PHP Security Cheat Sheet

keinerweiss.de

HTML

```
htmlspecialchars
```

E-Mail address

```
filter_var
  FILTER_SANITIZE_EMAIL
```

exec, system ...

```
escapeshellarg
```

include, require

```
basename
```

eval, preg_replace mit /e

```
do not use
filter everything
```

File paths

```
filter ../ ,
allow only base path
```

Upload

```
File ext and mimetype
```

HTTP Header

```
filter \r\n
```

SQL

```
*real_escape_string, bind
```

URL

```
rawurlencode
```