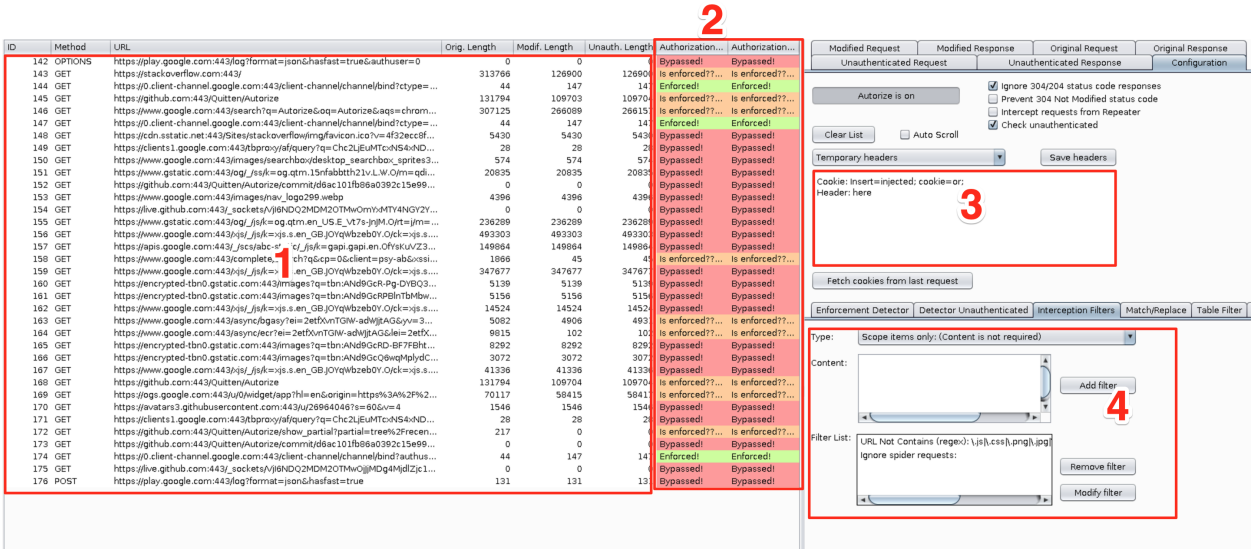
Burp: Authorize

Introduction
Usage
Interpreting the results

Introduction

Authorize will repeat any request you make with replaced authentication method (3 in screenshot below) and with empty authentication in an attempt to emulate another user and an unauthenticated user. It will then compare the response of the modified request to the response of the request you sent.

Usage



1. All your requests will show up in here
2. This will show if access control is properly implemented

3. Fill in the request header here that takes care of the authentication
4. There are some filters i recommend you set

- Scope items only (No text required): This will ensure you won't see too many weird non scope related requests
- URL not contains (text): Any request that is supposed to be public information, i try to filter out in here

Interpreting the results

This is what the statuses for (2) mean:

ENFORCED: This means there is no IDOR. The modified request returns a 403 forbidden or any other error code.

Is Enforced?: This means the modified the modified response did not return an error code, but not the exact same response as the unauthenticated request

Bypassed: THIS DOES NOT AUTOMATICALLY GUARANTEE AN IDOR! This means that the modified response matches the original response. You still have to confirm whether or not this is intended behavior. More often than not, it will be intended behaviour. Whether or not it is, is up to your discretion and this is also part of the reason why i recommend you really know your target well by exploring it before you hack. Always confirm this manually by

1. Right clicking the request
2. Sending the modified request to the repeater
3. Repeating the request and confirming you are seeing other peoples data that is not supposed to be public