

Overthewire Natas Solutions (1-4)

Oggi parlerò di Natas, che può essere trovato per maggiori informazioni su OverTheWire. Natas insegna le basi della sicurezza web lato server.

Natas Level 0

Effettuiamo il login a Natas0 andando su <http://natas0.natas.labs.overthewire.org> e utilizzando il nome utente: natas0 e la password: natas0.

Natas Level 0

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

You can find the password for the next level on this page.

Una volta effettuato l'accesso, il suggerimento appare al centro dello schermo. Otteniamo la password per natas1 dopo aver visualizzato il sorgente della pagina con il tasto Ctrl+U.

```
<html>
<head>
<!-- This stuff in the header has nothing to do with the level -->
<link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
<script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
<script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
<script src="http://natas.labs.overthewire.org/js/wechall-data.js"></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script>
<script>var wechallinfo = { "level": "natas0", "pass": "natas0" };</script></head>
<body>
<h1>natas0</h1>
<div id="content">
You can find the password for the next level on this page.

<!--The password for natas1 is 0nzCigAq7t2iALyvU9xcHlYN4MlkIwlq -->
</div>
</body>
</html>
```

Natas Level 1

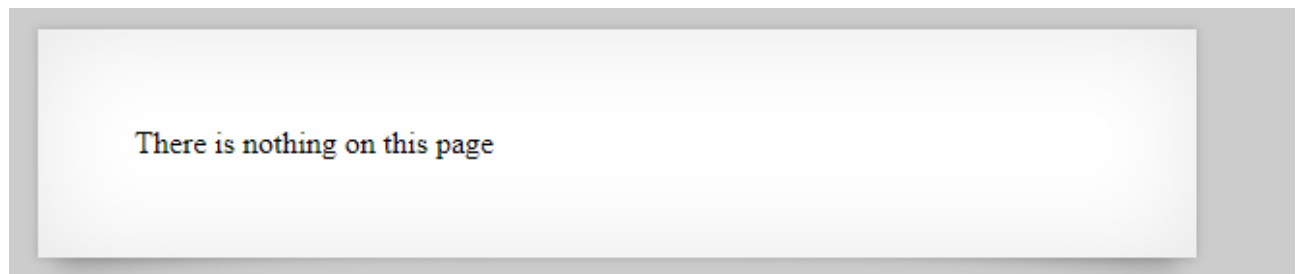
You can find the password for the next level on this page, but rightclicking has been blocked!

Non possiamo usare il tasto destro del mouse per visualizzare l'origine della pagina, ma possiamo usare <CTRL>+<U>. In alternativa, puoi anche ottenere la password premendo F12 e andando alla console, visualizzando il codice HTML.

```
<html>
<head>
<!-- This stuff in the header has nothing to do with the level -->
<link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
<script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
<script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
<script src="http://natas.labs.overthewire.org/js/wechall-data.js"></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script>
<script>var wechallinfo = { "level": "natas1", "pass": "0nzCigAq7t2iALyvU9xcHlYn4MlkIwlq" };</script></head>
<body oncontextmenu="javascript:alert('right clicking has been blocked!');return false;">
<h1>natas1</h1>
<div id="content">
You can find the password for the
next level on this page, but rightclicking has been blocked!

<!--The password for natas2 is TguMNXko1DSaitujBLuZJnDUlCcUAPLI -->
</div>
</body>
</html>
```

Natas Level 2



Controlliamo prima l'origine della Pagina.



Sembra che non ci sia nulla nei file/pixel.png. Navigando su /files/ , possiamo vedere users.txt che contiene la password per il livello successivo.

```
# username:password
alice:BYNdCesZqW
bob:jw2ueICLvT
charlie:G5vCxkVV3m
natas3:3gqisGdR0pjm6tpkDKdIW02hSvchLeYH
eve:zo4mJWynJ2
mallory:9urtcpzBmH
```

Natas Level 3

There is nothing on this page

Visualizziamo l'origine della pagina

```

1 <html>
2 <head>
3 <!-- This stuff in the header has nothing to do with the level -->
4 <link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
5 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
6 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
7 <script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
8 <script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
9 <script src="http://natas.labs.overthewire.org/js/wechall-data.js"></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script>
10 <script>var wechallinfo = { "level": "natas3", "pass": "sJIJNM6ucpu6HPZ1ZAchaDtwD7oGrD14" };</script></head>
11 <body>
12 <h1>natas3</h1>
13 <div id="content">
14 There is nothing on this page
15 <!-- No more information leaks!! Not even Google will find it this time... -->
16 </div>
17 </body></html>
18

```



Nemmeno Google lo troverà questa volta. Andiamo al file robots.txt e vediamo che /s3cr3t/, che è escluso da robots.txt.

← → ↻ 🏠 Non sicuro natas3.natas.labs.overthewire.org/robots.txt

User-agent: *
Disallow: /s3cr3t/

← → ↻ 🏠 Non sicuro natas3.natas.labs.overthewire.org/s3cr3t/

Index of /s3cr3t

Name	Last modified	Size	Description
 Parent Directory		-	
 users.txt	2024-07-17 15:52	40	

Apache/2.4.58 (Ubuntu) Server at natas3.natas.labs.overthewire.org Port 80

natas4:QryZXc2e0zahULdHrtHxzyYkj59kUxLQ

Natas Level 4

Access disallowed. You are visiting from "" while authorized users should come only from "http://natas5.natas.labs.overthewire.org/"

[Refresh page](#)

L'app Web indica che le utenti autorizzate devono provenire da http://natas5.natas.labs.overthewire.org/

