Model:

```
var tree = {
        “[id]“:{
                “l“:“[label]“,
                “p“:“[parent]“,
                “v“:“[view]“
                “o“:“[order]“
        },
        ….
};
```

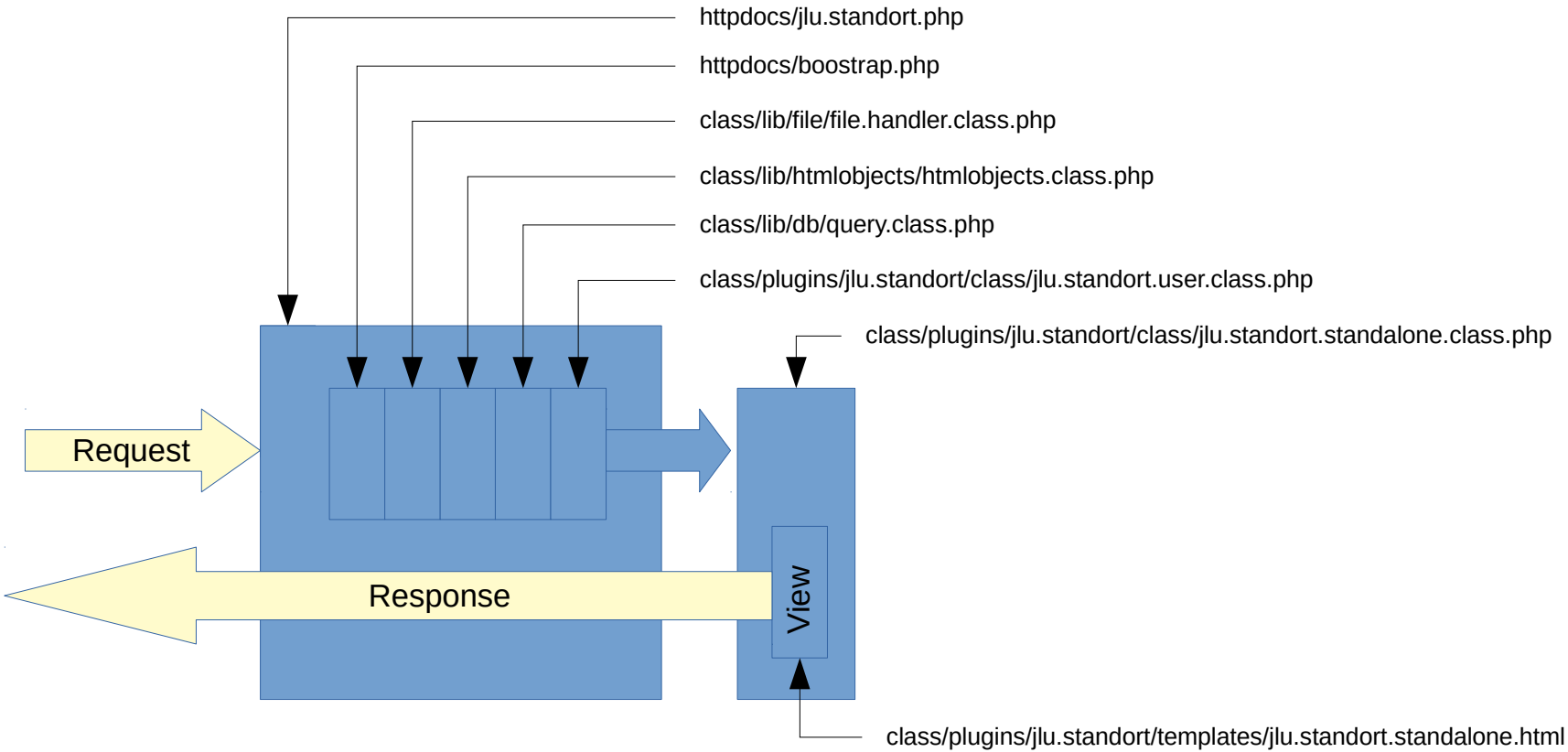
Mime: text/javascript
Charset: utf-8
Format: JSON
Name: tree.js

Legende:

[id] = Objekt ID
[label] = Beschriftung des Objektes (z.B. 1.OG etc.)
[parent] = Vorgänger ID
[view] = Kategorie (z.B. campus, etage, raum etc.)
[order] = Wert, nach dem [view] sortiert werden soll (optional)

Controller:

http://127.0.0.1/jlu.standort.php

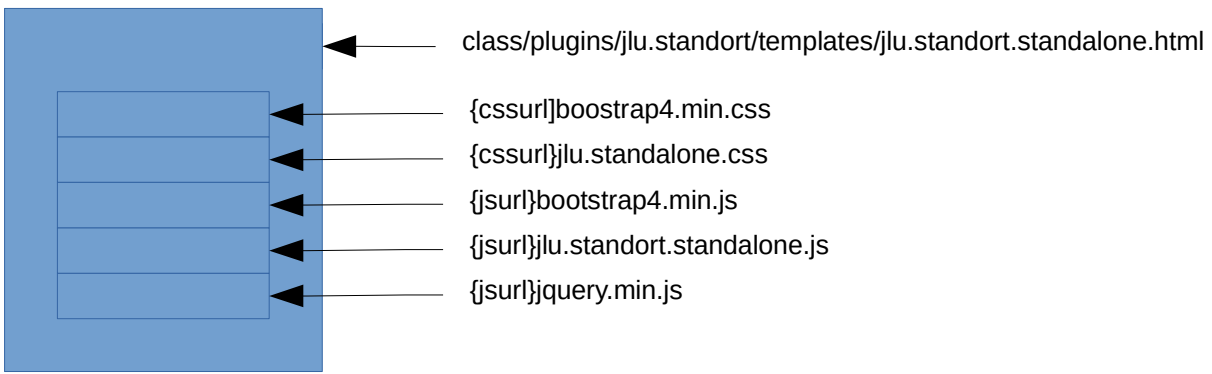


View:

HTML:
https://www.w3schools.com/html/

CSS:
https://getbootstrap.com/docs/4.1/getting-started/download/
https://www.w3schools.com/bootstrap4/

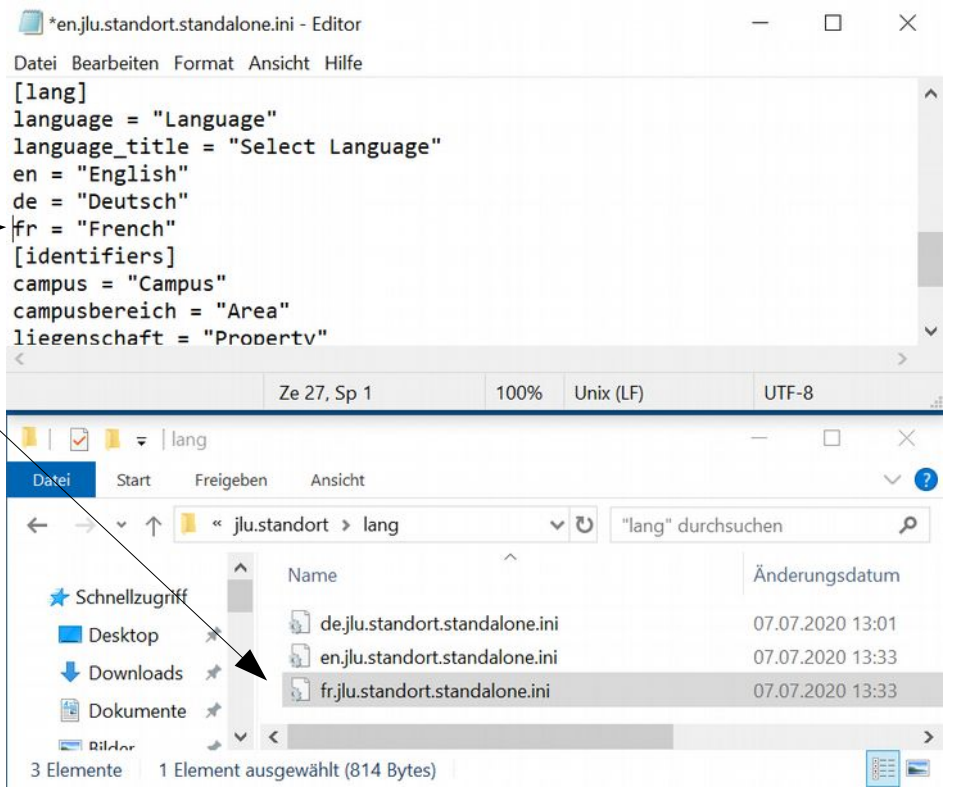
JS:
https://jquery.com/download/
https://api.jquery.com/



Internationalisierung:

Internationalisierung der GUI (Graphical User Interface) ist durchgängig möglich.
Jede Sprache wird In Form einer INI Datei beigefügt.

1. Verzeichnis class/plugins/jlu.standort/lang öffnen
2. Datei en.jlu.standort.standalone.ini mit Editor öffnen.
3. Neue Sprache hinzufügen
4. Schritt 2 für alle Sprachdateien wiederholen
5. de.standort.standalone.ini nach fr.standort.standalone.ini kopieren
6. fr.standort.standalone.ini übersetzen



Risiken:

Da es sich um einen im Internet verfügbaren Service handelt, gelten auch die üblichen Risiken.

1. Datenschutz:
Die Seite soll unter der Domain uni-giessen.de laufen und fällt somit unter deren Datenschutzerklärung (https://www.uni-giessen.de/ueber-uns/datenschutz). Diese Erklärung ist zwingend ein zu halten.

2. XSS und SQL Injection:
Diese Angriffe erfolgen üblicherweise über einen Request der Seite mit veränderten Parametern.
Beispiel:
http://127.0.0.1/standort.php?lang=%3Cscript%3Ealert(%22XSS%22);%3C/script%3E
Alle Parameter werden grundsätzlich Serverseitig überprüft (derzeit lang und id). SQL wird derzeit nicht verwendet.

3. Urheberrecht:
Alle Dateien die auf dem Server hinterlegt sind, können über das Internet abgerufen werden. Es ist zwingend darauf zu achten, daß keine Dateien hinterlegt werden, die das Urheberrecht Dritter beschädigen.

4. Server:
Ein im Internet verfügbarer Server kann grundsätzlich immer angegriffen werden (z.B. DoS https://de.wikipedia.org/wiki/Denial_of_Service). Da aber nur der HTTP Dienst (Apache Port: 80 und 443) benötigt wird, sind das Risiko bzw. die Folgen eher gering bzw. beherrschbar.