Server-Side Template Injection (SSTI)

Presented by **Basma Talaat**

TABLE OF CONTENTS

01

Templates and Template Engines

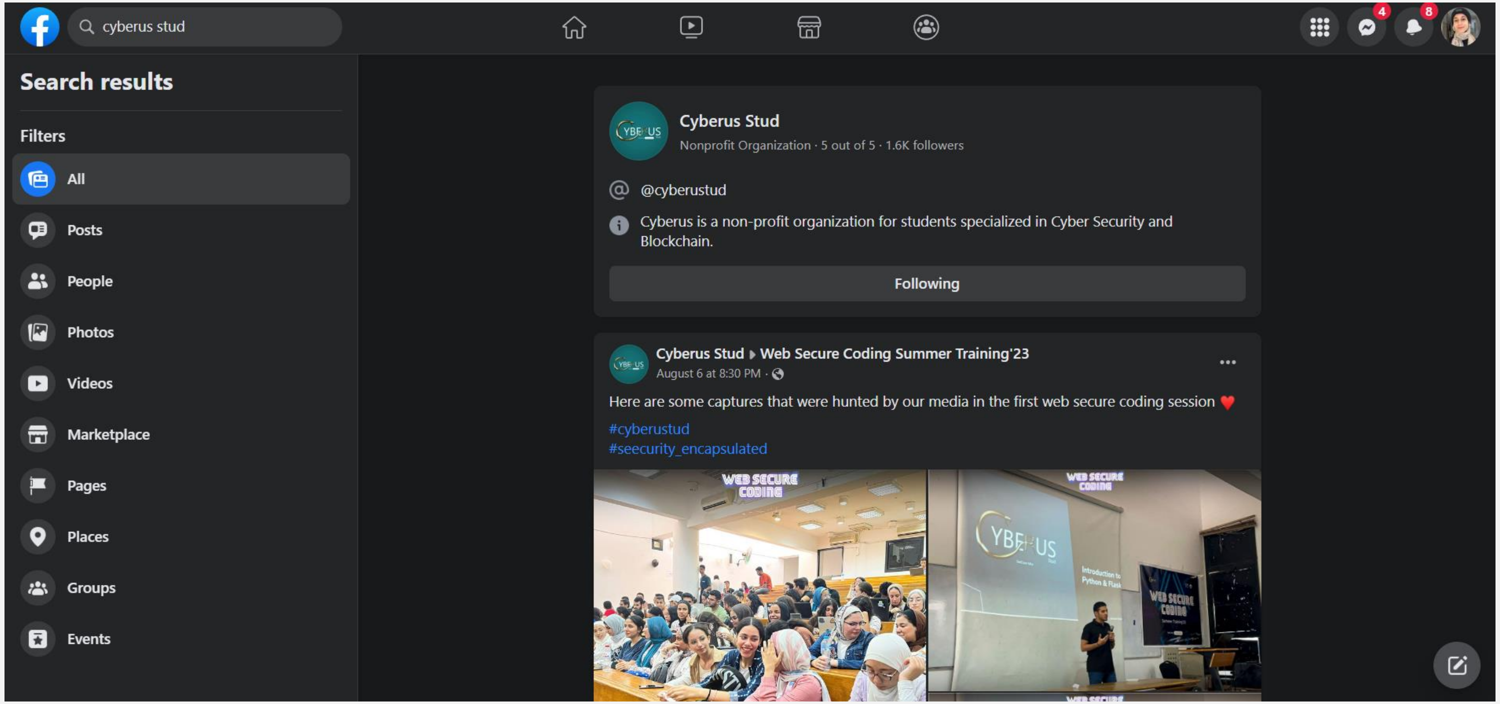
Templates and Template Engines

What is a Template?

- Templates are a pre-designed layouts that allow you to arrange dynamic content onto a web page to quickly create a well-designed website.

Templates and Template Engines

What is a Template?



Cyberus Stud
Nonprofit Organization · 5 out of 5 · 1.6K followers

@cyberustud

Cyberus is a non-profit organization for students specialized in Cyber Security and Blockchain.

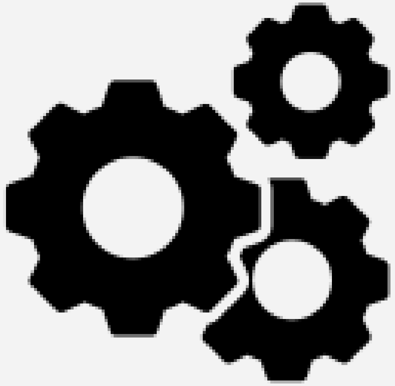
Cyberus Stud ▸ Web Secure Coding Summer Training'23
August 6 at 8:30 PM ·

Here are some captures that were hunted by our media in the first web secure coding session ❤️
#cyberustud
#seecurity_encapsulated

Templates and Template Engines

What is a Template Engine?

- Template engines are tools or libraries that **renders** and generates web pages by combining **fixed templates** with **dynamic data**.



02

What is a SSTI

What is a SSTI

Server-Side Template Injection

- It is a web vulnerability that occurs when the input of the user is rendered into the template as code instead of text.
- Therefore, allowing an attacker to use native template syntax to inject a malicious payload into a template, which is then executed server-side.

03

Risks of SSTI

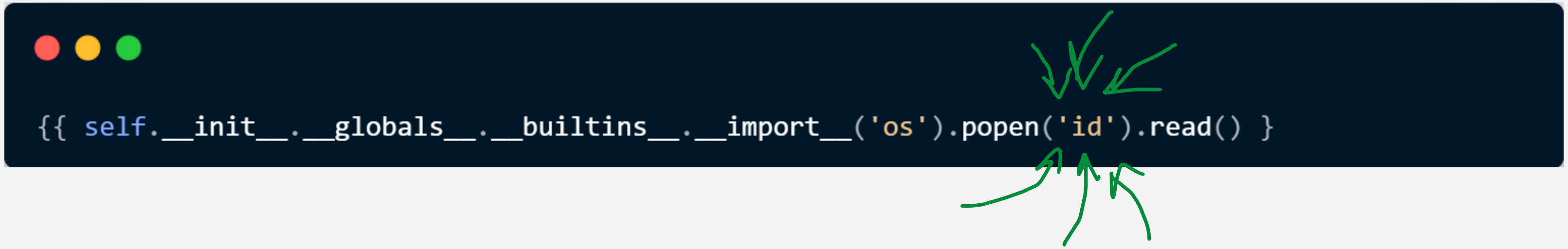
Risks of SSTI

- **Full access to the server:**
  An attacker can read, write and delete files from the sever.
- **Remote Code Execution (RCE):**
  the most severe impact of SSTI is is the ability for attackers to execute arbitrary code on the server.
- **Data Disclosure:**
  Attackers can exploit SSTI vulnerabilities to access and leak sensitive data, such as configuration files, database contents, API keys, and user credentials.
- ***..etc.***

04
Hands-on Exploit

Hands-on Exploit

- First, we’ll check if there’s a SSTI with the infamous **{{7*7}}** payload.
- Second, we’ll exploit it 😈.



```
{{ self.__init__.__globals__.__builtins__.__import__('os').popen('id').read() }
```

We insert whatever command we want to execute here

05

Mitigations

Mitigations

How to prevent SSTI?

- **Input validation and sanitization:**
  Ensure that user-provided data is properly validated and sanitized before using it in templates.

- **Use Safe Template Engines:**
  Choose template engines that have built-in security mechanisms to mitigate SSTI risks.

Ex: Jinja2

RESOURCES

https://portswigger.net/web-security/server-side-template-injection

https://book.hacktricks.xyz/pentesting-web/ssti-server-side-template-injection

https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Server%20Side%20Template%20Injection/README.md

CYBERUS Stud