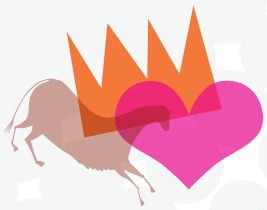


Elevation of Privilege (EoP)

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.

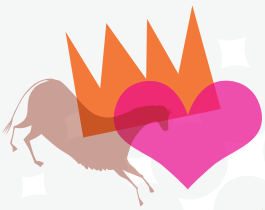
9. Caller (aufrufende Funktionen) haben keine Möglichkeit zu überprüfen, welche Validierung Ihr Programm auf die übergebenen Daten anwendet, bevor sie diese weitergeben.

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.