Segway-Ninebot 滲透測試 — 第二階段漏洞報告

> 測試時間：2026-07-11
> 測試者：Linux Hermes（接手 Windows Hermes 第一階段）
> 授權：Segway-Ninebot 集團
> 測試範圍：briefing 列出的 6 組 domain
> 本機出口：43.160.194.36（Tencent Cloud）
> 報告分類：依「漏洞盒子」收錄類型，僅呈現以下 8 類
> 1. SQL 注入 2. XSS 3. CSRF 4. 越权 5. 文件上傳/包含 6. RCE 7. 敏感信息泄露 8. 邏輯漏洞

漏洞統計

#	類別	確認漏洞數	待驗證數
1	SQL 注入	0	1（潛在）
2	XSS	0	0
3	CSRF	1	0
4	越权	0	1（攻擊面）
5	文件上傳/包含	0	0
6	命令/代碼執行	0	0
7	敏感信息泄露	11	2
8	邏輯漏洞	0	1（潛在）
合計		12	5

#7 敏感信息泄露（11 個確認漏洞 — 主要發現）

S1. SSL 證書 SAN 暴露內網 Exchange Server 拓撲【HIGH】

項目	內容
目標	`segwayrobotics.com:443`
證據	SSL 證書 SAN 包含內部 hostname
風險	暴露內部 MS Exchange Server 存在，attacker 可針對 OWA 做釣魚/字典攻擊

證據鏈：

```
$ openssl s_client -connect segwayrobotics.com:443 -servername segwayrobotics.com
X509v3 Subject Alternative Name:
    DNS:*.segwayrobotics.com
    DNS:owa.segwayrobotics.com         ← Outlook Web Access
    DNS:mail.segwayrobotics.com        ← Mail Server
    DNS:autodiscover.segwayrobotics.com ← Exchange 自動發現
    DNS:segwayrobotics.com
```

影響：直接證實內部 MS Exchange 部署，OWA 易受密碼噴灑/釣魚。

修復建議：為 OWA 簽發獨立證書，不在公開證書中暴露內部 hostname；或使用 wildcard 內網證書。

S2. DNS A 記錄洩漏內網 IP【MEDIUM】

項目	內容
目標	`git/iot/cloud/doc.ninebot.com`
證據	DNS 解析到 RFC 1918 私有地址

子域名	內網 IP	公網可達
git.ninebot.com	10.30.33.5	（防火牆擋）
iot.ninebot.com	10.64.20.98	
cloud.ninebot.com	10.64.20.38	
doc.ninebot.com	10.64.2.24	

影響：內網拓撲洩漏（內網 IP 段 10.30.x、10.64.x），雖公網不可達，仍為信息洩漏。

修復建議：移除公開 DNS 中對內網 IP 的 A 記錄，改用內部 DNS zone。

S3. Titan Operations Hub HTML 硬編碼 APM Plus 認證 Token【HIGH】

項目	內容
目標	`https://platform.ninebot.com/`
證據	HTML 中 inline JavaScript 暴露 APM token

證據鏈（GET `/`）：

```
<script>
  window.apmPlus('init', {
    aid: 661495,
    token: '574703cd874a4265a317b98520692468',
    env: getEnv(),
  });
</script>
```

SDK 來源：`https://apm.volccdn.com/mars-web/apmplus/web/browser.cn.js`（火山引擎 APM Plus）

影響：APM Plus token 洩漏。若該 token 可用於訪問火山引擎控制台或 APM 數據 API，attacker 可查看應用性能指標、用戶行為追蹤、錯誤堆疊等。

附帶發現 — 環境自動識別邏輯（洩漏內部環境命名）：

```
const getEnv = () => {
  if (hostname.includes('localhost')) return 'localhost';
  if (hostname.includes('dev')) return 'dev';
  if (hostname.includes('test')) return 'test';
  return 'prod';
};
```

修復建議：將 token 移到後端通過 session 注入；或使用臨時 token 機制。

S4. SSO JS Bundle 硬編碼 WeChat Work appid + 內部 CLIENT_ID【MEDIUM】

項目	內容
目標	`https://sso-app.ninebot.com/assets/index.ff7ad437.js`（1.27 MB）
證據	JS 源碼中硬編碼 OAuth credentials

證據鏈：

```
appid:"wxadb49f0cd1c87ae5"           // WeChat Work appid
CLIENT_ID:"1914672980459130881"      // 內部 SSO client identifier
```

影響：WeChat Work appid 雖為公開 OAuth 配置，但結合 CLIENT_ID 與其他內部 hostname 洩漏（S5），attacker 可分析 OAuth 流程，構造偽造登入頁。

修復建議：將 WeChat appid 移到後端配置；CLIENT_ID 屬於後端憑證不應出現在前端。

S5. Titan Hub JS Bundle 暴露完整內部基礎設施拓撲【HIGH】

項目	內容
目標	`https://platform.ninebot.com/assets/index.3d821b1f.js`（599 KB）
證據	JS bundle 內含內部 host URL

證據鏈（從 JS grep）：

```
https://api5-h5-app-test-bj.ninebot.com/titanAgent/
https://cn-cbu-gateway.ninebot.com
https://cn-dev-oms-gateway.ninebot.com
https://cn-test3-oms-gateway.ninebot.com
https://dev-doc.ninebot.com/
https://sso-app.ninebot.com
https://sso-dev-app.ninebot.com
https://sso-test-app.ninebot.com
https://m1.apifoxmock.com/m1/6231527-5925205-default   ← APIFox mock
https://doc.weixin.qq.com/sheet/e3_ADoAWwaFAMQCNM5Vh55Z3RlyA4ECz  ← 微信內部文檔
```

附帶發現（SSO JS）：

```
dev-app.ninebot.com
dev.ninebot.com
dev-oms-gateway.ninebot.com
test-app.ninebot.com
test.ninebot.com
```

影響：
- 完整生產/測試/開發環境拓撲圖
- APIFox mock URL 暗示他們的 API 設計文檔（可能含 request/response schema）
- 微信文檔連結可能含員工聯絡方式、內部電話

修復建議：前端 bundle 僅暴露必要 endpoint；內部 host 走反向代理；移除 mock/dev URL。

S6. Saturn-Portal RBAC API 表面完整洩漏【HIGH】

項目	內容
目標	`https://platform.ninebot.com/saturn-portal/api/...`
證據	Titan Hub JS bundle 含 30+ RBAC API path

完整清單：

```
/saturn-portal/api/auth/v1/me
/saturn-portal/api/common/user/account/detail-v2
/saturn-portal/api/common/role-manager/v2/role-list
/saturn-portal/api/common/role-manager/v1/detail
/saturn-portal/api/common/role-manager/v2/role-log-list
/saturn-portal/api/common/role-manager/v1/set-data-permission
/saturn-portal/api/common/role-manager/v2/has-old-role
/saturn-portal/api/common/role-manager/v2/role-suggest
/saturn-portal/api/common/role-manager/v1/show-data-scope
/saturn-portal/api/common/tenant-manager/v1/list
/saturn-portal/api/common/data-res-manager/v1/list
/saturn-portal/api/common/application-manager/v1/list
/saturn-portal/api/common/nav-manager/v1/all-nav
/saturn-portal/api/common/factor-def-manager/v1/list
/saturn-portal/api/common/factor-value-manager/v1/factor-tree
/saturn-portal/api/commondownload/download/v1/list
/saturn-portal/api/commondownload/download/v1/remove
/saturn-portal/api/common/nav-manager/v1/quick-nav/{add,list,remove,sort}
/api/permissions
/api/routes
```

影響：完整 RBAC API 表面洩漏，包含：
- 用戶帳號 CRUD（`user/account/detail-v2`）
- 角色管理（讀取/設定權限）— 含 `set-data-permission` 寫操作
- 租戶清單（多組織架構洩漏）
- 應用、資料資源、導航管理

attacker 可針對這些 API 構造攻擊腳本。

修復建議：前端僅暴露必要 path；後端做嚴格 RBAC 校驗；API 需 Bearer token 認證。

S7. Spring Boot Actuator 端點存在於開發環境【MEDIUM】

項目	內容
目標	`https://cn-dev-oms-gateway.ninebot.com/actuator` `https://cn-test3-oms-gateway.ninebot.com/actuator`
證據	`/actuator` 返回 403（不是 404）= 端點存在但 WAF 阻擋

測試響應：
- `GET /actuator` → 403 Forbidden（騰訊雲 WAF 攔截頁面）
- WAF UUID 洩漏：`6d57eabd3d931b8b99db52809bbe0f56-57ec41d180ac4bc67b455b105fbff987`
- 自定義 404 格式：`{"timestamp":"...","code":1,"message":"Server error","status":404}`（中國開發框架常見）

影響：Spring Boot Actuator 若未正確保護，洩漏 `/env`、`/heapdump`、`/configprops`、`/mappings`、`/beans`，可能包含數據庫連接字串、密鑰、內部服務地址。

修復建議：
- 生產環境禁用 actuator 或限制為內網
- 自定義 404 不應洩漏框架信息

S8. datasink-bj.ninebot.com 預設 nginx 歡迎頁【LOW-MEDIUM】

項目	內容
目標	`https://datasink-bj.ninebot.com/`
證據	顯示預設 nginx welcome page

證據：

```
<title>Welcome to nginx!</title>
```

影響：該主機未正確配置即上線，表明運維流程缺失；可能暴露後續部署意圖。

修復建議：立即配置反向代理或關閉；設置自定義 404/默認頁。

S9. ai-kb-private.ninebot.com 服務存在性暴露【LOW】

項目	內容
目標	`https://ai-kb-private.ninebot.com/`
證據	403 Forbidden（nginx）

影響：雖無內容洩漏，但 403 確認「私有 AI 知識庫」服務存在於公網，可能成為下一階段攻擊目標。

修復建議：限制僅內網/VPN 訪問。

S10. opsvpn.ninebot.com — NetBird VPN 管理後台公網暴露【HIGH】

項目	內容
目標	`https://opsvpn.ninebot.com/`
證據	Next.js NetBird Dashboard 直接可訪問

證據鏈：

```
<title>NetBird Dashboard</title>
<meta name="description" content="NetBird combines a configuration-free
peer-to-peer private network and a centralized access control system
in a single open-source platform"/>
```

Next.js 構建 ID：`bp-M570C04Pwumt3Y536R`

影響：NetBird 是 P2P VPN + 集中訪問控制平台。一旦獲得認證即可查看：
- 所有 peer（員工/伺服器 VPN 節點）
- 所有 policy（訪問規則）
- 所有 route（網絡路由）
- 所有 setup-key（VPN 加入密鑰）

修復建議：
- 限制僅內網/VPN 可訪問
- 啟用 SSO + MFA
- 檢查 audit log 有無異常登入嘗試

S11. cn-dev-oms-gateway 根路徑返回內部服務名【LOW】

項目	內容
目標	`https://cn-dev-oms-gateway.ninebot.com/`
證據	根路徑返回字串 `"ninebot gateway"`

影響：開發/測試環境未做 hardening，內部服務名直接暴露。

#3 CSRF 漏洞（1 個確認）

CSRF1. Titan Operations Hub CORS 配置過寬【MEDIUM】

項目	內容
目標	`https://platform.ninebot.com/`
證據	CORS 允許任意來源 + 接受 Authorization header

證據鏈（HTTP 響應 headers）：

```
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Content-Type, Authorization
```

影響：
- 寬鬆 CORS + 接受 Authorization header → 若 saturn-portal 使用 cookie 認證，attacker 可通過跨域請求偽造受害者操作
- 即便使用 Bearer token，仍可能對 GET 請求造成信息洩漏（如 `/auth/v1/me` 暴露用戶信息）
- POST/PUT/DELETE 方法全開啟為 CSRF 提供基礎

對比：Saturn-portal OPTIONS 跨域返回 403 Forbidden（CORS 嚴格），但 platform 根 path 寬鬆。

修復建議：
- `Access-Control-Allow-Origin` 限制為 `https://*.ninebot.com`
- 對 state-changing 請求加入 CSRF token 或 SameSite cookie

#4 越权漏洞（攻擊面確認）

AUTHZ1. Saturn-Portal API 缺乏可見認證校驗（需授權測試）【待驗證】

項目	內容
目標	`https://platform.ninebot.com/saturn-portal/api/...`
證據	所有 saturn-portal 端點返回 SPA shell（無 401/403 直接暴露）

測試結果：
- `GET /saturn-portal/api/auth/v1/me` → 200 (SPA shell)
- `GET /saturn-portal/api/common/role-manager/v2/role-list` → 200 (SPA shell)
- `GET /saturn-portal/api/common/user/account/detail-v2?userId=1` → 200 (SPA shell)

注意：SPA 路由對所有路徑都返回 index.html，curl 直接打不到後端。需瀏覽器 session + Bearer token 才能驗證 IDOR。

潛在風險（基於 API 設計）：
- `user/account/detail-v2?userId=X` — 若後端僅根據 userId 查詢未校驗當前用戶權限，可讀取任意用戶資料（水平越权）
- `role-manager/v1/set-data-permission` — 若無 role-based 校驗，可修改任意角色權限（垂直越权）
- `tenant-manager/v1/list` — 多租戶架構洩漏
- `data-res-manager/v1/list` — 資料資源清單洩漏

修復建議：
- 後端對每個 API 做嚴格 RBAC 校驗
- 記錄越权嘗試到 audit log

#1 SQL 注入漏洞（潛在，需深入測試）

SQLI1. SSO 登入端點 WAF 不完美 + 弱輸入校驗【POTENTIAL】

項目	內容
目標	`https://sso-app.ninebot.com/user/api/sso/v1/login`
證據	部分 SQLi payload 通過 WAF 但無明確注入確認

測試結果：

```
正常 JSON                → {"code":1,"msg":"Server error"} （校驗薄弱）
SQLi OR '1'='1'          → WAF 攔截
SQLi UNION SELECT        → WAF 攔截
SQLi AND SLEEP(5)        → WAF 攔截
SQLi 註釋繞過 admin"/*"  → 通過 WAF, 返回 "Server error"（未確認注入）
form-encoded HPP         → WAF 攔截
```

WAF 分析：騰訊雲 WAF 對常見 SQLi pattern 攔截有效，但：
- 註釋繞過（`/**/`）未攔
- 不說明「缺少欄位」只說「Server error」= 輸入校驗薄弱

未確認因素：
- 通過 WAF 的 payload 是否真實觸發 SQL 錯誤？
- 後端是否使用 ORM（MyBatis/Hibernate）？ORM 通常對 SQLi 免疫
- 需要更多編碼變換測試（chunked transfer, HTTP/2, double URL encode）

修復建議：
- 加強輸入校驗，明確區分「缺少欄位」「認證失敗」「系統錯誤」
- 即使有 WAF，後端必須使用參數化查詢（Prepared Statements）
- 添加 rate limiting

#8 邏輯漏洞（潛在）

LOGIC1. SSO SMS 驗證碼端點路徑不明確【待驗證】

項目	內容
目標	`https://sso-app.ninebot.com/...`
證據	JS 中含 `/user/api/sso/v1/todo-list/send/verify` 路徑

測試結果：
- `POST /user/api/sso/v1/sendSms` → 404 (Spring Boot 404)
- `POST /user/api/sso/v1/sendVerifyCode` → 404
- `POST /user/api/sso/v1/sms` → 404
- `POST /codeLogin` → 405 (POST 被禁，這是 SPA 路由)

JS 顯示的真實路徑（從 SSO JS bundle）：

```
/user/api/sso/v1/todo-list/send/verify    ← 簡訊驗證碼發送
/user/api/sso/v1/todo-list/update/mobile  ← 更新手機
/user/api/sso/v1/todo-list/verify-apply   ← 驗證申請
/user/api/sso/v1/wecom/login              ← 企業微信登入
```

未測試邏輯問題：
- 簡訊驗證碼是否有 rate limiting？（暴力枚舉風險）
- 驗證碼有效期多長？（重放風險）
- 是否綁定 session？（換手機接碼繞過風險）
- 修改手機是否需要舊手機驗證？（賬號接管風險）

修復建議：
- 簡訊發送加 IP/手機號 rate limit（每分鐘 1 次，每小時 5 次）
- 驗證碼有效期 ≤ 5 分鐘
- 敏感操作（修改手機、密碼）需多重認證

#2 XSS / #5 文件上傳 / #6 RCE（未發現）

未發現漏洞的類別。測試結果：

XSS（純 HTTP 測試）

- URL 參數反射（`?q=`、`?redirect=`、`?error=`、`?msg=`、`?return=`）→ 無反射
- 404 頁面 → 無反射
- 無法排除：stored XSS（需認證測試）

文件上傳/包含

- 常見上傳路徑（`/upload`、`/api/upload`、`/file/upload`、`/api/v1/upload`、`/common/upload`、`/avatar`、`/api/avatar`、`/user/avatar`）→ 全部 405 Method Not Allowed
- 注意：405 = 端點存在但 POST 被拒，可能是 GET-only API 路由
- LFI 測試（`?file=../../etc/passwd` 等）→ 無讀取跡象

RCE

- nginx CVE-2017-7529（integer overflow）對 segwayrobotics.com/loomo.com 測試 → 1 byte response（未洩漏記憶體，版本可能已修）
- SSTI（`{{7*7}}`、`${7*7}`、`<%= 7*7 %>`）→ 無模板執行跡象
- 未測試：Apache 2.4.7 已知 CVE 的實際 exploit（需謹慎，避免影響服務）

證據保存位置

路徑	內容
`/root/hexstrike-pentest/PHASE2-FINDINGS.md`	完整發現報告（舊版）
`/root/hexstrike-pentest/connectivity.log`	24 目標連通性記錄
`/root/hexstrike-pentest/js-analysis/`	平台 JS + SSO JS bundles
`/root/hexstrike-pentest/recon/`	5 個 domain 的子域名清單
`/root/hexstrike-pentest/vuln-tests/`	8 類漏洞測試日誌（本次新增）

建議下一步

強烈建議進行（需瀏覽器 session + 用戶授權）：
1. 瀏覽器深度測試 opsvpn NetBird — 嘗試默認登入、註冊流程
2. 瀏覽器查看微信文檔 `e3_ADoAWwaFAMQCNM5Vh55Z3RlyA4ECz`
3. 瀏覽器載入 platform.ninebot.com — 模擬用戶登入，捕獲 saturn-portal 實際 API 認證機制
4. 認證後 IDOR 測試 — 用不同 user ID 訪問 user/account/detail-v2

可選測試（風險較高）：
- Apache 2.4.7 Optionsbleed 完整測試（可能影響服務穩定性）
- nginx CVE-2017-7529 在不同 path 測試
- navimow APK 靜態分析（需要 APK 檔案）

報告生成時間：2026-07-11
測試 IP 來源：43.160.194.36（Tencent Cloud）
測試時長：~2 小時
覆蓋目標：briefing 6 組 domain，共 134 個子域名