When the Web Goes to Jail

David Runge

2019-08-10

Contents

Who?

- Trusted User (2017)/ Developer (2019)
- Pro-audio, Python tools, web apps
- Documentation

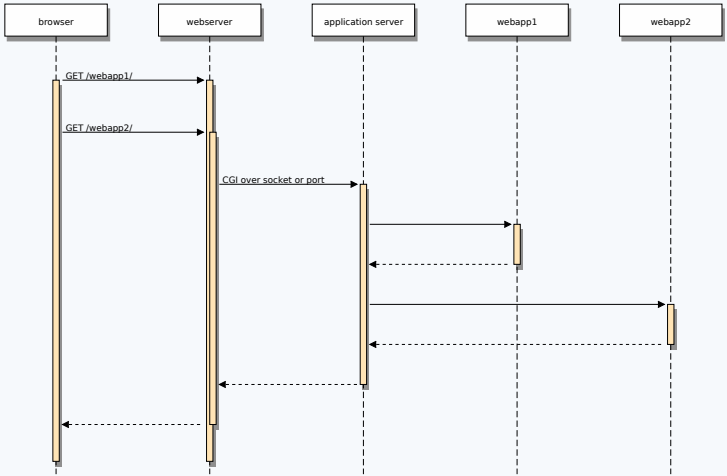
What?

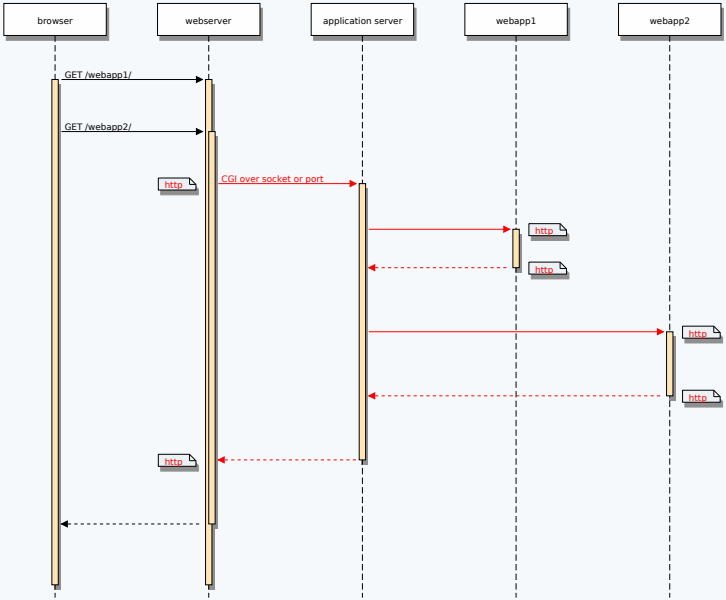
- Packaged web applications
- Use-case: One or more web applications on single host
- Interplay: Web servers, application servers, web applications
- Security and best practices
- Distribution agnostic
- WIP

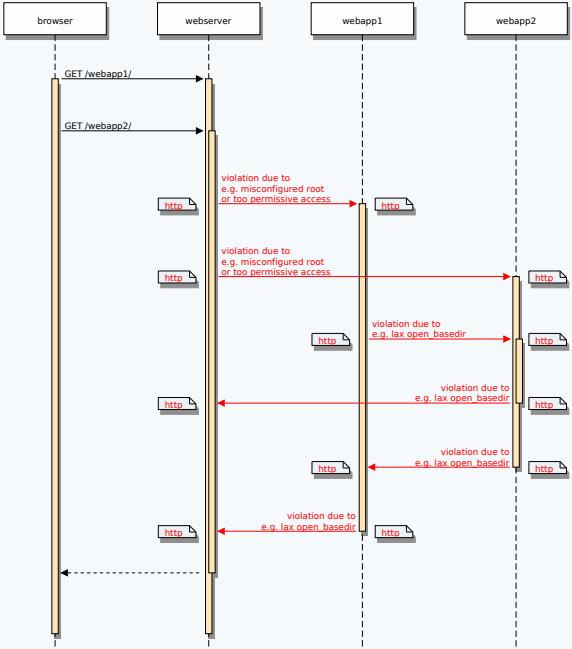
The Good Old Days

Creating users ~~is~~ was hard

- Propagating UID/GID pair necessary
- Using install file is error-prone
- Some permissions can be set in PKGBUILD
- Changing user/group non-trivial
- Manual chown/chmod after install
- */run* not packagable


browser
webserver
application server
webapp1
webapp2
GET /webapp1/
GET /webapp2/
CGI over socket or port

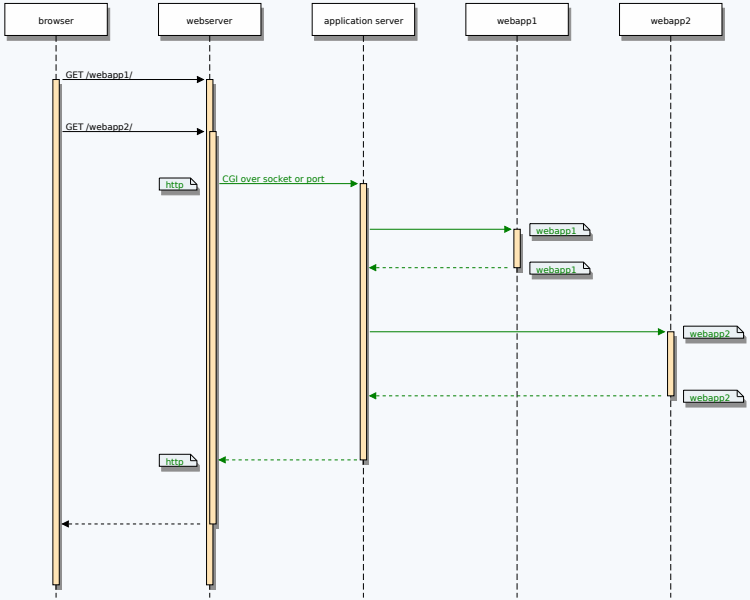

browser
webserver
application server
webapp1
webapp2
GET /webapp1/
GET /webapp2/
http
CGI over socket or port
http
http
http
http
http

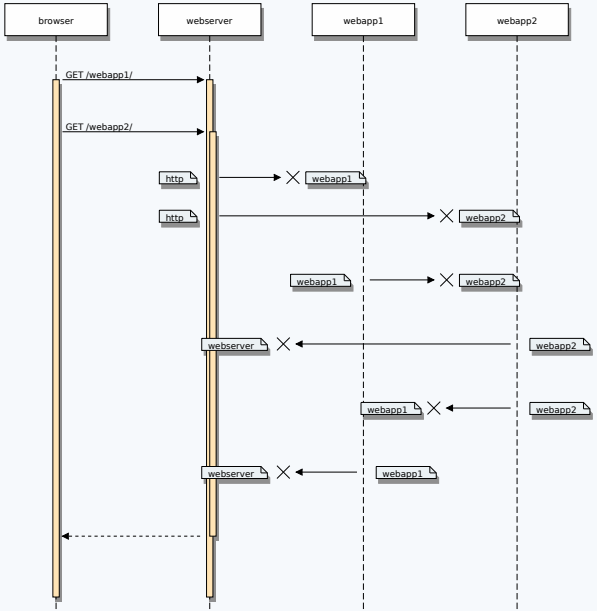

browser
webserver
webapp1
webapp2
GET /webapp1/
GET /webapp2/
violation due to
e.g. misconfigured root
or too permissive access
http
http
violation due to
e.g. misconfigured root
or too permissive access
http
http
violation due to
e.g. lax open_basedir
http
http
violation due to
e.g. lax open_basedir
http
http
violation due to
e.g. lax open_basedir
http
http
violation due to
e.g. lax open_basedir
http
http

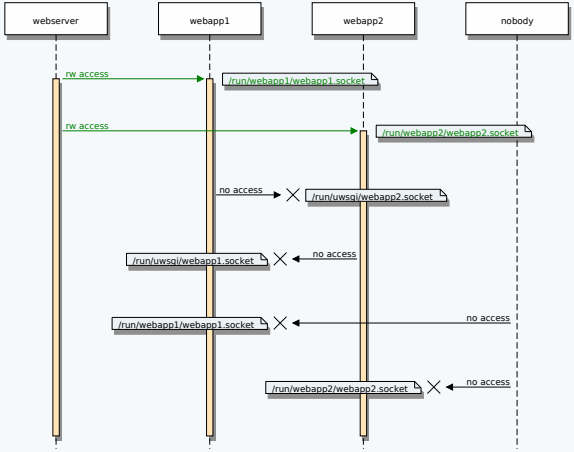

webserver
webapp1
webapp2
nobody
rw access
/run/uwsgi/webapp1.socket
rw access
/run/uwsgi/webapp2.socket
rw access
/run/uwsgi/webapp2.socket
rw access
/run/uwsgi/webapp1.socket
/run/uwsgi/webapp1.socket
rw access
/run/uwsgi/webapp2.socket
rw access

Where We Want to Be

- Stop using the **http** user for everyhing
- A user per web application
- Allow write access to local sockets only to web server (and root)
- Dissallow read access for everybody else


browser
webserver
application server
webapp1
webapp2
GET /webapp1/
GET /webapp2/
http
CGI over socket or port
webapp1
webapp1
webapp2
webapp2
http


browser
webserver
webapp1
webapp2
GET /webapp1/
GET /webapp2/
http
webapp1
http
webapp2
webapp1
webapp2
webserver
webapp2
webapp1
webapp2
webserver
webapp1


webserver
webapp1
webapp2
nobody
rw access
/run/webapp1/webapp1.socket
rw access
/run/webapp2/webapp2.socket
no access
/run/uwsgi/webapp2.socket
/run/uwsgi/webapp1.socket
no access
/run/webapp1/webapp1.socket
no access
/run/webapp2/webapp2.socket
no access

How We Get There

Packaging

- Ship users and groups[1]

```
man 5 sysusers.d
```

- Ship ownership and permissions, create files and directories (e.g. below */run*)[2]

```
man 5 tmpfiles.d
```

- DynamicUser, hardening[3] (e.g. uwsgi[4])

```
man 5 systemd.exec
```

- Generic permissions/ settings for sockets[5] (e.g. uwsgi[6])

```
man 5 systemd.socket
```

- Improve application server packaging (e.g. uwsgi's sockets and services are too permissive)
- Snippets, defaults (e.g. nginx, apache, uwsgi, php-fpm)

[1] https://www.freedesktop.org/software/systemd/man/sysusers.d.html
[2] https://www.freedesktop.org/software/systemd/man/tmpfiles.d.html
[3] https://www.freedesktop.org/software/systemd/man/systemd.exec.html
[4] https://wiki.archlinux.org/index.php/UWSGI#Hardening_uWSGI_service
[5] https://www.freedesktop.org/software/systemd/man/systemd.socket.html
[6] https://wiki.archlinux.org/index.php/UWSGI#Accessibility_of_uWSGI_socket

Fixing upstreams

- PHP calling PHP and not honoring configuration (e.g. cacti)
- Web applications with write-tentacles all over the filesystems (e.g. librenms)

Documentation

- ~~Update packaging guidelines for webapps~~[7]
- Extend information on (best practices for) php-fpm (there's no dedicated wiki page)
- Extend information on (best practices for) uwsgi[8]
- Revise wiki pages for webapps, removing bizarre suggestions (e.g. *"just let **http** own all files"*), pointing to php-fpm/ uwsgi

[7] https://wiki.archlinux.org/index.php/Web_application_package_guidelines
[8] https://wiki.archlinux.org/index.php/UWSGI

Where We Are

- Lots of legacy/ redundancy - room for improvement
- Scattered information (or information in the wrong places)
- Example web apps: cacti[9], librenms[10], mantisbt[11], postfixadmin[12]
- Time for a TODO[13] to fix all of them

[9] https://www.archlinux.org/packages/community/any/cacti/
[10] https://aur.archlinux.org/packages/librenms/
[11] https://aur.archlinux.org/packages/mantisbt/
[12] https://www.archlinux.org/packages/community/any/postfixadmin/
[13] https://www.archlinux.org/todo/

Contact

David Runge

Mail: dave@sleepmap.de

XMPP: dvzrv@sleepmap.de

IRC: dvzrv@{freenode,hackint,oftc}