



学长们好呀，这里是弱鸡 web 手第一周的 writeup，由于忘记了有 wp，所以没截图，

以下全是复现，很多摸索过程有省略和缺失。做题不规范，wp两行泪（哭

一、顺风车

这一题，我先用 Burp Suite 抓包，报文扔进 Repeater send 了一下，response 出来如下

405 Not Allowed

顺风车不是这么搭的

，查了一下 405 错误是 GET 请

nginx/1.14.0 (Ubuntu)

求错误，将 请求 GET 改为 POST 后，果然出现了下一个提示

The screenshot shows the Burp Suite Professional v2020.11.1 interface. The top menu bar includes Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Project options, and User options. The main window is divided into three panes: Request, Response, and Inspector.

Request Pane: Shows a POST request to `/hitchhikerGuide.php HTTP/1.1`. The raw request is displayed in a text area, showing headers like `Host: hitchhiker42.0727.site:42420`, `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0`, and `Referer: http://hitchhiker42.0727.site:42420/`.

Response Pane: Shows the response body, which contains the text: `只有使用“无限非概率引擎”(Infinite Improbability Drive)才能访问这里~`.

Inspector Pane: Shows the response headers, including `Content-Type: text/html; charset=utf-8` and `Content-Length: 281`.

看了一下翻译，完全一脸懵逼，不能说是非常有用吧，可以说是与题目毫无关系，看来是玩梗。于是猜测是访问的引擎指的是浏览器不对。查了一下怎么改浏览器来源，找到了这篇文章

支付宝

登录/注册 会员中心 收藏 消息 创作中心

论坛 问答 代码 直播 电子书

支付宝

解析请求头部来自哪个浏览器---浏览器User-Agent

原创 bestfeng1020 2017-05-10 10:28:23 1687 收藏

分类专栏: java 基础 文章标签: 浏览器 getHeader 支付宝 微信

前言

我们一般在做项目开发中会用到支付宝或者微信等浏览器，他们对一些数据的处理是不同的，因此我们需要在此之前就知道访问来自哪儿，这时候就可以解析访问头部，来获得访问来自哪个浏览器。

一般这样的功能大多数用于支付的时候，来识别用户是用微信支付还是支付宝支付。

Demo

```
1 @RequestMapping("/index")
2 public String index(HttpServletResponse response, HttpServletRequest request,Long sid,Model m){
3     String agent = request.getHeader("User-Agent").toLowerCase();
4     int payWay = 0;
5     if (agent.toLowerCase().indexOf("micromessenger") > 0) {
6         //微信访问
7         payWay = 1;
8     } else if (agent.toLowerCase().indexOf("alipayclient") > 0) {
9         payWay = 2;
10    } else{
11        m.addAttribute("ERROR_MESSAGE", "不支持当前浏览器访问，请用微信或支付宝支付！");
12        return "/cashier/";
13    }
```

点赞Mark关注该博主,随时了解TA的最新博文

于是找了一下 User-Agent 的用法，将报文中的 User-Agent 那一行改为 User-Agent: Infinite Improbability Drive，竟然还有

你知道吗？茄子特别要求：你得从他的Cardinal过来，茄子大大的

吩咐自然要照做，查了一下 Cardinal 有框架、枢机的意思，但是还是不懂，但突然看到词条下面有这么个东西



Cardinal



https://www.oschina.net/p/cardinal/mmsi-aiadun1...

Cardinal(英语单词) - 百度百科



cardinal, 英语单词, 形容词、名词, 作形容词时意为“主要的, 基本的; 深红色的”, 作名词时意为“红衣主教; 枢机主教; 鲜红色; 人名; (英、法、德、西)卡迪纳尔”。

[单词发音](#) [短语搭配](#) [双语例句](#)

baike.baidu.com/

cardinal是什么意思 cardinal在线翻译 英语 读音 用法 例...

名词: **cardinalship** **cardinal**的英文翻译是什么意思,词典释义与在线翻译: 详尽释义 n. (名词) 【天主教】枢机主教,红衣主教 深红色,鲜红色,主教服红 【数】...

dict.cn/cardinal [百度快照](#)

其他人还在搜

[cardinal和ordinal的区别](#) [cardinal是什么意思啊](#) [cardinal中文](#) [Ordinal](#)
[giuseppe mezzofanti](#) [cardinalis](#) [Maltese](#) [cardinal number](#) [翻译](#) [fluently](#)

Cardinal (TV Series 2017–2020) - IMDb

然后找到了这个

[网页](#) [资讯](#) [贴吧](#) [知道](#) [视频](#) [音乐](#) [图片](#) [地图](#) [文库](#) [百度首页](#) [贴吧用户_aZCV2Kb](#)



刀剑神域

进入贴吧

全吧搜索

吧内搜索



刀剑神域吧

+ 关注

关注: 1,214,927 帖子: 15,575,535

签到

02月07日
漏签0天

[看贴](#) [精品](#) [视频](#) [玩乐](#)

8 回复贴, 共1页

[<返回刀剑神域吧](#)

【讨论】基数系统Cardinal和序数系统Ordinal

[只看楼主](#) [收藏](#) [回复](#)



◆一条黑茶◆

二刀流

序数是1st, 2nd, 3rd, 4st...以此类推的表明排位的工具, 电影中重村教授正是采用了茅场当时废弃的Ordinal系统来开发了序列之争这一游戏.....序数在OS中体现为【排名越靠前的人能力越强, 排名第一的玩家是不死的】这一特点。

那么SAO采用的基数Cardinal系统, 体现在什么地方了...

基数是1,2,3,4...以此类推的自然数, 用来表示量值大小的工具。是表现在了浮游城1-100层的这个设定吗.....但是后面移植到UW里面又没有浮游城这种东西, 人格化之后也没有提到这个系统到底是什么功能?

求讨论解答



皇冠身份

发帖红色标题

显示红名

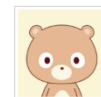
签到六倍经验

更多定制特权

兑换本吧会员

赠送补签卡1张, 获得[经验书购买权](#)

我在贴吧



贴吧用户_aZ...

0 [获取]

没想到大🐼是刀剑粉。看来是访问来源不对, 于是又去查怎么改访问来源 (此步花了我一个下午



, 最后用了手机科学上网 Google 了一下), 找到了 Referer 头的用法, 然后加上了一个

Referer 头, 从 <https://cardinal.ink/> 访问, 然后发现竟然还有, 提示 flag 仅能本地访问获得, 于是继续 Google, 是访问 IP 不是本地, 使用 X-Forwarded-For 可以伪造IP, 加上 X-Forwarded-For: 127.0.0.1

,完美搞定，获得flag一份

Response

Pretty Raw Render ↵ Actions ▾

```
hgame{s3Cret_of_HitCHhiking_in_the_GAl@xy_i5_dOnT_p@nic!}
```

二、合成大西瓜

先玩一会大西瓜，随便摆



得出分数然后抓包。本来我觉得这题目就是改一下分数就行了，结果还是加密的

```
POST /submit/telemetry/bcb8/d/e-y9eU-4dbc-ae3D-cabaZdc//b11/health/firefox/85.0/release/20210118133639?V=4 HTTP/1.1
Host: incoming.telemetry.mozilla.org
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/json; charset=UTF-8
Date: Sat, 06 Feb 2021 16:46:25 GMT
Content-Encoding: gzip
Content-Length: 329
Connection: close

{"eP8jÄ0u0zÜ²u,J2eZé¥-¥B2224a8»Jseâ*³3Äi\Y*îÈ:6e4*sQ7Mnkâm□+0XVÜ@Eie2KI\□03#1Q□BrQp;+6i□i□X·eÜNîE□□-S+6i□²Yvefiä□t□0aÜh0Iüfövk²B8FV¥.6i□1s7.â
E□×je"i/aOy/Byqi² äSi*Ci)hÄÇâdoÜLzÄ#z□Ü□laâ0uQXo|□|Üivü_¥ {RPyEpa□OâW1;□pp^E□*7b8&0E)□w8¥{'DaÜ;âmCw4oTÜsSWFos□d-/□s!8
```

完全找不到分数是哪个，一头雾水。然后完全没办法没思路，知识盲区，只能去看看审查元素，试图找到线索。最后好像找到了一个 score，但是复现不了了，忘记在哪找到的了，哭。最后刷新网页得到 flag。

三、求 100 道积分

这一题真的不会写，算完了100道题，写了一个c程序输入参数计算的，得到答案。

四、Base 家族

查了一下 Base 家族，是一种加密方式，于是先丢进 Base 64 解码，然后 Base 32，依次往下，最终得出 flag。