

Task 15 ○ [Severity 4] XML External Entity - XXE Payload

Did you know.. by [subscribing](#) your machines
deploy quicker and with more resources

Task 16 ○ [Severity 4] XML External Entity - Exploiting

Starting your machine.. please wait!

Task 17 ○ [Severity 5] Broken Access Control

Task 18 ○ [Severity 5] Broken Access Control (IDOR Challenge)

Task 19 ○ [Severity 6] Security Misconfiguration

Security Misconfiguration

▶ Start Machine

Security Misconfigurations are distinct from the other Top 10 vulnerabilities, because they occur when security could have been configured properly but was not.

Security misconfigurations include:

- Poorly configured permissions on cloud services, like S3 buckets
- Having unnecessary features enabled, like services, pages, accounts or privileges
- Default accounts with unchanged passwords
- Error messages that are overly detailed and allow an attacker to find out more about the system
- Not using [HTTP security headers](#), or revealing too much detail in the Server: HTTP header

This vulnerability can often lead to more vulnerabilities, such as default credentials giving you access to sensitive data, XXE or command injection on admin pages.

Title
Pensive Notes

IP Address
Shown in 55s

Expires
59m 55s



Add 1 hour

Terminate

- Not using [HTTP security headers](#), or revealing too much detail in the Server: HTTP header

This vulnerability can often lead to more vulnerabilities, such as default credentials giving you access to sensitive data, XXE or command execution pages.

For more info, I recommend having a look at the [OWASP top 10 entry for Security Misconfiguration](#)

Hooray! Your machine has been hacked in a few minutes to become a part of the AttackBox or OpenVuln

Default Passwords

Specifically, this VM focusses on default passwords. These are a specific example of a security misconfiguration. You could, and should, change any default passwords but people often don't.

It's particularly common in embedded and Internet of Things devices, and much of the time the owners don't change these passwords.

It's easy to imagine the risk of default credentials from an attacker's point of view. Being able to gain access to admin dashboards, services designed for system administrators or manufacturers, or even network infrastructure could be incredibly useful in attacking a business. From data exposure to easy RCE, the effects of default credentials can be severe.

In October 2016, Dyn (a DNS provider) was taken offline by one of the most memorable DDoS attacks of the past 10 years. The flood of traffic came mostly from Internet of Things and networking devices like routers and modems, infected by the Mirai malware.

How did the malware take over the systems? Default passwords. The malware had a list of 63 username/password pairs, and attempted to log in to exposed telnet services.

The DDoS attack was notable because it took many large websites and services offline. Amazon, Twitter, Netflix, GitHub, Xbox Live, PlayStation Network, and many more services went offline for several hours in 3 waves of DDoS attacks on Dyn.

Practical example

- github.com/gorilla/mux
- github.com/matttn/go-sqlite3

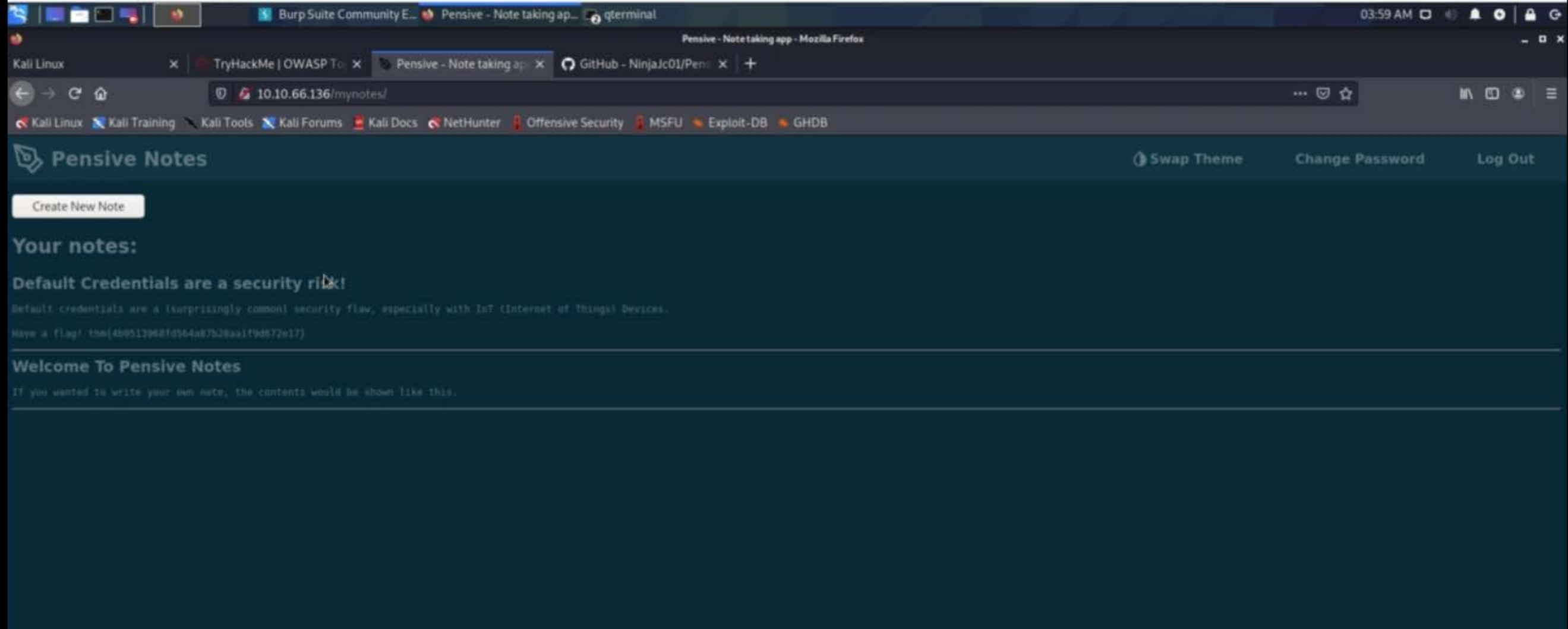
Installation

1. Install golang (1.14+)
2. Clone the repository
3. `go get github.com/matttn/go-sqlite3`
4. `go get github.com/gorilla/mux`
5. `go build -o server main.go`
6. `./server` If you'd like the server to be able to bind to ports under 1000, I recommend using Linux capabilities rather than running as root.

Using PensiveNotes

After downloading and compiling PensiveNotes, log in using the default credentials `pensive:PensiveNotes`

Make sure you change this password immediately!



Kali Linux

TryHackMe | OWASP Top 10

Pensive - Note taking app

GitHub - NinjaJc01/Pensive

← → ↻ 🏠

🔒 10.10.66.136/mynotes/

🔒 Kali Linux

🔒 Kali Training

🔒 Kali Tools

🔒 Kali Forums

🔒 Kali Docs


🔒 NetHunter

🔒 Offensive Security

🔒 MSFU

🔒 Exploit-DB

🔒 GHDB

 Pensive Notes

Create New Note

Your notes:

Default Credentials are a security risk!

Default credentials are a (surprisingly common) security flaw, especially with IoT (Internet of Things) Devices.

Have a flag! thm{4b9513968fd564a87b28aa1f9d672e17}

Welcome To Pensive Notes

If you wanted to write your own note, the contents would be shown like this.