5i1encee#0x000320-WEEK2-WP

5i1encee#0x000320

问卷

明年见！

填写问卷，复制粘贴

Web

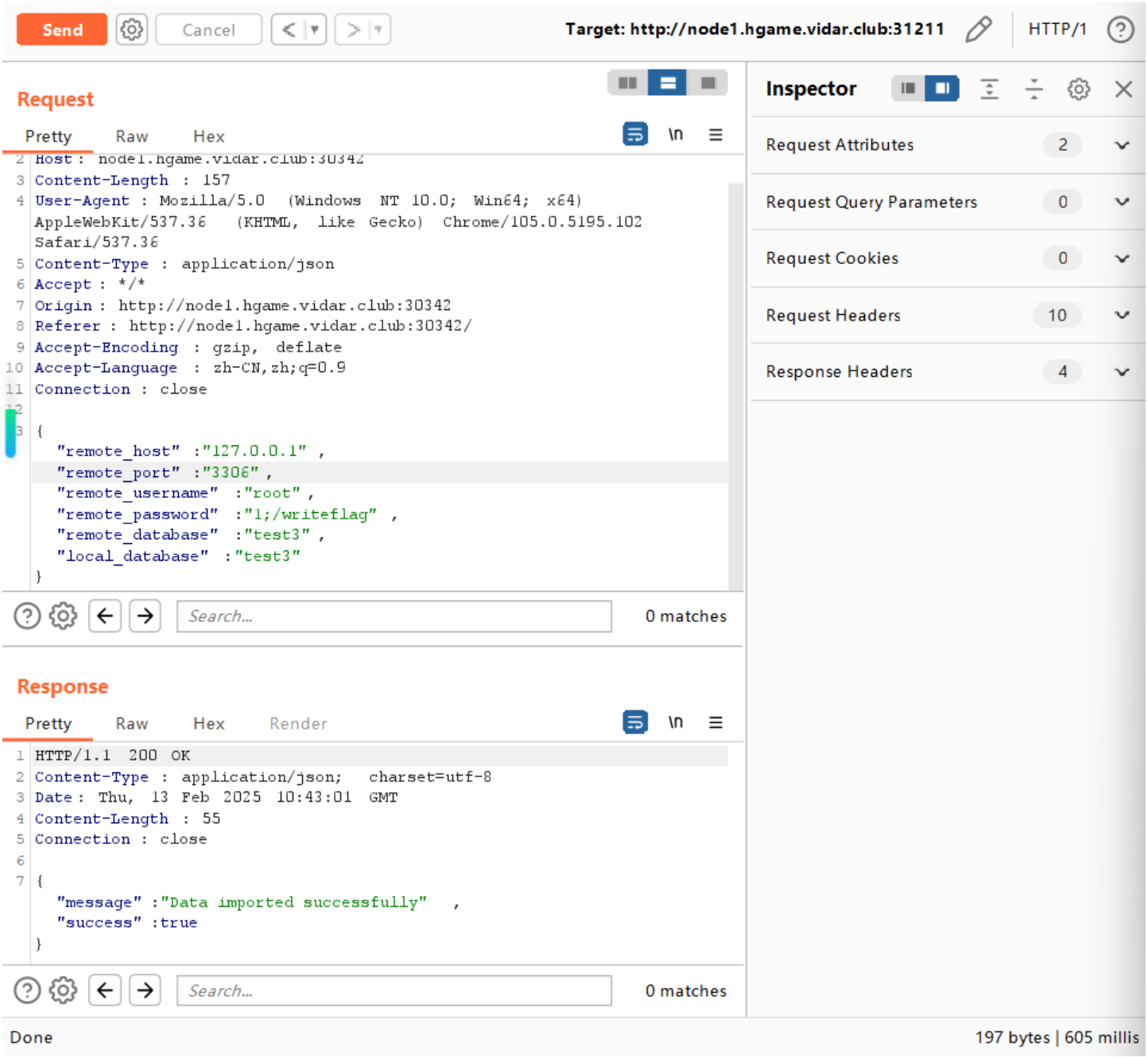
Level 21096 HoneyPot

目录扫描，存在 `/flag`，直接访问为 `fake_flag`

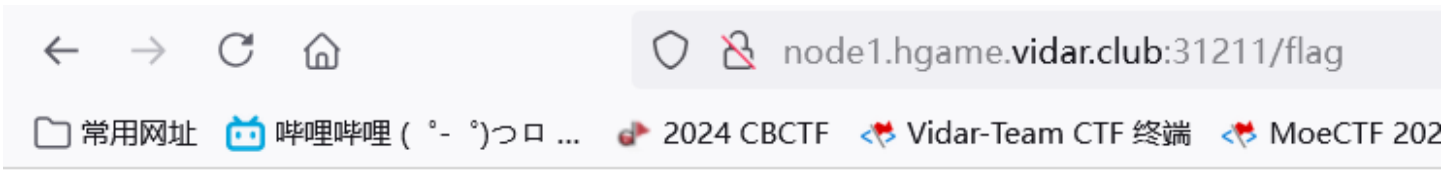
审计附件源码 `main.go`，主要实现了数据库连接测试、导入、查询这几个功能，发现存在函数 `sanitizeInput()` 和 `validateImportConfig()` 对各种输入严格过滤。

在注释的附近发现各个参数先拼接为字符串command，再用 `cmd := exec.Command("sh", "-c", command)` 执行命令，其中参数 `config.RemotePassword` 遗漏了对输入的过滤，从而可以实施命令注入。

点击导入数据，截包，在 `remote_password` 字段处加 `;` 来截断前面的命令，然后执行 `/writeflag`



再访问 `/flag`，得到flag



hgame{e562408d-96b6-24bc-b9ed-4c1301bade58}