Báo Cáo Lỗ Hổng Remote Code Execution (RCE)

Author: Vi Mạnh Tường – contact@manhtuong.net

I. Tóm Tắt

Trong quá trinh sử dụng cpanel chúng tôi phát hiện lỗ hổng cho phép chúng tôi leo quyền lên thực thi lệnh RCE trên hệ thống tiến tới chếm quyền cao nhất (root) của vps người dùng.

II. Chi Tiết Lỗ Hổng

Khi tiến hành phân tích code của cpanel chúng tôi nhận thấy dịch vụ có một file process phụ trách hết các câu lệnh thực thi như tạo thư mục cho domain xóa domain…… tuy nhiên file này được mã hóa bằng ioncube nên buộc tôi phải giải mã chúng để biết cách chúng hoạt động một công việc mất rất nhiều thời gian của tôi.

```
if (isset($_POST["postType"]) && $_POST["postType"] == 1) {
    $cms = isset($_POST["cms"]) && $_POST["cms"] ? $_POST["cms"] : "";
    $domainname = isset($_POST["domainname"]) && $_POST["domainname"] ? $_POST["domainname"] : "";
    $email = isset($_POST["email"]) && $_POST["email"] ? $_POST["email"] : "";
    $dbname = isset($_POST["dbname"]) && $_POST["dbname"] ? $_POST["dbname"] : "";
    $dbusername = isset($_POST["dbusername"]) && $_POST["dbusername"] ? $_POST["dbusername"] : "";
    $dbpassword = isset($_POST["dbpassword"]) && $_POST["dbpassword"] ? $_POST["dbpassword"] : "";
    $exec_str = "sudo kusanagi provision --" . $cms . " --wplang en_US --fqdn " . $domainname . " --email " . $email . " --dbname " . $dbname . " --dbuser " . $dbusername . " --dbpass " . $dbpassword . " " . $domainname;
    $output = shell_exec($exec_str);
    echo $output;
    exit;
}
```

Figure 1: Code Decode

Dựa trên kết quả decode được chúng tôi nhận thấy cách gọi shell exec các hàm nhập không đảm bảo an toàn

Cụ thể các dữ liệu nhập vào bên trong exec để chờ thực thi đều không được kiểm soát người dùng nhập bất cứ thông tin nào đều trở thành nội dung để shell_exec thực thi, lợi dụng điều này chúng tôi dùng dấu & để phá vỡ cấu trúc lệnh và từ đó thực thi được câu lệnh bất kỳ mà chúng tôi muốn.

Nguyên nhân chúng tôi phải dùng ký tự “&” là vì:

Khi tôi muốn thực thi được một câu lệnh nào thì phải thoát ra khỏi câu lệnh trước mà đảm bảo nó không bị lỗi câu lệnh trước đó để câu lệnh shell phía sau chúng tôi cần nó được thực thi, tuy nhiên đối với case này chúng tôi không thể đáp ứng được điều kiện đó nên chúng tôi dùng & để ép lệnh phía trước nó đang lỗi trở thành một đoạn mã chạy background và sau đó hệ thống sẽ thực thi câu lệnh của chúng tôi mong muốn theo đúng trình tự shell script. Sau khi tất cả các lệnh hoàn thành thì hệ thống sẽ trả về kết quả của shell đã chạy background

Kiểm tra xem mình là user nào có phải root không

Figure 2: Kusanagi User

Do user đang chạy web không phải root lên phải dùng sudo để lên quyền root tuy nhiên tôi cần chắc chắn tôi có thể dùng được lệnh sudo đã, vậy nên tôi cần đọc file sudoers, và vô cùng bất ngờ khi user Kusanagi có thể dùng lệnh sudo mà không bị yêu cầu mật khẩu đây là điều tuyệt vời cho phép chúng tôi tấn công leo lên quyền root của vps thông qua lệnh sudo.

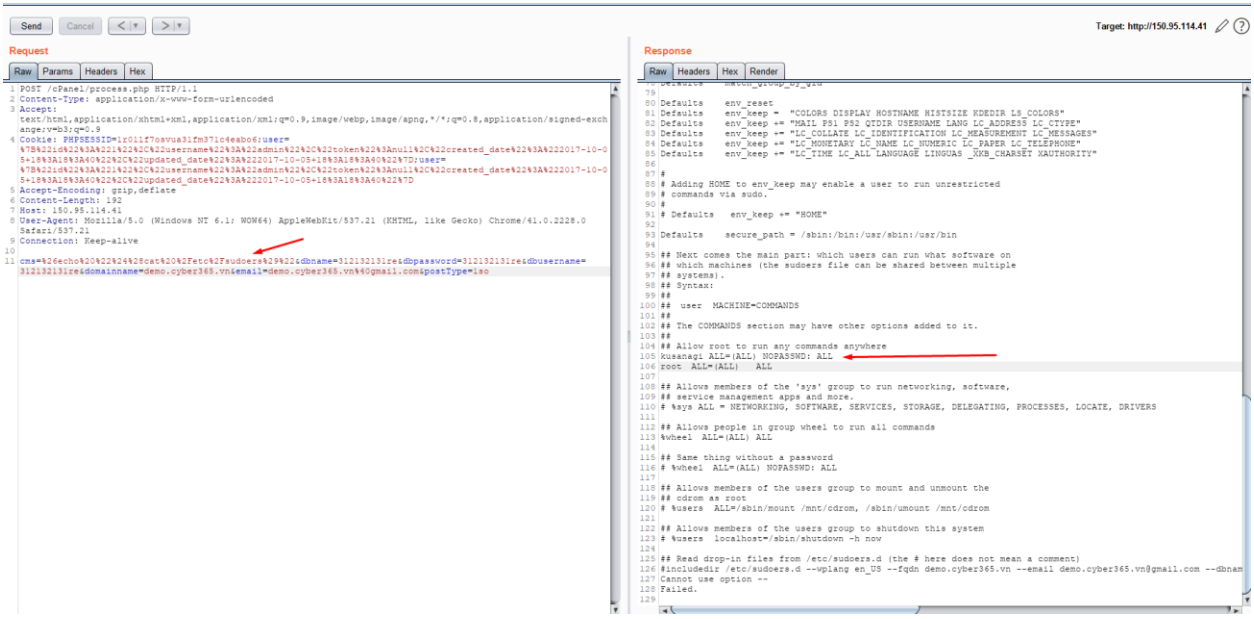

Figure 3: Kusanagi Sudo Without Password

Từ vấn đề trên tôi bắt đầu thiết kế cho mình một payload để leo thang chiếm quyền hệ thống.

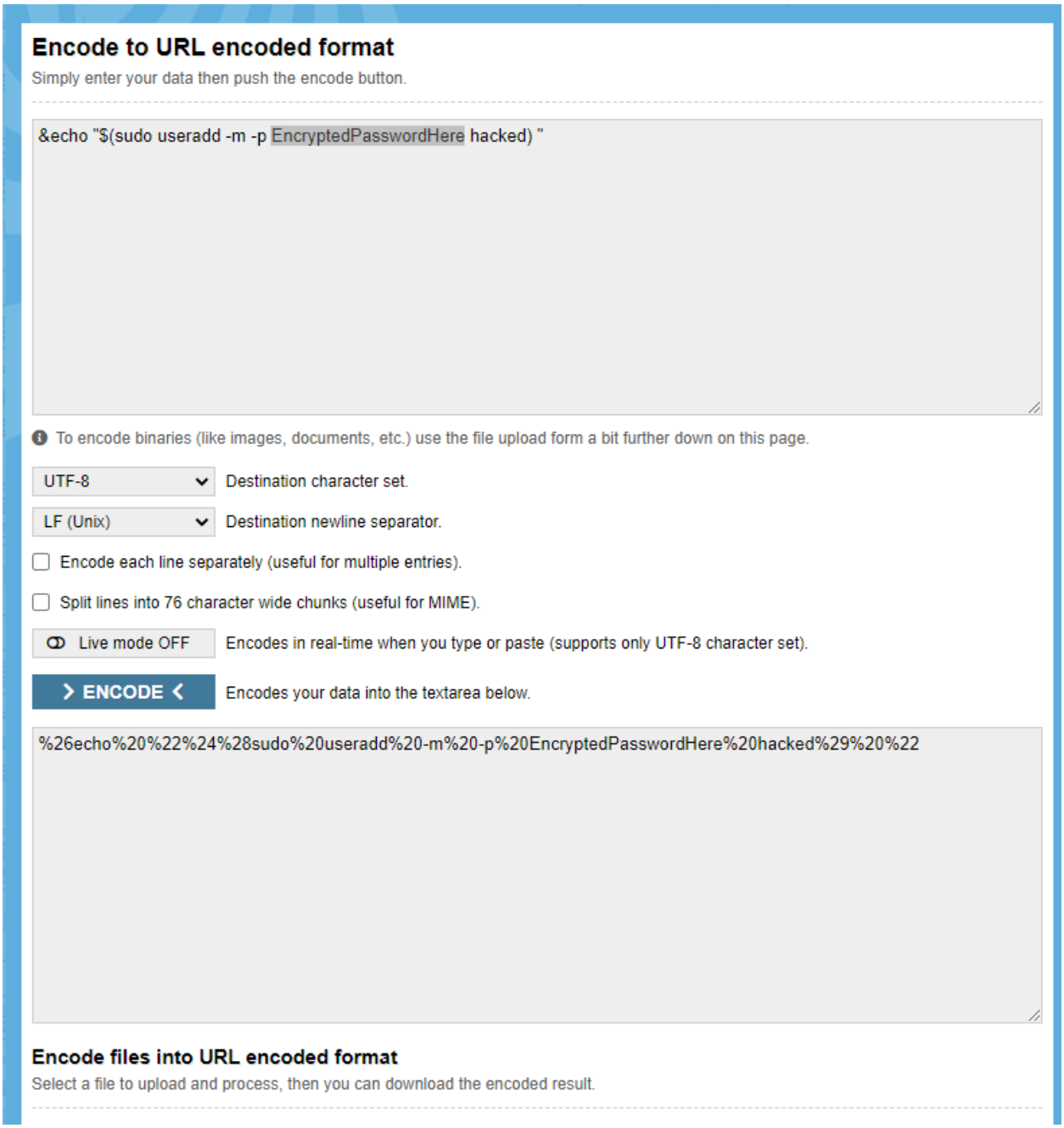

Figure 4: Khởi Tạo payload tạo user

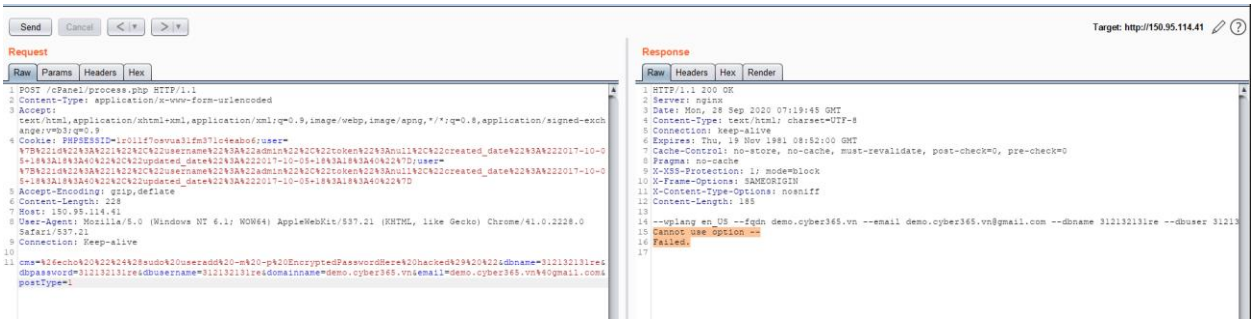

Figure 5: Gửi payload tạo tài khoản

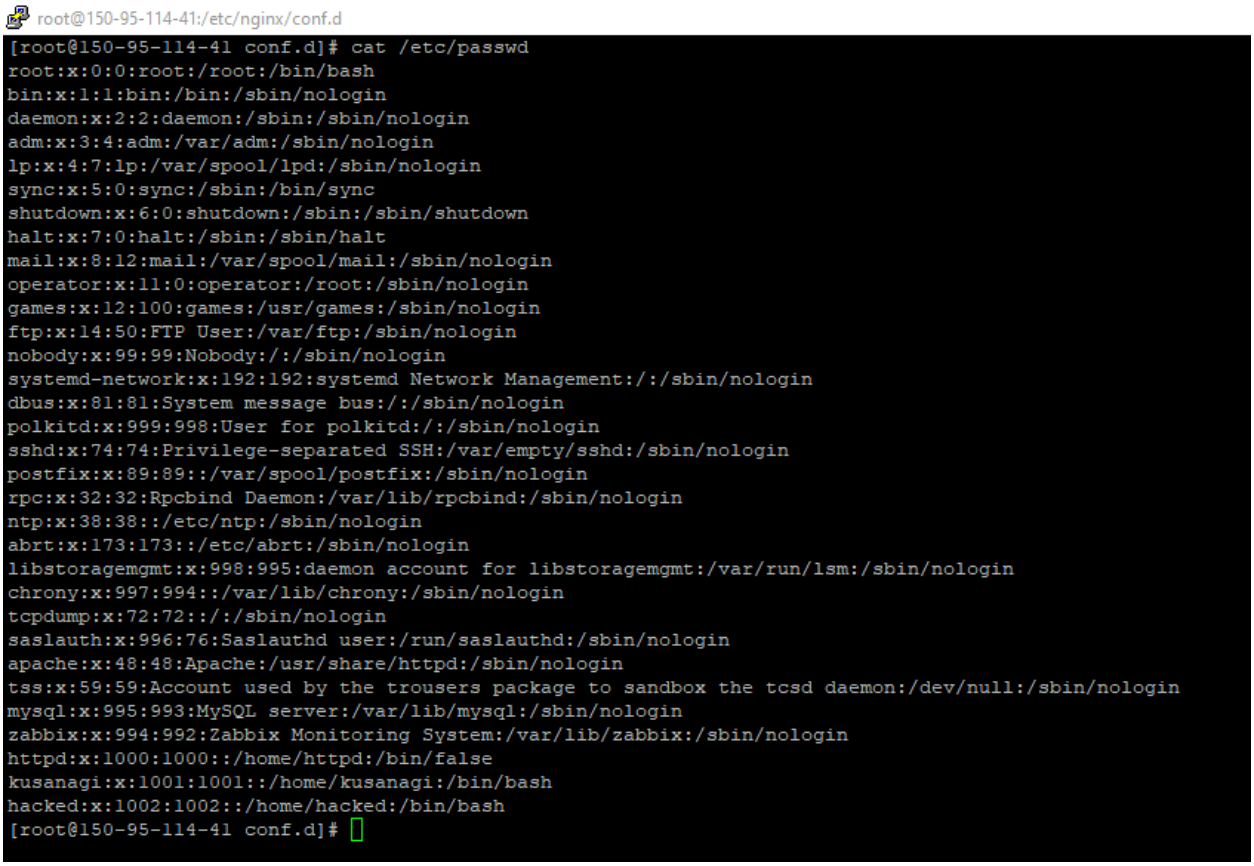

Figure 6: User Được Tạo Thành Công

```
[root@150-95-114-41 ~]# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
abrt:x:173:173::/etc/abrt:/sbin/nologin
libstoragemgmt:x:998:995:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
chrony:x:997:994::/var/lib/chrony:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
saslauth:x:996:76:Saslauthd user:/run/saslauthd:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
mysql:x:995:993:MySQL server:/var/lib/mysql:/sbin/nologin
zabbix:x:994:992:Zabbix Monitoring System:/var/lib/zabbix:/sbin/nologin
httpd:x:1000:1000::/home/httpd:/bin/false
kusanagi:x:1001:1001::/home/kusanagi:/bin/bash
hacked:x:1002:1002::/home/hacked:/bin/bash
username:x:1003:1003::/home/username:/bin/bash
```

Figure 7: Check Info User Trước Khi Thay Đổi Mật Khẩu

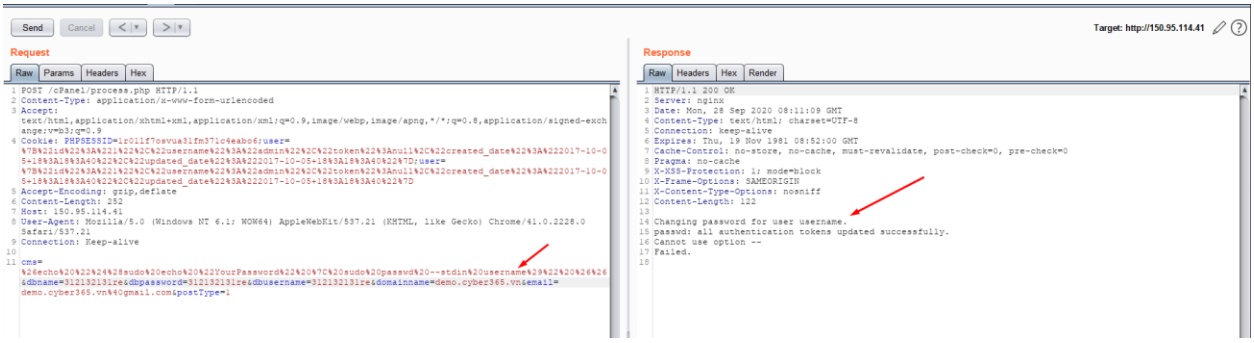

Figure 8: Thay đổi mật khẩu thành công của user bất kỳ

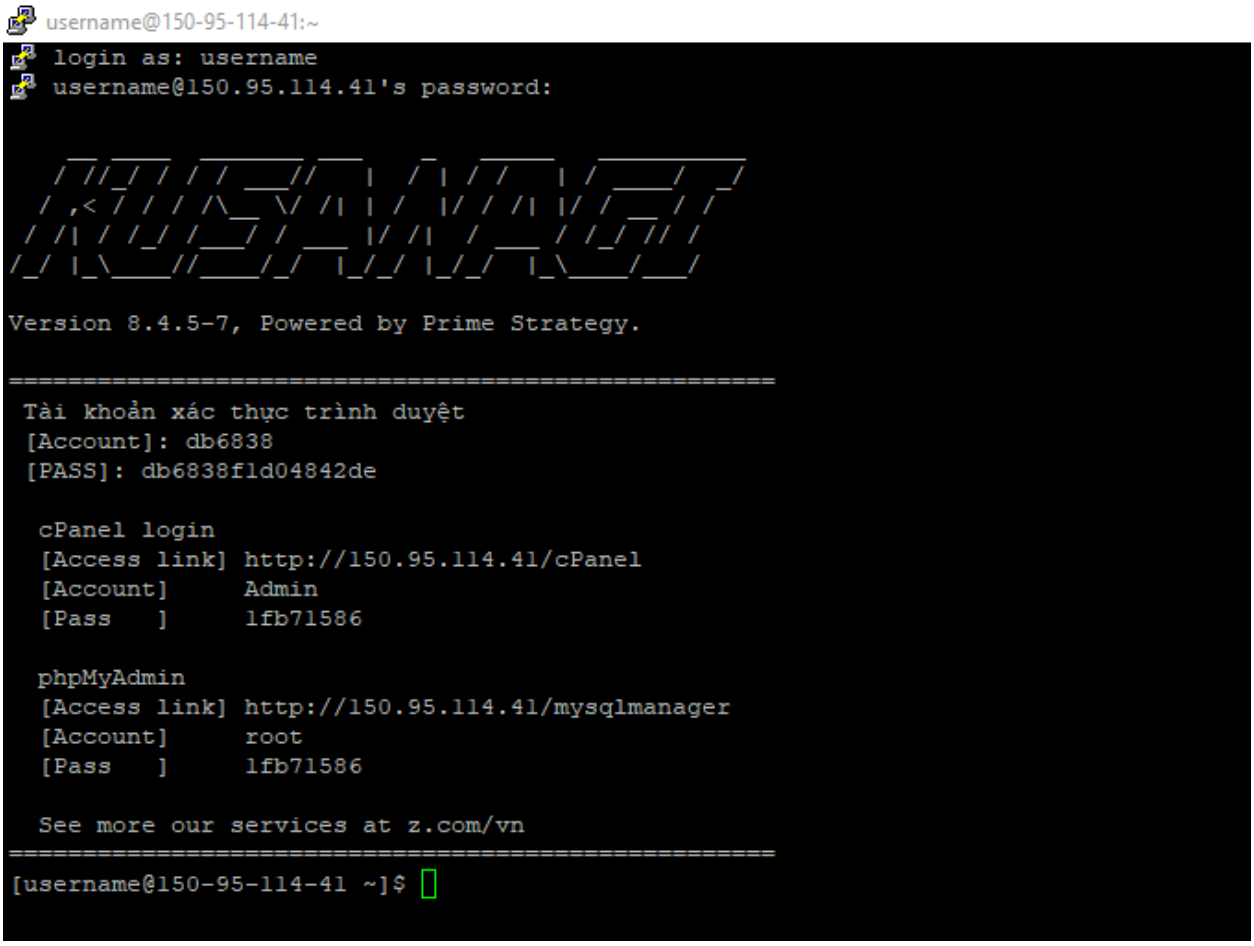

Figure 9: Đăng Nhập Thành Công Thông Qua Thông Tin Bi Thay Đổi

III. Khuyến Cáo

Cách sửa chữa lỗi này rất đơn giản thông qua việc kiểm tra các ký tự nhập vào của người dùng không cho phép xuất hiện các ký tự đặc biệt

```
if(preg_match("/([%\$#\*\&]+)/", $cms))
{
  echo 'Invalid cms name;
}
else
{
  echo $cms;
}
```