**Using Components with known Vunerabilities**

Bei diesem Angriff werden bekannte Fehler in Bibliotheken ausgenutzt, um Zugriff auf ein System zu bekommen. Ein Beispiel für so einen Fehler in einer Bibliothek ist das Exploit Framework. Diese Bibliothek wird dazu benutzt, um Objekte zu lesen und diese wie eine Anwendung behandeln zu können.

Nutzer installiert oder implementiert das Exploit Framework. Der Hacker kennt den Fehler, der in dem Exploit Framework eingebaut ist und schaltet sich in das Programm. Er nutzt den Fehler aus, damit er vollen Zugriff auf das Programm bekommt, ohne Berechtigung erlangen zu müssen. Mit dem vollen Zugriff kann er beliebigen Code auf dem System des Nutzers ausführen und machen auf dem System machen, was er möchte.

Schutzmaßnahmen: Der Nutzer soll beim Programmieren darauf achten, dass er ungenutzte Abhängigkeiten löscht, damit er nicht solche Opfer solcher bekannten Fehler wird. Zudem muss er darauf achten, dass die Versionen der Komponenten serverseitig, sowie benutzerseitig immer auf dem neusten Stand sind, damit bekannte Fehler, die von den Entwicklern entdeckt und behoben wurden, nicht weiterhin benutzt werden. Zudem sollten benutzte Komponenten nur von offiziellen Quellen kommen, die auch zertifiziert sind, da diese wenige bekannte Fehler haben und ebenfalls, wenn neue bekannt werden, schnell behoben werden

**Insufficient Logging & Monitoring**

Bei Insufficient Logging & Monitoring geht es darum, dass nicht ausreichend Protokolliert wird und ein Hacker kann dies ausnutzen.

Ein Angreifer lässt ein Skript laufen, dass für jeden Benutzer ein übliches Passwort wie „123456789 prüft. Der Angreifer bekommt dann alle Benutzer, die dieses Passwort benutzen und hat somit Zugriff auf diesen Benutzer. Durch die nicht ausreichende Protokollierung bleibt für die restlichen Benutzer nur ein falscher Loginversuch. Ein paar Tage später kann der Angreifer, dass gleiche Skript mit einem anderen Passwort laufen lassen und weitere Benutzer erhalten. Der Angreifer kann dies durch die nicht vorhandene Protokollierung wiederholen.

Zum Schutz sollten die Programmierer fehlgeschlagene Anmeldeversuche oder Eingabefehler protokollieren. Diese Protokolle können genutzt werden für Analysen, um regelmäßige fehlgeschlagene Anmeldeversuche zu erkennen und die Benutzer zu warnen oder weitere Kontrollen zu programmieren.