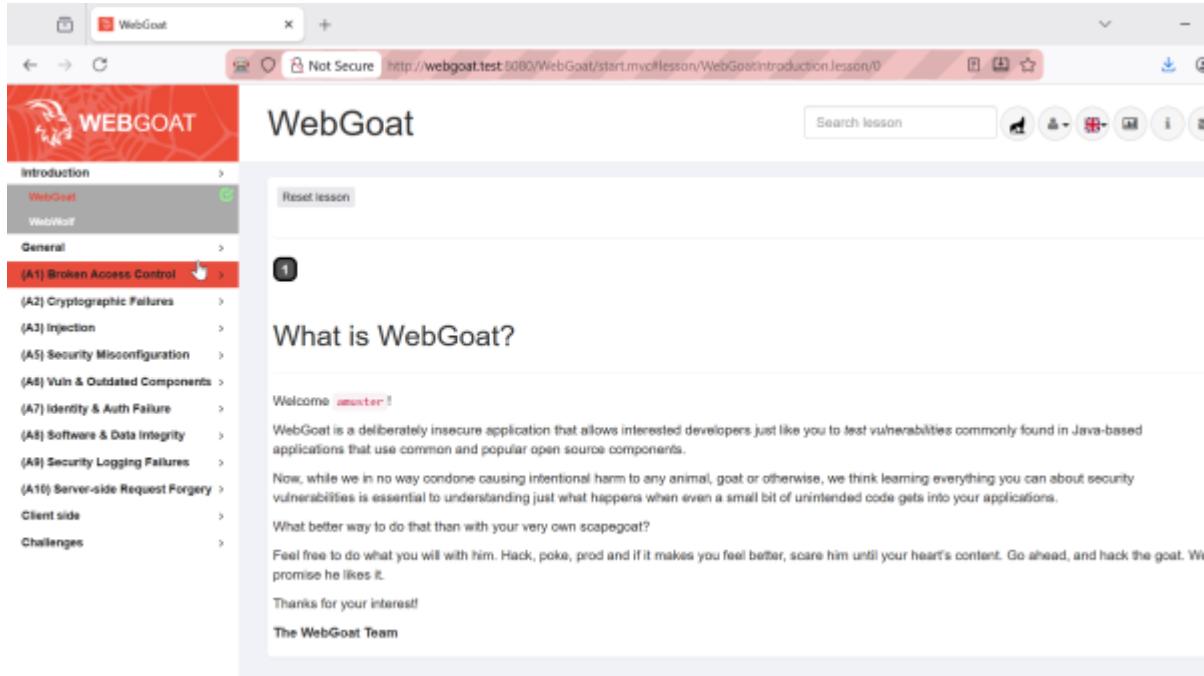


LU04.A03 - WebGoat in Betrieb nehmen

Was ist WebGoat?

WebGoat ist eine bewusst unsichere Webanwendung, die von OWASP betreut wird und dazu dient, Lektionen zur Sicherheit von Webanwendungen zu vermitteln. Dieses Programm demonstriert häufige Schwachstellen serverseitiger Anwendungen. Die Übungen sind dazu gedacht, Anwendern die Grundlagen der Anwendungssicherheit und Penetrationstests näherzubringen.

A screenshot of a web browser displaying the WebGoat application. The title bar says 'WebGoat'. The address bar shows 'Not Secure http://webgoat.test:8080/WebGoat/start.mvc?lesson/WebGoatIntroductionLesson/0'. The main content area is titled 'WebGoat' with a sub-section 'What is WebGoat?'. It includes a welcome message, information about the application being insecure, and a note that it's not condoning causing harm to animals. There's also a message from the WebGoat team. On the left, there's a sidebar with a navigation menu including 'Introduction', 'WebGoat' (which is selected and highlighted in red), 'WebWolf', 'General' (with 'A1 Broken Access Control' selected and highlighted in red), 'A2 Cryptographic Failures', 'A3 Injection', 'A5 Security Misconfiguration', 'A6 Vuln & Outdated Components', 'A7 Identity & Auth Failure', 'A8 Software & Data Integrity', 'A9 Security Logging Failures', 'A10 Server-side Request Forgery', 'Client side', and 'Challenges'. A 'Reset lesson' button is also visible.

WARNUNG 1

Während der Ausführung dieses Programms ist Ihr Computer extrem anfällig für Angriffe. Deshalb wurde die Webapplikation bewusst auf einer virtuellen Maschine (AWS EC2) installiert, wo sich keine privaten Daten befinden. WebGoat ist standardmäßig an localhost gebunden, um das Risiko zu minimieren.

WARNUNG 2

Dieses Programm dient ausschließlich Bildungszwecken. Wenn Sie diese Techniken ohne Genehmigung anwenden, werden Sie mit hoher Wahrscheinlichkeit erwischt. Bei unautorisierten Hacking-Aktivitäten werden Sie von den meisten Unternehmen entlassen oder von den öffentlichen Behörden juristisch verfolgt respektive belangt. Die Behauptung, Sie hätten Sicherheitsforschung

betrieben, ist nicht haltbar, da dies die erste Ausrede aller Hacker ist.

Übungen

Bearbeiten Sie die Übung in Kurs-Repository [01/02_Exercises/01 bis 04](#)

Source: <https://github.com/WebGoat/WebGoat/blob/main/README.md>



Daniel Garavaldi

From:
<https://wiki.bzz.ch/> - **BZZ - Modulwiki**

Permanent link:
<https://wiki.bzz.ch/modul/m183/learningunits/lu04/aufgaben/03?rev=1769517808>

Last update: **2026/01/27 13:43**

