Comprehensive Report on Juice Shop Vulnerabilities

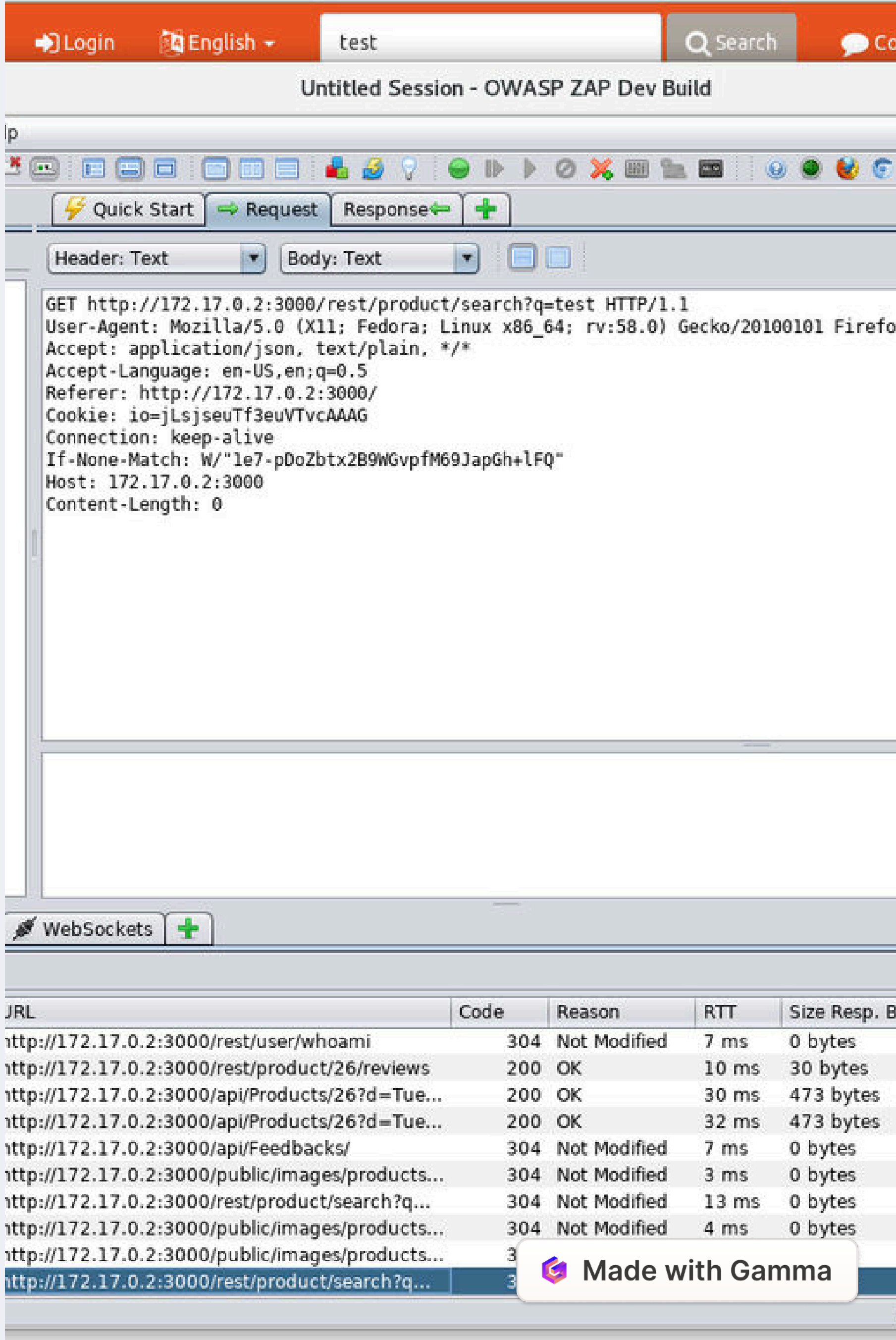
This document provides a detailed exploration and report on the various types of security vulnerabilities found within the Juice Shop web application, with a focus on Cross-Site Scripting (XSS), SQL Injection (SQLi), and Broken Access Control. Through meticulous analysis, we aim to shed light on the inherent risk factors and provide a methodology for uncovering such vulnerabilities.

by Atharva Puri

Overview of Juice Shop

The OWASP Juice Shop is an intentionally insecure web application designed for educational and testing purposes. It contains numerous security vulnerabilities similar to those found in real-world applications, making it an excellent resource for security enthusiasts and professionals to practice identifying and exploiting common web security flaws.

The application is built using modern technology stacks and demonstrates vulnerabilities from the OWASP Top 10 list, providing a contemporary scenario for security training. This hands-on experience aims to inform developers, security specialists, and enthusiasts about the importance of implementing secure coding practices.



```
GET http://172.17.0.2:3000/rest/product/search?q=test HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:58.0) Gecko/20100101 Firefo
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: http://172.17.0.2:3000/
Cookie: io=jLsjseuTf3euVTvcAAAG
Connection: keep-alive
If-None-Match: W/"1e7-pDoZbtx2B9WGvpfM69JapGh+lFQ"
Host: 172.17.0.2:3000
Content-Length: 0
```

JRL	Code	Reason	RTT	Size Resp. B
ttp://172.17.0.2:3000/rest/user/whoami	304	Not Modified	7 ms	0 bytes
ttp://172.17.0.2:3000/rest/product/26/reviews	200	OK	10 ms	30 bytes
ttp://172.17.0.2:3000/api/Products/26?d=Tue...	200	OK	30 ms	473 bytes
ttp://172.17.0.2:3000/api/Products/26?d=Tue...	200	OK	32 ms	473 bytes
ttp://172.17.0.2:3000/api/Feedbacks/	304	Not Modified	7 ms	0 bytes
ttp://172.17.0.2:3000/public/images/products...	304	Not Modified	3 ms	0 bytes
ttp://172.17.0.2:3000/rest/product/search?q...	304	Not Modified	13 ms	0 bytes
ttp://172.17.0.2:3000/public/images/products...	304	Not Modified	4 ms	0 bytes
ttp://172.17.0.2:3000/public/images/products...	3			
ttp://172.17.0.2:3000/rest/product/search?q...	3			

Types of Vulnerabilities

1

Cross-Site Scripting (XSS)

XSS allows attackers to inject malicious scripts into web pages viewed by other users, which can lead to information theft, session hijacking, or defacement of the website.

2

SQL Injection (SQLi)

SQLi flaws permit unauthorized manipulation of an application's database queries, enabling attackers to access, modify, or delete sensitive data and potentially gain administrative privileges.

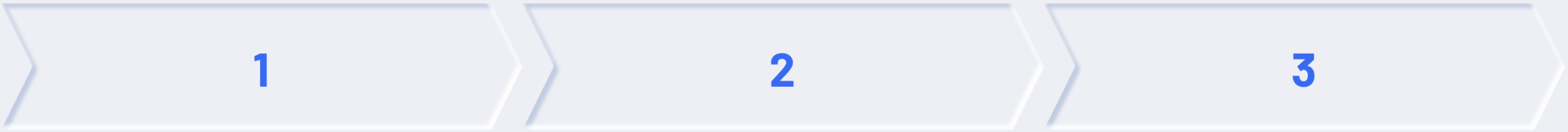
3

Broken Access Control

When access control is inadequately enforced, attackers can exploit these vulnerabilities to access unauthorized functionality or data, leading to privilege escalation and data breaches.

XSS Vulnerabilities in Juice Shop

Within Juice Shop, XSS vulnerabilities often occur due to improper validation and sanitization of user inputs. For instance, insufficient filtering of user comments or reviews can allow malicious JavaScript code to be injected and executed in the context of another user's browser session.



1

User Input

Users insert malicious scripts into input forms that lack proper escape mechanisms.

2

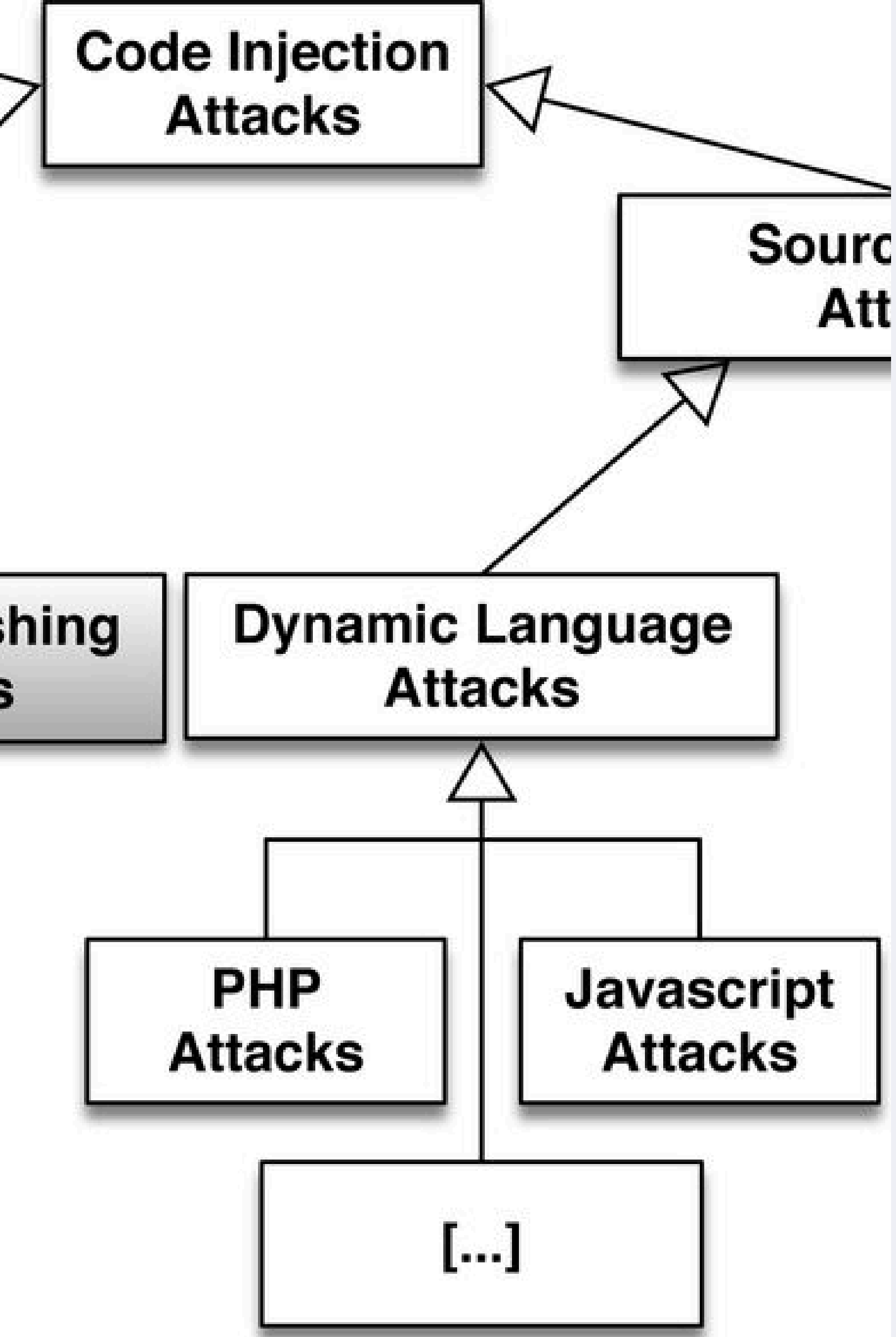
Storage & Retrieval

The unsafe data is stored and then later retrieved without being sanitized.

3

Execution

The script executes when another user views the tainted data, leading to a successful XSS attack.



SQL Injection Vulnerabilities in Juice Shop

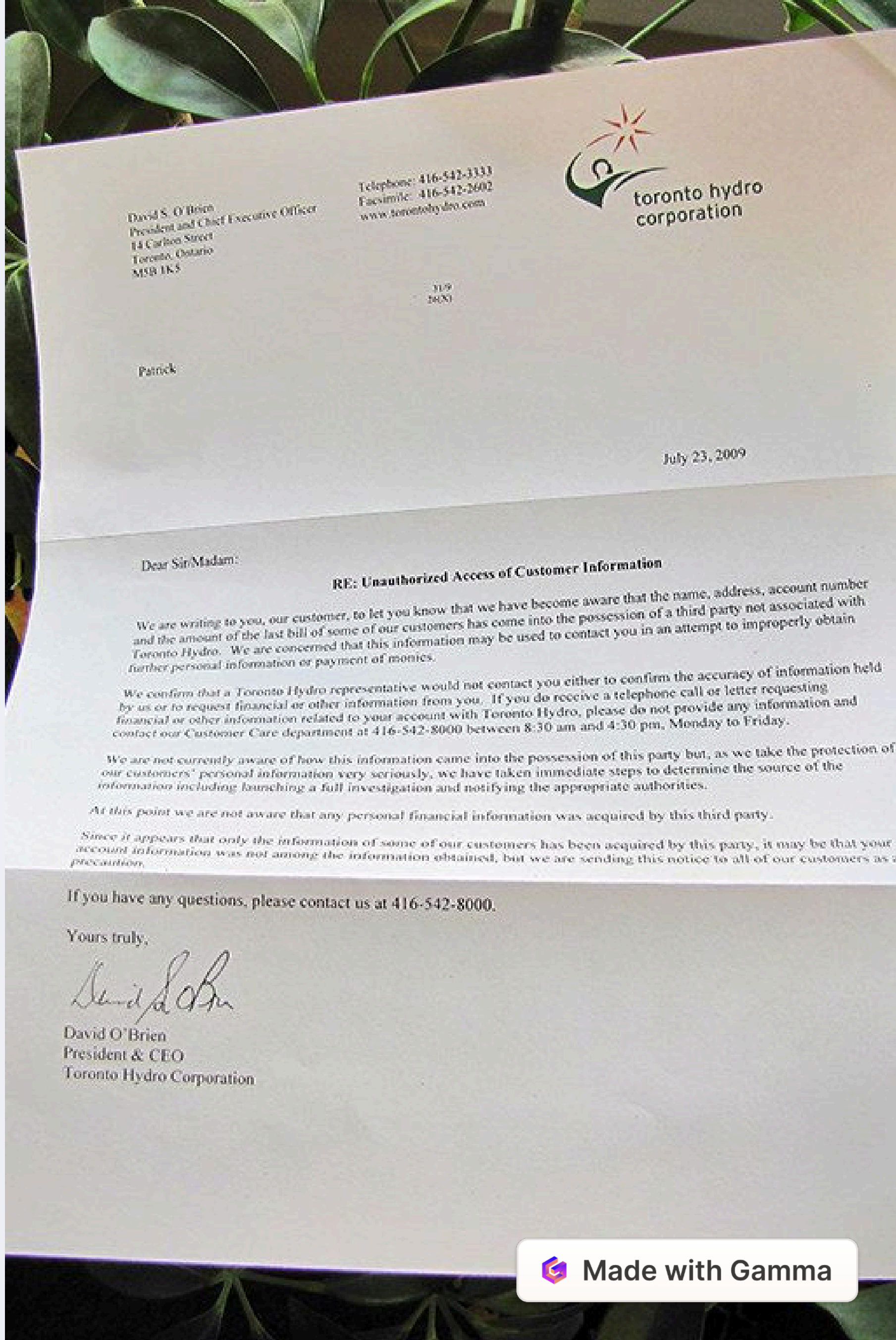
SQL Injection vulnerabilities become evident when user inputs are not correctly processed. Juice Shop features several vulnerable endpoints where SQL queries can be manipulated through the input fields, like login forms or search functionalities.

To detect SQLi vulnerabilities, an attacker may probe inputs with SQL syntax and observe the responses. Effective countermeasures for SQLi include using parameterized queries, stored procedures, and comprehensive input validation.

Broken Access Control Vulnerabilities in Juice Shop

Broken Access Control vulnerabilities manifest when an application fails to verify that the user's permissions correspond to the requested resources or actions. In Juice Shop, these flaws could be found in features like user account management, where unauthorized actions could be performed due to insufficient permission checks.

Vulnerable methods for changing user details, accessing other users' data, or administrative functions highlight the importance of strict access control policies and their enforcement in web applications.



David S. O'Brien
President and Chief Executive Officer
14 Carlton Street
Toronto, Ontario
M5B 1K5

Telephone: 416-542-3333
Facsimile: 416-542-2602
www.torontohydro.com

toronto hydro
corporation

31/9
26(X)

Patrick

July 23, 2009

Dear Sir/Madam:

RE: Unauthorized Access of Customer Information

We are writing to you, our customer, to let you know that we have become aware that the name, address, account number and the amount of the last bill of some of our customers has come into the possession of a third party not associated with Toronto Hydro. We are concerned that this information may be used to contact you in an attempt to improperly obtain further personal information or payment of monies.

We confirm that a Toronto Hydro representative would not contact you either to confirm the accuracy of information held by us or to request financial or other information from you. If you do receive a telephone call or letter requesting financial or other information related to your account with Toronto Hydro, please do not provide any information and contact our Customer Care department at 416-542-8000 between 8:30 am and 4:30 pm, Monday to Friday.

We are not currently aware of how this information came into the possession of this party but, as we take the protection of our customers' personal information very seriously, we have taken immediate steps to determine the source of the information including launching a full investigation and notifying the appropriate authorities.

At this point we are not aware that any personal financial information was acquired by this third party.

Since it appears that only the information of some of our customers has been acquired by this party, it may be that your account information was not among the information obtained, but we are sending this notice to all of our customers as a precaution.

If you have any questions, please contact us at 416-542-8000.

Yours truly,

David O'Brien
President & CEO
Toronto Hydro Corporation

Methodology for Finding Vulnerabilities

1. Initial Mapping - Enumerating the application's content and functionalities to understand its structure.
2. Discovery - Utilizing automated scanning tools and manual testing techniques to probe for common vulnerabilities.
3. Exploitation - Attempting to exploit found vulnerabilities to assess their impact and severity.
4. Reporting - Documenting vulnerabilities with details about their location, potential impact, and recommendations for remediation.
5. Remediation - Implementing fixes, security patches, and improved coding practices to mitigate vulnerabilities.

> Note: Providing developers with clear and actionable insights is crucial for effective vulnerability remediation and strengthening the application's security posture.

Conclusion and Report

Our exploration of the Juice Shop's vulnerabilities highlights serious security considerations that need to be addressed within web applications. Cross-Site Scripting, SQL Injection, and Broken Access Control pose significant risks but can be mitigated through deliberate and informed development practices.

The process of discovering, exploiting, and documenting these vulnerabilities has also reinforced the necessity of ongoing security training and awareness to proactively defend against potential cyber threats.

In conclusion, continuous security testing, combined with appropriate preventive measures, can significantly improve the security integrity of web applications like Juice Shop.