Natas CTF Levels 0-8

By: Ahmed Shaheen

Natas is a "wargame" CTF on OverTheWire that gives an introduction into web security. Each level provides a webpage that contains a password to login to the next level. The user must devise a way to obtain the password using any tools at their disposal. Each level is different and goes over a variety of concepts such as command injection, SQL injection, or just assessing vulnerabilities in source code. You generally want to analyze each page's source code so that you can understand what the code is doing and come up with different ways of exploiting it. If you're ever stumped on a challenge, always feel free to search something up that you don't understand and take your time with these challenges.

Website:https://overthewire.org/wargames/natas/natas0.html

Level 0

Go to: http://natas0.natas.labs.overthewire.org/. Login credentials for the level 0:

```
username: natas0
password: natas0
```

1. Inspect element the webpage using `Ctrl+Shift+i`
2. Click on the div tag `"content"` and that should reveal the password for Natas level 1: `gtVrDuiDfck831PqWsLEZy5gyDz1clto`

Level 1

Go to: http://natas1.natas.labs.overthewire.org/ Once you login with the newly found password, the webpage displays: **You can find the password for the next level on this page, but rightclicking has been blocked!**

1. Repeat the steps from level 0 and obtain the password for level 2: `ZluruAthQk7Q2MqmDeTiUij2ZvWy2mBi`

Level 2

Go to: http://natas2.natas.labs.overthewire.org/ Once you login with the newly found password, the webpage displays: **There is nothing on this page** 1. Inspect element and navigate to the content tag again. 2. As you can see, it contains an img tag `"files/pixel.png"` . Click on it. 3. This takes you to a webpage that displays nothing but a black page with the resulting link: http://natas2.natas.labs.overthewire.org/files/pixel.png 4. `files` looks like an interesting location to examine. To navigate to the previous directory, simply delete `pixel.png` from the link. 5. This takes you to webpage that contains an index of /files. Click on `users.txt` which reveals the password for natas3: `sJIJNW6ucpu6HPZ1ZAchaDtwd7oGrD14`

Level 3

Go to: http://natas3.natas.labs.overthewire.org/ Once you login with the newly found password, the webpage displays: **There is nothing on this page**

1. Inspect the webpage and navigate to the content tag. It contains this comment: `<!-- No more information leaks!! Not even Google will find it this time... -->` Think about search engines here.
2. Use robots.txt, an exclusion standard that stipulates on a search engine what URLs are accessible to webcrawlers on a website: http://natas3.natas.labs.overthewire.org/robots.txt
3. This redirects you to a webpage with the following information:

```
User-agent: *
Disallow: /s3cr3t/
```

4. `/s3cr3t/` looks like a directory you can access. Navigate to it: http://natas3.natas.labs.overthewire.org/**s3cr3t/**
5. Click on `users.txt` and obtain natas4's password: `Z9tkRkWmpt9Qr7XrR5jWRkgOU901swEZ`

Level 4

Go to: http://natas4.natas.labs.overthewire.org/ Once you login with the newly found password, the webpage displays: **Access disallowed. You are visiting from "" while authorized users should come only from "http://natas5.natas.labs.overthewire.org/"** The webpage is keeping track of the URL of origin you navigated from, and we must devise a way to change that location of origin.

1. Boot up Burp Suite, an application security testing software.
2. In the **Intercept Window**, modify the **Referrer** parameter to: http://natas5.natas.labs.overthewire.org/index.php
3. Click **Forward** on Burp. natas5's password: `iX6IOfmpN7AYOQGPwtn3fXpbaJVJcHfq`

Level 5

Go to: http://natas5.natas.labs.overthewire.org/ Once you login with the newly found password, the webpage displays: **Access disallowed. You are not logged in** 1. Intercept the Webpage again using Burp Suite.

2. In the intercept window, modify the **Cookie** param to `loggedin=1`

3. Click **Forward** on Burp. natas6's password: `aGoY4q2Dc6MgDq4oL4YtoKtyAg9PeHa1`

Level 6

Go to: http://natas6.natas.labs.overthewire.org/ Once you login with the newly found password, the webpage displays an input entry that prompts to input the "secret" and a button to view the source code. 1. View the source code and examine it carefully:

```
<?

include "includes/secret.inc";

if(array_key_exists("submit", $_POST)) {
    if($secret == $_POST['secret']) {
        print "Access granted. The password for natas7 is <censored>";
}   else {
        print "Wrong secret";
    }
}
?>
```

The code essentially compares any input entered to the contents contained in the file `includes/secret.inc`. We can possibly find more clues examining the file. 2. Access the file by searching up the following: **http://natas6.natas.labs.overthewire.org/includes/secret.inc** 3. This redirects us toa page displaying the secret to put into the input entry:

```
<?
$secret = "FOEIUWGHFEEUHOFUOIU";
?>
```

4. Input the secret in the input entry and natas7's password will be granted: `7z3hEENjQtflzgnT29q7wAvMNfZdh0i9`

Level 7

Go to: http://natas7.natas.labs.overthewire.org/ Once you login with the newly found password, the webpage displays two buttons for *Home* and *About* pages.

1. Click on the Home page
2. Inspect the webpage and view the content tag: `<!-- hint: password for webuser natas8 is in /etc/natas_webpass/natas8 -->` The hint refers to a pathway to a file that contains natas8's password. Also looking at the current URL, the segment `/index.php?page=home` indicates that files get passed into `index.php`.
3. Set the URL to pass the hint's reference file pathway to be passed through index.php: http://natas7.natas.labs.overthewire.org/index.php?page=/etc/natas_webpass/natas8

natas8's password is: `DBfUBfqQG69KvJvJ1iAbMoIpwSNQ9bWe`

Level 8

Go to: http://natas8.natas.labs.overthewire.org/ Once you login with the newly found password, another webpage displays an input entry that prompts for a "secret".

1. Examine the source code:

```
<?

$encodedSecret = "3d3d516343746d4d6d6c315669563362";

function encodeSecret($secret) {
    return bin2hex(strrev(base64_encode($secret)));
}

if(array_key_exists("submit", $_POST)) {
    if(encodeSecret($_POST['secret']) == $encodedSecret) {
        print "Access granted. The password for natas9 is <censored>";
}   else {
    print "Wrong secret";
    }
}
?>
```

The encoded secret is the resulting string from this webpage's php algorithm. The string is first encoded in base64 with the `base64_encrypt()`. It is then reverse using `strrev`. It's then finally converted from binary to hex using `bin2hex`.

2. You basically have to reverse the entire process to obtain the original string being the secret. Create a php algorithm to do so:

```
<?php

function decrypt($string){
    return base64_decode(strrev(hex2bin($string)));
}
print decodeSecret("3d3d516343746d4d6d6c315669563362");
print "\n";
?>
```

4. Run the program, you should output the following secret: `oubWYf2kBq`
5. Input the secret into the input entry and you should obtain natas9's password: `W0mMhUcRRnG8dcghE4qvk3JA9lGt8nDl`