GoodSecurity Penetration Test Report

[Chadwick Spencer @GoodSecurity.com](mailto:YOURNAMEHERE@GoodSecurity.com)

18 January 2021

# High-Level Summary

GoodSecurity was tasked with performing an internal penetration test on Juice Shop, an online juice product retailer. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, like those of a hacker and attempt to infiltrate Juice Shop and determine if it is at risk. GoodSecurity’s overall objective was to exploit any web application vulnerabilities in order to view the Score Board, access the administrator account, forge a customer comment, and view the basket of another customer while logged in as the GoodSecurity tester , while reporting the findings back to GoodCorp.

When performing the internal penetration test, there were several alarming vulnerabilities that were

identified on Hans’ desktop. When performing the attacks, GoodSecurity was able to find the Score Board, access the administrator’s account, forge a user comment and rating, and view a different user’s basket by exploiting some very simple, but dangerous, vulnerabilities. The details of the attack can be found in the ‘Findings’ category.

# Findings

**Machine IP:**

127.0. 0.1:3000

**Hostname:**

OWASP Juice Shop

**Vulnerability Exploited:**

Weak access control - Insecure direct object references

**Vulnerability Explanation:**

Weak access controls can take advantage of Insecure direct object references (IDORs). IDORs result when user-supplied input allows a user to directly access information, sometimes leading to unauthorized access. By inspecting the main-es2018.js file and searching for “score-board” it is possible to verify its existence and edit the url to gain access to this page.

**Severity:**

In this instance the vulnerability has a CVSS score of 0.0 and is extremely low and is not a concern since the Score Board page is public facing.

**Proof of Concept:**

After learning there is a Score Board page the main java script file, main-es2018.js, was inspected and searched for “score” revealing href=”#/socre-board”

Graphical user interface, website

Description automatically generated

Edit URL to read localhost:3000/#/score-board and reveal scoreboard.

A screenshot of a computer

Description automatically generated with medium confidence

Score Board is now present in the user navigation menu as a public facing page.

Graphical user interface, text

Description automatically generated

**Vulnerability Exploited:**

SQL injection (SQLi) and resulting privilege escalation

**Vulnerability Explanation:**

SQL injection allows the user to inject code circumvent the secure login function. In this case, circumventing the login in with ‘ or 1=1; for a username will allow any value for password and will admit the user as Administrator.

**Severity:**

The severity of the SQL injection vulnerability has a CVSS score of 8.6 and is High. Circumventing the secure login procedure and gaining Administrator access allows full violation of confidentiality, integrity, and availability.

**Proof of Concept:**

Entering a simple true logic statement, ‘ or 1=1; allows bypass of the secure login.

Graphical user interface, website

Description automatically generated

Administrator’s account is attained.

Graphical user interface, website

Description automatically generated

The Account menu displays admin@juice-sh.op.

Graphical user interface

Description automatically generated

**Vulnerability Exploited:**

Weak access controls - Insecure direct object references (IDORs)

**Vulnerability Explanation:**

Weak access controls can be combined with IDOrs to facilitate user enumeration attacks and possibly access to. By using Burp Suite to monitor Customer Feedback action it is possible to intercept the UserID, the comment, and the rating when a comment is posted. It is possible to change this information and to manipulate the Customer Feedback by forwarding the edited post from Burp Suite to the website.

**Severity:**

The severity of Weak access control - IDORs has a CVSS of 7.3 and is High. This vulnerability can result in the loss of confidentiality, the loss of integrity, and has a low impact on availability.

**Proof of Concept:**

A customer comment and rating are created and captured in Burp Suite.

Graphical user interface, text, application

Description automatically generated

The UserID, comment, and rating JSON code are easily identifiable and editable in Burb Suite.

Graphical user interface, text, application, email

Description automatically generated

The UserID is changed from UserID :21 to UserID:5 and the rating is changed from rating:5 to rating:1.

Graphical user interface, text, application, email

Description automatically generated

A comment and rating have now been attributed to another user.

A screenshot of a computer

Description automatically generated

**Vulnerability Exploited:**

Weak access controls - Insecure direct object references (IDORs)

**Vulnerability Explanation:**

Weak access control combined with IDORs can allow a user to see another user’s cart items and could lead to user enumeration on the victim system. Using Burb Suite it is possible to capture the HTTP header and edit the user id in the GET request.

**Severity:**

The severity of insecure direct object references has a CVSS of 7.3 and is High. This vulnerability can result in the loss of confidentiality, the loss of integrity, and has a low impact on availability.

**Proof of Concept:**

The cart of user 6 is viewed and captured by Burp Suite

Graphical user interface, text

Description automatically generated

This is a closer view of the HTTP header showing the “basket” or cart for user 6 in the GET request.

Graphical user interface, text, application, email

Description automatically generated

The user in the GET request is changed to user 10

Graphical user interface, text, application, email

Description automatically generated

Forwarding the edited GET request from Burp Suite shows another the basket for user 10.

Graphical user interface, text, application

Description automatically generated

# Recommendations

GoodSecurity recommends Juice Shop take the following steps to mitigate the discovered vulnerabilities.

Weak Access Controls – IDORs

* + Non-public facing pages should be password protected to prevent unauthorized access.
  + Serialized record numbers, such as userIDs, should be hashed or tokenized to prevent CIA Triad violations and user enumeration attacks.

SQL Injection

* Use parameterized queries or strong username/password validation for any database query to prevent injection and query manipulation.