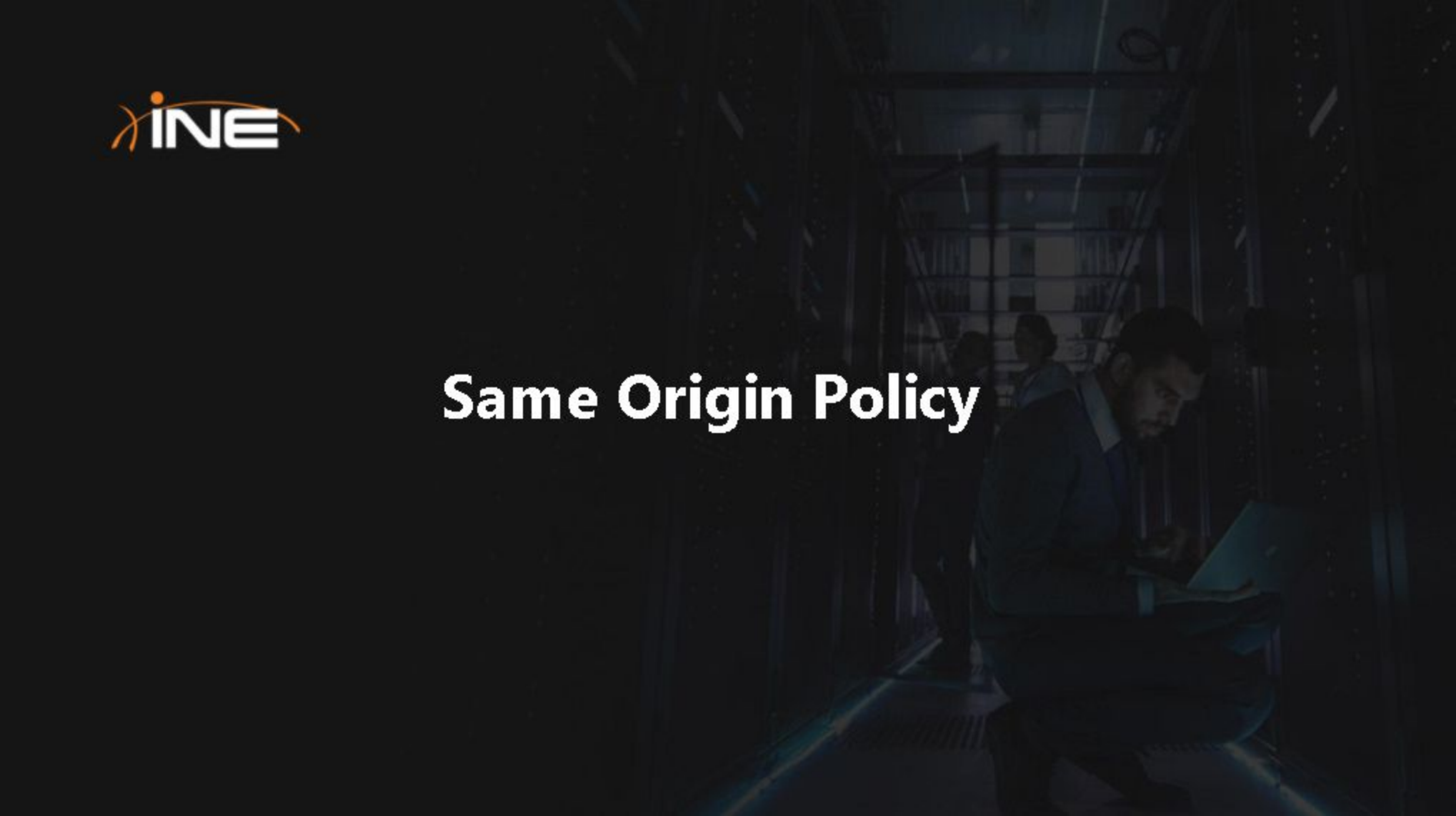

Same Origin Policy

3.5 Same Origin Policy

- **Same Origin Policy** (SOP) is a critical point of web application security.
- This policy prevents JavaScript code from getting or setting properties on a resource coming from a **different origin**.

3.5 Same Origin Policy

- The browser uses:

- To determine if JavaScript can access a resource: *Hostname*, *port*, and *protocol* **must match**.

3.5 Same Origin Policy

EXAMPLE

A JavaScript script on

- `https://www.elearnsecurity.com:345/`

protocol — hostname — port

can read resources from:

- `https://www.elearnsecurity.com:345/path`
- `https://www.elearnsecurity.com:345/path/2`

3.5 Same Origin Policy

EXAMPLE

+ But not from:
  - `https://www.elearnsecurity.com/path`
    (same protocol and domain but different port)
  - `http://www.elearnsecurity.com:345/path`
    (same port and domain but different protocol)
  - `https://www.heralab.net:345/path`
    (same port and protocol but different domain)

3.5.1 HTML Tags

- Note that SOP applies only to the **actual code of a script**.
- It is still possible to include external resources by using HTML tags like `img`, `script`, `iframe`, `object`, etc.

3.5 Same Origin Policy

- The entire web application security is based on Same Origin Policy.

- If a script on domain A was able to read content on domain B, it would be possible to steal clients' information and mount a number of very dangerous attacks.