

WebGoat vulnerability assessment report

Submission by: Goutham Vyasroimath Keshava Murthy

Assignment: AEP CS - Application and Web Application Security

Cohort: PGP AEP CS May 2022 Cohort



June 28, 2022

WHITE HATS organization

White Hat Street, White Hat State, White Hat Nation - 007007

Contents

[1. Abstract 2](#_Toc107299238)

[2. In-Scope 2](#_Toc107299239)

[3. Out-Of-Scope 2](#_Toc107299240)

[4. Executive Summary 2](#_Toc107299241)

[5. Definitions - Impact & exploitation probability 2](#_Toc107299242)

[6. Probability of exploitation 3](#_Toc107299243)

[7. WebGoat Vulnerabilities 3](#_Toc107299244)

[7.1. Vulnerability 1 4](#_Toc107299245)

[7.2. Finding 4](#_Toc107299246)

# Abstract

The objective of this report is to find web application vulnerabilities of a WebGoat hosted on a VM Linux machine by using manual SQL Injection techniques. A thorough investigation of SQL Injection vulnerabilities will be conducted. The impacts and probability of the exploitation of each vulnerability found will also be graded based on the standard vulnerability scoring scheme. Additionally, the vulnerabilities will be graded according to the consequences of the exploitation identified through the findings. This report could help any web application developers, providers, and users to better understand the inherent and possible security issues of web applications. This report assumes follow up corrective actions by the WebGoat team in implementing protection against reported SQL Injection security vulnerabilities

# In-Scope

Investigate and report SQL Injection vulnerabilities

# Out-Of-Scope

Recommendation to fix the SQL Injection vulnerabilities

# Executive Summary

WebGoat application only has implemented client-side validations only. This has made pages accessible to parameter tampering through user input of which the attacker can take advantage. Attacker could get more information from system and also end up making updates through SQL Injection which is not the intended behavior of the WebGoat application.

# Definitions - Impact & exploitation probability

|  |  |
| --- | --- |
| **Consequence of exploitation** | **Exploitation** |
| Low | Even if the attack is successful, the attacker would not have control  over what’s being exploited, modification of the contents is not  also, possible. Hence, the attack impact scope may be limited to  only allowing an attacker to access a specific level of only viewing  the system contents. |
| Medium | The attack needs some pre-conditions for the attacker to exploit the  whole system because the system is configured with some security  measures. Therefore, a successful attack may allow little  modifications on the specific system contents which may not affect  the entire system. |
| High | There is a total compromise of the whole system, and therefore,  loss in system protections, which leads to full system files and  configuration disclosure. Moreover, an attacker can modify or  control the entire system. |

# Probability of exploitation

|  |  |
| --- | --- |
| **Consequence of exploitation** | **Exploitation** |
| Low | There is a need for sophisticated tools to bypass systems  restrictions to expose the vulnerability before starting to exploit the  system. So, this vulnerability is very unlikely to occur. |
| Medium | The chance for this kind of vulnerability to occur requires some  preconditions. So, this vulnerability occurs moderately. |
| High | For this vulnerability to be exposed, require only some open  available tools with some little knowledge. So, this weakness is  very common to occur |

# WebGoat Vulnerabilities

# Vulnerability 1

|  |  |
| --- | --- |
| **SQL Injection** | String SQL Injection attack |
| **Impact** | High |
| **Probability** | High |

# Finding

Smith’ or ‘1’=’1

