Natas – Stage by stage explanation

Level 0 -> 1

After initially logging in to natas 0, by going to address `http://natas0.natas.labs.overthewire.org` and entering natas0 for both fields, we are greeted by a page which says "You can find the password for the next level on this page". A quick right click -> inspect element reveals the password as an HTML comment.

The password for natas 1 is `gtVrDuiDfck831PqWsLEZy5gyDz1clto`

Level 1 -> 2

Again, we are told that the password is somewhere on the page, but right clicking has been blocked this time. No bother; we can simply hit f12 to pull up the developer pane. The password is stored as an HTML comment again.

The password for natas 2 is `ZluruAthQk7Q2MqmDeTiUij2ZvWy2mBi`

Level 2 -> 3

Here, we are told that there is nothing on this page. A quick inspect element is, at first, promising - it reveals a .png file. However, this file seems to just be a single white pixel, and is of no use. We can see that it's stored in the /files folder - navigating to this (by adding /files/ to the end of the url) we find a file called users.txt. This contains the password for natas3.

The password for natas 3 is `sJIJNW6ucpu6HPZ1ZAchaDtwd7oGrD14`

Level 3 -> 4

As before, we are told that there is nothing on this page. A quick inspect element reveals to us an HTML comment, `<!-- No more information leaks!! Not even Google will find it this time... -->`. This suggests that this might have something to do with the robots.txt file; these exist in websites to tell a search engine to ignore certain pages. Sure enough, navigating to this file, we find out that natas3 wants google to ignore the file `/s3cr3t/`. Navigating here (again, via URL) we are greeted once more with the users.txt file.

The password for natas4 is `Z9tkRkWmpt9Qr7XrR5jWRkgOU901swEZ`

Level 4 -> 5

Arriving on the next page, we are greeted with `Access disallowed. You are visiting from "" while authorized users should come only from "http://natas5.natas.labs.overthewire.org/"`

Somehow, we need to convince the webpage that we came from natas5. This can be done with the funky program BurpSuite – this comes installed with kali linux, and otherwise can be downloaded pretty easily. Once installed, it needs to be configured with your browser - this can be done pretty easily; you just need to add it as a proxy. Once this is done, navigate to the proxy tab on burp, turn intercept on and then refresh the page. The details of the HTTP request we just sent should appear. The `Referer` attribute should be set to natas4 - if we simply change this to natas5 and then forward the request then we all set:). Doing so gives us the password.

The password for natas 5 is `iX6IOfmpN7AYOQGPwtn3fXpbaJVJcHfq`

Level 5 -> 6

On arrival, we are told that access wasn't allowed and we're not allowed in. Checking our cookies (this can be done with either a browser extension or with Burp Suite), we find a conspicuously named 'loggedin'. This is currently set to 0. Changing it to 1 and refreshing the page, the text changes to say we are now logged in. This also gives us the password.

The password for natas 6 is `aGoY4q2Dc6MgDq4oL4YtoKtyAg9PeHa1`

Level 6 -> 7