



CYBERSECURITY BOOTCAMP



Table Of Contents

Who Am I

The Server Side

- Introduction
- How It Works?

Server Side Vulnerabilities

- Server-side request forgery - SSRF
- SQL Injection - SQLi
- Server-Side Template Injection - SSTI
- Directory Traversal
- OS Command Injection

Demo

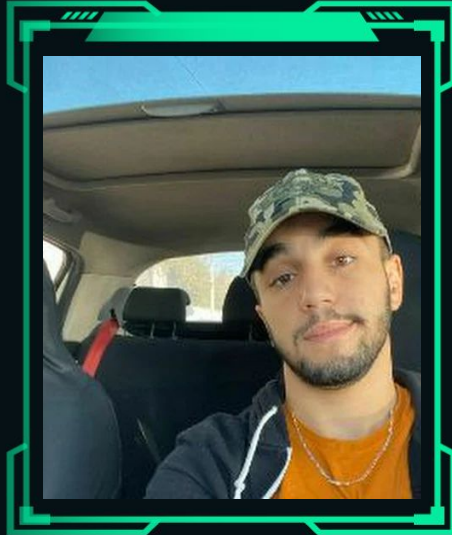
Conclusion



Who Am I



Who Am I



Madani Yousfi Abdelwahed



The Server Side



Introduction





Introduction

“In the client–server model, server-side refers to programs and operations that run on the server. This is in contrast to client-side programs and operations which run on the client side (browser ...)”

Wikipedia

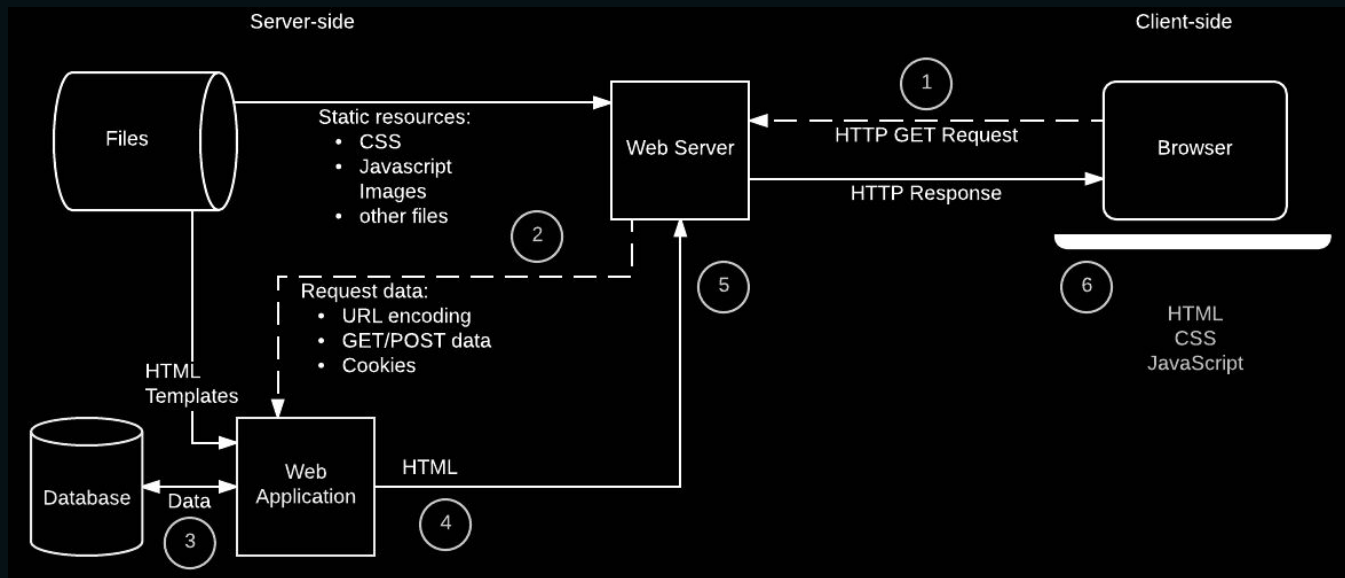


How it **works?**



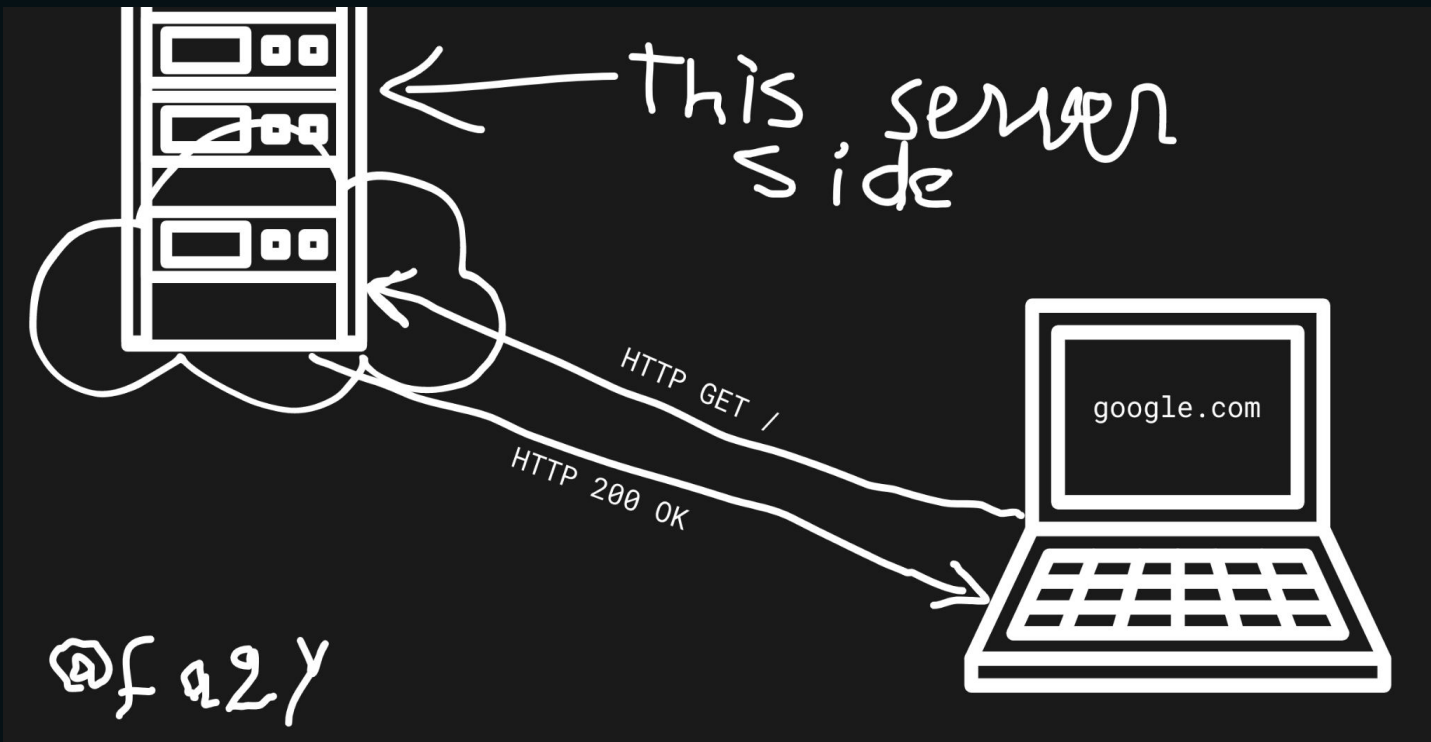


How it works?





How it works?





Server Side Vulnerabilities



Server-side request forgery SSRF





Server-side request forgery - SSRF

Description:

“Server-side request forgery (also known as SSRF) is a web security vulnerability that allows an attacker to induce the server-side application to make requests to an unintended location.”

PortSwigger - SSRF

Impact of SSRF:

- Unauthorized actions or access to data within the organization.
- Attack other back-end systems that the application can communicate with.
- Might allow an attacker to perform arbitrary command execution.
- Connections to external third-party systems.



SQL Injection

SQLi





SQL Injection – SQLi

Description:

“SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to affect the execution of predefined SQL commands.”

OWASP – SQL Injection

Impact of SQLi:

- Read sensitive data from the database.
- Modify database data (Insert/Update/Delete).
- Execute administration operations on the database (such as shutdown the DBMS).
- Recover the content of a given file present on the DBMS file system.
- Some cases issue commands to the operating system..



Server-Side Template Injection SSTI





Server-Side Template Injection - SSTI

Description:

"A server-side template injection occurs when an attacker is able to use native template syntax to inject a malicious payload into a template, which is then executed server-side."

Hacktricks - SSTI

Impact of Server-Side Template Injection - SSTI:

- Expose websites to a variety of attacks depending on the template engine
- Using the attack to perform other attacks on internal infrastructure.
- Use the attack as the basis for numerous other attacks, potentially gaining read access to sensitive data and arbitrary files on the server.



Directory traversal





Directory traversal

Description:

“Directory traversal (also known as File Path Traversal) is a vulnerability that allows an attacker to read arbitrary files on the server that is running an application.”

PortSwigger - Directory traversal

Impact of Directory traversal:

- Accessing application code and data
- Credentials for back-end systems, and sensitive operating system files.
- Might allow writing to arbitrary files on the server, allowing them to modify application data or behavior



OS Command Injection





OS Command Injection

Description:

“An OS command injection is a vulnerability that enables the execution of unauthorized operating system commands. An OS command injection vulnerability arises when a web application sends unsanitized, unfiltered system commands to be executed.”

White Hat - OS Command Injection

Impact of OS Command Injection:

- Almost full control of the system.
- Compromise other parts of the hosting infrastructure.
- Exploiting trust relationships to pivot the attack to other systems within the organization.



Demo



Conclusion

Conclusion

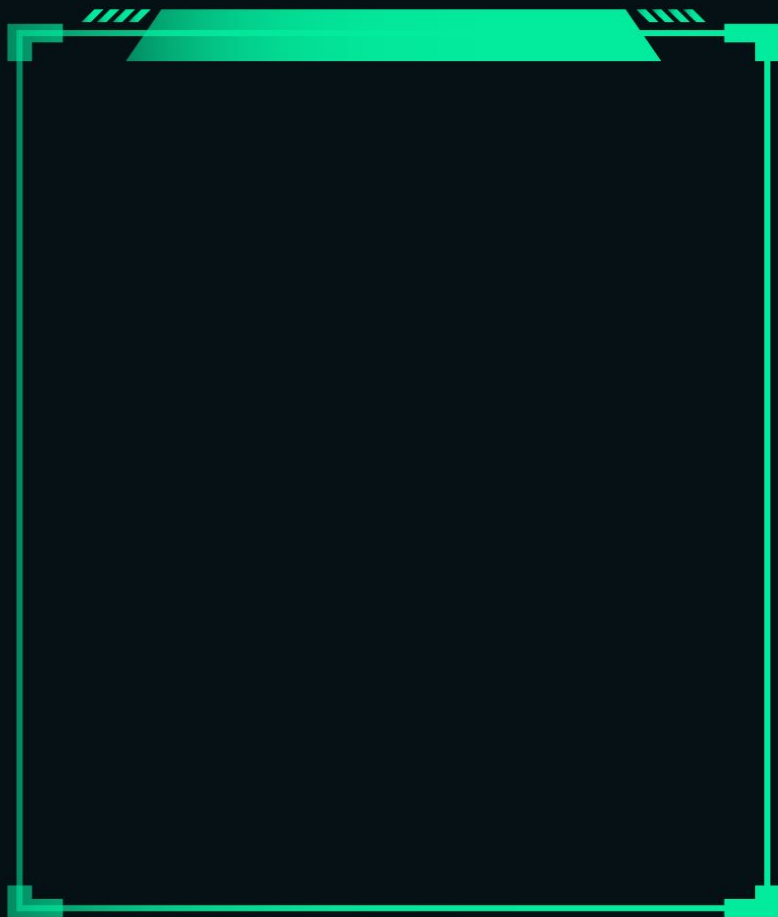
TODO





Thank you for your attention





Introduction:





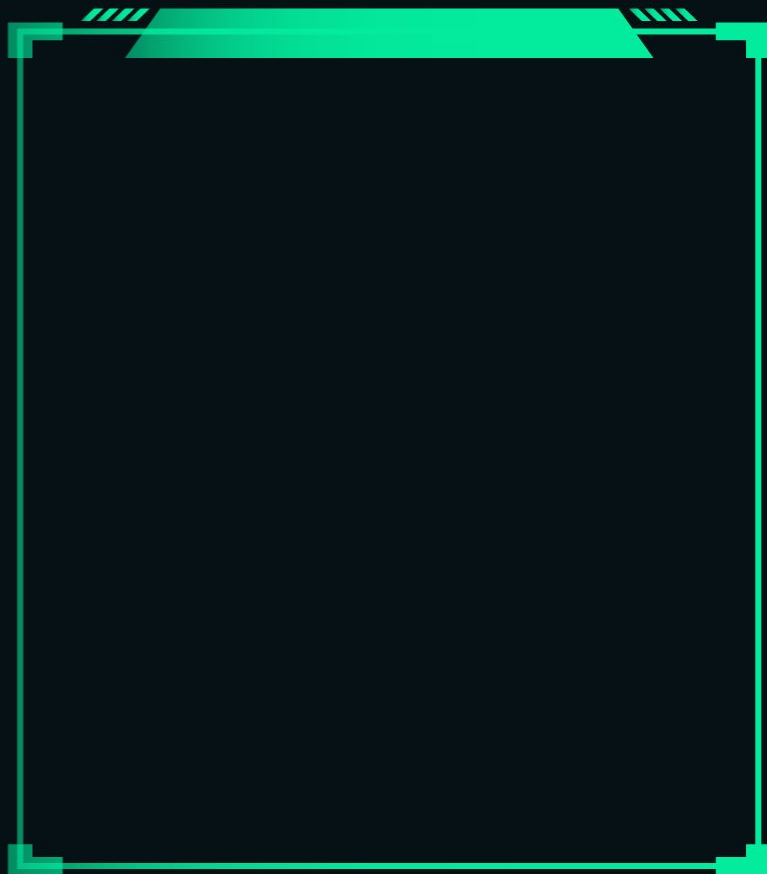
The Server Side :






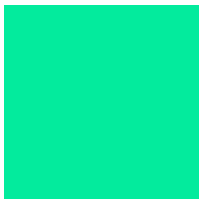






The image features a dark blue background with abstract, light blue geometric shapes in the corners. The top-left corner contains a series of nested, right-angled lines forming a jagged, stepped pattern. The bottom-right corner features a similar jagged, stepped pattern, also in light blue. The central text is white and reads "Color & Typography".

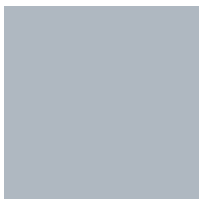
Color & Typography



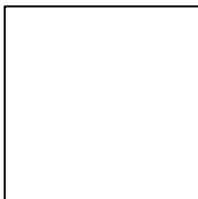
Titles color
#03EB9D



**Text secondary
color for white
background**
#061115



**Text scndary
color**
#afb8c1



Text main color
#ffffff

Google Sans

Regular

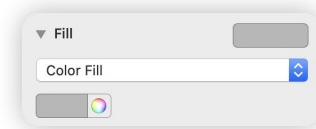
Bold

The image features a dark blue background with abstract geometric shapes in the corners. The top-left corner contains several overlapping, light blue-outlined polygons. The bottom-right corner features a single, continuous, light blue-outlined shape that resembles a stylized step or a corner bracket.

Icons

Icons

All icons are vector objects and can be recolored using the fill menu.



Accessibility



Expand



Late



Credit card



Extension



Thumb Up



Remove



Verified



GSA



Finance



Android



Turn in



Trash



Actions



Download



History



Store



List



Wallet



Announcement



Backup



Document



Favorite 1



Open



Home



Print



Swap



Account



Ratio



Tag



Server



Favorite 2



Grade/rate



Lock



Language



Receipt



Add shopping



Chart



Bug



Event



Find Page



Page view



Basket



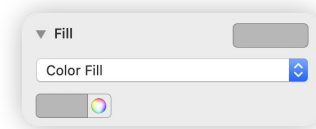
Time



Work

Icons

All icons are vector objects and can be recolored using the fill menu.



Alarm



Assessment



Sync



Exit App



Movie



Visibility



Trolley



Open



Location



Settings



Assignment



Check



Explore



Thumb Down



Today



Perm Media



People



Search



Airplane



Signal



Photo



Play 1



Block



Send



Smartphone



Style



Walk



Bluetooth



WiFi



Upload



Play 2



Email



Laptop



iPhone



Controls



Bike



Pie Chart



Money



Attachment



Video



Business



Chromebook



Security



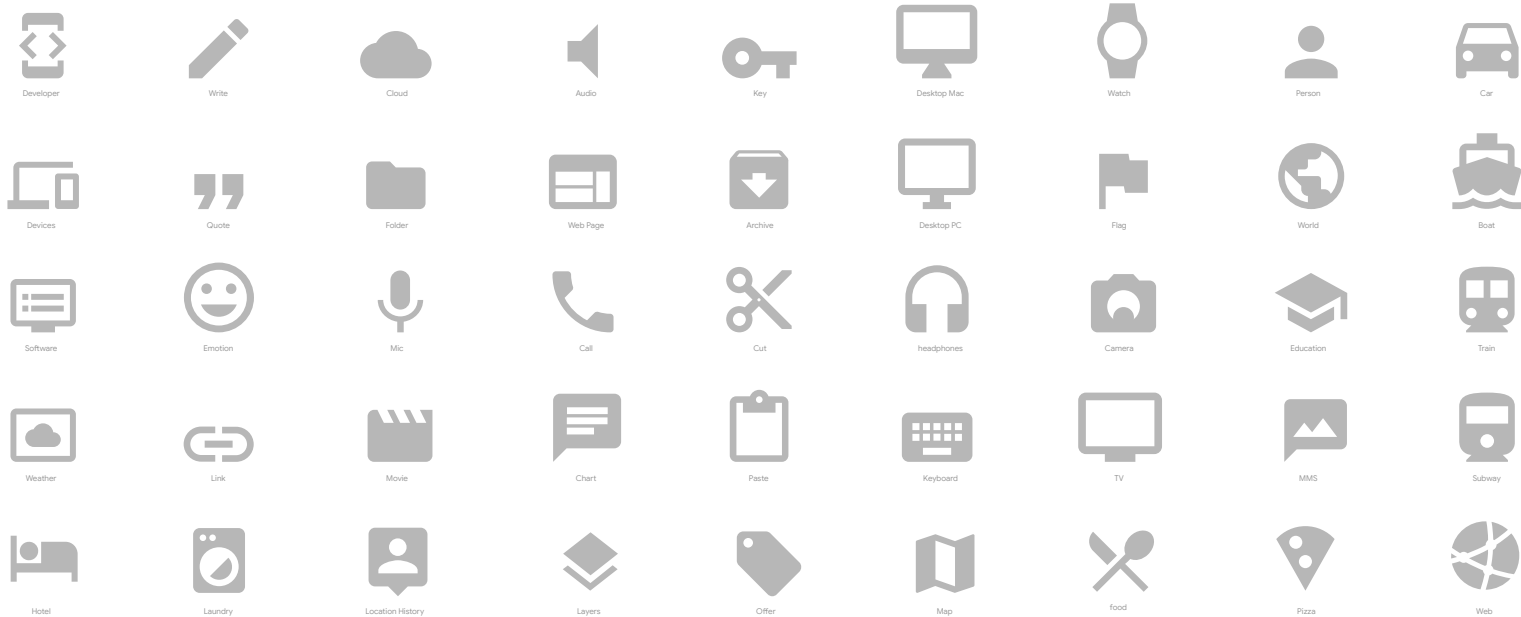
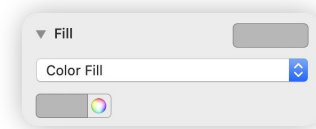
Notification



Bus

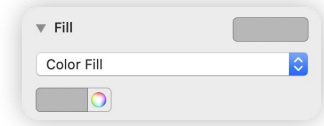
Icons

All icons are vector objects and can be recolored using the fill menu.



Icons

All icons are vector objects and can be recolored using the fill menu.



Cafe



Theatre



Gaming



Florist



Stream



Gas



Delivery



Hospital



Taxi



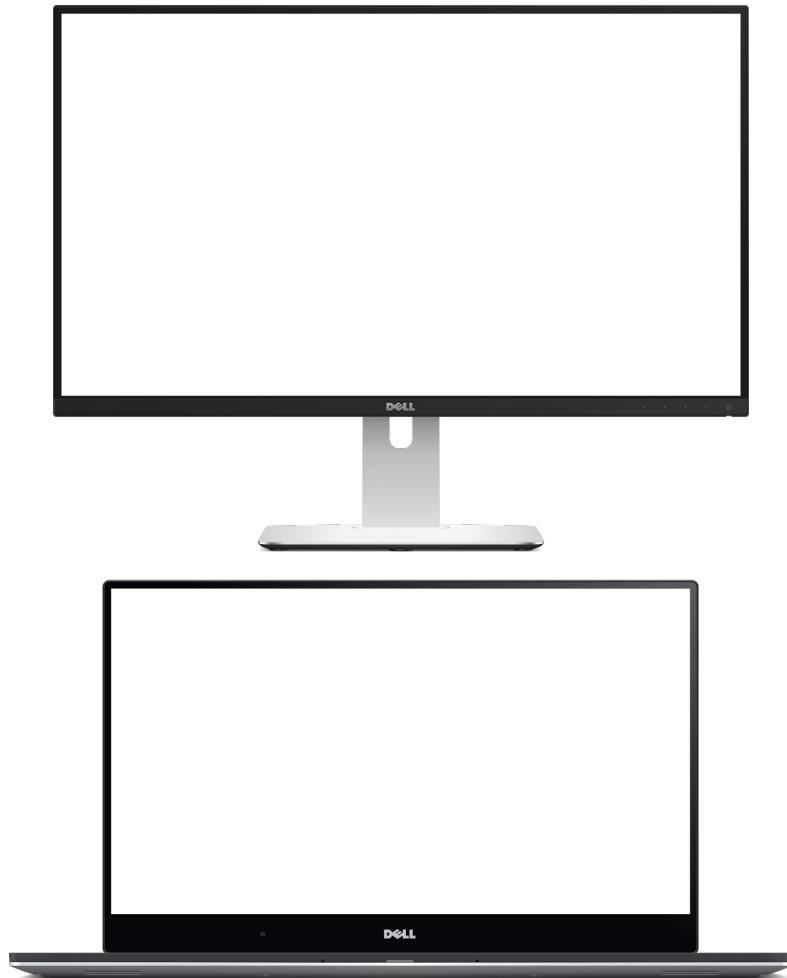
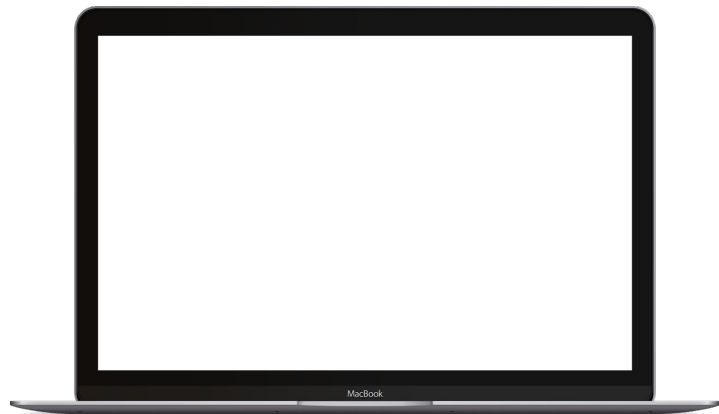
Print



Radio



Device Library



Logo Library

Logos can be scaled to any size

