1.1

a) Was ist das Hauptziel von CVE? Wie werden Verwundbarkeiten standardmäßig beschrieben? Wer ist Betreiber von CVE und welche Organisationen finanzieren das Projekt?

Betreiber

- Der Betreiber ist die Mitre Corporation, eine Non-Profit-Organisation, die aus Verschiedenen Forschungsinstituten besteht und sich aus einer Abspaltung vom MIT gebildet hat. Ihr „Auftraggeber“ sind die USA.
  Eines ihrer Institute ist z.B. das „Homeland Security Systems Engineering and Development Institute “.

Finanzierung

- Das CVE-Programm von der MITRE Corporation wird von der CISA (Cybersecurity and Infrastructure Security Agency) finanziert die dem bereits genanntem U.S. Department of Homeland Security.

b) Was umfasst NVD im Vergleich zu CVE und wie werden Verwundbarkeiten standardmäßig beschrieben? Wer ist Betreiber von NVD und welche Organisationen finanzieren das Projekt?

NVD

- NVD baut auf CVE auf und erweitert CVE um z.B. Analysen und Gegenmaßnahmen.
- NVD wird vom National Institute of Standards and Technology (NIST) betrieben und unter anderem von der US-Regierung finanziert.
- Beurteilt werden die Verwundbarkeiten mit Hilfe des Common Vulnerability Scoring System (CVSS), einem einheitlichen System für Beurteilung
- Weitere bereitgestellte Informationen sind:
  - Betroffene Software bzw. Versionen
  - Schweregrad
  - Auswirkungen
  - Gegenmaßnahmen

c)

nvd angegebener score: 7,5

d)

Was ist das Ziel von CWE?:

Häufig vorkommende schwachstellen zu vermeiden.
Sie bieten eine liste von den häufigsten schwachstellen für software firmware hardward und servies.

Wie werden Verwundbarkeitstypen standardmäßig beschrieben?:

Jede schwachstelle wird kategoresiert und hat jeweils folgende eigenschaften:
- WeaknessID
- Abstraktion Typ
- Struktur Typ
- Beschreibung

Und noch einige, die nicht immer auftauchen wie:
- Erweiterte beschreibung
- Alternativer Name
- Abhängigkeiten
- Beispiele

Wer ist Betreiber von CWE?

CWE wird von seiner communinty betrieben. Darunter gehören auch Apple, Intel und Microsoft

e) Was für ein Verwundbarkeitstyp ist Heartbleed laut CWE?

CWE-126: Buffer Over-read

- Entsteht, wenn eine Anwendung versucht, Daten von einem Puffer oder Speicherbereich zu lesen, der kleiner ist als die angeforderte Datenmen
- Führt dazu, dass die Anwendung auf Speicher zugreift, der außerhalb des zugewiesenen Bereichs liegt und möglicherweise Daten liest, die nicht für sie vorgesehen sind
- Kann zu unerwartetem Verhalten, einschließlich Abstürzen oder Sicherheitslücken führen

f) Lernen Sie weitere Details zu Heartbleed, bspw. hinsichtlich Gegenmaßnahmen, Exploits, betroffener Software und ähnlichen Verwundbarkeiten.

Betroffene Software: Heartbleed betraf die OpenSSL-Bibliothek, die von vielen Webservern, E-Mail-Servern, VPN-Gateways und anderen Netzwerkdiensten verwendet wird.

Gegenmaßnahmen:

- Als Unternehmen/Seitenbetriber: Um gegen Heartbleed geschützt zu sein, mussten betroffene Organisationen schnell reagieren, indem sie ihre OpenSSL-Versionen auf eine nicht anfällige Version aktualisierten.
- Als Entwickler: eine if-Abfrage

Exploits

- Entschlüsselung archivierter Daten
- Entschlüsselung während der Webserver-Verbindungsaufnahme
- Entschlüsselung der Verbindungsaufnahme an VoIP-Telefonen, Netzwerkdruckern und Routern

Ähnliche Schwachstellen, wie Heartbleed, die auf unsicheren Speicheroperationen beruhen:

- "Buffer Overflow"-Schwachstelle

    - Schwachstelle, die auftritt, wenn ein Programm versucht, mehr Daten in einen Puffer oder Speicherbereich zu schreiben, als dieser aufnehmen kann.
- "Catastrophic Backtracking" in OpenSSL (CVE-2015-0291),
    - ermöglichte Angreifern, den SSL-Server durch Senden eines speziell gestalteten Pakets zum Absturz zu bringen

1.2

a) Um welche Verwundbarkeit handelt es sich genau? Um welchen Verwundbarkeitstyp handelt es sich?

Die Schwachstelle mit der CVE-2017-5754 wird auch als Meltdown bezeichnet und betrifft Prozessoren von Intel sowie einige ARM- und IBM-Power-Prozessoren. Es handelt sich bei dieser Schwachstelle um eine Hardware-Schwachstelle, die aufgrund eines Designfehlers in der Prozessorarchitektur entstanden ist.

b) Was ist die Ursache der Verwundbarkeit und wie kann sie ausgenutzt werden?

Die Ursache für die Schwachstelle CVE-2017-5754, auch bekannt als Meltdown, liegt in der Art und Weise, wie moderne Prozessoren Speicherzugriffe optimieren, um eine höhere Leistung zu erzielen. Aufgrund dieser Optimierungen werden Speicherzugriffe teilweise vor der Berechtigungsprüfung durchgeführt, was es einem Angreifer ermöglicht, vertrauliche Informationen auszulesen, auf die er normalerweise keinen Zugriff hätte.

Ein Angreifer kann diese Schwachstelle ausnutzen, indem er einen speziell präparierten Programmcode ausführt, der es ihm erlaubt, den Inhalt des Speichers auszulesen, der normalerweise für andere Prozesse oder das Betriebssystem zugänglich ist. Durch die Ausnutzung dieser Schwachstelle kann ein Angreifer vertrauliche Informationen wie Passwörter, Kryptoschlüssel oder andere sensible Daten auslesen.

Es ist wichtig zu beachten, dass ein Angreifer bereits Zugriff auf das System haben und speziell präparierten Code ausführen muss, um diese Schwachstelle auszunutzen.

c) Welche Produkte sind von der Verwundbarkeit betroffen?

Die Schwachstelle betrifft hauptsächlich Prozessoren von Intel sowie einige ARM- und IBM-Power-Prozessoren, die seit 1995 entwickelt wurden. Die Schwachstelle wurde im Januar 2018 öffentlich bekannt gemacht und wurde als eine der schwersten Sicherheitslücken in der Geschichte der IT-Industrie eingestuft.

d) Welche Gegenmaßnahmen wurden ergriffen?

- Hardware-Hersteller haben Mikrocode-Updates und Firmware-Updates bereitgestellt, um die Anfälligkeit ihrer Chips gegenüber Meltdown zu verringern. Diese Updates beheben nicht den Designfehler, helfen jedoch dabei, die Auswirkungen der Verwundbarkeit zu begrenzen.
- Betriebssystemhersteller haben Sicherheitspatches und Updates veröffentlicht, um ihre Systeme gegen Meltdown zu schützen. Diese Updates beinhalten Kernel Page Table Isolation oder ähnliche Techniken, um den Kernel-Speicher vom Benutzerspeicher zu isolieren und so den Zugriff auf geschützte Speicherbereiche zu verhindern.

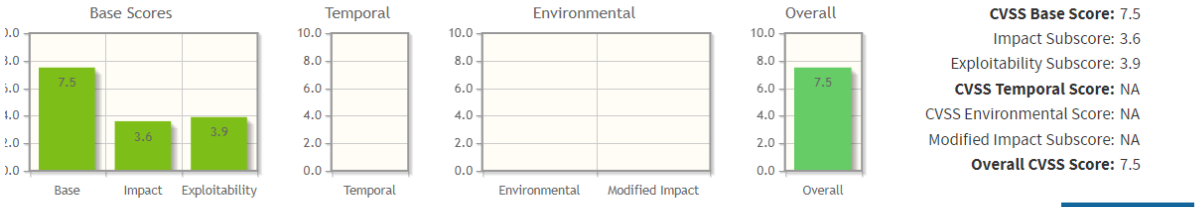
e)

Berechnen Sie den CVSS Score mit dem “Common Vulnerability Scoring System Calculator Version 3.1“. Welche qualitativen Unterschiede zum CVSS 3.1 Score von Heartbleed können Sie dabei feststellen?

Heartbleed:

Common Vulnerability Scoring System Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



CVSS Base Score: 7.5
Impact Subscore: 3.6
Exploitability Subscore: 3.9
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 7.5

Show Equations

CVSS v3.1 Vector
AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*
[Network (AV:N)] Adjacent Network (AV:A) Local (AV:L) Physical (AV:P)

Attack Complexity (AC)*
[Low (AC:L)] High (AC:H)

Privileges Required (PR)*
[None (PR:N)] Low (PR:L) High (PR:H)

User Interaction (UI)*
[None (UI:N)] Required (UI:R)

Scope (S)*
[Unchanged (S:U)] Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*
None (C:N) Low (C:L) [High (C:H)]

Integrity Impact (I)*
[None (I:N)] Low (I:L) High (I:H)

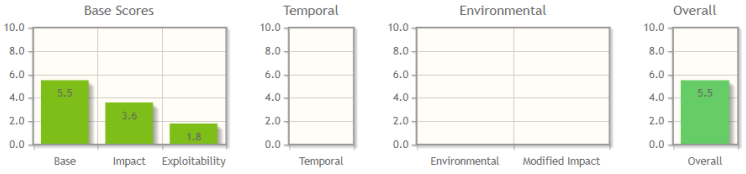
Availability Impact (A)*
[None (A:N)] Low (A:L) High (A:H)

* - All base metrics are required to generate a base score.

Meltdown:

Common Vulnerability Scoring System Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



CVSS Base Score: 5.5
Impact Subscore: 3.6
Exploitability Subscore: 1.8
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 5.5

Show Equations

CVSS v3.1 Vector
AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*
Network (AV:N) Adjacent Network (AV:A) [Local (AV:L)] Physical (AV:P)

Attack Complexity (AC)*
[Low (AC:L)] High (AC:H)

Privileges Required (PR)*
None (PR:N) [Low (PR:L)] High (PR:H)

User Interaction (UI)*
[None (UI:N)] Required (UI:R)

Scope (S)*
[Unchanged (S:U)] Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*
None (C:N) Low (C:L) [High (C:H)]

Integrity Impact (I)*
[None (I:N)] Low (I:L) High (I:H)

Availability Impact (A)*
[None (A:N)] Low (A:L) High (A:H)

Angriffsvektor

- Heartbleed: Über das Netzwerk
- Meltdown: Lokal

erforderliche Privilegien

- Meltdown erfordert niedrige Privilegien
- Heartbleed benötigt keine Privilegien

CVSS Score

- Meltdown: Base Score von 5.6(Medium)
- Heartbleed: Base Score von 7.5(High)

1.3

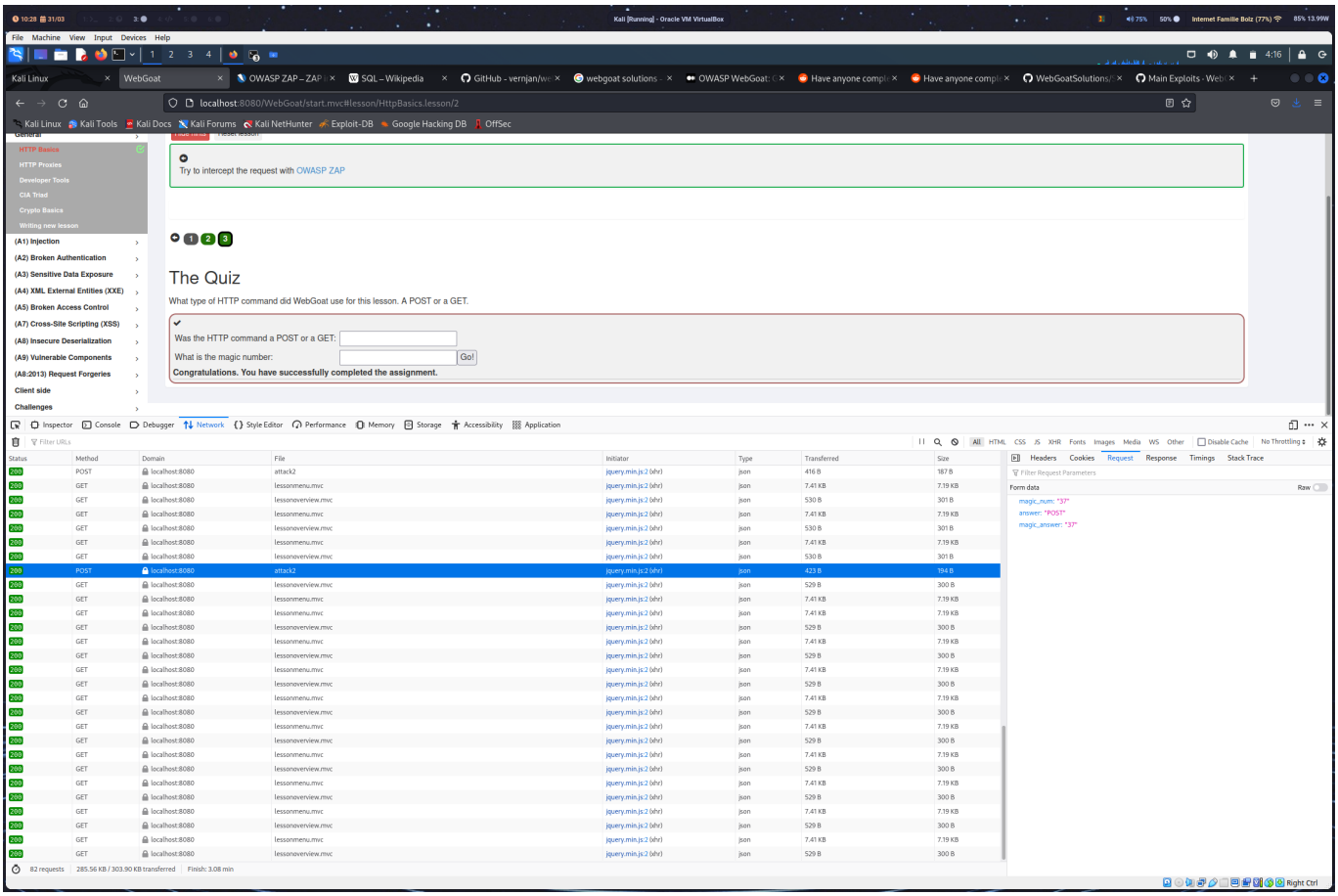
HTTP Basics

1

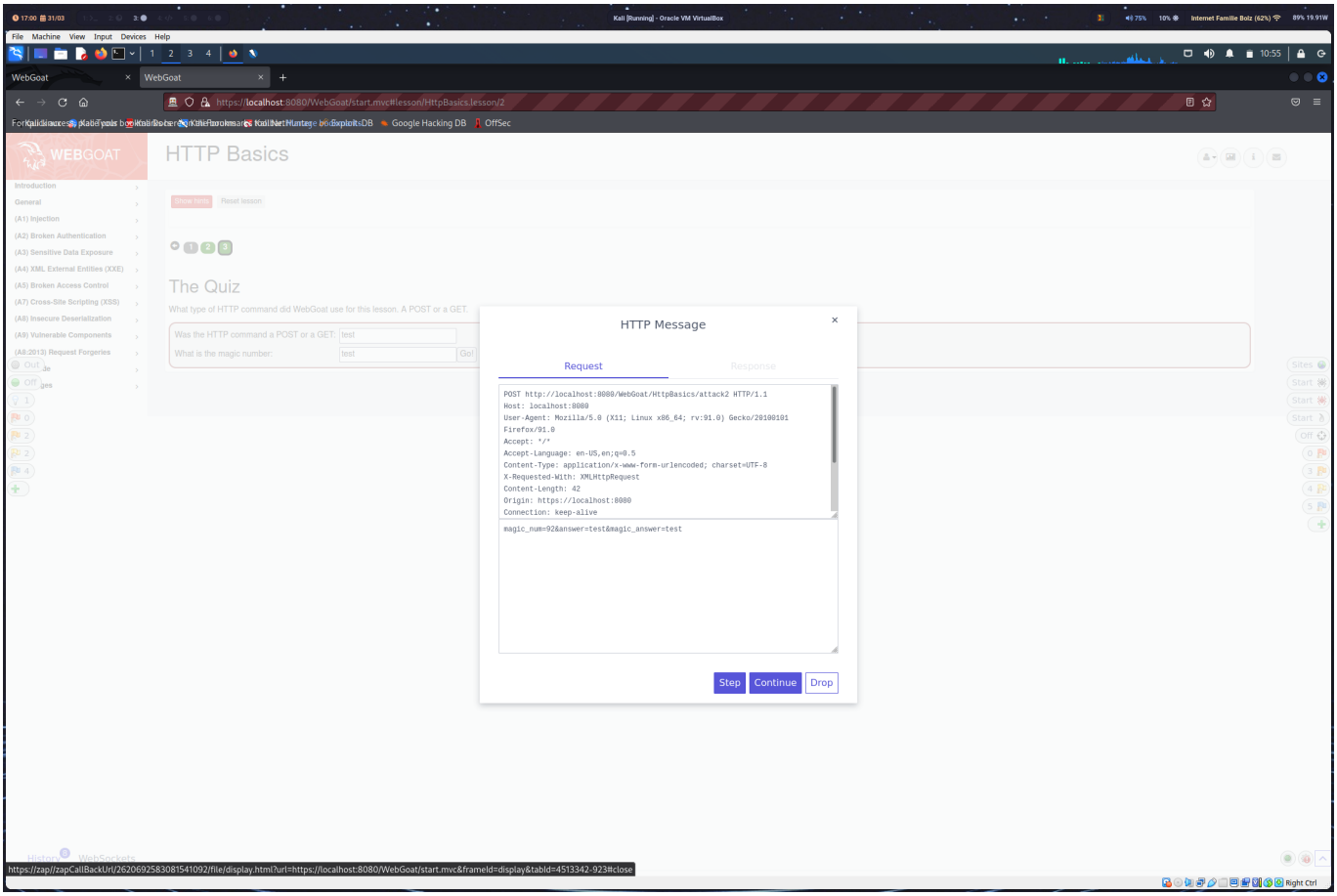
- Name eingeben
- Output wird zurückgegeben

2

- Mit Untersuchen nachgucken
    - Network Tab auswälen
    - POST request finden (attack2)
    - Im request Tab Daten auslesen



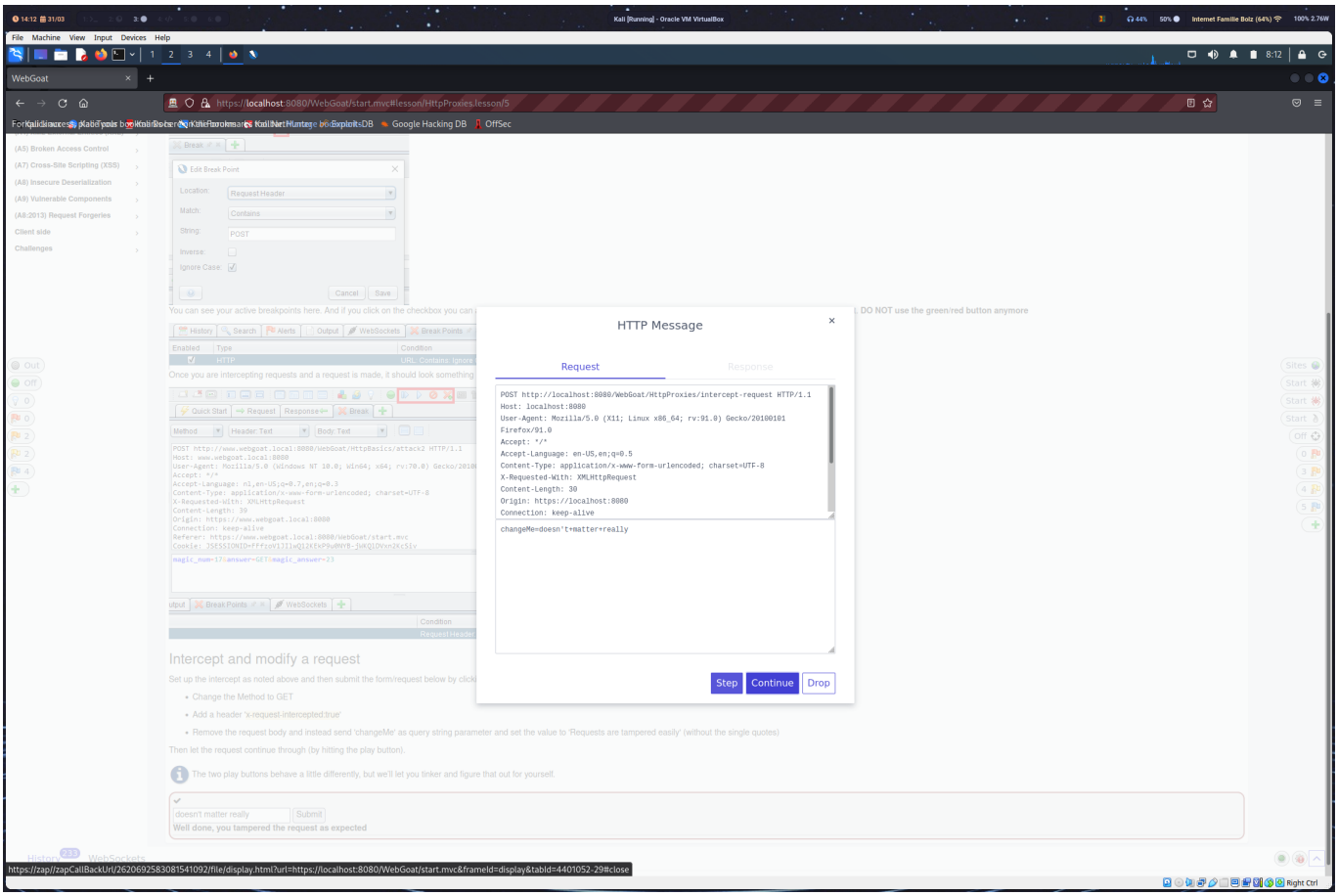
- Alternativ: ZAP interception
  - Schritte von HTTP Proxies durchführen



HTTP Proxies

1

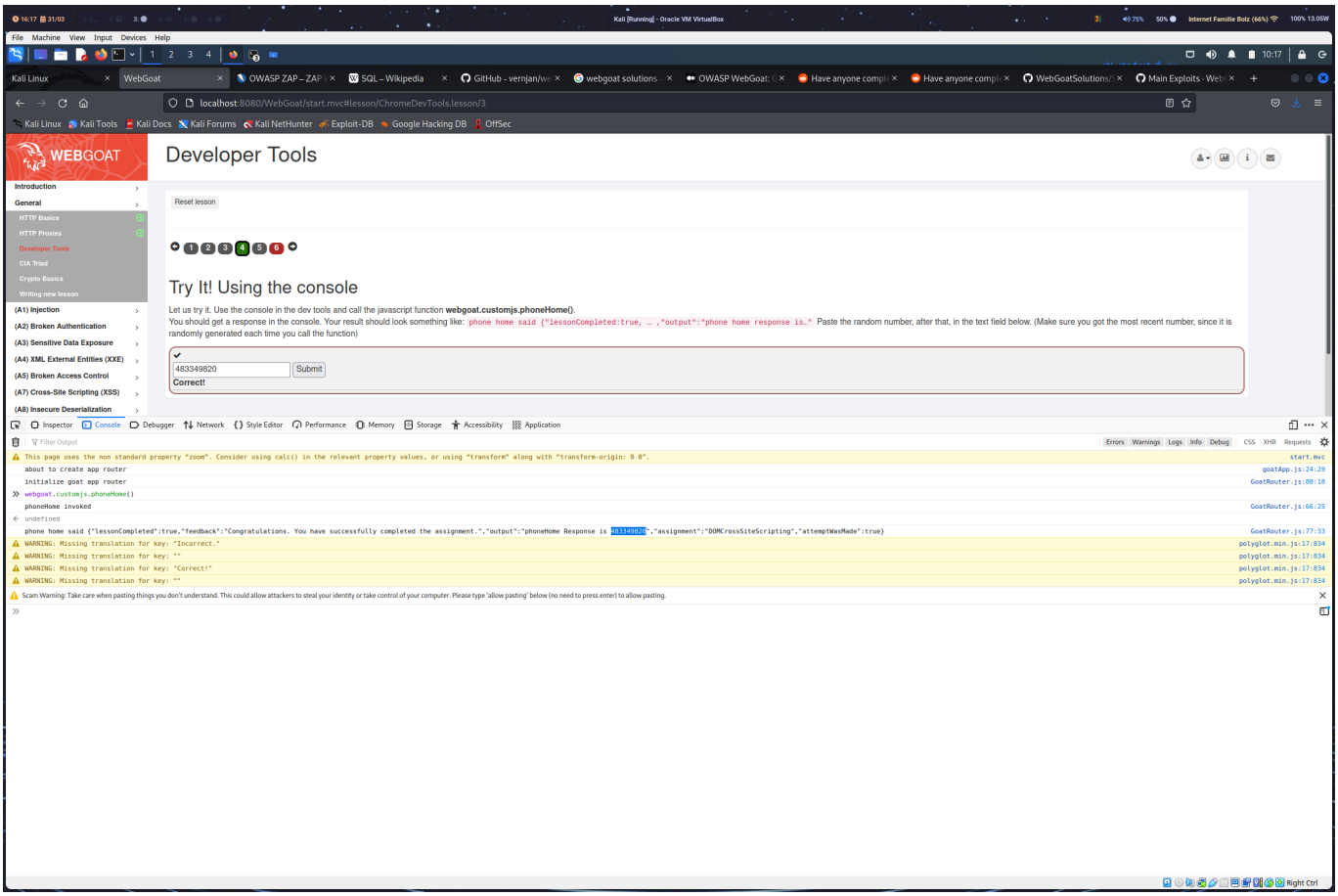
- Breakpoint filter erstellen
    - auf Request Header Contains POST setzen
- auf "Submit" drücken
- POST mit GET ersetzen
- 'x-request-intercepted:true' einfügen
- "doesn't+matter+really" mit "Requests are tampered easily" ersetzen
- auf "Continue" drücken



Developer Tools

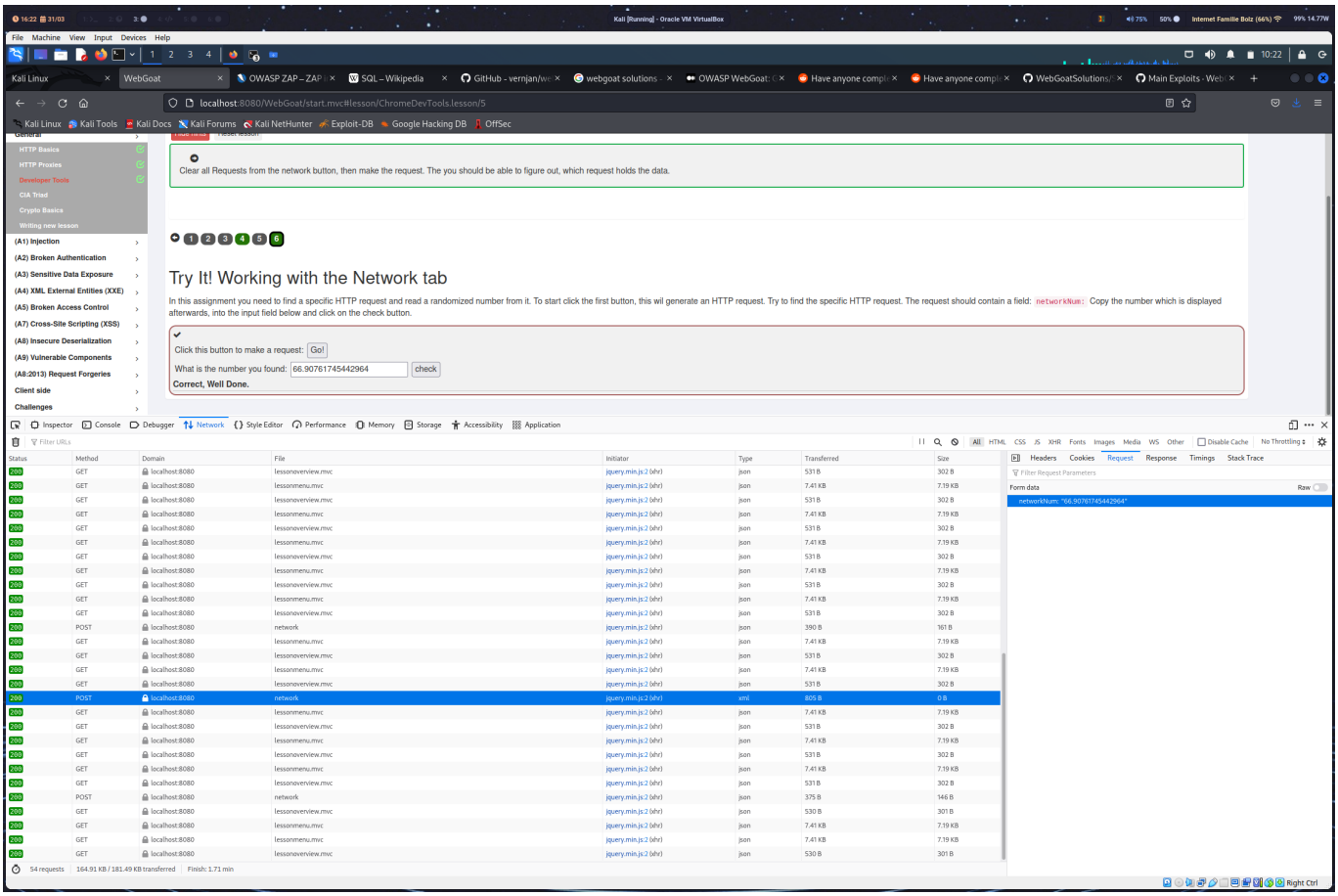
1

- Seite Untersuchen
- Zu den Console Tab wechseln
- webgoat.customjs.phoneHome() eingeben
- Die zufällig generierte Zahl abgeben



2

- Seite Untersuchen
- Zu den Network Tab wechseln
- Auf "Go" drücken
- POST request finden (der Name ist Network)
- Zum Request Tab wechsel
- NetworkNum auslesen

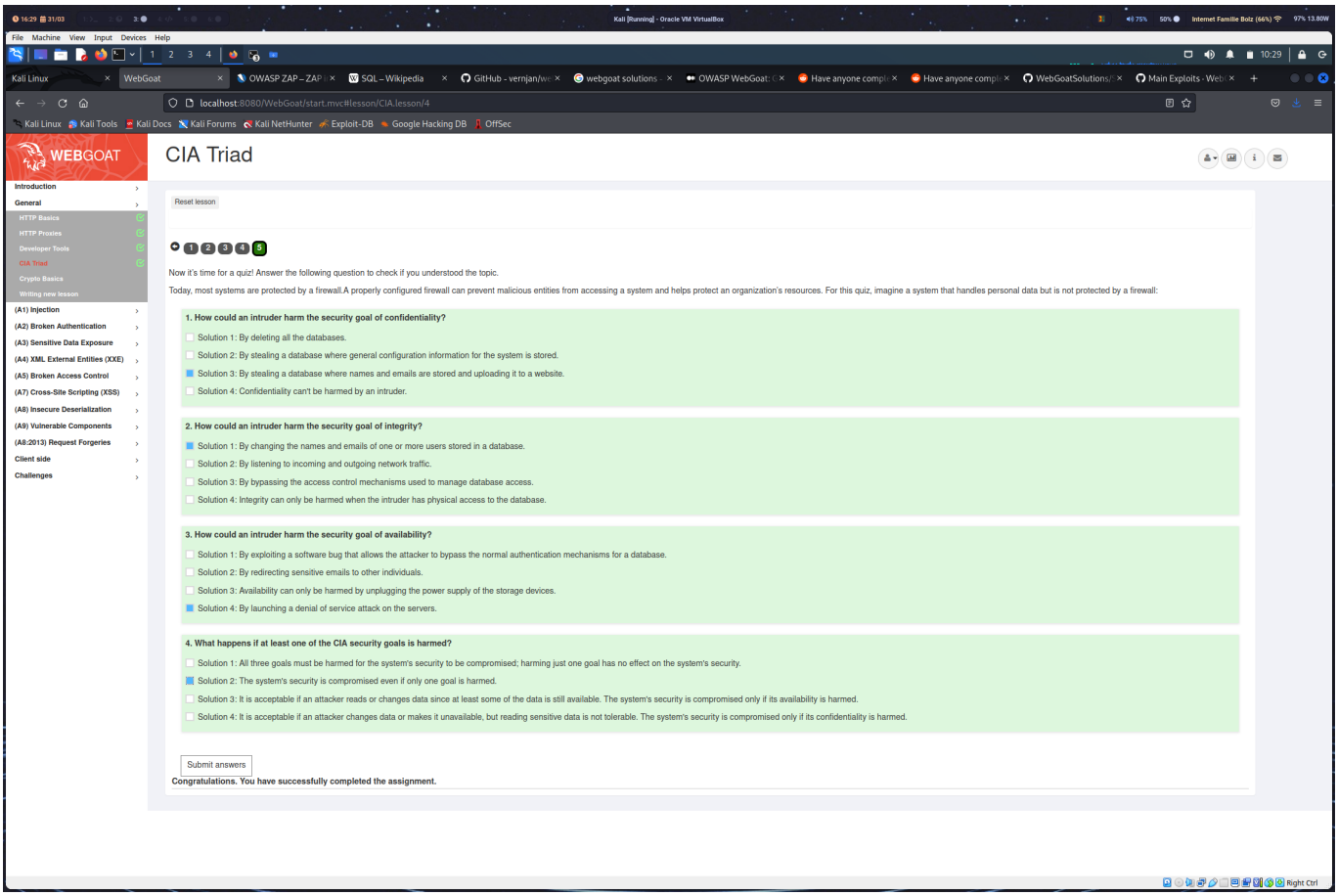


CIA Triad

1

Antworten:

- Frage 1
  - Antwort 3
- Frage 2
  - Antwort 1
- Frage 3
  - Antwort 4
- Frage 4
  - Antwort 2


WEBGOAT
CIA Triad
Introduction
General
HTTP Basics
HTTP Proxies
Developer Tools
CIA Triad
Crypto Basics
Writing new lesson
(A1) Injection
(A2) Broken Authentication
(A3) Sensitive Data Exposure
(A4) XML External Entities (XXE)
(A5) Broken Access Control
(A7) Cross-Site Scripting (XSS)
(A8) Insecure Deserialization
(A9) Vulnerable Components
(A8:2013) Request Forgeries
Client side
Challenges
Reset lesson
Now it's time for a quiz! Answer the following question to check if you understood the topic.
Today, most systems are protected by a firewall.A properly configured firewall can prevent malicious entities from accessing a system and helps protect an organization's resources. For this quiz, imagine a system that handles personal data but is not protected by a firewall:
1. How could an intruder harm the security goal of confidentiality?
Solution 1: By deleting all the databases.
Solution 2: By stealing a database where general configuration information for the system is stored.
Solution 3: By stealing a database where names and emails are stored and uploading it to a website.
Solution 4: Confidentiality can't be harmed by an intruder.
2. How could an intruder harm the security goal of integrity?
Solution 1: By changing the names and emails of one or more users stored in a database.
Solution 2: By listening to incoming and outgoing network traffic.
Solution 3: By bypassing the access control mechanisms used to manage database access.
Solution 4: Integrity can only be harmed when the intruder has physical access to the database.
3. How could an intruder harm the security goal of availability?
Solution 1: By exploiting a software bug that allows the attacker to bypass the normal authentication mechanisms for a database.
Solution 2: By redirecting sensitive emails to other individuals.
Solution 3: Availability can only be harmed by unplugging the power supply of the storage devices.
Solution 4: By launching a denial of service attack on the servers.
4. What happens if at least one of the CIA security goals is harmed?
Solution 1: All three goals must be harmed for the system's security to be compromised; harming just one goal has no effect on the system's security.
Solution 2: The system's security is compromised even if only one goal is harmed.
Solution 3: It is acceptable if an attacker reads or changes data since at least some of the data is still available. The system's security is compromised only if its availability is harmed.
Solution 4: It is acceptable if an attacker changes data or makes it unavailable, but reading sensitive data is not tolerable. The system's security is compromised only if its confidentiality is harmed.
Submit answers
Congratulations. You have successfully completed the assignment.