1 Webseite

1.1 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.

1.1.1 Login Handling

1.1.2 Absicherung

1.1.3 Two-Factor-Auth

1.1.4 XSS Protection

1.1.5 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.

1.1.6 XSS Targets:

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

1.1.7 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.

1.1.8 Beliebte Angriffsvektoren

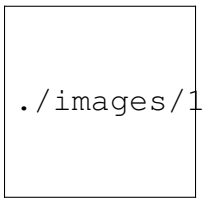
1. Session Hijacking
2. Website-Defacements

3. Phishing

1.1.9 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.

1.1.10 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. 

1.1.11 Phishing

1.1.12 Cross-Site-Tracing

1.1.13 XSRF/CSRF Protection

1.1.14 Sql-Injection Protection

1.1.15 Password Hashes

1.2 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.

1.2.1 Allgemeines MVC

1.2.2 Aufbau der Webseite

1.2.3 Link generation

1.2.4 Controller

1.2.5 Views

1.2.6 Services

1.2.7 User Datenbank

- Salt