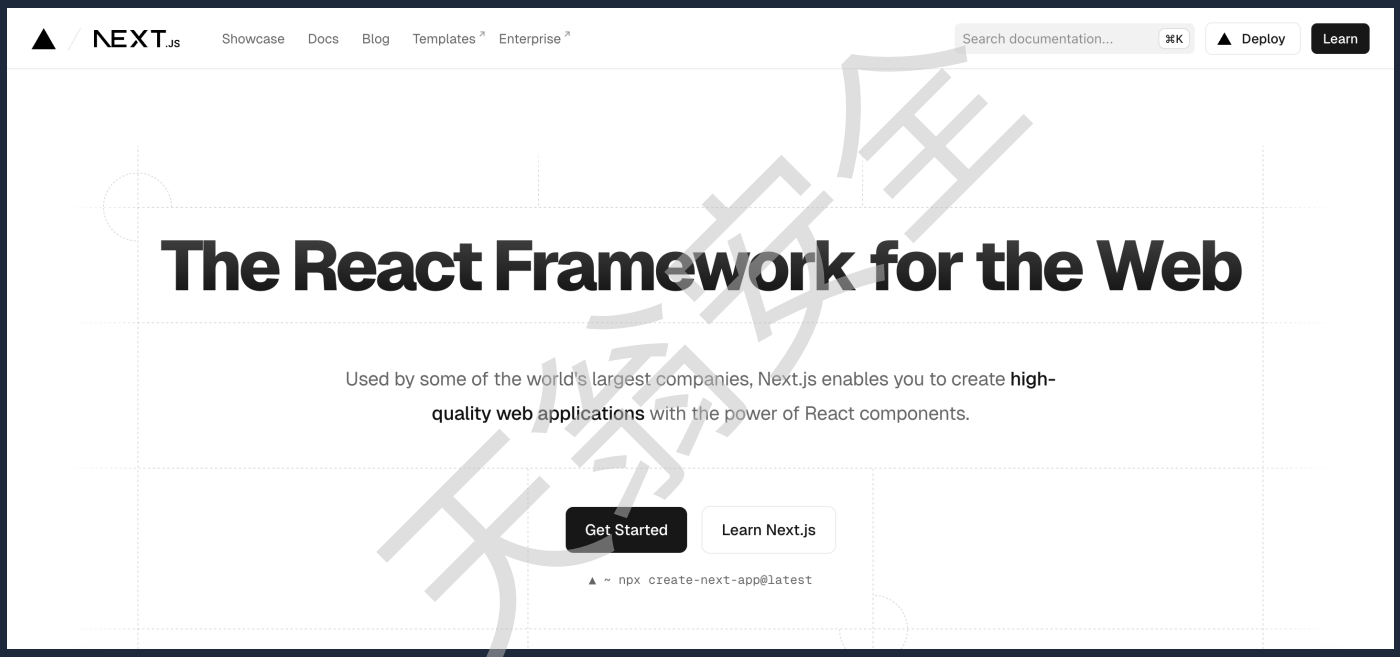
Next.js中间件授权绕过漏洞（CVE-2025-29927）

漏洞介绍

Next.js 是一个基于 React 的前端开发框架，旨在构建高性能的 Web 应用。它支持服务器端渲染（SSR）、静态网站生成（SSG）、增量静态生成（ISR）等多种渲染方式，提升页面加载速度和 SEO 效果。Next.js 还内置了路由系统、API 路由、图片优化和 TypeScript 支持，极大简化了开发流程，非常适合用于构建现代化的全栈 Web 应用。



CVE-2025-29927 是 Next.js 中间件存在的一个授权绕过漏洞。攻击者可通过在 HTTP 请求中注入 `x-middleware-subrequest` 请求头，绕过中间件中的授权检查，直接访问受保护的路由。此漏洞影响了 11.1.4 至 13.5.6、14.0 至 14.2.24，以及 15.0 至 15.2.2 版本的 Next.js。官方已在 14.2.25 和 15.2.3 版本中修复了该问题。建议受影响的用户尽快升级至最新版本，或采取措施阻止包含 `x-middleware-subrequest` 请求头的外部请求。

漏洞条件

- 对于Next.js 15.x，< 15.2.3
- 对于Next.js 14.x，< 14.2.25
- 对于Next.js 13.x，< 13.5.9
- 对于Next.js 12.x，< 12.3.5

可以看到，几乎升级前所有版本的Next.js都收到了影响，可见影响范围之广。

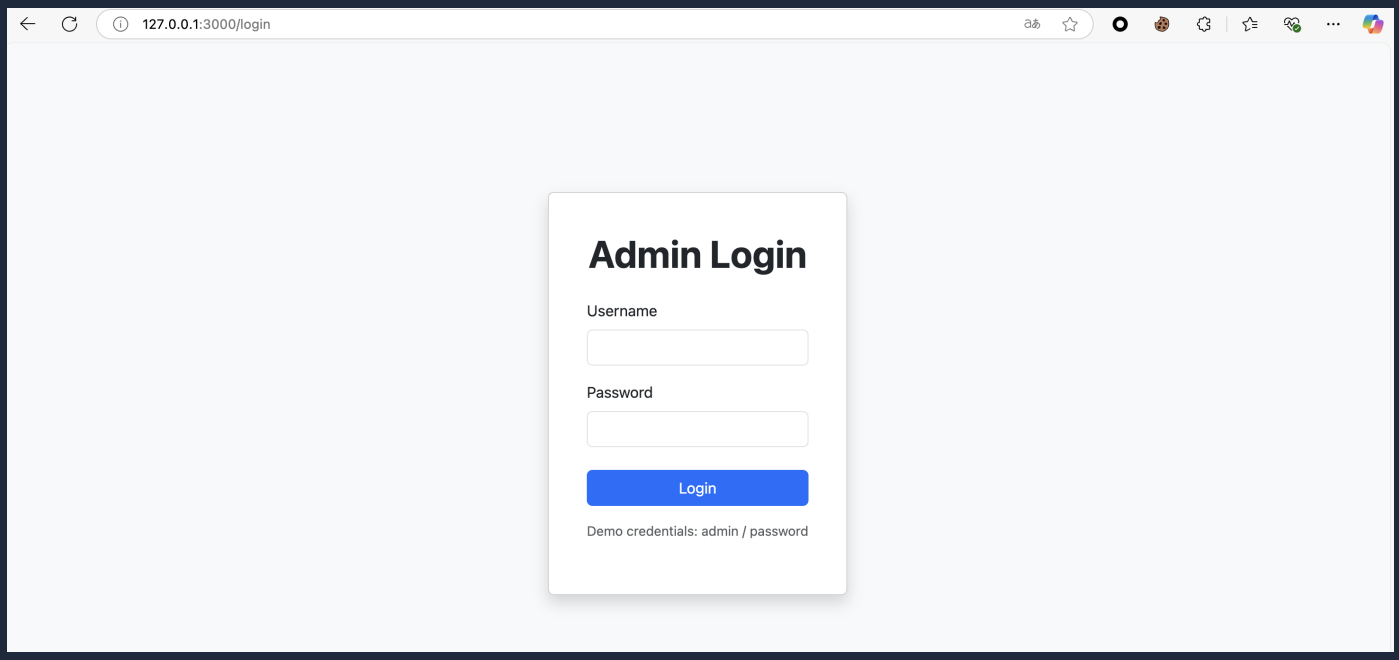
环境搭建

解压复现环境的文件夹

执行一条命令即可搭建好漏洞环境

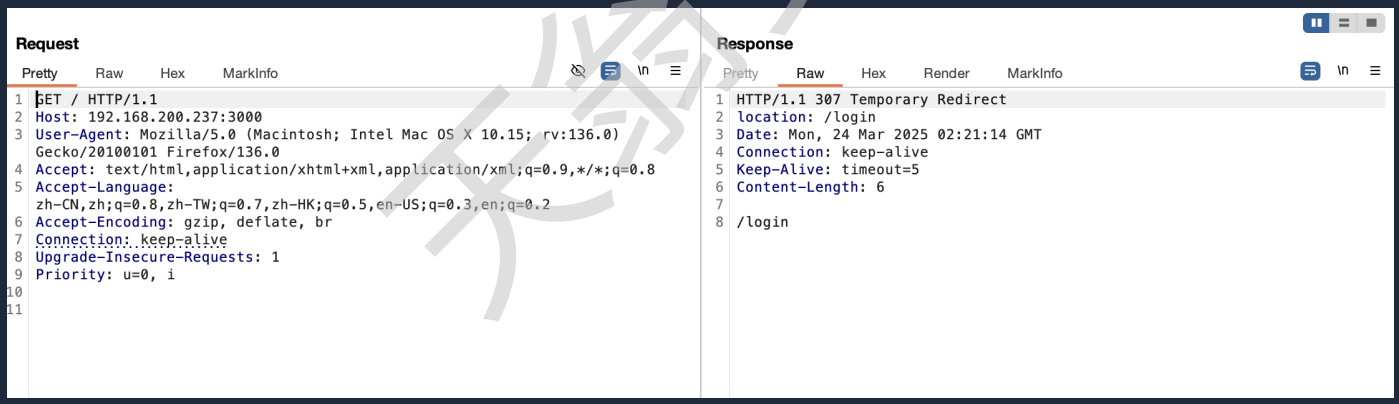
```
docker-compose up -d
```

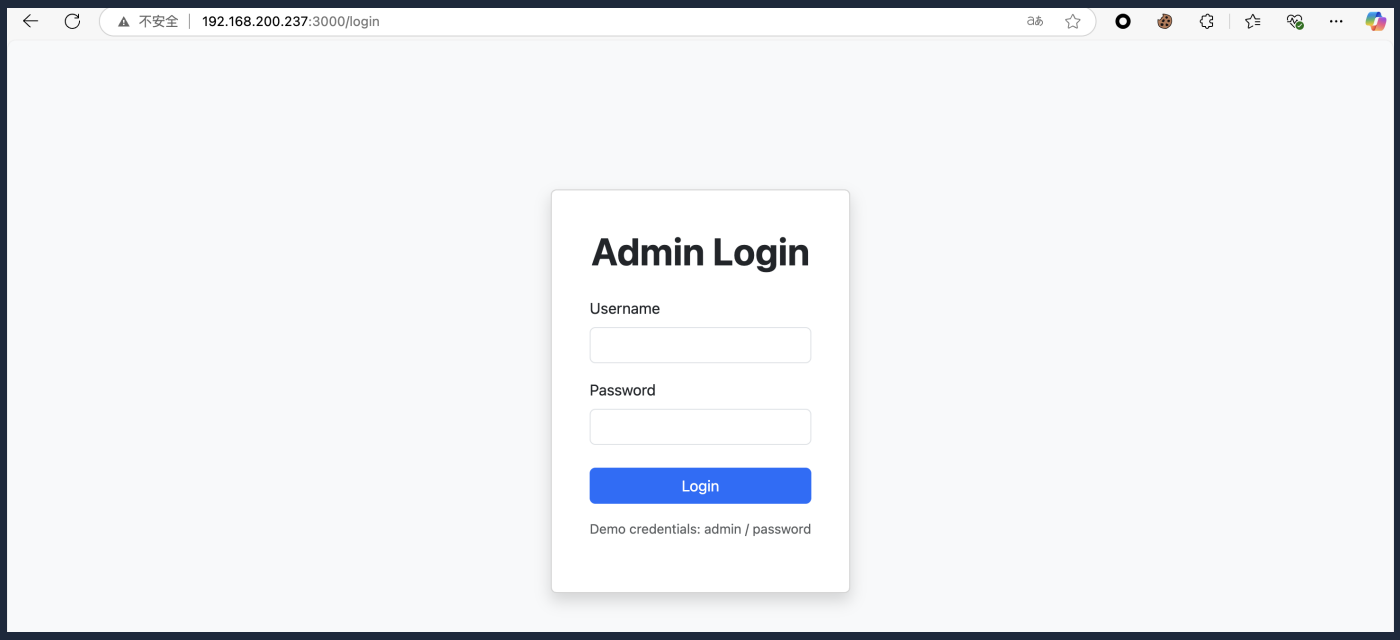
访问 http://your-ip:3000 即可



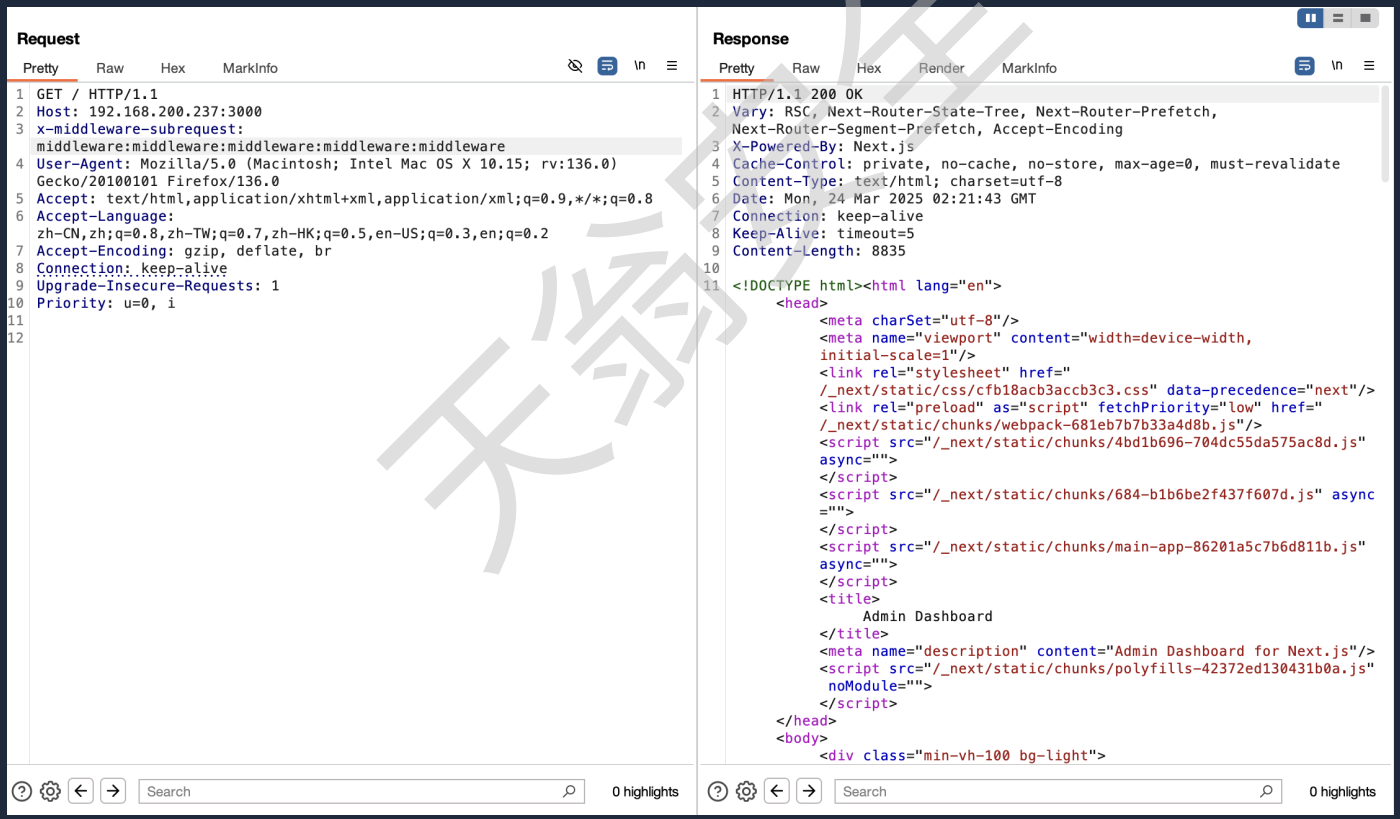
漏洞复现

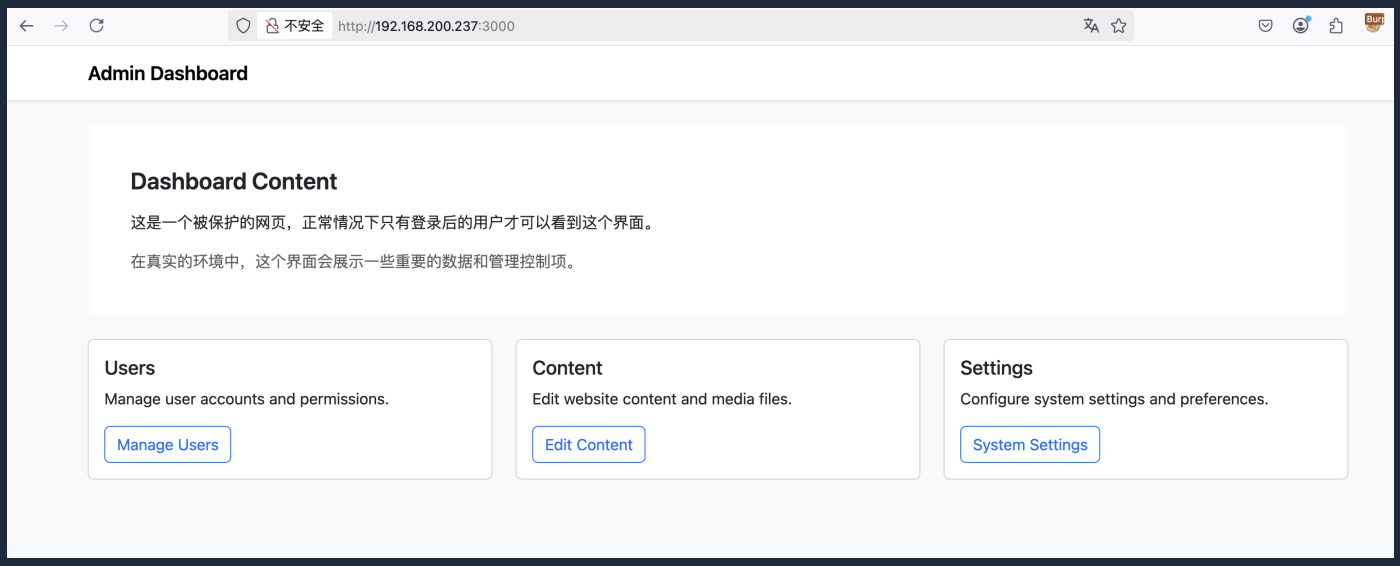
我们正常访问 http://your-ip:3000 发现页面会跳转至登录界面





添加请求头后访问 http://your-ip:3000 发现直接绕过了登录校验成功进入了后台





漏洞修复

临时解决方案：

- 在网关/代理层过滤或删除所有外部请求中的 `x-middleware-subrequest` 头

解决方案：

- 对于Next.js 15.x，升级到 `15.2.3` 及以上版本
- 对于Next.js 14.x，升级到 `14.2.25` 及以上版本
- 对于Next.js 13.x，升级到 `13.5.9` 及以上版本
- 对于Next.js 12.x，升级到 `12.3.5` 及以上版本