SAMPLE

WEB 应用
渗透测试报告

虚构样例，用于展示 YNM3000 的测试范围、漏洞证据、修复建议和复测结构。

目标	访问	日期	密级
app.example.test	外部 + 测试账号	JUL 2026	CONFIDENTIAL

01 / 总览

管理摘要

本虚构样例从外部攻击者视角，使用一个低权限测试账号评估一个 SaaS Web 应用。测试记录 1 个高危、2 个中危、3 个低危和 4 个提示项。最重要的问题是对象级授权缺失导致跨租户发票元数据泄露。

整体风险	高危	中危	低危 + 提示
风险偏高	1	2	7

优先行动

- 在下一次生产发布前优先修复跨租户授权问题。
- 账号身份信息发生变化后，立即使已有密码重置 Token 失效。
- 为每个发票对象读取操作应用一致的授权校验。
- 在套餐包含的 14 天窗口内复测严重和高危修复。

02 / 测试约定

范围与测试方法

测试边界必须明确。发现的新资产不会自动加入范围，所有测试始终遵守已确认的测试约定。

字段	样例确认值
测试目标	https://app.example.test
访问级别	外部测试 + 一个低权限测试账号
测试窗口	2026 年 7 月 7 日 02:00-06:00 UTC
排除范围	status.example.test、破坏性操作、批量数据访问
紧急联系人	security@example.test（虚构）
方法参考	OWASP WSTG、OWASP Top 10、基于风险的验证

测试方法

- 应用和技术发现
- 认证与会话行为
- 授权和对象所有权
- 输入处理和服务端请求行为
- 安全配置和信息暴露
- 聚焦业务逻辑测试
- 证据复核、风险判断和修复验证

安全限制

- 不进行拒绝服务、凭据攻击、持久化或横向移动
- 采用保守请求速率，出现不稳定立即停止
- 除临时测试对象外不修改数据
- 证据最小化，并对秘密和个人数据脱敏

03 / 漏洞

漏洞汇总

风险等级来自虚构范围内已验证的可利用性和影响，不是通用扫描器评分。

编号	等级	漏洞	状态
Y3K-001	高危	跨租户发票元数据泄露	未修复
Y3K-002	中危	邮箱变更后重置 Token 仍然有效	未修复
Y3K-003	中危	账单导出缺少二次身份确认	未修复
Y3K-004	低危	会话 Cookie 缺少 SameSite 策略	未修复
Y3K-005	低危	暴露详细框架错误标识	未修复
Y3K-006	低危	账号页面缓存策略不一致	未修复

高危

04 / 漏洞详情

Y3K-001 - 跨租户发票元数据泄露

低权限用户可以请求属于另一个虚构租户的发票标识。API 在返回发票元数据前没有验证对象所有权。

影响

持有有效账号的攻击者可能枚举标识，并读取其他租户的发票编号、日期、币种、金额和内部客户引用。本样例响应不包含银行卡数据。

复现步骤

1. 使用已提供的低权限测试账号登录。
2. 读取该账号自己的样例发票，并记录对象标识格式。
3. 只把对象标识替换为另一个已授权虚构测试对象。
4. 观察 HTTP 200 响应中返回了另一个虚构租户的元数据。

脱敏证据

```
GET /api/invoices/inv_sample_024 -> HTTP 200
会话租户：tenant_alpha
对象租户：tenant_beta
所有敏感值均替换为虚构占位符。
```

修复建议

- 在服务端对每次发票对象读取强制执行租户和对象所有权校验。
- 使用集中授权策略，而不是在不同控制器中分别实现校验。
- 对不存在和未授权对象返回相同且不泄露信息的响应。
- 为每个发票读取、导出、更新和附件接口增加负向授权测试。

中危

05 / 漏洞详情

Y3K-002 - 账号身份变更后密码重置 Token 仍有效

账号邮箱变更后，之前签发的密码重置 Token 仍可继续使用。已经泄露的旧 Token 因此保留了超出预期的价值。

影响

如果 Token 在账号身份或安全信息变更前被截获，攻击者仍可能在其原有效期内继续使用。本测试只使用专门为虚构样例创建的账号。

复现步骤

1. 为授权测试账号申请密码重置链接。
2. 通过正常个人资料流程修改账号邮箱。
3. 使用之前签发的重置 Token。
4. 观察重置流程继续执行，而不是拒绝已经过期的安全上下文。

脱敏证据

证据记录在受保护报告中。

修复建议

- 将重置 Token 绑定到当前身份版本或凭据版本。
- 邮箱、密码、MFA 或恢复方式变化后，使所有未使用重置 Token 失效。
- 采用短有效期，并在服务端保证 Token 只能消费一次。
- 记录并告警 Token 重复使用，或安全信息变化后的使用行为。

06 / 覆盖

覆盖范围、观察与限制

某个类别没有确认漏洞，并不能证明目标不存在该类弱点，只能说明在既定时间、权限和应用状态下完成了哪些评估。

已测试

- 登录、退出、密码重置与会话终止
- 发票和个人资料的租户级对象访问
- 常见输入路径与文档化同源 API
- 安全响应头、Cookie 属性、缓存和错误行为
- 部分账单和账号业务流程

未测试

- 其他主机名或第三方集成
- 移动应用、云控制面、内网或源码
- 未向测试提供的管理员角色
- 拒绝服务、社会工程、凭据攻击或破坏性操作
- 测试窗口后发布或发生重大变化的功能

07 / 修复

修复优先级路线图

先修复授权控制，再降低账号恢复和会话风险。应该在相似接口中验证授权控制模式，而不是只修补样例请求。

时间	负责人	行动	验证
0-72 小时	后端	统一所有发票操作的租户所有权校验	跨租户负向 API 测试
0-72 小时	安全	检查日志中的异常发票标识访问	记录审查和告警测试
14 天	身份团队	安全信息变化后使重置 Token 失效	变化前后对比测试
14 天	平台	统一安全 Cookie 和缓存策略	响应头回归测试
30 天	研发	在 CI 中增加授权测试矩阵	覆盖所有对象 API

系统性修复

不要只修补样例对象 ID。应盘点所有租户对象接口，通过共享的服务端控制和负向测试，对同类接口执行一致授权策略。

08 / 复测

复测附录与评估限制

本样例展示套餐包含的修复验证如何记录。真实复测只覆盖报告交付后 14 个自然日内集中提交一次的原报告严重和高危漏洞修复。

漏洞	原始状态	复测状态	证据
Y3K-001	高危 / 未修复	未执行	仅为报告样例
Y3K-002	中危 / 未修复	不在套餐复测内	只包含严重和高危
Y3K-003	中危 / 未修复	不在套餐复测内	只包含严重和高危

重要限制

- 本文档是虚构设计样例，不是真实安全评估。
- 限时渗透测试无法保证发现所有漏洞。
- 代码、配置、基础设施、身份或依赖变化后，风险也会变化。
- YNM3000 报告属于技术评估，不是合规认证或法律意见。
- 任何真实测试开始前都必须获得客户授权并确认测试约定。

联系：support@ynm3000.com | 仅测试已授权系统 | ynm3000.com