

【高效漏洞挖掘】HaE与Authz的搭配

HaE与Authz均为BurpSuite插件生态的一员，两者搭配可以避免“越权”、“未授权”两类漏洞的重复测试行为。（适用于业务繁杂，系统模块功能多的场景）

介绍

HaE – <https://github.com/gh0stkey/HaE> : HaE(Highlighter and Extractor)，这是一款基于Python开发的BurpSuite插件，它主要用于高亮和提取HTTP响应报文的内容，而你可以自定义正则来选择你需要高亮或提取的信息，具体使用方法和介绍请移步至：

<https://gh0st.cn/archives/2020-03-18/1>。

Authz – <https://github.com/portswigger/authz> : Authz是一款用于测试“权限类”（越权、未授权）漏洞的插件，将所有有疑问的请求发送至该插件即可，在去年（2019年）我写过一篇文章关于它的介绍和使用，请移步至：<https://gh0st.cn/archives/2019-06-27/1>

注：Authz插件可于BApp Store下载

搭配

首先根据我所列的文章将HaE插件安装完成，默认的配置文件即可。

BurpSuite监听状态，进入一个业务系统进行一些操作（基本测试步骤）；

当你觉得测试完成之后或包都抓的差不多了，进入 `Proxy - HTTP History - Filter` 只展示高亮的请求：

Dashboard
Target
Proxy
Intruder
Repeater
Sequencer

Intercept
HTTP history
WebSockets history
Options

Filter: Hiding CSS content; hiding specific extensions

?
Filter by request type

☐ Show only in-scope items
☐ Hide items without responses
☐ Show only parameterized requests

Filter by MIME type

☒ HTML
☒ Other text
☒ Script
☒ Images
☒ XML
☒ Flash
☐ CSS
☒ Other binary

Filter by status code

☒ 2xx [success]
☒ 3xx [redirection]
☒ 4xx [request error]
☒ 5xx [server error]

Filter by search term

☐ Regex
☐ Case sensitive
☐ Negative search

Filter by file extension

☐ Show only: asp,aspx,jsp,php
☒ Hide: js,gif,jpg,png,css

Filter by annotation

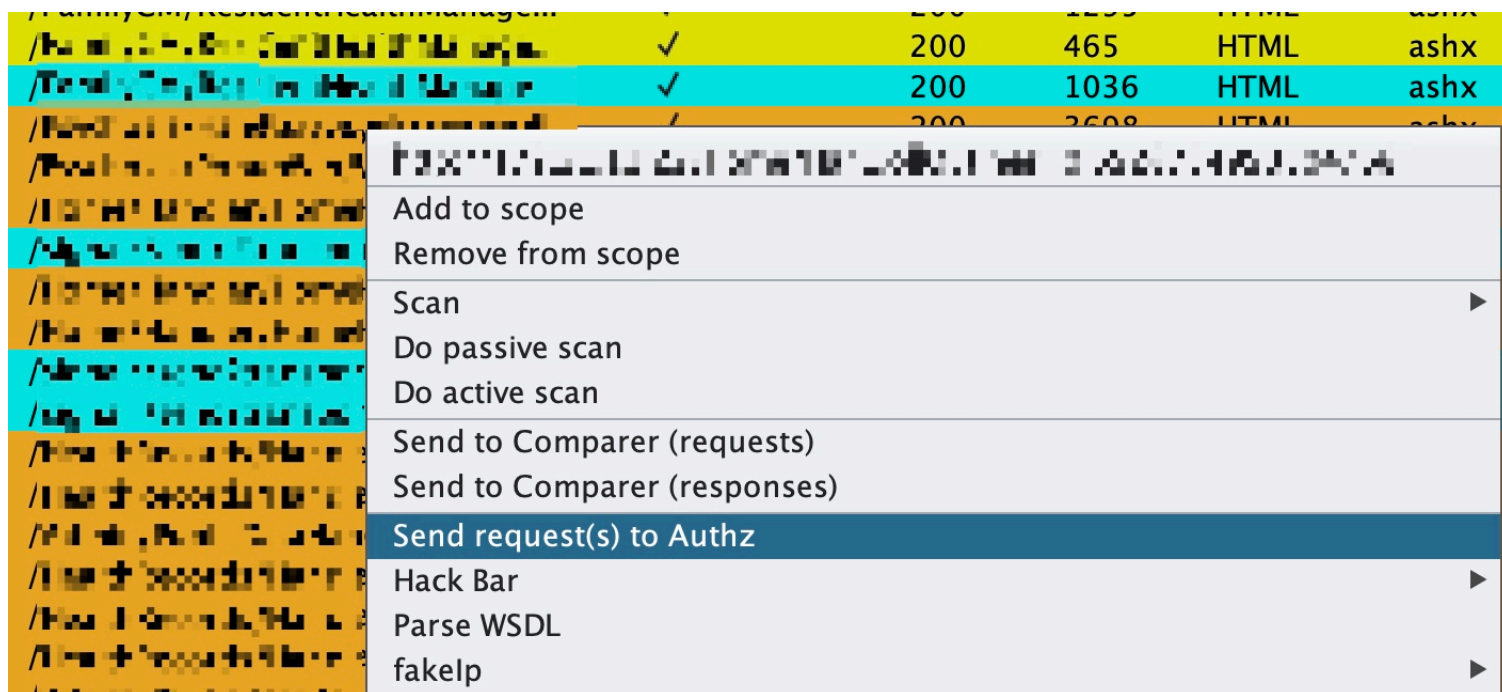
☐ Show only commented items
☒ Show only highlighted items

Filter by listener

Port

Show all
Hide all
Revert changes

选中这些高亮请求， 右击 - Send request(s) to Authz ，将高亮请求发送至Authz



这里仅测试未授权访问漏洞，将身份认证的Header（这里为Cookie）设置为123或空：

New Header

1 Cookie: 123

?
<
+
>
Type a search

然后直接RUN即可，比对原响应报文大小和替换后的大小，一样则存在未授权访问漏洞，如下图所示我已经发现了3个未授权访问漏洞：

Orig Response Size	Response Size
2258	94
2884	0
9	9
9	9
27610	22721
8212	8212
22505	22505
17324	103
80426	63
8212	8212
1604	104

同理，越权漏洞也可以用这种方式快速发现。