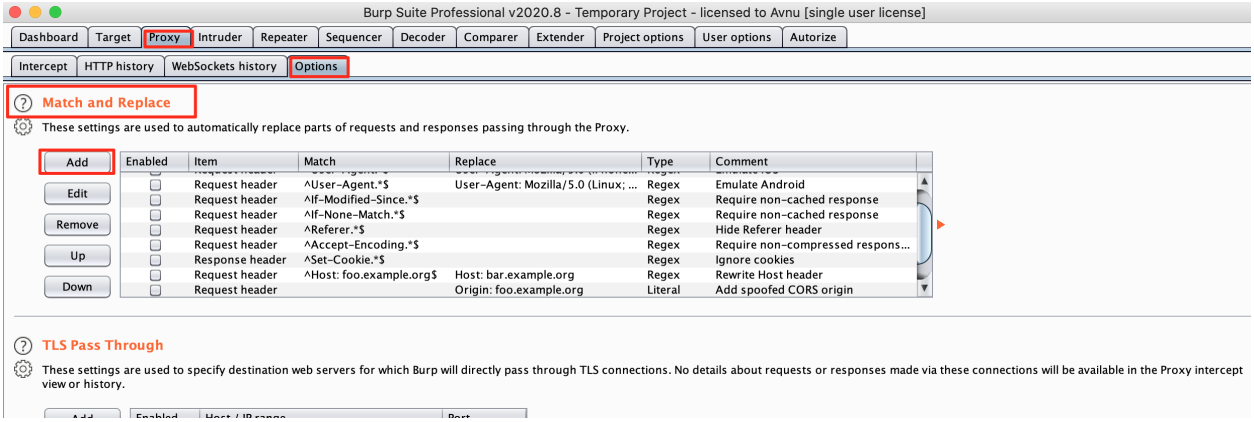
Burp: Match and replace

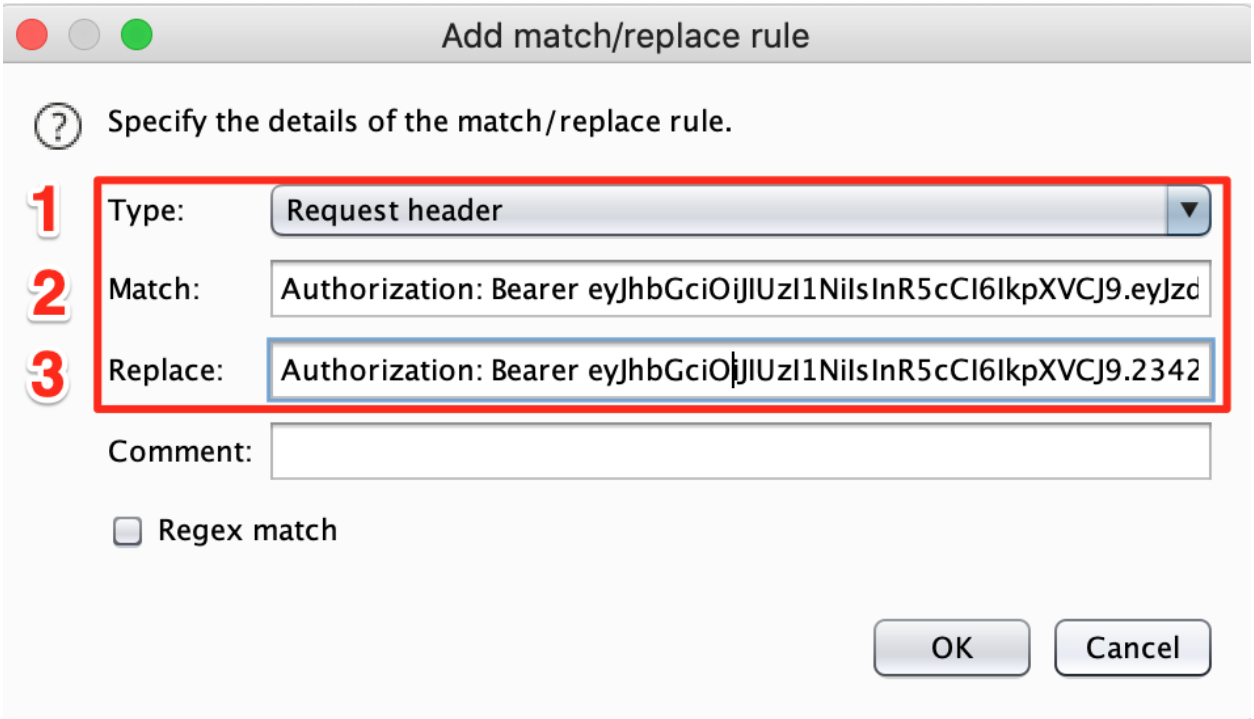
Introduction

Burp suite's proxy options have an option called "Match and replace" available. This option has many rich uses that can help us automate our testing process. With some smart uses of this amazing option, we can automatically test for CSRF, IDOR, command injection,.. by just clicking around in the application! Let's explore this magical tool and it's many options.

Replacing authorization headers

Since authorize basically just matches the authorization headers and attempts to replace them with the ones the user supplied, we can set up a similar rule in the proxy.

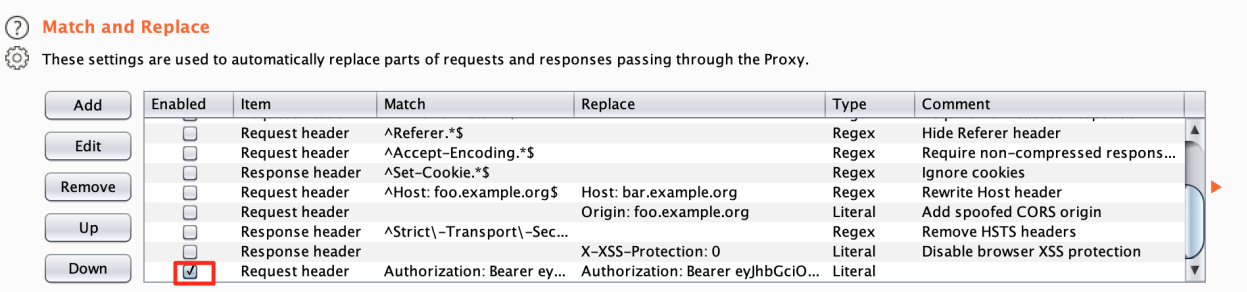




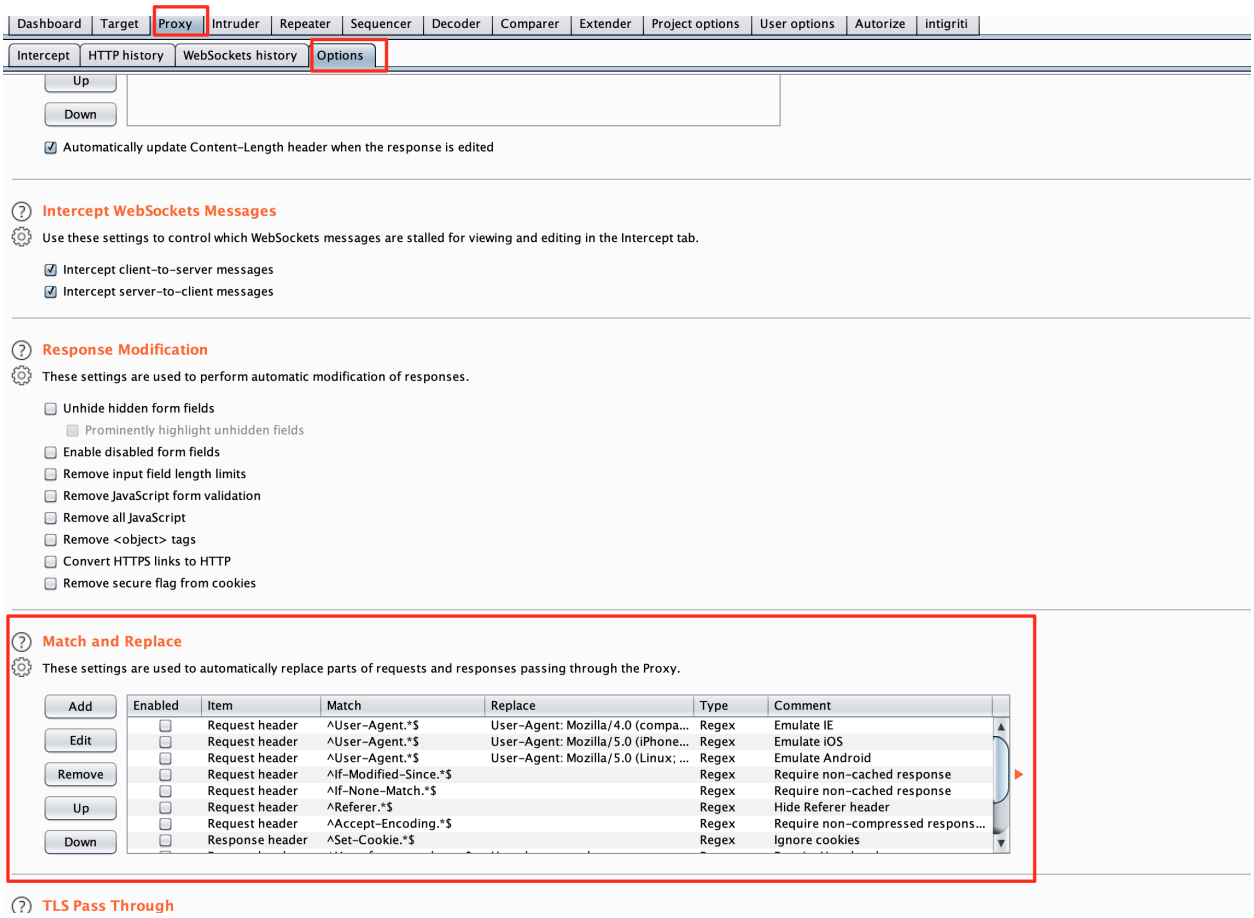
1. Usually the request header will contain the authorization methods
2. Fill in the tokens of the logged in user
3. Fill in the tokens of a second user you want to use

Now, as long as this rule is active you can click around in the application. If you can open any information that should not be public, we have an IDOR on our hands.

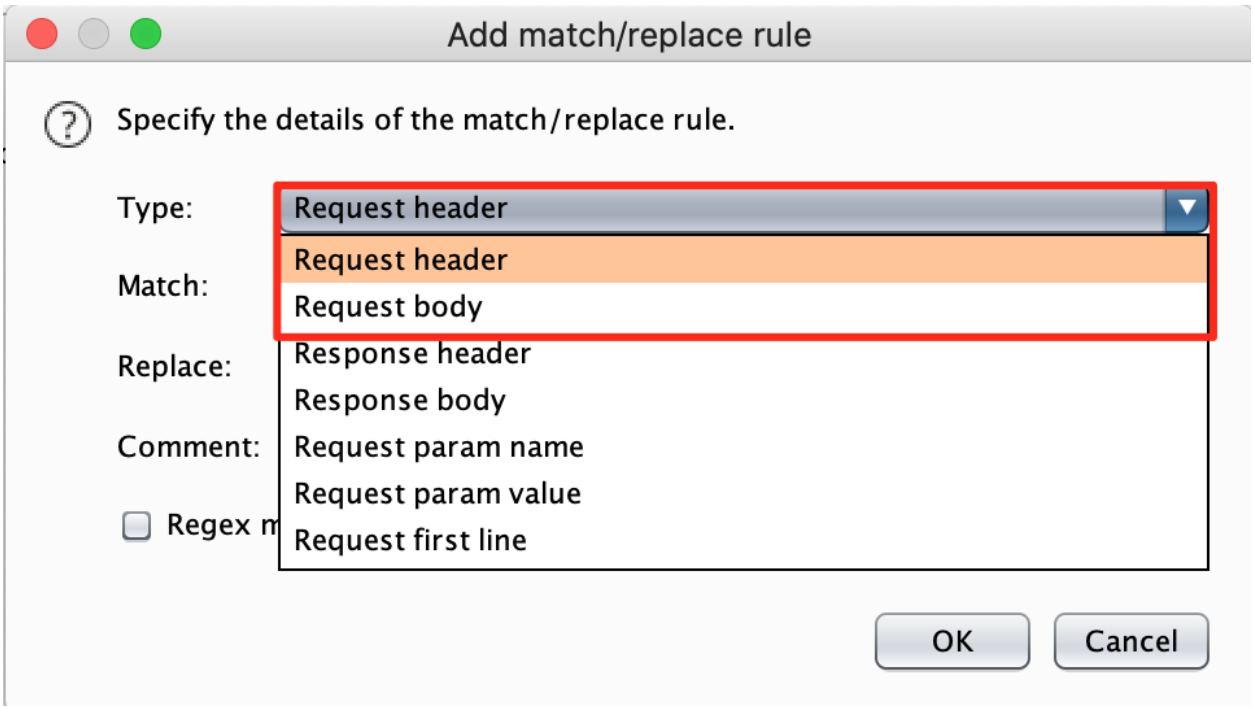
To disable this rule, simple uncheck the checkbox in front of it.



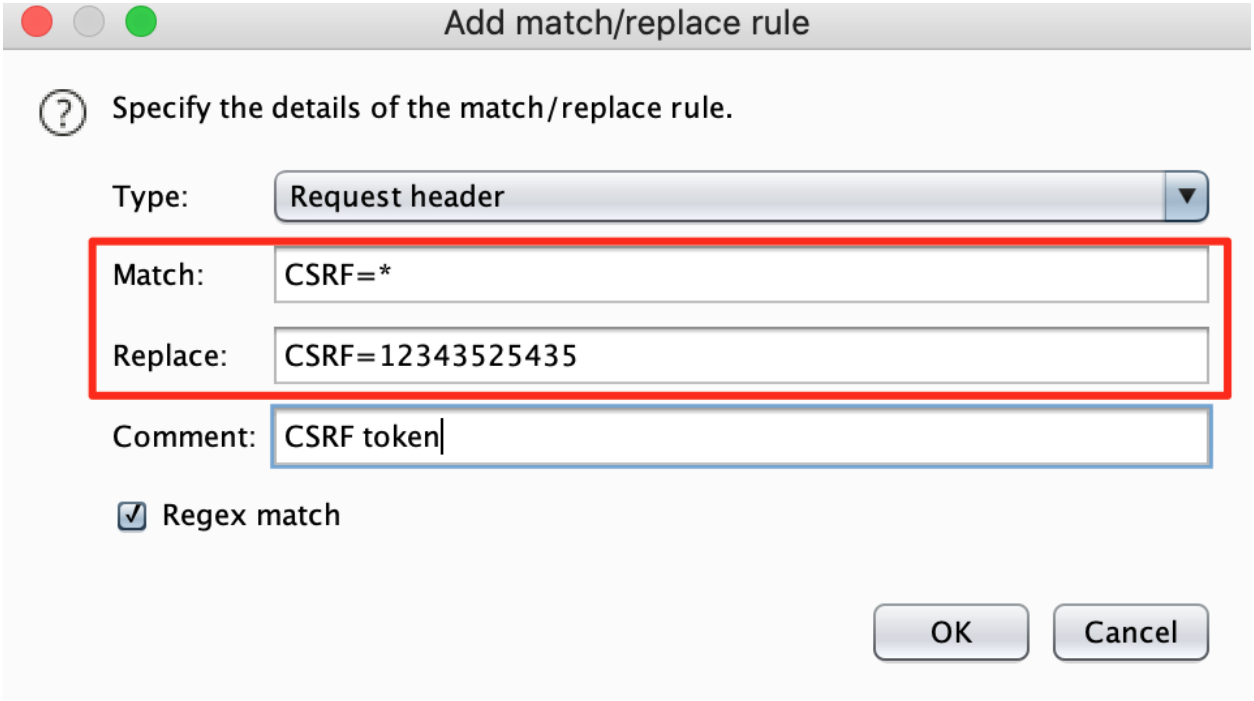
Automatically replacing CSRF tokens



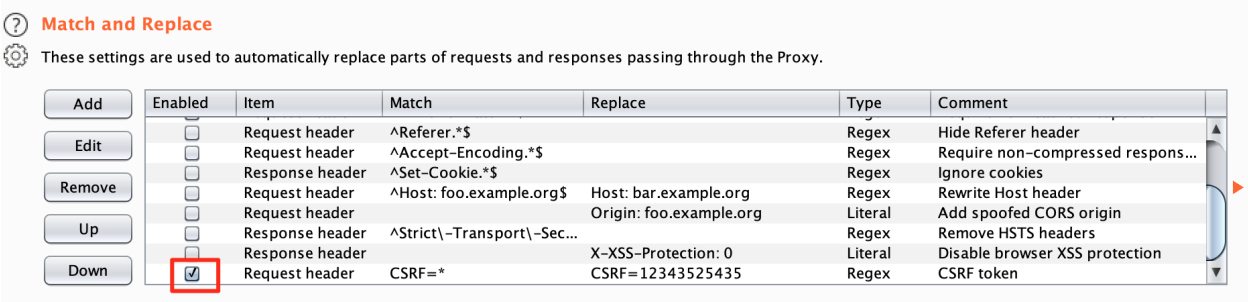
Depending on if the CSRF token is in the HEADER or the BODY section of the request, we will need to pick one.



Fill in the regex to indicate to burp how it can find the CSRF token in your request and replace it with a value of your own. Be careful, this is just an example, it may be different for your target.



When this rule is active, click through the application and try to make changes. If you are able to make changes where a CSRF token is normally expected, investigate this further. It may be a vulnerability. To restore normal functionality, simply disable this rule.



The sky is the limit

You can change any value you want in either

- The response
- The request

And in either

- The header
- The body
- Request Parameter names
- Request Parameter values
- Request first line

These give us an infinte amount of possibilites so the sky is the limit... Think outside the box!