# **OWASP ZAP**

# https://hub.docker.com/r/psiinon/bodgeit

# 

<https://owasp.org/www-project-zap/>

<https://www.zaproxy.org/download/>

<https://www.zaproxy.org/blog/2016-02-19-zap-newsletter-2016-february/>

<https://resources.infosecinstitute.com/topic/the-bodgeit-store-part-1-2/>

## Register with user

Add any username and password

1. Admin

[https://localhost:8080/bodgeit/admin.jsp](https://localhost:8080/bodgeit/search.jsp)

1. Search

<https://localhost:8080/bodgeit/search.jsp>

<u>Whatsits</u>

### **Search**

**You searched for:** Whatsits

**No Results Found**

<script>alert("XSS")</script>

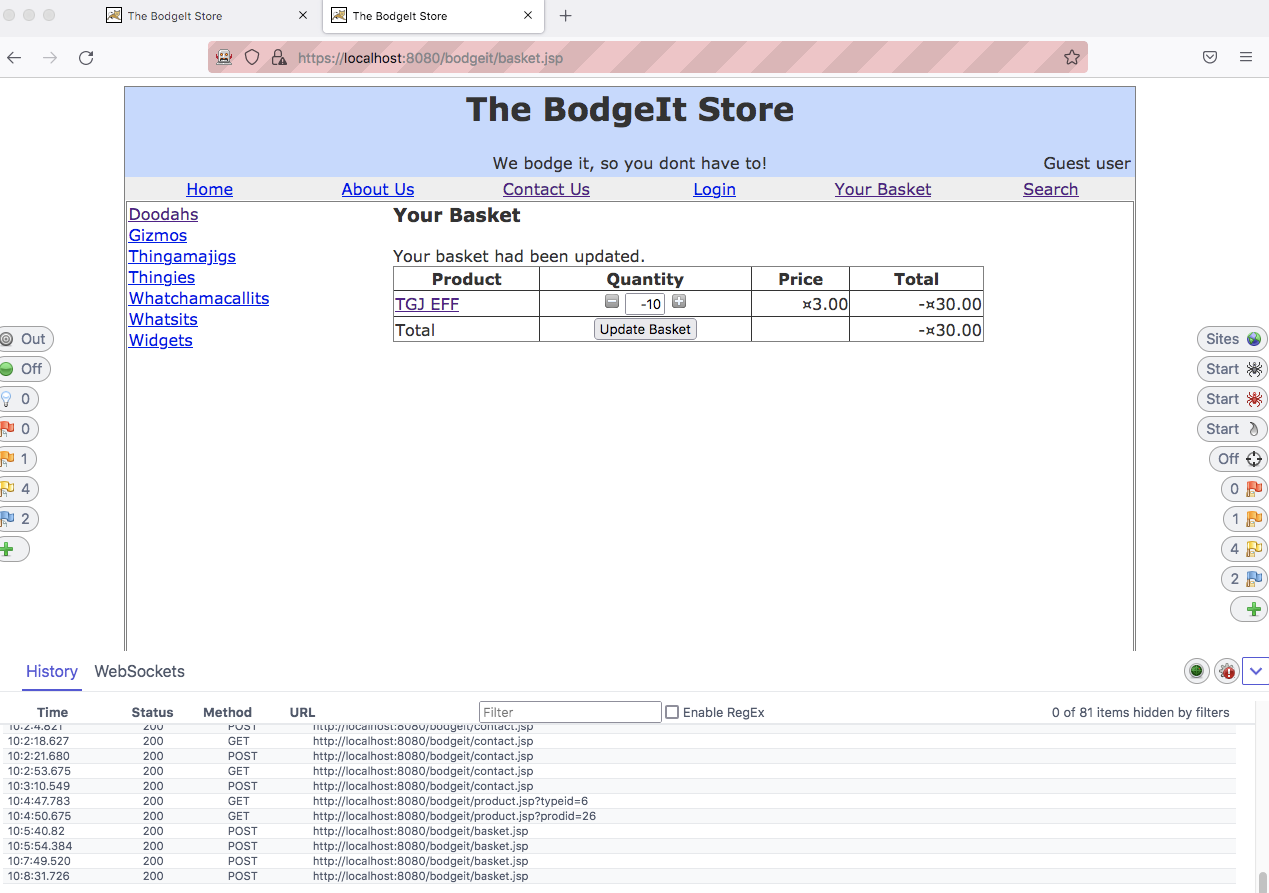
1. Contact

<https://localhost:8080/bodgeit/search.jsp>

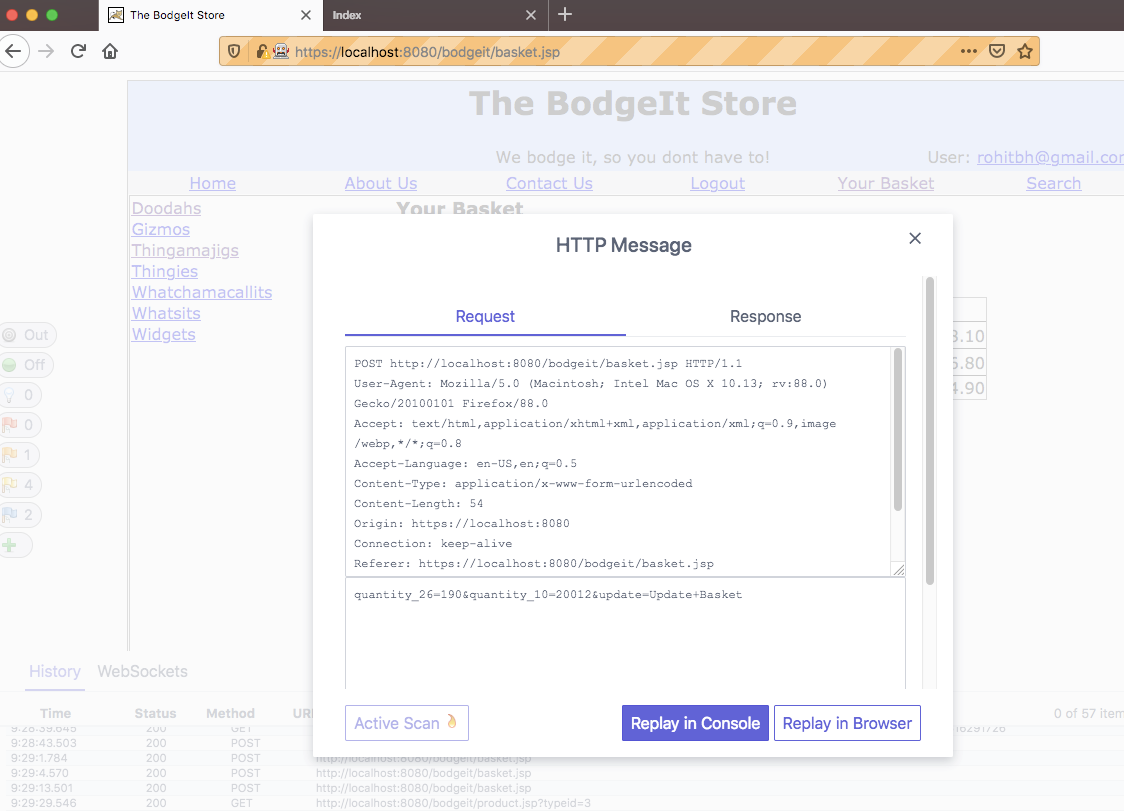
<u>Hello NFJS World</u>

<script>alert("XSS")</script>

1. Update quantity



Update quantity on fly



Change the quantity to 100

## Impersonate as Admin

<https://localhost:8080/bodgeit/admin.jsp>

## 

## Go to Feedback - Contact us

Add in search:

<u>Hello NFJS</u>

<SCRIPT>ALERT(‘XSS’)</SCRIPT>