OWASP Jakarta Chapter – October Meetup (Remote)

# Server Side Template Injection

**Discovery to Exploitation**

# THANKS

# /me: Sanoop Thomas @s4n7h0

- Chapter Moderator at Null Singapore
- 8+ years in Information Security
- Created Halcyon IDE – an IDE for Nmap Script Developers
  - https://halcyon-ide.org/
- Host SecTools Podcast at Infosec Campus
  - https://infoseccampus.com/
- Barely get time to write blogpost, but presentations/talks are updated
  - https://devilslab.in/
- Presented at OWASP India, Nullcon Goa, BlackHat (USA, Asia), HITBGSEC, ROOTCON

# What are templates

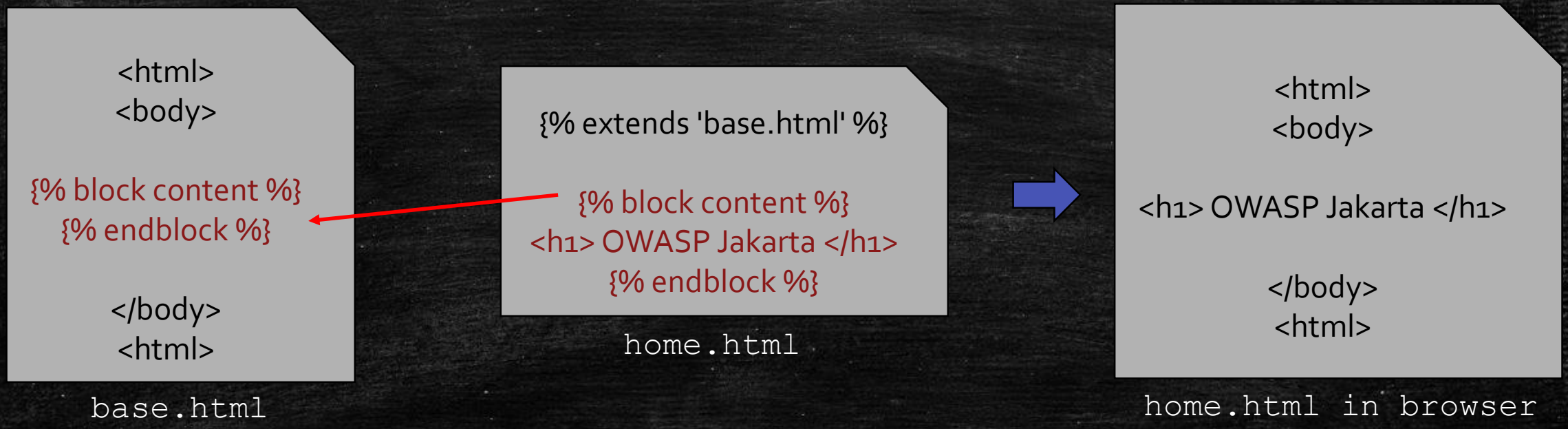
- Templates are simple text files
- It contains variables or expressions, which get replaced with values.
- When templates are executed, the tags are evaluated and render the result.
- Example:

```
<p> <?php echo $username; ?> </p>
```

```
<p> {{ username }}</p>
```

# Why should Apps do this ?

- Easiness in handing web pages and rendering
- Template inheritance



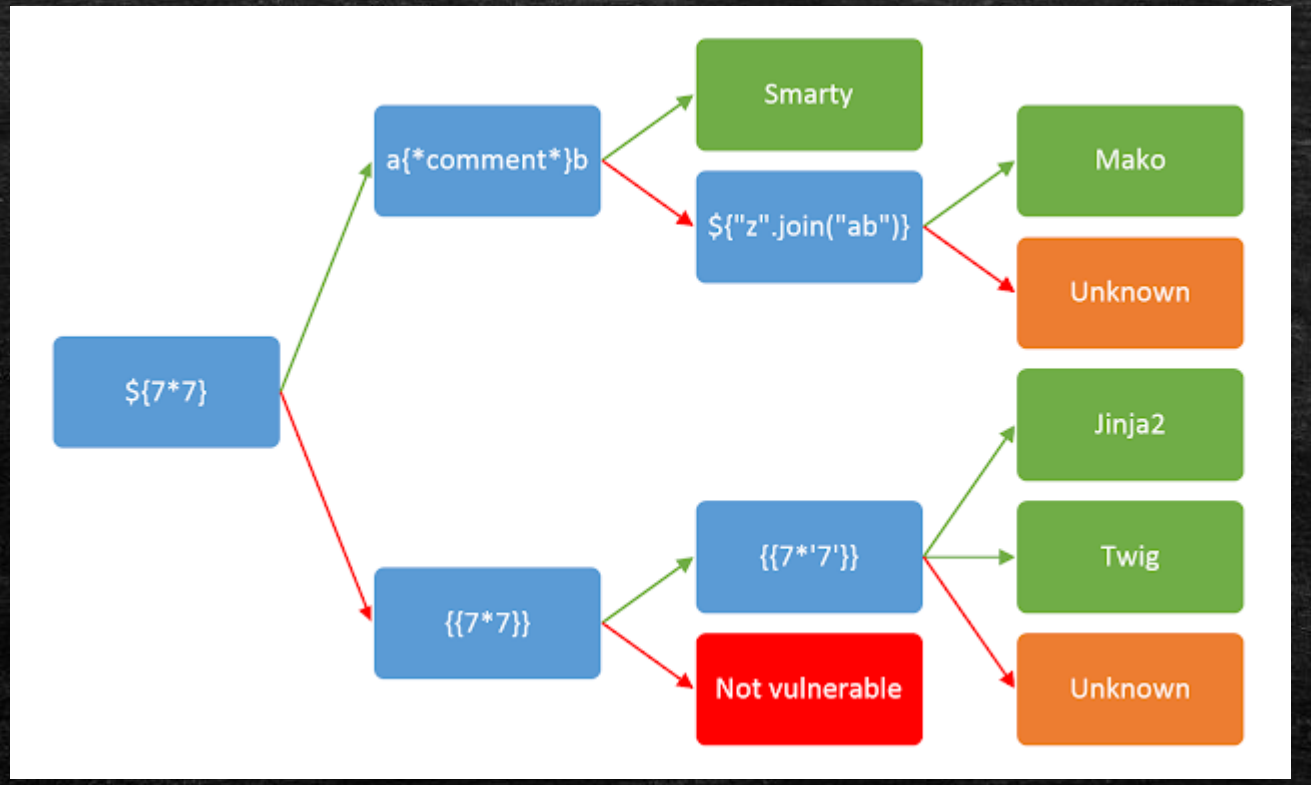
# Example in jtwig

```
{% if (user.loggedIn) %}
<div class="greeting">
   Hello <span class="usename">{{ user.greetingName }}</span>!
</div>
{% else %}
<div class="login">
   Hello there! Try to <a href="/login">Login</a>
</div>
{% endif %}
```

# SSTI – Server Side Template Injection

- Unsafe user inputs are embedded into templates.
- It can be easily mistaken for XSS attacks.
- Can lead to complete server compromise .
- Some examples: smarty, freemarker, mustache, mako, jinja2, twig, jtwig  and lot more.
- More reading:
  - https://portswigger.net/blog/server-side-template-injection

# Detection Techniques




https://portswigger.net/blog/server-side-template-injection

# DEMO

Setup:

- Xtreme Vulnerable Web Application (XVWA)
  - https://github.com/s4n7h0/xvwa

# Takeaway

- Traditional testing methodologies may happen to miss SSTI, unless you explicitly look for it.
- Impacts finding severity and overall security posture of application.
  - XSS (medium/low)
  - RCE (critical/high)