HACK THE BOX

Penetration Test Report

Machine: Armageddon

Candidate Name: Aliakbar Babayev

Customer: Hack The Box

Date: January 31, 2026

Version: 1.0

CONFIDENTIAL

Contents

1 Statement of Confidentiality **2**

2 Engagement Contacts **2**

3 Executive Summary **3**
3.1 Approach . . . 3
3.2 Scope . . . 3
3.3 Assessment Overview and Recommendations . . . 3

4 Network Penetration Test Assessment Summary **4**
4.1 Summary of Findings . . . 4

5 Internal Network Compromise Walkthrough **5**
5.1 Detailed Walkthrough . . . 5
5.1.1 1. Reconnaissance & Enumeration . . . 5
5.1.2 2. Initial Access (RCE) . . . 5
5.1.3 3. Lateral Movement . . . 5
5.1.4 4. Privilege Escalation to Root . . . 5

6 Remediation Summary **6**
6.1 Short Term . . . 6
6.2 Medium Term . . . 6
6.3 Long Term . . . 6

7 Technical Findings Details **7**
7.1 Remote Code Execution via Drupalgeddon 2 . . . 7
7.2 Cleartext Credentials in Configuration Files . . . 7
7.3 Privilege Escalation via Insecure Sudo (Snap) . . . 7

8 Appendix A: Host & Service Discovery **8**
8.1 A.1 Host Information . . . 8
8.2 A.2 Service Scan Results . . . 8
8.3 A.3 Compromised Users . . . 8

1 Statement of Confidentiality

The information contained in this document is confidential and proprietary to Hack The Box. This report is intended solely for the use of the client and its authorized representatives. Unauthorized distribution, reproduction, or disclosure of this document, in whole or in part, is strictly prohibited without prior written consent.

2 Engagement Contacts

Role	Name	Contact
Penetration Tester	Aliakbar Babayev	candidate@htb.com
Client Contact	HTB Admin	admin@hackthe-box.com

3 Executive Summary

3.1 Approach

The penetration test was conducted using a black-box approach, simulating an external attacker with no prior knowledge of the internal network or credentials. The assessment followed industry-standard methodologies, including the Penetration Testing Execution Standard (PTES).

3.2 Scope

The scope of this assessment was limited to the single host **Armageddon** with the IP address **10.129.48.89**. The assessment focused on identifying vulnerabilities in the web application and the underlying operating system that could lead to unauthorized access or privilege escalation.

3.3 Assessment Overview and Recommendations

During the penetration test against **Armageddon**, the assessor identified **3** findings that threaten the confidentiality, integrity, and availability of the target's information systems. The findings were categorized by severity level, with **1** finding assigned a **Critical** risk rating, **2** assigned a **High** risk rating, **0** Medium, and **0** Low.

The assessment revealed a critical vulnerability in the web application layer, specifically an outdated Drupal installation vulnerable to remote code execution (Drupalgeddon 2). This allowed for immediate initial access to the internal system. Furthermore, internal enumeration revealed cleartext credentials stored in configuration files and a misconfigured 'sudo' permission for the 'snap' utility, which ultimately allowed for complete system compromise (Root privileges).

Recommendation Highlights:

- Upgrade Drupal to the latest stable version immediately.
- Encrypt configuration files containing database credentials.
- Restrict 'sudo' permissions and remove dangerous binaries like 'snap'from password-less execution lists.

4 Network Penetration Test Assessment Summary

4.1 Summary of Findings

The following table summarizes the vulnerabilities identified during the assessment, ranked by severity.

#	Severity	Finding Name
1	Critical	Remote Code Execution via Drupalgeddon 2
2	High	Cleartext Credentials in Configuration Files
3	High	Privilege Escalation via Insecure Sudo (Snap)

Risk Rating Definitions:

- **Critical (9.0 - 10.0):** Exploitation is straightforward and results in system compromise (e.g., RCE).
- **High (7.0 - 8.9):** Significant risk of compromise; may require some conditions to be met.
- **Medium (4.0 - 6.9):** Vulnerabilities that may leak information or be chained for deeper access.
- **Low (0.1 - 3.9):** Issues that provide information but do not directly lead to compromise.

5 Internal Network Compromise Walkthrough

5.1 Detailed Walkthrough

The following steps outline the exact path taken to compromise the Armageddon host:

5.1.1 1. Reconnaissance & Enumeration

A port scan was conducted against the target IP `10.129.48.89` using Nmap.

```
nmap -A -Pn -p22 ,80 10.129.48.89
```

The scan revealed OpenSSH on port 22 and an Apache web server on port 80. Further web enumeration identified the CMS as **Drupal 7**. Checking the `CHANGELOG.txt` file confirmed the version as **7.56**.

5.1.2 2. Initial Access (RCE)

Research indicated that Drupal 7.56 is vulnerable to **CVE-2018-7600**, known as "Drupalgeddon 2". This vulnerability allows unauthenticated attackers to execute arbitrary code. Using the Metasploit Framework, the assessor successfully exploited this flaw.

```
msfconsole
use exploit/unix/webapp/ drupal_drupalgeddon2
set RHOSTS 10.129.48.89
run
```

This resulted in a reverse shell as the `apache` user.

5.1.3 3. Lateral Movement

During post-exploitation enumeration, the Drupal configuration file was inspected.

```
cat /var/www/html/sites/default/settings.php
```

The file contained cleartext database credentials:

- **User:** drupaluser
- **Password:** CQHEy@9M*m23gBVj

The system had a user named `brucetherealadmin`. The assessor attempted to reuse the database password for this system user via SSH and was successful.

5.1.4 4. Privilege Escalation to Root

Checking the `sudo` privileges for `brucetherealadmin`:

```
sudo -l
User brucetherealadmin may run the following commands on armageddon:
    (root) NOPASSWD: /usr/bin/snap install *
```

The user could install Snap packages as root. The assessor created a malicious Snap package containing a hook to modify `/etc/sudoers`, granting full root access.

6 Remediation Summary

6.1 Short Term

- **Patch Management:** Update Drupal to the latest secure version immediately to close the RCE vector.
- **Credential Hygiene:** Remove cleartext passwords from the `settings.php` file. Ensure unique passwords are used for database and system accounts to prevent lateral movement.

6.2 Medium Term

- **Least Privilege:** Revoke the ability for the `brucetherealadmin` user to run `snap install` with sudo privileges. If specific snaps are needed, restrict the command to those specific filenames rather than using a wildcard.

6.3 Long Term

- **Security Hardening:** Implement a regular vulnerability scanning schedule to detect outdated software like Drupal.
- **Configuration Management:** Use automated tools (e.g., Ansible, Puppet) to enforce secure configuration states and detect drift in sensitive files like `sudoers`.

7 Technical Findings Details

7.1 Remote Code Execution via Drupalgeddon 2

Severity	Critical
CVSS	9.8 (Critical)
Impact	Complete System Compromise

Description:
The target application is running Drupal version 7.56, which is vulnerable to CVE-2018-7600 (Drupalgeddon 2). This vulnerability stems from insufficient input sanitization in the Drupal Form API, allowing an attacker to inject and execute arbitrary code.

Evidence:
The assessor utilized the 'drupalgeddon2' exploit to gain a shell.

```
[*] Meterpreter session 1 opened
uid =48( apache) gid =48( apache) groups =48( apache)
```

Remediation:
Upgrade to the latest version of Drupal 7 or migrate to Drupal 9/10.

7.2 Cleartext Credentials in Configuration Files

Severity	High
CVSS	7.5 (High)
Impact	Credential Theft, Lateral Movement

Description:
Database credentials were found stored in plain text within the `/var/www/html/sites/default/settings.ph` file. These credentials were valid for the system user `brucetherealadmin`.

Remediation:
Store sensitive credentials in environment variables or use a secrets management service.

7.3 Privilege Escalation via Insecure Sudo (Snap)

Severity	High
CVSS	7.8 (High)
Impact	Privilege Escalation to Root

Description:
The `sudoers` configuration allows the user to run `snap install` as root without a password. Snap packages can contain installation hooks that execute as root, allowing for arbitrary command execution.

Remediation:
Remove the entry from `/etc/sudoers` or strictly limit which packages can be installed.

8 Appendix A: Host & Service Discovery

8.1 A.1 Host Information

IP Address: 10.129.48.89
OS: Linux (CentOS)

8.2 A.2 Service Scan Results

Port	Protocol	Service	Version
22	TCP	SSH	OpenSSH 7.4
80	TCP	HTTP	Apache 2.4.6 / PHP 5.4.16

8.3 A.3 Compromised Users

Username	Type	Method
apache	Service Account	Remote Code Execution (CVE-2018-7600)
brucetherealadmin	Local User	Password Reuse (settings.php)
root	Administrator	Sudo Privilege Escalation (Snap)