Over The Wire -- Natas

by Martin Ren

Hint

Level 0 - Level 1

Right click and read page source, then you can easily find password.

Level 1 - Level 2

There are several ways to solve. One is try to use different browser like firefox which you can still use right click. Another way is add “view-source” before url.

Level 2 - Level 3

When you read page source, you can find there is a png file locate at **files/**. Go to that path by changing url and check files.

Level 3 - Level 4

Web site owners use the /robots.txt file to give instructions about their site to web robots; this is called *The Robots Exclusion Protocol*. And there exist robots.txt in this level.

Level 4 - Level 5

When we log into this page, we are users from level 4. But it require users from level 5. So we can change header request.

Level 5 - Level 6

Just view and change cookie. Extensions in some browsers can help you change cookie.

Level 6 - Level 7

When you view page source they provide, you can find there is a path called **includes/secrets.inc**. Go there and check secrets.

Level 7 - Level 8

Click **Home** or **About**. Try to change path after **?page=**.

Level 8 - Level 9

Read source code and know how they decode. Do reverse steps to decode and get secret.

Level 9 - Level 11

These two levels are similar. Use egrep they provide to get password from **/etc/natas_webpass**. Use **#** to comment out rest of code in origin code.

Level 11 - Level 12

If string A xor string B can get string C, then A xor C is B and B xor C is A. Try to decode cookie without change anything when you log in and encode default data. Then calculate xor of two data to get key. Modify data and set new cookie.

Answer

Level 0 - Level 1

Read page source
gtVrDuiDfck831PqWsLEZy5gyDz1clto

Level 1 - Level 2

Add “view-source:” before url
ZluruAthQk7Q2MqmDeTiUij2ZvWy2mBi

Level 2 - Level 3

Read from page source get path files/pixel.png
Go to files/ and get password from users.txt
sJIJNW6ucpu6HPZ1ZAchaDtwd7oGrD14

Level 3 - Level 4

Go to robots.txt
Get link and go to get password
Z9tkRkWmpt9Qr7XrR5jWRkgOU901swEZ

Level 4 - Level 5

Change header request
iX6IOfmpN7AYOQGPwtn3fXpbaJVJcHfq

Level 5 - Level 6

Change cookie
aGoY4q2Dc6MgDq4oL4YtoKtyAg9PeHa1

Level 6 - Level 7

Click view pagesource and get includes/secrets.inc
Go to this path and get secret
Enter secret and get password
7z3hEENjQtflzgnT29q7wAvMNfZdh0i9

Level 7 - Level 8

Read hint from page source
Change url index.php?page=/etc/natas_webpass/natas8
DBfUBfqQG69KvJvJ1iAbMoIpwSNQ9bWe

Level 8 - Level 9

Get encoded secret from page source
hex to acsii

strrev(ascii)
decode base64
Decoded secret and get password
W0mMhUcRRnG8dcghE4qvk3JA9lGt8nDl

Level 9 - Level 10

; cat /etc/natas_webpass/natas10 #
nOpp1igQAkUzaI1GUUjzn1bFVj7xCNzu

Level 10 - Level 11

.* /etc/natas_webpass/natas11 #
U82q5TCMMQ9xuFoI3dYX61s7OZD9JKoK

Level 11 - Level 12

1. Get cookie from website(Use the default color #ffffff)
   ClVLIh4ASCsCBE8lAxMacFMZV2hdVVotEhhUJQNVAmhSEV4sFxFeaAw=
2. Decode cookie from base64 to hex(We can skip this step)
   0A554B221E00482B02044F2503131A70531957685D555A2D12185425035502685211
5E2C17115E680C
3. Json encode the default data from page source
   {"showpassword":"no","bgcolor":"#ffffff"}
4. Calculate xor of decoded cookie and encoded data to hex(You can get the key)
   7177384a7177384a7177384a7177384a7177384a7177384a7177384a7177384a717738
4a7177384a71
   The key is 7177384a in hex and qw8J in ascii
5. Edit a new data which show password is true
   {"showpassword":"yes","bgcolor":"#ffffff"}
6. Transfer data to hex
   7b2273686f7770617373776f7264223a22796573222c226267636f6c6f72223a22236666
66666666227d
7. Modify key so that it get same length with transferred data
   7177384a7177384a7177384a7177384a7177384a7177384a7177384a7177384a717738
4a7177384a7177
8. Xor modified data and key, then encode by base64
   ClVLIh4ASCsCBE8lAxMacFMOXTlTWxooFhRXJh4FGnBTVF4sFxFeLFMK
9. Set cookie in http://natas11.natas.labs.overthewire.org/ and refresh
   EDXp0pS26wLKHZy1rDBPUZk0RKfLGIR3