



# Mitigating Software Vulnerabilities

## Encryption Challenges in Networking

# Mitigating Software Vulnerabilities

Presented by Ahmed Mamdouh Bayoumi

Ahmed Mamdouh Bayoumi

# Agenda

01

## Reflected XSS Attack

Understanding and executing a Cross-Site Scripting attack.

02

## SQL Injection Attack

Demonstrating an SQL Injection attack on a login page.

03

## Mitigation Strategies

Proposing effective steps to prevent XSS and SQLi vulnerabilities.

Ahmed Mamdouh Bayoumi

# 1. Perform a Reflected XSS Attack

## A. Setting up the Vulnerable Application

To demonstrate a Reflected XSS attack, we first need to set up a deliberately insecure web application. We will use OWASP Juice Shop, installed and run via Docker.

Docker installation

```
$ sudo apt install docker.io -y
[sudo] password for ahmed:
The following packages were automatically installed and are no longer required:
liblzo2-2.1 liblzo2-2.1 liblzo2-common1.8 liblzsoup2.4-common liblzfread0
libgdal36 libgdal4-0-3alt libgsfframe0 libtheora0 libvpx9
libgdata-common libgdiplus1.4 libgsigev2 libtheoradec1 python3-packaging-whl
libgdata22 libgpmtdio libgsoup-2.4-1 libtheoraenc1 python3-wheel-whl
Use 'sudo apt autoremove' to remove them.

Installing:
  docker.io

Installing dependencies:
  containerd docker-buildx libcompecli libintl-xs-perl libproc-processtable-perl needrestart runc
  curl docker-clli libintl-perl libmodule-find-perl libsort-naturally-perl python3-pycru tini

Suggested packages:
  containerNetworking-plugins aufs-tools cgroups-mount rinse xfsprogs | zfsutils-linux
  docker-doc btrfs-progs debootstrap rootlesskit zfs-fuse

Summary:
  Upgrading: 0, Installing: 15, Removing: 0, Not Upgrading: 4
  Download size: 81.8 MB
  Space needed: 337 MB / 35.6 GB available

Get:1 http://ftp.halifax.rwth-aachen.de/kali kali-rolling/main amd64 runc amd64 1.1.15+ds1-2+b4 [3,230 kB]
Get:2 http://ftp.halifax.rwth-aachen.de/kali kali-rolling/main amd64 containerd amd64 1.7.24+ds1-8 [33.2 kB]
Get:3 http://ftp.halifax.rwth-aachen.de/kali kali-rolling/main amd64 tini amd64 0.19-0+ds3 [20 kB]
Get:4 http://ftp.halifax.rwth-aachen.de/kali kali-rolling/main amd64 docker amdgpu 4.1.1-2+b9 [23.0 MB]
Get:5 http://ftp.halifax.rwth-aachen.de/kali kali-rolling/main amd64 libcompecli amd64 4.1.1-2 [6.1 kB]
Get:6 http://ftp.halifax.rwth-aachen.de/kali kali-rolling/main amd64 criu amd64 4.1.1-2 [560 kB]
Get:7 http://ftp.halifax.rwth-aachen.de/kali kali-rolling/main amd64 docker-buildx amd64 0.13.1+ds1-3 [13.2 kB]
Get:8 http://ftp.halifax.rwth-aachen.de/kali kali-rolling/main amd64 docker-distro amdgpu 4.1.1-2+b9 [7,334 kB]
Get:9 http://ftp.halifax.rwth-aachen.de/kali kali-rolling/main amd64 libIntl-all all 1.35-1 [690 kB]
Get:10 http://ftp.halifax.rwth-aachen.de/kali kali-rolling/main amd64 libIntl-xs-perl amd64 1.35-1 [15.3 kB]
Get:11 http://ftp.halifax.rwth-aachen.de/kali kali-rolling/main amd64 libmodule-find-perl all 0.17-1 [10.7 kB]
Get:12 http://ftp.halifax.rwth-aachen.de/kali kali-rolling/main amd64 libproc-processtable-perl amd64 0.637-1 [42.1 kB]
Get:13 http://ftp.halifax.rwth-aachen.de/kali kali-rolling/main amd64 libsort-naturally-perl all 1.03-4 [13.1 kB]
Get:14 http://ftp.halifax.rwth-aachen.de/kali kali-rolling/main amd64 needrestart all 3.11-1 [68.6 kB]
Get:15 http://ftp.halifax.rwth-aachen.de/kali kali-rolling/main amd64 python3-pycru all 4.1.1-2 [43.8 kB]
Fetched 81.8 MB in 30min 40s (44.2 kB/s)
Selecting previously unselected package containerd.
Preparing to unpack .../01-containerd_1.7.24+ds1-8_amd64.deb ...
Unpacking containerd (1.7.24+ds1-8) ...
Selecting previously unselected package tini.
Preparing to unpack .../00-runc_1.1.15+ds1-2+b4_amd64.deb ...
Unpacking runc (1.1.15+ds1-2+b4) ...
Selecting previously unselected package libcompecli.
Preparing to unpack .../01-libcompecli_4.1.1-2_amd64.deb ...
Unpacking libcompecli (4.1.1-2) ...
Selecting previously unselected package libIntl-all.
Preparing to unpack .../01-libIntl-all_1.35-1_all.deb ...
Unpacking libIntl-all (1.35-1) ...
Selecting previously unselected package libIntl-xs-perl.
Preparing to unpack .../01-libIntl-xs-perl_1.35-1_amd64.deb ...
Unpacking libIntl-xs-perl (1.35-1) ...
Selecting previously unselected package libmodule-find-perl.
Preparing to unpack .../01-libmodule-find-perl_0.17-1_all.deb ...
Unpacking libmodule-find-perl (0.17-1) ...
Selecting previously unselected package libproc-processtable-perl.
Preparing to unpack .../01-libproc-processtable-perl_0.637-1_amd64.deb ...
Unpacking libproc-processtable-perl (0.637-1) ...
Selecting previously unselected package libsort-naturally-perl.
Preparing to unpack .../01-libsort-naturally-perl_1.03-4_all.deb ...
Unpacking libsort-naturally-perl (1.03-4) ...
Selecting previously unselected package needrestart.
Preparing to unpack .../01-needrestart_3.11-1_all.deb ...
Unpacking needrestart (3.11-1) ...
Selecting previously unselected package python3-pycru.
Preparing to unpack .../01-python3-pycru_4.1.1-2_amd64.deb ...
Unpacking python3-pycru (4.1.1-2) ...

```

```
[~]
$ rm -p 3000:3000 bkimminich/juice-shop
e.js version v22.18.0 (OK)
linux (OK)
x64 (OK)
n default validated (OK)
s 20 of 20 are initialized (OK)
e server.js is present (OK)
e index.html is present (OK)
e styles.css is present (OK)
e main.js is present (OK)
e runtime.js is present (OK)
e vendor.js is present (OK)
e tutorial.js is present (OK)
available (OK)
ning data botDefaultTrainingData.json validated (OK)
://www.alchemy.com/ is reachable (OK)
ning on port 3000
```

```
[~]
$ sudo systemctl start docker
[sudo] password for ahmed:
[ahmed@Ahmed: ~]
$ sudo systemctl enable docker
Synchronizing state of docker.service with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable docker
[ahmed@Ahmed: ~]
$ sudo docker pull bkimminich/juice-shop
Using default tag: latest
latest: Pulling from bkimminich/juice-shop
35d697fe2738: Pull complete
bf6598b2a9b6: Pull complete
4eff9a62d988: Pull complete
62d2e2d4a08b: Pull complete
72897a64fb: Pull complete
7c12895b77fb: Pull complete
3214acf345c6: Pull complete
5664015f10b8: Pull complete
045716a10a88: Pull complete
4a90e3141191: Pull complete
da7816fa9a95e: Pull complete
ddf7a463f7d8: Pull complete
d00c3209d029: Pull complete
c0588aefcf0c: Pull complete
754f9c955c5: Pull complete
5b14fc9a9313: Pull complete
33cebb1d9fc: Pull complete
f45e8372cc60: Pull complete
46b4d4ee13c: Pull complete
2971899a935: Pull complete
c7239157a9: Pull complete
Digest: sha256:c6f965f8929c2c43e76a3c55cd19d482c0084400195db07ed7513a04f346bb5
Status: Downloaded newer image for bkimminich/juice-shop:latest
docker.io/bkimminich/juice-shop:latest
```

Running the application

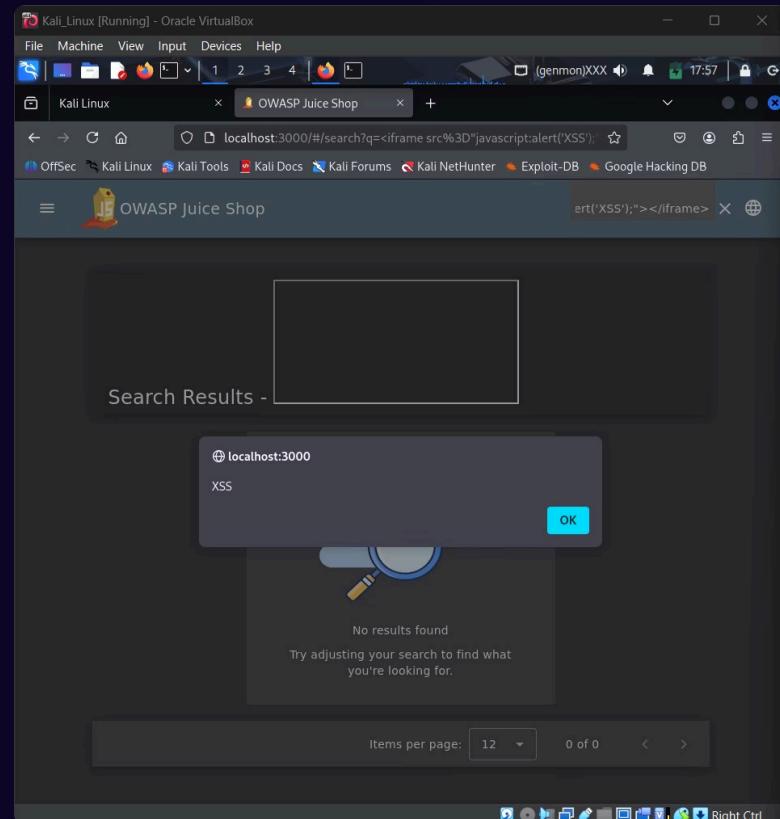
Ahmed Mamdouh Bayoumi

## B. Identifying an Input Field and Executing the Attack

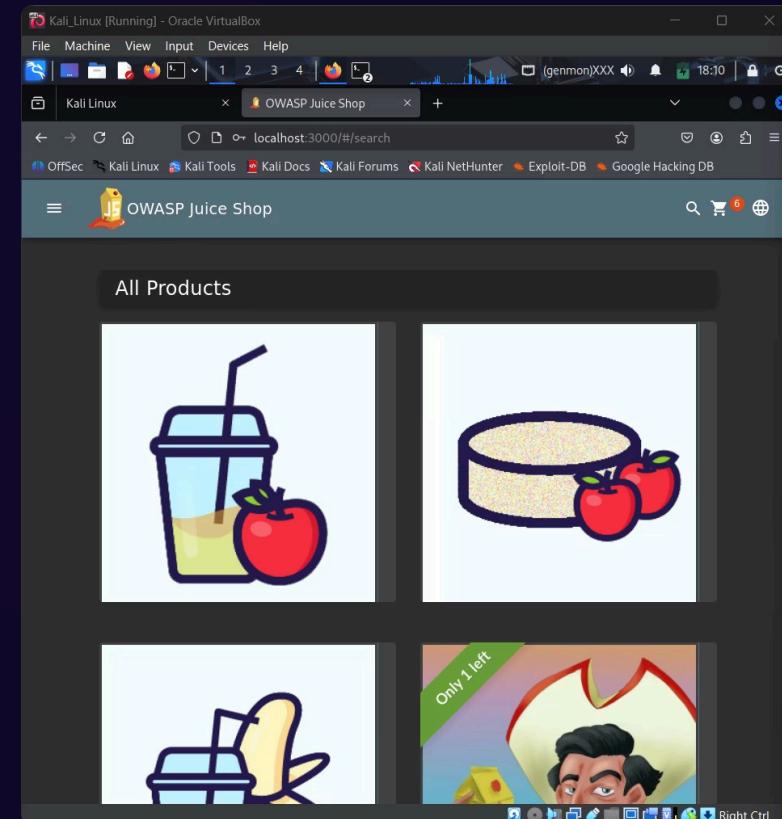
The next step involves identifying an input field that reflects user input back to the page. The search bar is a common and effective target for this type of attack.

## C. Entering the Script Payload and Observing the Results

The attack is performed by entering a malicious JavaScript payload into the search field. This payload, typically a simple alert box script, triggers a pop-up, demonstrating the vulnerability.



Entering the malicious payload



Observing the alert box

## D. How the Attack Works and Its Potential Impact

A Reflected XSS attack occurs when a malicious script from user input is reflected off a web server and executed in the victim's browser. The attacker sends a specially crafted URL containing the malicious code to the victim. When clicked, the vulnerable web application includes the script in the response, and the browser executes it.

### Session Hijacking

Stealing the victim's session cookies to impersonate them.

### Malware Distribution

Redirecting the user to a malicious website that downloads malware.

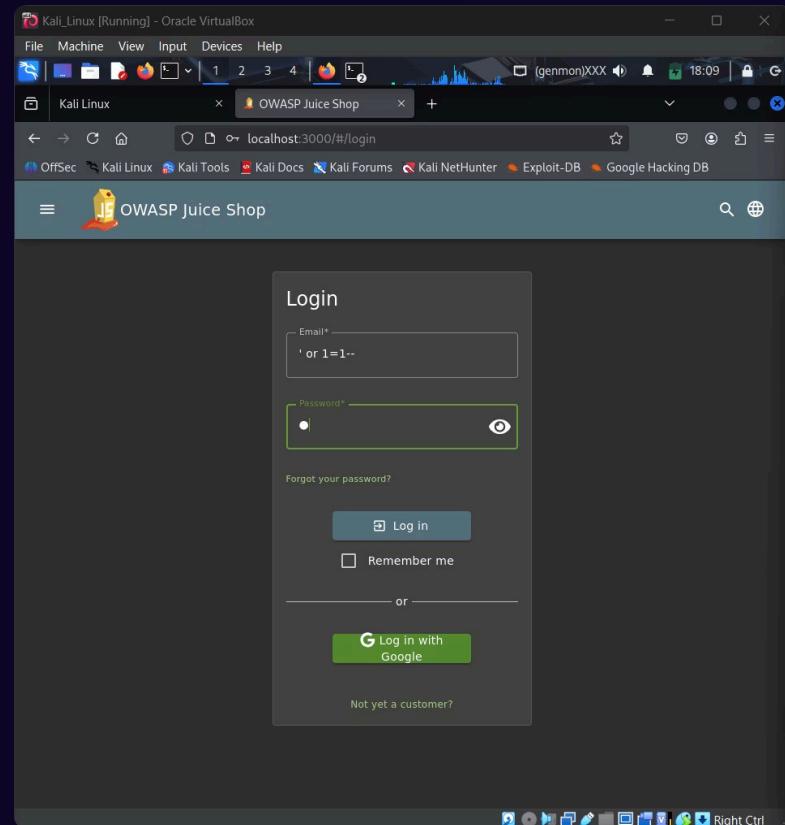
### Data Theft

Stealing sensitive information displayed on the page, like personal data or credit card numbers.

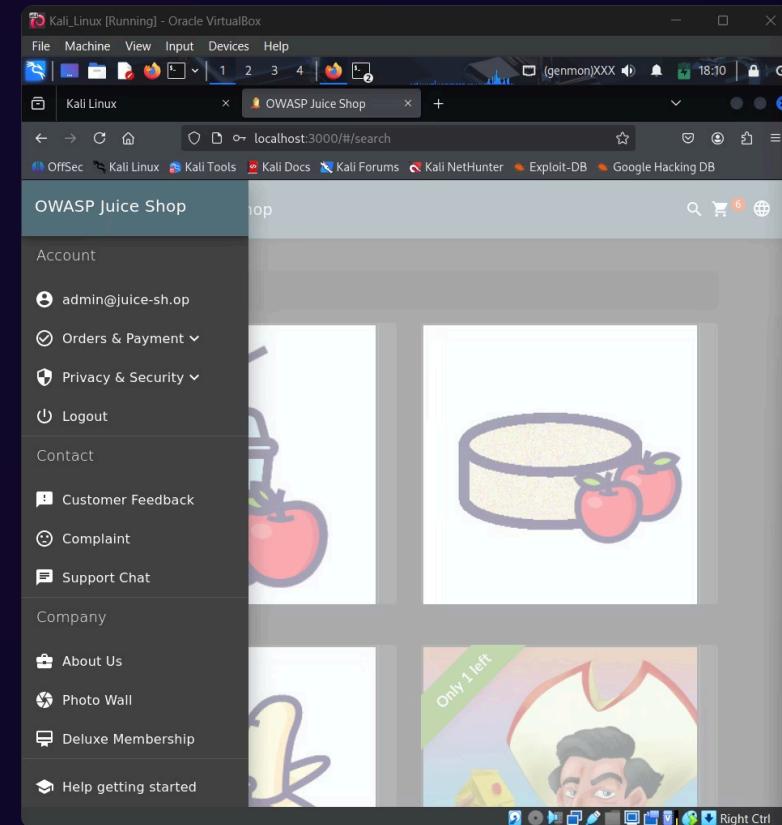
# 2. Conduct an SQL Injection Attack

## A. Using a Testing Environment and Injecting Malicious Commands

An SQLi attack exploits vulnerabilities in an application's database queries. This demonstration uses a manual attack on the login form of OWASP Juice Shop.



SQLi login bypass attempt



Successful login bypass

ing] - Oracle VirtualBox

ew Input Devices Help

ahmed@Ahmed: ~

Edit View Help

http://localhost:3000/rest/products/search?q=apple" --batch --dbs

{1.9.9#stable}

<https://sqlmap.org>

imer: Usage of sqlmap for attacking targets without prior mutual consent is illegal.  
ility to obey all applicable local, state and federal laws. Developers assume no liab  
for any misuse or damage caused by this program

3:06:33 /2025-09-15/

] testing connection to the target URL  
] checking if the target is protected by some kind of WAF/IPS  
] testing if the target URL content is stable  
] target URL content is stable  
] testing if GET parameter 'q' is dynamic  
] GET parameter 'q' appears to be dynamic  
**ING] heuristic (basic) test shows that GET parameter 'q' might not be injectable**  
] testing for SQL injection on GET parameter 'q'  
] testing 'AND boolean-based blind - WHERE or HAVING clause'  
] testing 'Boolean-based blind - Parameter replace (original value)'  
] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause'  
  
] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'  
] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'  
] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'  
] testing 'Generic inline queries'  
] testing 'PostgreSQL > 8.1 stacked queries (comment)'  
] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'  
] testing 'Oracle stacked queries (DBMS\_PIPE.RECEIVE\_MESSAGE - comment)'  
] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'  
] testing 'PostgreSQL > 8.1 AND time-based blind'  
] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'  
] testing 'Oracle AND time-based blind'  
d to perform only basic UNION tests if there is not at least one other (potential) te  
reduce the number of requests? [Y/n] Y  
] testing 'Generic UNION query (NULL) - 1 to 10 columns'  
**ING] GET parameter 'q' does not seem to be injectable**  
**ICAL]** all tested parameters do not appear to be injectable. Try to increase values fo  
f you wish to perform more tests. If you suspect that there is some kind of protectio  
) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or  
  
**ING]** HTTP error codes detected during run:  
rver Error) - 33 times

06:36 /2025-09-15/

## B. Recording the Results and Explaining Consequences

The manual SQLi attack successfully bypassed the login authentication, granting unauthorized access to the admin account. The consequences of SQLi vulnerabilities can be catastrophic.

### Data Breach

Stealing, modifying, or deleting sensitive data, including customer information, financial records, and intellectual property.

### Full System Control

Attackers can gain administrative control over the database and the underlying server.

### Application Downtime

Malicious queries can cause the database to crash, leading to a denial of service.

Ahmed Mamdouh Bayoumi

### 3. Propose Mitigation Steps

#### A. XSS Mitigation

The most effective way to mitigate XSS attacks is through robust input validation and sanitization.

1

##### **Input Validation**

Ensure user input matches the expected format (e.g., only alphabetic characters for a name field).

2

##### **Output Encoding/Sanitization**

Sanitize or escape special characters before displaying user-generated content to prevent browser interpretation as executable code.

## B. SQLi Mitigation

The best way to prevent SQL Injection is by using parameterized queries or prepared statements, along with the principle of least privilege.

1

### Parameterized Queries

Use placeholders instead of embedding user input directly into SQL strings. This separates the command from the data, treating input as a literal value.

2

### Principle of Least Privilege

Ensure database user accounts have only the minimum necessary permissions to perform their functions, avoiding administrative privileges for applications.