



Bug Bounty Report

Target Application: OWASP Juice Shop

Date of Testing: 22/08/2025

Tested By: Ambadi Kurup S G

Scope: Authentication vulnerabilities

Table of Contents

1. Executive Summary	2
2. Vulnerability Findings	2
2.1. Authentication Vulnerability (Brute Force – Weak Login Protection)	2
<ul style="list-style-type: none">• Impact• Remediation• Proof of Concept	
2.2. Authentication Vulnerability (SQL Injection – Authentication Bypass)	4
<ul style="list-style-type: none">• Impact• Remediation• Proof of Concept	
2.3. Authentication Vulnerability	
(Insecure Password Reset Mechanism – Account Takeover)	5
<ul style="list-style-type: none">• Impact• Remediation• Proof of Concept	

1. Executive Summary

During the security assessment of the target application OWASP Juice Shop, several authentication vulnerabilities were identified that could potentially compromise the confidentiality, integrity, and availability of the system. The vulnerabilities mainly revolve around weak authentication mechanisms and improper input validation. Authentication Vulnerabilities were exposed by brute forcing weak login protection and SQL injection.

2. Vulnerability Findings

2.1. Authentication Vulnerability (Brute Force – Weak Login Protection)

Impact:

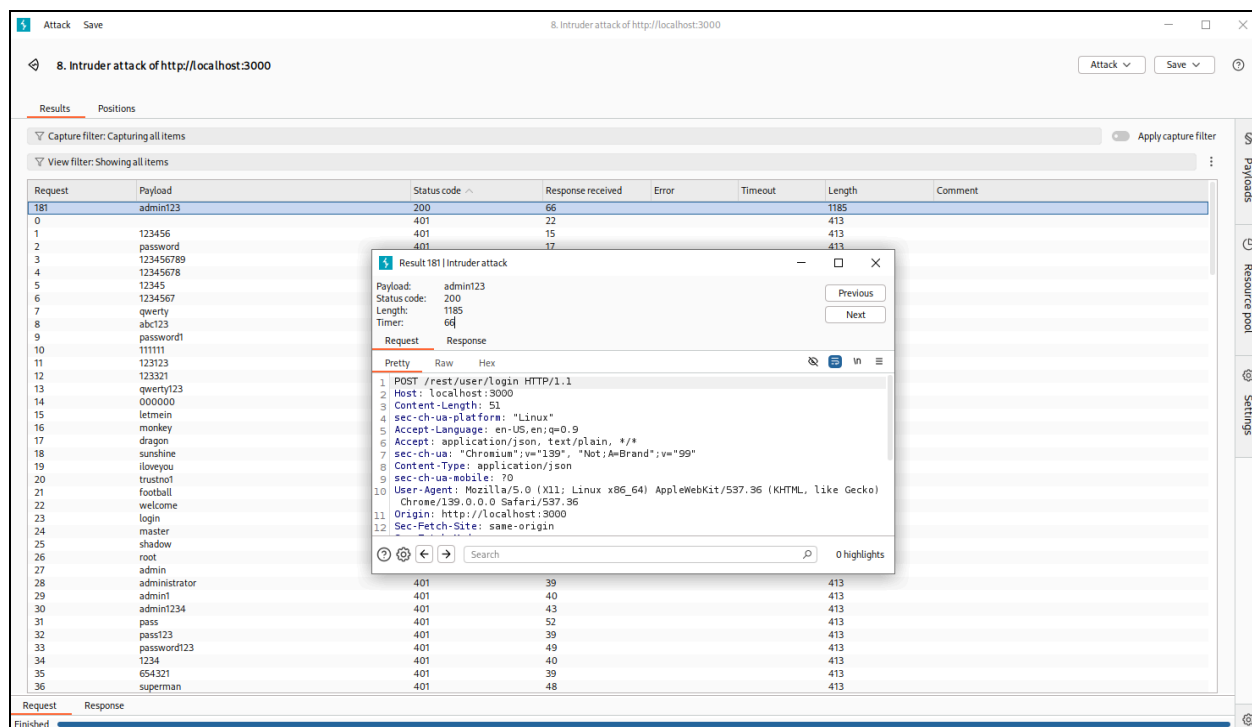
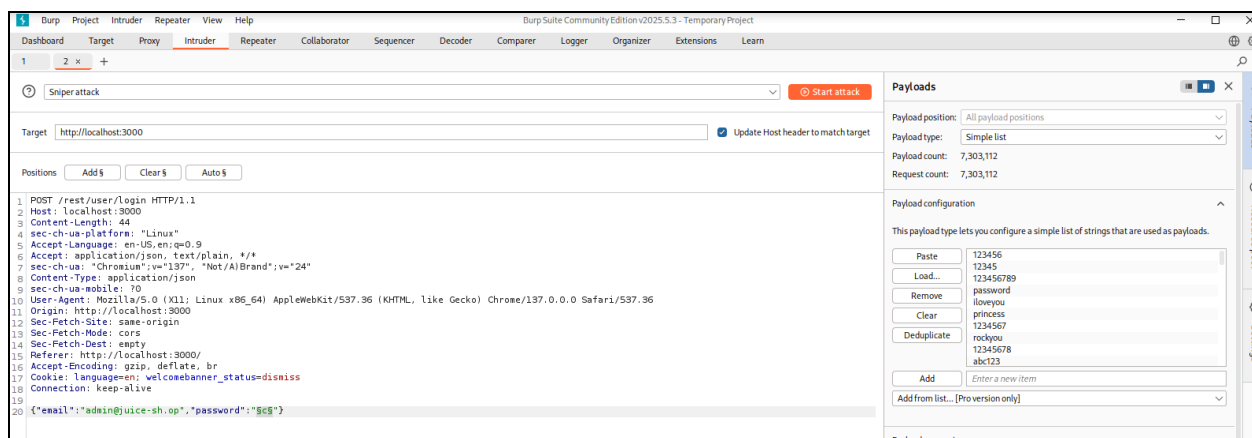
An attacker can perform automated login attempts using a wordlist (e.g., `rockyou.txt`) to guess valid credentials. Without protections such as account lockout, rate-limiting, or CAPTCHA, brute-force attacks can eventually succeed, allowing unauthorized access to user accounts. This could lead to compromise of sensitive data and potential privilege escalation if administrative accounts are targeted.

Remediation:

- Implement account lockout or temporary suspension after a defined number of failed login attempts.
- Introduce CAPTCHA or multi-factor authentication (MFA) to prevent automated login attempts.
- Enforce strong password policies (length, complexity, expiration).
- Monitor login attempts and alert on abnormal activity such as repeated failures from the same IP.

Proof of Concept:

Enumerated the admin email and used it in the login page for capturing the login request via Burp Suite. The request was sent to Intruder and brute forced potential passwords with a wordlist. Successfully obtained the password for admin which was then used to login and access sensitive contents and privileges. Some of them include admin profile page, order history, payment credentials and address information.



2.2. Authentication Vulnerability (SQL Injection – Authentication Bypass)

Impact:

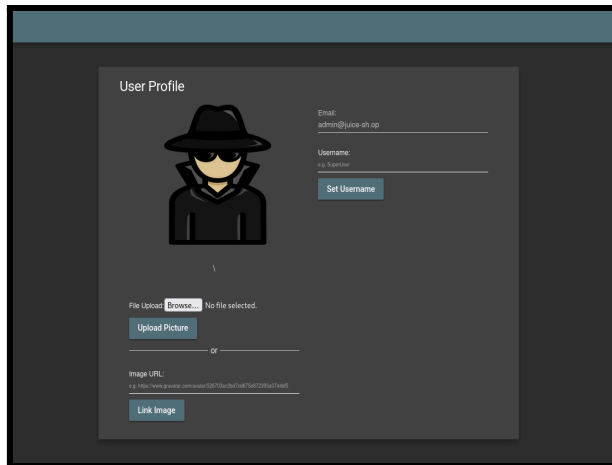
By exploiting SQL injection in the login form, an attacker can bypass authentication entirely without knowing valid credentials. This could result in direct access to administrative accounts, exposure of sensitive data, and full compromise of the application. Successful exploitation could also allow further attacks, such as data extraction, privilege escalation, and complete takeover of the database server.

Remediation:

- Use parameterized queries (prepared statements) to handle user input safely.
- Apply input validation and sanitization to ensure special characters (e.g., `'`, `--`) are not directly executed in SQL statements.
- Implement the principle of least privilege for database accounts (e.g., the application should not connect with admin-level rights).
- Regularly perform security testing, including automated scans and manual code reviews, to identify injection flaws.

Proof of Concept:

SQL injection was utilized in login query to bypass and authenticate the admin account. The single quote (`'`) is used to prematurely terminate the string in the SQL query, allowing the attacker to manipulate the logic of the statement. By injecting the clause `OR 1=1`, which always evaluates to true, the condition in the query is bypassed, resulting in the system treating the input as valid. Consequently, this grants unauthorized access, often defaulting to the first user in the database (commonly the administrator account). The `--` operator is used to comment out the remainder of the query, effectively disabling any additional security checks or constraints.



5

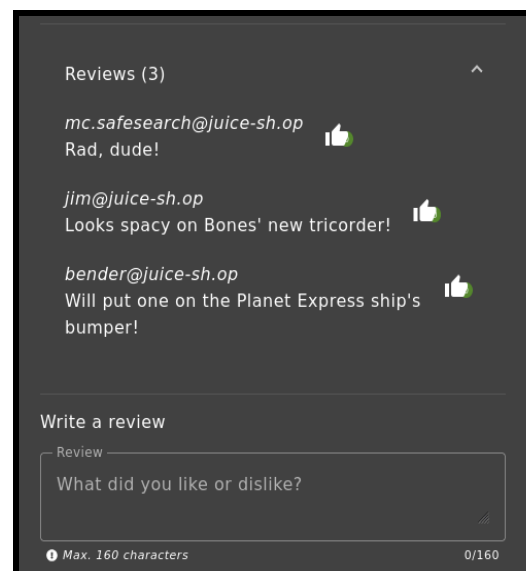
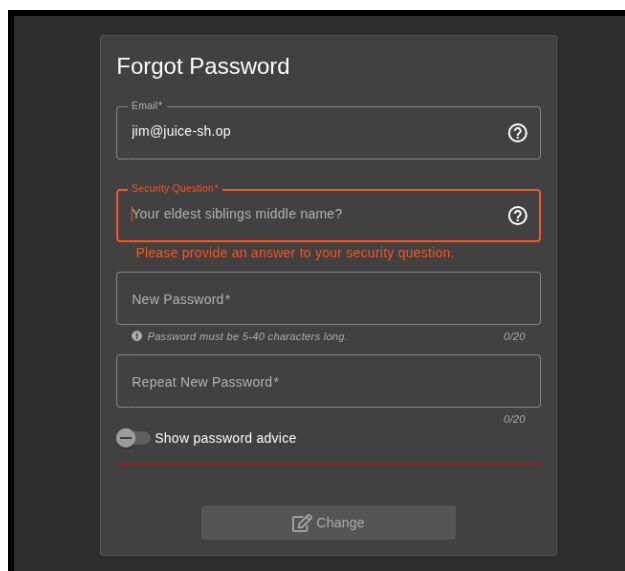
account takeover, granting unauthorized access to sensitive user data and account functionality. If high-privileged accounts (e.g., administrators) are targeted, this could result in complete compromise of the application environment.

Remediation:

- Eliminate knowledge-based questions (e.g., “What’s your favorite color?”) as the sole recovery method.
- Implement **time-limited, single-use reset tokens** sent to a verified email or phone number.
- Enforce **multi-factor authentication (MFA)** for account recovery operations.
- Log and alert unusual password reset attempts (e.g., multiple failed recovery attempts).
- Conduct periodic reviews of password reset mechanisms against OWASP ASVS requirements.

Proof of Concept:

Navigated to the forgot password page and entered the email of the target account obtained from enumeration in review comments. Provided the answer to the predictable security question using Google recon. Application allowed the password reset without further verification. After setting a new password logged in successfully confirming the account takeover.



Google

what is tricoder


AI Mode All Images Videos Short videos Shopping Forums More options - Tools -

Including results for what is **tricorder**
Search only for what is tricoder

AI Overview

Listen

A tricorder is a **fictional, multi-functional handheld device for sensing, analyzing, and recording data**, most famously from the Star Trek franchise, with applications ranging from environmental scanning to medical diagnosis. While not a single device in real-world technology, its functions are being developed in separate, specialized technologies, including advanced portable medical scanners and large-scale program analysis platforms like Google's Tricorder for software development.



Tricorder - Wikipedia
The tricorder is a multifunctional hand-held device that can perform environmental scans,...

Medical tricorder - Wikipedia
A medical tricorder is a handheld portable scanning device to be used by consumers to...

Kali Linux OWASP Juice Shop star trek characters - Google

https://www.google.com/search?q=star+trek+characters+&client=firefox-b-e&scasv=3a4cf79754e4f0d&channel=entpr&ei=dWoaMgnIyTseMPmt3smAg&... Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Google

star trek characters


AI Mode All Images Videos Short videos Shopping Forums More options - Tools -

Fictional Characters / star trek
From sources across the web

Spock Admiral James T. Kirk Jean-Luc Picard

Admiral James T. Kirk

James Tiberius Kirk, often known as Captain Kirk, is a fictional character in the Star Trek media franchise. Originally played by Canadian actor William Shatner, Kirk first appeared in Star Trek serving aboard the starship USS Enterprise as captain. Wikipedia



James T. Kirk (Trek) The original captain, whose appeal hasn't waned in the slightest over the past five decades. Kirk is the perfect mix of geek and space ...

Captain Christopher Pike was always linked with tragedy. As James T. Kirk's predecessor as captain of the U.S.S. Enterprise, Pike was a cerebral, stoic ...

James T. Kirk
https://www.thewrap.com > ...
'Star Trek': All 39 Classic TV Main Chara...
https://www.ign.com > artic...
Top 25 Star Trek Characters

Capt. James T. Kirk Captain James T. Kirk Captain

Wikipedia
https://en.wikipedia.org > wiki > James_T

James T. Kirk

James Tiberius Kirk, often known as Captain Kirk, is a fictional character in the Star Trek media franchise. Originally played by Canadian actor William ...

People also ask

Why is James Kirk called Jim?

Kirk, McCoy and Spock were the shows main billed characters. As such the writers made them a tight group of friends. **McCoy called him Jim since that was his name.** McCoy was not a command level officer or crew member. 16 Feb 2024

