

1.1

a

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

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

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 Datenmenge
- 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/Seitenbetreiber: 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-Verbindungsauftnahme
 - Entschlüsselung der Verbindungsauftnahme 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) Was ist die Ursache der Verwundbarkeit und wie kann sie ausgenutzt werden?

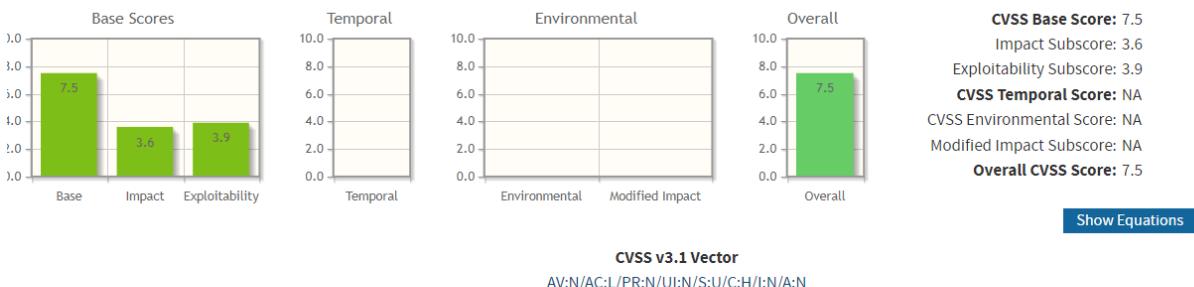
- Hardware-Hersteller haben Mikrocode-Updates und Firmware-Updates bereitgestellt, um die Anfälligkeit ihrer Chips gegenüber Meltdown zu verringern. Diese Updates beheben nicht den Designfehler, helfen jedoch dabei, die Auswirkungen der Verwundbarkeit zu begrenzen.
- Betriebssystemhersteller haben Sicherheitspatches 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?

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.



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)*

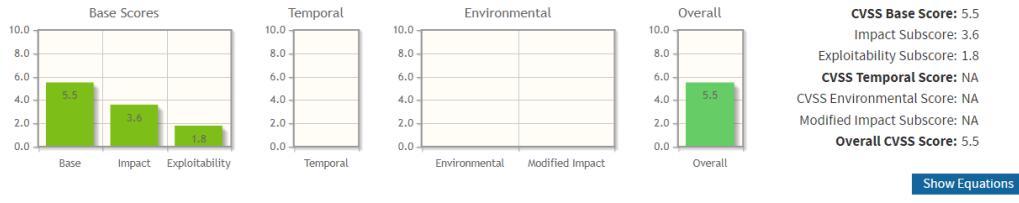
None (A:N) Low (A:L) High (A:H)

* - 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.



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)

1.1

a

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

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

1.2

c

(Bilder)

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)

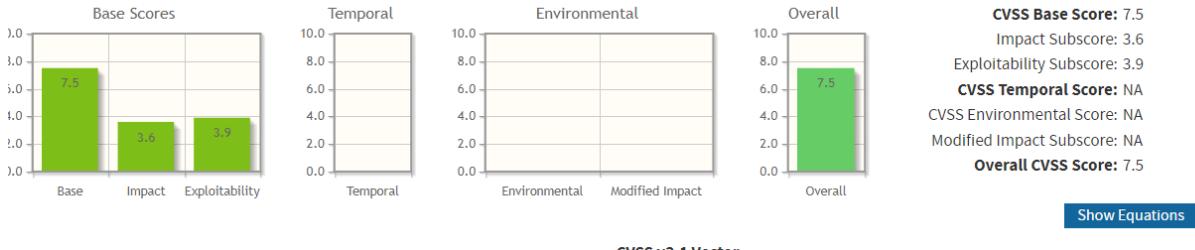
d

- 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?

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 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)*

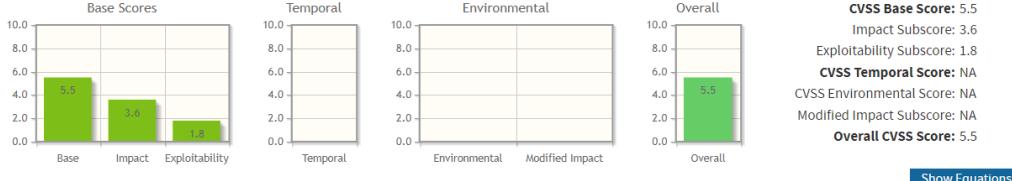
None (A:N) Low (A:L) High (A:H)

* - 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 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)

1.3

HTTP Basics

1

- Name eingeben

- Output wird zurückgegeben

2

- Mit Untersuchen nachgucken

The screenshot shows a browser window with multiple tabs open, including Kali Linux, WebGoat, OWASP ZAP - ZAP, SQL - Wikipedia, GitHub, and several exploit-related pages. The main content area displays a 'The Quiz' page from WebGoat. A red box highlights the 'Request' tab in the OWASP ZAP interface, which is intercepting a POST request to the quiz page. The request parameters show 'magic_num: 53' and 'answer: POST'. The response message says 'Congratulations. You have successfully completed the assignment.'

- Alternativ: ZAP interception
 - Schritte von HTTP Proxies durchführen

The Quiz

What type of HTTP command did WebGoat use for this lesson. A POST or a GET.

Was the HTTP command a POST or a GET: test

What is the magic number: test

HTTP Message

Request

```
POST http://localhost:8080/WebGoat/HttpBasics/attack2 HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 42
Origin: https://localhost:8080
Connection: keep-alive
```

Response

Step Continue Drop

https://zap/CallBackUI/2620692583081541092/file/display.html?url=https://localhost:8080/WebGoat/start.mvc&frameId=display&tabId=4513342-923#close

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

The screenshot shows a Firefox browser window titled "WebGoat" with the URL <https://localhost:8080/WebGoat/start.mvc#lesson/HttpProxies.lesson/5>. The browser interface includes tabs for "File", "Machine", "View", "Input", "Devices", and "Help". The main content area displays a challenge titled "Http Proxies" with a sidebar containing various security topics like "Broken Access Control", "Cross-Site Scripting (XSS)", etc. A "Break Points" dialog is open, showing a configuration for intercepting POST requests. Below it, a "HTTP Message" dialog shows a POST request to "localhost:8080" with various headers and a body containing a tampered cookie. The response section is empty. At the bottom, there's a note: "DO NOT use the green/red button anymore". To the right of the browser, a Kali Linux terminal window is visible, showing a debugger session with commands like "break", "step", and "continue". The terminal also displays some log output related to the challenge.

Developer Tools

1

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

The screenshot shows a Firefox browser window with multiple tabs open, including Kali Linux, WebGoat, OWASP ZAP - ZAP, SQL - Wikipedia, GitHub - vernjan/wi..., webgoat solutions..., OWASP WebGoat..., Have anyone comp..., Have anyone comp..., WebGoatSolutions..., Main Exploits - Web..., and Internet Famille Boltz (6%). The main content area is the 'Developer Tools' interface for the WebGoat application. On the left, there's a sidebar with a tree view of security topics: Introduction, General, HTTP Basics, HTTP Proxies, Developer Tools (which is selected), CIA Triad, Crypto Basics, and Writing new lesson. The 'Developer Tools' tab is active. In the center, under 'Try It! Using the console', there's a text input field with the value '483349820' and a 'Submit' button. Below the input field, the word 'Correct!' is displayed. At the bottom, the Firefox developer tools' Console tab is open, showing several warning messages:

- This page uses the non-standard property "zoom". Consider using calc() in the relevant property values, or using "transform" along with "transform-origin: 0 0".
- WARNING: Missing translation for key: "Incorrect."
- WARNING: Missing translation for key: "Correct!"
- WARNING: Missing translation for key: ""

Scan Warning: Take care when pasting things you don't understand. This could allow attackers to steal your identity or take control of your computer. Please type 'allow pasting' below (no need to press enter) to allow pasting.

2

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

The screenshot shows a NetworkMiner capture of traffic from a Kali Linux VM. The Network tab is selected, displaying a list of requests. A specific POST request at index 288 is highlighted, showing the parameter 'networkNum=66.90761745442964'. The Request pane shows the raw XML of this POST request.

CIA Triad

1

Antworten:

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

The screenshot shows a Firefox browser window running on a Kali Linux VM. The title bar indicates it's running on Oracle VM VirtualBox. The address bar shows the URL localhost:8080/WebGoat/start.mvc#lesson/CIA.lesson. The main content is a quiz titled "CIA Triad". On the left is a sidebar with navigation links for "Introduction", "General", "HTTP Basics", "HTTP Proxies", "Developer Tools", "CIA Triad" (which is highlighted in red), and "Crypto Basics". Below that is a link to "Writing new lesson". The main area has a "Reset lesson" button and a numbered navigation bar (1, 2, 3, 4, 5) where number 5 is highlighted in green. A note at the top says: "Now it's time for a quiz! Answer the following question to check if you understand 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." The quiz consists of four questions, each with a list of four options. Question 1: "How could an intruder harm the security goal of confidentiality?" Options: Solution 1: By deleting all the databases. (unchecked) Solution 2: By stealing a database where general configuration information for the system is stored. (unchecked) Solution 3: By stealing a database where names and emails are stored and uploading it to a website. (checked) Solution 4: Confidentiality can't be harmed by an intruder. (unchecked) Question 2: "How could an intruder harm the security goal of integrity?" Options: Solution 1: By changing the names and emails of one or more users stored in a database. (checked) Solution 2: By listening to incoming and outgoing network traffic. (unchecked) Solution 3: Integrity can only be harmed by bypassing the access control mechanisms used to manage database access. (unchecked) Solution 4: Integrity can only be harmed when the intruder has physical access to the database. (unchecked) Question 3: "How could an intruder harm the security goal of availability?" Options: Solution 1: By exploiting a software bug that allows the attacker to bypass the normal authentication mechanisms for a database. (unchecked) Solution 2: By redirecting sensitive emails to other individuals. (unchecked) Solution 3: Availability can only be harmed by unplugging the power supply of the storage devices. (unchecked) Solution 4: By launching a denial of service attack on the servers. (checked) Question 4: "What happens if at least one of the CIA security goals is harmed?" Options: 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. (unchecked) Solution 2: The system's security is compromised even if only one goal is harmed. (checked) 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. (unchecked) 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. (unchecked) At the bottom, there is a "Submit answers" button and a message: "Congratulations. You have successfully completed the assignment." The status bar at the bottom of the browser shows various icons and the text "Right Ctrl".