LU02h - LB2 - Fokusthema: DoS / DDoS - TBD

1. Einleitung

...

2. Angriffsvarianten

...

2.1 Full: Simple and Plain

...

3. Gegenmassnahmen gegen Brute Force

...

3.1 Einfache Massnahmen

. . .

Note 4.0 - 4.5

Software/Programmierung

- Es ist eine vulnerabler (node.js oder python) Server vorhanden, dass überwunden werden muss
- Es können Angriffe mittels der unter 2.1 und 2.2 beschrieben Art durchgeführt werden
- Es gibt eine secure-Version der Software, bei der erfolge Angriff mittels eine der unter 3.1 genannten Massnahmen verunmöglicht wurde.

Formale Aspekte

- Die Best-Practice-Coding-Standard wurden eingehalten
- Es wird colaborativ gearbeitet inkl. einer Ausfallsicherheit und Versionierung

Abgrenzung

- Es braucht kein Frontend, sprich der Angriff und die Verteidigung können im gleichen Script sein.
- Sprich der Fokus liegt auf dem Server

Note 4.5 - 5.2

Last update: 2025/09/18 15:03

Software/Programmierung

- Es ist eine vulnerabler (node.js oder python) Server vorhanden, dass überwunden werden muss
- Es können Angriffe mittels der unter 2.1, 2.2 und 2.3 beschrieben Art durchgeführt werden
- Es gibt eine secure-Version der Software, bei der erfolge Angriff mittels eine der unter 3.1 und 3.2 genannten Massnahmen verunmöglicht wurde.

Formale Aspekte

- Die Best-Practice-Coding-Standard wurden eingehalten
- Es wird colaborativ gearbeitet inkl. einer Ausfallsicherheit und Versionierung

Abgrenzung

- Es braucht kein Frontend, sprich der Code kann entweder über Commandline oder als separates Angriffsscriptdurchgeführt werden.
- Bei dieser Version gibt es den Server und ein Script, dass den Agriff durchführt

Note 5.3 - 6.0

Software/Programmierung

- Es ist eine vulnerabler (node.js oder python) Server vorhanden, dass überwunden werden muss
- Es können Angriffe mittels der unter 2.1, 2.2, 2.3 und 2.4beschrieben Art durchgeführt werden
- Es gibt eine *secure-Version* der Software, bei der erfolge Angriff mittels eine der unter 3.1, 3.2 und 3.3 genannten Massnahmen verunmöglicht wurde.

Formale Aspekte

- Die Best-Practice-Coding-Standard wurden eingehalten
- Es wird colaborativ gearbeitet inkl. einer Ausfallsicherheit und Versionierung

Abgrenzung

- Es braucht kein Frontend, sprich der Code kann entweder über Commandline oder als separates Angriffsscriptdurchgeführt werden.
- Bei dieser Version gibt es den Server und ein Script, dass den Agriff durchführt



https://wiki.bzz.ch/ Printed on 2025/11/20 01:50

From:

https://wiki.bzz.ch/ - BZZ - Modulwiki

Permanent link:

https://wiki.bzz.ch/modul/m183/learningunits/lu02/08

Last update: **2025/09/18 15:03**

