Diplomarbeit

iCal Web-Service

Wagner Dario Stering Marcel Franz Matthias

8. 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

Danksagung

1 Projektmanagement und Organisation

1.1 Team

Dario Wagner

Verantwortlich für:

- Parser
- iCal

Marcel Stering

Verantwortlich für:

- Security
- Webseite

Matthias Franz

Verwantwortlich 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 Schewiz. Unsere Ansprechpartner waren Rudolf Rauch und Mathias Schober. Intact bietet maßgeschneiderte Softwarelösungen und standartisierte. Intacts bekantestes 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.

2 Webseite

2.1 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.

2.1.1 Login Handling

2.1.2 Absicherung

2.1.3 Two-Factor-Auth

2.1.4 XSS Protection

2.1.5 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 bösartigen 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 bösartiges Skript zu platzieren, welches dann von einem nichts ahnenden User aufgerufen wird.

2.1.6 XSS Targets:

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

2.1.7 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.

2.1.8 Beliebte Angriffsvektoren

1. Session Hijacking
2. Website-Defacements

3. Phishing

2.1.9 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.

2.1.10 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.

2.1.11 Phishing

2.1.12 Cross-Site-Tracing

2.1.13 XSRF/CSRF Protection

2.1.14 Sql-Injection Protection

2.1.15 Password Hashes

2.2 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.

2.2.1 Allgemeines MVC

2.2.2 Aufbau der Webseite

2.2.3 Link generation

2.2.4 Controller

2.2.5 Views

2.2.6 Services

2.2.7 User Datenbank

- Salt