

# Shellshock With all details

Proseminar - Aktuelle IT-Sicherheitsvorfälle und Lösungsansätze Martin Weiss, Kay Schmitteckert | 16. Dezember 2015

FORSCHUNGSGRUPPE DEZENTRALE SYSTEME UND NETZDIENSTE - TM & SCC



4日 5 4周 5 4 5 5 4 5

# **Agenda**



- Shellshock
- Hätte man Shellshock vorbeugen können?
- Präventive Verteidigungsmaßnahmen
- Maßnahmen gegen SQL-Injections
- Fazit und Resümee



#### Shellshock



#### Was ist Shellshock?

- Bash Sicherheitslücke
- Entdeckung September 2014
- Existiert seit 1989
- CVE-Nummern CVE-2014-6271, -7169, -7168, -7187, -6277, -6278

Shellshock Hätte man Shellshock vorbeugen können? Präventive Verteidigungsmaßnahmen Maßnahmen gegen SQL-Injections Fazit und F

3 Patches bis zur Behebung



#### Shellshock



#### Ausmaß des Exploits

- Bash Standard-Shell bei vielen unixoiden Systemen
- Großteil der Webserver laufen unter unixoiden Systemen
- Weltweit waren hunterte Millionen Computer betroffen
  - Unter anderem Server von Yahoo, Winzip und Lycos
- Forscher halten die Sicherheitslücke für gravierender als Heartbleed



### **Ungepatchte Bash**

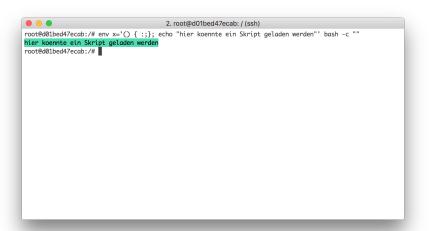






### **Ungepatchte Bash**







# Vorbeugung von Shellshock möglich?



Ja!



# Vorbeugung von Shellshock möglich?



- Präventive Verteidigungsmaßnahmen

# Vorbeugung von Shellshock möglich?



- Präventive Verteidigungsmaßnahmen
- Maßnahmen gegen SQL-Injections





#### Mehrschichtige Sicherheitsstrukturen

- Experten: Sicherheitslücken nicht zu 100% ausschließbar



#### Mehrschichtige Sicherheitsstrukturen

- Experten: Sicherheitslücken nicht zu 100% ausschließbar
- Können aber durch mehrschichtige Sicherheitsstrukturen migriert werden



#### Mehrschichtige Sicherheitsstrukturen

- Experten: Sicherheitslücken nicht zu 100% ausschließbar
- Können aber durch mehrschichtige Sicherheitsstrukturen migriert werden
- Torvalds: "The only real solution to security is to admit that bugs happen, and then mitigate them by having multiple layers, so if you have a hole in one component, the next layer will catch the issue."



- Zugriffskontrolle kann eine Schicht sein





- Zugriffskontrolle kann eine Schicht sein
- Zentrale Frage: Wer darf auf welche Daten lesen, schreiben, ausführen?





- Zugriffskontrolle kann eine Schicht sein
- Zentrale Frage: Wer darf auf welche Daten lesen, schreiben, ausführen?
- Drei grundlegene Modelle:





- Zugriffskontrolle kann eine Schicht sein
- Zentrale Frage: Wer darf auf welche Daten lesen, schreiben, ausführen?
- Drei grundlegene Modelle:





- Zugriffskontrolle kann eine Schicht sein
- Zentrale Frage: Wer darf auf welche Daten lesen, schreiben, ausführen?
- Drei grundlegene Modelle:
  - Mandatory Access Control (MAC)





- Zugriffskontrolle kann eine Schicht sein
- Zentrale Frage: Wer darf auf welche Daten lesen, schreiben, ausführen?
- Drei grundlegene Modelle:
  - Mandatory Access Control (MAC)
  - Discretionary Access Control (DAC)





- Zugriffskontrolle kann eine Schicht sein
- Zentrale Frage: Wer darf auf welche Daten lesen, schreiben, ausführen?
- Drei grundlegene Modelle:
  - Mandatory Access Control (MAC)
  - Discretionary Access Control (DAC)
  - Role-based Access Control (RBAC)





### Sandboxing

blablabla...





#### **AppArmor**

- Einfache Umsetzung von Mandatory Access Control (MAC)
- Schränkt die Rechte von Applikationen ein
- Im Vergleich zu SELinux einfache Konfiguration





#### Docker

blabla...





### Vergleich AppArmor & Docker

blabla...



### **Fazit**

blabla...



# Maßnahmen gegen SQL-Injections



- Präventive Verteidigungsmaßnahmen



# Maßnahmen gegen SQL-Injections



- Präventive Verteidigungsmaßnahmen
- Maßnahmen gegen SQL-Injections



### Fazit und Resümee



- Präventive Verteidigungsmaßnahmen



### Fazit und Resümee



- Präventive Verteidigungsmaßnahmen
- Maßnahmen gegen SQL-Injections

