

Anforderungen an die zu entwickelnde Software.

Die zu entwickelnde Software muss folgenden Anforderungen entsprechen: Sie muss interaktiv nutzbar, leicht verständlich, kostengünstig und laufzeiteffizient sein und zudem auf allen Plattformen laufen. Eine interaktiv nutzbare Anwendung bezieht den User möglichst stark mit ein. Dadurch soll eine persönliche Identifizierung mit der Anwendung geschaffen werden, die dem Nutzer ein positives Erlebnis bereitet. Außerdem sollte die Software den Nutzer durch die einzelnen Anwendungsschritte leiten, ohne dass sich der Nutzer bevormundet fühlt. Dadurch soll ein Spaßfaktor geschaffen werden. Dieses führt wiederum dazu, dass die Anwendung weiterempfohlen und stärker frequentiert wird, was eine höhere Anzahl an Einträgen nach sich zieht. Die Anwendung sollte für möglichst alle Benutzer zugänglich gemacht werden. Hierzu ist es notwendig, dass sie auf den wichtigsten Plattformen läuft. Außerdem sollte es angestrebt werden, möglichst kostengünstig zu arbeiten, sowohl in der Entwicklung als auch im späteren Betrieb. Dies könnte durch die Verwendung von Open-Source Software erreicht werden. Eine Möglichkeit der Erfolgsmessung sollte in Form von Benutzerstatistiken geschaffen werden, damit man später um Werbepartner buhlen kann.

Schutz vor unerwünschten Einträgen und Mails.

Die Anwendung sollte außerdem über wirksame Schutzmechanismen gegen unerwünschte Einträge verfügen. Diese Einträge, welche auch als Spam bezeichnet werden, sind vom Betreiber der Internetseite so nicht gewünscht und vorgesehen. Mittlerweile gibt sogar automatische Programme, die dazu da sind Spam zu produzieren und diesen auf Webseiten und in Foren verbreiten. Außerdem durchsuchen diese so genannten Spam-Bots alle auffindbaren Seiten nach lesbaren E-Mail-Adressen, und bombardieren diese anschließend mit so genannten Spam-Mails. Einige Techniken, um Spam so gering wie möglich zu halten werden auf den nächsten Seiten abgehandelt werden.

Schutz vor Spam-Bots.

Der frei erhältliche, bewährte und sehr beliebte Apache Web-Server bietet verschiedene Erweiterungen. Mod-Rewrite¹ ist eine dieser Erweiterungen und kann für verschiedene Zwecke eingesetzt werden. Eine häufige Verwendung ist es, bei unterschiedlichen Domainnamen für eine Seite den Client umzuleiten. Dies ist vor allem für die Suchmaschinenoptimierung wichtig. Mehr dazu in Kapitel 4.10. Mod-Rewrite liest, unter anderem, von jedem Besucher der Seite die IP-Adresse und den sogenannten „HTTP_USER_AGENT“² aus. Dadurch lassen sich bestimmte IP-Adressen und HTTP_USER_AGENT's aussperren. Dies lässt sich auch mit Spam-Bots machen. Es gibt Listen³ bekannter Spam-Bots, welche automatisch eingebunden werden können. Diese Listen sind zwar nicht top-aktuell, doch bieten sie einen guten Schutz vor bereits bekannten Spam-Bots. Hierbei sollte man aber darauf achten, dass man nicht versehentlich einen der Suchmaschinen-Bots aussperrt.

Eine weitere Möglichkeit, um eine Anwendung im Internet vor unerwünschten Einträgen durch Spam-Bots zu schützen, ist das sogenannte Captcha-Verfahren.⁴ Dabei wird dem Benutzer eine sehr einfach zu lösende Frage gestellt, welche dieser beantworten muss. Für Menschen sind diese Fragen einfach zu lösen, für Computer hingegen nicht. Diese Fragen

¹ Vergleiche: <http://www.modrewrite.de>. Datum: 17.09.2008.

² Das Programm des Clients. Vergleich: http://de.wikipedia.org/wiki/User_Agent. Datum: 17.09.2008.

³ Vergleiche: http://www.spywareinfo.com/harvest_project/spambots.txt. Datum: 17.09.2008.

⁴ Vergleiche: <http://de.wikipedia.org/wiki/Captcha>. Datum: 17.09.2008.

können einfache Rechenaufgaben sein, aber auch zufallsgenerierte Bilder, welche eine kurze Zeichenkette enthalten. Zum Beispiel „E1gY3m“. Diese Zeichenkette muss der Benutzer eingeben und bestätigen. Dadurch „weiß“ die Anwendung, dass ein menschlicher Benutzer vor dem Rechner sitzt. Da dieses Verfahren allerdings seit einigen Jahren sehr bekannt und beliebt ist, bietet es lange nicht mehr den Schutz, den es einmal bot. Mittlerweile verfügen Spam-Bots über die Möglichkeit Texterkennung zu verwenden und so den Captcha-Code zu „knacken“. Dies kann durch animierte Grafiken erschwert werden, oder aber durch immer schlechter lesbare Captcha-Grafiken, was auch den Benutzer ärgert, weil er oft mehrere Versuche benötigt, um den richtigen Code einzugeben. Ein weiteres Problem stellt sich, wenn der Benutzer sehbehindert oder gar taubblind ist. Diese Benutzer können diesen Anwendungsschritt nicht erfolgreich absolvieren.⁵

Eine barrierefreie⁶ Möglichkeit, um Spam-Bots auszutricksen, ist es, bei HTML-Formularen unsichtbare Felder einzutragen, welche der Benutzer nicht sehen kann. Diese werden durch ein CSS-Element⁷ versteckt. Da Spam-Bots nicht darauf geschult sind, dies zu erkennen, füllen sie dieses Feld aus. Wird nun ein solches, für einen Benutzer nicht sichtbares Feld ausgefüllt, ist der Anwendung klar, dass es sich dabei um einen Spam-Bot handeln muss. Dessen Benutzer und IP-Adresse können nun ausgeschlossen werden.⁸

Eine weitere barrierefreie Methode gegen Spam-Bots ist es, die Anwendung prüfen zu lassen, wie lange der Benutzer braucht, um ein Formular auszufüllen. Benötigt er weniger als fünf Sekunden für zehn Felder, so ist etwas faul. Das kann kein Mensch sein.⁹ Hierdurch lässt sich auch ein Bot aussperren. Eine weitere Möglichkeit ist, es den eingegebenen Inhalt mittels einer „bad word list“¹⁰ auszufiltern. Gibt der Benutzer beispielsweise Wörter wie „Sex“, „Porn“, „Viagra“ ein, so weiß die Anwendung mittels hinterlegter bad word list, dass es sich um einen ungewünschten Eintrag handelt und dieser ausgefiltert werden muss.

Des Weiteren sollten alle auftauchenden E-Mail-Adressen für Spam-Bots unsichtbar gemacht werden, da diese gern von allen durchsuchten Seiten die lesbaren E-Mail-Adressen speichern und anschließend mit ungewollten E-Mails bombardieren. Auch zum Selbstschutz sollte der Webseitenbetreiber versuchen, alle auftauchenden E-Mail-Adressen zu verschlüsseln. Gar keine E-Mail-Adresse anzugeben ist nicht möglich, da das Impressum die Angabe einer E-Mail-Adresse verlangt. Ein Vorteil beim Kampf gegen Spam-Bots ist, dass diese unfähig sind, Javascript-Code auszuführen. Um nun eine E-Mail-Adresse zu verschlüsseln, zerlegt man diese in mindestens zwei Bestandteile. Beim Aufruf der Seite wird dann durch einen Javascript-Aufruf die E-Mail-Adresse wieder zusammengesetzt.¹¹

Bestätigung des Eintrags durch Validierung der E-Mail-Adresse.

Eine weitere Möglichkeit Spameinträge zu verhindern ist die Bestätigung des Eintrags durch Prüfung der E-Mail-Adresse des Benutzers. Hierbei können ungewollte Einträge, wie aufgesprochene Fäkalausdrücke, ausgefiltert werden. Es wird angenommen, dass ein Benutzer, welcher „Schabernack“ treiben will, eine falsche E-Mail-Adresse hinterlegen wird.

⁵ Vergleiche: <http://www.1ngo.de/web/captcha-spam.html>. Datum: 17.09.2008.

⁶ Gestaltung von Inhalten, so dass sie von jedem genutzt und gelesen werden können. Vergleiche: <http://www.barrierefreies-webdesign.de/>. Datum: 17.09.2008.

⁷ Cascading Style Sheets (CSS) ist eine beschreibende Sprache für Dokumente wie zum Beispiel HTML-Dokumente. Darin werden Informationen über Formatierung und Aussehen einzelner Elemente deklariert. Vergleiche: http://de.wikipedia.org/wiki/Cascading_Style_Sheets. Datum: 17.09.2008.

⁸ Vergleiche: <http://www.1ngo.de/web/captcha-spam.html>. Datum: 17.09.2008.

⁹ Vergleiche: <http://www.1ngo.de/web/captcha-spam.html>. Datum: 17.09.2008.

¹⁰ Liste von ungewollten Wörtern.

¹¹ Vergleiche: http://www.drweb.de/email/email_verschluesseln_Javascript.shtml. Datum: 17.09.2008.

Aus diesem Grund wurde eine E-Mail-Prüfung eingebaut. Der Benutzer bekommt nach erfolgreicher Erstellung seines Eintrages eine E-Mail zugeschickt. Diese E-Mail beinhaltet einen Aktivierungs-Link, welchen der Benutzer aufrufen muss. Erst dadurch wird der Eintrag freigeschaltet und ist für alle Benutzer sichtbar. Ein Problem ist hierbei, dass die E-Mail mit dem Aktivierungs-Link im Spam Ordner des E-Mail Postfaches landen könnte und so der Benutzer den Beitrag nie bestätigt. Durch aktives Hinweisen in der Anwendung auf die Aktivierungs-Mail kann dem aber entgegen gewirkt werden.

Prüfung des Eintrags durch den Administrator.

Um letztendlich 100-prozentig sicher zu gehen, dass es sich bei dem Eintrag um einen Echten und Vertretbaren handelt, wird nach der E-Mail-Bestätigung durch den Benutzer der Eintrag von einem Administrator oder einer Administratorgruppe geprüft. Diese bekommen eine E-Mail, in der sie darauf hingewiesen werden, dass ein neuer Eintrag erstellt wurde und sie diesen prüfen müssen. Hierfür gehen die Administratoren in das Eintrag-prüfen-Modul der Anwendung und bekommen dort alle ungeprüften Einträge angezeigt. Ungewollte Einträge können so ausgefiltert werden. Hierdurch wird auch der Nachteil, dass die E-Mails beim Benutzer nicht angekommen sind, wieder ausgeglichen, da der Administrator erkennt, ob es sich um einen ernsthaften Eintrag handelt oder nicht. Allerdings kostet diese Art der Spam-Vermeidung viel Zeit und Geld.

Letztendlich geeignet für die Vermeidung von Spam-Einträgen sind all diese Verfahren. Doch scheint es am sinnvollsten zu sein, eine Mischung aus allen Möglichkeiten einzusetzen. Das macht deswegen den meisten Sinn, weil dadurch die Kosten für Administratoren gering gehalten werden können und die Benutzer der Seite nur wirklich sinnvolle Beiträge präsentiert bekommen.