

Anleitung 1

Elevation of Privilege Anleitung

1. Zeichnen Sie ein Diagramm des Systems, für das Sie ein Bedrohungsmödell erstellen möchten.
2. Teilen Sie die Karten an 3 - 6 Spieler aus.
3. Das Spiel beginnt mit der Karte "Tampering 3".
Es wird im Uhrzeigersinn gespielt. Wer an der Reihe ist, versucht die Suite (z.B. Tampering) zu bedienen, mit der die Runde eingeleitet wurde. Wer nicht bedienen kann, spielt eine Karte einer anderen Suite. Wer mit der höchstwertigen Karte bedienen kann, gewinnt die Runde, außer eine "Elevation of Privilege" Karte wird gespielt, die dann gewinnt. Um eine Karte zu spielen, lesen Sie die Bedrohung auf der Karte laut vor. Können Sie die Bedrohung nicht auf Ihr System anwenden, geht das Spiel weiter. Wer die Runde gewinnt, wählt Karte (und Suite), mit der die nächste Runde begonnen wird. Machen Sie nach jeder Runde eine kurze Pause, um über die Bedrohungen nachzudenken.

Punkte:

1 wenn Sie die Bedrohung auf Ihr System anwenden können, +1 für den Rundengewinn

Anleitung

Elevation of Privilege Anleitung

Artikulieren Sie Bedrohungen klar und nachvollziehbar. Bedrohungen müssen testfähig/überprüfbar sein. Überlegen Sie, wie. Bedrohungen sollen innerhalb des Systems adressierbar sein. Streit um die Gültigkeit einer Bedrohung können Sie mit der Frage auflösen: "Würden wir einen Bugreport, ein Feature-Request oder eine Design-Änderung hierfür akzeptieren?". Ist die Antwort "ja", handelt es sich um eine relevante Bedrohung. Dies bedeutet nicht, dass Bedrohungen außerhalb dieser Betrachtung nicht real sind. Es hilft lediglich, sich auf adressierbare Bedrohungen zu konzentrieren.

Bedrohungen die einleiten mit "Ein Angreifer könnte..." werden erläutert im Stile "...und zwar wie folgt". Karten mit "Ihr Code..." werden wie folgt vorgetragen: "Unser Code... und zwar wie folgt". Das Kartendeck enthält einige Spezialkarten: Trümpfe und offene Bedrohungen. EoP Karten sind Trümpfe. Sie gewinnen die Runde, auch wenn sie einen niedrigeren Wert haben, als die Suite/Farbe, mit der die Runde begonnen wurde. Asse sind offene Bedrohungen. Wer ein Ass spielt, muss eine Bedrohung finden, die auf keiner anderen Karte steht und versuchen, sie auf das System anzuwenden. Wenn alle Karten gespielt sind, gewinnt der Spieler mit der höchsten Punktzahl.

Viel Spaß beim Spielen!

Anleitung

Anleitung 2

Elevation of Privilege Varianten

Optionale Varianten:

- a)** Sie können Karten, die Sie nicht auf das System anwenden können, nach der 3. Runde abgeben. Vielleicht kann es jemand anders.
- b)** Verdoppeln Sie die Punktzahlen und geben Sie 1 Punkt für Bedrohungen auf Karten anderer Spieler.
- c)** Spieler die nicht an der Reihe sind können nach Spielen einer Karte binnen 1 Minute Varianten einer Bedrohung einwerfen und erläutern, die auf das System anwendbar sind. Geben Sie hierfür 1 Extrapunkt. Markieren Sie im Diagramm, wo die Bedrohung statt findet.

Thanks to Laurie Williams for inspiration.

Anleitung

Inhalt:

- **2** Karten mit der Spielanleitung
- **1** Karte mit einem Strategie-Diagramm
- **6** STRIDE "Suites" von Spielkarten:
 1. Spoofing: 2-K, Ace
 2. Tampering: 3-K, Ace
 3. Repudiation: 2-K, Ace
 4. Information Disclosure: 2-K, Ace
 5. Denial of Service: 2-K, Ace
 6. Elevation of Privilege: 5-K, Ace (Trumpf Karten)
- **6** STRIDE Bedrohung Referenz Karten
- **1** About Threat Modeling und SDL card

© 2010 Microsoft Corporation. This work is licensed under the Creative Commons Attribution 3.0 United States License. To view the full content of this license, visit <http://creativecommons.org/licenses/by/3.0/us/> or send a letter to Creative Commons, 171 Second Street, Suite 300, San Francisco, California, 94105, USA.

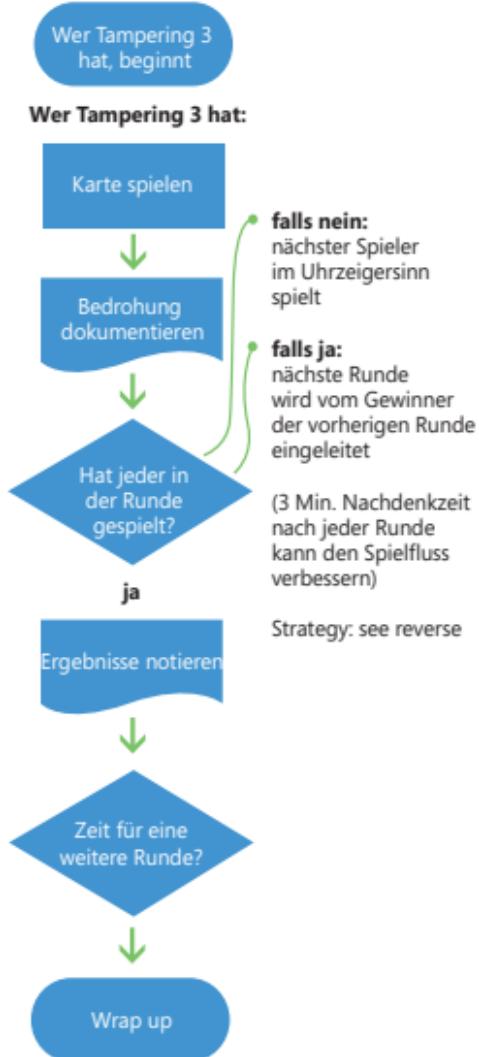
Deutsche Übersetzung: Detmar Liesen, test4bounty@gmail.com

Anleitung

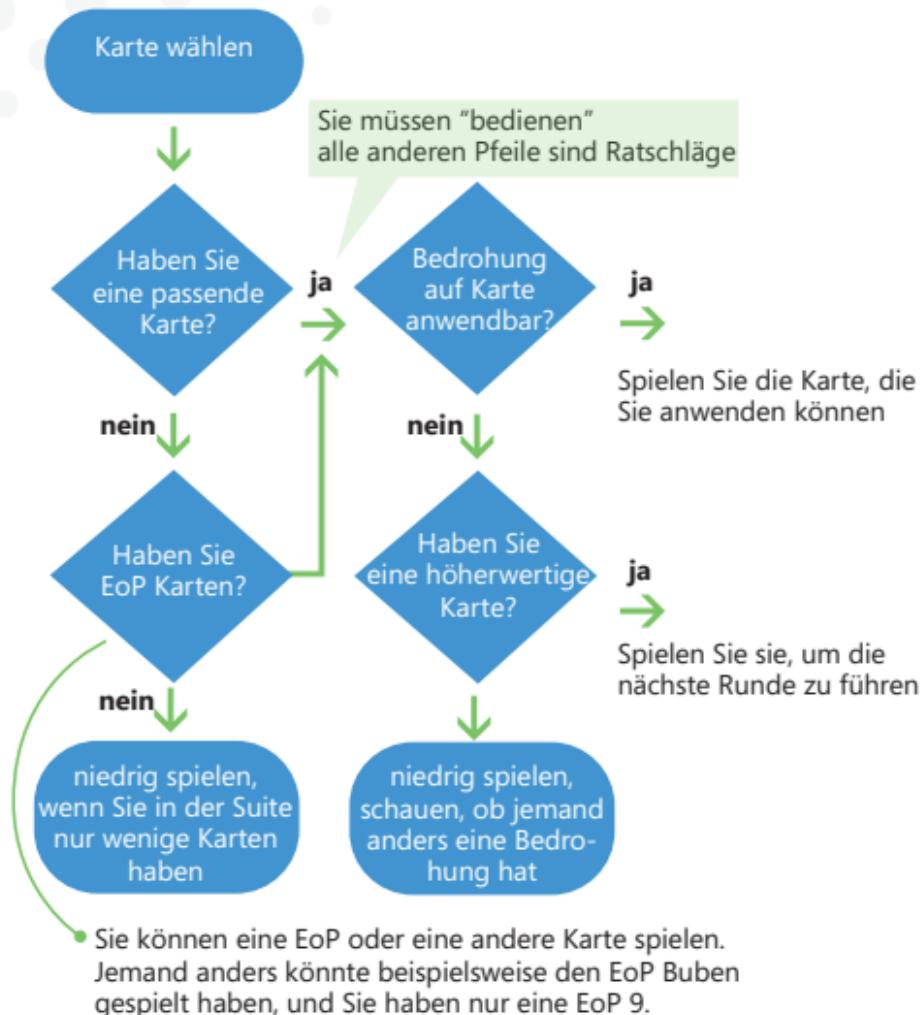
Context



Play



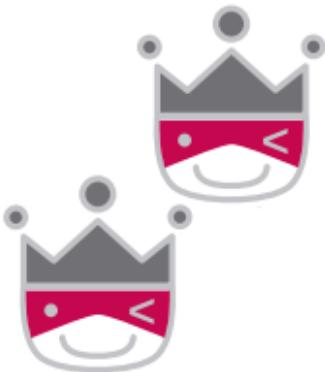
Strategie



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®

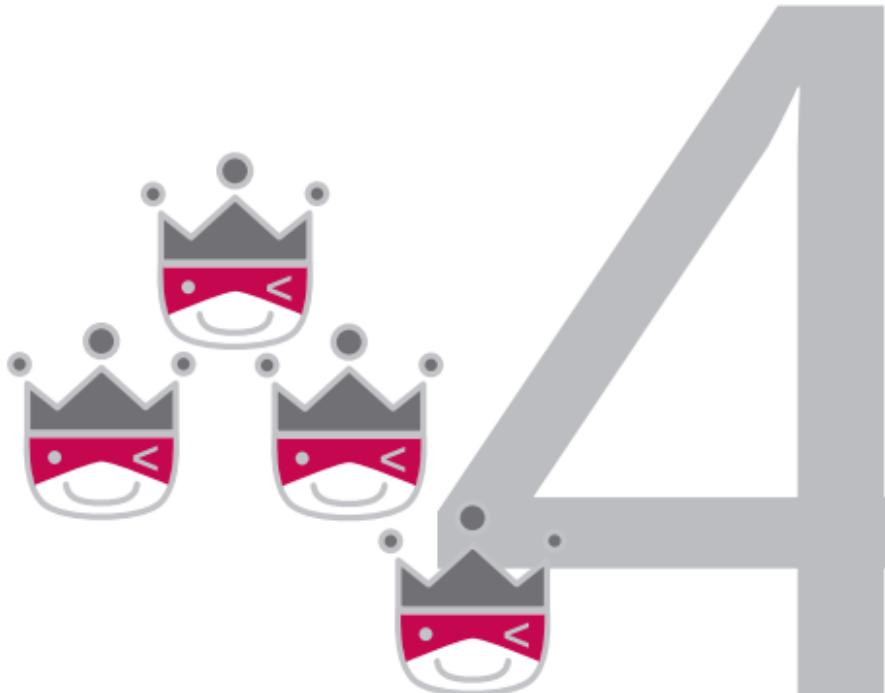
elevation of privilege



4

Spoofing

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



Microsoft®

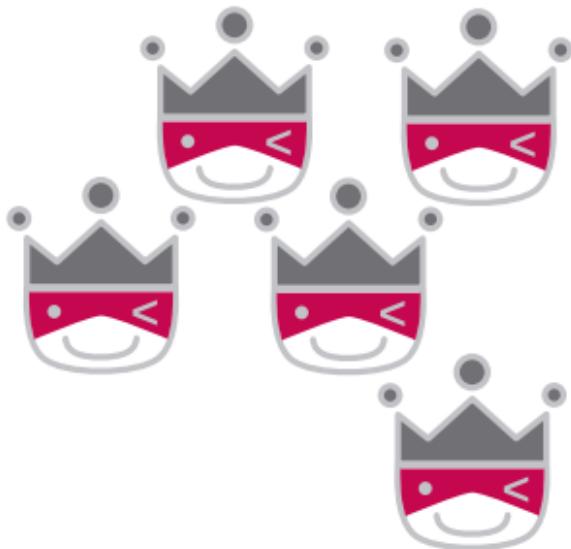
elevation of privilege



5

Spoofing

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



Microsoft®

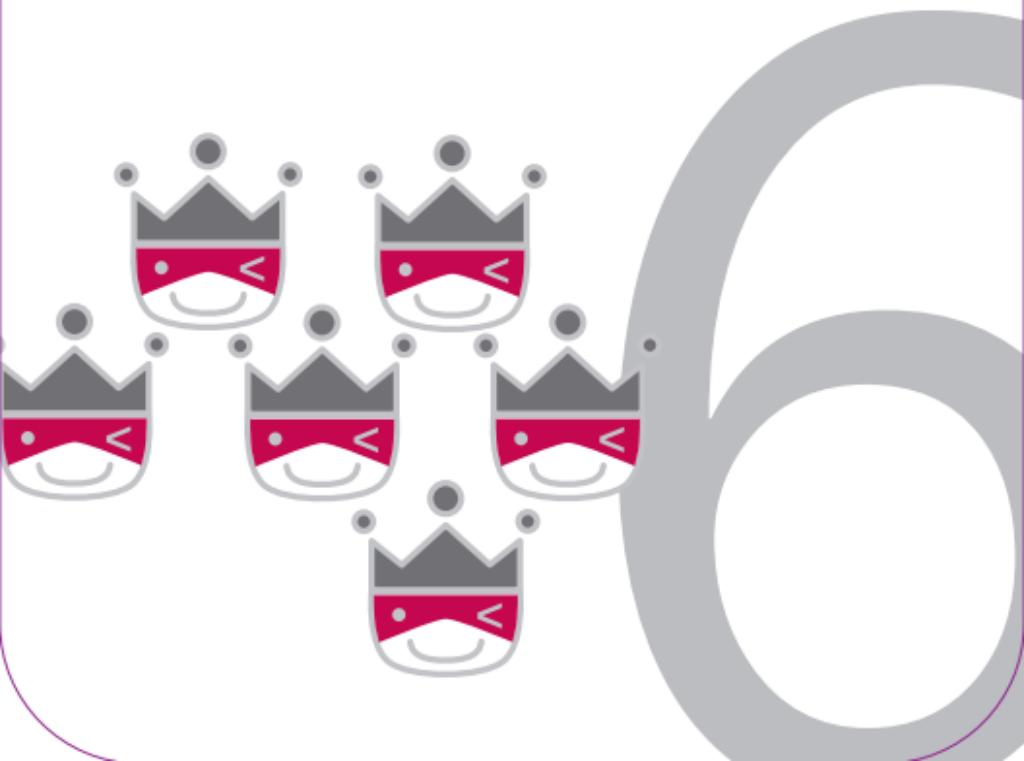
elevation of privilege



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®

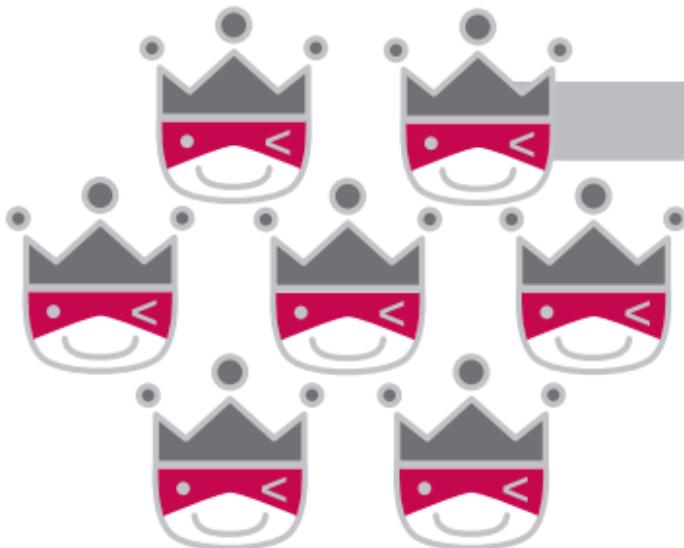
elevation of privilege



7

Spoofing

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



Microsoft®

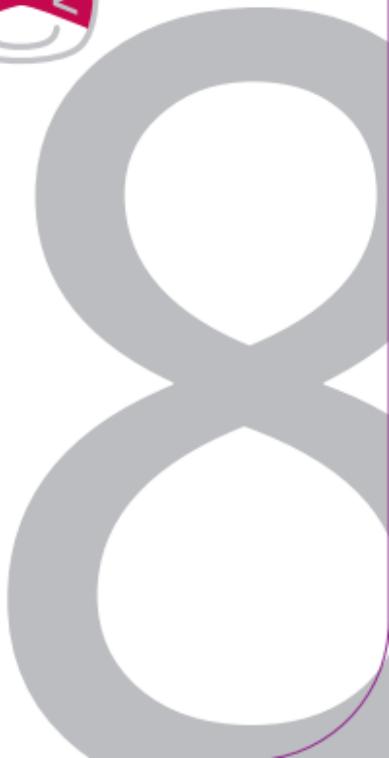
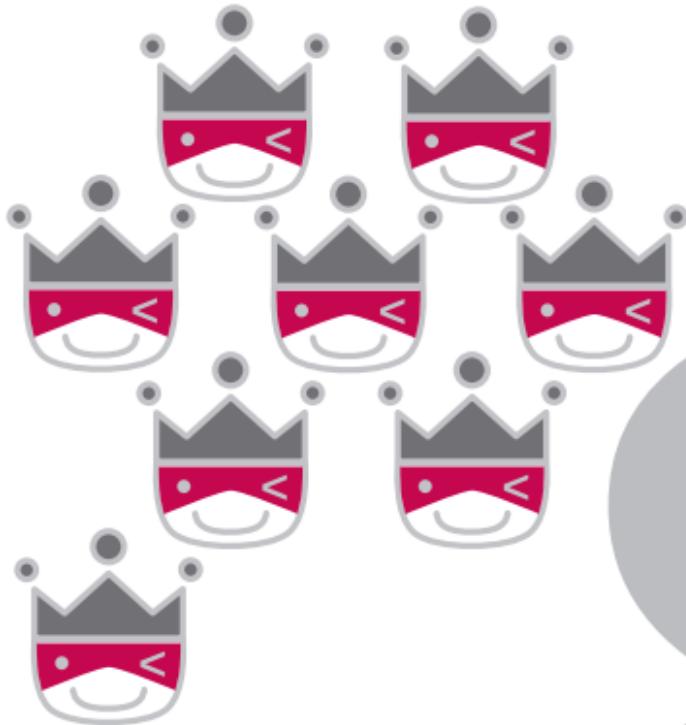
elevation of privilege



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®

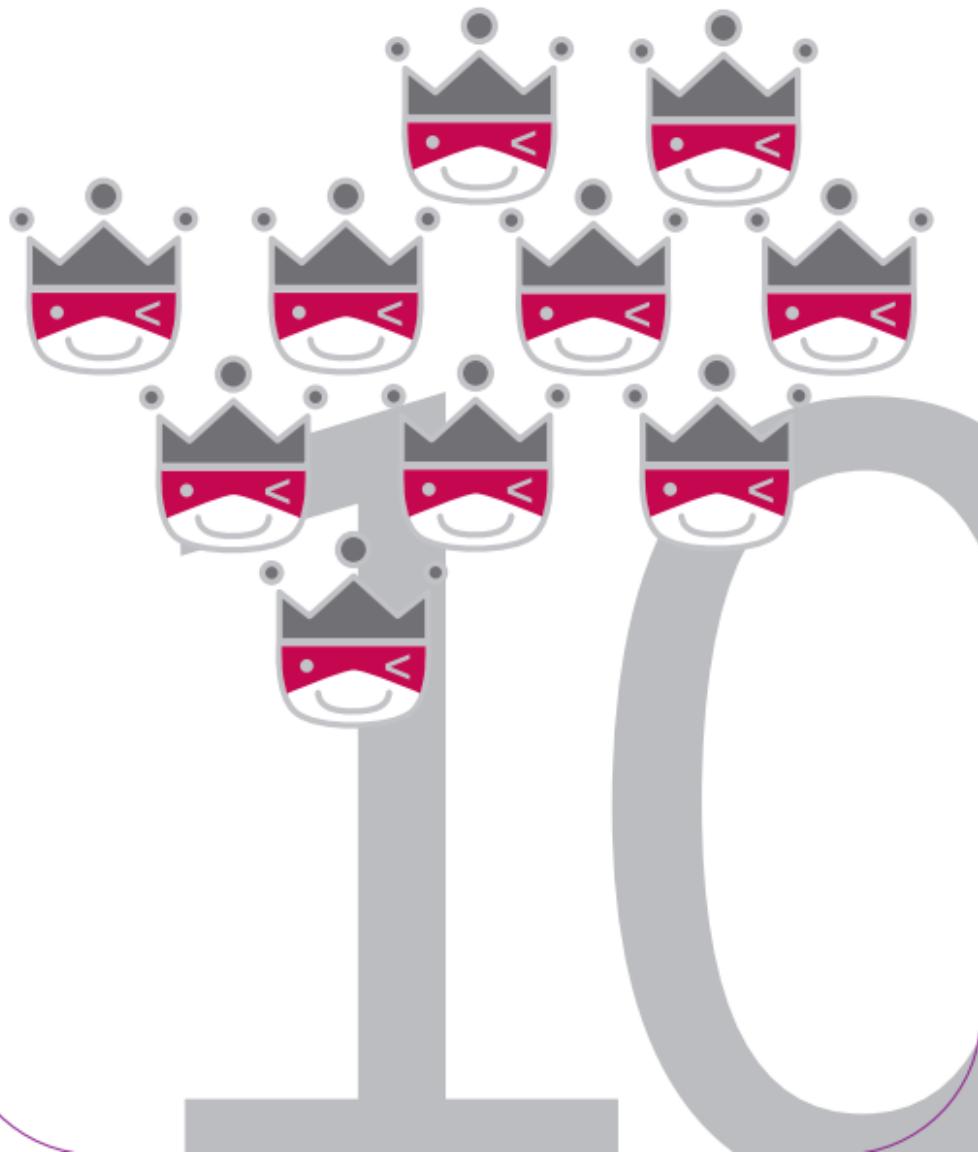
elevation of privilege



10

Spoofing

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



Microsoft®

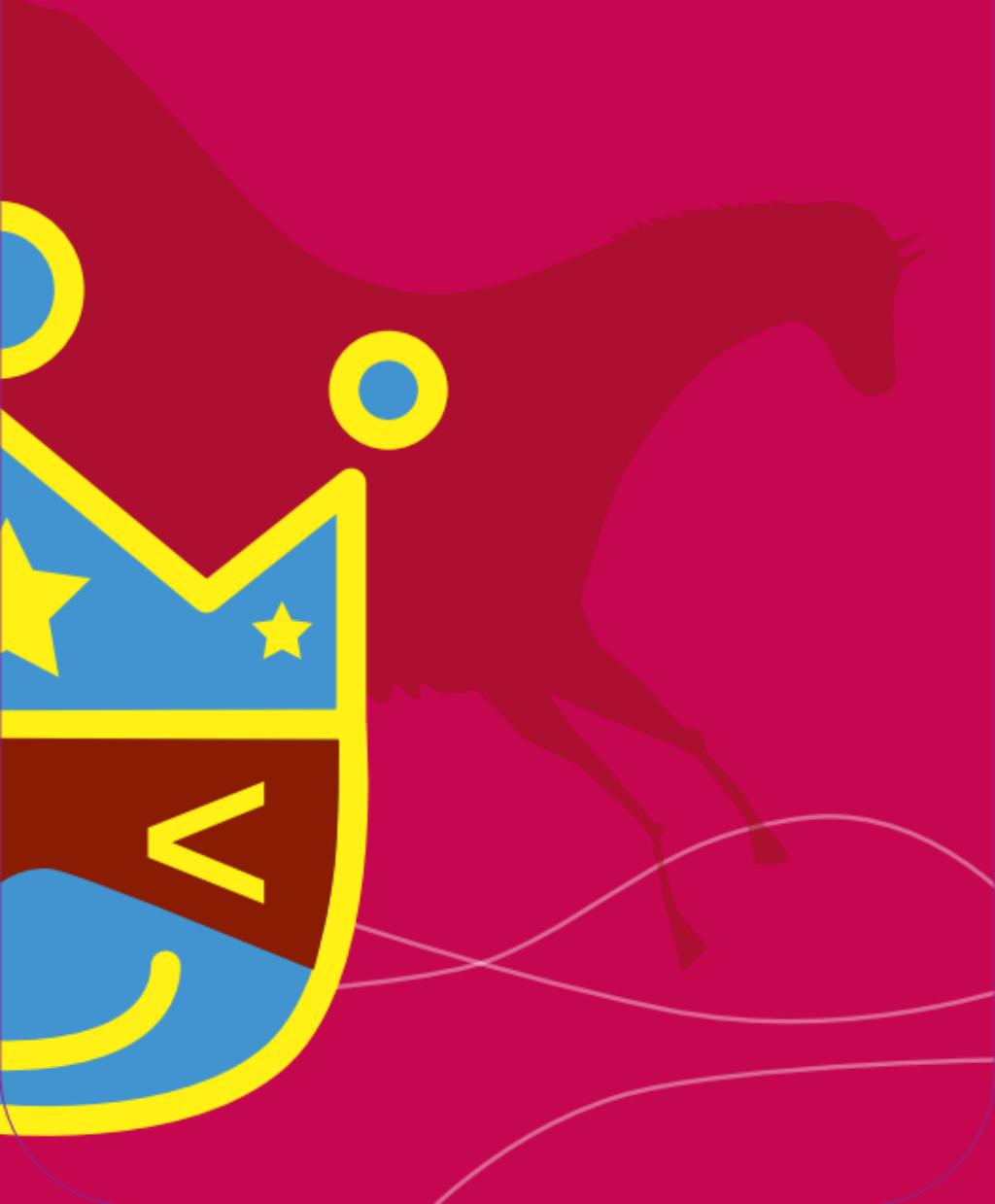
elevation of privilege



J

Spoofing

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



Microsoft®

elevation of privilege



Q

Spoofing

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



Microsoft®

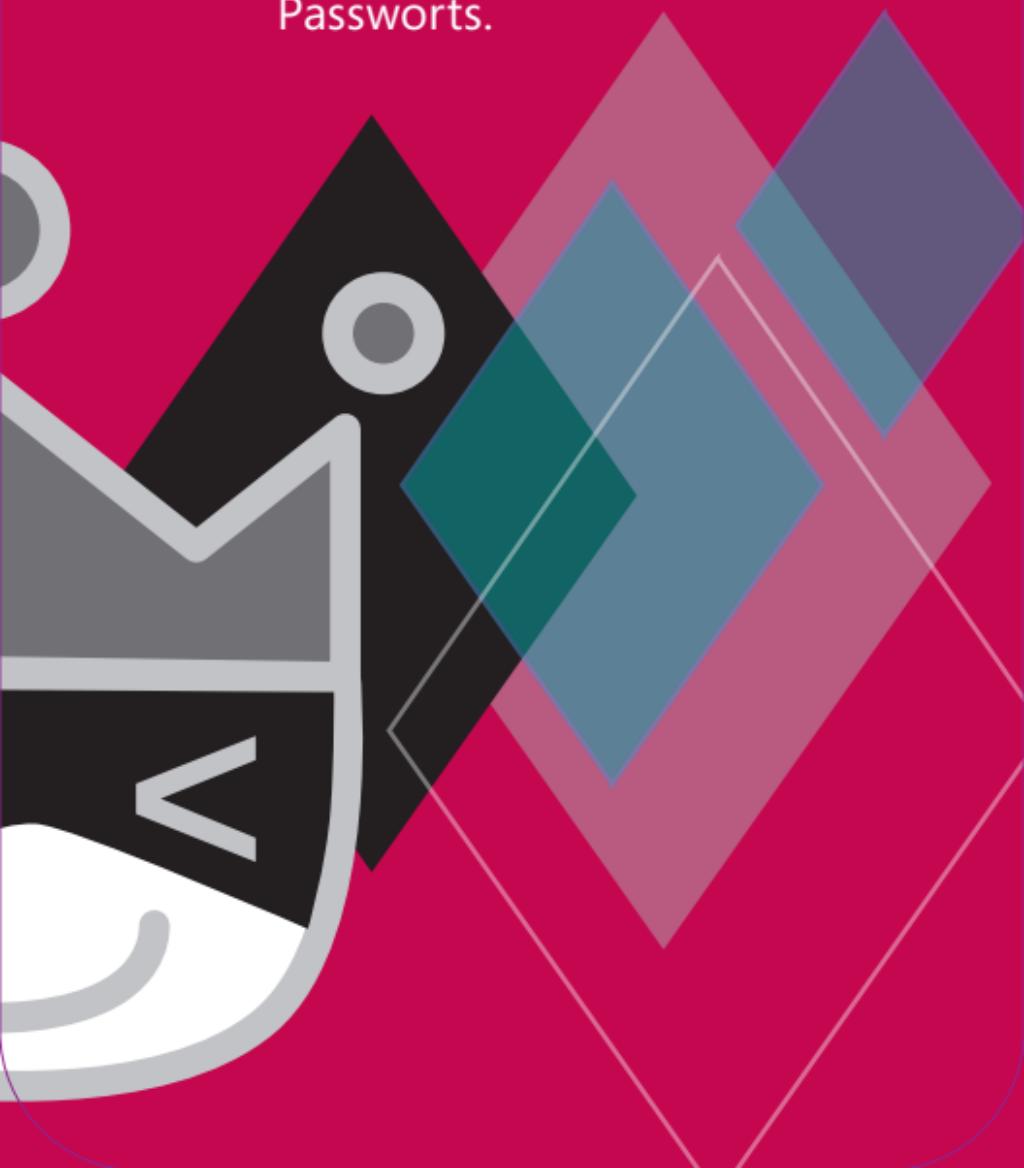
elevation of privilege



K

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®

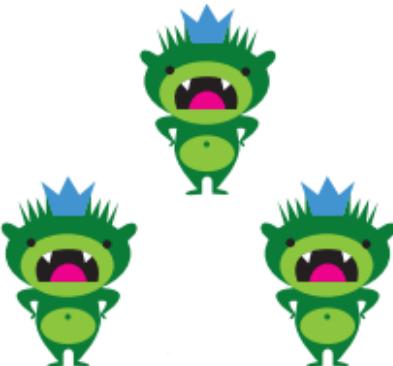
elevation of privilege



3

Tampering

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



Microsoft®

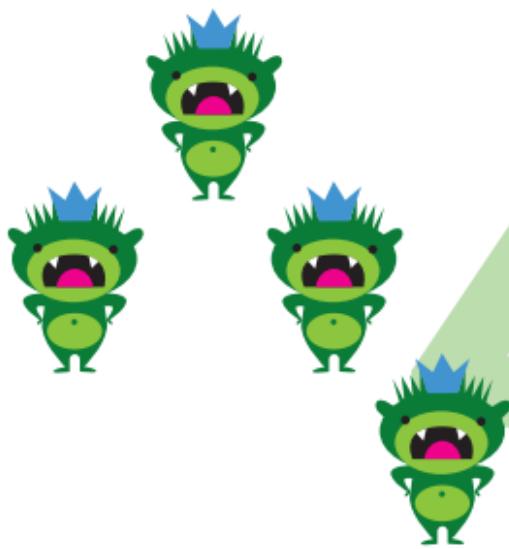
elevation of privilege



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®

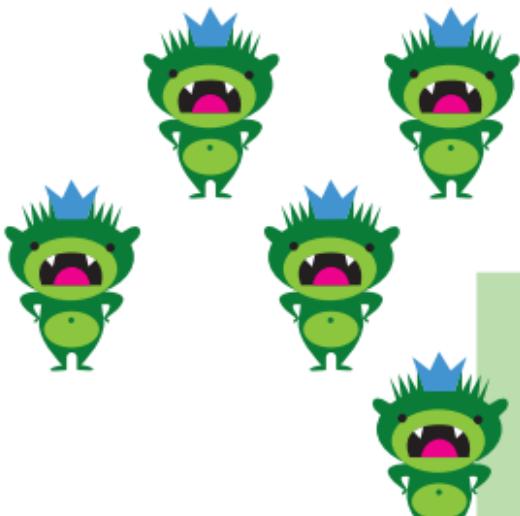
elevation of privilege



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®

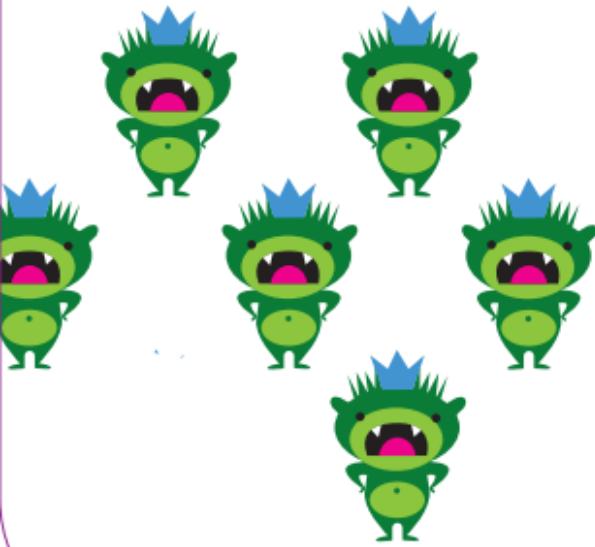
elevation of privilege



6

Tampering

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



Microsoft®

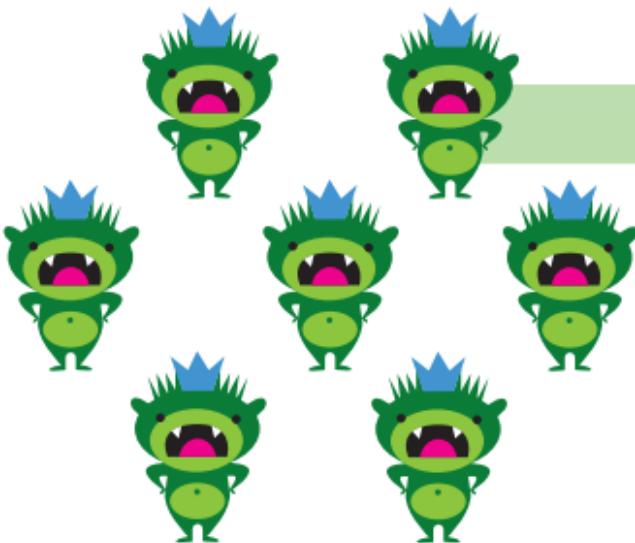
elevation of privilege



7

Tampering

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



Microsoft®

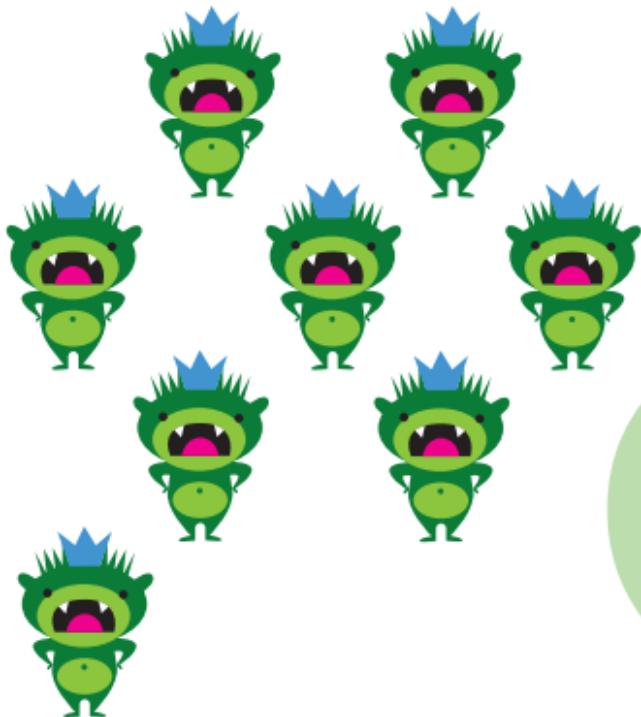
elevation of privilege



8

Tampering

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



Microsoft®

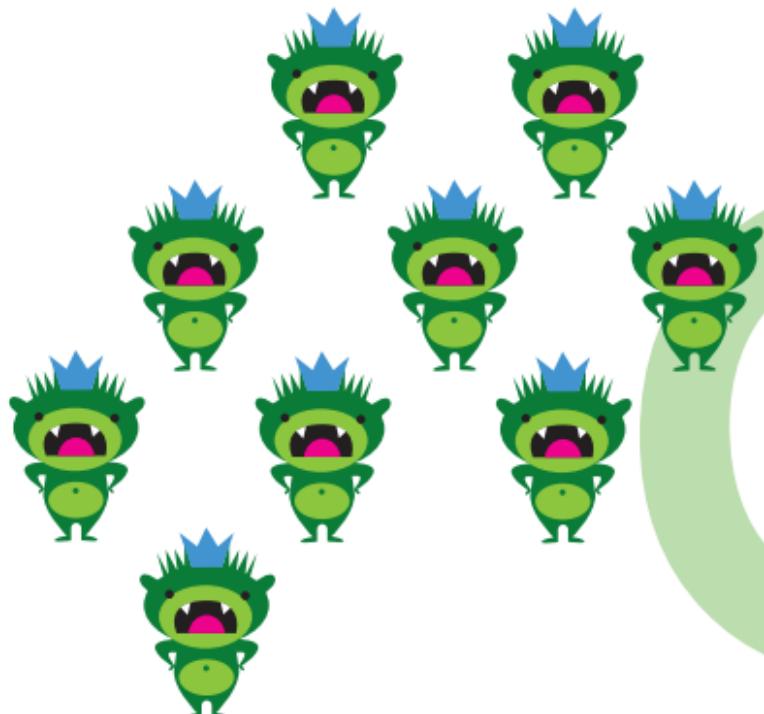
elevation of privilege



9

Tampering

Ein Angreifer kann Statusinformationen beeinflussen.



Microsoft®

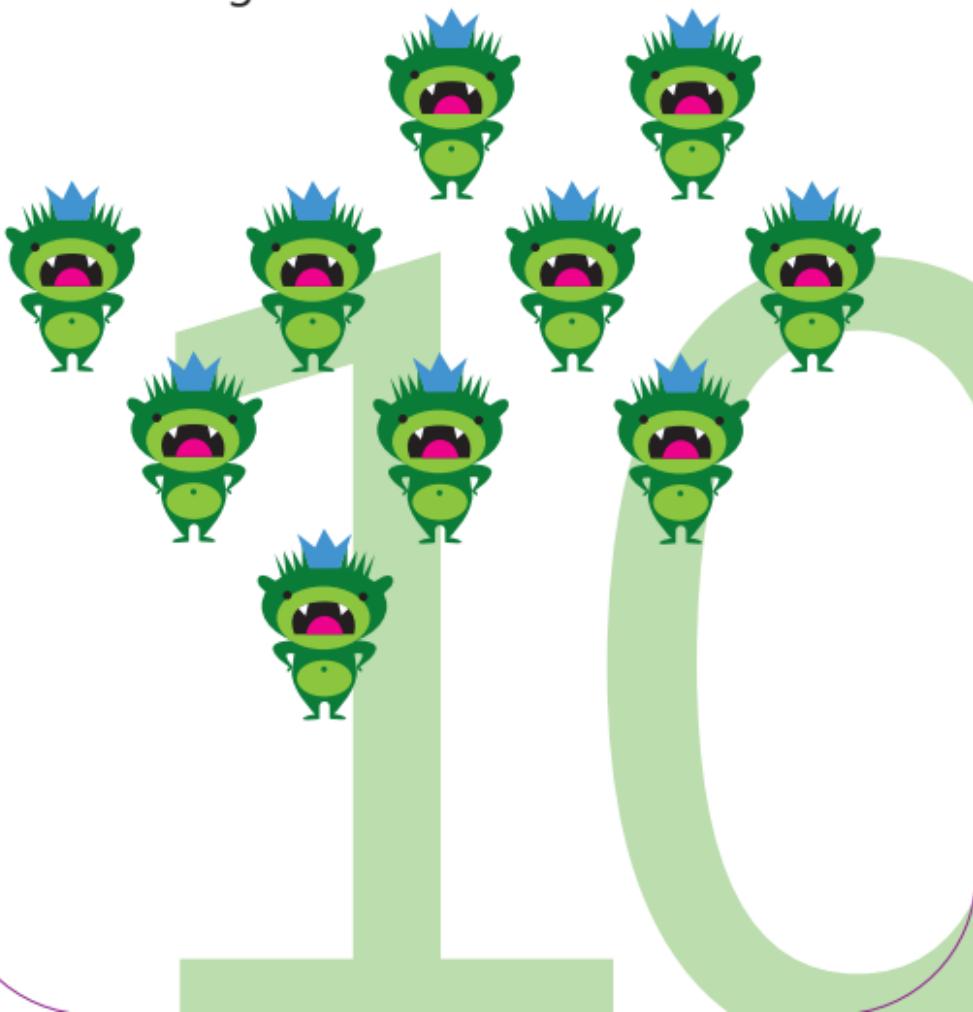
elevation of privilege



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.

R
R

2

Microsoft®

elevation of privilege



3

Repudiation

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

R
R R

3

Microsoft®

elevation of privilege



4

Repudiation

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



Microsoft®

elevation of privilege



5

Repudiation

Ein Angreifer kann Lognachrichten verändern, die über das 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 Zeitsstempel).



R R
R R R
R

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.

R R
R R R
R R
R

8

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 mitgeologt 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

Repudiation

Sie haben einen neuen
Repudiation Angriff erfunden.

RA

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 sicherheits-relevante 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.



Found it!

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.



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®

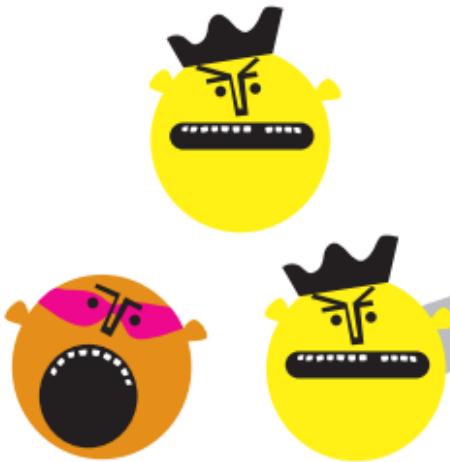
elevation of privilege



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®

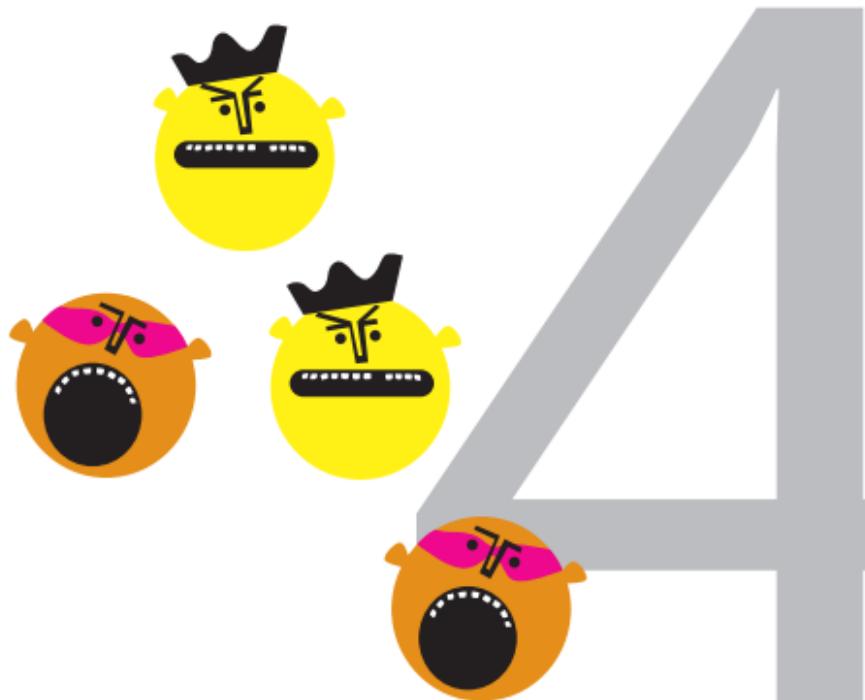
elevation of privilege



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®

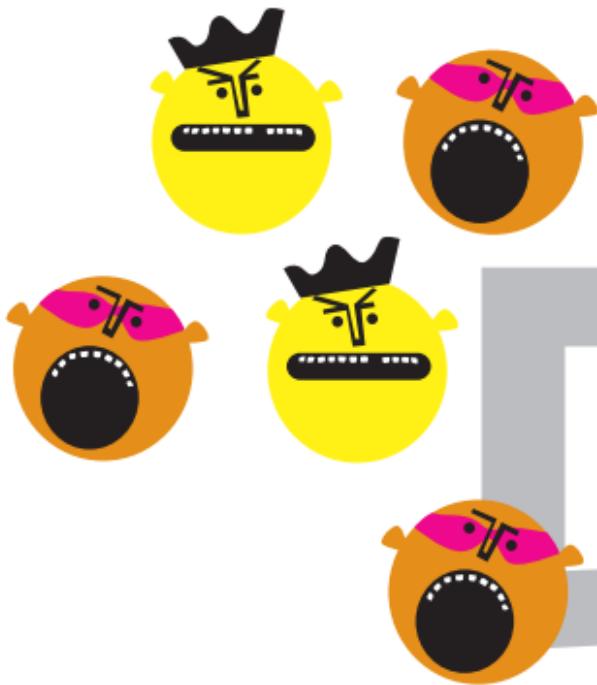
elevation of privilege



5

Denial of Service

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



Microsoft®

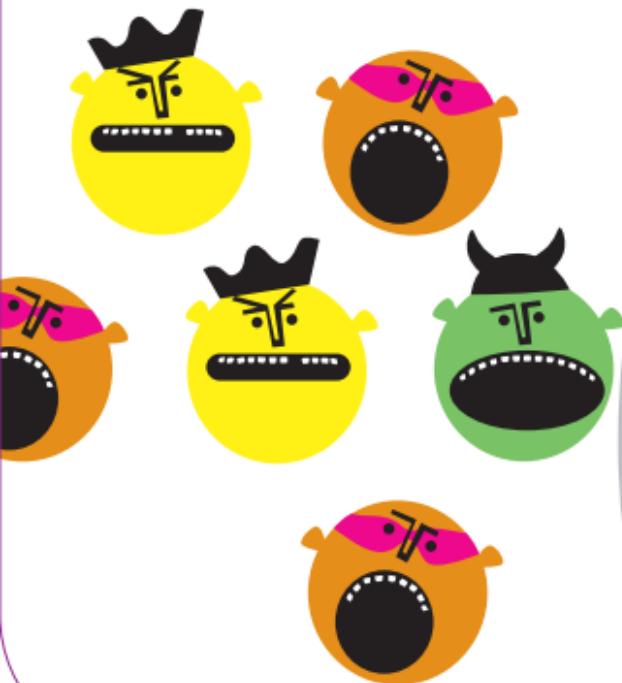
elevation of privilege



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®

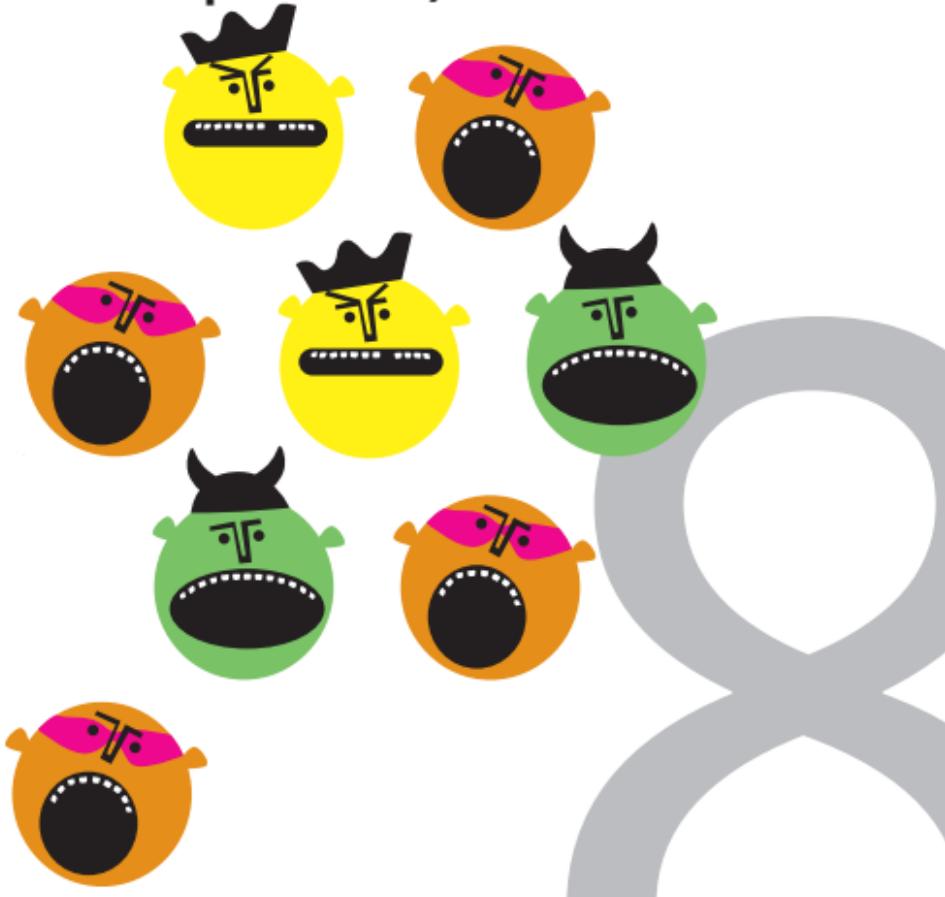
elevation of privilege



8

Denial of Service

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



Microsoft®

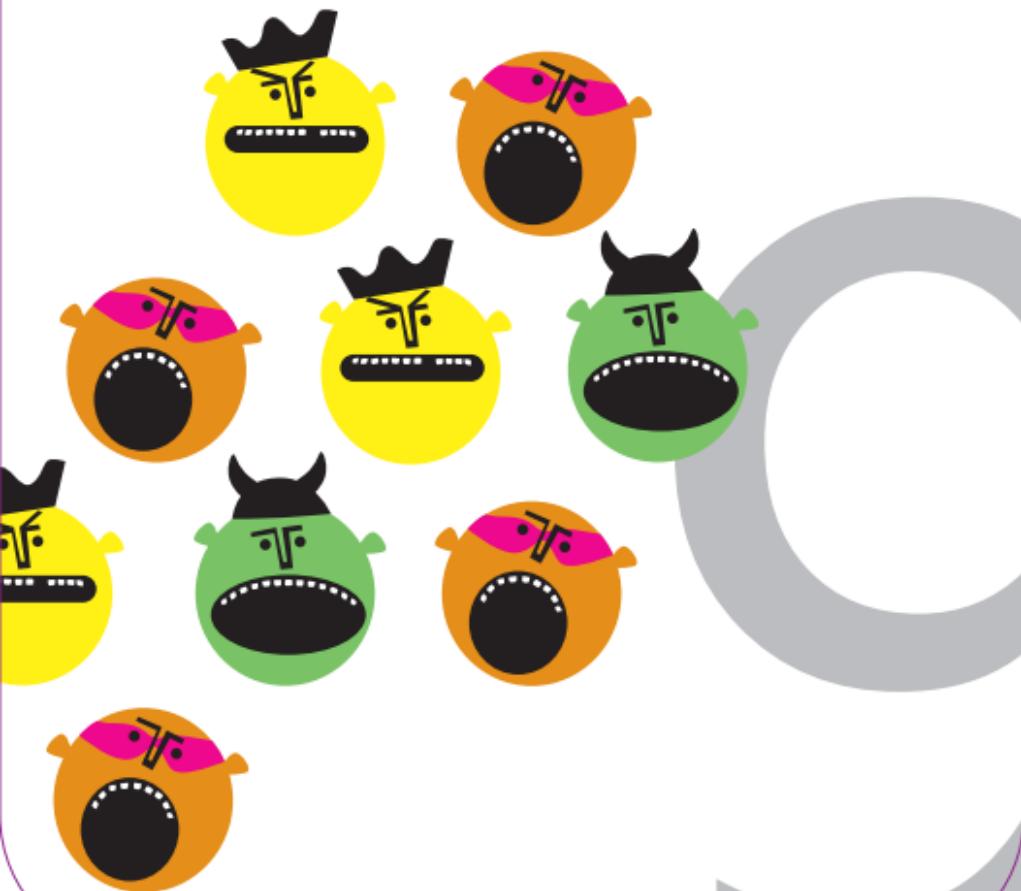
elevation of privilege



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®

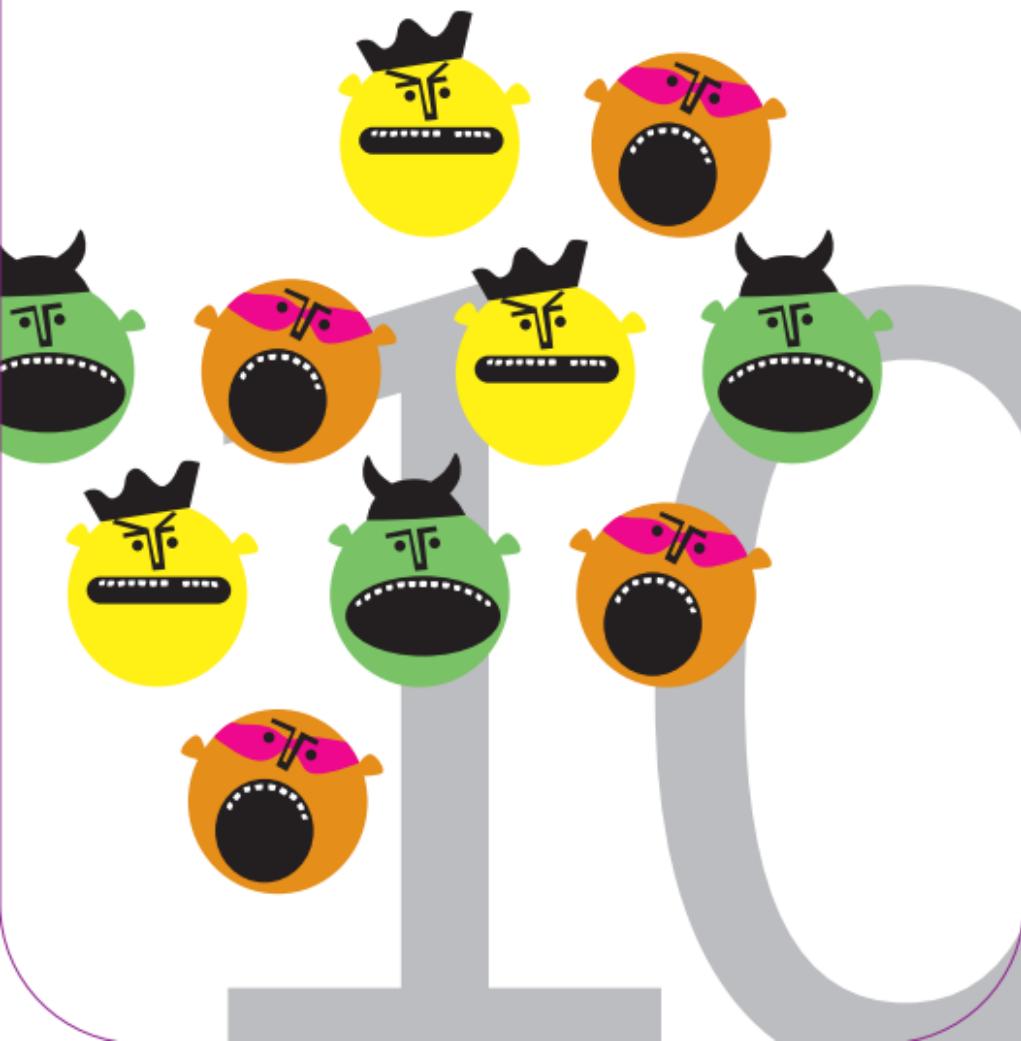
elevation of privilege



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 (volumen-basierte) 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®

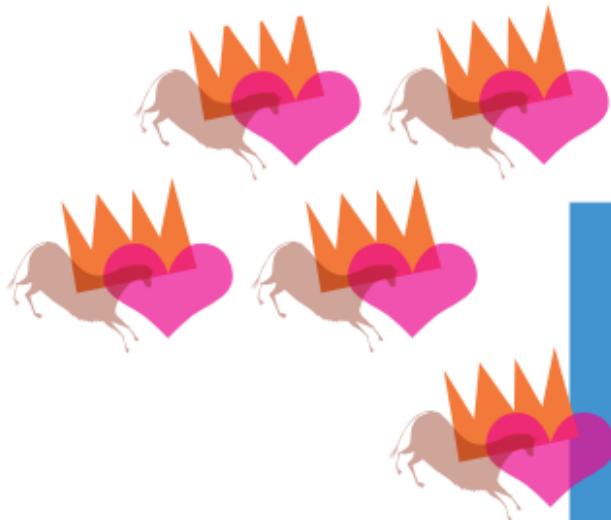
elevation of privilege



5

Elevation of Privilege

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



Microsoft®

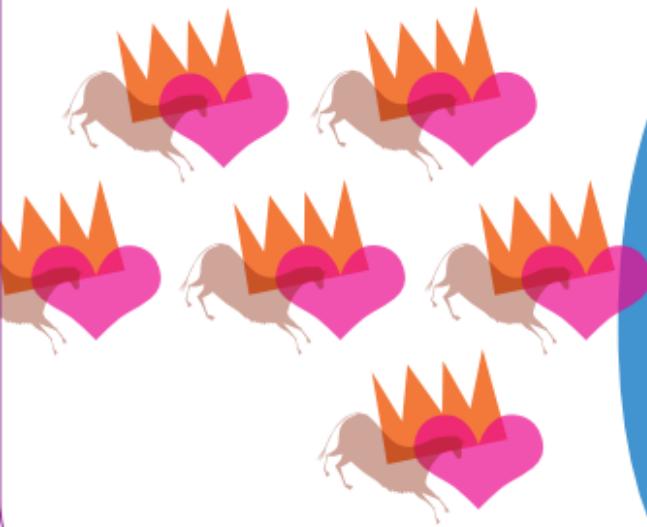
elevation of privilege



6

Elevation of Privilege

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



Microsoft®

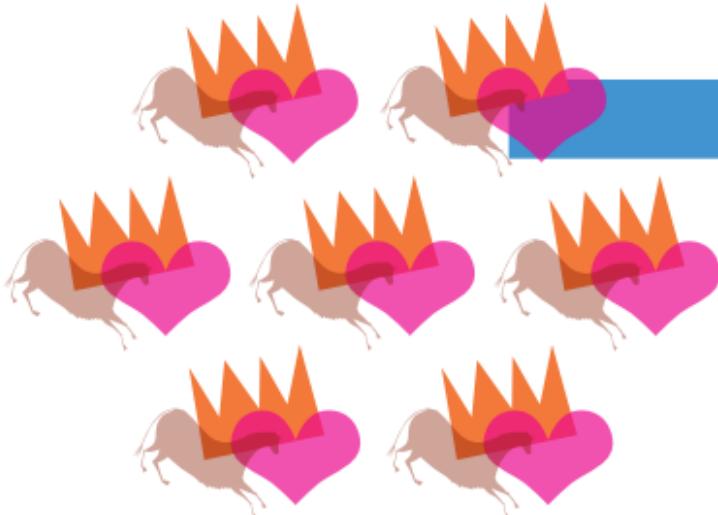
elevation of privilege



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®

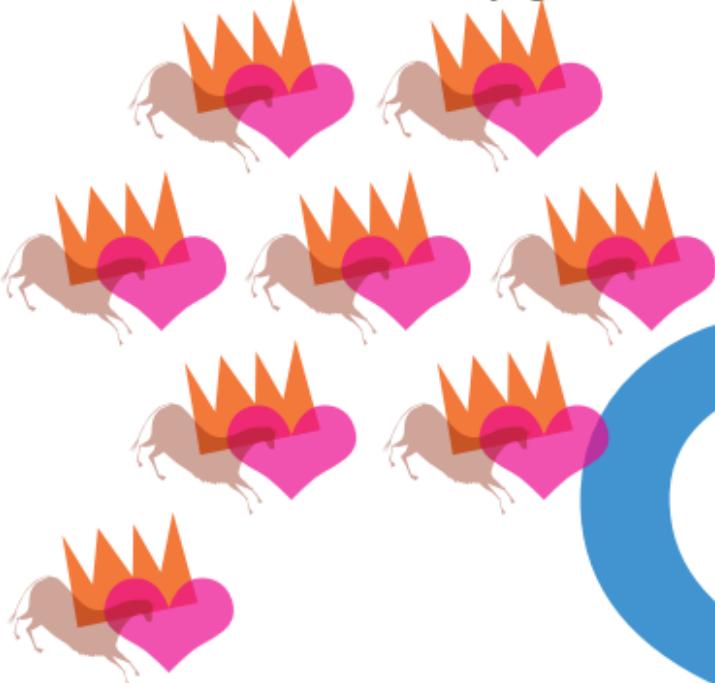
elevation of privilege



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®

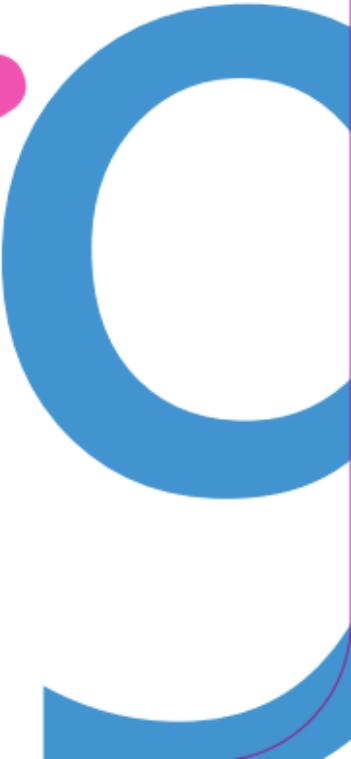
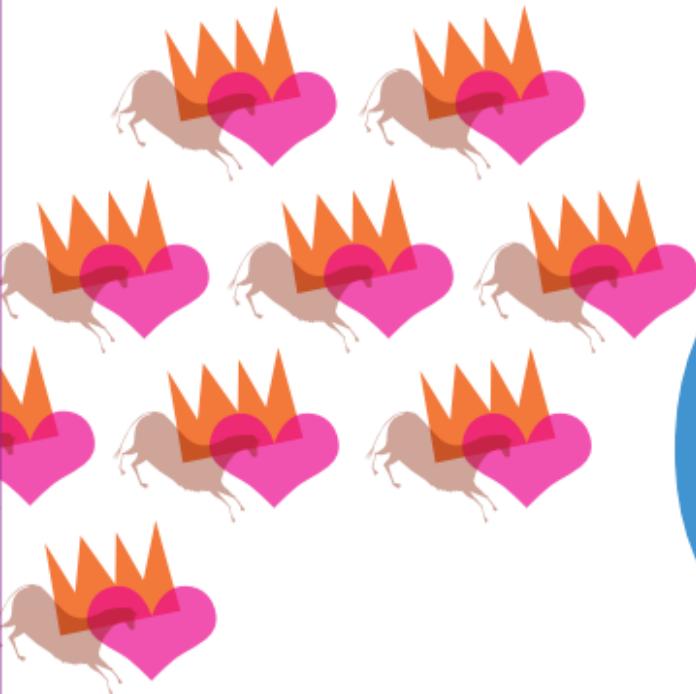
elevation of privilege



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®

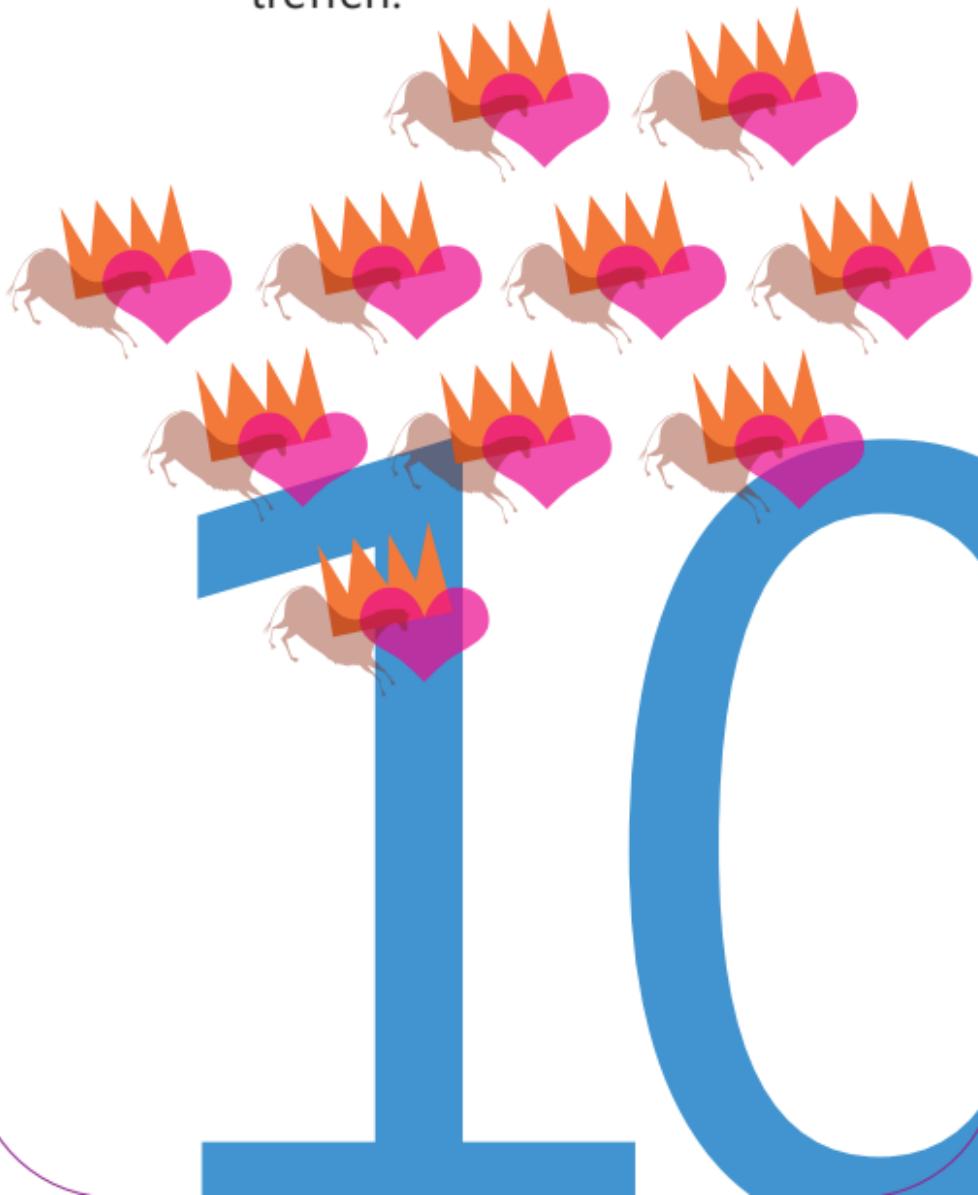
elevation of privilege



10

Elevation of Privilege

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



Microsoft®

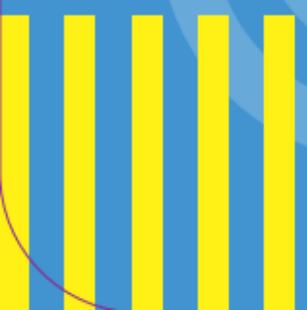
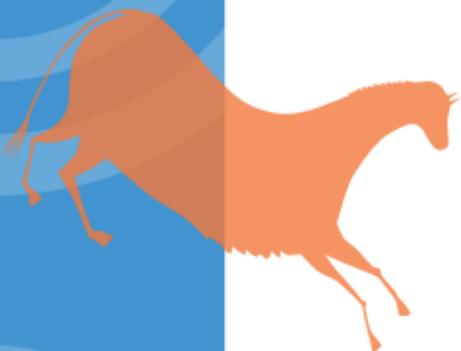
elevation of privilege



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®

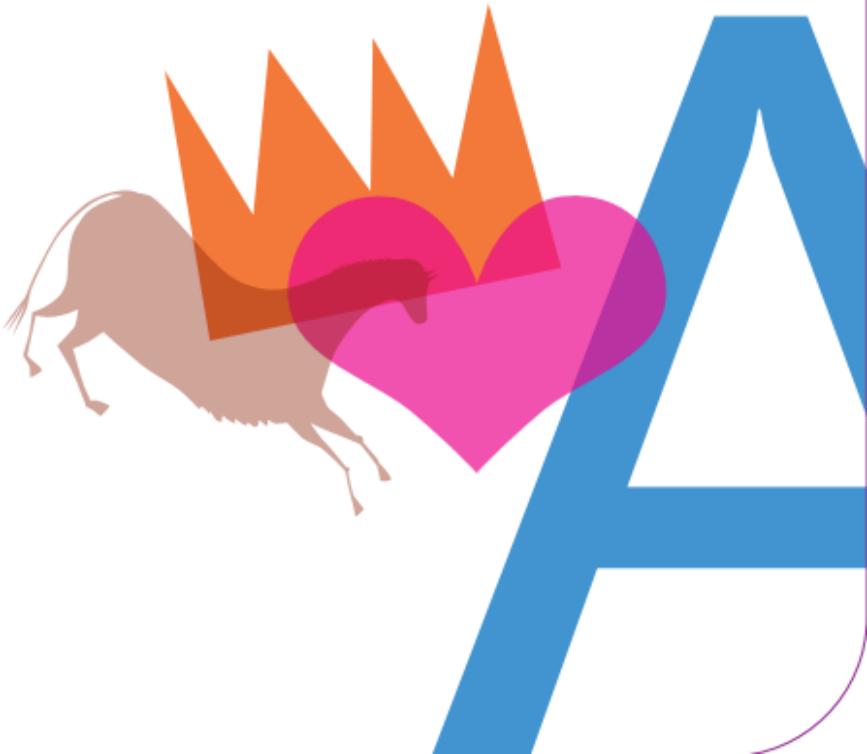
elevation of privilege



A

Elevation of Privilege

Sie haben einen neuen
Elevation of Privilege Angriff
erfunden.



Microsoft®

elevation of privilege





Spoofing

2. Ein Angreifer "sitzt" (lauscht) auf einem zufälligen Port oder Socket, den der Server üblicherweise nutzt.
3. Ein Angreifer kann alle möglichen Credentials der Reihe nach durchprobieren (online oder offline) und es gibt keinen Mechanismus, der ihn ausbremsst.
4. Ein Angreifer kann sich anonym verbinden, weil Sie davon ausgehen, dass Authentisierung auf einer höheren Schicht stattfindet.
5. Ein Angreifer kann einen Client verwirren, weil es zu viele Wege gibt, einen Server zu identifizieren.
6. 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).
7. Ein Angreifer kann sich zu einem Server oder Peer über einen nicht authentisierten unverschlüsselten Kanal verbinden.

Fortsetzung umseitig

Spoofing



Spoofing cont.

8. Ein Angreifer kann auf einem Server gespeicherte Credentials stehlen und wieder verwenden (z.B. Schlüssel in einer für andere lesbaren Datei).
9. Ein Angreifer, der Zugang zu einem Passwort bekommt, kann es wieder verwenden (nutzen Sie stärkere Authentisierungsmethoden).
10. Ein Angreifer kann wählen, dass eine schwächere oder gar keine Authentisierung genutzt wird.
- J. Ein Angreifer kann die auf einem Client gespeicherten Credentials stehlen und wieder verwenden.
- Q. Ein Angreifer kann den Mechanismus angreifen, mit dem Passwörter zurückgesetzt oder aktualisiert werden (Account Recovery erfordert nicht die Eingabe des alten Passworts).
- K. Ihr System wird mit einem Default Adminpasswort ausgeliefert und erzwingt nicht die Änderung dieses Passworts. doesn't force a change.
- A. Sie haben einen neuen Spoofing Angriff erfunden.

Spoofing



Tampering

3. Statt auf Standard-Kryptografie zurück zu greifen, haben Sie sich selbst einen Mechanismus zur Gewährleistung von Integrät oder für den Schlüsselaustausch ausgedacht. Ein Angreifer kann sich dies zunutze machen.
4. Ihr Code trifft Entscheidungen zur Zugangskontrolle an vielen unterschiedlichen Stellen, anstatt diese Funktion an zentraler Stelle (in einem Security Kernel) zu implementieren.
5. 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.
6. Ein Angreifer kann Daten an Speicherorten schreiben, an denen Ihr Code liegt oder die durch Ihren Code interpretiert werden.
7. Ein Angreifer kann Berechtigungen umgehen, weil Sie Namen nicht kanonisieren (normalisieren), bevor Zugriffsrechte geprüft werden.
8. Ein Angreifer kann Daten manipulieren, die per Netzwerk übertragen werden, weil Ihr Code keine Integritätssicherung vorsieht.

Fortsetzung umseitig

Tampering



Tampering cont.

9. Ein Angreifer kann Statusinformationen beeinflussen.
 10. 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.
- J. Ein Angreifer kann auf eine Ressource schreiben, weil es keine ACLs gibt, oder weil jeder berechtigt ist (world writable).
- Q. 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).
- K. Ein Angreifer kann Code mithilfe eines Extension Points einbinden.
- A. Sie haben einen neuen Tampering Angriff erfunden.

Tampering

R

Repudiation

2. 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.
3. Ein unprivilegierter Nutzer oder Angreifer hat lesend Zugang zu interessanten Sicherheitsinformationen in den Logs.
4. Ein Angreifer kann digitale Signaturen manipulieren, weil Sie einen MAC Algorithmus statt eines Signierverfahrens nutzen, oder weil das Signierverfahren unsicher ist.
5. Ein Angreifer kann Lognachrichten verändern, die übers Netz übertragen werden, weil kein starker Mechanismus zur Gewährleistung der Integrität implementiert ist.
6. Ein Angreifer kann einen Logeintrag ohne Zeitstempel erzeugen (oder die Logs haben generell keine Zeitstempel).
7. Ein Angreifer kann das Log zum Überlaufen bringen, so dass alte Logdaten überschrieben werden und somit verloren sind (wrap-around).

Fortsetzung umseitig

Repudiation

R

Repudiation cont.

8. Ein Angreifer kann das Logging so austricksen, dass sicherheitsrelevante Logdaten nicht geschrieben werden oder durcheinander geraten.
 9. Ein Angreifer kann einen Shared Key nutzen, um sich als jemand anders auszugeben, so dass seine Aktionen ebenfalls unter dieser Identität mitgeloggt werden.
 10. Ein Angreifer kann beliebige Logdaten in ein Logsystem einschleusen, weil die Logquellen nicht oder nur schwach authentisiert werden.
- J. Ein Angreifer kann unbemerkt Logs editieren, löschen oder deren Übermittlung unterbinden.
- Q. Ein Angreifer kann abstreiten, etwas getan zu haben und es gibt keine brauchbaren Daten, um das Gegenteil zu beweisen.
- K. Das System hat keine Logs.
- A. Sie haben einen neuen Repudiation Angrif erfunden.

Repudiation



Information Disclosure

2. Ein Angreifer kann verschlüsselte Dateien mittels Brute-Force entschlüsseln, weil keine geeigneten Sicherheitsmaßnahmen dagegen vorhanden sind.
3. Ein Angreifer kann sicherheitsrelevante Fehlermeldungen sehen.
4. Ein Angreifer kann Dateninhalte lesen, weil die Nachrichten (z.B. E-Mails oder Cookies) nicht verschlüsselt sind, selbst wenn der Transportkanal verschlüsselt ist.
5. Ein Angreifer kann unter Umständen Daten lesen, die mit einem nicht standardisierten kryptografischen Algorithmus verschlüsselt sind.
6. 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.
7. Ein Angreifer kann als "Man in the Middle" verschlüsselte Daten lesen, weil die Endpunkte einer Netzwerkverbindung nicht authentisiert sind.

Fortsetzung umseitig

Information Disclosure



Information Disclosure cont.

- 8. Ein Angreifer kann (sensible) Informationen mithilfe eines Such-Indexers, Loggers oder eines anderen Mechanismus zugreifen.
- 9. Ein Angreifer kann sensible Informationen in einer Datei lesen, weil deren Zugriffsrechte falsch gesetzt sind (schwache ACL).
- 10. Ein Angreifer kann mangels Zugriffsbeschränkung eine sensible Datei lesen.
- J. Ein Angreifer kann den statischen Schlüssel finden, der zur Verschlüsselung genutzt wird.
- Q. Ein Angreifer kann einen Kommunikationskanal vollständig mitlesen, weil dieser unverschlüsselt ist.
- K. Ein Angreifer kann Netzwerkinformationen lesen, weil keine Kryptografie genutzt wird.
- A. Sie haben einen neuen Information Disclosure Angriff erfunden.

Information Disclosure



Denial of Service

2. Ein Angreifer kann Ihr Authentisierungs-System unbrauchbar oder unverfügbar machen.
3. Ein Angreifer kann einen Client unverfügbar oder unbrauchbar machen, aber das Problem verschwindet, sobald der Angriff aufhört (**Client, authentisiert, temporär**).
4. Ein Angreifer kann einen Server unverfügbar oder unbrauchbar machen, aber das Problem verschwindet, sobald der Angriff aufhört (**Server, authentisiert, temporär**).
5. Ein Angreifer kann einen Client unverfügbar machen, ohne dass eine Authentisierung stattgefunden hat. Das Problem verschwindet nach dem Angriff (**Client, anonym, temporär**).
6. Ein Angreifer kann einen Server unverfügbar machen, ohne dass eine Authentisierung stattgefunden hat. Das Problem verschwindet nach dem Angriff (**Server, anonym, temporär**).
7. Ein Angreifer kann einen Client unverfügbar machen und das Problem besteht fort, nachdem der Angriff aufgehört hat (**Client, authentisiert, persistent**).

Denial of Service



Denial of Service cont.

8. Ein Angreifer kann einen Server unverfügbar machen und das Problem besteht fort, nachdem der Angriff aufgehört hat (**Server, authentisiert, persistent**).
 9. 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**).
 10. Ein Angreifer kann, ohne zu authentisieren, einen Server unverfügbar machen. Das Problem besteht fort, nachdem der Angriff aufgehört hat (**Server, anonym, persistent**).
- J. Ein Angreifer kann das Logging-Subsystem außer Betrieb setzen.
- Q. Ein Angreifer kann eine verwundbare Systemkomponente dazu missbrauchen, eine (volumenbasierte) DoS Attacke um den Faktor 10 zu verstärken.
- K. Ein Angreifer kann eine verwundbare Systemkomponente dazu missbrauchen, eine DoS Attacke mehr als 100fach zu verstärken.
- A. Sie haben eine neue DoS Attacke erfunden.

Denial of Service



Elevation of Privilege (EoP)

5. Ein Angreifer kann Einfluss darauf nehmen, welche Art Validierung Daten durchlaufen, die jeweils unterschiedliche Ergebnisse liefern.
6. Ein Angreifer kann Berechtigungen für sich ausnutzen, die Ihr Programm verlangt, aber nicht wirklich benötigt.
7. Ein Angreifer kann einen Pointer über eine Trust-Boundary hinweg angeben, anstatt Daten eingeben zu müssen, die eine Validierung durchlaufen.
8. Eingegebene Daten befinden sich während der Überprüfung noch unter Kontrolle des Angreifers und werden später jenseits der Trust-Boundary genutzt.
9. Caller (aufrufende Funktionen) haben keine Möglichkeit zu überprüfen, welche Validierung Ihr Programm auf die übergebenen Daten anwendet, bevor sie diese weitergeben.
10. Es ist für einen Aufrufer / Caller nicht klar ersichtlich, welche Sicherheitsmaßnahmen Sie treffen.
- J. Ein Angreifer kann Eingaben zum Nutzer zurückspiegeln, z.B. per Cross-Site-Scripting (XSS).

Fortsetzung umseitig

Elevation of Privilege



Elevation of Privilege cont.

- Q.** Sie inkludieren User Generated Content (UGC) in Ihrer Webseite, der auch Inhalte beliebiger URLs etc. enthalten kann.
- K.** Ein Angreifer kann ein Kommando einschleusen, welches vom System mit einer höheren Berechtigung ausgeführt wird.
- A.** Sie haben einen neuen Elevation of Privilege Angriff erfunden.

Elevation of Privilege

About

Threat Modeling

The Elevation of Privilege game is designed to be the easiest way to start looking at your design from a security perspective. It's one way to threat model, intended to be picked up and used by any development group. Because the game uses STRIDE threats, it gives you a framework for thinking, and specific actionable examples of those threats.

STRIDE stands for:

Spoofing: Impersonating something or someone else.

Tampering: Modifying data or code.

Repudiation: Claiming not to have performed an action.

Information Disclosure: Exposing information to someone not authorized to see it.

Denial of Service: Denying or degrading service to users.

Elevation of Privilege: Gain capabilities without proper authorization.

At www.microsoft.com/security/sdl/eop we have videos, score sheets and tips and tricks for playing.

About



SDL

The Elevation of Privilege game is a fun and easy way to get started understanding the security of your systems by threat modeling. As you discover and correct design-level security problems, it's worth thinking about the other ways security issues can creep into your code. Microsoft has a large collection of free resources available to help you get started with the Security Development Lifecycle (SDL).

To learn more about threat modeling and the Microsoft Security Development Lifecycle, visit our website at
microsoft.com/sdl/

Microsoft®

Security Development Lifecycle