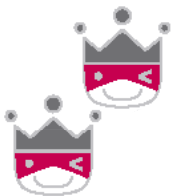


# 2

## Spoofing

Ein Angreifer "sitzt" (lauscht) auf einem zufälligen Port oder Socket, den der server üblicherweise nutzt.



Microsoft

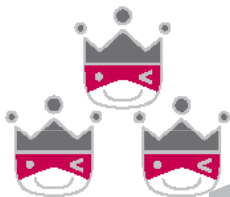
elevation of privilege



# 3

## Spoofing

Ein Angreifer kann alle möglichen Credentials der Reihe nach durchprobieren (online oder offline) und es gibt keinen Mechanismus, der ihn ausbremst.



Microsoft

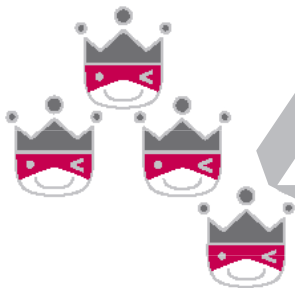
elevation of privilege



# 4

## Spoofing

Ein Angreifer kann sich anonym verbinden, weil Sie davon ausgehen, dass Authentisierung auf einer höheren Schicht stattfindet.



Microsoft

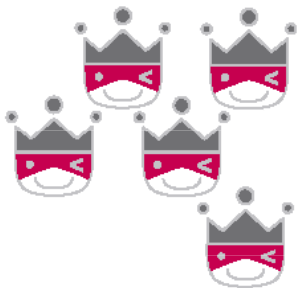
elevation of privilege



# 5

## Spoofing

Ein Angreifer kann einen Client verwirren, weil es zu viele Wege gibt, einen Server zu identifizieren.



Microsoft

elevation of privilege

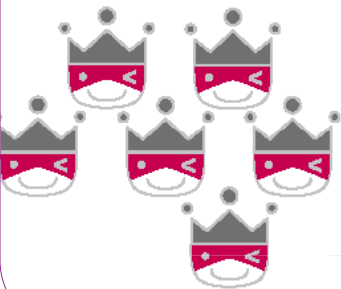




# 6

## Spoofing

Ein Angreifer kann einen Server spoofen, weil auf dem Client keinerlei Identifizierungsmerkmale gespeichert sind, die bei erneuter Verbindung überprüft würden (es gibt keine Key-persistence).



**Microsoft**

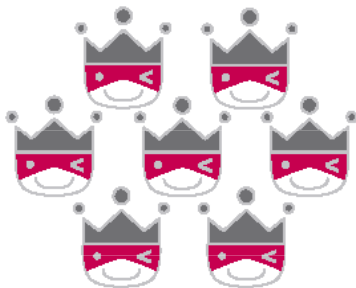
elevation of privilege



# 7

## Spoofing

Ein Angreifer kann sich zu einem Server oder Peer über einen nicht authentisierten unverschlüsselten Kanal verbinden.



Microsoft

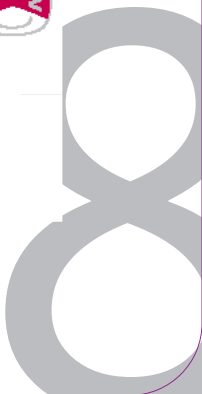
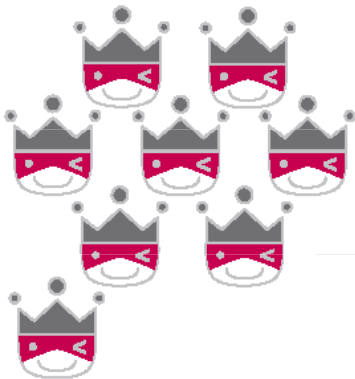
elevation of privilege



# 8

## Spoofing

Ein Angreifer kann auf einem Server gespeicherte Credentials stehlen und wieder verwenden (z.B. Schlüssel in einer für andere lesbaren Datei).



Microsoft

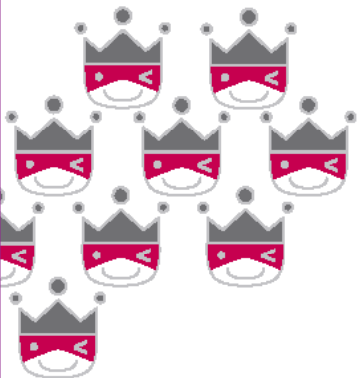
elevation of privilege



# 9

## Spoofing

Ein Angreifer, der Zugang zu einem Passwort bekommt, kann es wieder verwenden (nutzen Sie stärkere Authentisierungsmethoden).



Microsoft

elevation of privilege

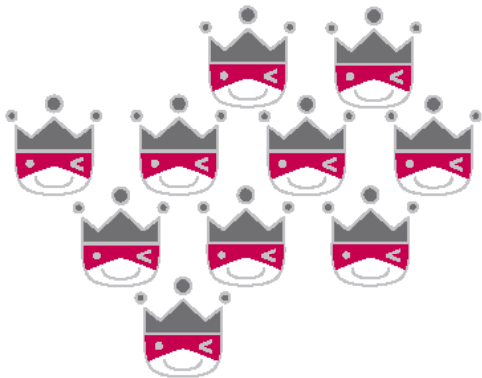




# 10

## Spoofing

Ein Angreifer kann wählen, dass eine schwächere oder gar keine Authentisierung genutzt wird.



Microsoft

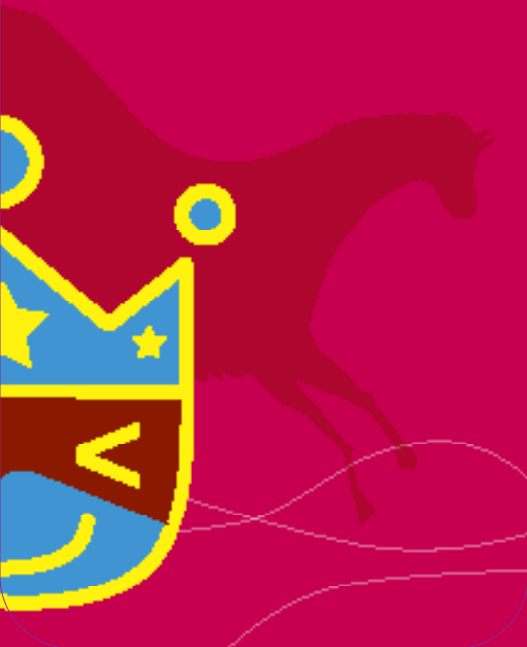
elevation of privilege



# J

## Spoofing

Ein Angreifer kann die auf einem Client gespeicherten Credentials stehlen und wieder verwenden.



Microsoft

elevation of privilege



A large, white, stylized letter 'Q' is centered within a brown rounded square. The background of the entire slide is a vibrant pink with a pattern of overlapping hearts in various shades of pink and orange. On the left side, there is a large, stylized graphic of a crown or shield with orange and white segments, featuring three small hearts and a large 'V' shape.

# Spoofing

Ein Angreifer kann den Mechanismus angreifen, mit dem Passwörter zurückgesetzt oder aktualisiert werden (Account Recovery erfordert nicht die Eingabe des alten Passworts).

Microsoft

elevation of privilege



A large, white, stylized letter 'K' is centered within a dark red rounded square. The background of the entire slide is a vibrant red, featuring abstract geometric shapes in the lower half, including a large black triangle with a white circle, a grey triangle with a white 'V', and several overlapping translucent diamonds in shades of blue, teal, and pink.

# Spoofing

Ihr System wird mit einem Default Adminpasswort ausgeliefert und erzwingt nicht die Änderung dieses Passworts.

Microsoft

elevation of privilege

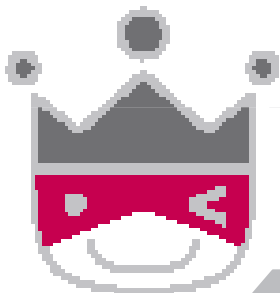




# A

## Spoofing

Sie haben einen neuen Spoofing  
Angriff erfunden.



Microsoft

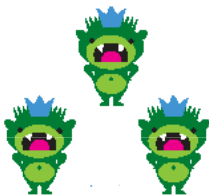
elevation of privilege



# 3

## Tampering

Statt auf Standard-Kryptografie zurück zu greifen, haben Sie sich selbst einen Mechanismus zur Gewährleistung von Integrität oder für den Schlüsselaustausch ausgedacht. Ein Angreifer kann sich dies zunutze machen.



Microsoft

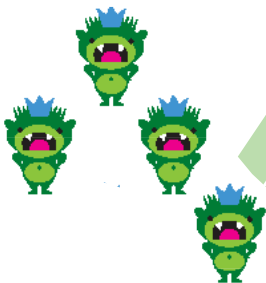
elevation of privilege



# 4

## Tampering

Ihr Code trifft Entscheidungen zur Zugangskontrolle an vielen unterschiedlichen Stellen, anstatt diese Funktion an zentraler Stelle (in einem Security Kernel) zu implementieren.



Microsoft

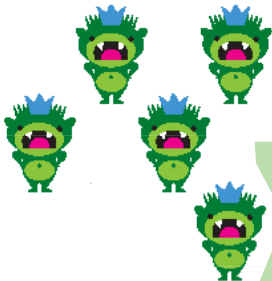
elevation of privilege



# 5

## Tampering

Ein Angreifer kann unbemerkt bereits übermittelte Daten erneut übertragen, weil Ihr Code keine Zeitstempel, Sequenznummern oder ähnliches nutzt, um dies zu verhindern oder zu erkennen.



Microsoft

elevation of privilege

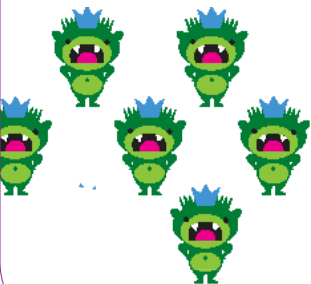




# 6

## Tampering

Ein Angreifer kann Daten an Speicherorten schreiben, an denen Ihr Code liegt oder die durch Ihren Code interpretiert werden.



Microsoft

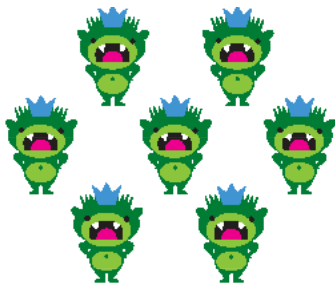
elevation of privilege



# 7

## Tampering

Ein Angreifer kann Berechtigungen umgehen, weil Sie Namen nicht kanonisieren (normalisieren), bevor Zugriffsrechte geprüft werden.



Microsoft

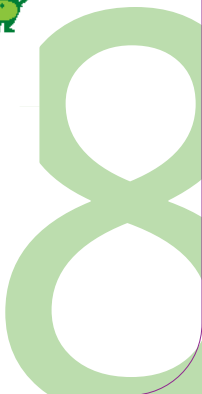
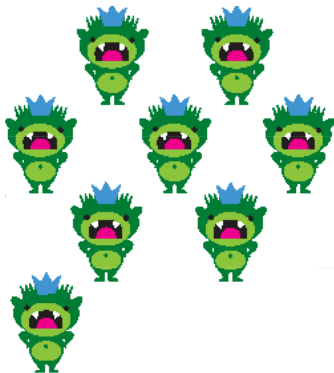
elevation of privilege



# 8

## Tampering

Ein Angreifer kann Daten manipulieren, die per Netzwerk übertragen werden, weil Ihr Code keine Integritätssicherung vorsieht.



Microsoft

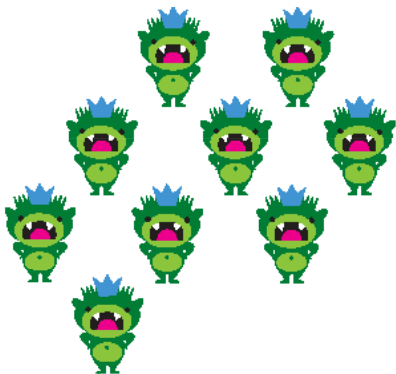
elevation of privilege



# 9

## Tampering

Ein Angreifer kann Status-  
informationen beeinflussen.



Microsoft

elevation of privilege

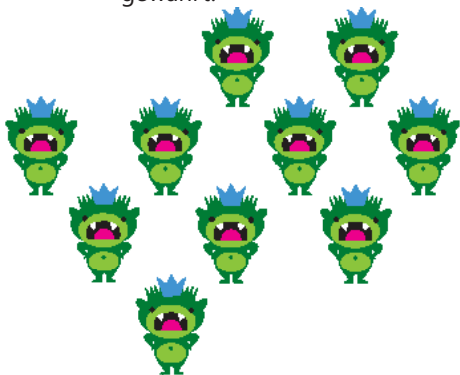




# 10

## Tampering

Ein Angreifer kann gespeicherte Daten verändern, weil die Berechtigungen (ACLs) zu wenig restriktiv sind oder eine Gruppe verwendet wird, die letztlich jedem Nutzer Zugriff gewährt.



**Microsoft**

elevation of privilege



# J

## Tampering

Ein Angreifer kann auf eine Ressource schreiben, weil es keine ACLs gibt, oder weil jeder berechtigt ist (world writable).



Microsoft

elevation of privilege



# Q

## Tampering

Ein Angreifer kann Parameter über eine Trust Boundary hinweg ändern, nachdem sie validiert wurden (z.B. in einem HTML hidden field, oder einem Pointer an eine kritische Speicherstelle im RAM übergeben).



**Microsoft**

elevation of privilege



# K

## Tampering

Ein Angreifer kann Code mithilfe eines Extension Points einbinden.



Microsoft

elevation of privilege





A

# Tampering

Sie haben einen neuen  
Tampering Angriff erfunden.



Microsoft

elevation of privilege



# 2

## Repudiation

Ein Angreifer kann den Inhalt von Logdaten beeinflussen, einen Log Reader (Programm oder Nutzer darüber angreifen und es ist nicht dokumentiert, ob und wie verschiedene Logdaten validiert werden.



Microsoft

elevation of privilege



# 3

## Repudiation

Ein unprivilegierten Nutzer oder Angreifer hat lesend Zugang zu interessanten Sicherheitsinformationen in den Logs.



Microsoft

elevation of privilege



# 4

## Repudiation

Ein Angreifer kann digitale Signaturen manipulieren, weil Sie einen MAC Algorithmus statt eines Signiervorgangs nutzen, oder weil das Signiervorgang unsicher ist.



Microsoft

elevation of privilege





# 5

## Repudiation

Ein Angreifer kann Lognachten verändern, die übers Netz übertragen werden, weil kein starker Mechanismus zur Gewährleistung der Integrität implementiert ist.



Microsoft

elevation of privilege



# 6

## Repudiation

Ein Angreifer kann einen Logeintrag ohne Zeitstempel erzeugen (oder die Logs haben generell keine Zeitstempel).



Microsoft

elevation of privilege



# 7

## Repudiation

Ein Angreifer kann das Log zum Überlaufen bringen, so dass alte Logdaten überschrieben werden und somit verloren sind (wrap-around).



Microsoft

elevation of privilege



# 8

## Repudiation

Ein Angreifer kann das Logging so austricksen, dass sicherheitsrelevante Logdaten nicht geschrieben werden oder durcheinander geraten.



Microsoft

elevation of privilege





# 9

## Repudiation

Ein Angreifer kann einen Shared Key nutzen, um sich als jemand anders auszugeben, so dass seine Aktionen ebenfalls unter dieser Identität mitgeloggt werden.



Microsoft

elevation of privilege



# 10

## Repudiation

Ein Angreifer kann beliebige Logdaten in ein Logsystem einschleusen, weil die Logquellen nicht oder nur schwach authentisiert werden.



Microsoft

elevation of privilege



# J

## Repudiation

Ein Angreifer kann unbemerkt Logs editieren, löschen oder deren Übermittlung unterbinden.



Microsoft

elevation of privilege



# Q

## Repudiation

Ein Angreifer kann abstreiten, etwas getan zu haben und es gibt keine brauchbaren Daten, um das Gegenteil zu beweisen.



**I didn't  
do that.**

Microsoft

elevation of privilege







K

# Repudiation

Das System hat keine Logs.

**logs = 0**

**Microsoft**

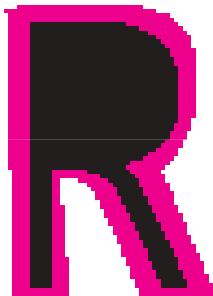
elevation of privilege



A large, stylized white letter 'A' is positioned inside a dark gray rounded square. The 'A' is composed of two thick strokes, with the right stroke extending slightly beyond the top and bottom of the square.

# Repudiation

Sie haben einen neuen  
Repudiation Angriff erfunden.

A large, stylized black letter 'R' is centered on the page. It has a thick, vibrant pink outline. The 'R' is composed of a solid black shape with a pink border, giving it a pixelated or blocky appearance. In the bottom right corner, there are abstract orange and pink geometric shapes that partially overlap the edge of the frame.

**Microsoft**

elevation of privilege



# 2

## Information Disclosure

Ein Angreifer kann verschlüsselte Dateien mittels Brute-Force entschlüsseln, weil keine geeigneten Sicherheitsmaßnahmen dagegen vorhanden sind.



**Microsoft**

elevation of privilege



# 3

## Information Disclosure

Ein Angreifer kann sicherheitsrelevante Fehlermeldungen sehen.



**Microsoft**

elevation of privilege





# 4

## Information Disclosure

Ein Angreifer kann Dateninhalte lesen, weil die Nachrichten (z.B. E-Mails oder Cookies) nicht verschlüsselt sind, selbst wenn der Transportkanal verschlüsselt ist.



**Microsoft**

elevation of privilege



# 5

## Information Disclosure

Ein Angreifer kann unter Umständen Daten lesen, die mit einem nicht standardisierten kryptografischen Algorithmus verschlüsselt sind.



**Microsoft**

elevation of privilege



# 6

## Information Disclosure

Ein Angreifer kann Daten lesen, die lediglich versteckt oder verschleiert sind (z.B. für eine Undo-Funktion), so dass dem Nutzer gar nicht bewusst ist, dass die Daten (noch) existieren.



Microsoft

elevation of privilege



# 7

## Information Disclosure

Ein Angreifer kann als "Man in the Middle" verschlüsselte Daten lesen, weil die Endpunkte einer Netzwerkverbindung nicht authentisiert sind.



**Microsoft**

elevation of privilege





## 8

# Information Disclosure

Ein Angreifer kann (sensible) Informationen mithilfe eines Such-Indexers, Loggers oder eines anderen Mechanismus zugreifen.



Microsoft

elevation of privilege



# 9

## Information Disclosure

Ein Angreifer kann sensible Informationen in einer Datei lesen, weil deren Zugriffsrechte falsch gesetzt sind (schwache ACL).



Microsoft

elevation of privilege



10

# Information Disclosure

Ein Angreifer kann mangels Zugriffsbeschränkung eine sensible Datei lesen.



Microsoft

elevation of privilege



# J

## Information Disclosure

Ein Angreifer kann den statischen Schlüssel finden, der zur Verschlüsselung genutzt wird.



**Microsoft**

elevation of privilege





# Q

## Information Disclosure

Ein Angreifer kann einen Kommunikationskanal vollständig mitlesen, weil dieser unverschlüsselt ist.

Don't tell anyone, but...



Microsoft

elevation of privilege



# K

## Information Disclosure

Ein Angreifer kann Netzwerk-informationen lesen, weil keine Kryptografie genutzt wird.



What!?!#@!  
No cryptography was used?

Microsoft

elevation of privilege





A

# Information Disclosure

Sie haben einen neuen  
Information Disclosure  
Angriff erfunden.



**Microsoft**

elevation of privilege



# 2

## Denial of Service

Ein Angreifer kann Ihr Authentisierungs-System unbrauchbar oder unverfügbar machen.



**Microsoft**

elevation of privilege





# 3

## Denial of Service

Ein Angreifer kann einen Client unverfügbar oder unbrauchbar machen, aber das Problem verschwindet, sobald der Angriff aufhört (**Client, authentisiert, temporär**).



Microsoft

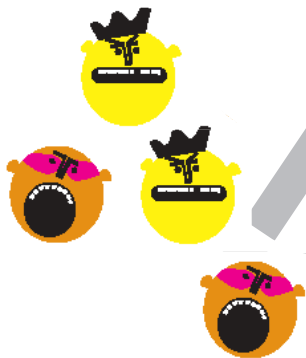
elevation of privilege



# 4

## Denial of Service

Ein Angreifer kann einen Server unverfügbar oder unbrauchbar machen, aber das Problem verschwindet, sobald der Angriff aufhört (**Server, authentisiert, temporär**).



Microsoft

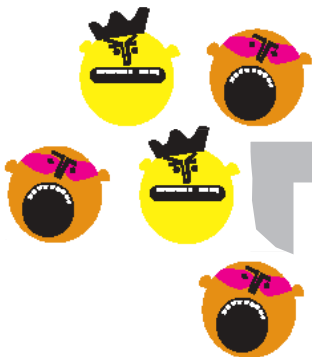
elevation of privilege



# 5

## Denial of Service

Ein Angreifer kann einen Client un verfügbar machen, ohne dass eine Authentisierung stattgefunden hat. Das Problem verschwindet nach dem Angriff (**Client, anonym, temporär**).



Microsoft

elevation of privilege



# 6

## Denial of Service

Ein Angreifer kann einen Server unverfügbar machen, ohne dass eine Authentisierung stattgefunden hat. Das Problem verschwindet nach dem Angriff (**Server, anonym, temporär**).



**Microsoft**

elevation of privilege





## 7

# Denial of Service

Ein Angreifer kann einen Client unverfügbar machen und das Problem besteht fort, nachdem der Angriff aufgehört hat (**Client, authentisiert, persistent**).



Microsoft

elevation of privilege



## 8

# Denial of Service

Ein Angreifer kann einen Server un verfügbar machen und das Problem besteht fort, nachdem der Angriff aufgehört hat  
**(Server, authentisiert, persistent).**



**Microsoft**

elevation of privilege



## 9

# Denial of Service

Ein Angreifer kann einen Client unverfügbar machen, ohne dass je eine Authentisierung stattgefunden hat, und das Problem besteht fort, nachdem der Angriff aufgehört hat (**Client, anonym, persistent**).



Microsoft

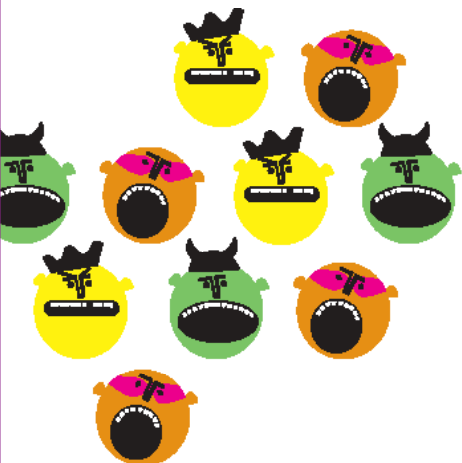
elevation of privilege



# 10

## Denial of Service

Ein Angreifer kann, ohne zu authentisieren, einen Server unverfügbar machen. Das Problem besteht fort, nachdem der Angriff aufgehört hat (**Server, anonym, persistent**).



Microsoft

elevation of privilege





J

# Denial of Service

Ein Angreifer kann das Logging-Subsystem außer Betrieb setzen.



**Microsoft**

elevation of privilege



# Q

## Denial of Service

Ein Angreifer kann eine verwundbare Systemkomponente dazu missbrauchen, eine (volumenbasierte) DoS Attacke um den Faktor 10 zu verstärken.



Microsoft

elevation of privilege



# K

## Denial of Service

Ein Angreifer kann eine verwundbare Systemkomponente dazu missbrauchen, eine DoS Attacke mehr als 100fach zu verstärken.



**Microsoft**

elevation of privilege



A

# Denial of Service

Sie haben eine neue Denial of Service Attacke erfunden.



Microsoft

elevation of privilege

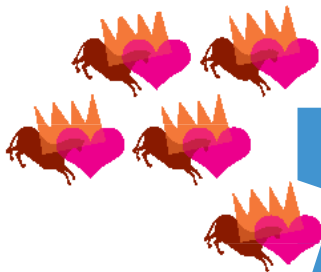




## 5

# Elevation of Privilege

Ein Angreifer kann Einfluss darauf nehmen, welche Art Validierung Daten durchlaufen, die jeweils unterschiedliche Ergebnisse liefern.



Microsoft

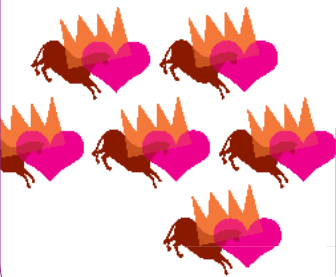
elevation of privilege



# 6

## Elevation of Privilege

Ein Angreifer kann Berechtigungen für sich ausnutzen, die Ihr Programm verlangt, aber nicht wirklich benötigt.



Microsoft

elevation of privilege



## 7

# Elevation of Privilege

Ein Angreifer kann einen Pointer über eine Trust-Boundary hinweg angeben, anstatt Daten eingeben zu müssen, die eine Validierung durchlaufen.



Microsoft

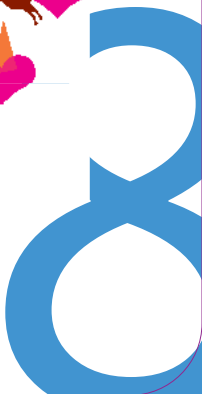
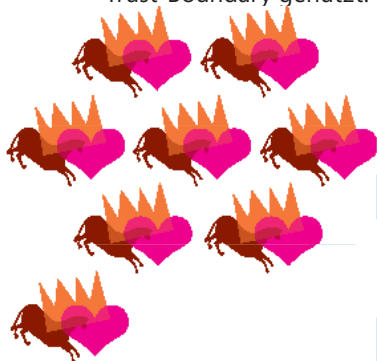
elevation of privilege



## 8

# Elevation of Privilege

Eingegebene Daten befinden sich während der Überprüfung noch unter Kontrolle des Angreifers und werden später jenseits der Trust-Boundary genutzt.



Microsoft

elevation of privilege

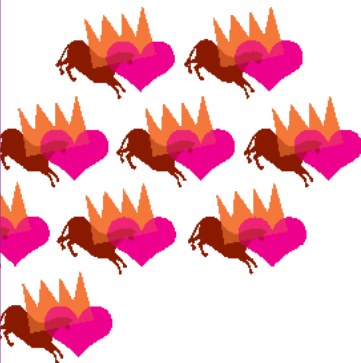




## 9

# Elevation of Privilege

Caller (aufrufende Funktionen) haben keine Möglichkeit zu überprüfen, welche Validierung Ihr Programm auf die übergebenen Daten anwendet, bevor sie diese weitergeben.



**Microsoft**

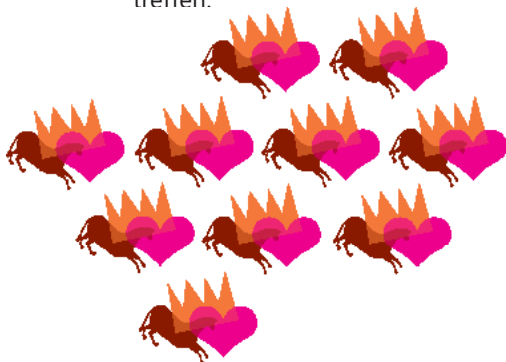
elevation of privilege



# 10

## Elevation of Privilege

Es ist für einen Aufrufer / Caller nicht klar ersichtlich, welche Sicherheitsmaßnahmen Sie treffen.



Microsoft

elevation of privilege





J

# Elevation of Privilege

Ein Angreifer kann Eingaben zum Nutzer zurückspiegeln, z.B. per Cross-Site-Scripting (XSS).



Microsoft

elevation of privilege





Q

# Elevation of Privilege

Sie inkludieren User Generated Content (UGC) in Ihrer Webseite, der auch Inhalte beliebiger URLs etc. enthalten kann.



Microsoft

elevation of privilege



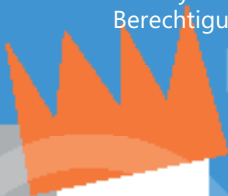




# K

# Elevation of Privilege

Ein Angreifer kann ein Kommando einschleusen, welches vom System mit einer höheren Berechtigung ausgeführt wird.



Microsoft

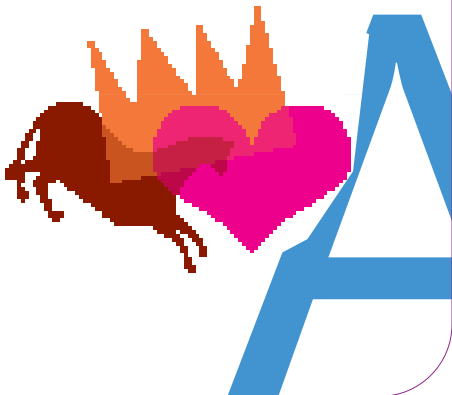
elevation of privilege



A

# Elevation of Privilege

Sie haben einen neuen  
Elevation of Privilege Angriff  
erfunden.



**Microsoft**

elevation of privilege

