Semesterprüfung APSI 2019, FHNW 16.12.2019

Dozenten: Dr. Arno Wagner, Dr. Michael Schläpfer

Kandidat

Name: _____

Vorname: _____

Studentennummer: _____

Aufgabe	1	2	3	4	5	6	7	Σ
Maximalpunkte	15	9	9	12	8	9	11	73
Erreichte Punkte								

Note: _____

1 Aufgabe: Vermischte Fragen (15 P)

1.1 OS Schutz (2 P)

Ist bei einem System mit nur einem Benutzer eine Trennung zwischen ”user”-Mode und ”root”-Mode noch sinnvoll? Warum/warum nicht?

1.2 Java (2 P)

Wenn sie in Java programmieren, sind sie dann prinzipiell sicher vor Buffer-Overflows? Begrüenden sie warum, oder geben sie 2 Beispiele an wo dies nicht gegeben ist.

1.3 Zufallserzeugung (2 P)

Nehmen Sie an, Sie haben einen Hardware-Zufallsgenerator mit einem kompromittierten Design (z.B. Intel RDRAND) zur Verfügung. Können Sie diesen trotzdem sinnvoll und sicher einsetzen? Wie geht das, bzw. warum geht das nicht?

1.4 Testen von Sicherheit (2 P)

Ist ein Pen-Test ausreichend um die Sicherheit einer Server-Software zu beurteilen? Warum, bzw. warum nicht?

1.5 Logging (2 P)

Nehemen Sie an, Sie konfigurieren das Logging für einen Web-Shop. Spielt der Preis der Einkäufe eine Rolle für das Loggen zum Zweck der Angriffserkennung? Warum, bzw. warum nicht?

1.6 HTTP GET vs. POST Parameter (2 P)

Welcher Unterschied ergibt sich bei der Parameterübergabe aus Benutzersicht? Hat dies Auswirkungen auf die Sicherheit?

1.7 CSRF (3 P)

Was ist ein CSRF Token (Synchronizer Token), und wie wird es eingesetzt? Warum kann damit CRSF verhindert werden?

2 Aufgabe: Privilege-Separation (10 P)

2.1 Libraries (3 P)

Nehemen Sie an, Sie muessen eine bestimmte Library benutzen. Leider hat der Maintainer beschlossen jetzt Surflehrer auf Hawaii zu sein und Source-Code ist auch keiner verfügbar. Diese Library hat jetzt einen bekannten Buffer-Overflow in einem bestimmten Aufruf. Wie gehen Sie mit diesem Problem sinnvollerweise um?

2.2 Libraries (2 P)

Welche weiteren Massnahmen sind in der Situation aus der letzten Teilaufgabe sinnvoll?

2.3 Input Validation (4 P)

Geben Sie Pseudo-Code füer die Validierung der Folgenden Eingabe an: Eine Liste von ganzen Zahlen, Komma-separiert, mit optionalem Whitespace.
Beispiel: `[1, 28,501234 ,-3, 42 ]`

3 Aufgabe: Passworte (9 P)

Wo nicht anders angegeben, gilt für diese Aufgabe, dass Argon2 mit standard-Parametern und 1 sec Iterationszeit benutzt wird. Geben Sie alle Berechnungen an.

3.1 Entropie (3 P)

Nehmen Sie an, Passworte bestehen aus 10 zufaelligen Ziffern und Kleinbuchstaben. Berechnen Sie die Entropie eines Passwortes.

3.2 Entropie (4 P)

Es werden nun Passworte wie in der letzten Teilaufgabe eingesetzt. Als Eingabehilfe darf aber nun 1 Zeichen falsch eigegeben werden. (Zur Vereinfachung geben die Benutzer auch immer genau 1 Zeichen falsch ein.) Berechnen Sie die Entropie der Passworte in dieser Situation.

3.3 Entropie (2 P)

Wie legen Sie die Passworte bei der Situation aus der letzten Teilaufgabe trotzdem sicher in eine Datenbank ab?

4 Aufgabe: Web-Application Security (12 P)

4.1 Cookies (2 P)

Müssen zum sicheren Betrieb einer Web-Applikation alle Cookies geschützt werden oder nur bestimmte? Begründen Sie Ihre Antwort.

4.2 Cookies (2 P)

Können Sie sicherstellen, daß ein gesetzter Cookie auch wieder an den Server geschickt wird? Wie, bzw. warum geht das nicht?

4.3 Cookies (2 P)

Wenn ein Cookie mit ”HttpOnly” gesetzt wird, wo findet Authorization statt und wo Access Control?

4.4 Ausführungsumgebung (3 P)

Bei einer Web-Applikation mit Client-seitigem JavaScript Code haben Sie keine Kontrolle über die Ausführungsumgebung (Browser). Was sind die Implikationen für die Applikationssicherheit?

4.5 Ausführungsumgebung (3 P)

Können Sie Daten, die der Benutzer nicht sehen oder verändern darf sicher und zuverlässig im Webbrowser-State (als auf Client Seite) abspeichern? Wie geht das und wo sind die Grenzen?

5 Aufgabe: Web-Application Sicherheit, OWASP (8 P)

5.1 Same-Origin Policy (2 P)

Welchem Zweck dient die ”Same Origin Policy” in Web-Browsern und welche Art von Angriff währe ohne sie möglich?

5.2 Risk-Ratings - Verteidiger(2 P)

Der OWASP Katalog klassifiziert Risiken für die verschiedenen Verwundbarkeitsklassen (Gelb-Orange-Rot-Violett). Wofür können Sie diese Klassifikation praktisch benutzen wenn sie selber eine Web-Applikation schreiben?

5.3 Risk-Ratings - Angreifer (2+2 P)

Für welche Art von Angriffen sind Verwundbarkeiten interessant, die schwer auszunutzen sind (Exploitability), aber dem Angreifer grossen Zugriff verschaffen (Impact)? Mit Begründung.

Für welche Art von Angriffen sind Verwundbarkeiten interessant, die einfach zu finden (Prevalence), einfach zu erkennen (Detectability) und einfach auszunutzen (Exploitability) sind, aber relativ wenig Zugriff erlauben (Impact)? Mit Begründung.

6 Aufgabe: Public Key Cryptography und JWT (9 P)

6.1 Symmetrisch vs. asymmetrisch (3 P)

Fast alle gängigen Verschlüsselungsverfahren heute sind hybrid, d.h. die eigentlichen Daten werden symmetrisch verschlüsselt, während der symmetrische Schlüssel dann in einem asymmetrischen Verfahren, also mit einem öffentlichen Schlüssel, verschlüsselt wird. Weshalb wird nicht alles einfach nur symmetrisch oder nur asymmetrisch verschlüsselt? Welche Problemstellungen werden durch die unterschiedlichen Verfahren gelöst?

6.2 Zertifikate (2 P)

Was ist im Zusammenhang mit Public Key Cryptography ein Zertifikat? Was beinhaltet es und wofür wird es benötigt?

6.3 Trust (2 P)

Wenn Sie die Webseite der Bank Ihres Vertrauens besuchen, zeigt Ihnen Ihr Browser an, dass es sich um eine ”sichere” Verbindung handelt (z.B. grünes Schloss). Was sind die Grundvoraussetzungen hierfür, wie weiss der Browser das? Welche Sicherheitsgarantien haben Sie als Benutzer, wenn der Browser eine sichere Verbindung zu Ihrer Bank anzeigt?

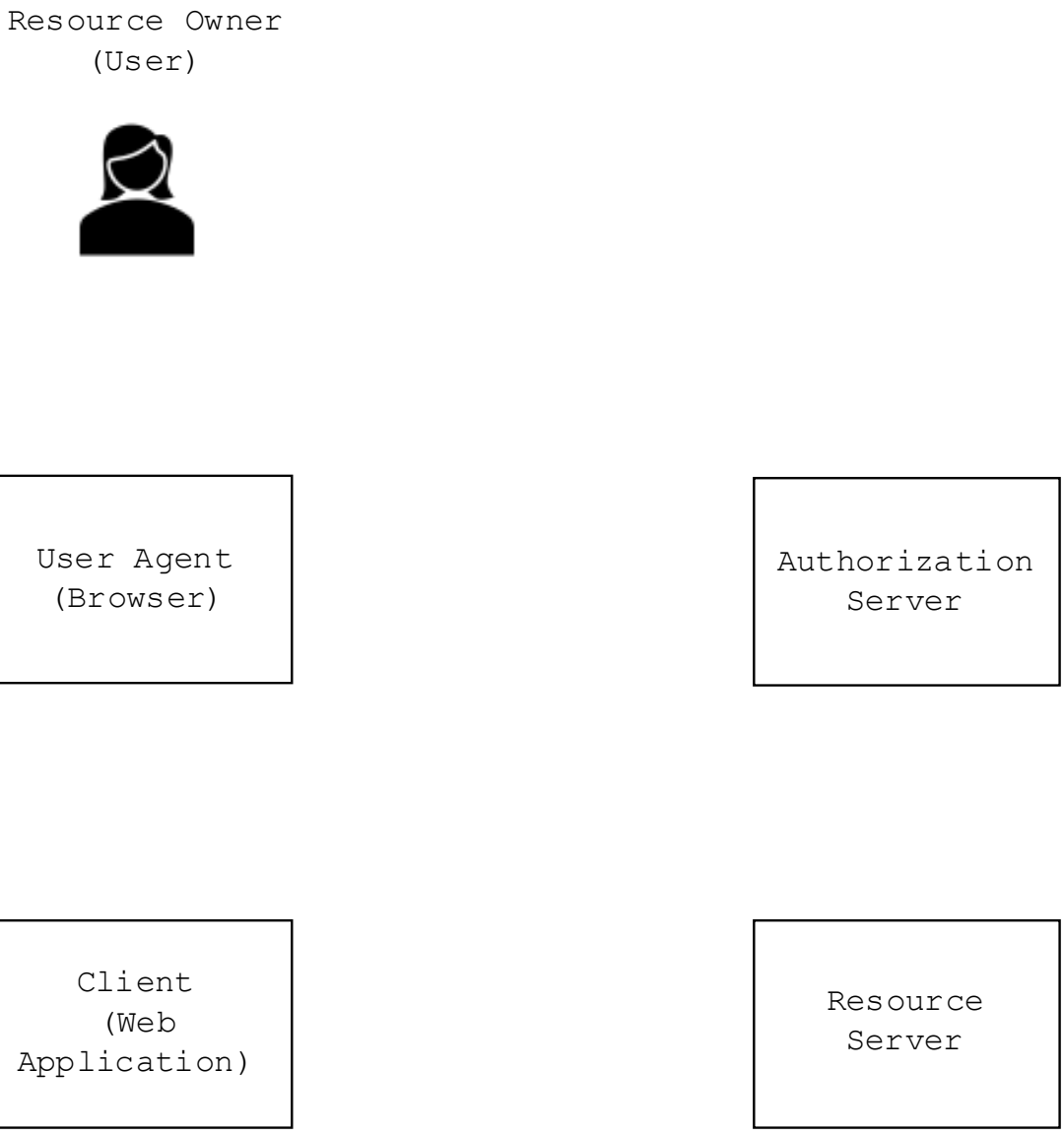
6.4 JWT (2 P)

JSON Web Tokens werden heute vielerorts eingesetzt um, unter anderem, Benutzerinformationen zu übertragen. Wie ist ein JWT aufgebaut? Worauf müssen Sie achten, damit ein Angreifer nicht die Informationen im Payload verändern kann?

7 Aufgabe: Authorization & Identity Federation (11 P)

7.1 OAuth 2.0 (4 P)

Die nachfolgende Abbildung zeigt die wesentlichen Komponenten beim Ablauf einer Autorisierung mittels OAuth 2.0 Protokoll. Dabei versucht der Client (Web Application) auf Ressourcen zuzugreifen, welche auf dem Resource Server liegen.



Zeichnen Sie in der Abbildung oben mittels nummerierten Pfeilen den Ablauf des Protokolls ein.

Listen Sie nachfolgend für die einzelnen Teilschritte auf, welche Nachrichten ausgetauscht werden.

7.2 Angriffe auf OAuth 2.0 (2 P)

Im Zusammenhang mit OAuth 2.0 wurden verschiedene Angriffe veröffentlicht. Einer dieser Angriffe ermöglicht es, die Antwort des Autorisierungs-Servers zu einem anderen Client, welcher unter Kontrolle des Angreifers ist, umzuleiten. Was kann der Angreifer nun machen? Wie könnte man sich gegen diesen Angriff schützen?

7.3 Identity Federation (2 P)

Was versteht man unter *Identity Federation* und wofür wird dies verwendet?

7.4 SAML 2.0 POST Binding vs. Artifact Binding (3 P)

SAML 2.0 ist der aktuell am weitesten verbreitete Standard für Identity Federation. In der Vorlesung wurden zwei *Bindings* vorgestellt, welche durch SAML 2.0 unterstützt werden. Dabei geht es um den Austausch der *SAML 2.0 Assertion* nach erfolgreicher Authentisierung. Was sind die Unterschiede von *POST Binding* und *Artifact Binding*? Nennen Sie je zwei Vor- und Nachteile.