Ruben van Vreeland

Founder of BITsaver Web Application Security

Ruben van Vreeland

INDIEGOGO

YOUR CAMPAIGN

DRAFT This campaign is not yet live. Don't t campaign)

BITsa d XSS

ogy

Story | Updates 0 | Comments 0 | Fund

$0 USD
raised by **0 people** in less than a minute

0% funded

$500 USD goal

Do you think this campaign contains prohibited content? Let us know.

BITsaver Advanced XSS. We are a web application security company. Visit us at http://bitsaver.nl/

Fixed

CONTINUE WITH FACEBOOK

No automatic posts, ever.

Or log in with email

ruv

Remember Me Forgot Password?

LOG IN

New to Indiegogo? Sign up

Topics

- Typical XSS vectors
- Hijacking with style and class

Attacker executes script in the victims browser, in the context (origin) of the vulnerable application, to attack the user

Common XSS vectors

Unsanitized HTML

<script>payload</script>

Unescaped attribute

<script>payload</script><a “” />

Unsanitized attribute content

<a href=“javascript:payload” />

Unsanitized/Wrongly encoded script

Var a = b; Payload;

Unsanitized Style (IE 8 and below only)

Whitelisting Case

<a href="*">

<* width="*" height="*" class="*" />

You have found your vulnerability

```
<a href="javascript:alert(/Exploit me!/)">
    javascript:alert(/Exploit me!/)
</a>
```

javascript:alert(/Exploit me!/)

Exploiting with style

```
<a href="javascript:payload"
    style= "background: rgba(255, 0, 0, 0.5);
            position: fixed;
            left: 0px; top: 0px;
            width: 100%; height: 100%; " >
</a>
```

http://output.jsbin.com/cipozanute/1/

But, wait

<a href="*">

<* width="*" height="*" class="*" />

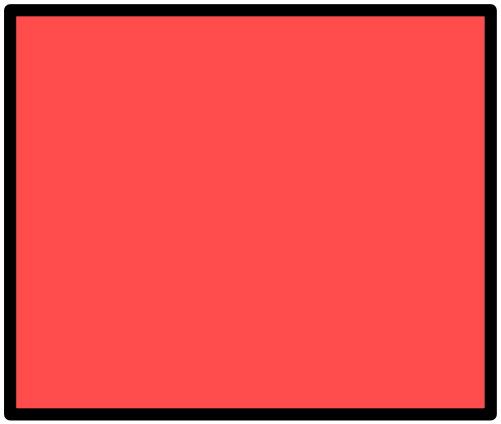
Defined

```
3663 .dropdown-backdrop {
3664   position: fixed;
3665   top: 0;
3666   right: 0;
3667   bottom: 0;
3668   left: 0;
3669   z-index: 990;
3670 }
```

```
4299 .navbar-fixed-top,
4300 .navbar-fixed-bottom {
4301   position: fixed;
4302   right: 0;
4303   left: 0;
4304   z-index: 1030;
4305 }
```

Exploiting with style

```
<a
   width="100%"
   height="100%"
   href="javascript:payload"
   class="dropdown-backdrop navbar-fixed-top">
</a>
```



http://output.jsbin.com/zoqipeloca/1/

Embeddable content

Embed.ly

OEmbed proxy

300+ content providers

https://jsfiddle.net/bitsaver/b3nwskp0/1/

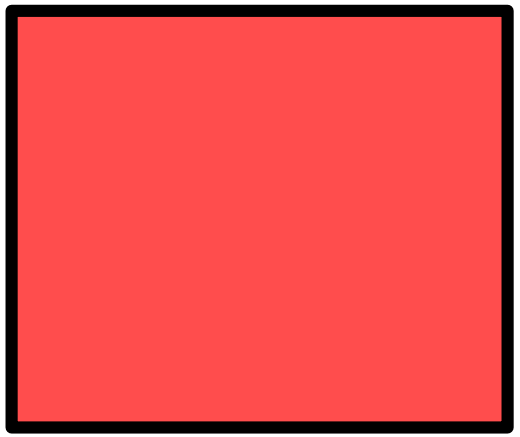
BITsaver

Embed.ly case

<iframe href="https://api.embed.ly/*">
<* width="*" height="*" class="*" />

Exploiting with style

```
<iframe
   width="100%"
   height="100%"
   src="api.embed.ly/*"
   class="dropdown-backdrop navbar-fixed-top">
</iframe>
```



http://output.jsbin.com/mupegoxahu/1/

Whitelisting Case

<form action="*">

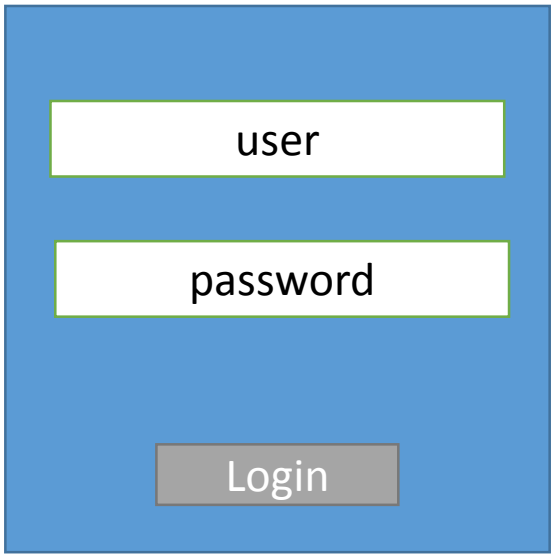
<input type="*"> <button type="*">

<* class="*" id="*">

Hijack login

Using class attribute

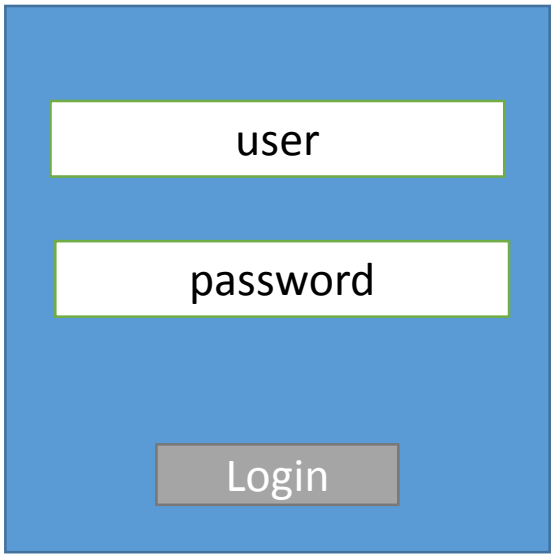
Recreate pixel-perfect clone



http://jsbin.com/dejite/13/edit

Abuse Password Manager

- Prefill
  - Same origin
- *form action* classic JavaScript payload



http://jsbin.com/dejite/13/edit

To conclude

- id, class
- style
- oembed/embed.ly

Disclose responsibly!

Questions?

Happy hacking!