

OTW web-security: Natas

1

Стартовая информация

Natas teaches the basics of serverside web-security.

Each level of natas consists of its own website located at `http://natasX.natas.labs.overthewire.org`, where X is the level number. There is no SSH login. To access a level, enter the username for that level (e.g. natas0 for level 0) and its password.

Each level has access to the password of the next level. Your job is to somehow obtain that next password and level up. All passwords are also stored in `/etc/natas_webpass/`. E.g. the password for natas5 is stored in the file `/etc/natas_webpass/natas5` and only readable by natas4 and natas5.

Natas 2

2

NATAS2

There is nothing on this page



На предыдущих уровнях можно было найти пароль, не покидая страницу, но здесь нам говорят, что на странице ничего нет

```
<html>
  <head> ... </head>
  <body>
    <h1>natas2</h1>
    <div id="content">
      ::before
      There is nothing on this page
      
      ::after
    </div>
```



Но что-то все же есть!

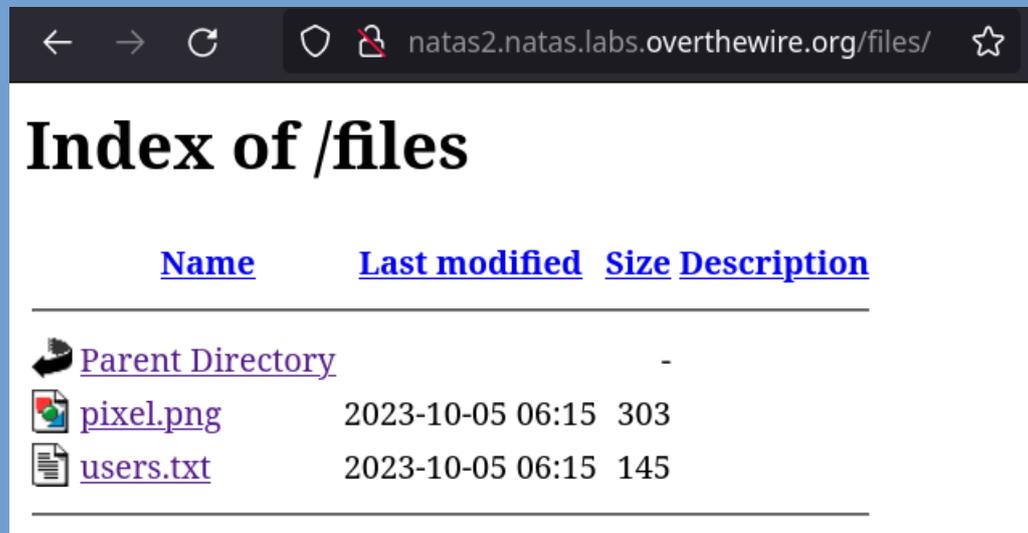
Natas 2

3

Давайте перейдем по ссылке

Отлично, красивый пиксель!

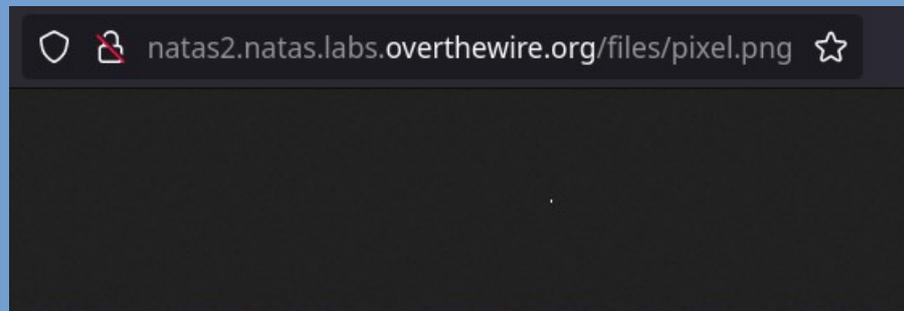
Но, возможно, мы сможем попасть в /files



← → ↻   natas2.natas.labs.overthewire.org/files/ ☆

Index of /files

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 pixel.png	2023-10-05 06:15	303	
 users.txt	2023-10-05 06:15	145	



Неосторожный админ не закрыл доступ к директориям, и мы нашли наш пароль!

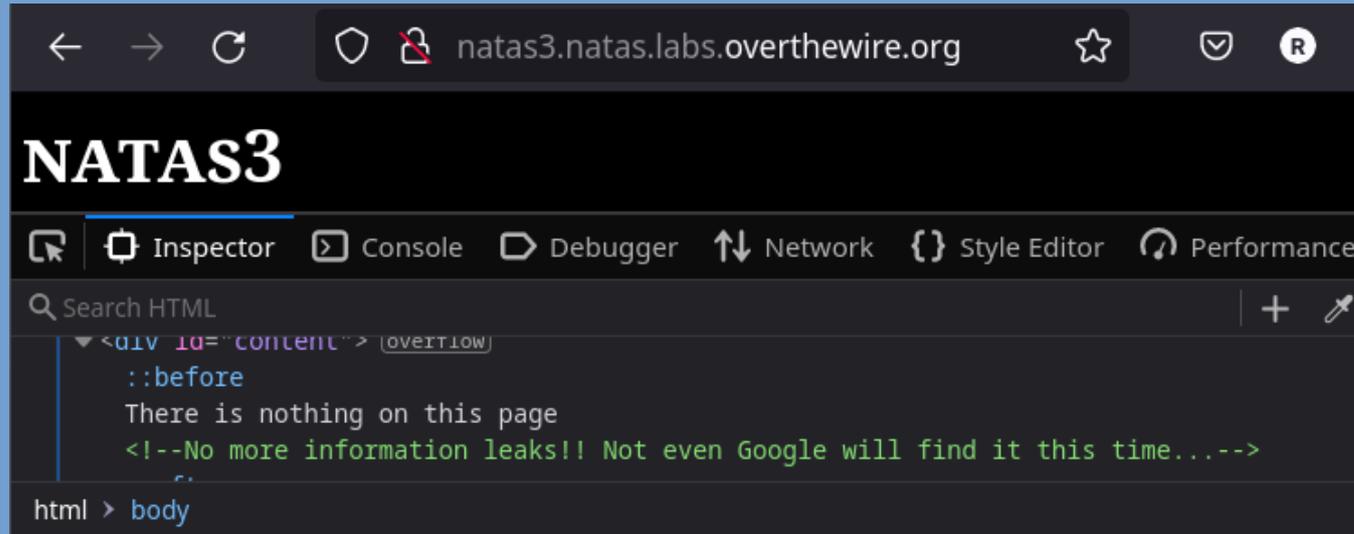
Это атака **Path Traversal**[1]

Natas 3

4

Let's go to the next lvl!

На странице все еще ничего нет, а еще нам говорят, что утечек больше нет, и даже гугл не найдет их, что же это значит?...



```
← → ↻ 🛡️ 🔒 natas3.natas.labs.overthewire.org ☆ 📧 Ⓜ️  
NATAS3  
🔍 Inspector 📄 Console 🐛 Debugger ⬆️⬆️ Network {} Style Editor 🕒 Performance  
🔍 Search HTML + ✎  
▼ <div id="content"> [overthewire]  
  ::before  
  There is nothing on this page  
  <!--No more information leaks!! Not even Google will find it this time...-->  
  ...  
html > body
```

Natas 3; robots.txt file

5

Файл robots.txt представляет собой набор инструкций для ботов. Этот файл включен в исходные файлы большинства веб-сайтов. Файлы robots.txt в основном предназначены для управления действиями “хороших” ботов, таких как web crawlers, поскольку “плохие” боты вряд ли будут следовать инструкциям.

Любой человек или программа, активная в Интернете, будет иметь «user agent» или назначенное имя.

Этому агенту запрещено посещать любые страницы домена

А этому можно все, но с запросами не чаще, чем раз в секунду

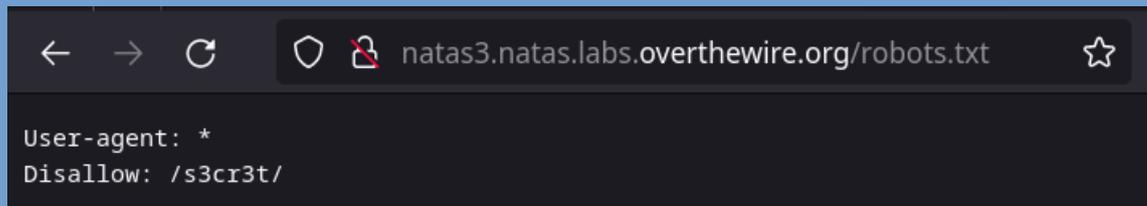


```
User-agent: 008  
Disallow: /
```

```
User-agent: SiteAuditBot  
Crawl-delay: 1  
Allow: /
```

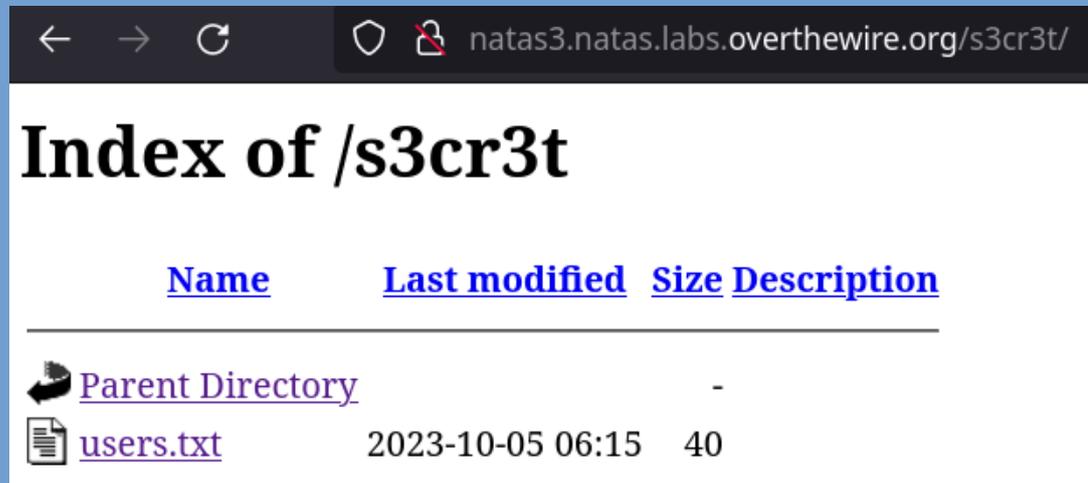
Natas 3

6



A screenshot of a web browser showing the robots.txt file for the URL `natas3.natas.labs.overthewire.org/robots.txt`. The browser's address bar shows the URL with a lock icon and a star icon. Below the address bar, the content of the robots.txt file is displayed: `User-agent: *` and `Disallow: /s3cr3t/`.

Давайте посмотрим на robots.txt



A screenshot of a web browser showing a directory listing for the URL `natas3.natas.labs.overthewire.org/s3cr3t/`. The browser's address bar shows the URL with a lock icon and a star icon. The main content area displays the title **Index of /s3cr3t** and a table with columns for Name, Last modified, Size, and Description. The table contains two entries: a directory named `Parent Directory` and a file named `users.txt` with a last modified date of 2023-10-05 06:15 and a size of 40 bytes.

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 users.txt	2023-10-05 06:15	40	

Может гугл и не смог бы, но мы нашли наш пароль, ура!

Natas 4

7

Нам говорят, что мы должны прийти из natas5, но как?

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

[Refresh page](#)

Давайте кликнем на “обновить страницу”

Чуда не случилось, но он как-то понимает, откуда мы пришли

```
Access disallowed. You are visiting from "http://natas4.natas.labs.overthewire.org/" while authorized users should come only from "http://natas5.natas.labs.overthewire.org/"
```

[Refresh page](#)

Natas 4; "Referer" (a misspelling of Referrer)

8

Заголовок HTTP-запроса Referer содержит абсолютный или частичный адрес, с которого был запрошен ресурс. Заголовок Referer позволяет серверу идентифицировать ссылающиеся страницы, с которых люди переходят на ресурс, или где используются запрошенные ресурсы. Эти данные можно использовать для аналитики, ведения журналов, оптимизированного кэширования и многого другого.

Когда вы переходите по ссылке, Referer содержит адрес страницы, на которой есть ссылка. Когда вы отправляете запросы ресурсов в другой домен, Referer содержит адрес страницы, которая использует запрошенный ресурс.

Natas 4

9

Два пути



Установить curl



Какой выберет
юноша?



Установить
расширение в браузер



25 лет
Сдержанность и экономия



25 лет
Моральное разложение
и разгульная жизнь



36 лет
Заслуженный успех



36 лет
Пороки и дегенерация



60 лет
Почтенная старость



60 лет
Омерзительная развалина

Давайте как-то подменим наш referer

Например, используем cURL

cURL — command line tool and library
for transferring data with URLs

Natas 4

10

Найдем нужную опцию:

```
~ > curl --help all | grep refer
-e, --referer <URL>      Referrer URL
```

Запросим страницу с подмененным referer, грегнемся по regexp "pass", и пароль у нас в руках консоли!

```
~ > curl -u natas4:tK0cJIbzM4lTs8hbCmzn5Zr4434fGZQm -e http://natas5.natas.labs.overthewire.org/ http://natas4.natas.labs.overthewire.org/ | grep pass
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload  Total      Spent    Left     Speed
100  962  100  962    0     0   4473      0  ---:---:--  ---:---:--  ---:---:--  4516
<script>var wechallinfo = { "level": "natas4", "pass": "tK0cJIbzM4lTs8hbCmzn5Zr4434fGZQm" };</script></head>
Access granted. The password for natas5 is Z0NsrtIkJoKALBCLi5eqFfcRN82Au2oD
```

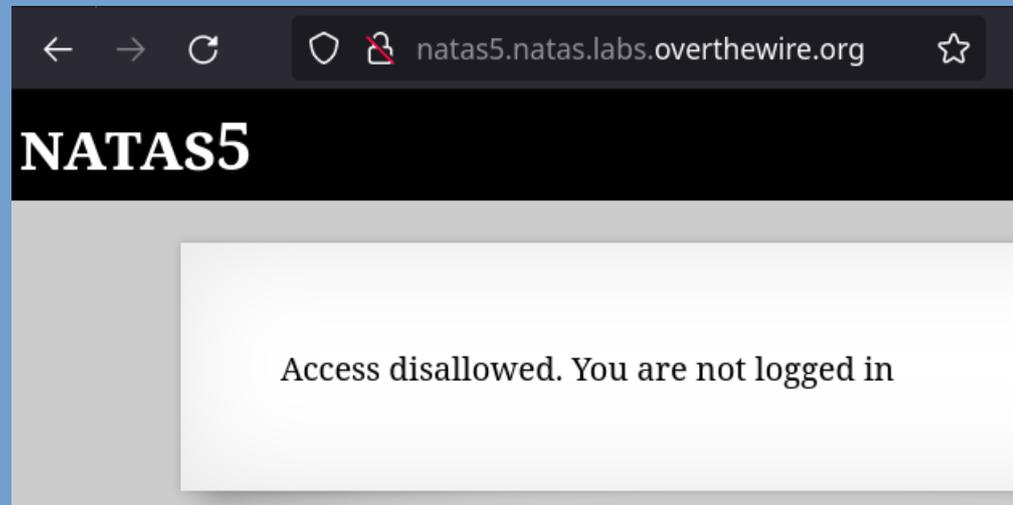
Natas 5

11

Мы в natas5

Неожиданно нам говорят, что мы не залогинились, но ведь мы сделали это только что...

Код страницы не содержит ничего интересного, как быть?



Natas 5; cookies

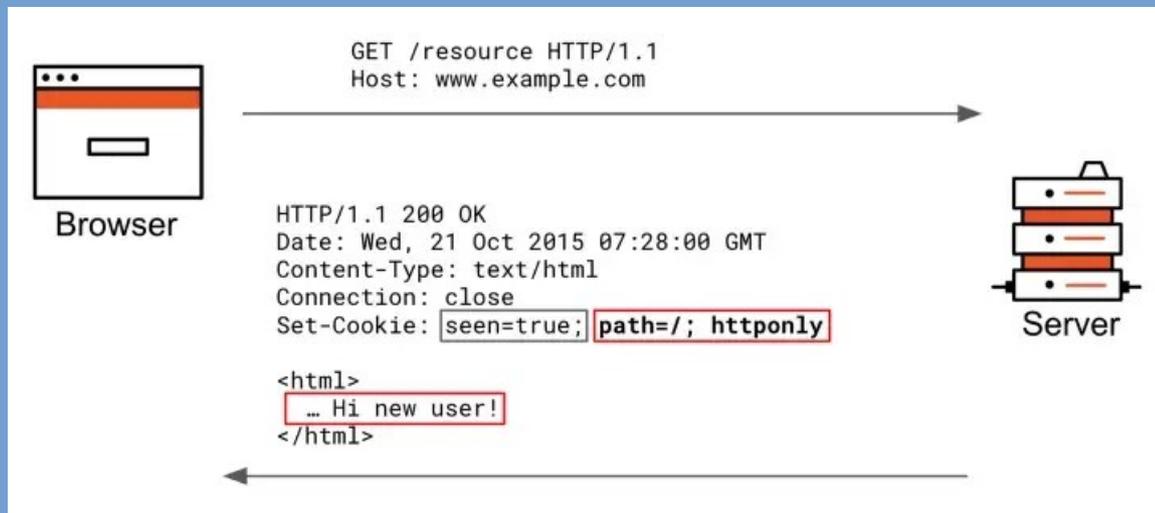
12

Протокол http не поддерживает статические данные, это и не было нужно раньше, когда на сайтах не было аккаунтов, и не нужно было поддерживать сессию.

Ответом на недостаток стали cookie.

Cookies — это фрагмент данных, в которых сервер передаёт важную информацию о клиенте. Браузер получает этот фрагмент, сохраняет его и с каждым последующим запросом отправляет обратно на сервер. Так он понимает, от какого клиента пришёл запрос. Куки выглядят, как пара **ключ=значение**.

На деревьях везде гуки, они нашли меня по cookie



Natas 5

13

Давайте посмотрим на куки:

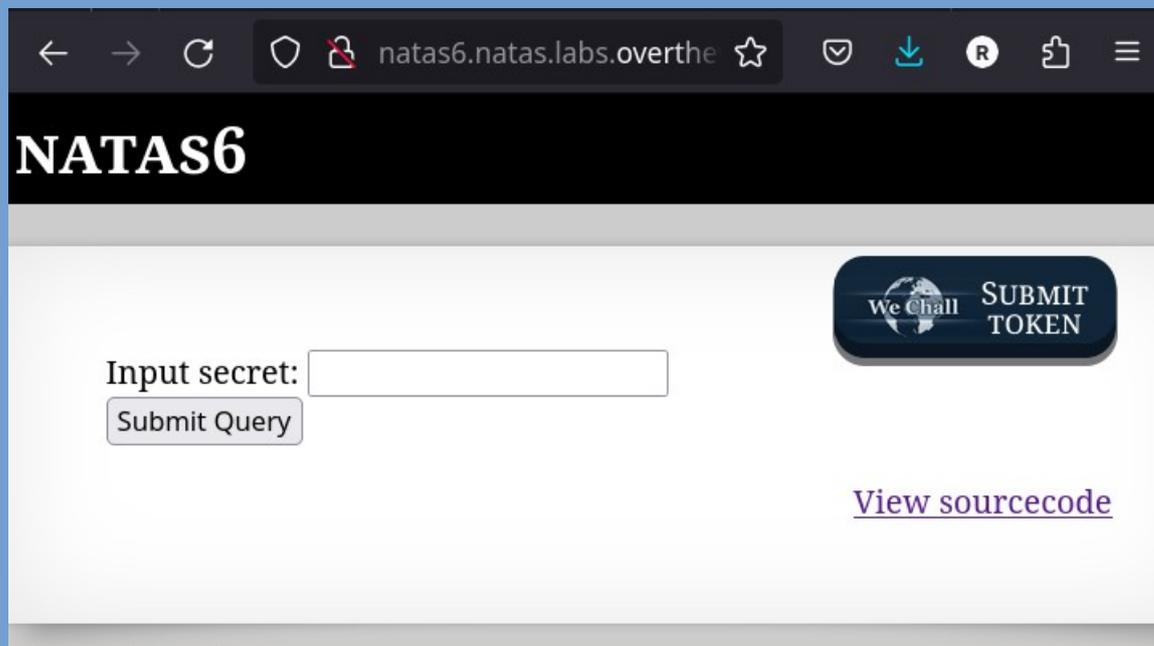
The screenshot shows a browser window with the URL `natas5.natas.labs.overthewire.org`. The developer tools are open to the Storage tab, specifically the Cookies section. The following table displays the cookies for the current page:

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
loggedin	0	natas5.natas.labs.ov...	/	Session	9	false	false	None	Sat, 20 Apr 2024 2...

Кука `loggedin` отвечает за то, залогинились мы, или нет. Изменим значение на 1, тыкнем F5, и, вуаля, пароль наш!

Natas 6

14



Что-то новенькое, нам предлагают ввести некое тайное значение

Также можно посмотреть исходный код

Давайте посмотрим

Natas 6

15

Некая PHP функция. Давайте перебором отвлечемся от веб-разработке и разберемся, что она делает.

Функция сравнивает переданное значение со значением переменной `$secret` из соответствующей библиотеки.

Но ее значение не известно, что же делать, должна быть какая-то утечка данных...

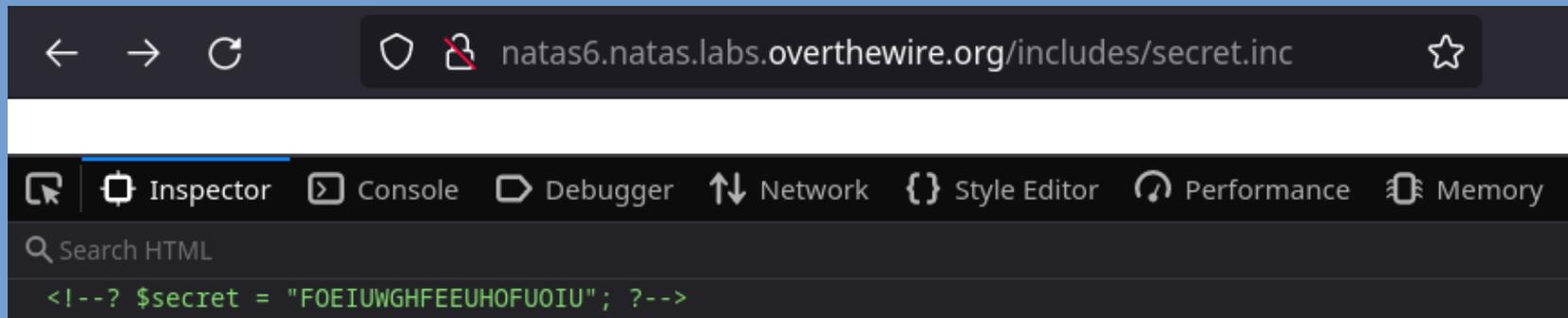
```
<?
include "includes/secret.inc";

if(array_key_exists("submit", $_POST)) {
    if($secret == $_POST['secret']) {
        print "Access granted. The password for natas7 is <censored>";
    } else {
        print "Wrong secret";
    }
}
?>
```

Natas 6

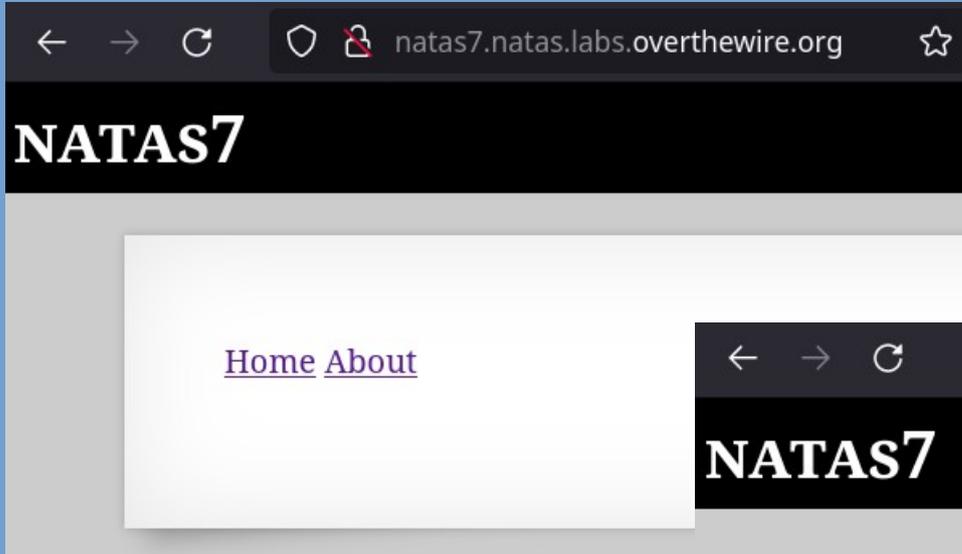
16

Админ снова совершил ту же ошибку!



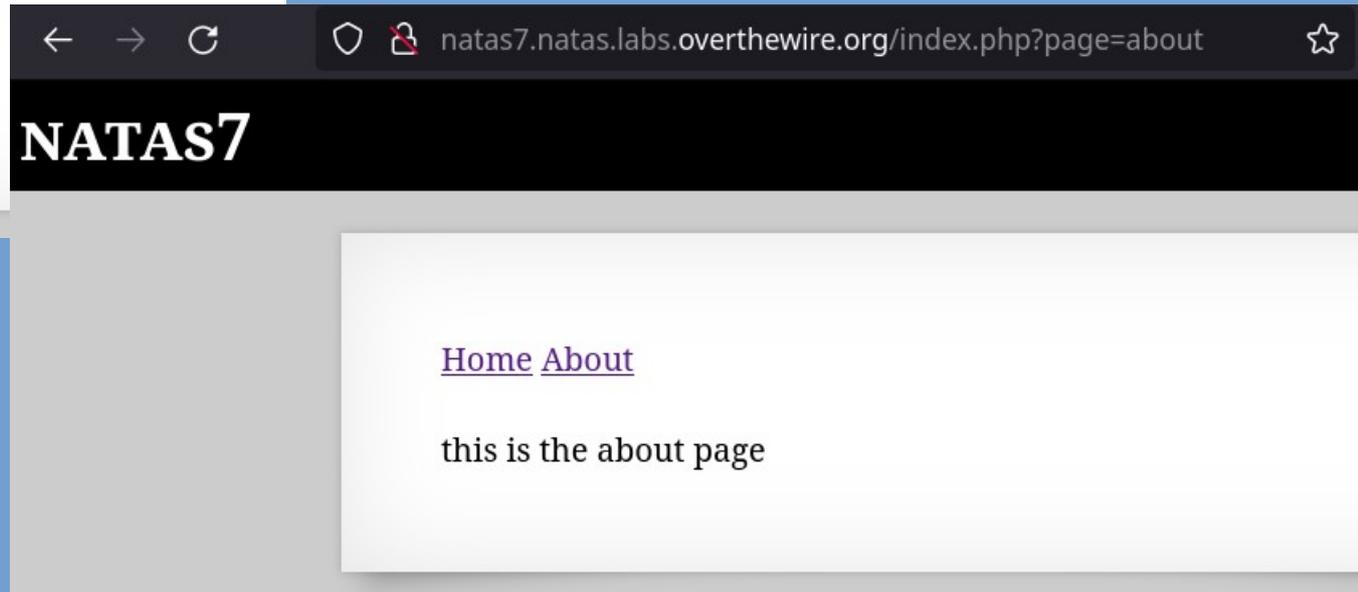
Natas 7

17



Не очень содержательно, но...

Теперь для перехода на другие страницы используется PHP, это должно что-то дать



Natas 7; index.php

18

index.php — это стартовая точка запуска программы на PHP

index.php как правило содержит инициализацию всех компонентов сайта, подгружаемых с помощью конструкций `include` и `require`

На этот раз
перебороть
неприятнь к web'у
не удалось...

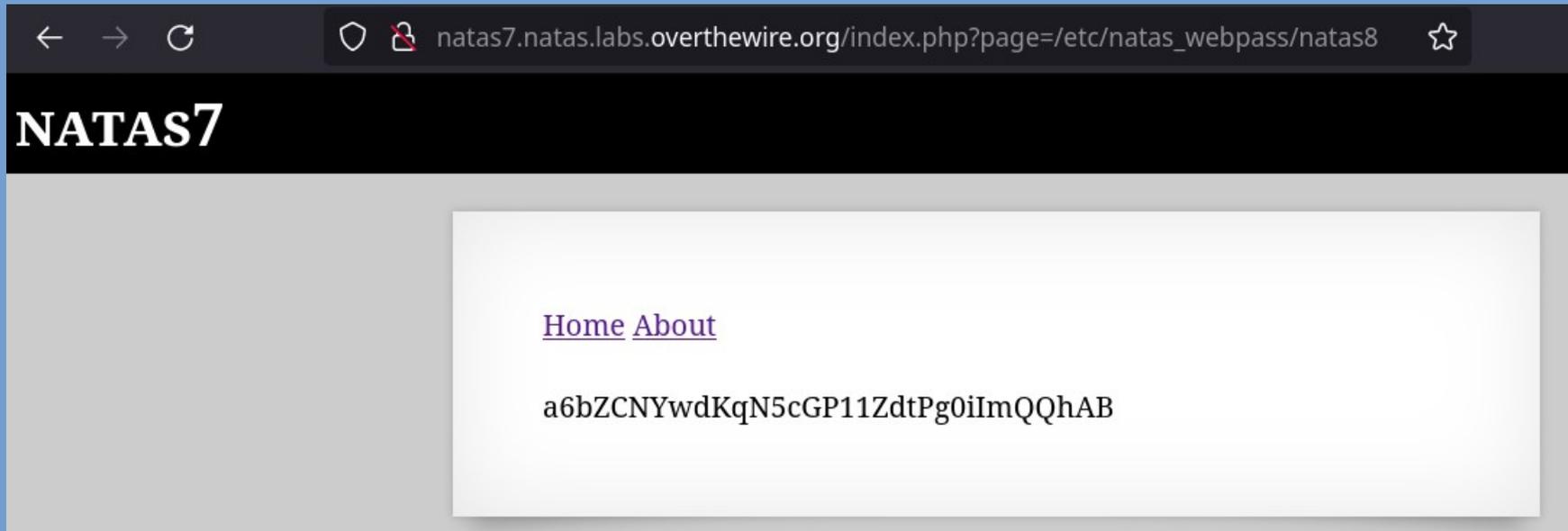
```
<?php
define("APPLICATION_PATH",  dirname(__FILE__));

$app = new Yaf_Application(APPLICATION_PATH . "/conf/application.ini");
$app->bootstrap() //call bootstrap methods defined in Bootstrap.php
->run();
?>
```

Natas 7

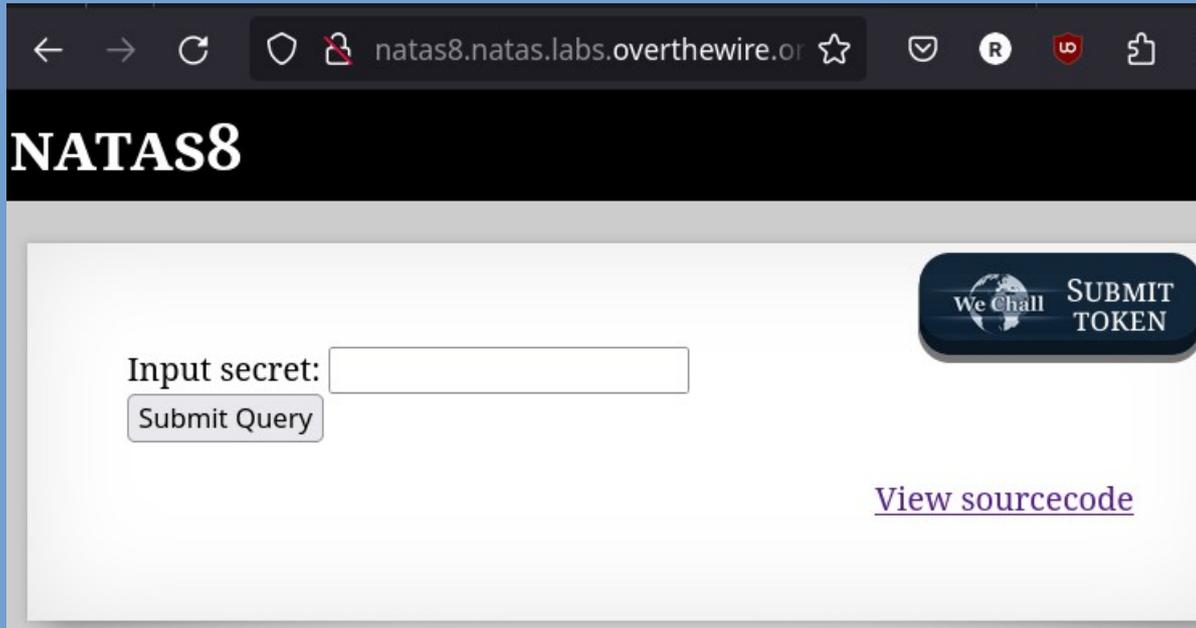
19

Так или иначе, использовать незащищенность
php-скрипта было не сложно



Natas 8

20



Где-то я уже это видел...

Natas 8

21

Больше никаких инклюдников, закодированное значение известно. Что ж, нам остается только заняться раскодировкой.

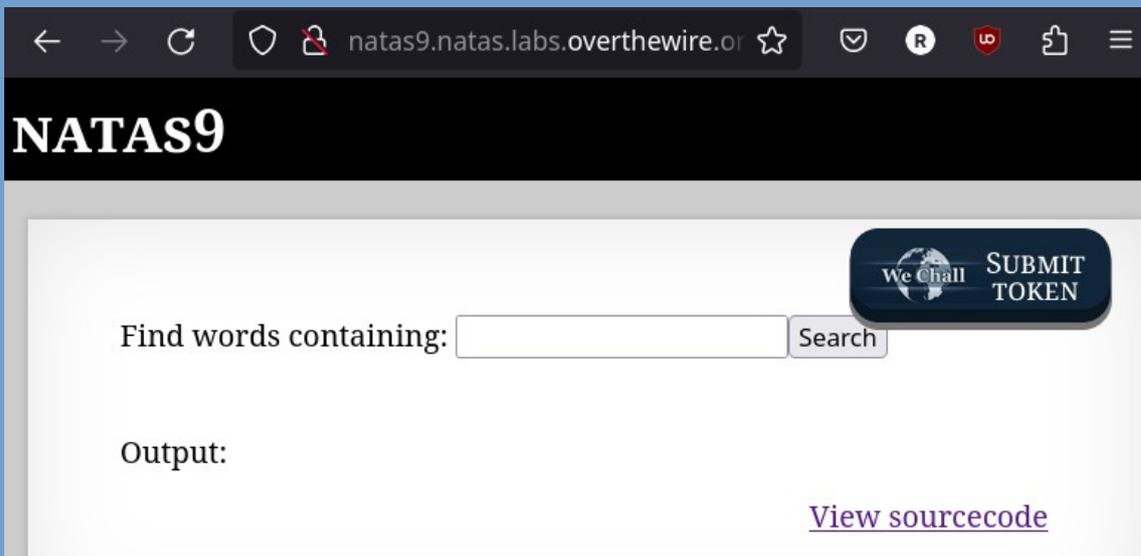
```
<?
$encodedSecret = "3d3d516343746d4d6d6c315669563362";

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";
    }
}
?>
```


Natas 9

23



Хм, какой-то поисковик

Ага, он грепается по словарю и ищет совпадения
Скачаем словарь, потратим 10 минут на просмотр его в less и ничего...

Output:

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

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

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

Natas 9

24

```
; cat /etc/natas_webpass/natas10 #
```

А ларчик просто открывался!

Natas 9

25



ПОТИМУ...

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

NATAS10



For security reasons, we now filter on certain characters

Find words containing:

Output:

[View sourcecode](#)

Однако мы все еще можем как-то эксплуатировать исполнение этой строки в sh

Natas 9

26

```
./etc/natas_webpass/natas11 #
```

Все еще просто, для тех, что прошел OTW bandit ;)

THE END OF PRESENTATION