environment之BrowserEnv 一、二代的介绍

一代版本

browser env

作用:

1.提供真实的浏览器环境执行js脚本

2.导出全局的加密参数

3.导出全局的加密方法

缺点:

1.不能导出局部作用域的加密参数或方法

2.不能修改浏览器的请求与响应

3.不能替换js文件

--------------------------------------

以下痛点如何解决？

若加密参数不能直接引用？（加密参数不是全局的，仅在局部作用域，或者运行时环境）

若加密方法不能直接调用？（加密方法不是全局的，仅在局部作用域，或者运行时环境）

若JS文件名是动态变化的?

若JS文件代码结构是动态变化的？

--------------------------------------

二代版本

wire browser env

兼容版本:

Python 3.6+

selenium 3.4.0+

作用:

在一代版本原有的基础上

新增 mitmproxy 模块

1.支持拦截网络请求

2.捕获的 HTTP 和 HTTPS 请求

3.拦截请求和响应

4.即时修改标题、参数、正文内容

解决痛点:

若加密参数不能直接引用？（加密参数不是全局的，仅在局部作用域，或者运行时环境）

答：注入JS，将加密参数导出为全局变量， 如 window.\_\_token = token

若加密方法不能直接调用？（加密方法不是全局的，仅在局部作用域，或者运行时环境）

答：注入JS，将加密参数导出为全局变量， 如 window.\_\_func = t.func 之后需要调用则 window.\_\_func()

若JS文件名是动态变化的?

https://www.posti.fi/featureEmbed-a86bb47076742e03e8f4.js

https://www.posti.fi/featureEmbed-477d60de2122aef8b476.js

答: url.startswith('https://www.posti.fi/featureEmbed') 即可锁定该url

若JS文件代码结构是动态变化的？

答: 正则定位加密位置, 注入目标js

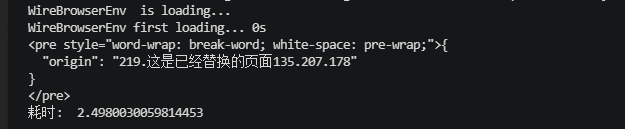
--------------------------------------

功能实现

测试例子 https://httpbin.org/ip

实现: 在一段 html 中插入文字

py文件: TestBrowserEnv.py



实战例子 FinlandPostBrowserEnv.py

实现: 将多个加密参数存为数组并导出 window.\_\_tokens={"id\_token": t.id\_token, "role\_token": t.role\_tokens[0].token};

py文件: FinlandPostBrowserEnv.py

