
Moreover, it is necessary to understand that it automatically sets the default comparison to “And” when assessing multiple filters. Therefore, if the application generates distinct error messages, such as one for trying to read a file and another for attempting to access administrative features, you should create a filter for each scenario and switch the “And” to “Or.”

Follow the same procedure for the Unauthenticated Detector

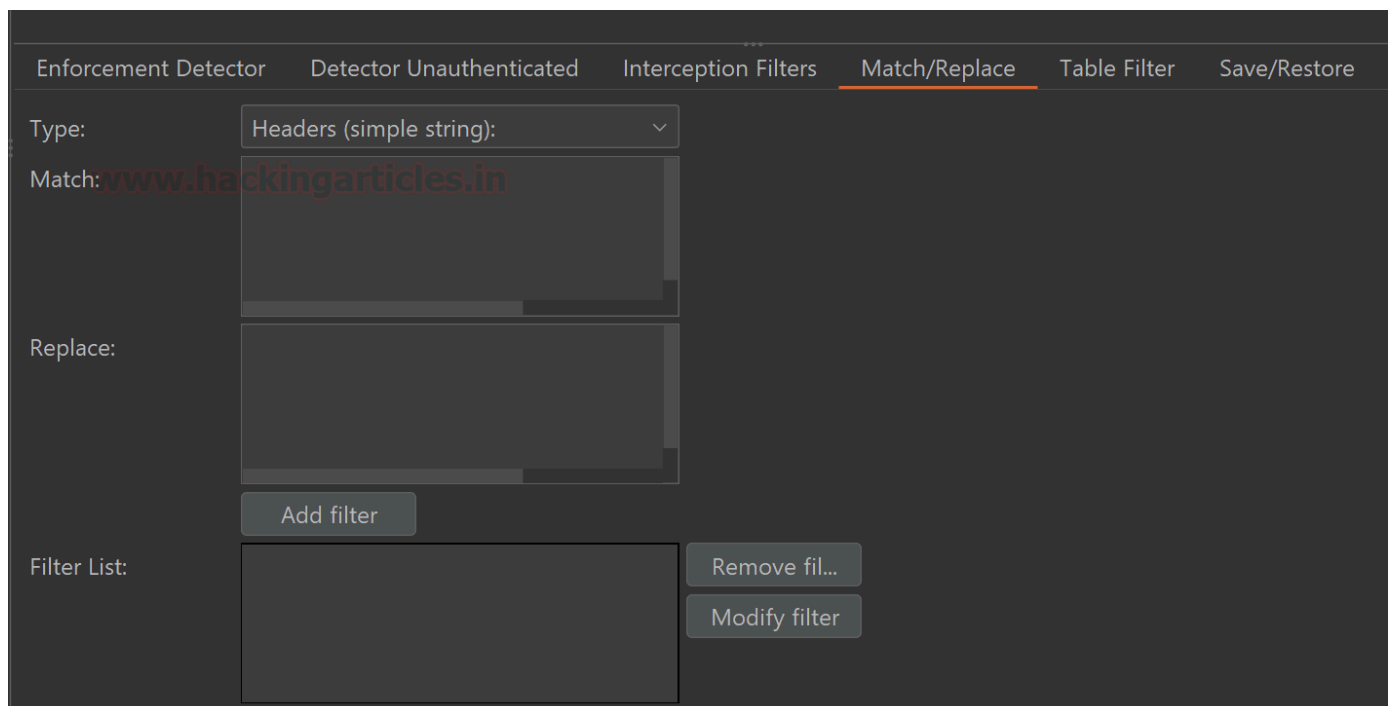


The interception filter will intercept “Scope items only” regardless of content and from those requests, it will ignore spider requests and URLs containing image extensions. You may select on your preference and click “Add filter” when type is selected.





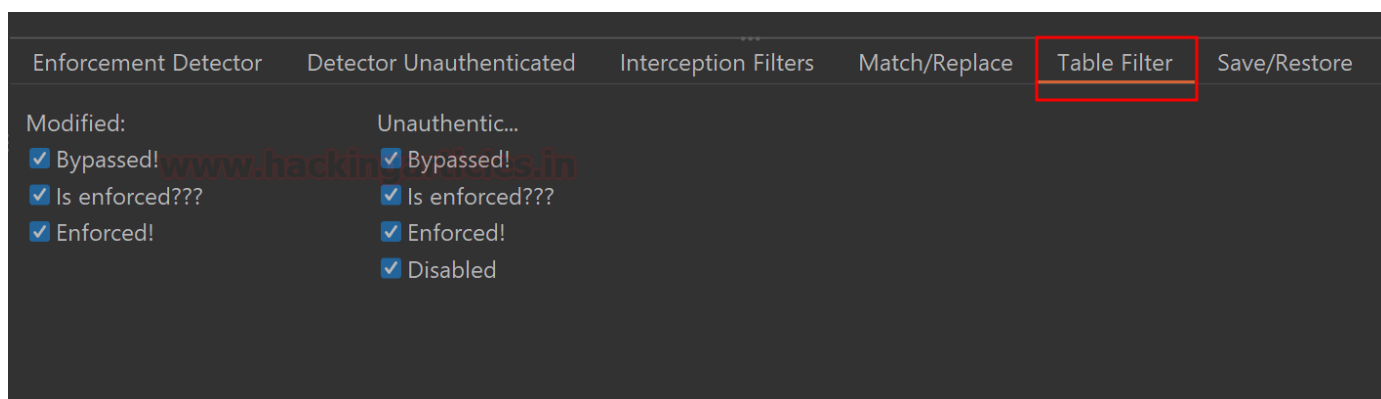
This is another additional feature Match/Replace. You can select it from this site if you need to change any specific header or body parameter on the Authorize request. Suppose there is a parameter name 'u.name' on the request body, and it has to be replaced by an Admin EID (i.e.:="a.name") for proper access circumvention. You can tell Authorize via adding here.



You can select the type of requests that you want to see under the Table Filter bar,

- bypassed!: the endpoint may be vulnerable to IDOR,
- Is enforced!: endpoint seems to be protected but re-check once,
- Enforcing!: against IDOR, the endpoint is clearly protected.





You can save and export the data for further analysis under the Save/Restore tab.

Practical Demonstration of Authorize in Action

Let's do a quick demonstration to understand in an easy way, to perform this practical we are going to use a pre-setup Port Swigger lab "Method-based access control can be circumvented". Click on access the lab and browser the application.

This will show a Broken Access Control vulnerability with two users that have different role higher and lower privilege users. The same concept can be applied to same-level users.

Host	Method	URL	Params	Status code	Length	MIME type	Title
https://0aa000f3040eb...	GET	/academyLabHeader		101	147		
https://0aa000f3040eb...	GET	/		200	10810	HTML	Method-based
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	

First, we have to capture the cookies for low privileged user (normal user). We are using the default normal user credentials,

Wiener:peter

And logged into the application to capture session cookie.



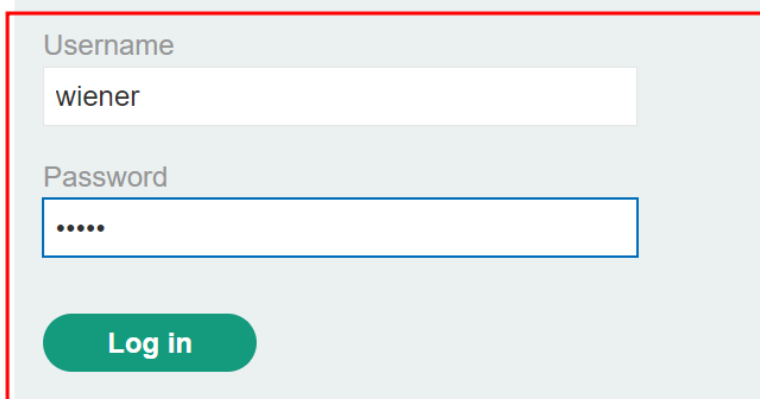
The screenshot shows a web browser with the address bar displaying `https://0aa000f3040eb78c86a1cae2004300d4.web-security-academy.net/login`. A red arrow points to the address bar. The page header features the "Web Security Academy" logo and the title "Method-based access control can be circumvented". Below the title is a link "Back to lab description >>".

Web Security Academy

Method-based access control can be circumvented

[Back to lab description >>](#)

Login



The login form is enclosed in a red rectangular border. It contains two input fields: "Username" with the value "wiener" and "Password" with masked characters "....". Below the fields is a green "Log in" button.

Username

wiener

Password

....

Log in

Updated some more details.



My Account

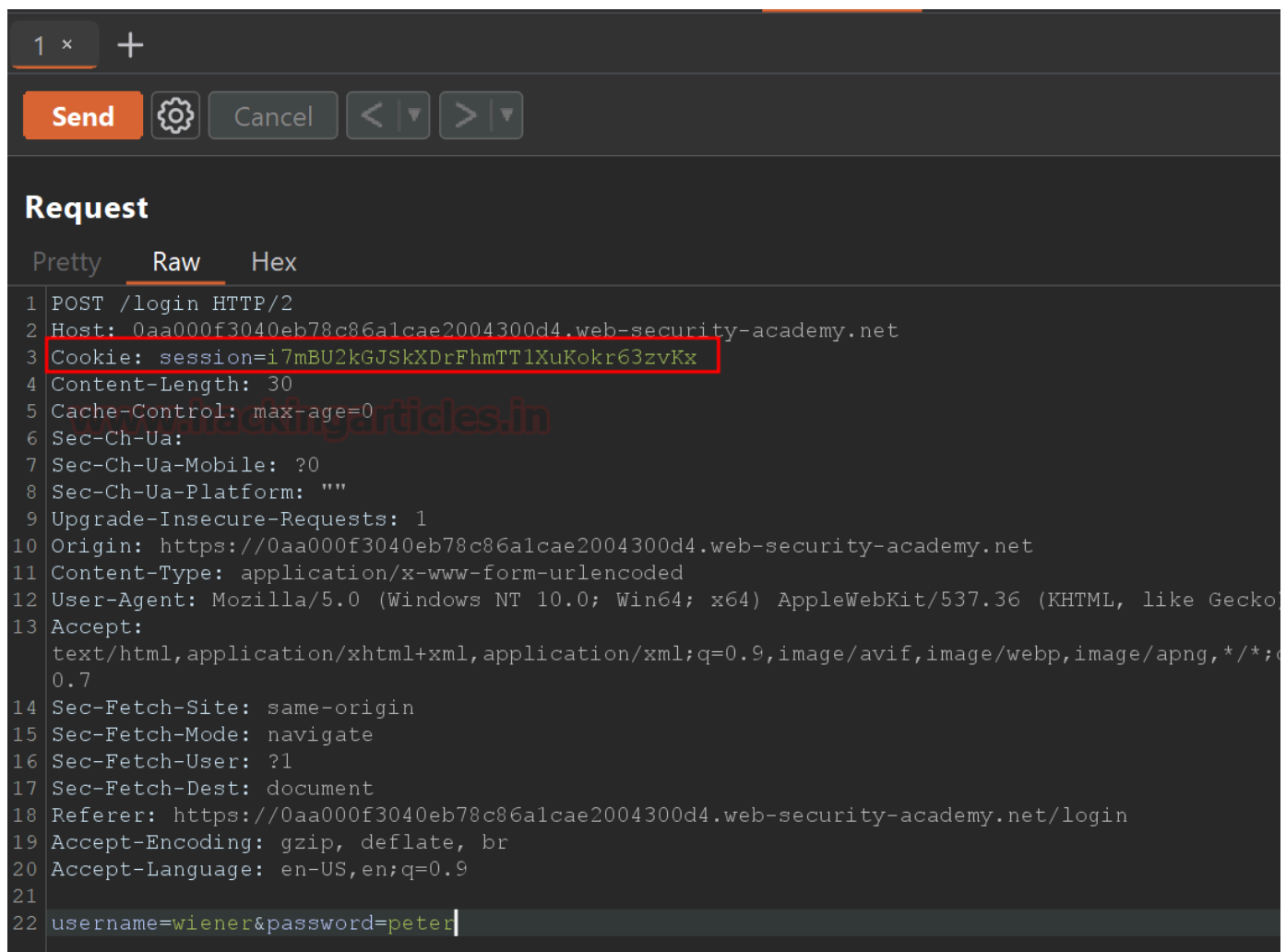
Your username is: wiener

Email

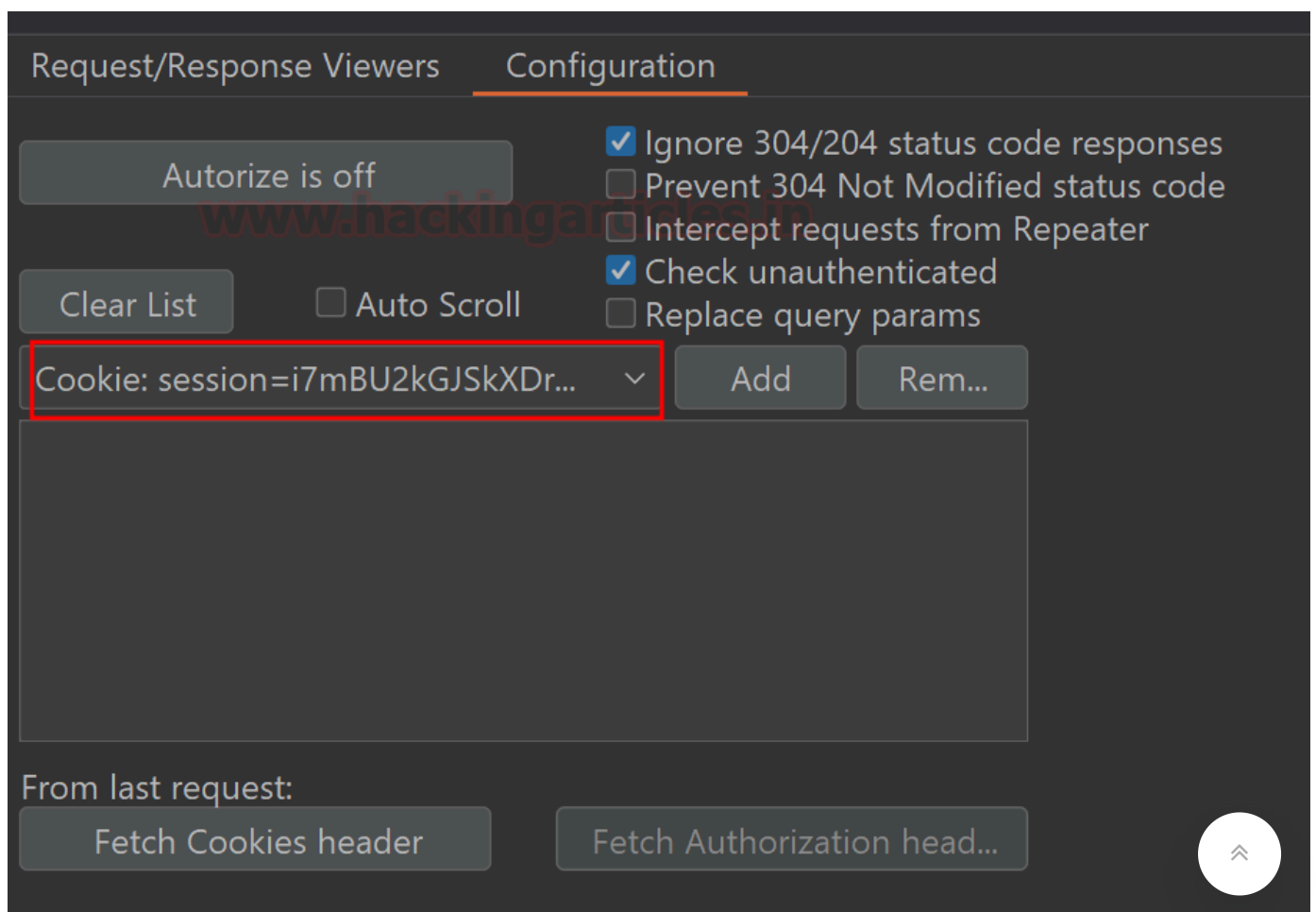
raj@ignitetechnologies.in|

Update email

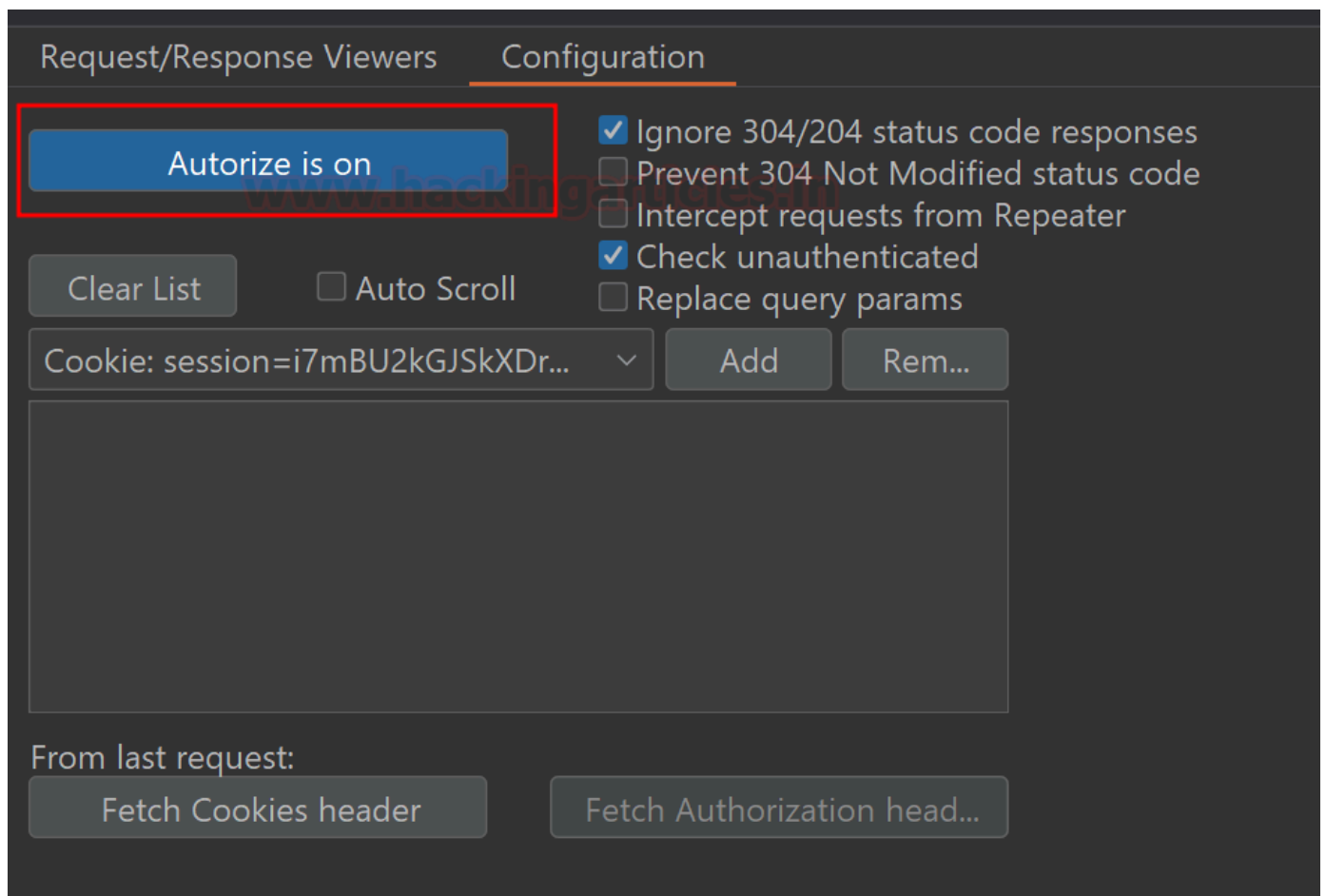
You will see the below capture session cookie in to the login request. Now copy this cookie header.



Add this cookie header value to Authorize tab as shown below,



And keep Authorize on.



In order to, check the auth bypass now we have to log in with high privilege (admin user). Go to login page again and use admin credentials to log in,

Administrator:admin

Login

Username

administrator

Password

.....

Log in

After successfully logging in and browsing the all admin-only URLs. You can see under the Authorize tab some highlighted requests

The **Authz. Status** indicates which endpoints are accessible to wiener (normal user).

The **Unauth. Status** pertains to unauthorized users, effectively eliminating the cookie and all authorization headers. You can opt to disable this feature by deselecting the “Check unauthenticated” option in the Authorize configuration tab.

Red [Bypassed!] : endpoint could be vulnerable to access control/IDOR issues.

Orange [Is enforced!] : endpoint seems to be protected but cross-check manually by replacing the cookies value.

Green [Enforced!] : endpoint is clearly protected against access control/IDOR issues.

...	...	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!

As visible in above image, request 1, 2, 6, and 7 are having Broken access control issue.

Keep in mind that do not blindly follow the Authorize result, The Red highlight requests do not mean that all endpoints are vulnerable or bypassed. There may be false positives; You must do a cross-check.

Some other possible scenarios, Suppose you are testing auth issues with the two same level of users. As a result, you will see Authz. Status shows Bypassed! And Unauth. Status shows Enforced! In that case improper authorization can be found on the request which shows that the specific endpoint can be accessed by the 2nd user but has correctly implemented authorization for any unauthorized users.

When you select any highlighted request, on the right side you will see the detailed information about modified, original & unauthenticated request and responses.




```
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=rrai%40ignitetechnologies.in
```

That's a wrap for now. Cheers!

Conclusion

Pour effectuer des examens de sécurité complets, l'extension « Autorize Burp » est un outil essentiel. En automatisant l'authentification et en permettant le test des zones restreintes, il améliore l'efficacité et l'efficacité des évaluations de sécurité. Cette extension est un outil indispensable pour effectuer des tests complets et identifier les vulnérabilités potentielles qui ne peuvent être accessibles qu'aux utilisateurs authentifiés.

◀ PREVIOUS POST

Un moyen facile de générer un shell inversé

NEXT POST ▶

Un guide détaillé sur Ligolo-Ng

Abonnez-Vous Au Blog Par E-Mail

Entrez votre adresse e-mail pour vous abonner à ce blog et recevoir des notifications de nouveaux articles par e-mail.



A banner for Ignite Technologies' Cyber Security Training Programs. The background shows a desk with two computer monitors. The left monitor displays binary code (0s and 1s) and a padlock icon. The right monitor shows a blue circle with a white key icon. The text 'JOIN OUR CYBER SECURITY TRAINING PROGRAMS' is in large, bold, blue and white letters. Below it, a dark blue button says 'Enroll Today' with a white arrow. The Ignite Technologies logo is in the top left. Social media icons for Twitter and LinkedIn are in the bottom left. The website 'www.ignitetechnologies.in' is in the bottom right.

IGNITE
Technologies

**JOIN OUR CYBER
SECURITY TRAINING
PROGRAMS**

Enroll Today ➔

www.ignitetechnologies.in

A banner for Forensic Articles. The background is a blue, pixelated fingerprint. The text 'FORENSIC ARTICLES' is in a large, white, serif font. Below it, a white button with a black border says 'click here to view'.

FORENSIC ARTICLES

[click here to view](#)

A banner for Cyber Security Mindmaps & Cheatsheet. The background is a colorful, abstract design with a silhouette of a person standing in front of a large, glowing, circular network of nodes and lines. The text 'CYBER SECURITY Mindmaps & Cheatsheet' is in large, bold, white letters. The Ignite Technologies logo is in the top right. The website 'www.ignitetechnologies.in' is in the bottom left. The website 'www.hackingarticles.in' is in the bottom right.

IGNITE
Technologies

**CYBER
SECURITY**
Mindmaps &
Cheatsheet

www.ignitetechnologies.in

www.hackingarticles.in





Support Us

Catégories

Choisir une catégorie

