

Web-1 谁吃了我的 flag

根据残缺的 flag (hgame{3eek_diScI0Sure) 的 hint disclosure(泄露), 后来又要新的 hint vim 和随意关闭, vim 的特性是会存在一个隐藏的备份文件, 在文件未保存关闭时, 该备份文件会存在而不被删除。根据文件名 index.html 得到备份文件名为 .index.html 下载该文件, 以 html 格式打开即可得到 flag=hgame{3eek_diScI0Sure_fRom+wEbsit@}

Web-2 换头大作战

网页打开后点击 submit 出现 request method is error.I think POST is better 以及标题换头大作战, 就是用 bp 抓包, 将 GET 头改为 POST 后发送, 发送完后出现 https://www.wikiwand.com/en/X-Forwarded-For only localhost can get flag, 意味着要伪造 ip, 另外提示 only localhost can get flag, 而域名 localhost 对应的 ip 是 127.0.0.1, 所以要将 X-Forwarded-For 设为 127.0.0.1, 即如下图

Content-Type	application/x-www-form
Content-Length	5
X-Forwarded-For	127.0.0.1
want	

发送后出现 https://www.wikiwand.com/en/User_agent please use Waterfox/50.0 说明要修改用户代理 将其改为提示中的 Waterfox/50.0, 即如下图

Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Waterfox/50.0
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8

发送后又出现 https://www.wikiwand.com/en/HTTP_referer the requests should referer from www.bilibili.com 说明要更改 referer, 将其改为 www.bilibili.com

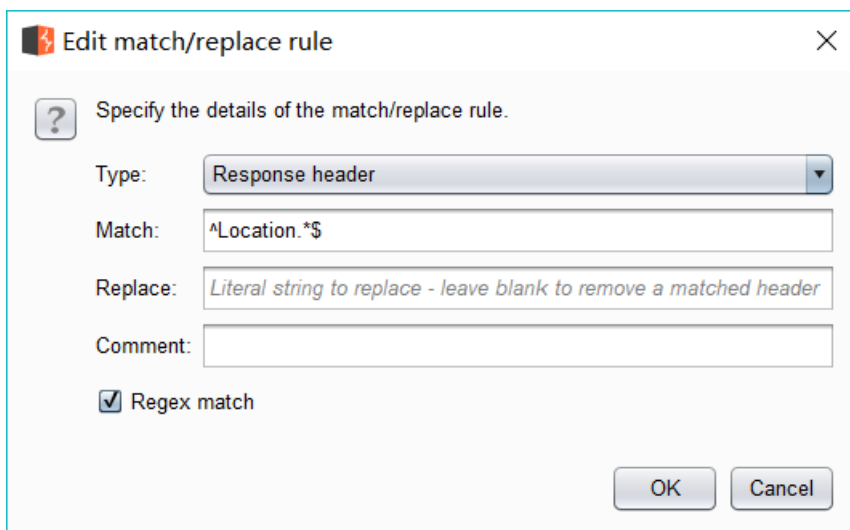
发送后又出现 https://www.wikiwand.com/en/HTTP_cookie you are not admin 于是要将 admin 设为 1, 改完发送后就得到 flag hgame{hTTp_HeaDeR_iS_Ez}

Web-3 very easy web

观察代码看到第一个 if 就发送 id 为 vidar 的 post 请求试了下, 结果如代码所说收到了干巴爹, 看到后来的 urldecode, url 解码, 然后将 vidar 进行 url 编码, 即%76%69%64%61%72 发送后又得到干巴爹, 后来搜索资料发现原来浏览器会先自己解码一次, 所以需要二次 url 编码, % 的编码为%25, 于是将 id 改为%2576%2569%2564%2561%2572 发送, 即可得到 flag hgame{urlDecode_Is_GoOd}

Web-4 can u find me?

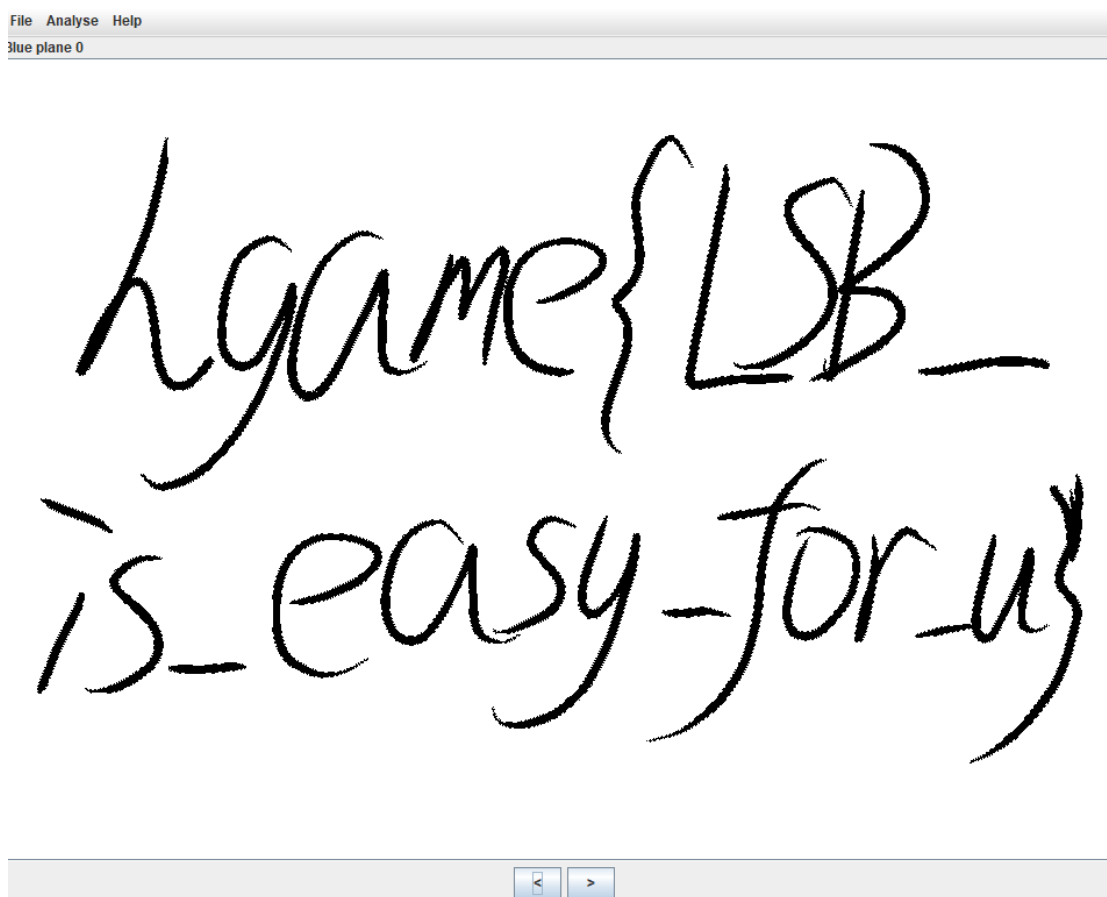
打开网页看到 the gate has been hidden can you find it? Xixixi 要找门, 查看网页源代码即可得到 f12.php, 打开后看到 yeah!you find the gate but can you find the password? please post password to me! I will open the gate for you! 于是开始寻找密码, 对网页进行检查, 最后终于在 network 中 f12.php 的 Response Headers 信息中找到了 password:woyaoflag 发送后打开了 gate, 出现了一个链接, 点进去发现从 iamflag.php 跳到了 toofast.php, 另外在 network 中 iamflag.php 的 status 为 302, 于是就寻找阻止 302 重定向的方法。在 bp 中找到 Proxy 的 options, 在 Match and Replace 添加选项, 如下图



将包拦截加上该选项后即可阻止重定向，得到 iamflag.php，从中可得到
flag:hgame{f12_1s_aMazIng111}

Misc-1 Hidden Image in LSB

如提示所说用 stegsolve 打开文件中的图片，将图片改到 Blue plane 0/Red plane 0/Green plane 0 状态，如下图



Misc-2 打字机

根据 flag 格式，可以猜出前五个字母为 hgame，e 的字母符号也得到，可以应用于后面，根据打字机图片可把所有的大写字母根据键盘上字母的位置都猜出来，根据小写于大写的相近可以猜出个别小写，猜出了几个字母后发现最后一部分好像是打字机的英文 typewriter，于是就猜出了一三部分的所有字符，中间部分的字符再根据字型猜测，于是就得到 flag hgame{My_violet_tyPewRiter}

Misc-3 Broken Chest

下载文件后发现无法解压，把它作为 txt 打开，发现其中有 flag.txt，还看到开头是 OK，压缩包的开头一般为 PK，开头的十六进制码一般为 50 4B 03 04，用 010 edit 打开查看十六进制码发现是 4F 4B 03 04 于是将 4F 改为 50 保存后打开压缩包，发现需要密码，不过这次的密码直接给了我们 S0mETh1ng_U5efuL，输入后得到 flag hgame{Cra2y_D1aM0nd}

Crypto-1 Mix

看到.-先摩尔斯电码解密解得 744B735F6D6F7944716B7B6251663430657D 然后这是十六进制 ASCII 码，解得 tKs_moyDqk{bQf40e}，根据 hgame 是五个字符所以进行栅栏解密，得到 tsnyq{Q4eK_oDkbf0} 然后凯撒解密得到 hgame{E4sY_cRypt0}