Matomo Security hardening

Common mistakes, from bare-metal to Docker

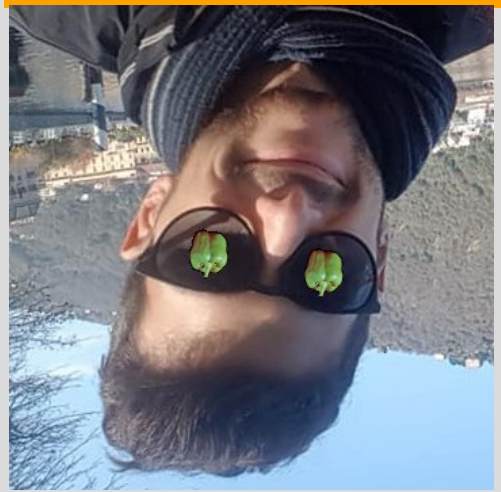
by Valerio Bozzolan

It’s me! Valerio (boz)

boz@reyboz.it

- **Italian Linux Society** board director

- IT consultant for Wikimedia Switzerland
- Volunteer sysadmin in Wikimedia Italy
- Member of
  - Free Software Foundation
  - Free Software Foundation Europe
  - Border Radio
  - InformAzioni.wiki + WMI



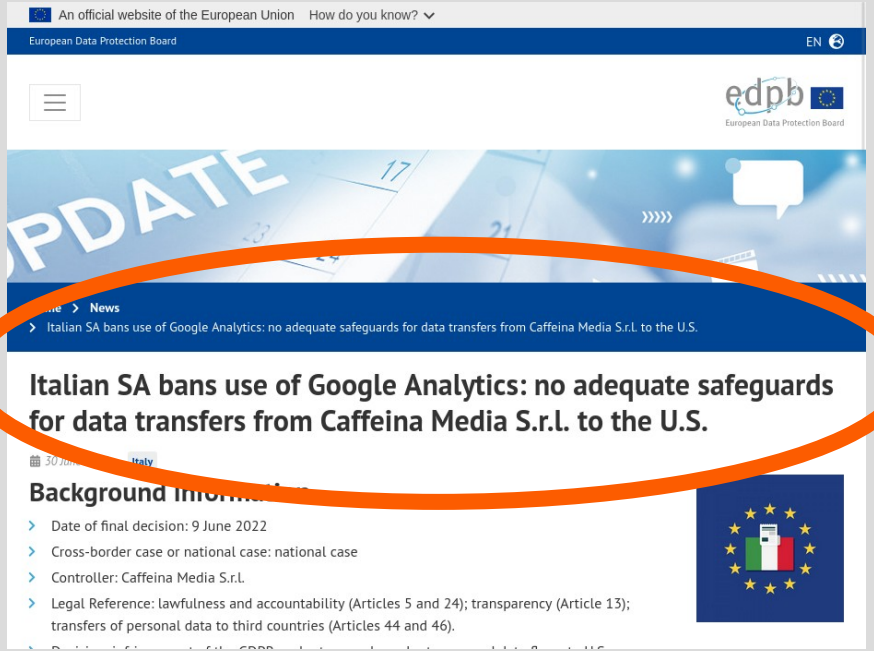
Again…

I'm not Illuminati / investor in Matomo / etc.

I just love **software freedom**, privacy and **data protection** <3

Why I’m here

Some legal+local context



Italian Data Protection Authority:
Ban Google Analytics
June 2022

Some legal+local context

«an **IP address is a personal data**»

«would not be anonymised even if it were truncated – given **Google's capabilities to enrich such data**»

«Users' personal data was found to be **transferred to the U.S.**»

«**violation** of Chapter V of the GDPR»

«**Google … did not ensure an adequate level of protection** in the light of the guidance provided by the EDPB through its Recommendations No 1/2020 of 18 June 2021.»

– citation from EDPB.Europe.EU

(Legal local context)

«US-based governmental and **intelligence agencies** may indeed access the personal data being **transferred without the required safeguards**»

– citation from EDPB.Europe.EU

1. Don't be legally vulnerable

1. **Don't embed**: download locally
   (images, fonts, etc.)
   (e.g. download legally from OpenStreetMap)

2. **Adopt** Free/Libre Open Source client-side
   and server-side
   (e.g. Matomo)

matomo

Dashboard All

PIPPO BLOG | FROM 2022-05-24 TO 2022-06-22 | ALL VISITS | DASHBOARD | NEW UPDATE: MATOMO 4.10.1

- Dashboard
  - Dashboard
- Visitors
- Behaviour
- Acquisition
- Goals

Visits in Real-time

DATE	VISITS	ACTIONS
Last 24 hours	5	11
Last 30 minutes	0	0

Thursday, June 23, - 00:26:51 (16 min 4s)
Google

Actions:

Wednesday, June 22, - 23:46:38
Social network: Twitter

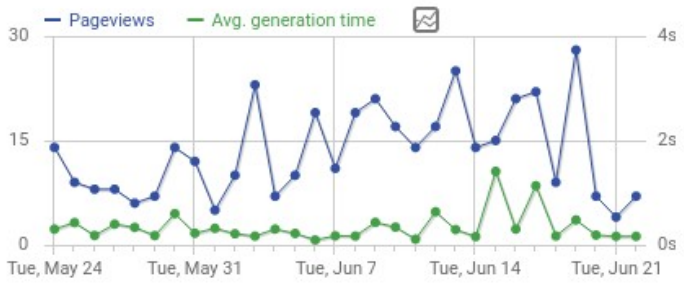
Actions:

Wednesday, June 22, - 21:42:15
Social network: Twitter

Actions:

Wednesday, June 22, - 16:57:28
Google

Visits Over Time



Search Engines

SEARCH ENGINE	VISITS
Google	109
Bing	14
DuckDuckGo	5
Yandex	5
Baidu	3

Visitor Map

Countries

Browsers

BROWSER
Chrome
Firefox
Chrome Mobile
Mobile Safari

Kerckhoffs's principle

Design your system assuming that your attackers know it.
I mean, in details.

+

KISS principle

Keep it simple and stupid.

Mitigation #1
Reduce attack surface

```
$ cd matomo
$ sloccount . | less

SLOC-by-Language (Sorted)


Totals grouped by language (dominant language first):
xml:          345092 (38.46%)
javascript:   280861 (31.30%)
Php:          271020 (30.21%)
perl:            149 (0.02%)
sh:               83 (0.01%)
```

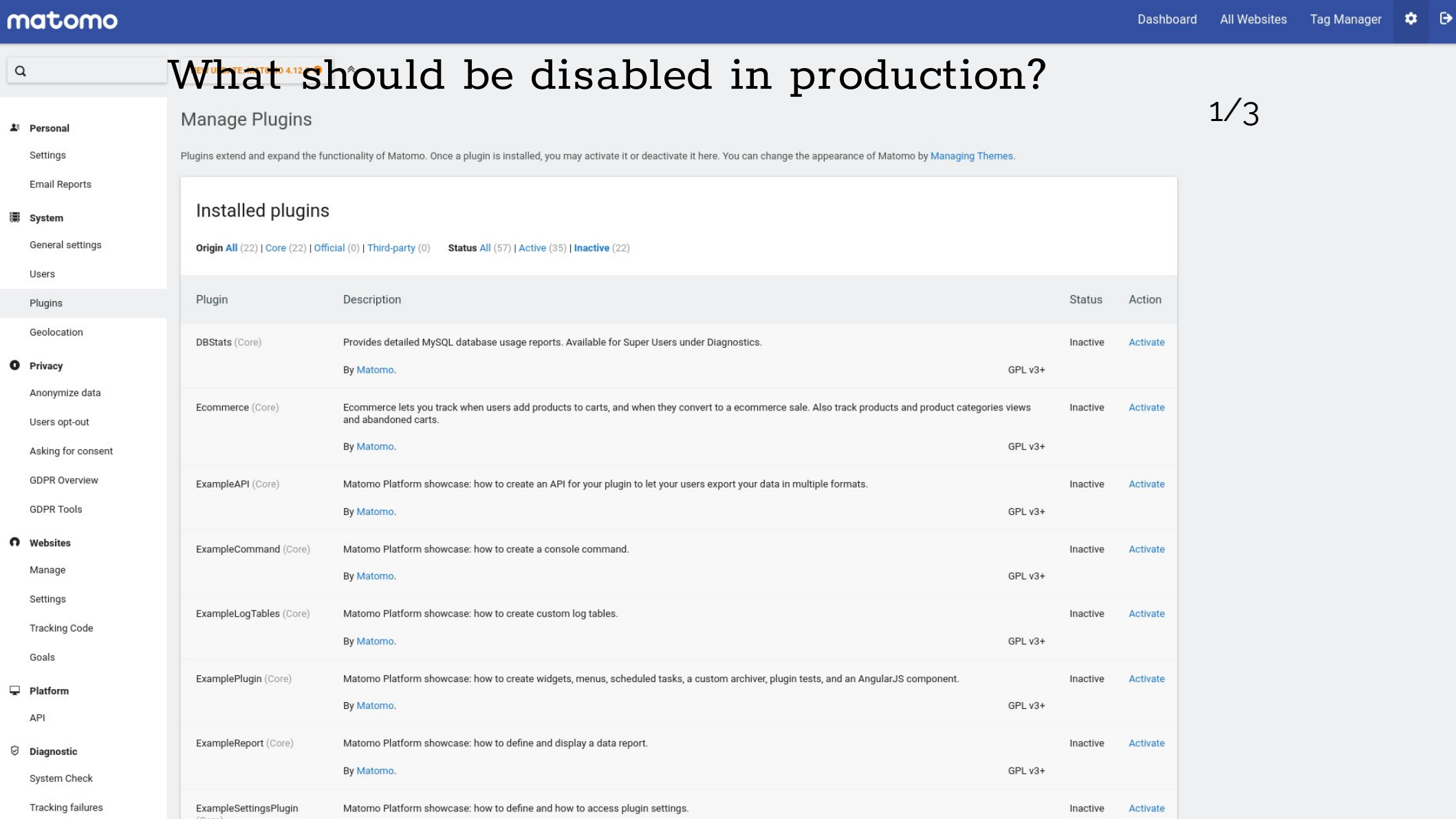
```
$ cd matomo
$ sloccount . | less

SLOC    Directory       SLOC-by-Language (Sorted)
385354  tests           xml=238705,javascript=88061,php=58402,perl=149,sh=37
292650  plugins         php=132529,xml=106184,javascript=53937
125240  node_modules    javascript=125240
61000   core            php=61000
27178   libs            php=18450,javascript=8707,sh=21
4693    js              javascript=4640,php=53
430     top_dir         javascript=276,php=115,xml=39
357     config          php=357
303     misc            xml=164,php=114,sh=25
0       lang            (none)
0       tmp             (none)
```

Reduce in-app attack surface

1. How many unused plugins do you have?

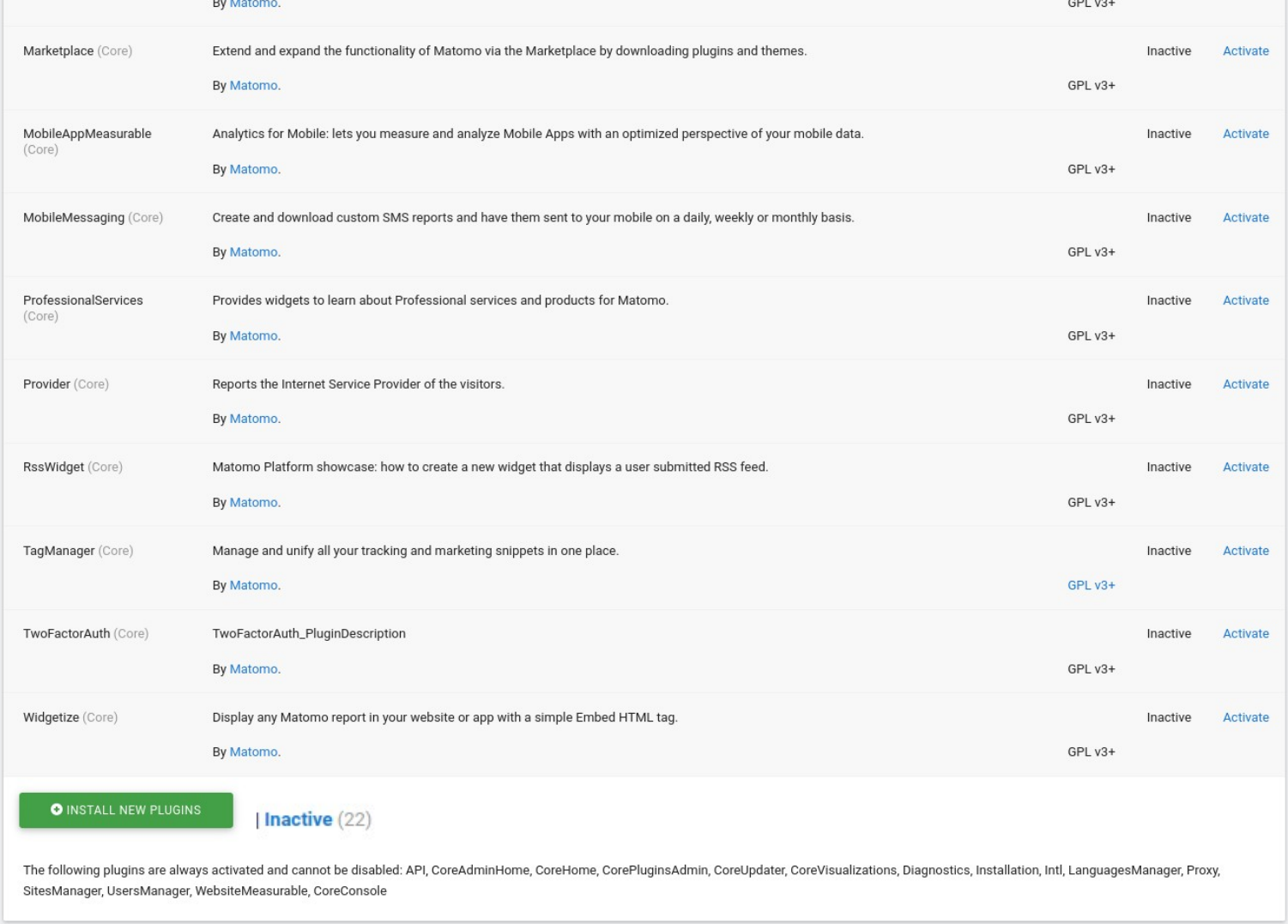
:monkey emoji don't see:

What should be disabled in production?



- Tracking failures
- Custom Variables
- Config file
- Brute Force Log
- Device detection

ExampleSettingsPlugin (Core)	Matomo Platform showcase: how to define and how to access plugin settings. By Matomo.	GPL v3+	Inactive	Activate
ExampleTracker (Core)	Matomo Platform showcase: how to track additional custom data creating new database table columns. By Matomo.	GPL v3+	Inactive	Activate
ExampleUI (Core)	Matomo Platform showcase: how to display data tables, graphs, and the UI framework. By Matomo.	GPL v3+	Inactive	Activate
ExampleVisualization (Core)	Matomo Platform showcase: how to create a new custom data visualization. By The Matomo Team.	GPL v3+	Inactive	Activate
Feedback (Core)	Send your Feedback to the Matomo Team. Share your ideas and suggestions to make Matomo the best analytics platform in the world! By Matomo.	GPL v3+	Inactive	Activate
IntranetMeasurable (Core)	Analytics for the web: lets you measure and analyze intranet websites. By Matomo.	GPL v3+	Inactive	Activate
Marketplace (Core)	Extend and expand the functionality of Matomo via the Marketplace by downloading plugins and themes. By Matomo.	GPL v3+	Inactive	Activate
MobileAppMeasurable (Core)	Analytics for Mobile: lets you measure and analyze Mobile Apps with an optimized perspective of your mobile data. By Matomo.	GPL v3+	Inactive	Activate
MobileMessaging (Core)	Create and download custom SMS reports and have them sent to your mobile on a daily, weekly or monthly basis. By Matomo.	GPL v3+	Inactive	Activate
ProfessionalServices (Core)	Provides widgets to learn about Professional services and products for Matomo. By Matomo.	GPL v3+	Inactive	Activate
Provider (Core)	Reports the Internet Service Provider of the visitors. By Matomo.	GPL v3+	Inactive	Activate
RssWidget (Core)	Matomo Platform showcase: how to create a new widget that displays a user submitted RSS feed. By Matomo.	GPL v3+	Inactive	Activate
TagManager (Core)	Manage and unify all your tracking and marketing snippets in one place.		Inactive	Activate



Assess **what** you are using, and **disable** what it's unused by you

«Yeah... I'm safe... I have 2FA..»

1. Any multi-factor authentication is **not** a good excuse not to keep your system as secure as possible.

2. **Forcing** 2FA on **every** user **may** not be a very good idea
→ think about social media managers without ITSec experience
→ think about additional potential malware on phone
→ think about additional exposure to social engineering

3. Train all your existing and new users **before enforcing**.

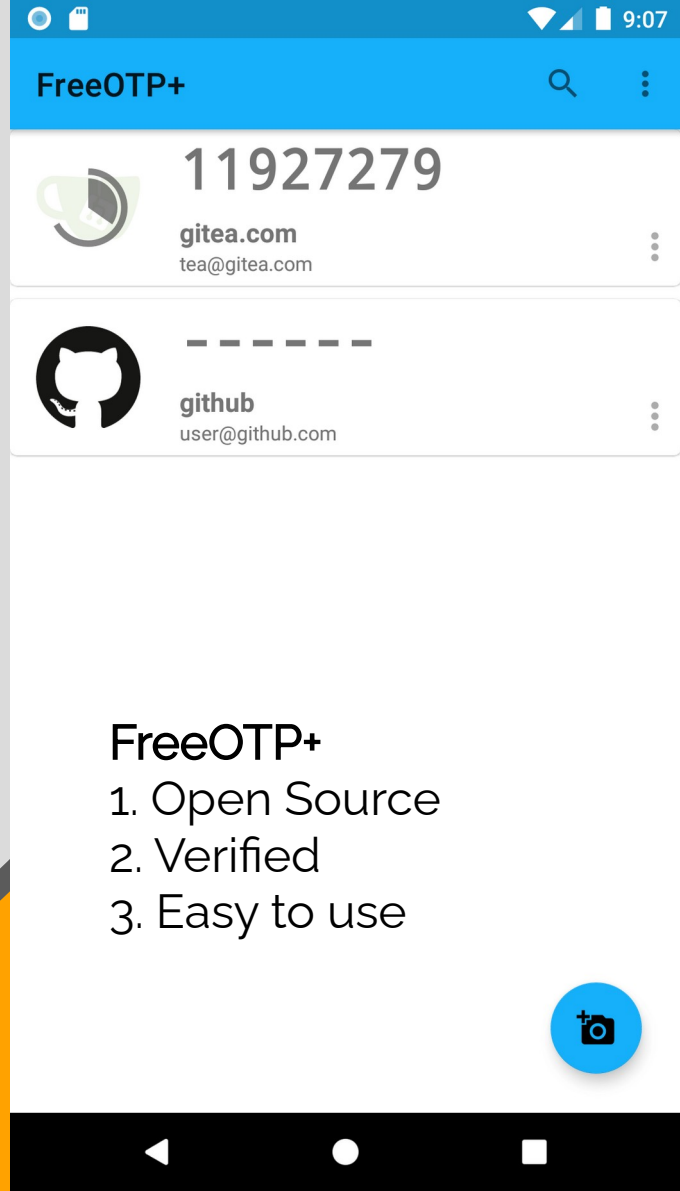
Do **your** evaluations.

FreeOTP+ from F-Droid

GET IT ON F-Droid

https://f-droid.org/en/packages/org.liberty.android.freeotpplus/

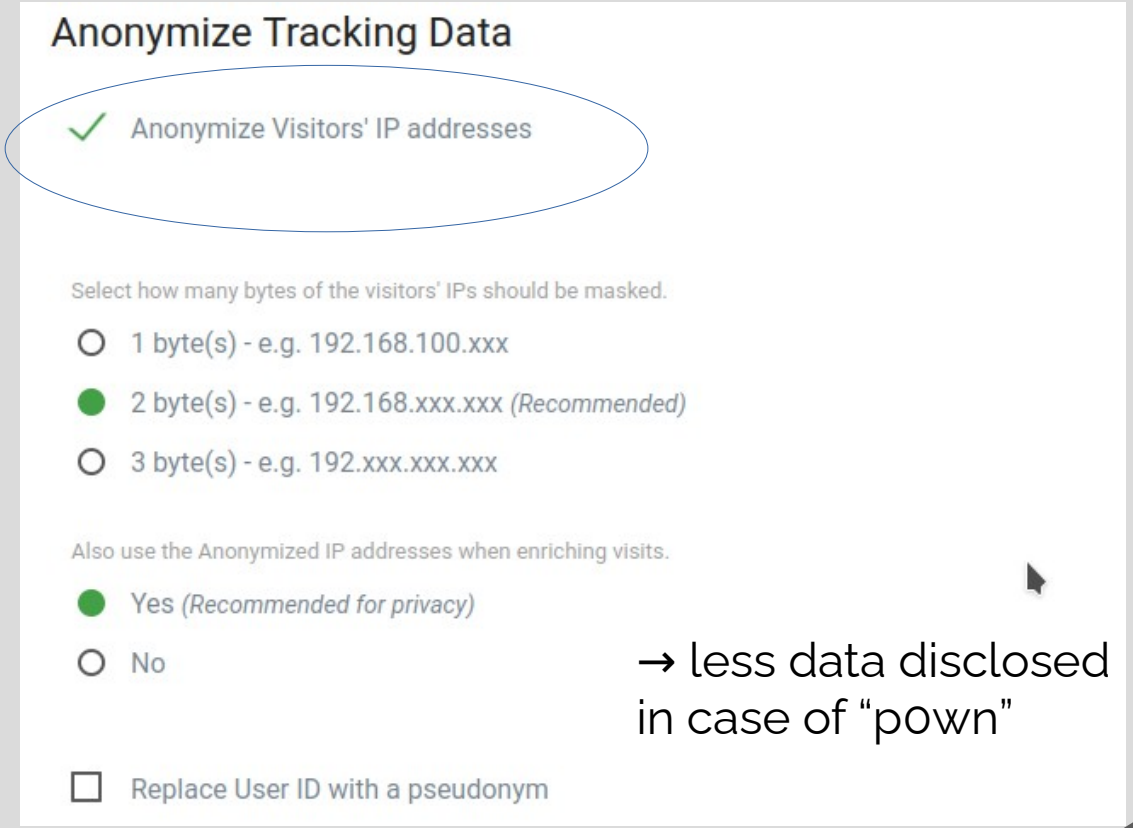
What is F-Droid?
Catalogue of FOSS (Free and Open Source Software) applications for the Android platform



FreeOTP+
1. Open Source
2. Verified
3. Easy to use

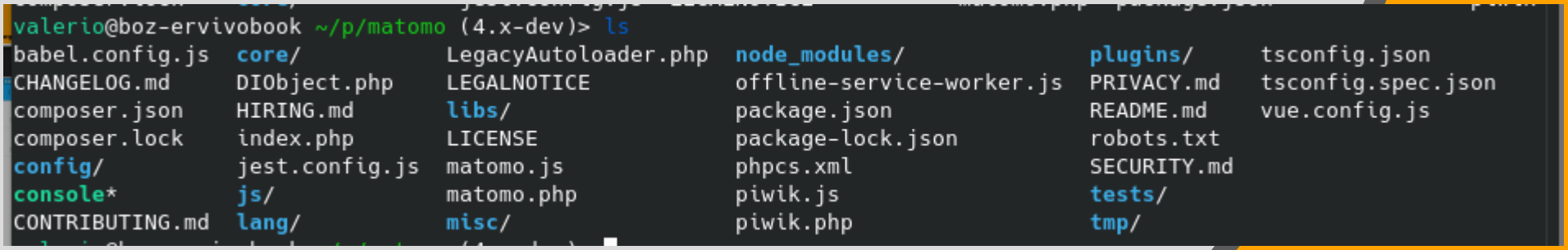
What if...
My Matomo is compromised

Reduce data you need to protect



→ less data disclosed in case of “pown”

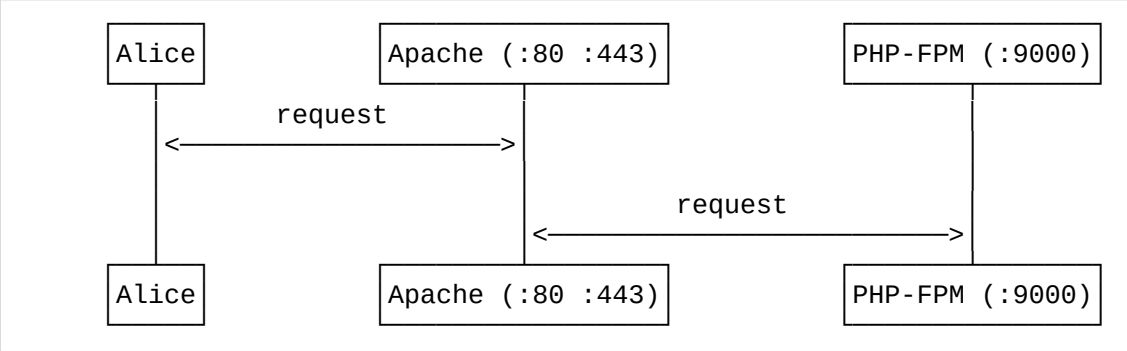
Matomo's project structure



For each file:
Who should its user be? What can the user do?
Who should its group be? What can the group do?
What can the others?

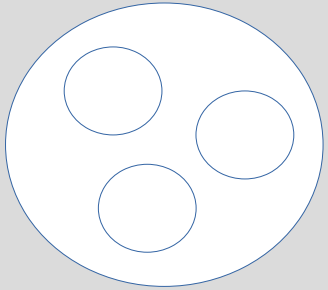
Matomo's webserver

PHP-FPM method

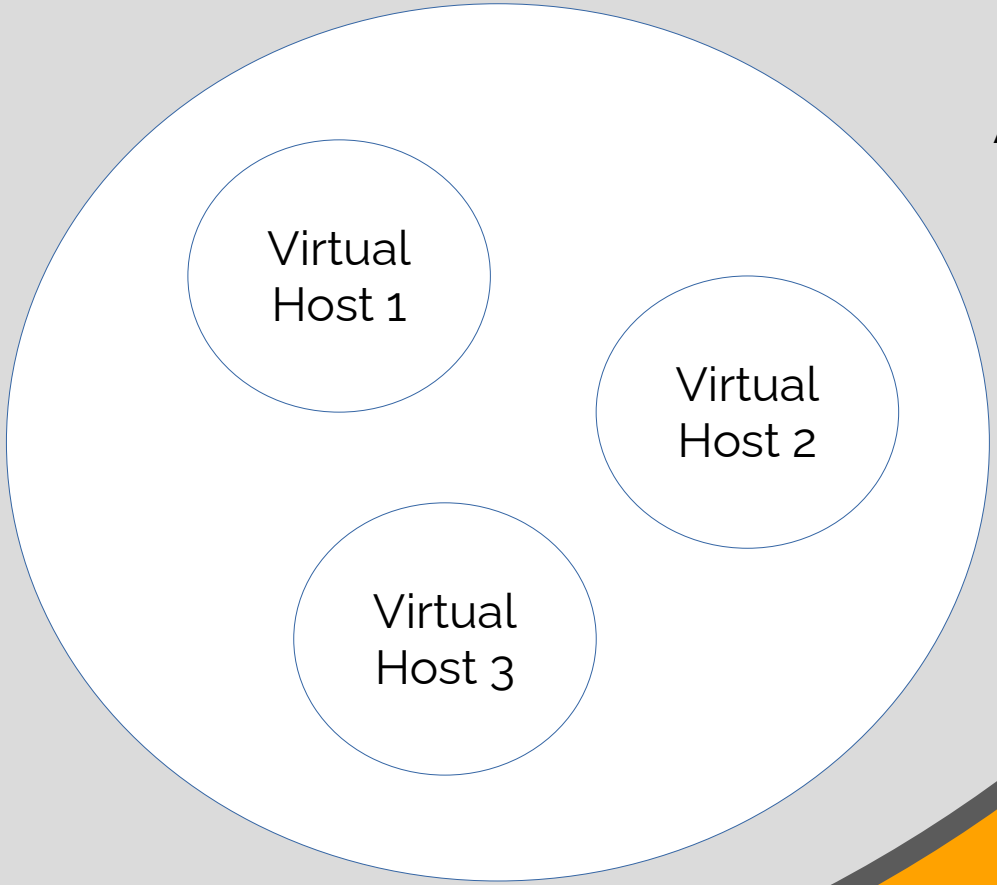


VS

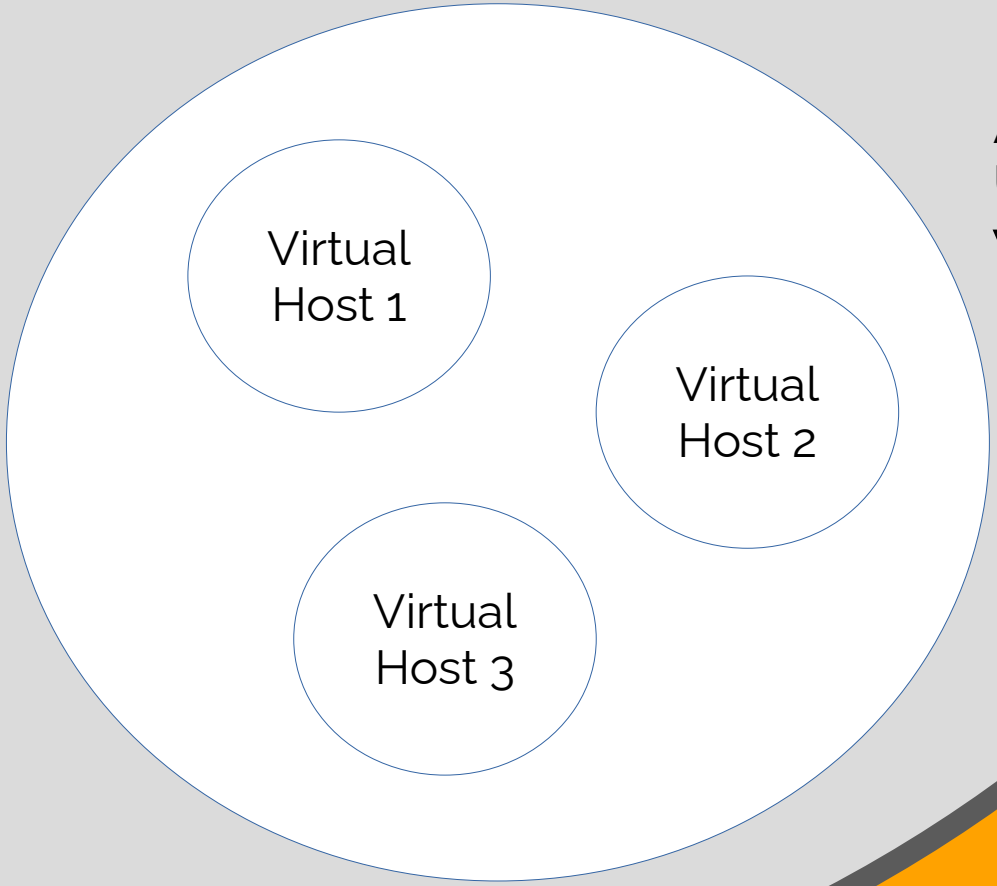
mod_php



Notes about mod_php

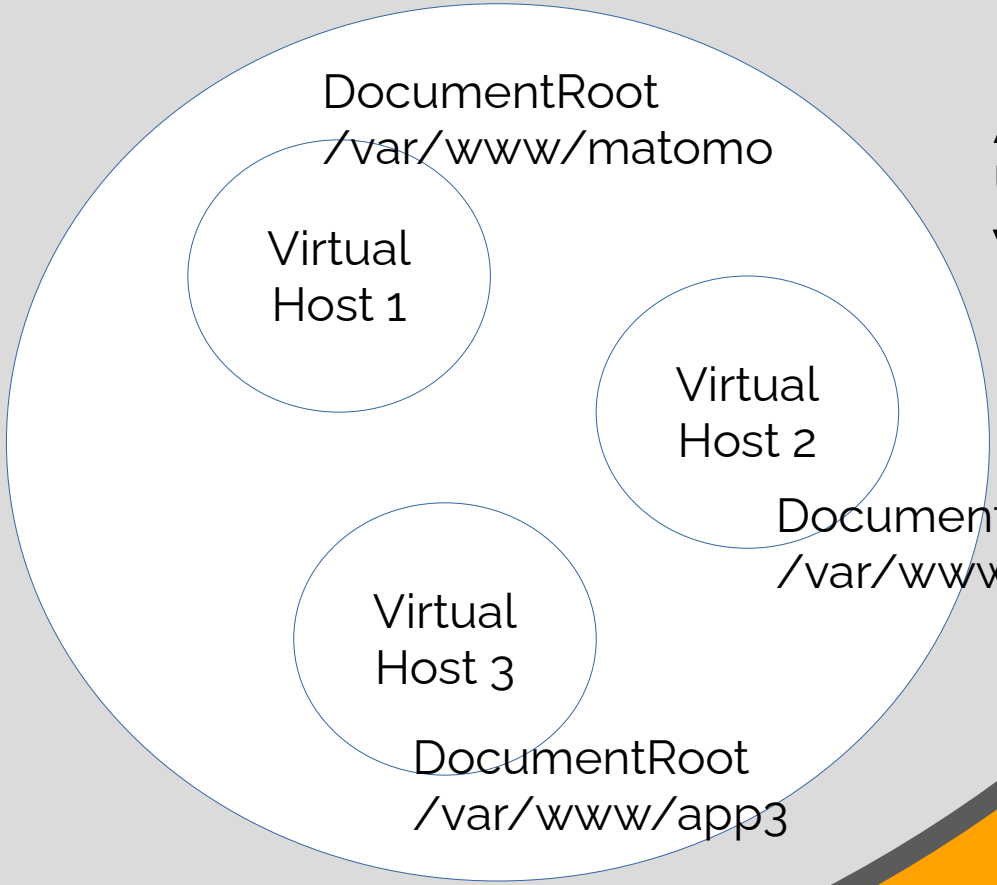


Notes about mod_php



Apache's
Unix user:
www-data

Notes about mod_php



Apache's
Unix user:
www-data

What if "app2 is
compromised?

« Yeah but I use open_basedir»

`open_basedir` string

Limit the files that can be accessed by PHP to the specified directory-tree, including the file itself. This directive is *NOT* affected by whether Safe Mode is turned On or Off.

When a script tries to access the filesystem, for example using include, or fopen(), the location of the file is checked. When the file is outside the specified directory-tree, PHP will refuse to access it. All symbolic links are resolved, so it's not possible to avoid this restriction with a symlink. If the file doesn't exist then the symlink couldn't be resolved and the filename is compared to (a resolved) **open_basedir**.

open_basedir can affect more than just filesystem functions; for example if `MySQL` is configured to use `mysqlnd` drivers, `LOAD DATA INFILE` will be affected by **open_basedir**. Much of the extended functionality of PHP uses `open_basedir` in this way.

The special value `.` indicates that the working directory of the script will be used as the base-directory. This is, however, a little dangerous as the working directory of the script can easily be changed with chdir().

https://www.php.net/manual/en/ini.core.php#ini.open-basedir

Common mistakes

« Yeah I use open_basedir»

```
<VirtualHost *:443>
    ServerName matomo.example.com
    DocumentRoot /var/www/matomo/www
    php_value date.timezone "Europe/Rome"
    php_value memory_limit 1024M
    php_admin_value open_basedir /var/www/matomo
```

What is it?

« Yeah but I use open_basedir»

`open_basedir` string

Limit the files that can be accessed by PHP to the specified directory-tree, including the file itself. This directive is *NOT* affected by whether Safe Mode is turned On or Off.

> **Caution** `open_basedir` is just an extra safety net, that is in no way comprehensive, and can therefore not be relied upon when security is needed.

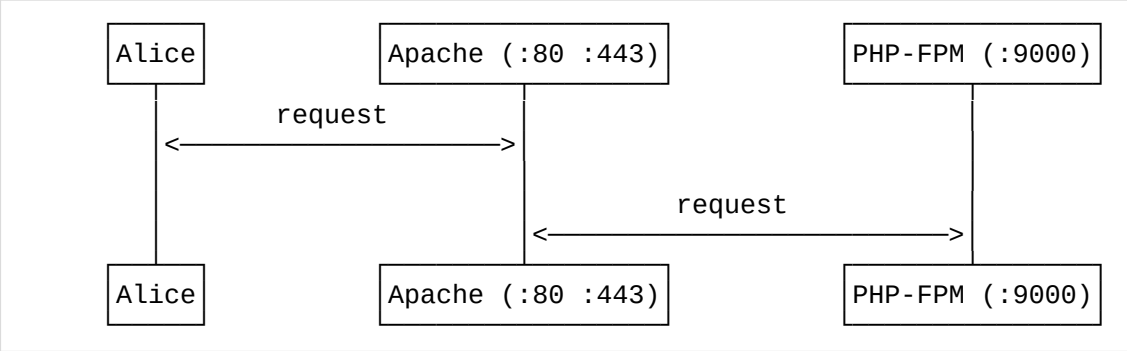
open_basedir can affect more than just filesystem functions; for example if `MySQL` is configured to use `mysqlnd` drivers, `LOAD DATA INFILE` will be affected by **open_basedir**. Much of the extended functionality of PHP uses `open_basedir` in this way.

The special value `.` indicates that the working directory of the script will be used as the base-directory. This is, however, a little dangerous as the working directory of the script can easily be changed with chdir().

https://www.php.net/manual/en/ini.core.php#ini.open-basedir

Notes about PHP-FPM

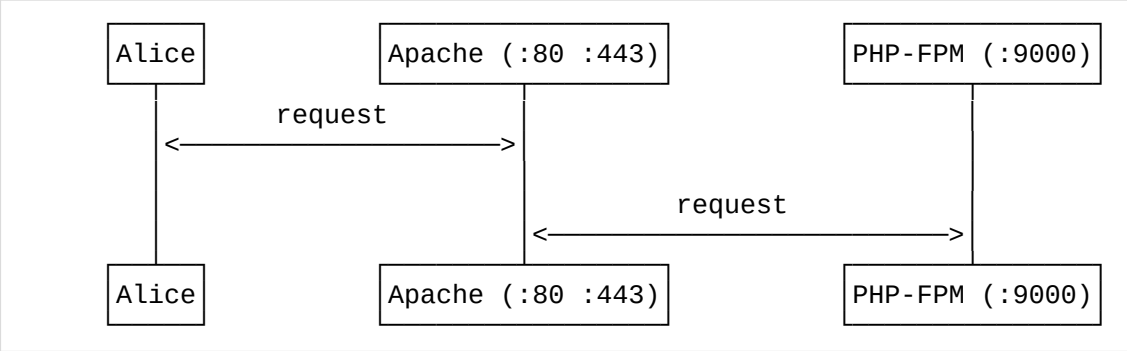
PHP-FPM method



Notes about PHP-FPM

PHP-FPM method

↓ serve dynamic files

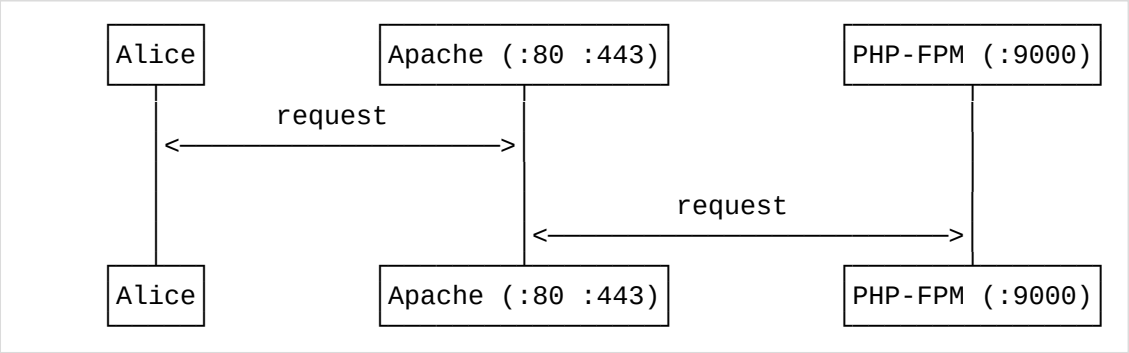


↑ serve static files

Notes about PHP-FPM

PHP-FPM method

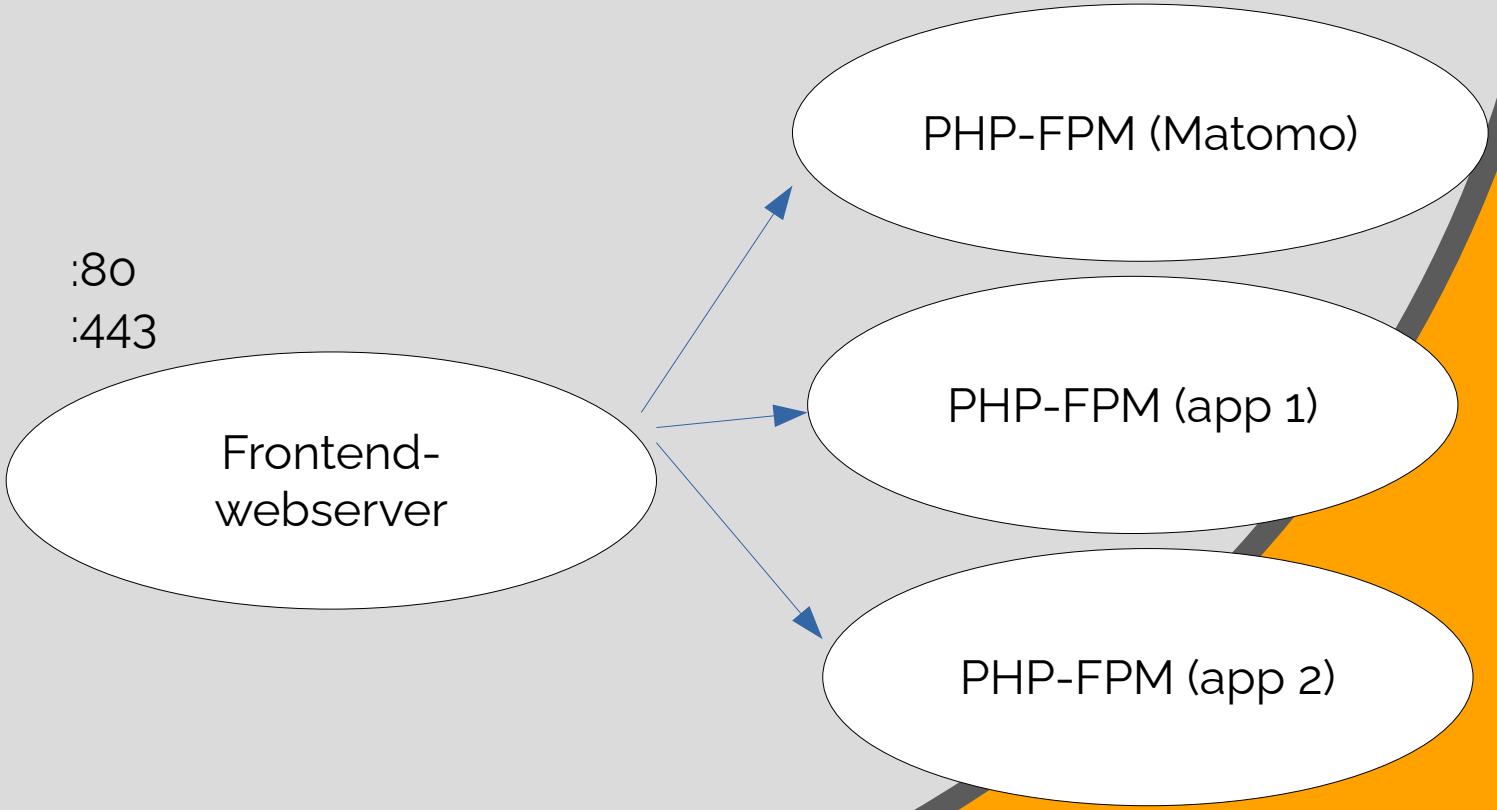
↓ (This can be Docker)



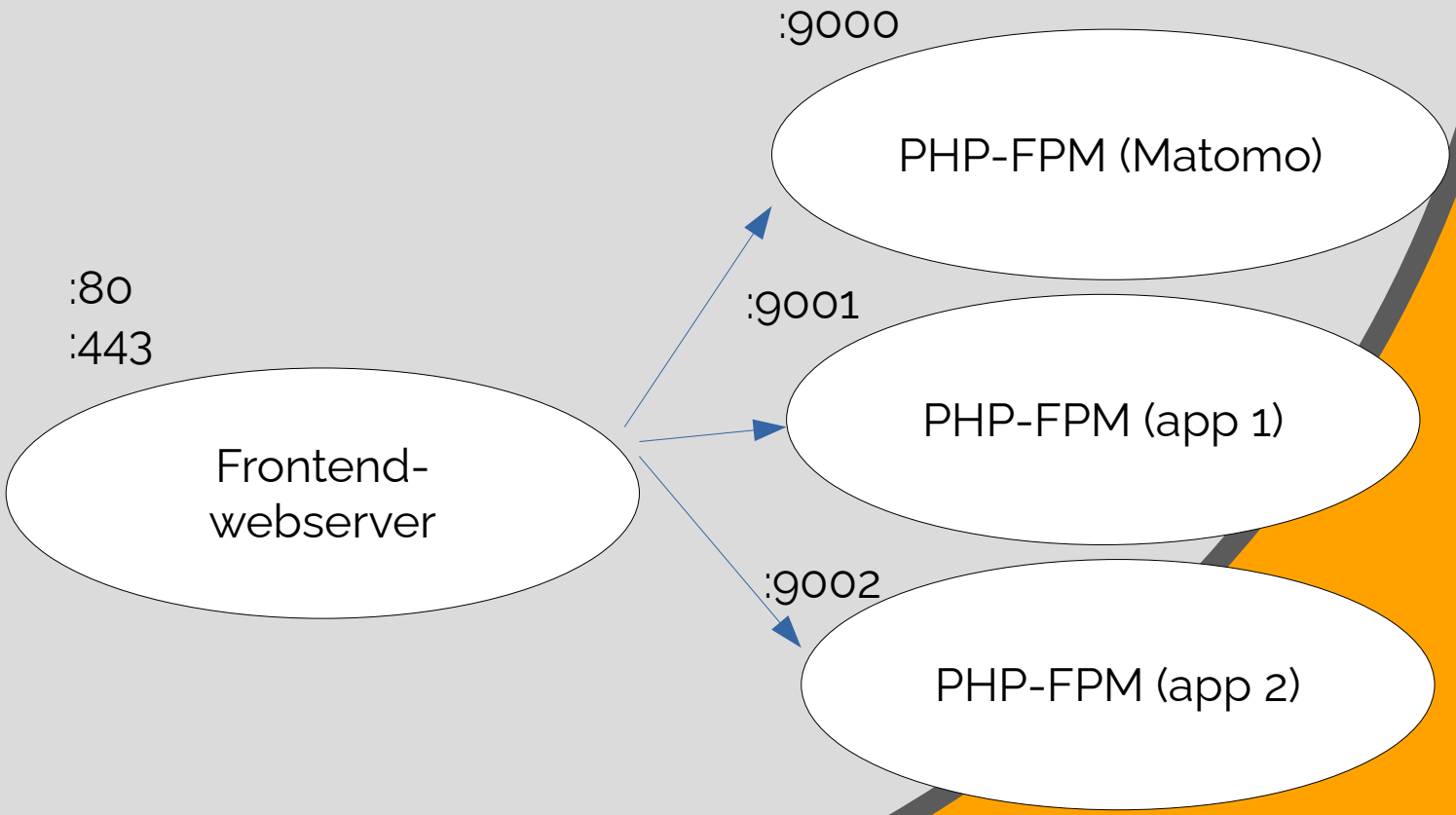
↑

(This can be nginx)

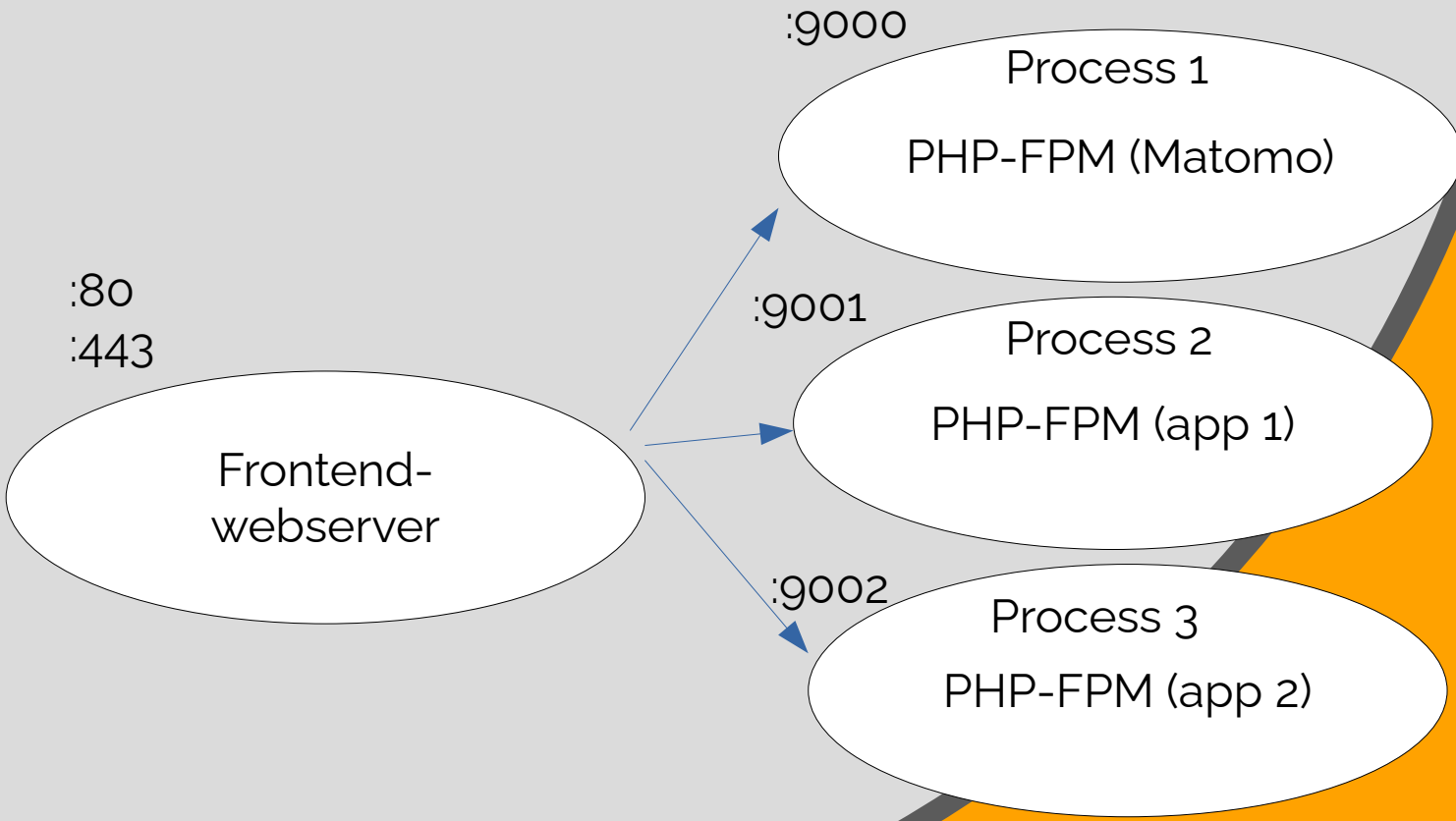
PHP-FPM


:80
:443
Frontend-
webserver
PHP-FPM (Matomo)
PHP-FPM (app 1)
PHP-FPM (app 2)

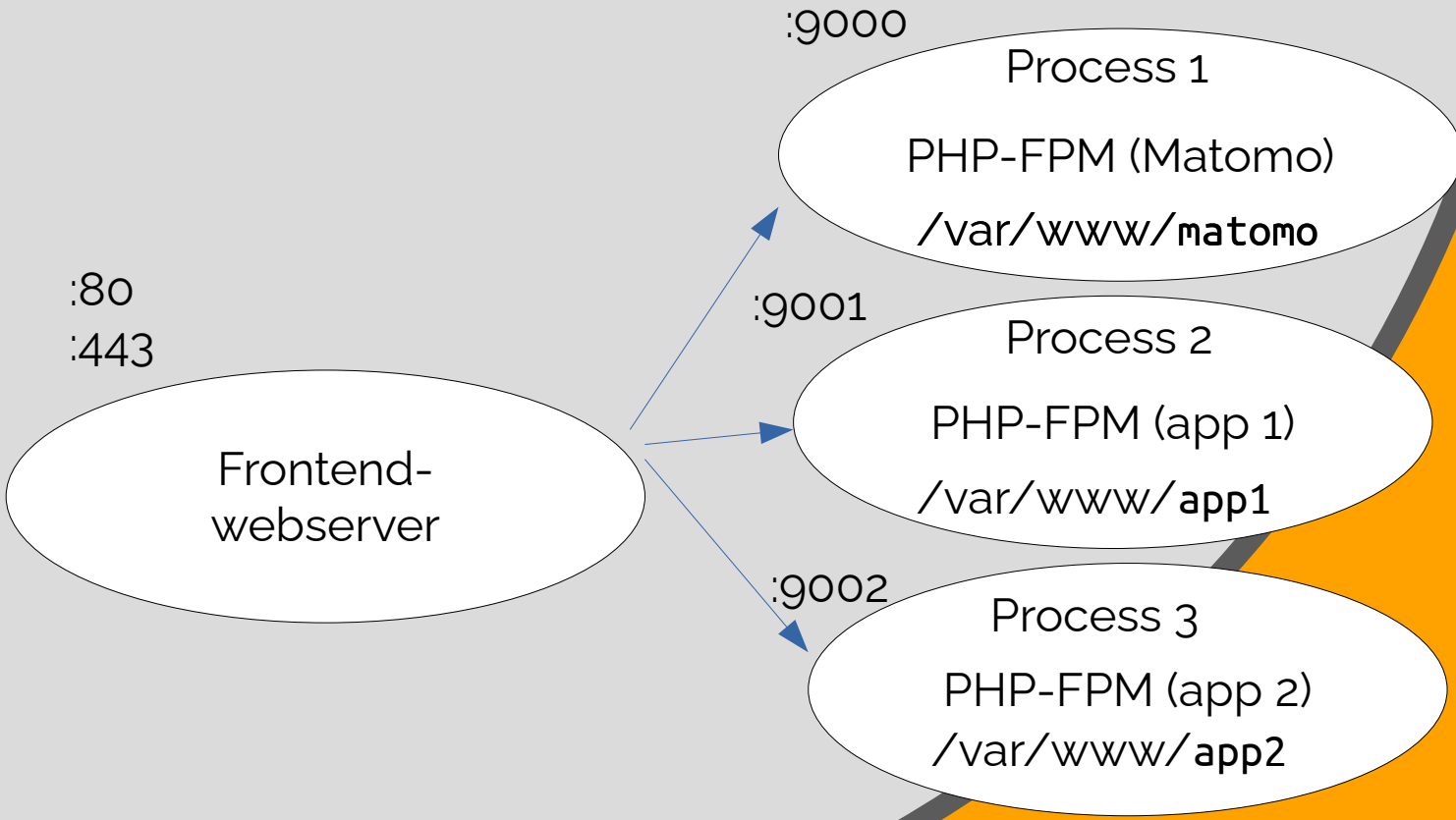
PHP-FPM


:9000
PHP-FPM (Matomo)
:80
:443
:9001
Frontend-
webserver
PHP-FPM (app 1)
:9002
PHP-FPM (app 2)

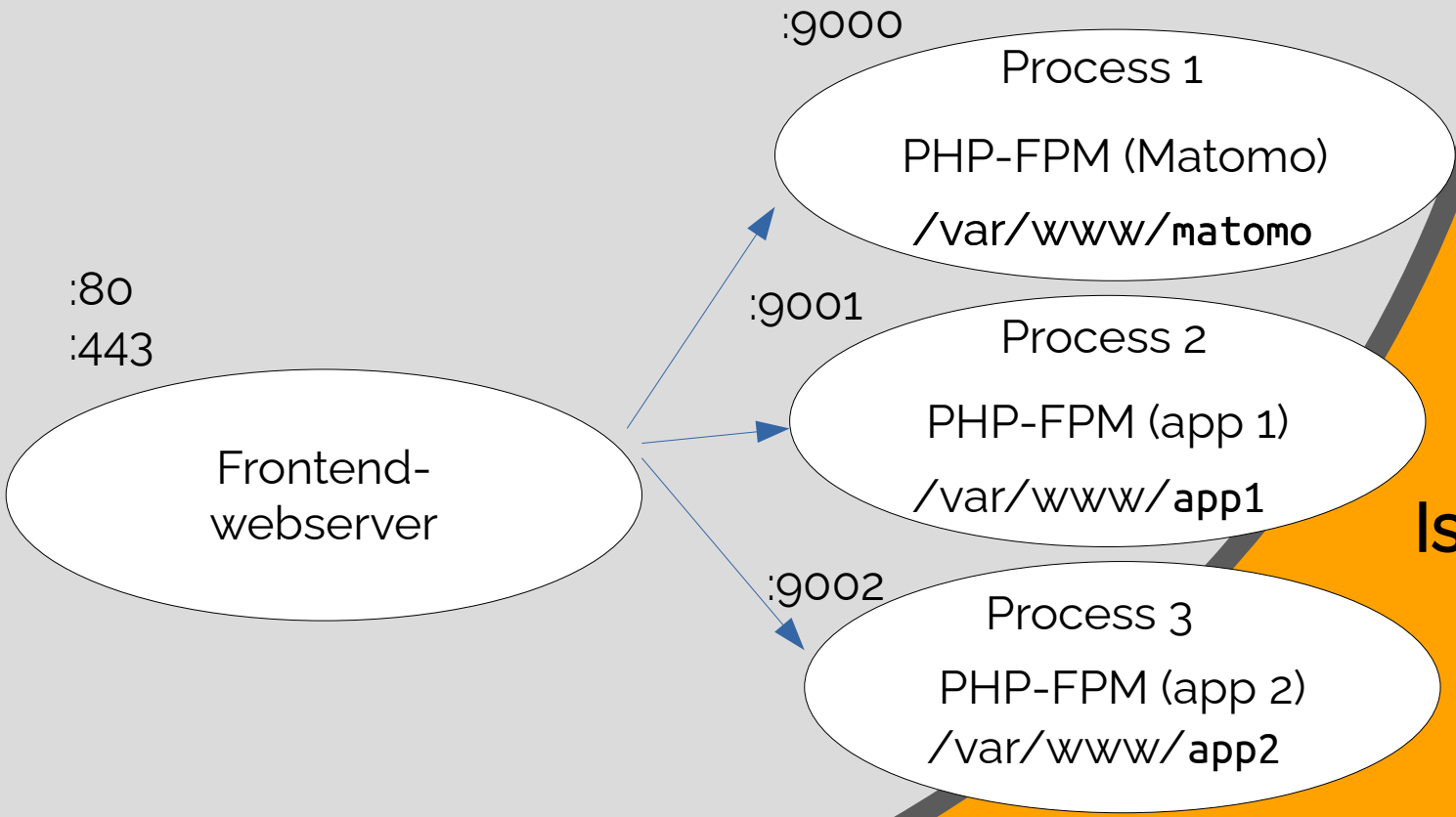
PHP-FPM


:9000
Process 1
PHP-FPM (Matomo)
:80
:443
:9001
Process 2
PHP-FPM (app 1)
Frontend-
webserver
:9002
Process 3
PHP-FPM (app 2)

PHP-FPM

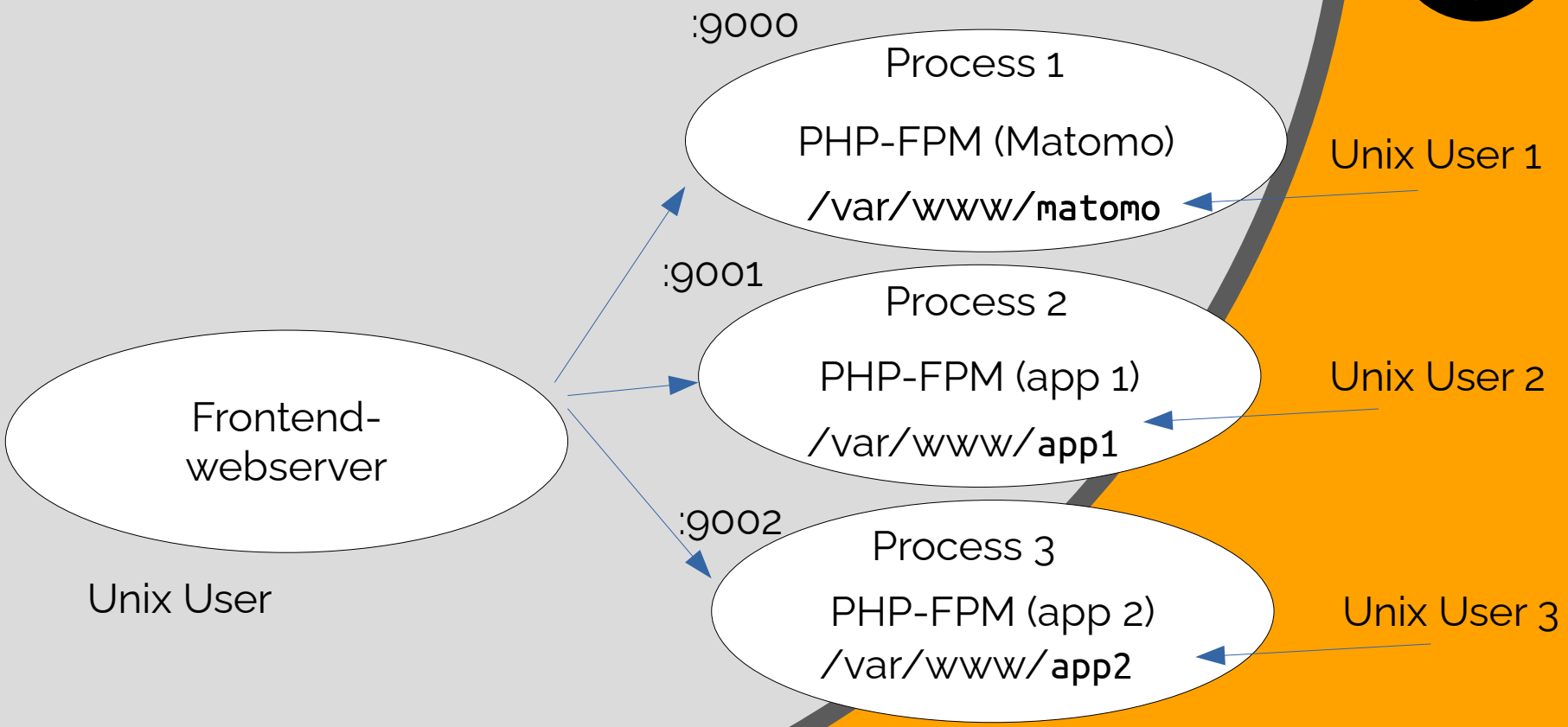

:9000
Process 1
PHP-FPM (Matomo)
/var/www/matomo
:80
:443
:9001
Process 2
PHP-FPM (app 1)
/var/www/app1
Frontend-
webserver
:9002
Process 3
PHP-FPM (app 2)
/var/www/app2

PHP-FPM



Isolation?

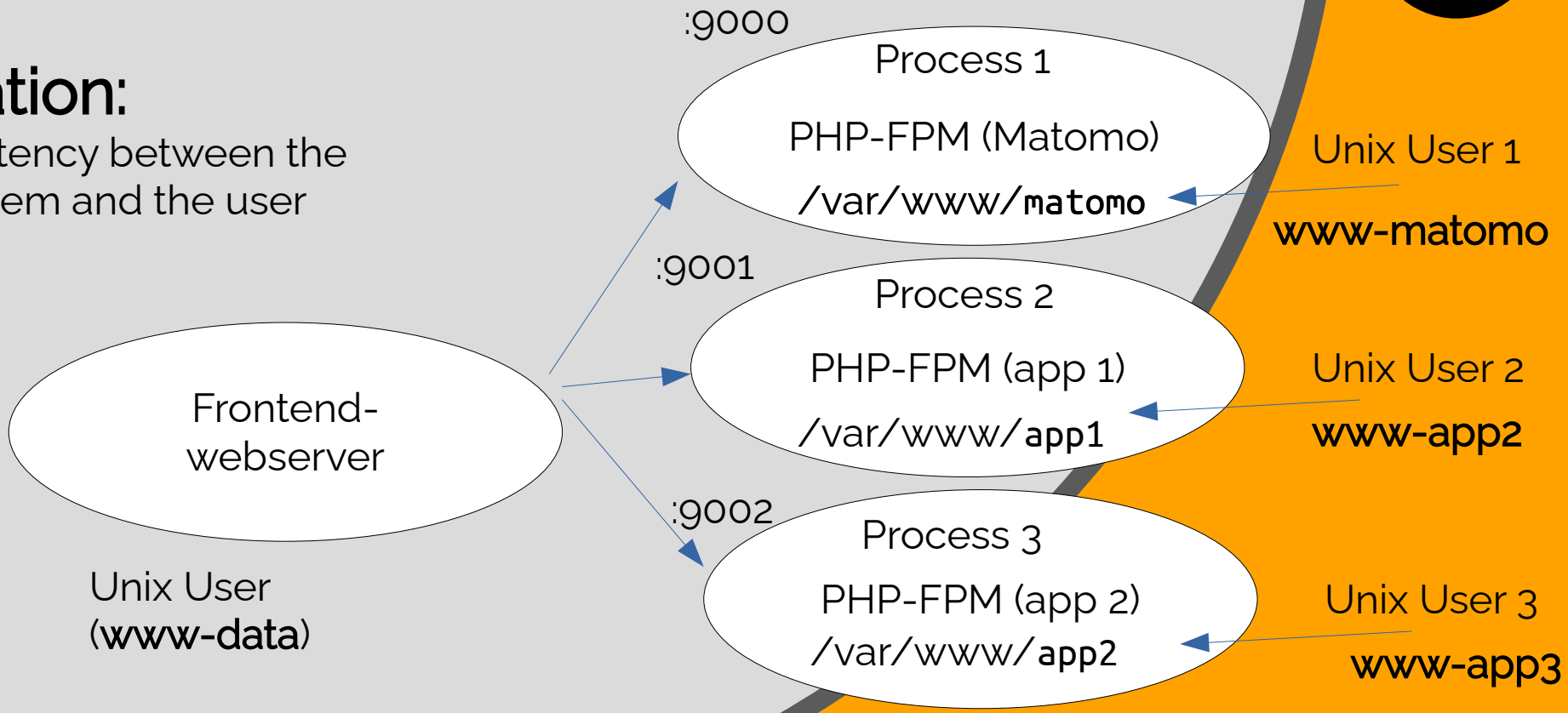
PHP-FPM


:9000
Process 1
PHP-FPM (Matomo)
/var/www/matomo
Unix User 1
:9001
Process 2
PHP-FPM (app 1)
/var/www/app1
Unix User 2
Frontend-
webserver
Unix User
:9002
Process 3
PHP-FPM (app 2)
/var/www/app2
Unix User 3

PHP-FPM

Isolation:

Consistency between the filesystem and the user



Basic example

Frontend webserver (e.g. apache:

```
DocumentRoot                                    /var/www/matomo/www
```

PHP-FPM

```
User  = apache-matomo
group = apache-matomo

# use a dedicated tmp directory
php_admin_value[upload_tmp_dir] = /var/www/matomo/tmp
php_admin_value[sys_temp_dir] =   /var/www/matomo/tmp

# harden the installation
php_admin_value[open_basedir]=    /var/www/matomo
```

```
# ls -l /var/www/matomo/
total 12
drwxrwx---  2 apache-matomo apache-matomo 4096 23 dic 13.39 tmp
lrwxrwxrwx  1 root          root            16 24 gen 22.24 www -> www-matomo.4.1.0
drwxrwxr-x 13 apache-matomo apache-matomo 4096 30 dic 11.24 www-matomo.4.1.0
```

Isolation example (PHP-FPM)

```
[matomo]
Port  = 9000
User  = apache-matomo
group = apache-matomo

# use a dedicated tmp directory
php_admin_value[upload_tmp_dir] = /var/www/matomo/tmp
php_admin_value[sys_temp_dir] =   /var/www/matomo/tmp

# harden the installation
php_admin_value[open_basedir]=    /var/www/matomo
```

Matomo structure and chmod

```
# ls -l /var/www/matomo/www/
total 380
-rw-r--r--  1 root          root          91119 22 dic 06.05 CHANGELOG.md
drwxr-xr-x  3 apache-matomo apache-matomo  4096 29 dic 21.27 config
-rwxr-xr-x  1 root          root            753 22 dic 06.05 console
-rw-r--r--  1 root          root            929 22 dic 06.05 CONTRIBUTING.md
drwxr-xr-x 51 root          root           4096 29 dic 21.27 core
-rw-r--r--  1 root          root            578 22 dic 06.05 DIObject.php
-rw-r--r--  1 root          root              0 29 dic 21.26 favicon.ico
-rw-r--r--  1 root          root            712 22 dic 06.05 index.php
drwxr-xr-x  2 root          root           4096 29 dic 21.27 js
drwxr-xr-x  2 root          root           4096 29 dic 21.27 lang
-rw-r--r--  1 root          root            828 22 dic 06.05 LegacyAutoloader.php
-rw-r--r--  1 root          root           8620 22 dic 06.05 LEGALNOTICE
drwxr-xr-x  9 root          root           4096 29 dic 21.27 libs
-rw-r--r--  1 root          root          35146 22 dic 06.05 LICENSE
-rw-r--r--  1 apache-matomo apache-matomo 61980 22 dic 06.05 matomo.js
-rw-r--r--  1 root          root            328 22 dic 06.05 matomo.php
drwxr-xr-x  8 root          root           4096  6 gen 02.44 misc
drwxr-xr-x 21 root          root           4096 29 dic 21.27 node_modules
-rw-r--r--  1 root          root           6381 22 dic 06.05 offline-service-worker.js
-rw-r--r--  1 root          root           4601 22 dic 06.05 package-lock.json
-rw-r--r--  1 apache-matomo apache-matomo 61980 22 dic 06.05 piwik.js
-rw-r--r--  1 root          root           2685 22 dic 06.05 piwik.php
drwxr-xr-x 69 root          root           4096 29 dic 21.27 plugins
-rw-r--r--  1 root          root           4617 22 dic 06.05 PRIVACY.md
-rw-r--r--  1 root          root           5688 22 dic 06.05 README.md
-rw-r--r--  1 root          root            744 22 dic 06.05 robots.txt
-rw-r--r--  1 root          root           1174 22 dic 06.05 SECURITY.md
drwxr-xr-x  2 root          root           4096 22 dic 06.06 tests
drwxrwx--- 10 apache-matomo apache-matomo  4096 29 dic 21.27 tmp
drwxr-xr-x 23 root          root           4096 29 dic 21.27 vendor
```

Assigning to root?
Spoiler:
It's a **very** good idea
to achieve strict readonly.

Matomo structure and ch*

```
# ls -l /var/www/matomo/www/
total 380
-rw-r--r--  1 root          root          91119 22 dic 06.05 CHANGELOG.md
drwxr-xr-x  3 apache-matomo apache-matomo  4096 29 dic 21.27 config
-rwxr-xr-x  1 root          root            753 22 dic 06.05 console
-rw-r--r--  1 root          root            929 22 dic 06.05 CONTRIBUTING.md
drwxr-xr-x 51 root          root           4096 29 dic 21.27 core
-rw-r--r--  1 root          root            578 22 dic 06.05 DIObject.php
-rw-r--r--  1 root          root              0 29 dic 21.26 favicon.ico
-rw-r--r--  1 root          root            712 22 dic 06.05 index.php
drwxr-xr-x  2 root          root           4096 29 dic 21.27 js
drwxr-xr-x  2 root          root           4096 29 dic 21.27 lang
-rw-r--r--  1 root          root            828 22 dic 06.05 LegacyAutoloader.php
-rw-r--r--  1 root          root           8620 22 dic 06.05 LEGALNOTICE
drwxr-xr-x  9 root          root           4096 29 dic 21.27 libs
-rw-r--r--  1 root          root          35146 22 dic 06.05 LICENSE
-rw-r--r--  1 apache-matomo apache-matomo 61980 22 dic 06.05 matomo.js
-rw-r--r--  1 root          root            328 22 dic 06.05 matomo.php
drwxr-xr-x  8 root          root           4096  6 gen 02.44 misc
drwxr-xr-x 21 root          root           4096 29 dic 21.27 node_modules
-rw-r--r--  1 root          root           6381 22 dic 06.05 offline-service-worker.js
-rw-r--r--  1 root          root           4601 22 dic 06.05 package-lock.json
-rw-r--r--  1 apache-matomo apache-matomo 61980 22 dic 06.05 piwik.js
-rw-r--r--  1 root          root           2685 22 dic 06.05 piwik.php
drwxr-xr-x 69 root          root           4096 29 dic 21.27 plugins
-rw-r--r--  1 root          root           4617 22 dic 06.05 PRIVACY.md
-rw-r--r--  1 root          root           5688 22 dic 06.05 README.md
-rw-r--r--  1 root          root            744 22 dic 06.05 robots.txt
-rw-r--r--  1 root          root           1174 22 dic 06.05 SECURITY.md
drwxr-xr-x  2 root          root           4096 22 dic 06.06 tests
drwxrwx--- 10 apache-matomo apache-matomo  4096 29 dic 21.27 tmp
drwxr-xr-x 23 root          root           4096 29 dic 21.27 vendor
```

Assigning to root?
Spoiler:
It's a **very** good idea
to achieve strict readonly.

Matomo structure and ch*

```
# ls -l /var/www/matomo/www/
total 380
-rw-r--r--  1 root          root          91119 22 dic 06.05 CHANGELOG.md
drwxr-xr-x  3 apache-matomo apache-matomo  4096 29 dic 21.27 config
-rwxr-xr-x  1 root          root            753 22 dic 06.05 console
-rw-r--r--  1 root          root            929 22 dic 06.05 CONTRIBUTING.md
drwxr-xr-x 51 root          root           4096 29 dic 21.27 core
-rw-r--r--  1 root          root            578 22 dic 06.05 DIObject.php
-rw-r--r--  1 root          root              0 29 dic 21.26 favicon.ico
-rw-r--r--  1 root          root            712 22 dic 06.05 index.php
drwxr-xr-x  2 root          root           4096 29 dic 21.27 js
drwxr-xr-x  2 root          root           4096 29 dic 21.27 lang
-rw-r--r--  1 root          root            828 22 dic 06.05 LegacyAutoloader.php
-rw-r--r--  1 root          root           8620 22 dic 06.05 LEGALNOTICE
drwxr-xr-x  9 root          root           4096 29 dic 21.27 libs
-rw-r--r--  1 root          root          35146 22 dic 06.05 LICENSE
-rw-r--r--  1 apache-matomo apache-matomo 61980 22 dic 06.05 matomo.js
-rw-r--r--  1 root          root            328 22 dic 06.05 matomo.php
drwxr-xr-x  8 root          root           4096  6 gen 02.44 misc
drwxr-xr-x 21 root          root           4096 29 dic 21.27 node_modules
-rw-r--r--  1 root          root           6381 22 dic 06.05 offline-service-worker.js
-rw-r--r--  1 root          root           4601 22 dic 06.05 package-lock.json
-rw-r--r--  1 apache-matomo apache-matomo 61980 22 dic 06.05 piwik.js
-rw-r--r--  1 root          root           2685 22 dic 06.05 piwik.php
drwxr-xr-x 69 root          root           4096 29 dic 21.27 plugins
-rw-r--r--  1 root          root           4617 22 dic 06.05 PRIVACY.md
-rw-r--r--  1 root          root           5688 22 dic 06.05 README.md
-rw-r--r--  1 root          root            744 22 dic 06.05 robots.txt
-rw-r--r--  1 root          root           1174 22 dic 06.05 SECURITY.md
drwxr-xr-x  2 root          root           4096 22 dic 06.06 tests
drwxrwx--- 10 apache-matomo apache-matomo  4096 29 dic 21.27 tmp
drwxr-xr-x 23 root          root           4096 29 dic 21.27 vendor
```

Assigning to root?
Spoiler:
It's a **very** good idea
to achieve strict readonly.

Matomo : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2020-29578				2020-12-08	2020-12-22	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
	The official piwik Docker images before fpm-alpine (Alpine specific) contain a blank password for a root user. Systems using the Piwik Docker container deployed by affected versions of the Docker image may allow an remote attacker to achieve root access.													
2	CVE-2009-4137	20		Exec Code	2009-12-24	2019-11-21	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
	The loadContentFromCookie function in core/Cookie.php in Piwik before 0.5 does not validate strings obtained from cookies before calling the unserialize function, which allows remote attackers to execute arbitrary code or upload arbitrary files via vectors related to the __destruct function in the Piwik_Config class; php://filter URIs; the __destruct functions in Zend Framework, as demonstrated by the Zend_Log destructor; the shutdown functions in Zend Framework, as demonstrated by the Zend_Log_Writer_Mail class; the render function in the Piwik_View class; Smarty templates; and the _eval function in Smarty.													
3	CVE-2015-7815	22		Dir. Trav.	2015-11-16	2019-11-21	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
	Directory traversal vulnerability in core/ViewDataTable/Factory.php in Piwik before 2.15.0 allows remote attackers to include and execute arbitrary local files via the viewDataTable parameter.													
4	CVE-2015-7816			Exec Code	2015-11-16	2019-11-21	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
	The DisplayTopKeywords function in plugins/Referrers/Controller.php in Piwik before 2.15.0 allows remote attackers to conduct PHP object injection attacks, conduct Server-Side Request Forgery (SSRF) attacks, and execute arbitrary PHP code via a crafted HTTP header.													
5	CVE-2010-2786	22		Dir. Trav.	2010-08-02	2019-11-21	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
	Directory traversal vulnerability in Piwik 0.6 through 0.6.3 allows remote attackers to include arbitrary local files and possibly have unspecified other impact via directory traversal sequences in a crafted data-renderer request.													
6	CVE-2011-4941			Exec Code	2012-09-18	2019-11-21	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
	Unspecified vulnerability in Piwik 1.2 through 1.4 allows remote attackers with the view permission to execute arbitrary code via unknown attack vectors.													
7	CVE-2011-0398	264		Bypass	2011-01-10	2019-11-21	6.4	None	Remote	Low	Not required	Partial	Partial	None
	The Piwik_Common::getIP function in Piwik before 1.1 does not properly determine the client IP address, which allows remote attackers to bypass intended geolocation and logging functionality via (1) use of a private (aka RFC 1918) address behind a proxy server or (2) spoofing of the X-Forwarded-For HTTP header.													
8	CVE-2009-1085	264		+Info	2009-03-25	2019-11-21	5.0	None	Remote	Low	Not required	Partial	None	None
	Piwik 0.2.32 and earlier stores sensitive information under the web root with insufficient access control, which allows remote attackers to obtain the API key and other sensitive information via a direct request for misc/cron/archive.sh.													
9	CVE-2011-0400	16			2011-01-10	2019-11-21	5.0	None	Remote	Low	Not required	Partial	None	None
	Cookie.php in Piwik before 1.1 does not set the secure flag for the session cookie in an https session, which makes it easier for remote attackers to capture this cookie by intercepting its transmission within an http session.													
10	CVE-2011-0401	264		DoS	2011-01-10	2019-11-21	5.0	None	Remote	Low	Not required	None	None	Partial
	Piwik before 1.1 does not properly limit the number of files stored under tmp/sessions/, which might allow remote attackers to cause a denial of service (inode consumption) by establishing many sessions.													
11	CVE-2011-3791	200		+Info	2011-09-24	2019-11-21	5.0	None	Remote	Low	Not required	Partial	None	None
	Piwik 1.1 allows remote attackers to obtain sensitive information via a direct request to a .php file, which reveals the installation path in an error message, as demonstrated by plugins/Widgetize/Widgetize.php and certain other files.													
12	CVE-2013-2633	20		+Info	2013-03-21	2019-11-21	5.0	None	Remote	Low	Not required	Partial	None	None
	Piwik before 1.11 accepts input from a POST request instead of a GET request in unspecified circumstances, which might allow attackers to obtain sensitive information by leveraging the logging of parameters.													
13	CVE-2010-1453	79		XSS	2010-05-07	2019-11-21	4.3	None	Remote	Medium	Not required	None	Partial	None
	Cross-site scripting (XSS) vulnerability in the Login form in Piwik 0.1.6 through 0.5.5 allows remote attackers to inject arbitrary web script or HTML via the form_url parameter.													
14	CVE-2011-0004	79		XSS	2011-01-10	2019-11-21	4.3	None	Remote	Medium	Not required	None	Partial	None
	Multiple cross-site scripting (XSS) vulnerabilities in Piwik before 1.1 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.													
15	CVE-2011-0399				2011-01-10	2019-11-21	4.3	None	Remote	Medium	Not required	None	Partial	None
	Piwik before 1.1 does not prevent the rendering of the login form inside a frame in a third-party HTML document, which makes it easier for remote attackers to conduct clickjacking attacks via a crafted web site.													
16	CVE-2012-4541	79		XSS	2012-11-19	2019-11-21	4.3	None	Remote	Medium	Not required	None	Partial	None
	Cross-site scripting (XSS) vulnerability in Piwik before 1.9 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.													

DON'T BE p0wned please

«One hour invested in reading documentation can save your company»

Thank you!

Questions? Ideas?
Valerio (boz)
boz@reyboz.it