Description

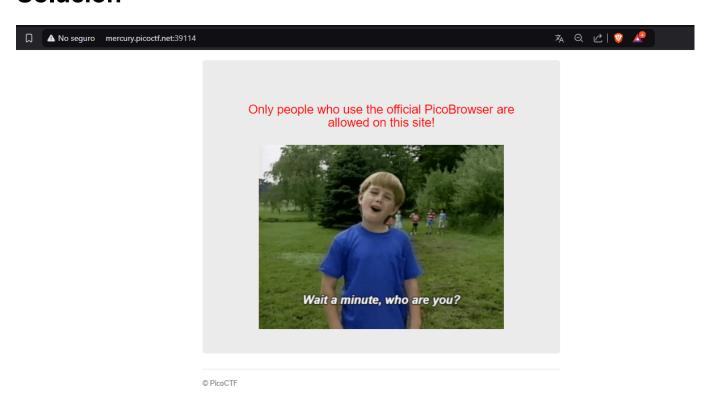Let me in. Let me iiiiiiinnnnnnnnnnnnnnnnnnnnnn http://mercury.picoctf.net:39114/

Hints

- It ain't much, but it's an RFC https://tools.ietf.org/html/rfc2616

Solución


```
  ┌──(kali㉿kali)-[~/…/parciales/parcial_02/parte_02_web_02/who_ru]
  └─$ wget http://mercury.picoctf.net:39114/ --header='Referer:
  http://mercury.picoctf.net:39114/' --header='Date: 2018' --header="DNT: dnt"
  --2024-11-04 01:48:35--  http://mercury.picoctf.net:39114/
  Resolving mercury.picoctf.net (mercury.picoctf.net)... 18.189.209.142
  Connecting to mercury.picoctf.net
  (mercury.picoctf.net)|18.189.209.142|:39114... connected.
  HTTP request sent, awaiting response... 200 OK
  Length: 1073 (1.0K) [text/html]
  Saving to: 'index.html.2'

  index.html.2              100%[===========================>]   1.05K  --.-KB/s
  in 0s
```

```
2024-11-04 01:48:35 (35.6 MB/s) - 'index.html.2' saved [1073/1073]


┌──(kali㉿kali)-[~/…/parciales/parcial_02/parte_02_web_02/who_ru]
└─$ nano index.html.2


┌──(kali㉿kali)-[~/…/parciales/parcial_02/parte_02_web_02/who_ru]
└─$ vi index.html.2


┌──(kali㉿kali)-[~/…/parciales/parcial_02/parte_02_web_02/who_ru]
└─$ wget http://mercury.picoctf.net:39114/ -U PicoBrowser --header='Referer:
http://mercury.picoctf.net:39114/' --header='Date: 2018' --header="DNT: dnt"
--2024-11-04 01:50:47--  http://mercury.picoctf.net:39114/
Resolving mercury.picoctf.net (mercury.picoctf.net)... 18.189.209.142
Connecting to mercury.picoctf.net
(mercury.picoctf.net)|18.189.209.142|:39114... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1047 (1.0K) [text/html]
Saving to: 'index.html.3'

index.html.3          100%[===========================>]   1.02K  --.-KB/s
in 0s

2024-11-04 01:50:47 (33.4 MB/s) - 'index.html.3' saved [1047/1047]


┌──(kali㉿kali)-[~/…/parciales/parcial_02/parte_02_web_02/who_ru]
└─$ vi index.html.3


┌──(kali㉿kali)-[~/…/parciales/parcial_02/parte_02_web_02/who_ru]
└─$ wget http://mercury.picoctf.net:39114/ -U PicoBrowser --header='Referer:
http://mercury.picoctf.net:39114/' --header='Date: 2018' --header="DNT: dnt"
--header="X-Forwarded-For: 88.80.28.16"
--2024-11-04 01:52:10--  http://mercury.picoctf.net:39114/
Resolving mercury.picoctf.net (mercury.picoctf.net)... 18.189.209.142
Connecting to mercury.picoctf.net
(mercury.picoctf.net)|18.189.209.142|:39114... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1056 (1.0K) [text/html]
Saving to: 'index.html.4'

index.html.4          100%[===========================>]   1.03K  --.-KB/s
in 0s

2024-11-04 01:52:11 (35.7 MB/s) - 'index.html.4' saved [1056/1056]
```

```
┌──(kali㉿kali)-[~/…/parciales/parcial_02/parte_02_web_02/who_ru]
└─$ cat index.html.4
<!DOCTYPE html>
<html lang="en">

<head>
    <title>Who are you?</title>


    <link
href="https://maxcdn.bootstrapcdn.com/bootstrap/3.2.0/css/bootstrap.min.css"
rel="stylesheet">

    <link href="https://getbootstrap.com/docs/3.3/examples/jumbotron-
narrow/jumbotron-narrow.css" rel="stylesheet">

    <script
src="https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js">
</script>

    <script
src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js">
</script>


</head>

<body>

    <div class="container">
      <div class="jumbotron">
        <p class="lead"></p>
                <div class="row">
                        <div class="col-xs-12 col-sm-12 col-md-12">
                            <h3 style="color:red">You&#39;re in Sweden
but you don&#39;t speak Swedish?</h3>
                        </div>
                </div>
                <br/>

                        <img src="/static/who_r_u.gif"></img>

        </div>
    <footer class="footer">
```

```
            <p>&copy; PicoCTF</p>
    </footer>

</div>
<script>
$(document).ready(function(){
    $(".close").click(function(){
        $("myAlert").alert("close");
    });
});
</script>
</body>

</html>
```
┌──(kali㉿kali)-[~/…/parciales/parcial_02/parte_02_web_02/who_ru]
└─$ wget http://mercury.picoctf.net:39114/ -U PicoBrowser --header='Referer: http://mercury.picoctf.net:39114/' --header='Date: 2018' --header="DNT: dnt" --header="X-Forwarded-For: 88.80.28.16" --header="Accept-language: sv"
--2024-11-04 01:54:24-- http://mercury.picoctf.net:39114/
Resolving mercury.picoctf.net (mercury.picoctf.net)... 18.189.209.142
Connecting to mercury.picoctf.net (mercury.picoctf.net)|18.189.209.142|:39114... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1062 (1.0K) [text/html]
Saving to: 'index.html.5'

index.html.5   100%[===========================>]   1.04K --.-KB/s   in 0s

2024-11-04 01:54:24 (32.3 MB/s) - 'index.html.5' saved [1062/1062]

┌──(kali㉿kali)-[~/…/parciales/parcial_02/parte_02_web_02/who_ru]
└─$ cat index.html.5
<!DOCTYPE html>
<html lang="en">

<head>
    <title>Who are you?</title>

    <link href="https://maxcdn.bootstrapcdn.com/bootstrap/3.2.0/css/bootstrap.min.css" rel="stylesheet">

    <link href="https://getbootstrap.com/docs/3.3/examples/jumbotron-
```

```html
narrow/jumbotron-narrow.css" rel="stylesheet">

    <script
src="https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js">
</script>

    <script
src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js">
</script>


</head>

<body>

    <div class="container">
      <div class="jumbotron">
        <p class="lead"></p>
                <div class="row">
                        <div class="col-xs-12 col-sm-12 col-md-12">
                                <h3 style="color:green">What can I say
except, you are welcome</h3>
                        </div>
                </div>
                <br/>

                        <b>picoCTF{http_h34d3rs_v3ry_c00l_much_w0w_20ace0e4}
</b>

        </div>
    <footer class="footer">
        <p>&copy; PicoCTF</p>
    </footer>

</div>
<script>
$(document).ready(function(){
    $(".close").click(function(){
        $("myAlert").alert("close");
    });
});
</script>
</body>

</html>
```

Bandera

```
flag: picoCTF{http_h34d3rs_v3ry_c00l_much_w0w_20ace0e4}
```

Notas Adicionales

Referencias

-