030. Automated BAC hunting with burp suite

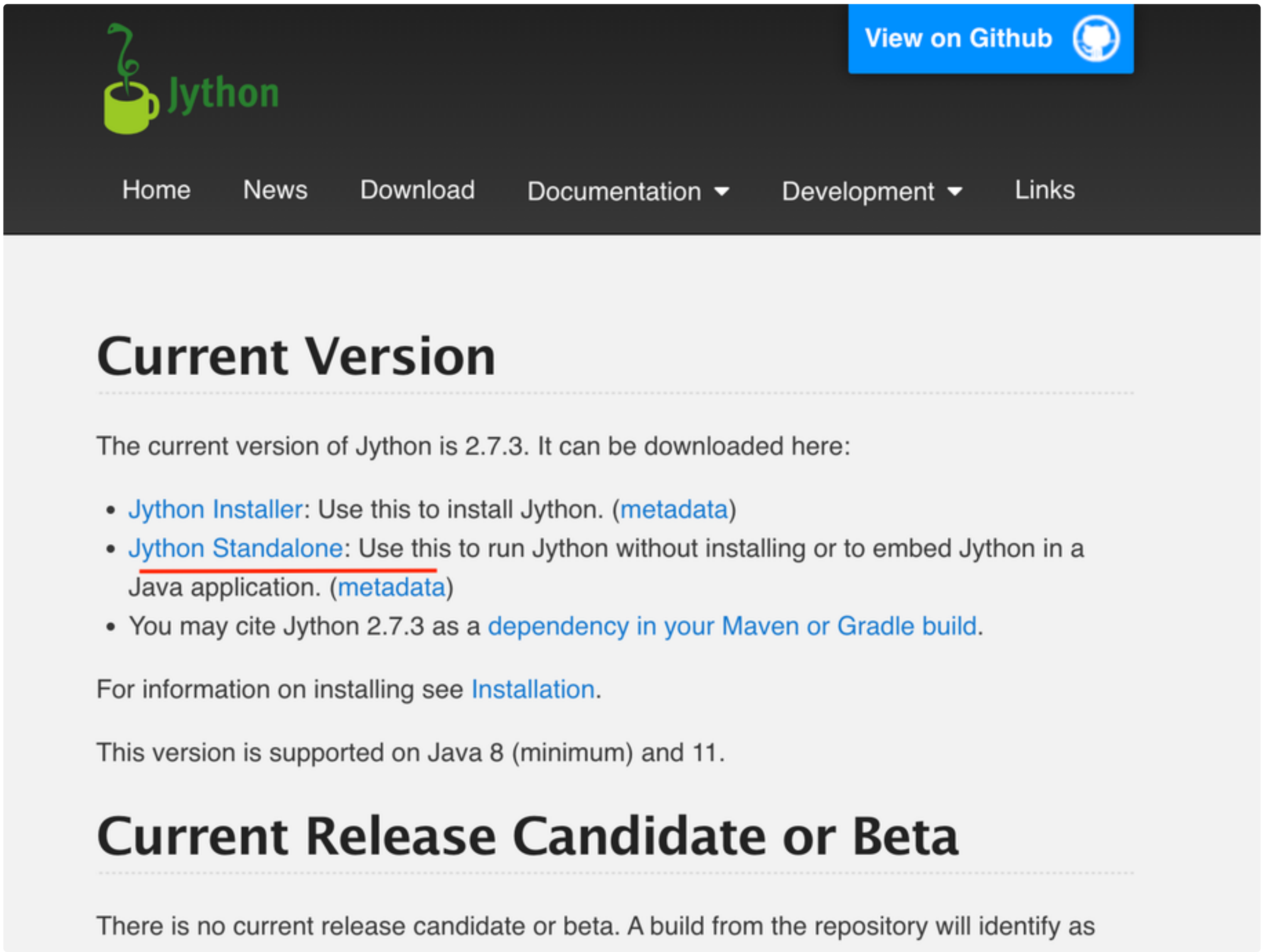
Introduction

So now that we know what to do manually, we can start introducing tools. We can never 100% fully automatically check it but we can certainly make our work easier and semi-automate it. We can use a plugin for this in burp suite called “authorise” and this plugin is made for testing BAC and IDOR.

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.

How to install

Installing might confuse you for a bit but it’s not as hard as it first seems, you need to download the jython standalone JAR from this website: Downloads



Current Version

The current version of Jython is 2.7.3. It can be downloaded here:

- Jython Installer: Use this to install Jython. (metadata)
- Jython Standalone: Use this to run Jython without installing or to embed Jython in a Java application. (metadata)
- You may cite Jython 2.7.3 as a dependency in your Maven or Gradle build.

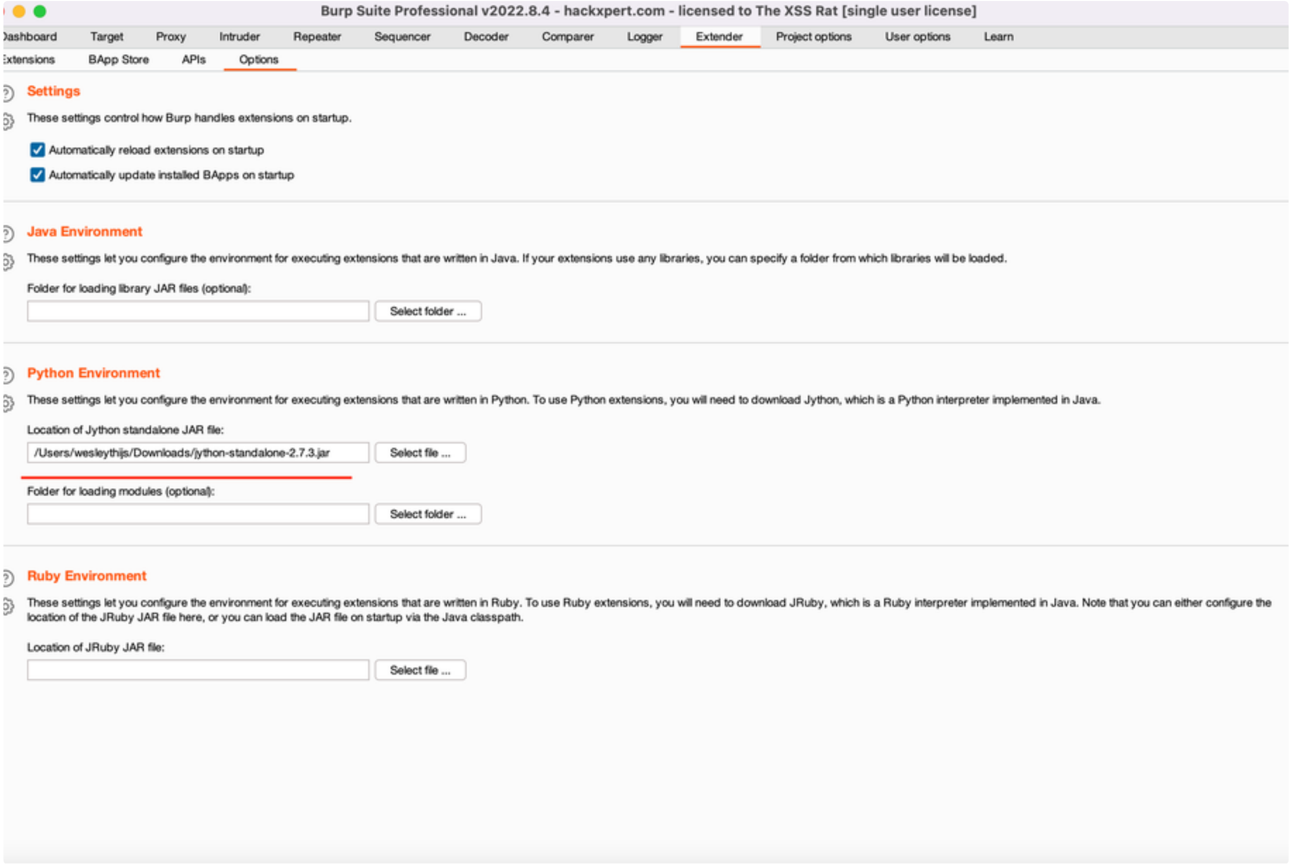
For information on installing see Installation.

This version is supported on Java 8 (minimum) and 11.

Current Release Candidate or Beta

There is no current release candidate or beta. A build from the repository will identify as

And now you can import that in burp suite:



Settings

These settings control how Burp handles extensions on startup.

☑ Automatically reload extensions on startup

☑ Automatically update installed BApps on startup

Java Environment

These settings let you configure the environment for executing extensions that are written in Java. If your extensions use any libraries, you can specify a folder from which libraries will be loaded.

Folder for loading library JAR files (optional):

Python Environment

These settings let you configure the environment for executing extensions that are written in Python. To use Python extensions, you will need to download Jython, which is a Python interpreter implemented in Java.

Location of Jython standalone JAR file: /Users/wesleythijs/Downloads/jython-standalone-2.7.3.jar

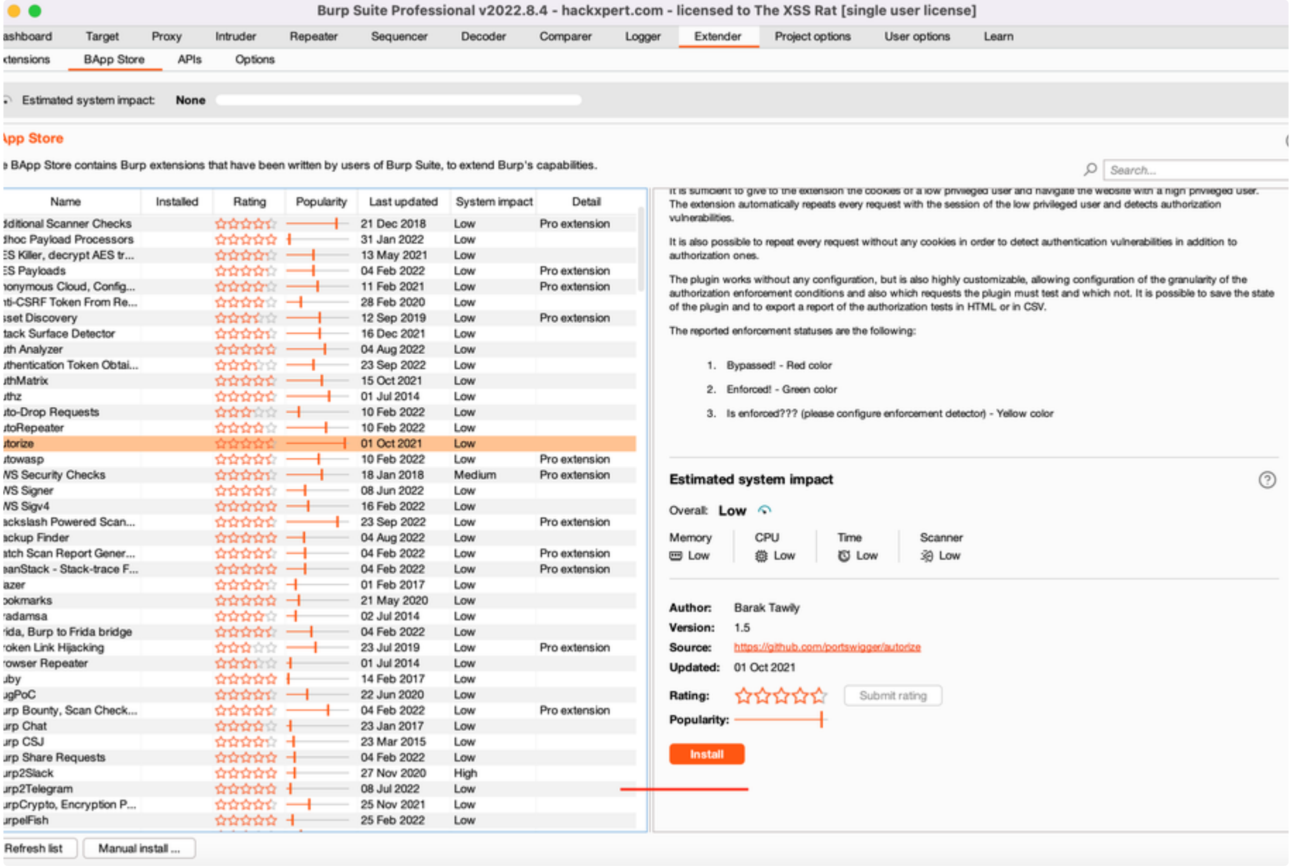
Folder for loading modules (optional):

Ruby Environment

These settings let you configure the environment for executing extensions that are written in Ruby. To use Ruby extensions, you will need to download JRuby, which is a Ruby interpreter implemented in Java. Note that you can either configure the location of the JRuby JAR file here, or you can load the JAR file on startup via the Java classpath.

Location of JRuby JAR file:

And we are done!



Estimated system impact: **None**

App Store

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

Name	Installed	Rating	Popularity	Last updated	System impact	Detail
dditional Scanner Checks				21 Dec 2018	Low	Pro extension
dhoc Payload Processors				31 Jan 2022	Low	
ES Killer, decrypt AES tr...				13 May 2021	Low	
ES Payloads				04 Feb 2022	Low	Pro extension
nonymous Cloud, Config...				11 Feb 2021	Low	Pro extension
nti-CSRF Token From Re...				28 Feb 2020	Low	
sset Discovery				12 Sep 2019	Low	Pro extension
ttack Surface Detector				16 Dec 2021	Low	
uth Analyzer				04 Aug 2022	Low	
uthentication Token Obtai...				23 Sep 2022	Low	
uthMatrix				15 Oct 2021	Low	
uthz				01 Jul 2014	Low	
uto-Drop Requests				10 Feb 2022	Low	
utoRepeater				10 Feb 2022	Low	
utorize				01 Oct 2021	Low	
utowasp				10 Feb 2022	Low	Pro extension
WS Security Checks				18 Jan 2018	Medium	Pro extension
WS Signer				08 Jun 2022	Low	
WS Sigv4				16 Feb 2022	Low	
ackslash Powered Scan...				23 Sep 2022	Low	Pro extension
ackup Finder				04 Aug 2022	Low	
atch Scan Report Gener...				04 Feb 2022	Low	Pro extension
eanStack - Stack-trace F...				04 Feb 2022	Low	Pro extension
lazer				01 Feb 2017	Low	
ookmarks				21 May 2020	Low	
radamsa				02 Jul 2014	Low	
rida, Burp to Frida bridge				04 Feb 2022	Low	
roken Link Hijacking				23 Jul 2019	Low	Pro extension
rowser Repeater				01 Jul 2014	Low	
uby				14 Feb 2017	Low	
ugPoC				22 Jun 2020	Low	
urp Bounty, Scan Check...				04 Feb 2022	Low	Pro extension
urp Chat				23 Jan 2017	Low	
urp CSJ				23 Mar 2015	Low	
urp Share Requests				04 Feb 2022	Low	
urp2Slack				27 Nov 2020	High	
urp2Telegram				08 Jul 2022	Low	
urpCrypto, Encryption P...				25 Nov 2021	Low	
urpelFish				25 Feb 2022	Low	

It is sufficient to give to the extension the cookies of a low privileged user and navigate the website with a high privileged user. The extension automatically repeats every request with the session of the low privileged user and detects authorization vulnerabilities.

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

The plugin works without any configuration, but is also highly customizable, allowing configuration of the granularity of the authorization enforcement conditions and also which requests the plugin must test and which not. It is possible to save the state of the plugin and to export a report of the authorization tests in HTML or in CSV.

The reported enforcement statuses are the following:

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

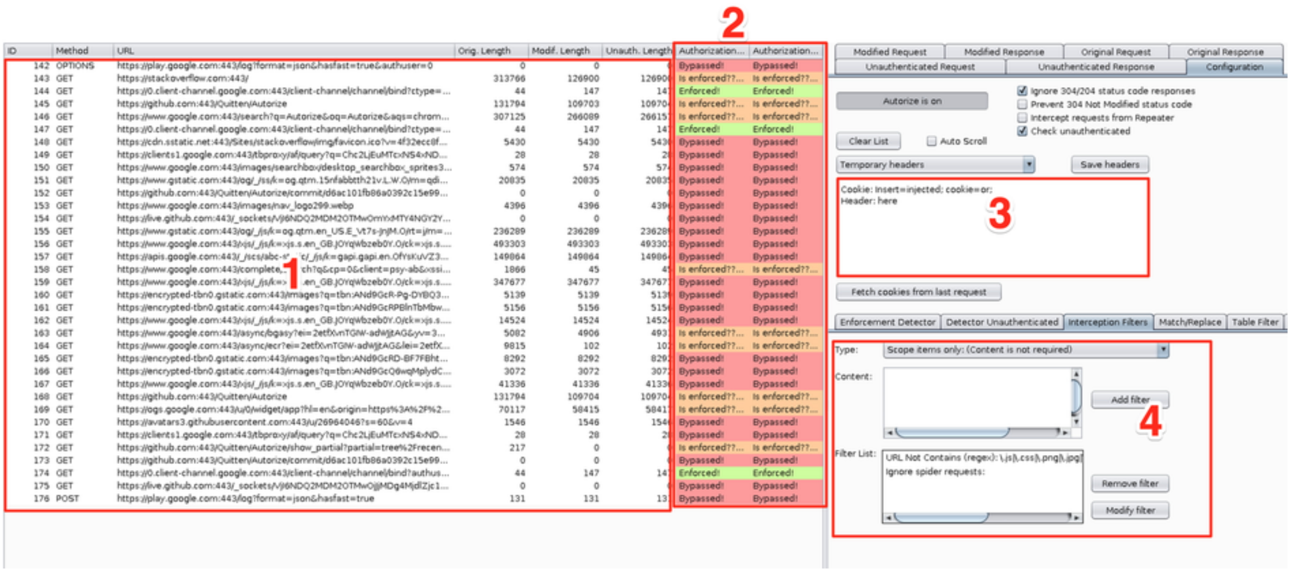
Estimated system impact

Overall: **Low**

Memory	CPU	Time	Scanner
Low	Low	Low	Low

Author: Barak Tawily
Version: 1.5
Source: https://github.com/portswigger/autorize
Updated: 01 Oct 2021
Rating:
Popularity:

Usage



ID	Method	URL	Orig. Length	Modif. Length	Unauth. Length	Authorization...	Authorization...
142	OPTIONS	https://play.google.com:443/log?format=json&hasfast=true&authuser=0	0	0	0	Bypassed!	Bypassed!
143	GET	https://stackoverflow.com:443/	313766	126900	126900	Is enforced??...	Is enforced??...
144	GET	https://0.client-channel.google.com:443/client-channel/channel/bind?ctype=...	44	147	147	Enforced!	Enforced!
145	GET	https://github.com:443/Quitten/Autorize	131794	109703	109704	Is enforced??...	Is enforced??...
146	GET	https://www.google.com:443/search?q=Autorize&oq=Autorize&aqs=chrom...	307125	266089	266157	Is enforced??...	Is enforced??...
147	GET	https://0.client-channel.google.com:443/client-channel/channel/bind?ctype=...	44	147	147	Enforced!	Enforced!
148	GET	https://cdn.sstatic.net:443/Sites/stackoverflow/img/favicon.ico?v=4f32ecc8f...	5430	5430	5430	Bypassed!	Bypassed!
149	GET	https://clients1.google.com:443/tbproxy/af/query?q=Chc2LjEuMTcxNS4xND...	28	28	28	Bypassed!	Bypassed!
150	GET	https://www.google.com:443/images/searchbox/desktop_searchbox_sprites3...	574	574	574	Bypassed!	Bypassed!
151	GET	https://www.gstatic.com:443/og/_/ss/k=og.qtm.15nfabbtth21v.L.W.O/m=qdi...	20835	20835	20835	Bypassed!	Bypassed!
152	GET	https://github.com:443/Quitten/Autorize/commit/d6ac101fb86a0392c15e99...	0	0	0	Bypassed!	Bypassed!
153	GET	https://www.google.com:443/images/nav_logo299.webp	4396	4396	4396	Bypassed!	Bypassed!
154	GET	https://live.github.com:443/_sockets/VjI6NDQ2MDM2OTMwOmYxMTY4NGY2Y...	0	0	0	Bypassed!	Bypassed!
155	GET	https://www.gstatic.com:443/og/_/js/k=og.qtm.en_US.E_Vt7s-JnJM.O/rt=j/m=...	236289	236289	236289	Bypassed!	Bypassed!
156	GET	https://www.google.com:443/xjs/_/js/k=xjs.s.en_GB.JOYqWbzeb0Y.O/ck=xjs.s....	493303	493303	493303	Bypassed!	Bypassed!
157	GET	https://apis.google.com:443/_/scs/abc-st c/_/js/k=gapi.gapi.en.OfYsKuVZ3...	149864	149864	149864	Bypassed!	Bypassed!
158	GET	https://www.google.com:443/complete, ch?q&cp=0&client=psy-ab&xssi...	1866	45	45	Is enforced??...	Is enforced??...
159	GET	https://www.google.com:443/xjs/_/js/k=x .en_GB.JOYqWbzeb0Y.O/ck=xjs.s....	347677	347677	347677	Bypassed!	Bypassed!
160	GET	https://encrypted-tbn0.gstatic.com:443/images?q=tbn:ANd9GcR-Pg-DYBQ3...	5139	5139	5139	Bypassed!	Bypassed!
161	GET	https://encrypted-tbn0.gstatic.com:443/images?q=tbn:ANd9GcRPBlnTbMbw...	5156	5156	5156	Bypassed!	Bypassed!
162	GET	https://www.google.com:443/xjs/_/js/k=xjs.s.en_GB.JOYqWbzeb0Y.O/ck=xjs.s....	14524	14524	14524	Bypassed!	Bypassed!
163	GET	https://www.google.com:443/async/bgasy?ei=2etfXvnTGIW-adWjtAG&yv=3...	5082	4906	493	Is enforced??...	Is enforced??...
164	GET	https://www.google.com:443/async/ecr?ei=2etfXvnTGIW-adWjtAG&lei=2etfX...	9815	102	102	Is enforced??...	Is enforced??...
165	GET	https://encrypted-tbn0.gstatic.com:443/images?q=tbn:ANd9GcRD-BF7FBht...	8292	8292	8292	Bypassed!	Bypassed!
166	GET	https://encrypted-tbn0.gstatic.com:443/images?q=tbn:ANd9GcQ6wqMplydC...	3072	3072	3072	Bypassed!	Bypassed!
167	GET	https://www.google.com:443/xjs/_/js/k=xjs.s.en_GB.JOYqWbzeb0Y.O/ck=xjs.s....	41336	41336	41336	Bypassed!	Bypassed!
168	GET	https://github.com:443/Quitten/Autorize	131794	109704	109704	Is enforced??...	Is enforced??...
169	GET	https://ogs.google.com:443/u/0/widget/app?hl=en&origin=https%3A%2F%2...	70117	58415	58417	Is enforced??...	Is enforced??...
170	GET	https://avatars3.githubusercontent.com:443/u/26964046?s=60&v=4	1546	1546	1546	Bypassed!	Bypassed!
171	GET	https://clients1.google.com:443/tbproxy/af/query?q=Chc2LjEuMTcxNS4xND...	28	28	28	Bypassed!	Bypassed!
172	GET	https://github.com:443/Quitten/Autorize/show_partial?partial=tree%2Frecen...	217	0	0	Is enforced??...	Is enforced??...
173	GET	https://github.com:443/Quitten/Autorize/commit/d6ac101fb86a0392c15e99...	0	0	0	Bypassed!	Bypassed!
174	GET	https://0.client-channel.google.com:443/client-channel/channel/bind?authus...	44	147	147	Enforced!	Enforced!
175	GET	https://live.github.com:443/_sockets/VjI6NDQ2MDM2OTMwOjjMDg4MjdlZjc1...	0	0	0	Bypassed!	Bypassed!
176	POST	https://play.google.com:443/log?format=json&hasfast=true	131	131	131	Bypassed!	Bypassed!

Modified Request | Modified Response | Original Request | Original Response | Unauthenticated Request | Unauthenticated Response | Configuration

Autorize is on

☑ Ignore 304/204 status code responses
☐ Prevent 304 Not Modified status code
☐ Intercept requests from Repeater
☑ Check unauthenticated

Clear List ☐ Auto Scroll

Temporary headers ▾ Save headers

```
Cookie: Insert=injected; cookie=or;
Header: here
```

Fetch cookies from last request

Enforcement Detector | Detector Unauthenticated | Interception Filters | Match/Replace | Table Filter

Type: Scope items only: (Content is not required) ▾

Content:

Add filter

Filter List:

URL Not Contains (regex): \.js|\.css|\.png|\.jpg|
Ignore spider requests:

Remove filter

Modify filter

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

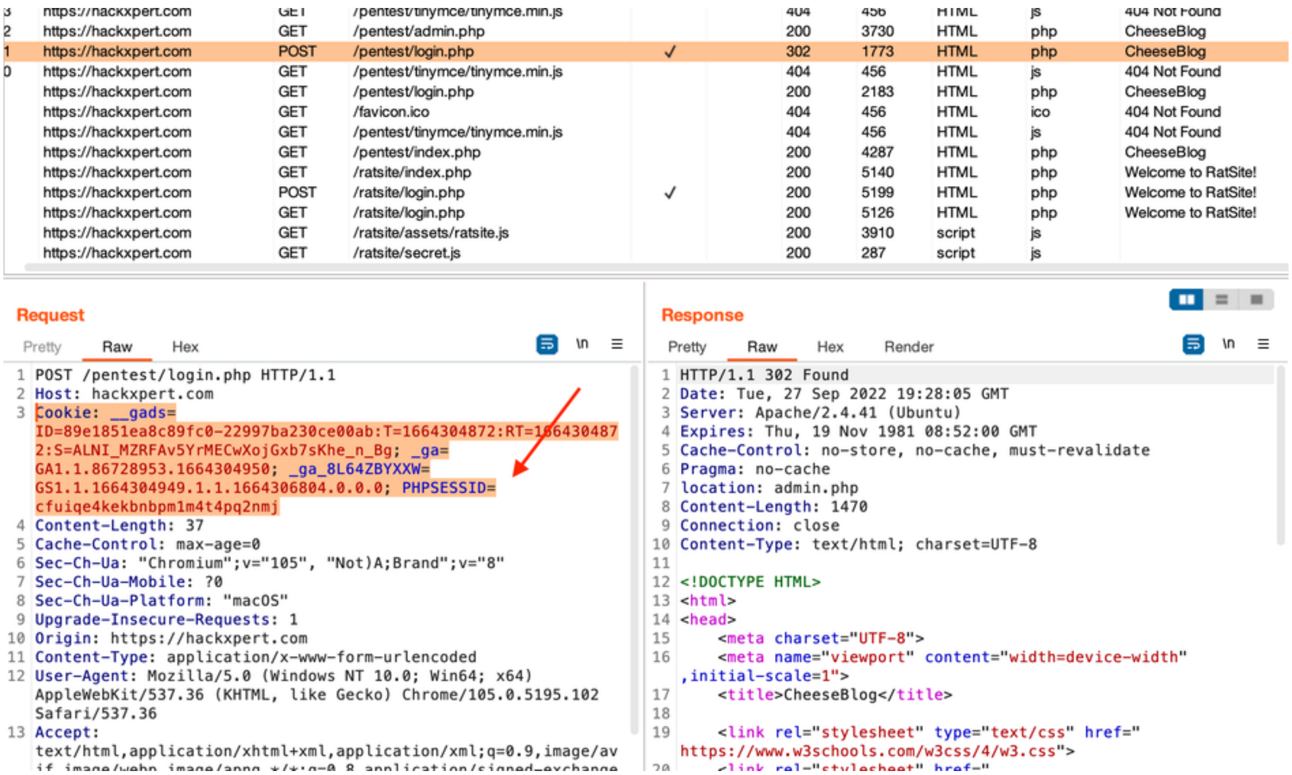
1. Right clicking the request
2. Sending the modified request to the repeater
3. Repeating the request and confirming you are seeing other peoples data that is not supposed to be public

Practice

Let's go practice this on Are you a hackxpert? but I am going to only give you rats one tip this time before we go. DO NOT COPY ALL THE HEADERS. This lab is built to be life like and sometimes headers can mess with authorise so make sure to only use the cookies or authorisation headers and nothing else. This is not as important now but will come into play soon!

Your target: CheeseBlog

You should already know to log in as the "test" user first with their weak password of "test" to grab their auth headers.



3	https://hackxpert.com	GET	/pentest/tinymce/tinymce.min.js		404	456	HTML	js	404 Not Found
2	https://hackxpert.com	GET	/pentest/admin.php		200	3730	HTML	php	CheeseBlog
1	https://hackxpert.com	POST	/pentest/login.php	✓	302	1773	HTML	php	CheeseBlog
0	https://hackxpert.com	GET	/pentest/tinymce/tinymce.min.js		404	456	HTML	js	404 Not Found
	https://hackxpert.com	GET	/pentest/login.php		200	2183	HTML	php	CheeseBlog
	https://hackxpert.com	GET	/favicon.ico		404	456	HTML	ico	404 Not Found
	https://hackxpert.com	GET	/pentest/tinymce/tinymce.min.js		404	456	HTML	js	404 Not Found
	https://hackxpert.com	GET	/pentest/index.php		200	4287	HTML	php	CheeseBlog
	https://hackxpert.com	GET	/ratsite/index.php		200	5140	HTML	php	Welcome to RatSite!
	https://hackxpert.com	POST	/ratsite/login.php	✓	200	5199	HTML	php	Welcome to RatSite!
	https://hackxpert.com	GET	/ratsite/login.php		200	5126	HTML	php	Welcome to RatSite!
	https://hackxpert.com	GET	/ratsite/assets/ratsite.js		200	3910	script	js	
	https://hackxpert.com	GET	/ratsite/secret.js		200	287	script	js	

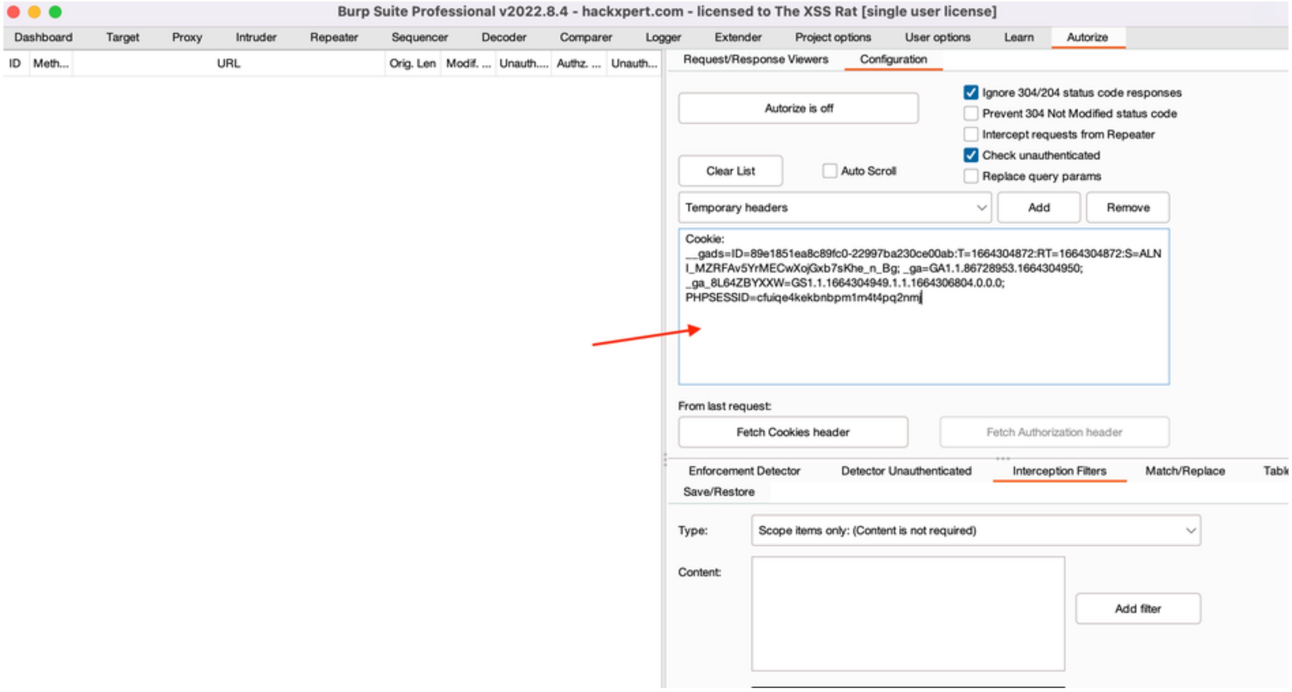
```
POST /pentest/login.php HTTP/1.1
Host: hackxpert.com
Cookie: __gads=
ID=89e1851ea8c89fc0-22997ba230ce00ab:T=1664304872:RT=166430487
2:S=ALNI_MZRFAv5YrMECwXojGxb7sKhe_n_Bg; _ga=
GA1.1.86728953.1664304950; _ga_8L64ZBYXXW=
GS1.1.1664304949.1.1.1664306804.0.0.0; PHPSESSID=
cfuiqe4kekbnbpm1m4t4pq2nmj
Content-Length: 37
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "macOS"
Upgrade-Insecure-Requests: 1
Origin: https://hackxpert.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.5195.102
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
```

```
HTTP/1.1 302 Found
Date: Tue, 27 Sep 2022 19:28:05 GMT
Server: Apache/2.4.41 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
location: admin.php
Content-Length: 1470
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE HTML>
<html>
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width"
,initial-scale=1">
    <title>CheeseBlog</title>

    <link rel="stylesheet" type="text/css" href="
https://www.w3schools.com/w3css/4/w3.css">
    <link rel="stylesheet" href="
```

Paste these in the authorise window.



Burp Suite Professional v2022.8.4 - hackxpert.com - licensed to The XSS Rat [single user license]

☑ Ignore 304/204 status code responses
☐ Prevent 304 Not Modified status code
☐ Intercept requests from Repeater
☑ Check unauthenticated
☐ Replace query params
☐ Auto Scroll

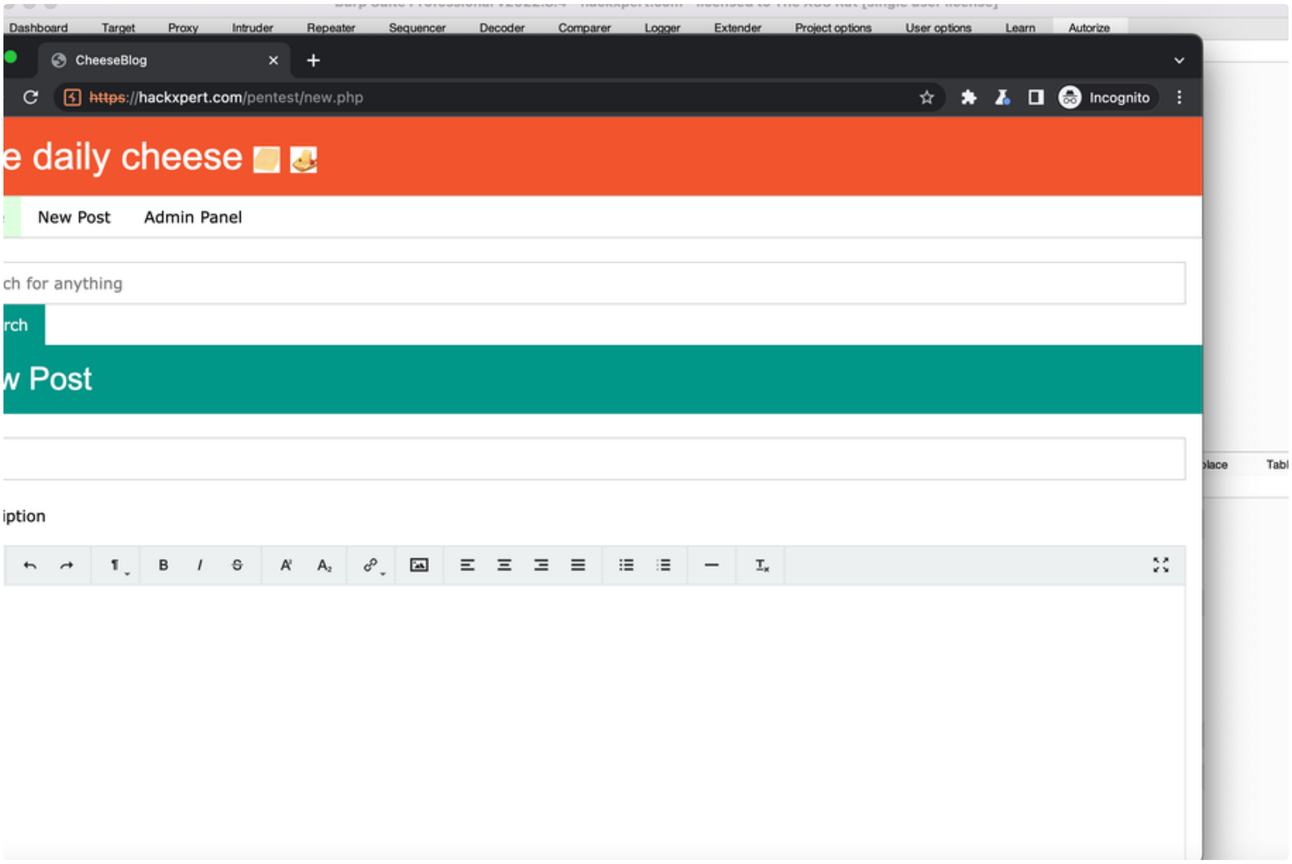
Temporary headers

```
Cookie:
__gads=ID=89e1851ea8c89fc0-22997ba230ce00ab:T=1664304872:RT=1664304872:S=ALN
I_MZRFAv5YrMECwXojGxb7sKhe_n_Bg; _ga=GA1.1.86728953.1664304950;
_ga_8L64ZBYXXW=GS1.1.1664304949.1.1.1664306804.0.0.0;
PHPSESSID=cfuiqe4kekbnbpm1m4t4pq2nmj
```

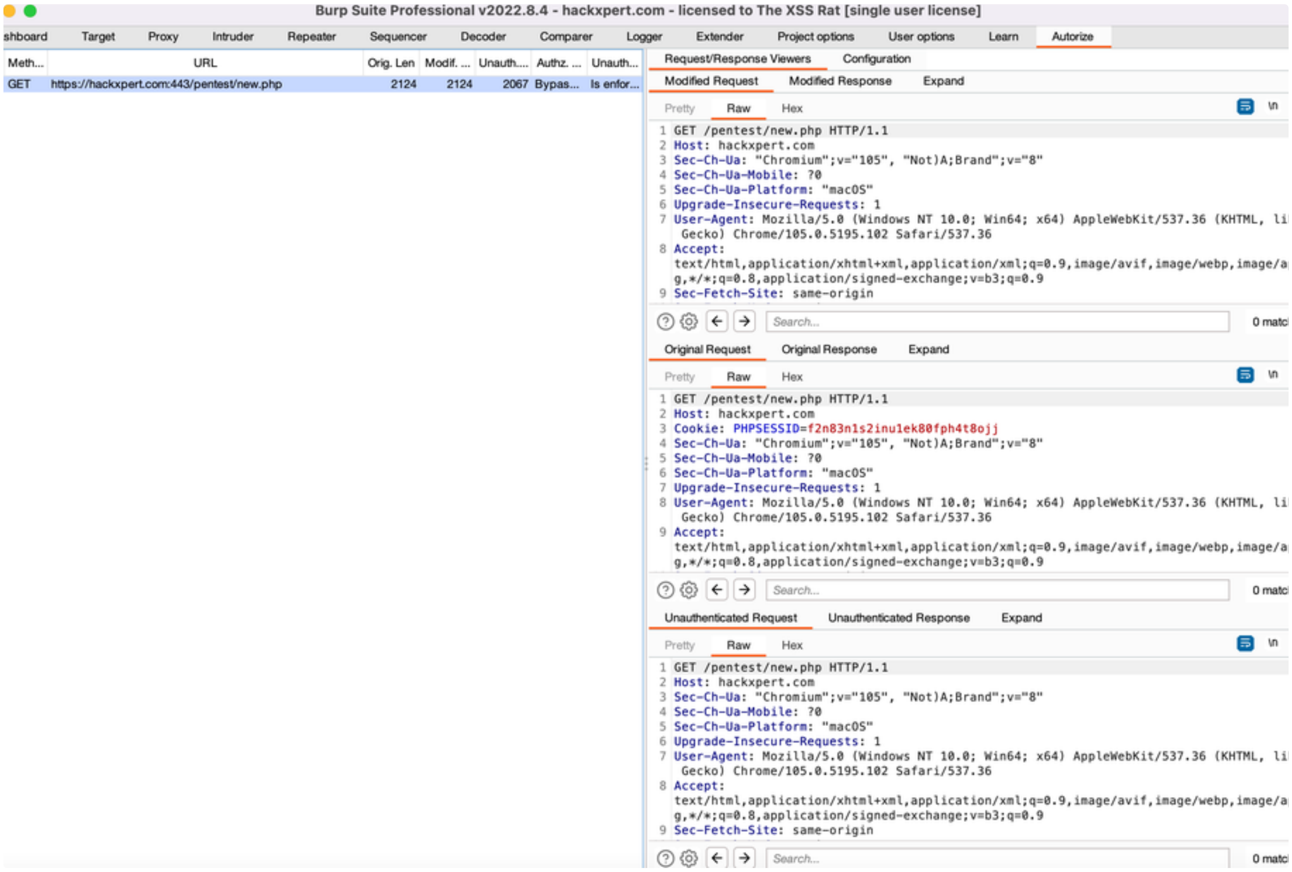
Type: Scope items only: (Content is not required)

Content:

Your admin privileged user here is “admin/test” so log in as them but **DO IT IN A PRIVATE BROWSER WINDOW!** now and click “authorise is off” to activate it!



For example, even just creating a new post is something the test/test account should not be able to do but authorise points us into the direction of a BAC!



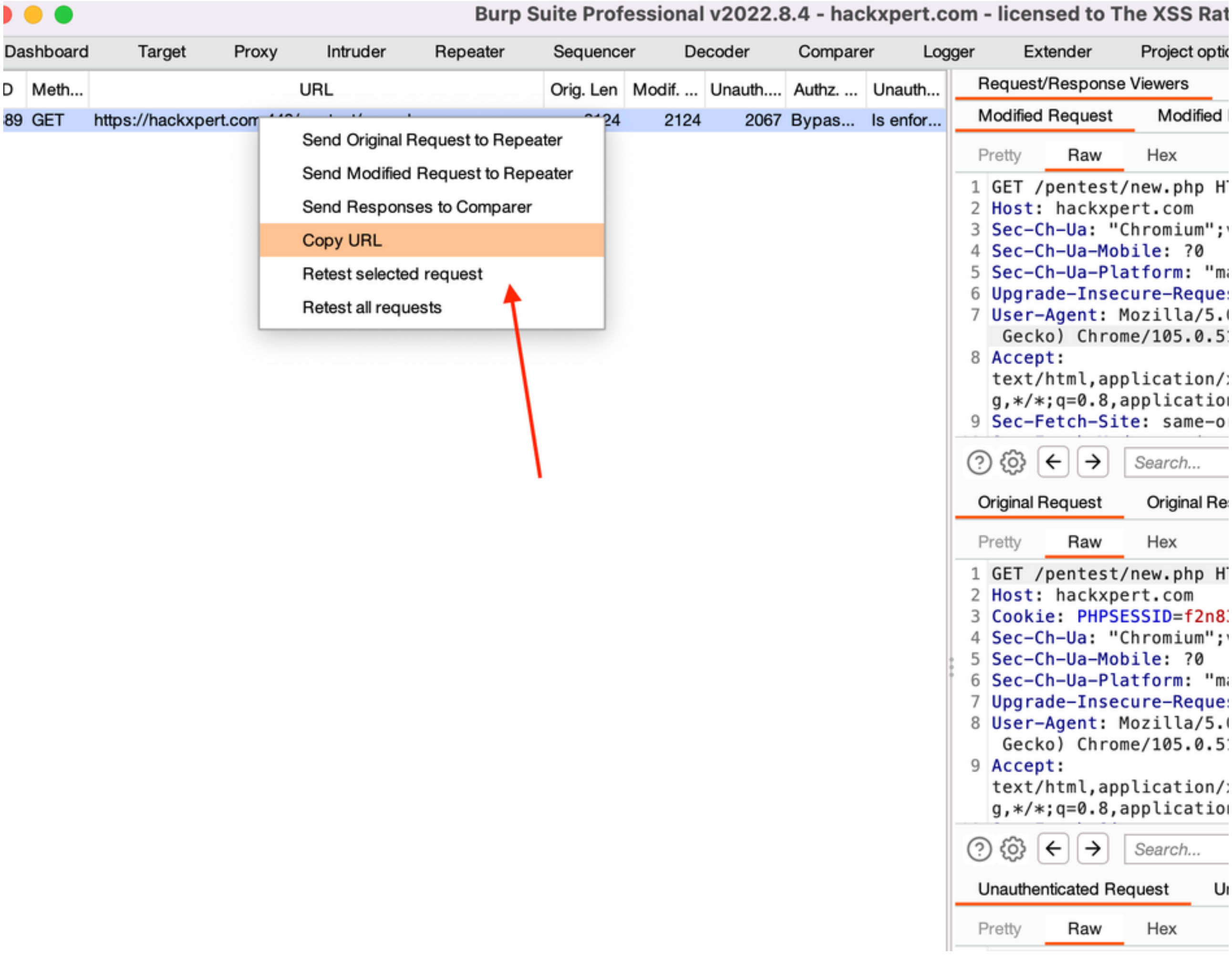
Meth...	URL	Orig. Len	Modif. ...	Unauth....	Authz. ...	Unauth...
GET	https://hackxpert.com:443/pentest/new.php	2124	2124	2067	Bypas...	Is enfor...

```
GET /pentest/new.php HTTP/1.1
Host: hackxpert.com
Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "macOS"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li
 Gecko) Chrome/105.0.5195.102 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
```

```
GET /pentest/new.php HTTP/1.1
Host: hackxpert.com
Cookie: PHPSESSID=f2n83n1s2inu1ek80fph4t8ojj
Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "macOS"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li
 Gecko) Chrome/105.0.5195.102 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
```

```
GET /pentest/new.php HTTP/1.1
Host: hackxpert.com
Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "macOS"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li
 Gecko) Chrome/105.0.5195.102 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
```

ALWAYS INVESTIGATE MANUALLY! THIS SHOULD EITHER BE A PRIVATE RESOURCE OR SOMETHING ABOVE YOUR PRIVILEGE LEVELS! Copy the URL and paste it in the browser of the Low priv user to confirm. Can you find all the IDORs and BACs?



D	Meth...	URL	Orig. Len	Modif. ...	Unauth....	Authz. ...	Unauth...
89	GET	https://hackxpert.com	24	2124	2067	Bypas...	Is enfor...

Modified Request

```
GET /pentest/new.php H
Host: hackxpert.com
Sec-Ch-Ua: "Chromium";
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "m
Upgrade-Insecure-Reque
User-Agent: Mozilla/5.
 Gecko) Chrome/105.0.5
Accept:
text/html,application/
g,*/*;q=0.8,applicatio
Sec-Fetch-Site: same-o
```

Original Request

```
GET /pentest/new.php H
Host: hackxpert.com
Cookie: PHPSESSID=f2n8
Sec-Ch-Ua: "Chromium";
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "m
Upgrade-Insecure-Reque
User-Agent: Mozilla/5.
 Gecko) Chrome/105.0.5
Accept:
text/html,application/
g,*/*;q=0.8,applicatio
```