Web Security and Malware Analysis

Answers for Assignment 1

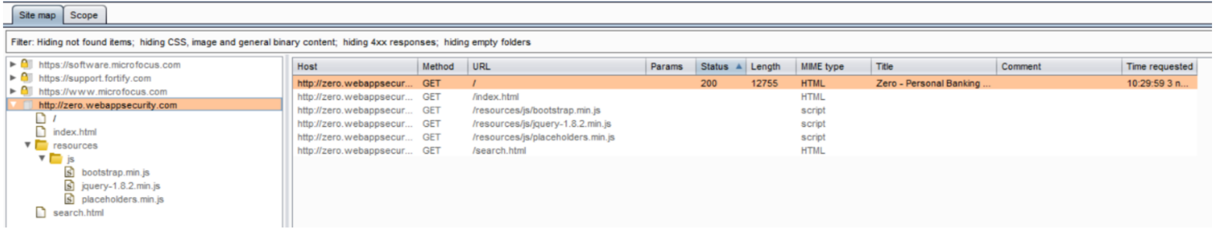
SILVIA LUCIA SANNA – 70/90/00053

Task 1 - Spidering

In this task I had to make a spidering, even automatically either manually, on this web site http://zero.webappsecurity.com/

I did 3 things:

- First, I explored all the possible buttons, links manually using “Burp” and seeing the directories on its “target” and “site map” options. I noticed that some pages are not displayed until I click on them. Of course, the pages related to the user are not showed until I login. Some other links are not displayed until I click on a specific page, this could be explained because the web app accesses to that specific link only when a page is opened.

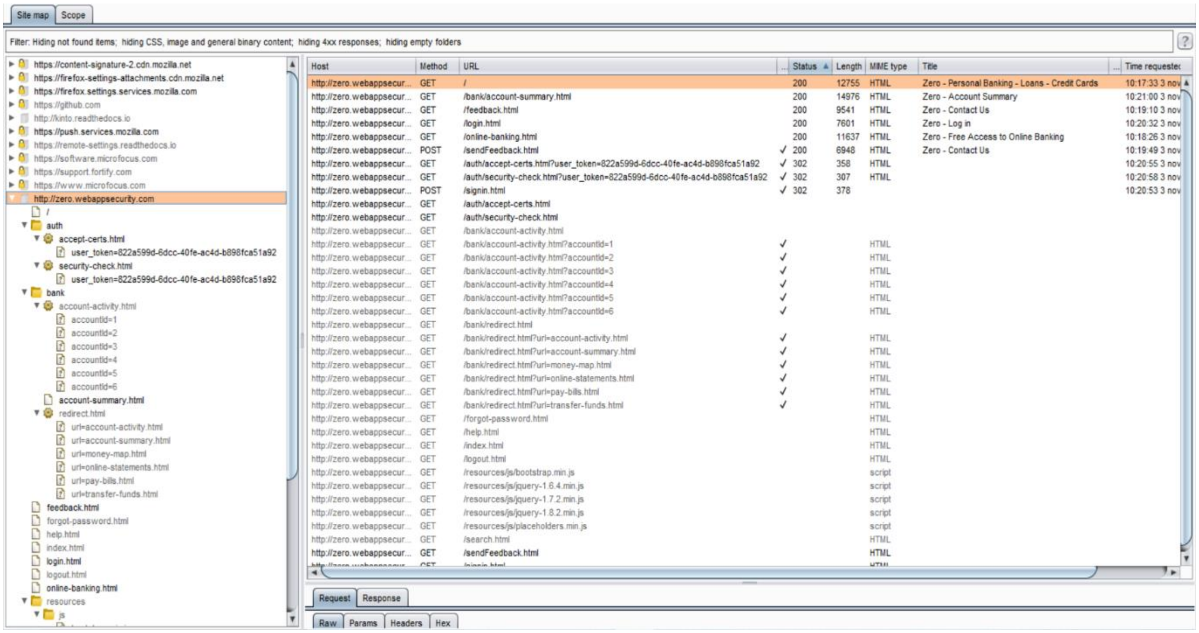


Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

```
▶ https://software.microfocus.com
▶ https://support.fortify.com
▶ https://www.microfocus.com
▼ http://zero.webappsecurity.com
    /
    index.html
  ▼ resources
    ▼ js
        bootstrap.min.js
        jquery-1.8.2.min.js
        placeholders.min.js
    search.html
```

Host	Method	URL	Params	Status ▲	Length	MIME type	Title	Comment	Time requested
http://zero.webappsecur...	GET	/		200	12755	HTML	Zero - Personal Banking ...		10:29:59 3 n...
http://zero.webappsecur...	GET	/index.html				HTML			
http://zero.webappsecur...	GET	/resources/js/bootstrap.min.js				script			
http://zero.webappsecur...	GET	/resources/js/jquery-1.8.2.min.js				script			
http://zero.webappsecur...	GET	/resources/js/placeholders.min.js				script			
http://zero.webappsecur...	GET	/search.html				HTML			

Figure 1: Spidering when just I clicked on the link



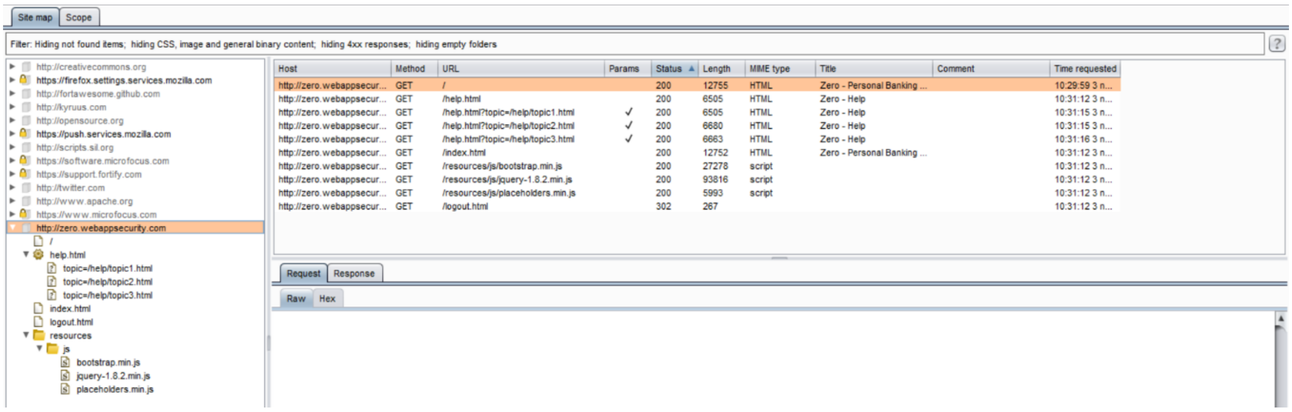
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

```
▶ https://content-signature-2.cdn.mozilla.net
▶ https://firefox-settings-attachments.cdn.mozilla.net
▶ https://firefox.settings.services.mozilla.com
▶ https://github.com
▶ http://kinto.readthedocs.io
▶ https://push.services.mozilla.com
▶ https://remote-settings.readthedocs.io
▶ https://software.microfocus.com
▶ https://support.fortify.com
▶ https://www.microfocus.com
▼ http://zero.webappsecurity.com
    /
  ▼ auth
    ▼ accept-certs.html
        user_token=822a599d-6dcc-40fe-ac4d-b898fca51a92
    ▼ security-check.html
        user_token=822a599d-6dcc-40fe-ac4d-b898fca51a92
  ▼ bank
    ▼ account-activity.html
        accountId=1
        accountId=2
        accountId=3
        accountId=4
        accountId=5
        accountId=6
      account-summary.html
    ▼ redirect.html
        url=account-activity.html
        url=account-summary.html
        url=money-map.html
        url=online-statements.html
        url=pay-bills.html
        url=transfer-funds.html
    feedback.html
    forgot-password.html
    help.html
    index.html
    login.html
    logout.html
    online-banking.html
  ▼ resources
    ▼ js
```

Host	Method	URL	...	Status ▲	Length	MIME type	Title	...	Time requestec
http://zero.webappsecur...	GET	/		200	12755	HTML	Zero - Personal Banking - Loans - Credit Cards		10:17:33 3 nov
http://zero.webappsecur...	GET	/bank/account-summary.html		200	14976	HTML	Zero - Account Summary		10:21:00 3 nov
http://zero.webappsecur...	GET	/feedback.html		200	9541	HTML	Zero - Contact Us		10:19:10 3 nov
http://zero.webappsecur...	GET	/login.html		200	7601	HTML	Zero - Log in		10:20:32 3 nov
http://zero.webappsecur...	GET	/online-banking.html		200	11637	HTML	Zero - Free Access to Online Banking		10:18:26 3 nov
http://zero.webappsecur...	POST	/sendFeedback.html	✓	200	6948	HTML	Zero - Contact Us		10:19:49 3 nov
http://zero.webappsecur...	GET	/auth/accept-certs.html?user_token=822a599d-6dcc-40fe-ac4d-b898fca51a92	✓	302	358	HTML			10:20:55 3 nov
http://zero.webappsecur...	GET	/auth/security-check.html?user_token=822a599d-6dcc-40fe-ac4d-b898fca51a92	✓	302	307	HTML			10:20:58 3 nov
http://zero.webappsecur...	POST	/signin.html	✓	302	378				10:20:53 3 nov
http://zero.webappsecur...	GET	/auth/accept-certs.html							
http://zero.webappsecur...	GET	/auth/security-check.html							
http://zero.webappsecur...	GET	/bank/account-activity.html							
http://zero.webappsecur...	GET	/bank/account-activity.html?accountId=1	✓			HTML			
http://zero.webappsecur...	GET	/bank/account-activity.html?accountId=2	✓			HTML			
http://zero.webappsecur...	GET	/bank/account-activity.html?accountId=3	✓			HTML			
http://zero.webappsecur...	GET	/bank/account-activity.html?accountId=4	✓			HTML			
http://zero.webappsecur...	GET	/bank/account-activity.html?accountId=5	✓			HTML			
http://zero.webappsecur...	GET	/bank/account-activity.html?accountId=6	✓			HTML			
http://zero.webappsecur...	GET	/bank/redirect.html							
http://zero.webappsecur...	GET	/bank/redirect.html?url=account-activity.html	✓			HTML			
http://zero.webappsecur...	GET	/bank/redirect.html?url=account-summary.html	✓			HTML			
http://zero.webappsecur...	GET	/bank/redirect.html?url=money-map.html	✓			HTML			
http://zero.webappsecur...	GET	/bank/redirect.html?url=online-statements.html	✓			HTML			
http://zero.webappsecur...	GET	/bank/redirect.html?url=pay-bills.html	✓			HTML			
http://zero.webappsecur...	GET	/bank/redirect.html?url=transfer-funds.html	✓			HTML			
http://zero.webappsecur...	GET	/forgot-password.html				HTML			
http://zero.webappsecur...	GET	/help.html				HTML			
http://zero.webappsecur...	GET	/index.html				HTML			
http://zero.webappsecur...	GET	/logout.html				HTML			
http://zero.webappsecur...	GET	/resources/js/bootstrap.min.js				script			
http://zero.webappsecur...	GET	/resources/js/jquery-1.6.4.min.js				script			
http://zero.webappsecur...	GET	/resources/js/jquery-1.7.2.min.js				script			
http://zero.webappsecur...	GET	/resources/js/jquery-1.8.2.min.js				script			
http://zero.webappsecur...	GET	/resources/js/placeholders.min.js				script			
http://zero.webappsecur...	GET	/search.html				HTML			
http://zero.webappsecur...	GET	/sendFeedback.html				HTML			

Figure 2: Spidering when I manually logged in

- Second, I downloaded burp version 1.7.30 and made an auto-spidering using the "Spider" option. I did it all automatically except for the login (even if I put "auto login using this credential it did not work, I do not know why; I repeated it different times to be sure that the pages Burp showed me did not change, but at a certain time the login was not successful even if the credentials where right). Before the login I had only very few pages, after the login I found all pages related to the user such as "Account Summary", "Account Activity", "Transfer funds", "Pay Bills", "My Money Map", "Online Statements".



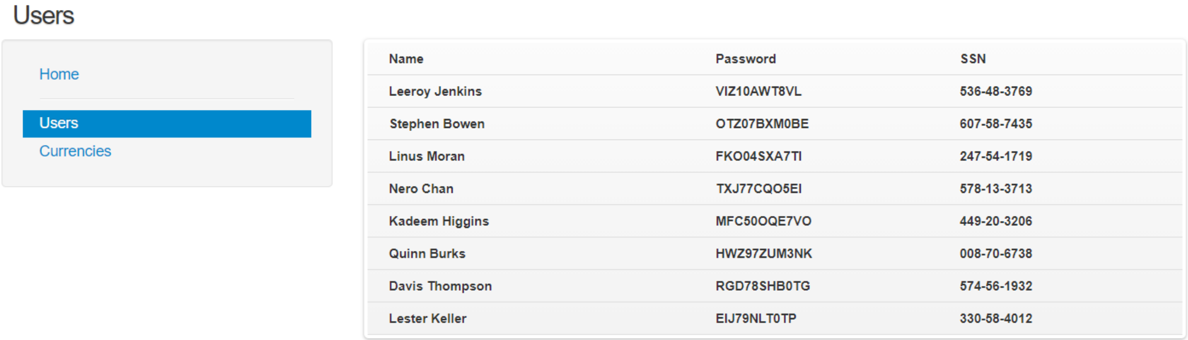
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

```
▶ http://creativecommons.org
▶ https://firefox.settings.services.mozilla.com
▶ http://fortawesome.github.com
▶ http://kyruus.com
▶ http://opensource.org
▶ https://push.services.mozilla.com
▶ http://scripts.sil.org
▶ https://software.microfocus.com
▶ https://support.fortify.com
▶ http://twitter.com
▶ http://www.apache.org
▶ https://www.microfocus.com
▼ http://zero.webappsecurity.com
    /
  ▼ help.html
      topic=/help/topic1.html
      topic=/help/topic2.html
      topic=/help/topic3.html
    index.html
    logout.html
  ▼ resources
    ▼ js
        bootstrap.min.js
        jquery-1.8.2.min.js
        placeholders.min.js
```

Host	Method	URL	Params	Status ▲	Length	MIME type	Title	Comment	Time requested
http://zero.webappsecur...	GET	/		200	12755	HTML	Zero - Personal Banking ...		10:29:59 3 n...
http://zero.webappsecur...	GET	/help.html		200	6505	HTML	Zero - Help		10:31:12 3 n...
http://zero.webappsecur...	GET	/help.html?topic=/help/topic1.html	✓	200	6505	HTML	Zero - Help		10:31:15 3 n...
http://zero.webappsecur...	GET	/help.html?topic=/help/topic2.html	✓	200	6680	HTML	Zero - Help		10:31:15 3 n...
http://zero.webappsecur...	GET	/help.html?topic=/help/topic3.html	✓	200	6663	HTML	Zero - Help		10:31:16 3 n...
http://zero.webappsecur...	GET	/index.html		200	12752	HTML	Zero - Personal Banking ...		10:31:12 3 n...
http://zero.webappsecur...	GET	/resources/js/bootstrap.min.js		200	27278	script			10:31:12 3 n...
http://zero.webappsecur...	GET	/resources/js/jquery-1.8.2.min.js		200	93816	script			10:31:12 3 n...
http://zero.webappsecur...	GET	/resources/js/placeholders.min.js		200	5993	script			10:31:12 3 n...
http://zero.webappsecur...	GET	/logout.html		302	267				10:31:12 3 n...

Figure 3: Auto spidering without login

- Third I tried to explore the web site with the common crawler such as robots.txt, files, secret but I found only the directory “admin”. (Images 13-14). This directory was not found by the automatic spidering maybe because this page has some private and sensitive data (login credentials such as usernames and passwords) and it could have some blocks to not be find automatically but only manual disclosure.



Name	Password	SSN
Leeroy Jenkins	VIZ10AWT8VL	536-48-3769
Stephen Bowen	OTZ07BXM0BE	607-58-7435
Linus Moran	FKO04SXA7TI	247-54-1719
Nero Chan	TXJ77CQO5EI	578-13-3713
Kadeem Higgins	MFC50OQE7VO	449-20-3206
Quinn Burks	HWZ97ZUM3NK	008-70-6738
Davis Thompson	RGD78SHB0TG	574-56-1932
Lester Keller	EIJ79NLT0TP	330-58-4012

Figure 4: Users list when I manually browsed to admin page

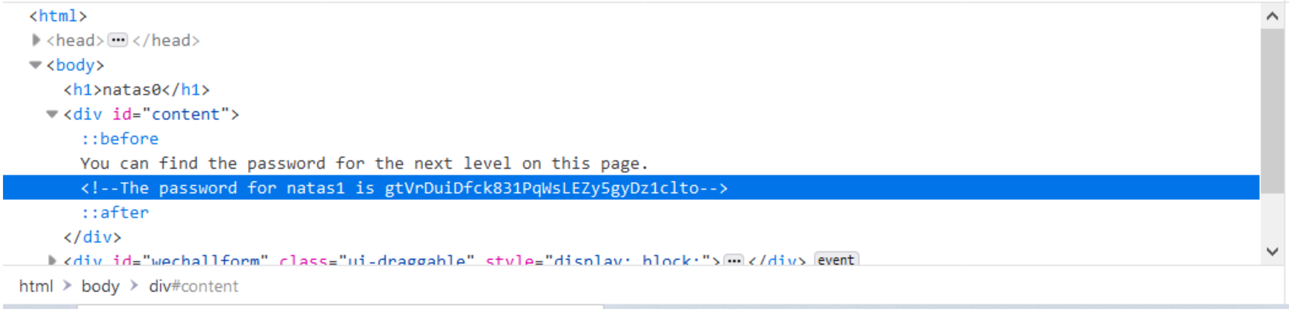
In this website I also tried some SQL injection (in the login platform and search bar) and Javascript injection (in feedback page) but I have found no vulnerabilities.

Moreover, I have noticed that there is an enumeration between the account id. So, I have tried to change that number (in auto spidering I only see the first 6) with different ones and I have noticed that from number 7 so on they prompt to me the same account activity. I do not know why they do this but maybe can be a sort of hiding some information so that the attacker cannot see anything, use some errors to attack, cannot inject anything.

Task 2 – Basic Web Hacking

In this task I had to find each password to access to the next level of this challenge.

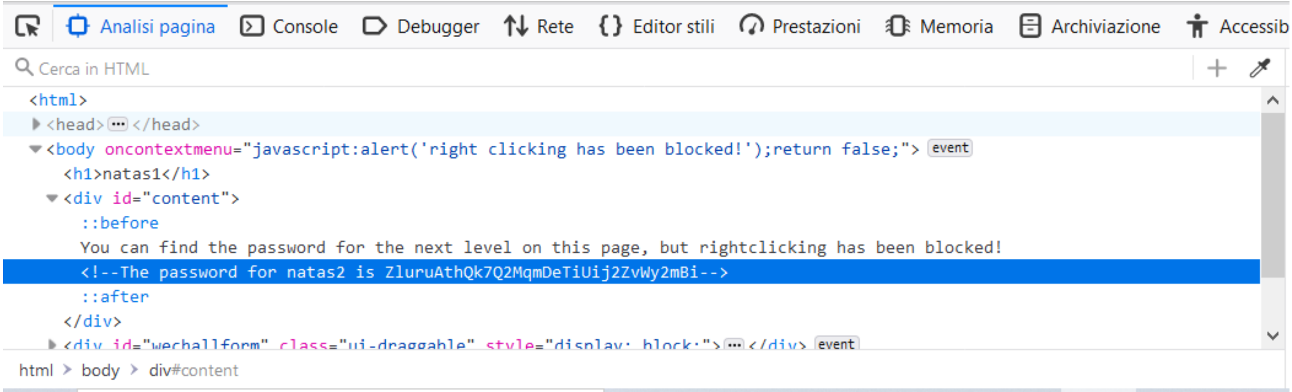
- Natas 0: in this level I found the password for natas 1 by only inspecting the source code



```
<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" class="ui-draggable" style="display: block;">…</div> event
```

Figure 5: Password for natas 1

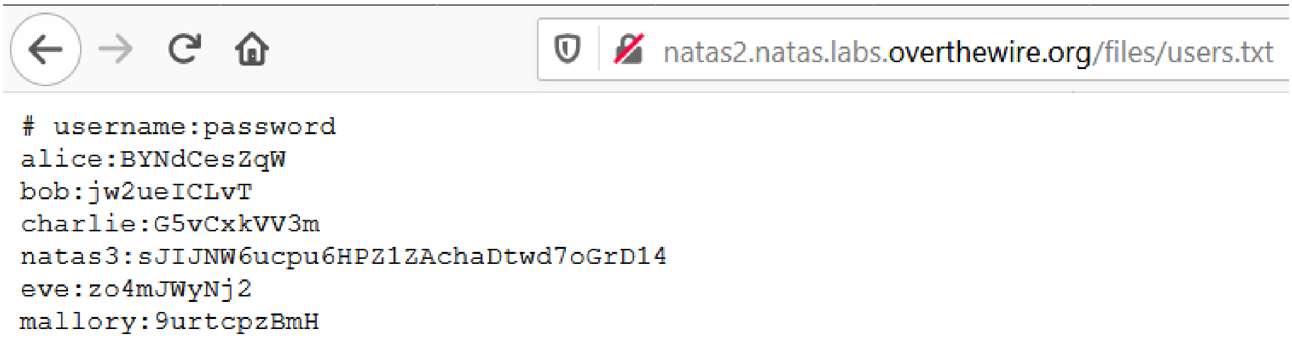
- Natas 1: here again I found the password for natas 2 by inspecting the html body



```
<html>
  <head>…</head>
  <body oncontextmenu="javascript:alert('right clicking has been blocked!');return false;"> event
    <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" class="ui-draggable" style="display: block;">…</div> event
```

Figure 6: Password for natas 2

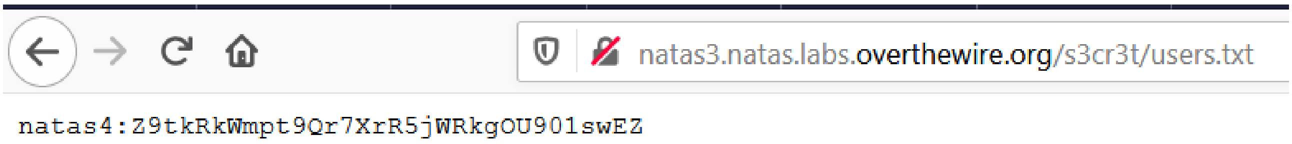
- Natas2: here I tried some manual spidering and one of the common directories to try is /files. Here this directory does exist so I found a .txt file, called users.txt, when I opened I saw natas3 password with other users passwords.



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

Figure 7: Password for natas 3

- Natas3: another common file for manual spidering is the robots.txt file, commonly used for deny or allow accesses to specific files and it is the file of the omonim protocol. Where in natas3 I searched for robots.txt in the URL (http://natas3.natas.labs.overthewire.org/robots.txt) it showed me a secret directory, so my URL became http://natas3.natas.labs.overthewire.org/s3cr3t/. In this URL I found a users.txt file where was the natas4 password

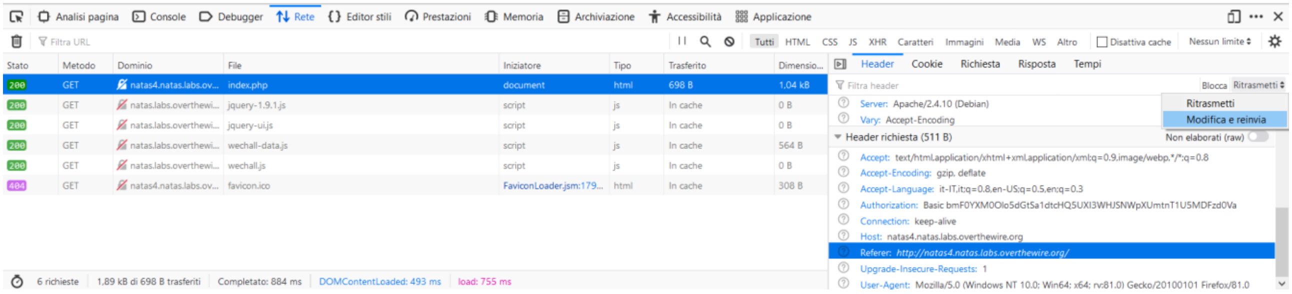


natas3.natas.labs.overthewire.org/s3cr3t/users.txt

```
natas4:Z9tkRkWmpt9Qr7XrR5jWRkgOU901swEZ
```

Figure 8: Password for natas 4

- Natas4: as I browsed in natas4, the page said me that my network origin was wrong and I must come from another source. There was also a link to refresh the page, as I clicked on it was generated a file index.php where the origin was natas4. So, I thought to change my provenience on that file: in the "Network-Header" section of the analysis I changed the "Referer" field which stands for "From which URL are you coming from?". As I changed the referer with the right one and I sent it, I clicked on the same file and in the "HTTP Response" I had the natas5 password.



Stato	Metodo	Dominio	File	Iniziatore	Tipo	Trasferito	Dimensio...
200	GET	natas4.natas.labs.ov...	index.php	document	html	698 B	1,04 kB
200	GET	natas.labs.overthewi...	jquery-1.9.1.js	script	js	In cache	0 B
200	GET	natas.labs.overthewi...	jquery-ui.js	script	js	In cache	0 B
200	GET	natas.labs.overthewi...	wechall-data.js	script	js	In cache	564 B
200	GET	natas.labs.overthewi...	wechall.js	script	js	In cache	0 B
404	GET	natas4.natas.labs.ov...	favicon.ico	FaviconLoader.jsm:179...	html	In cache	308 B

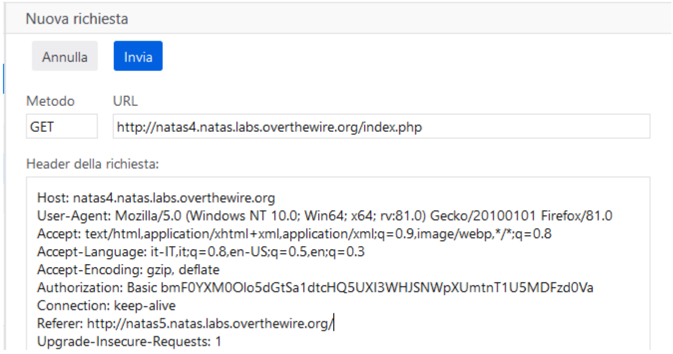
6 richieste | 1,89 kB di 698 B trasferiti | Completato: 884 ms | DOMContentLoaded: 493 ms | load: 755 ms

Server: Apache/2.4.10 (Debian)
Vary: Accept-Encoding

Header richiesta (511 B)

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Authorization: Basic bmF0YXM0Olo5dGtSa1dtcHQ5UXI3WHJSNWpXUmtnT1U5MDFzd0Va
Connection: keep-alive
Host: natas4.natas.labs.overthewire.org
Referer: http://natas4.natas.labs.overthewire.org/
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0

Figure 9: Network interception in natas 4



Nuova richiesta

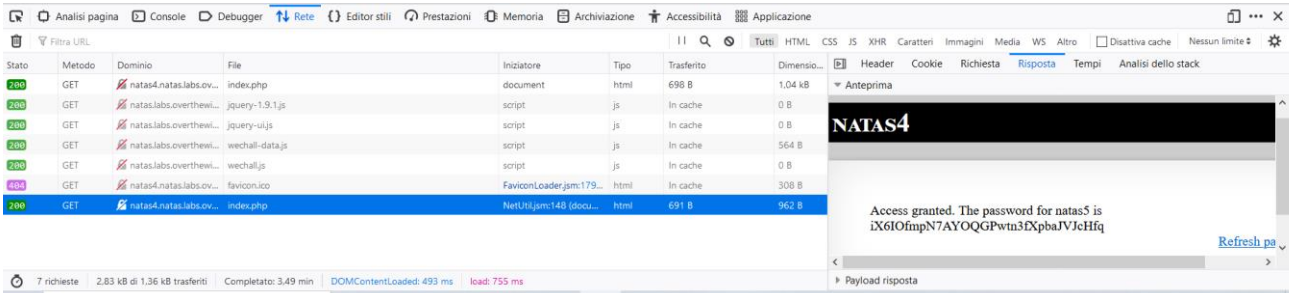
Metodo: GET

URL: http://natas4.natas.labs.overthewire.org/index.php

Header della richiesta:

```
Host: natas4.natas.labs.overthewire.org
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Authorization: Basic bmF0YXM0Olo5dGtSa1dtcHQ5UXI3WHJSNWpXUmtnT1U5MDFzd0Va
Connection: keep-alive
Referer: http://natas5.natas.labs.overthewire.org/
Upgrade-Insecure-Requests: 1
```

Figure 10: Change referer in natas 4 to reach natas 5



Stato	Metodo	Dominio	File	Iniziatore	Tipo	Trasferito	Dimensio...
200	GET	natas4.natas.labs.ov...	index.php	document	html	698 B	1,04 kB
200	GET	natas.labs.overthewi...	jquery-1.9.1.js	script	js	In cache	0 B
200	GET	natas.labs.overthewi...	jquery-ui.js	script	js	In cache	0 B
200	GET	natas.labs.overthewi...	wechall-data.js	script	js	In cache	564 B
200	GET	natas.labs.overthewi...	wechall.js	script	js	In cache	0 B
404	GET	natas4.natas.labs.ov...	favicon.ico	FaviconLoader.jsm:179...	html	In cache	308 B
200	GET	natas4.natas.labs.ov...	index.php	NetUtil.jsm:148 (docu...	html	691 B	962 B

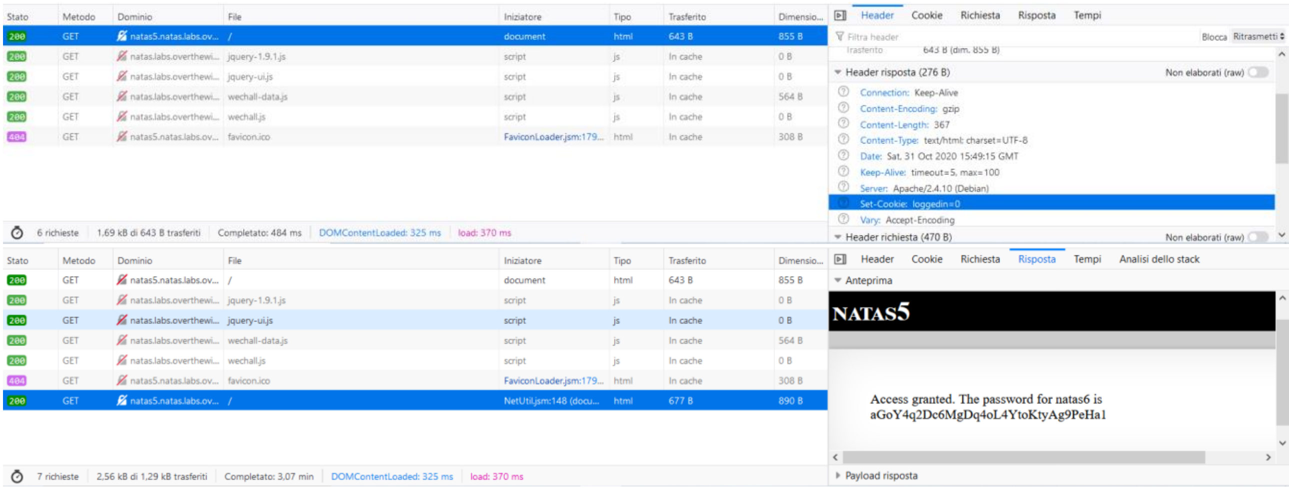
7 richieste | 2,83 kB di 1,36 kB trasferiti | Completato: 3,49 min | DOMContentLoaded: 493 ms | load: 755 ms

NATAS4

Access granted. The password for natas5 is iX6IOfmpN7AYOQGPwtn3fXpbaJVJcHfq

Figure 11: After changing the referer that's the response in natas 4, so I see the password for natas 5

- Natas5: when I browse to natas5 I see that I am not logged in. I immediately notice that is the same problem as the previous one but the field must be different. So I select the "/" file and see that there is a field "Set-Cookie" with a variable "loggedin=0", I change that to 1 and resent. I had the password for natas6 by only changing the cookie value.



Stato	Metodo	Dominio	File	Iniziatore	Tipo	Trasferito	Dimensio...
200	GET	natas5.natas.labs.ov...	/	document	html	643 B	855 B
200	GET	natas.labs.overthewi...	jquery-1.9.1.js	script	js	In cache	0 B
200	GET	natas.labs.overthewi...	jquery-ui.js	script	js	In cache	0 B
200	GET	natas.labs.overthewi...	wechall-data.js	script	js	In cache	564 B
200	GET	natas.labs.overthewi...	wechall.js	script	js	In cache	0 B
404	GET	natas5.natas.labs.ov...	favicon.ico	FaviconLoader.jsm:179...	html	In cache	308 B

6 richieste | 1,69 kB di 643 B trasferiti | Completato: 484 ms | DOMContentLoaded: 325 ms | load: 370 ms

Trasferito 643 B (dim. 855 B)

Header risposta (276 B)

```
Connection: Keep-Alive
Content-Encoding: gzip
Content-Length: 367
Content-Type: text/html; charset=UTF-8
Date: Sat, 31 Oct 2020 15:49:15 GMT
Keep-Alive: timeout=5, max=100
Server: Apache/2.4.10 (Debian)
Set-Cookie: loggedin=0
Vary: Accept-Encoding
```

Header richiesta (470 B)

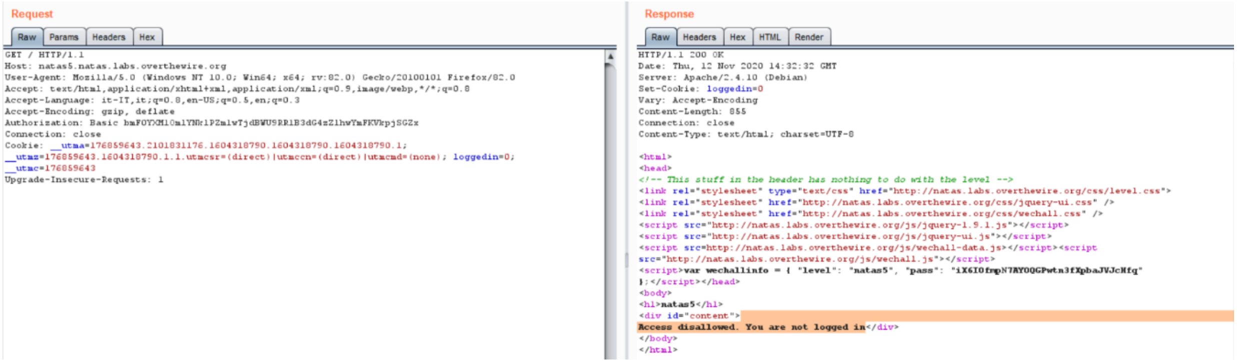
Stato	Metodo	Dominio	File	Iniziatore	Tipo	Trasferito	Dimensio...
200	GET	natas5.natas.labs.ov...	/	document	html	643 B	855 B
200	GET	natas.labs.overthewi...	jquery-1.9.1.js	script	js	In cache	0 B
200	GET	natas.labs.overthewi...	jquery-ui.js	script	js	In cache	0 B
200	GET	natas.labs.overthewi...	wechall-data.js	script	js	In cache	564 B
200	GET	natas.labs.overthewi...	wechall.js	script	js	In cache	0 B
404	GET	natas5.natas.labs.ov...	favicon.ico	FaviconLoader.jsm:179...	html	In cache	308 B
200	GET	natas5.natas.labs.ov...	/	NetUtil.jsm:148 (docu...	html	677 B	890 B

7 richieste | 2,56 kB di 1,29 kB trasferiti | Completato: 3,07 min | DOMContentLoaded: 325 ms | load: 370 ms

NATAS5

Access granted. The password for natas6 is aGoY4q2Dc6MgDq4oL4YtoKtyAg9PeHa1

Figure 12: Network interception in natas 5, change cookies to see next level password as suggested in the home page

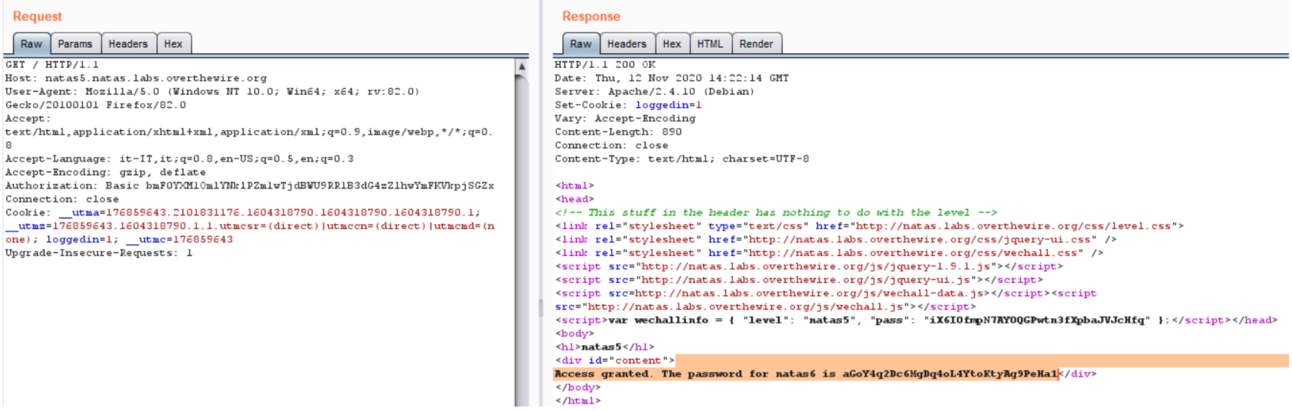


```
GET / HTTP/1.1
Host: natas5.natas.labs.overthewire.org
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Authorization: Basic bmF0YXM1OmlYNkl1PZmlwTjdBWU9RR1B3dG4zZlhwYmFKVkpjSGZx
Connection: close
Cookie: __utma=176859643.2101831176.1604318790.1604318790.1604318790.1;
__utmz=176859643.1604318790.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none); loggedin=0;
__utmc=176859643
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Date: Thu, 12 Nov 2020 14:32:32 GMT
Server: Apache/2.4.10 (Debian)
Set-Cookie: loggedin=0
Vary: Accept-Encoding
Content-Length: 855
Connection: close
Content-Type: text/html; charset=UTF-8

<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"></script>
<script>var wechallinfo = { "level": "natas5", "pass": "iX6IOfmpN7AYOQGPwtn3fXpbaJVJcHfq"
};</script></head>
<body>
<h1>natas5</h1>
<div id="content">
Access disallowed. You are not logged in</div>
</body>
</html>
```

Figure 13: Original request and respons with Burp



```
GET / HTTP/1.1
Host: natas5.natas.labs.overthewire.org
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0)
Gecko/20100101 Firefox/82.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
8
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Authorization: Basic bmF0YXM1OmlYNkl PZmlwTjdBWU9RR1B3dG4zZlhwYmFKVkpjSGZx
Connection: close
Cookie: __utma=176859643.2101831176.1604318790.1604318790.1604318790.1;
__utmz=176859643.1604318790.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(n
one); loggedin=1; __utmc=176859643
Upgrade-Insecure-Requests: 1
```

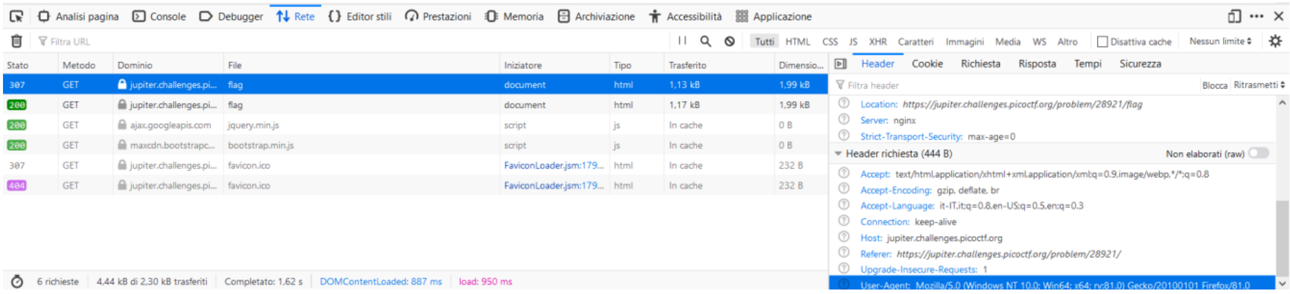
```
HTTP/1.1 200 OK
Date: Thu, 12 Nov 2020 14:22:14 GMT
Server: Apache/2.4.10 (Debian)
Set-Cookie: loggedin=1
Vary: Accept-Encoding
Content-Length: 890
Connection: close
Content-Type: text/html; charset=UTF-8

<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"></script>
<script>var wechallinfo = { "level": "natas5", "pass": "iX6IOfmpN7AYOQGPwtn3fXpbaJVJcHfq" };</script></head>
<body>
<h1>natas5</h1>
<div id="content">
Access granted. The password for natas6 is aGoY4q2Dc6MgDq4oL4YtoKtyAg9PeHa1</div>
</body>
</html>
```

Figure 14: Cookie changed with Burp's Repeater

Task 3 – Mangling Requests/Responses

When I browsed to https://jupiter.challenges.picoctf.org/problem/28921/ there was only a big green button with "Flag" text. I clicked on it and I had an alert saying that my browser was not allowed and to change with the allowed one. So I selected the "flag" document and changed the "User-Agent" in the "Network-Header" section with

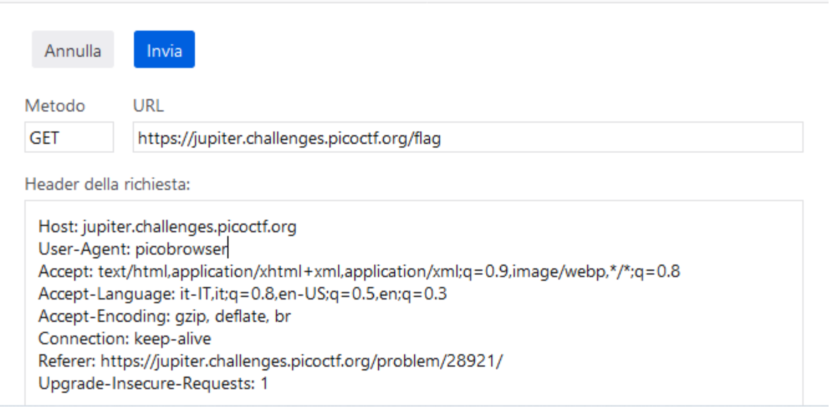


Stato	Metodo	Dominio	File	Iniziatore	Tipo	Trasferito	Dimensio...
307	GET	jupiter.challenges.pi...	flag	document	html	1,13 kB	1,99 kB
200	GET	jupiter.challenges.pi...	flag	document	html	1,17 kB	1,99 kB
200	GET	ajax.googleapis.com	jquery.min.js	script	js	In cache	0 B
200	GET	maxcdn.bootstrapc...	bootstrap.min.js	script	js	In cache	0 B
307	GET	jupiter.challenges.pi...	favicon.ico	FaviconLoader.jsm:179...	html	In cache	232 B
404	GET	jupiter.challenges.pi...	favicon.ico	FaviconLoader.jsm:179...	html	In cache	232 B

6 richieste | 4,44 kB di 2,30 kB trasferiti | Completato: 1,62 s | DOMContentLoaded: 887 ms | load: 950 ms

```
Location: https://jupiter.challenges.picoctf.org/problem/28921/flag
Server: nginx
Strict-Transport-Security: max-age=0
Header richiesta (444 B)                                Non elaborati (raw)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Connection: keep-alive
Host: jupiter.challenges.picoctf.org
Referer: https://jupiter.challenges.picoctf.org/problem/28921/
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0
```

Figure 15: Original user Agent



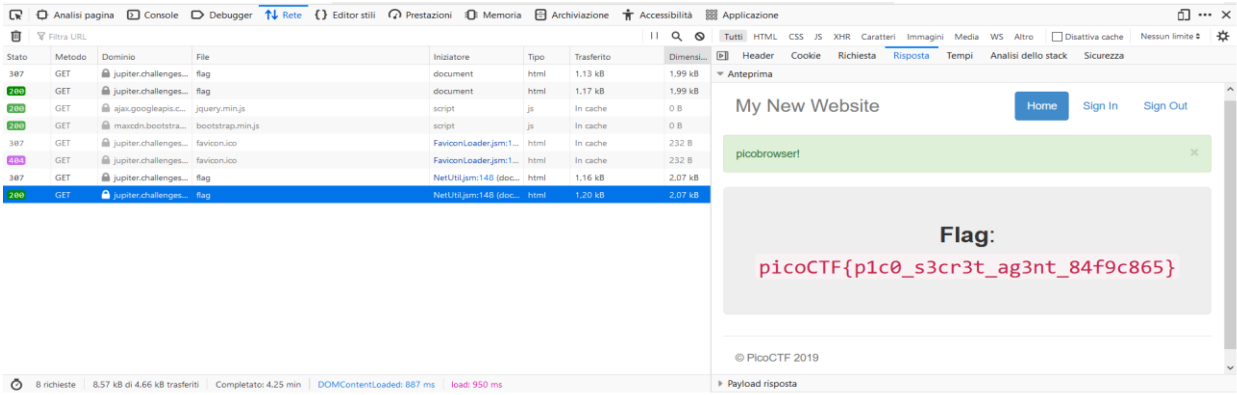
Metodo: GET

URL: https://jupiter.challenges.picoctf.org/flag

Header della richiesta:

```
Host: jupiter.challenges.picoctf.org
User-Agent: picobrowser
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: https://jupiter.challenges.picoctf.org/problem/28921/
Upgrade-Insecure-Requests: 1
```

Figure 16: Change user agent with the right one



Stato	Metodo	Dominio	File	Iniziatore	Tipo	Trasferito	Dimensi...
307	GET	jupiter.challenges...	flag	document	html	1,13 kB	1,99 kB
200	GET	jupiter.challenges...	flag	document	html	1,17 kB	1,99 kB
200	GET	ajax.googleapis.c...	jquery.min.js	script	js	In cache	0 B
200	GET	maxcdn.bootstra...	bootstrap.min.js	script	js	In cache	0 B
307	GET	jupiter.challenges...	favicon.ico	FaviconLoader.jsm:1...	html	In cache	232 B
404	GET	jupiter.challenges...	favicon.ico	FaviconLoader.jsm:1...	html	In cache	232 B
307	GET	jupiter.challenges...	flag	NetUtil.jsm:148 (doc...	html	1,16 kB	2,07 kB
200	GET	jupiter.challenges...	flag	NetUtil.jsm:148 (doc...	html	1,20 kB	2,07 kB

8 richieste | 8,57 kB di 4,66 kB trasferiti | Completato: 4,25 min | DOMContentLoaded: 887 ms | load: 950 ms

My New Website — Home | Sign In | Sign Out

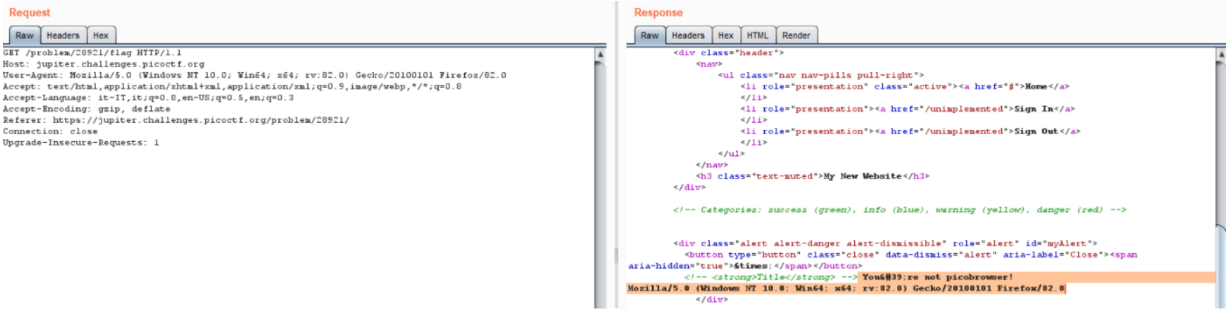
picobrowser!

Flag:

picoCTF{p1c0_s3cr3t_ag3nt_84f9c865}

© PicoCTF 2019

Figure 17: see the response, flag found



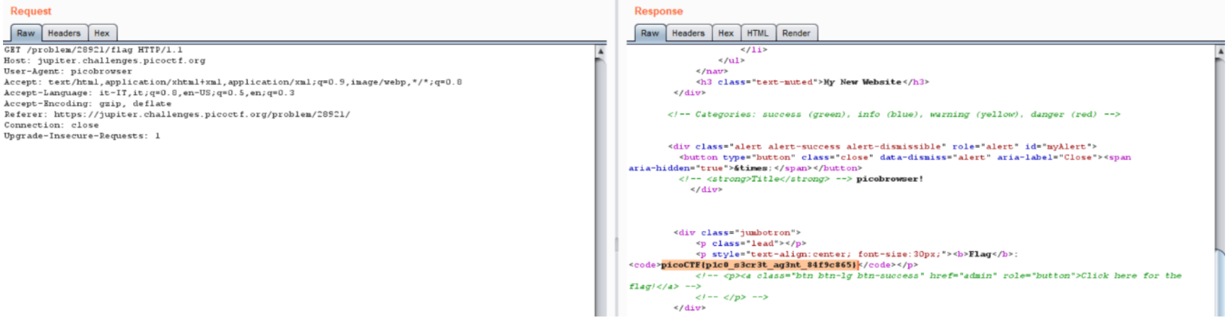
```
GET /problem/28921/flag HTTP/1.1
Host: jupiter.challenges.picoctf.org
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://jupiter.challenges.picoctf.org/problem/28921/
Connection: close
Upgrade-Insecure-Requests: 1
```

```
        <div class="header">
            <nav>
                <ul class="nav nav-pills pull-right">
                    <li role="presentation" class="active"><a href="#">Home</a>
                    </li>
                    <li role="presentation"><a href="/unimplemented">Sign In</a>
                    </li>
                    <li role="presentation"><a href="/unimplemented">Sign Out</a>
                    </li>
                </ul>
            </nav>
            <h3 class="text-muted">My New Website</h3>
        </div>

        <!-- Categories: success (green), info (blue), warning (yellow), danger (red) -->


        <div class="alert alert-danger alert-dismissible" role="alert" id="myAlert">
          <button type="button" class="close" data-dismiss="alert" aria-label="Close"><span
aria-hidden="true">&times;</span></button>
          <!-- <strong>Title</strong> --> You&#39;re not picobrowser!
Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
            </div>
```

Figure 18: Original request and response seen from Burp



```
GET /problem/28921/flag HTTP/1.1
Host: jupiter.challenges.picoctf.org
User-Agent: picobrowser
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://jupiter.challenges.picoctf.org/problem/28921/
Connection: close
Upgrade-Insecure-Requests: 1
```

```
                    </li>
                </ul>
            </nav>
            <h3 class="text-muted">My New Website</h3>
        </div>

       <!-- Categories: success (green), info (blue), warning (yellow), danger (red) -->


       <div class="alert alert-success alert-dismissible" role="alert" id="myAlert">
         <button type="button" class="close" data-dismiss="alert" aria-label="Close"><span
aria-hidden="true">&times;</span></button>
         <!-- <strong>Title</strong> --> picobrowser!
           </div>



        <div class="jumbotron">
            <p class="lead"></p>
            <p style="text-align:center; font-size:30px;"><b>Flag</b>:
<code>picoCTF{p1c0_s3cr3t_ag3nt_84f9c865}</code></p>
            <!-- <p><a class="btn btn-lg btn-success" href="admin" role="button">Click here for the
flag!</a> -->
            <!-- </p> -->
        </div>
```

Figure 19: Change User-Agent with Burp's Repeater