UNIVERSITÀ DEGLI STUDI DI MILANO

Web security

Matteo Zoia, Sicurezza e Privatezza

Computer Security laboratory

Faculty of Computer Science

Università degli Studi di Milano

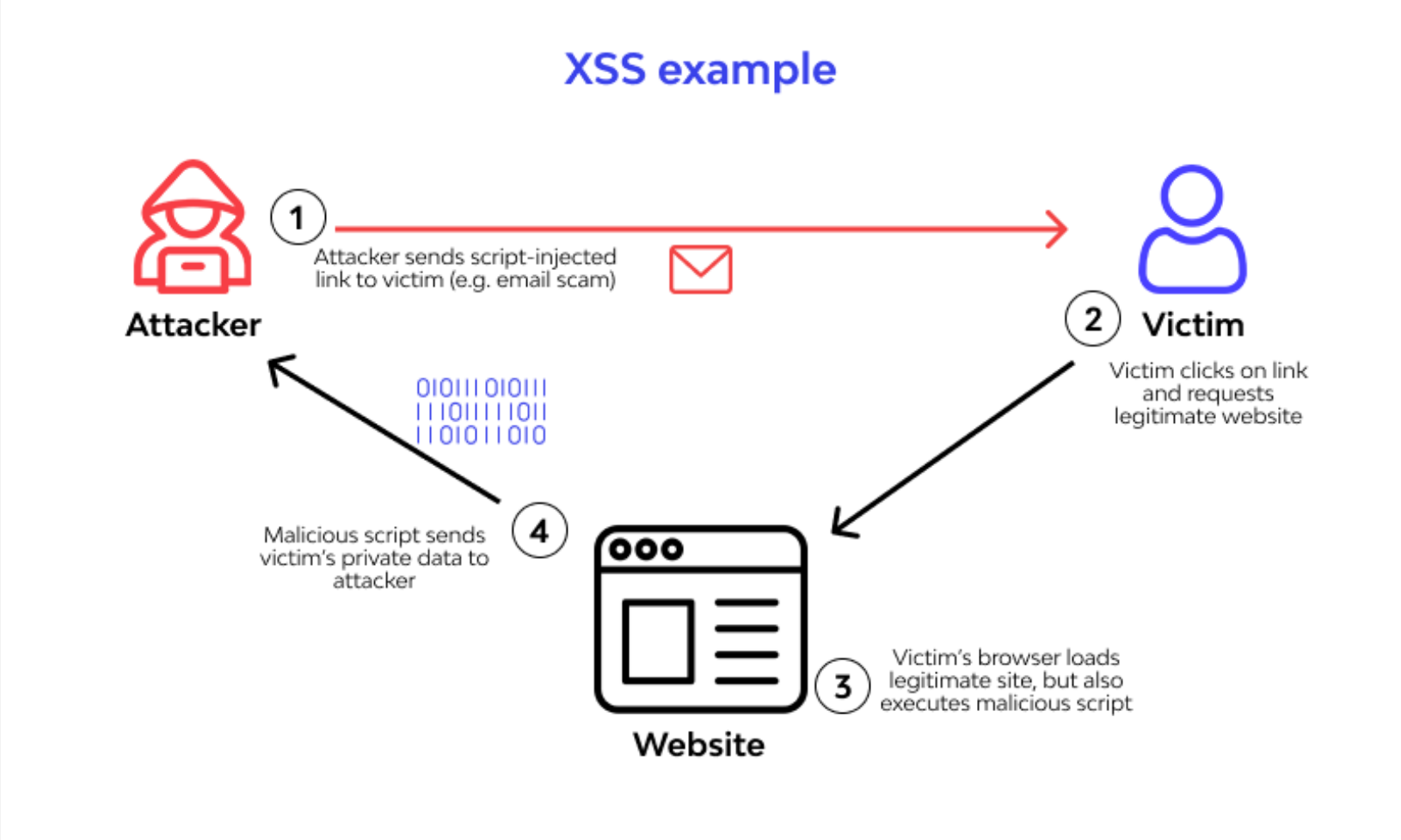
October 17, 2023

XSS

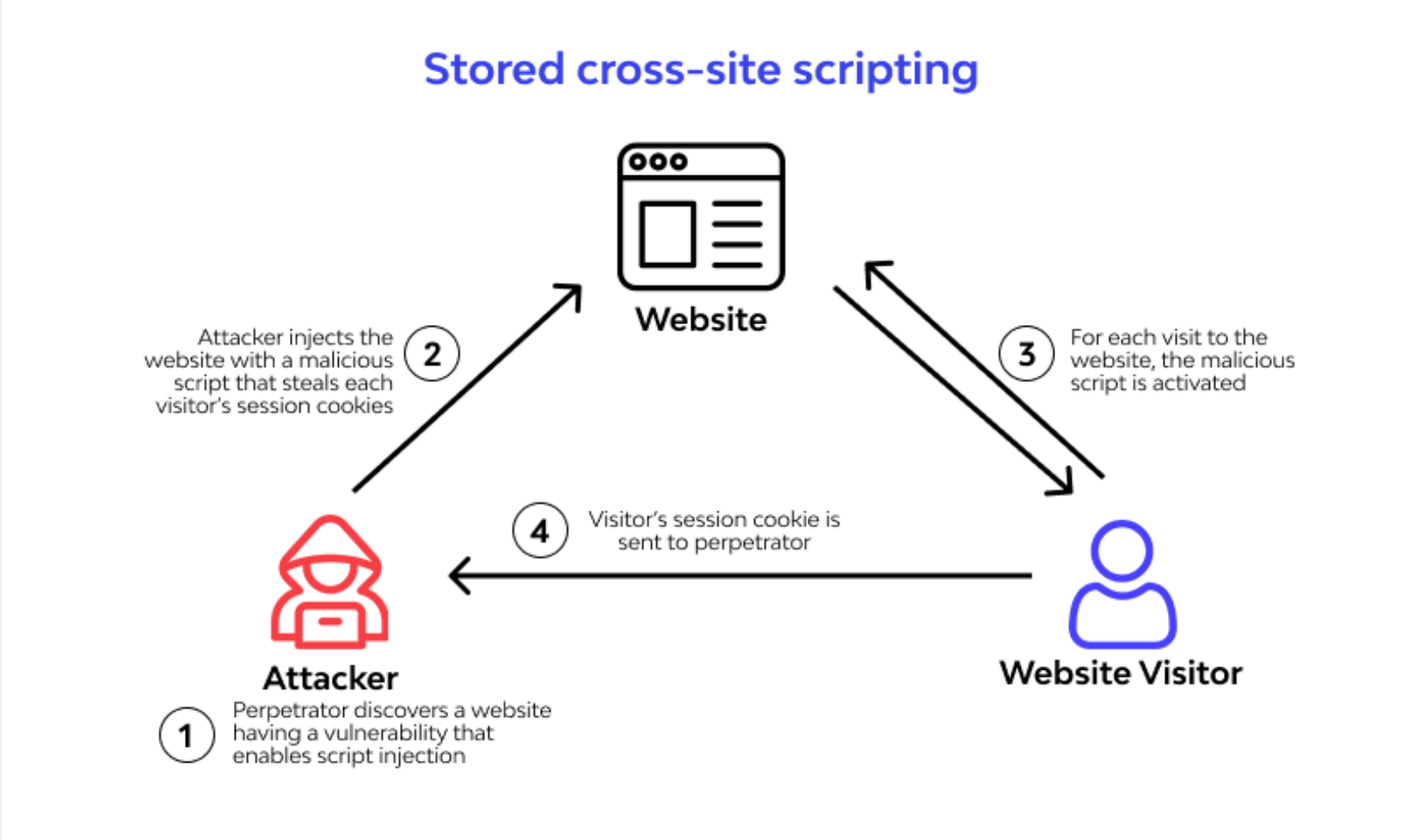
- Cross-site scripting (XSS) is an attack in which an attacker injects malicious executable scripts into the code of a trusted application or website
- Attackers often initiate an XSS attack by sending a malicious link to a user (user must click it)

- Reflected
- Stored
- https://github.com/cure53/DOMPurify

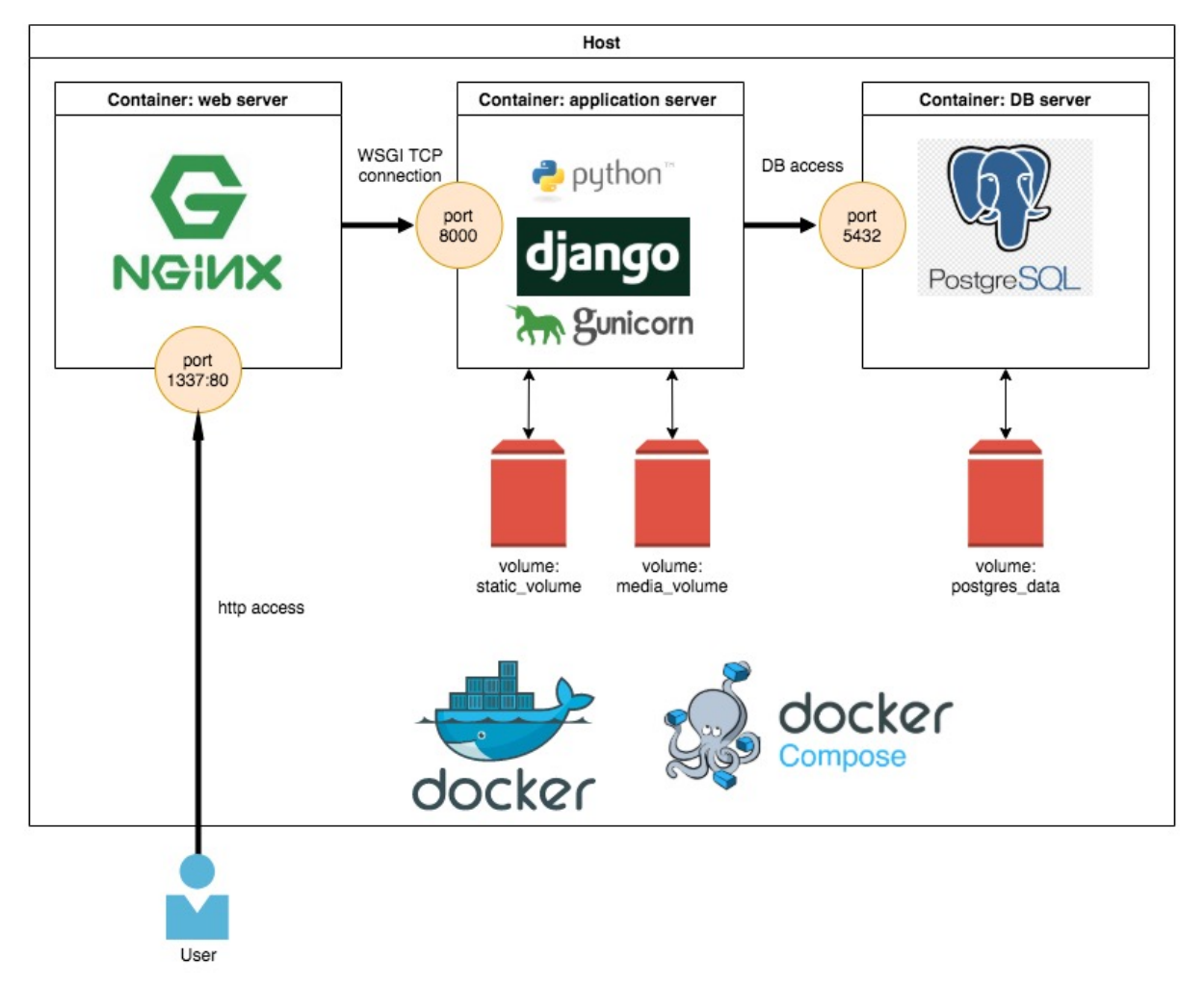
XSS reflected



XSS stored


Stored cross-site scripting
Website
Attacker injects the website with a malicious script that steals each visitor's session cookies
2
3
For each visit to the website, the malicious script is activated
4
Visitor's session cookie is sent to perpetrator
Attacker
Website Visitor
1
Perpetrator discovers a website having a vulnerability that enables script injection

Web application



SQL injection

SQL injection

```sql
SELECT * FROM Products WHERE ProductId = 15; DROP TABLE Suppliers;
SELECT * FROM Orders WHERE OrderId = 16 AND 1=1;
SELECT * FROM Users WHERE Login = 'Administrator' -- ' AND Password = ' '
```

- These queries have in common that they were not anticipated when developing the API.
- It seems that **users have managed to insert additional commands** or alter the SQL queries originally programmed into your site.

SQL injection

- This type of vulnerability is called SQL code injection
- It allows a user to modify an unprotected query to perform operations that they would not normally have access to. These injections are enabled by the need to integrate user-supplied information into dynamic queries: the resulting query is different depending on what is requested by the user.

```
sqlRequest = "SELECT * FROM Products WHERE Name CONTAINS '" + USER_INPUT + "' ";
```

Thank you

Question time