**📄 TripPlanner Ltd – Penetration Test Summary Report**

**Client:** TripPlanner Ltd  
**Test Window:** 24–28 July 2025  
**Assessment Type:** Grey Box  
**Conducted by:** SageSecOps

**🔹 Objective**

Assess the security posture of TripPlanner’s public and internal infrastructure with a focus on identifying high-risk vulnerabilities.

**🔹 Scope**

* Web App: tripplanner.io, admin.tripplanner.io, api.tripplanner.io
* Internal: 10.1.10.10, 10.1.10.25

**🔹 Key Findings**

| **Risk Level** | **Vulnerability** | **Impact** |
| --- | --- | --- |
| Critical | Unauthenticated File Upload (CMS) | Remote code execution |
| High | Misconfigured Cron Job (Privilege Escalation) | Root access |
| Medium | Brute Force Login (Customer Portal) | Credential compromise |
| Low | Verbose API Errors | Information leakage |

**🔹 Tools Used**

* Nmap
* Burp Suite Pro
* Hydra
* LinPEAS
* Metasploit
* CherryTree

**🔹 Recommendations**

* Apply strict upload filters and server permissions
* Fix cron job permissions and run as least-privileged user
* Add rate-limiting and CAPTCHA to login endpoints
* Suppress detailed error messages from APIs

**🔹 Final Notes**

* All backdoors removed after validation
* Detailed logs shared securely with client IT
* No customer data accessed or extracted

**Prepared by:**  
WisSecOps  
📅 1 August 2025