



# Anleitung

## DA-FormMaker Formmail-Script

Dunkel und Iwer GbR  
Gartenstr. 12a  
15907 Lübben (Spreewald)

[info@ekiwi.de](mailto:info@ekiwi.de)  
<https://da-software.net>

## Inhalt

Einleitung.....	3
Probleme bei der Installation des Scriptes / Installationservice.....	3
Systemanforderungen.....	3
Lizenzbedingungen.....	3
Installation des Scriptes.....	4
Einrichten der „config.php“.....	4
IP-Sperre.....	5
IP-Sperre Datenbank oder Textdatei.....	5
Datenbankzugangsdaten.....	5
Log-Funktion aktivieren.....	5
Spamfilter aktivieren.....	5
Fehlerseiten.....	6
Konfiguration des Mailversands.....	6
Einstellungen Captcha.....	7
Upload des Scriptes.....	8
Datenbank einrichten.....	8
Dateiberechtigungen vergeben.....	9
Fehlerdiagnose.....	10
Spamfilter.....	11
Blackliste.....	11
Automatische Aktualisierung der Blackliste.....	12
Link-Spam.....	13
HTML-Spam.....	13
Captcha Überprüfung.....	14
Anpassung der E-Mail-Vorlage.....	14

## Einleitung

In dieser Anleitung beschreiben wir Ihnen die Schritte zur Installation des Formmail-Scriptes für den DA-FormMaker auf ihren eigenen Webservice. Die Installation erlaubt Ihnen den unabhängigen Betrieb ihrer Formulare.

### Probleme bei der Installation des Scriptes / Installationservice

Sollten Sie Fragen oder Probleme haben, wenden Sie sich bitte einfach an unseren Support:

- <https://da-software.net/kontakt/>

Gerne übernehmen wir auch die Installation des Scriptes für Sie. Die Informationen zu unserem Installationservice finden Sie hier:

- <https://da-software.net/support/installationsservice-fuer-php-formmail-scripte/>

### Systemanforderungen

Folgende Systemanforderungen gelten für das Script:

- PHP 7.4, PHP 8
- MySQL-Datenbank (optional)
- Linux / Unix Server (Windows eingeschränkt)

### Lizenzbedingungen

Als Käufer der Software DA-FormMaker dürfen Sie dieses Script uneingeschränkt nutzen. Sie dürfen das Script beliebig oft auf Ihren Servern installieren. Auch eine Installation und Weitergabe auf Kundenwebsites ist zulässig.

Sie können das Script auf eigene Gefahr hin entsprechend Ihren Wünschen anpassen, sowie Dritte mit der Änderung des Scripts beauftragen.

Das Script und die dazugehörigen Dateien werden ohne Funktionsgarantie für die im Umfeld verwendete Hardware oder Software verkauft. Das Risiko der Benutzung des Scriptes obliegt dem Lizenznehmer, jegliche Erstattungen im Rechtsfall erstrecken sich maximal auf den Kaufpreis der Lizenz. Die Lizenz ist zeitlich unbegrenzt nutzbar.

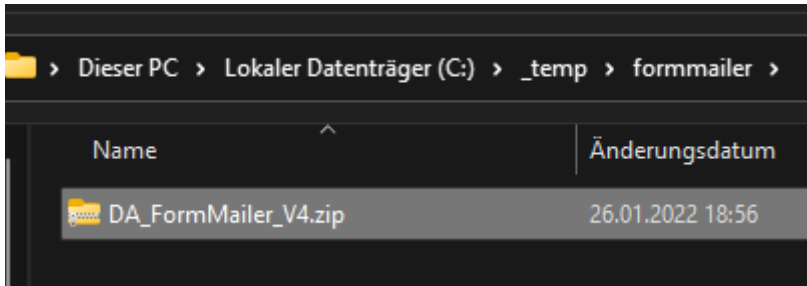
Das Script enthält weitere Open-Source-Komponenten mit jeweils eigener Lizenz (Ordner vendor).

## Installation des Scriptes

Die jeweils aktuelle Version des Scriptes gibt es auf unserer Webseite:

<https://secure.da-software.de/DA-FormMaker/index.html>

Der Download ist ein ZIP-Archiv. Für die Installation muss dieses entpackt werden.



### Einrichten der „config.php“

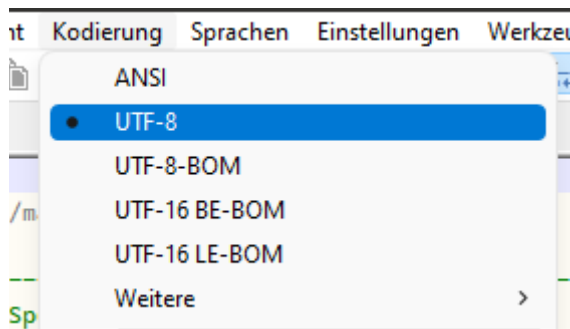
Die Konfiguration des Scriptes erfolgt über die Datei „config.php“. Öffnen Sie diese mit einem Texteditor. Es empfiehlt sich ein Editor wie Notepad++.

The screenshot shows the Notepad++ editor with the file 'C:\\_temp\formmailer\formmail\_v4\config.php' open. The code is as follows:

```

1 <?php
2 include_once('_logic/mail.php');
3
4 //-----
5 // Konfiguration IP-Sperre / Configuration IP lock
6 //-----
7 $iplock = 0; //IP-Sperre aktivieren 0 = aus ; 1 = an / IP lock active 0 = off ; 1 =
8 $iplocktime = 60; //Dauer der IP-Sperre in Sekunden / Duration of the ip lock
9
10 //-----
11 //Verwenden Sie eine Datei oder eine Datenbank für die IP-Sperre, falls Sie DATEI kon
12 //keine Datenbank ist für IP-Sperre als Datei erforderlich
  
```

Achten Sie beim Speichern darauf, dass die Datei als **UTF-8 Datei, ohne BOM**, abgespeichert wird.



Ansonsten kann es zu Fehlern bei der Scriptausführung kommen. In der Datei finden Sie verschiedene Abschnitte und Einstellungen. Beachten Sie ebenfalls die Hinweise in der Datei.

### *IP-Sperre*

Die IP-Sperre überprüft, ob das Formular innerhalb einer festgelegten Zeit von einer IP-Adresse bereits abgesendet worden ist. Falls ja, wird das Formular nicht nochmal abgesendet. Die Sperre dient als Schutz vor dem massenhaften Absenden des Formulars. Für die Aktivierung setzen Sie den Wert auf 1:

```
$iplock = 1; //IP-Sperre aktivieren 0 = aus ; 1 = an
```

Sie können außerdem festlegen, innerhalb welcher Zeit die Sperre gelten soll:

```
$iplocktime = 60; //Dauer der IP-Sperre in Sekunden
```

Die Angabe ist in Sekunden.

### *IP-Sperre Datenbank oder Textdatei*

Für die Nutzung der IP-Sperre müssen die IP-Adressen der Benutzer für die festgelegte Zeit gespeichert werden. Dies kann entweder in einer MySQL-Datenbank erfolgen oder in einer Textdatei. Wenn Sie die Textdatei verwenden wollen, stellen Sie folgende Einstellung in der „config.php“:

```
$conf_iplock_type = IpCheckType::FILE;
```

Für die Nutzung der MySQL-Datenbank:

```
$conf_iplock_type = IpCheckType::DB;
```

Unsere Empfehlung ist die Nutzung der Datenbank, da diese parallele Zugriffe erlaubt. Die Nutzung der Text-Datei empfiehlt sich nur, wenn Sie keine MySQL-Datenbank verwenden können.

### *Datenbankzugangsdaten*

Die Datenbank wird für Captcha und IP-Sperre verwendet. Sofern Sie Captcha und IP-Sperre mit Datenbank verwenden wollen, geben Sie hier die Zugangsdaten ein:

```
$dbname = 'formmail'; //Datenbankname / database name
$dbhost = 'localhost'; //Datenbankserver / database server
$dbuser = 'root'; //Benutzername / user name
$dbpass = ''; //Datenbank-Passwort / password
```

### *Log-Funktion aktivieren*

Mit der Log-Funktion werden die E-Mails zusätzlich noch im Ordner „archiv“ abgelegt.

```
$conf_log = 0; //1 = Log aktivieren
```

### *Spamfilter aktivieren*

Mit der folgenden Option aktivieren Sie den Spam-Filter:

```
$conf_antispam = 1;
```

Der Spamfilter analysiert die E-Mails und verwirft Spam-Nachrichten. In aller Regel empfiehlt sich die Nutzung des Spamfilters. Die genaue Funktion des Spam-Filters und die Einrichtung erklären wir in einem späteren Kapitel.

Wenn Sie die Funktion des Spamfilters testen wollen, können Sie Spam-Mails nicht nur verwerfen, sondern auch an eine eigene E-Mail-Adresse zur Überprüfung senden. Dies geht mit der folgenden Einstellung:

```
$conf_antispam_copy_mail = 1;
$conf_antispam_mail_address = "devnull@ekiwi.de";
```

Ist die Einstellung auf „1“ gestellt werden Spammnachrichten nicht verworfen, sondern an die Mail-Adresse gesendet. Hiermit können Sie überprüfen, ob der Spamfilter korrekt funktioniert.

### Fehlerseiten

Es folgen verschiedene Einstellungen zu Fehlerseiten. Teilweise können diese Seiten vom Formular überschrieben werden. Sofern im Formular keine extra festgelegt sind, werden diese verwendet.

```
$IPErrorPage = 'https://www.ekiwi-scripts.de/form/errorpages/blockip.htm';
```

Legt die Fehlerseite fest, welche erscheint, wenn die IP-Sperre das Absenden verhindert.

```
$CaptchaErrorPage =
'https://www.ekiwi-scripts.de/form/errorpages/blockcaptcha.htm';
```

Legt die Fehlerseite fest, welche erscheint, wenn ein ungültiges Captcha eingetragen worden ist.

```
$FileErrorPage =
'https://www.ekiwi-scripts.de/form/errorpages/blockfile.htm';
```

Legt die Fehlerseite fest, welche erscheint, wenn die maximal konfigurierte Dateigröße überschritten worden ist. Die maximale Dateigröße können Sie mit folgender Einstellung festlegen:

```
$max_attach_size = 5000000;
```

Die Angabe ist in Bytes. 1 Megabyte entspricht 1048576 Bytes.

```
$BlockFilePage =
'https://www.ekiwi-scripts.de/form/errorpages/blockfiletype.htm';
```

Die Fehlerseite für nicht erlaubte Dateuploads. Standardmäßig sind alle Dateitypen für den Upload erlaubt. Um nur bestimmte Dateitypen zu erlauben, ändern Sie diese Zeile ab:

```
$BlockFileList = array();
```

Um nur bestimmte Dateitypen bzw. Endungen zuzulassen, geben Sie diese im Array an:

```
$BlockFileList = array( ".pdf", ".exe", ".doc", ".xls" );
```

Die Einträge werden mit Komma getrennt und müssen in Anführungszeichen und Punkt angegeben werden.

### Konfiguration des Mailversands

Ein weiterer wichtiger Punkt ist die Versandart, zur Auswahl stehen Sendmail und SMTP:

```
$c_mail_send_type = MailSend::Sendmail;
```

Oder

```
$c_mail_send_type = MailSend::SMTP;
```

Sendmail versendet die E-Mails direkt über den Webserver. Diese Variante benötigt keine weitere Konfiguration, hat allerdings den Nachteil, dass Spamfilter manchmal die Mails ausfiltern, wenn diese von einem eher unbekanntem Server kommen.

Wir empfehlen dafür die SMTP-Konfiguration. Sie legen hierzu ein SMTP-Konto bei Ihrem Webhoster an und tragen anschließend die Zugangsdaten in die config.php ein:

```
$c_smtp_host = "localhost"; //Serveradresse  
$c_smtp_username = "ihrname@example.com"; //Benutzername  
$c_smtp_password = "ihrpasswort"; //Passwort
```

Die Übertragung erfolgt verschlüsselt, sofern der Port abweicht, kann er mit folgender Einstellung festgelegt werden:

```
$c_smtp_port = 587;
```

Falls zu Problemen beim Versand der E-Mails kommt, z.B. Mails nicht ankommen, dann kann es helfen einen Standardabsender zu definieren:

```
$c_standard_mail = "andy.dunkel@ekiwi.de";
```

Diese E-Mail-Adresse wird anschließend immer als Absender-E-Mail verwendet und sollte einer existierenden Adresse entsprechen, welche zum Server bzw. Weospace gehört.

Sollten Probleme beim Versand auftreten, kann das SMTP-Debugging aktiviert werden:

```
$c_smtp_debug = true;
```

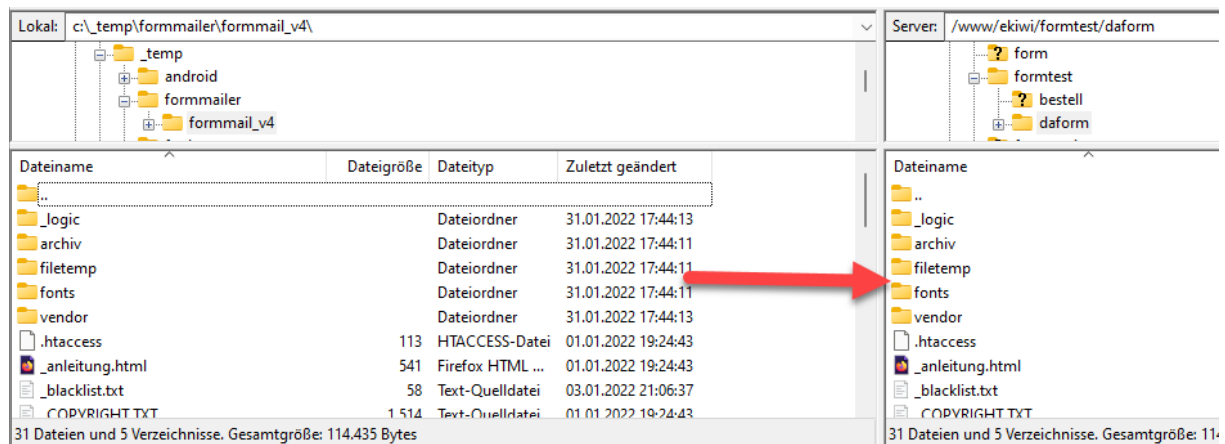
Ist die Einstellung auf „true“ gesetzt, erfolgt nach dem Absenden eine detaillierte Ausgabe. Hier werden dann Fehlermeldungen und Warnungen ausgegeben. Für den Produktivbetrieb muss die Einstellung wieder auf „false“ gestellt werden.

### *Einstellungen Captcha*

In diesem Abschnitt kann das Captcha konfiguriert werden, z.B. Anzahl der Störungen, Farben etc. Die Details entnehmen Sie der „config.php“.

## Upload des Scriptes

Nachdem Sie die Konfiguration des Scriptes abgeschlossen haben, können Sie das Script mit einem FTP-Programm auf Ihrem Webservice übertragen.



## Datenbank einrichten

Sofern Sie die Captcha-Funktion nutzen wollen oder die IP-Sperre für MySQL konfiguriert ist, müssen Sie nun die MySQL-Tabellen einrichten. Legen Sie hierzu eine MySQL-Datenbank im Admin-Bereich ihres Webhoster an. Anschließend rufen Sie im Browser die Installation des Formmail-Scripts auf, indem Sie die „sqlinstall.php“ Datei des Scripts aufrufen.

[https://ihrserver.de/pfad/formmail\\_v4/sqlinstall.php](https://ihrserver.de/pfad/formmail_v4/sqlinstall.php)

### Installation MySQL-Tabellen / Installation MySQL tables

**Zugangsdaten für MySQL / Credentials for MySQL:**

**Datenbankserver / Server name:**  
localhost

**Datenbankname / Database name:**  
formmailer

**Benutzername / User name:**  
root

**Passwort / Password:**

**Tabellen installieren / Install tables**

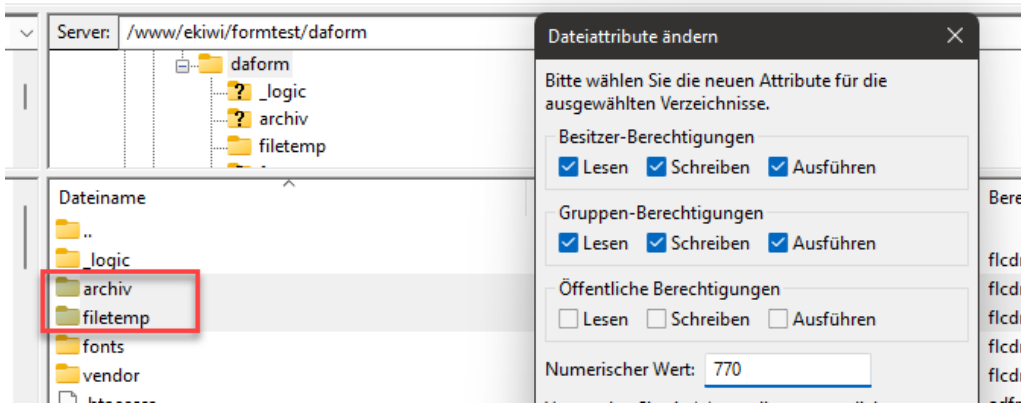
Geben Sie die Zugangsdaten zur Datenbank ein und klicken Sie auf „Tabellen installieren“. Die Tabellen werden nun in der Datenbank angelegt. Es empfiehlt sich die Datei „sqlinstall.php“ nach der Einrichtung vom Webservice zu löschen.



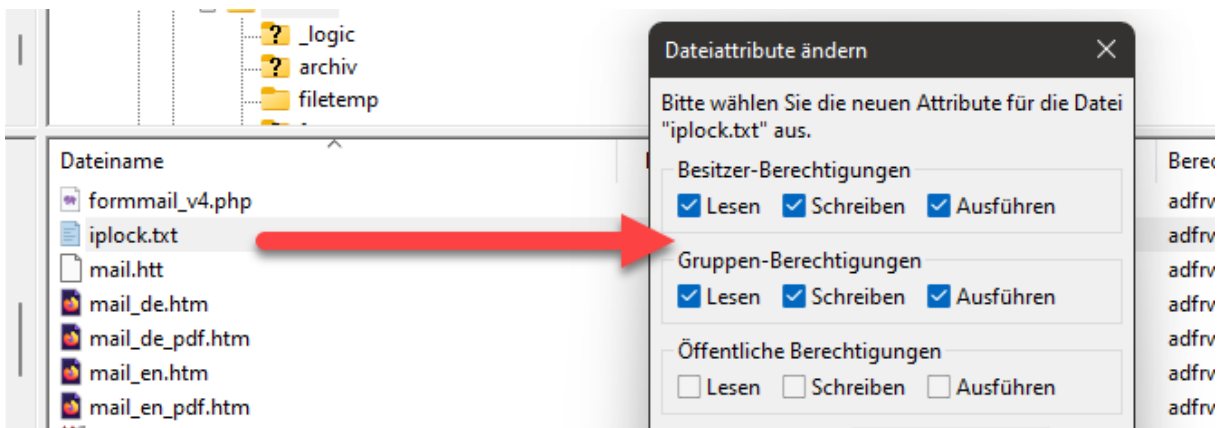
## Dateiberechtigungen vergeben

Sofern Ihre Formulare Dateiuploads verwenden, muss der Ordner „filetemp“ über Schreibrechte für das Script verfügen. Der „archiv“ Ordner benötigt ebenfalls Schreibrechte, sofern die Archivfunktion aktiviert ist.

Folgende Einstellung ist beispielhaft und hängt von der Konfiguration Ihres Webhosters ab:

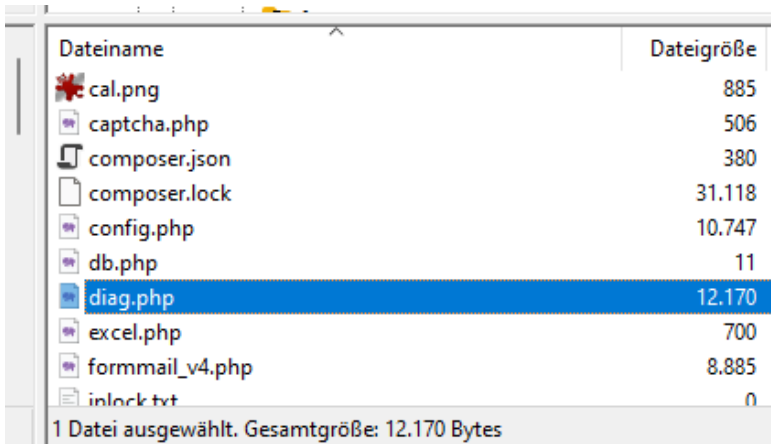


Sofern Sie die IP-Sperre als Datei eingerichtet haben, benötigt die Datei „iplock.txt“ ebenfalls Schreibrechte.



## Fehlerdiagnose

Sollte Sie Probleme bei der Ausführung des Scriptes haben, können Sie die Diagnosefunktion aktivieren, benennen Sie hierzu die Datei „diag.\_\_\_\_“ nach „diag.php“ um.



Dateiname	Dateigröße
cal.png	885
captcha.php	506
composer.json	380
composer.lock	31.118
config.php	10.747
db.php	11
diag.php	12.170
excel.php	700
formmail_v4.php	8.885
inlock.txt	0

1 Datei ausgewählt. Gesamtgröße: 12.170 Bytes

Anschließend können Sie diese Seite im Browser aufrufen. Die Liste enthält die aktuelle Konfiguration und zeigt auch Warnungen und Fehler an.

Formmail-Script Diagnose	
Script-Einstellungen	
iplock	0
iplocktime	60
dbname	
dbhost	
dbuser	
Config Log	0

**Hinweis:** Falls Sie Probleme mit der Installation haben, dann aktivieren Sie die Diagnose und schicken Sie uns den Link zur Diagnose, zusammen mit Ihrer Anfrage.

## Spamfilter

Ist der Spamfilter aktiviert, werden folgende Spamfilter aktiviert.

### Blackliste

Über eine Blackliste bzw. Textdatei können E-Mails mit bestimmten Begriffen gefiltert werden. Kommt ein Eintrag in der Liste vor, wird die E-Mail gefiltert. Wir führen für unsere Formmail-Scripte eine täglich aktualisierte Spamliste, welche direkt von uns heruntergeladen werden kann.

#### Beispiel für Blacklist-Filterung nach „folmax.pw“:

**Telefon:** 030 [REDACTED]  
**Email:** jack [REDACTED]  
**Frage:** Mllscke, Abfallscke alle  
 Sorten.  
 Gewebescke. Kartoffelscke.  
 Laubscke.  
 Raschelscke. Zwiebelscke.  
 Spnescke.

Hochwertige Waren vom  
 Produzent. Fabrikverkauf.  
 Versand am gleichen Tag  
 aus Frankfurt. Bis 95 %  
 gntiger als auf dem Markt.

Arbeitshandschuhe und  
 Vieles mehr.

Info auf: folmax.pw

Mit freundlichen Gr

**Zustimmung:** Aktiviert

Die Blackliste wird in der Datei „\_blacklist.txt“ geführt.

Dateiname	Dateigröße	Dateityp
_blacklist.txt	58	Text-Qu
_COPYRIGHT.TXT	1.514	Text-Qu
_version.txt	1.276	Text-Qu

Die Datei enthält die Begriffe, nach denen gefiltert wird. Pro Zeile ein Begriff:

```

_blacklist.txt
1 buy levitra
2 canadian online pharmacy
3 cialis
4 levitra
5 viagra
6 omasex
7 pricelevitra
8 hottier

```

Wir selbst pflegen und aktualisieren eine vorgefertigte Blackliste mit jeweils den aktuellen Spambegriffen. Diese können Sie von folgender Adresse herunterladen:

<https://ekiwi-scripts.de/antispam/spam.php>

Automatische Aktualisierung der Blackliste

Über die Datei „update\_blacklist.php“ können Sie die Blackliste auch automatisch von unserem Server aktualisieren. Bearbeiten Sie die Datei zuerst mit einem Texteditor und geben Sie ein zufälliges Secret ein.

```

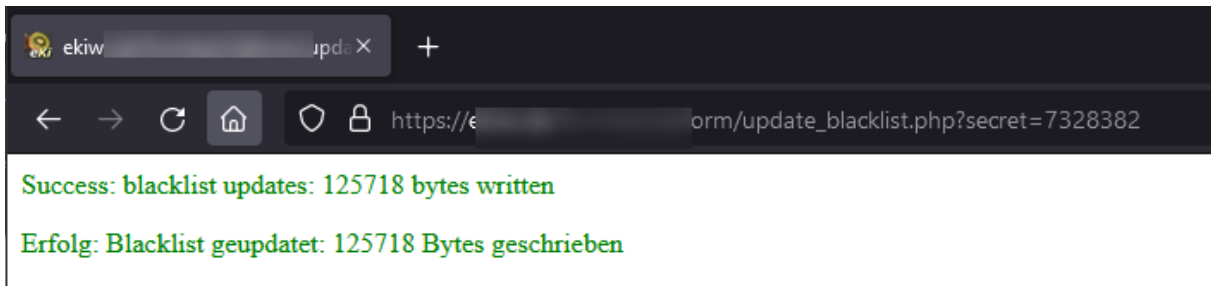
24
25 //please change the secret - example: $secret = "4324324325";
26 //das Secret bitte abändern - Beispiel: $secret = "4324324325";
27 $secret = "|";
28
29 //for more changes

```

Aus Sicherheitsgründen muss dieses beim Aufruf der Seite als Parameter mit übergeben werden:

[https://ihrserver.de/formmail\\_v4/update\\_blacklist.php?secret=444555](https://ihrserver.de/formmail_v4/update_blacklist.php?secret=444555)

Die Datei „\_blacklist.php“ müssen vorher Schreibrechte zugewiesen werden. Rufen Sie die Datei im Browser auf, die Blackliste wird nun heruntergeladen und installiert.



Für eine automatische Aktualisierung können Sie auch einen Cron-Job einrichten.

**Hinweis:** Beim automatischen Update wird die Datei bei jedem Update überschrieben. Falls Sie zusätzlich eine eigene Blackliste parallel pflegen wollen, können Sie die Datei „\_blacklist\_user.txt“ verwenden.

## Link-Spam

Spammer möchten, dass man eine Webseite besucht. Daher kommen oft viele Links in Spammnachrichten vor. Das Script prüft daher, ob überdurchschnittliche viele Links vorkommen.

### Beispiel für Link-Spam:

**Datum:**  
**Name:** BrunetteBabelaw  
**Telefon:** 84644476285  
**eMail:** tuftoncar@gmail.com  
**AnmerkungenWuensche:** <http://knowledge.skem>  
[cidReq=MIBGM145&link\\_](http://cidReq=MIBGM145&link_)  
<http://apps.tacoma.uw>  
<https://clubs.london.ed>  
<0050569d64d5&r=https>  
<https://brunette.pro ht>  
<example=SimpleForm&ui>  
<http://www.vlatkovic.n>  
<http://hanoimuare.com/>  
<http://www.allmon.biz/>  
<https://www.creadrean>  
<http://clipart.disneysite>  
<bannerid=232&zoneid=0>  
<http://www.kimoi.us/>

## HTML-Spam

HTML-Spam geht in die gleiche Richtung. Oft werden HTML-Tags in das Formular eingebaut, so dass z. B. ein anklickbarer Link in der E-Mail entsteht.

### Beispiel für HTML-Spam:

## ***Kontaktformular***

Sie haben eine Nachricht von KaryORigh aus KaryORigh erhalten.  
 Folgende Nachricht wurde hinterlassen:  
 Ferienhaus

Osimert (ÐÑÐ\_Ð¼ÑÑÐ\_Ð½Ð\_Ð± 80 Ð¼Ð³) -  
 ÐÑÐ\_Ð¼ÑÑ (Osimertinib) â ÐÐÐÐ«Ð Ð°Ð½Ð°  
 Ð»Ð¼³ Tagrisso/Ð¢Ð°ÑÑÑ¼  
 Osimert (ÐÑÐ\_Ð¼ÑÑÐ\_Ð½Ð\_Ð± 80 Ð¼Ð³) -  
 ÐÑÐ\_Ð¼ÑÑ (Osimertinib) â Ð»Ð¼Ð°ÑÑÑ²Ð¼,  
 Ð½Ð°Ð²Ð°ÑÑÐ²»Ð¼Ð½Ð½Ð¼Ð¼ Ð½Ð°  
 Ð±¼ÑÑÑÑÑÑÑÑÑÑ¼Ð²Ñ¼Ð, Ð°Ð»Ð¼ÑÐ°  
 Ð¼Ð, Ð² Ð¼Ð³Ð°ÑÑÑÑÑÑÑÑÑÑ¼ÑÑÑÑ¼ÑÑ¼

## Captcha Überprüfung

Neben der Eingabe des Captchas, wird auch die Zeit geprüft, in welcher das Formular ausgefüllt wird. Spambots füllen automatisiert das Formular aus und senden es umgehend ab. Wird das Formular in unter 3 Sekunden abgesendet, wird es als Spam gewertet.

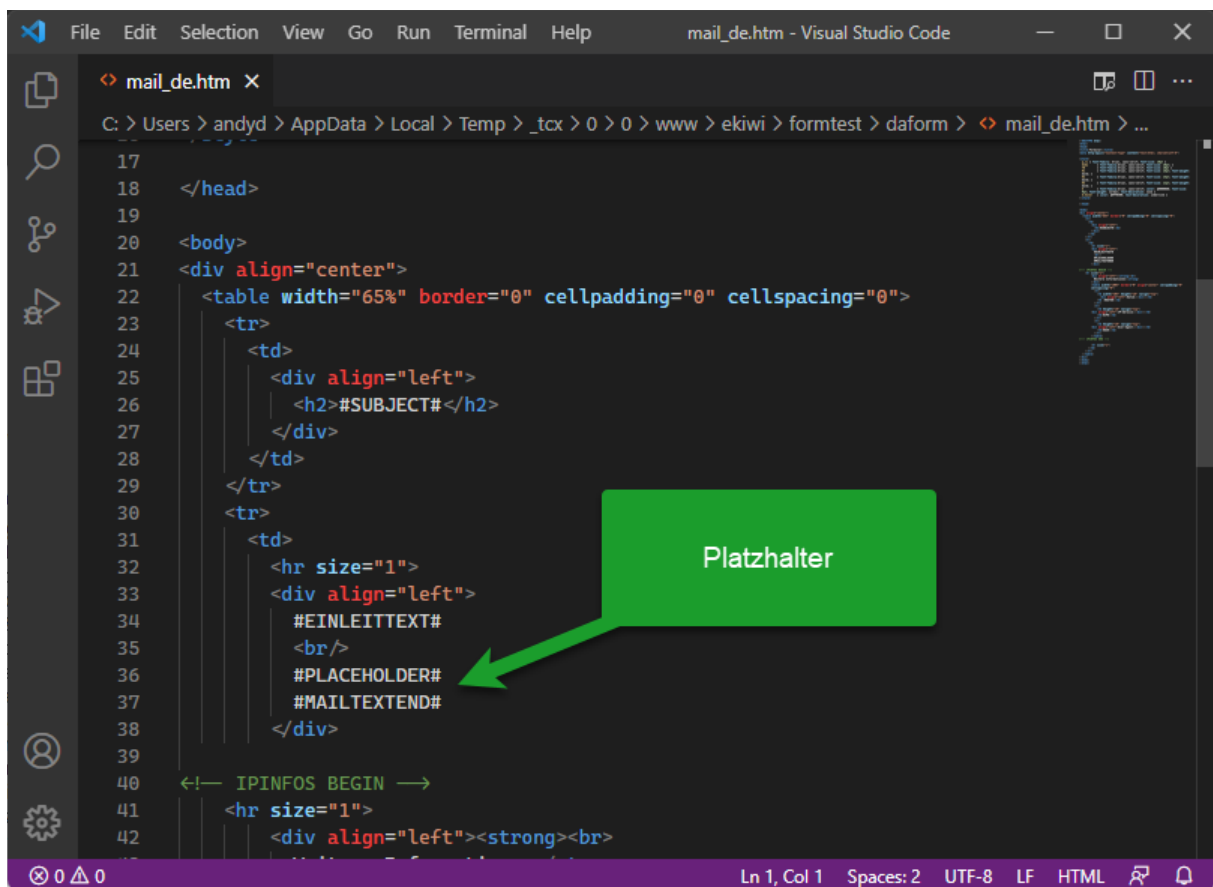
## Anpassung der E-Mail-Vorlage

Das Script enthält Vorlagendateien, welche für die E-Mails verwendet werden:

iplock.txt	0	Text-Quell...	02.1
mail.htt	76	HTT-Datei	01.1
mail_de.htm	1.967	Firefox HT...	22.1
mail_de_pdf.htm	3.058	Firefox HT...	22.1
mail_en.htm	1.957	Firefox HT...	22.1
mail_en_pdf.htm	3.052	Firefox HT...	22.1
refresh.png	3.001	Firefox HT...	01.1

Die „mail.htt“ wird für Textmails verwendet. Die .htm Dateien werden für den Versand von HTML-Mails verwendet, bzw. für die Erstellung des PDF-Dokuments.

Bitte beachten Sie, dass die Platzhalter weiterhin vorhanden sind, damit die E-Mails / PDF richtig erzeugt werden.



```

17
18 </head>
19
20 <body>
21 <div align="center">
22 <table width="65%" border="0" cellpadding="0" cellspacing="0">
23 <tr>
24 <td>
25 <div align="left">
26 <h2>#SUBJECT#</h2>
27 </div>
28 </td>
29 </tr>
30 <tr>
31 <td>
32 <hr size="1">
33 <div align="left">
34 #EINLEITTEXT#
35 <br />
36 #PLACEHOLDER#
37 #MAILTEXTEND#
38 </div>
39
40 <!-- IPINFOS BEGIN -->
41 <hr size="1">
42 <div align="left"><strong><br>

```