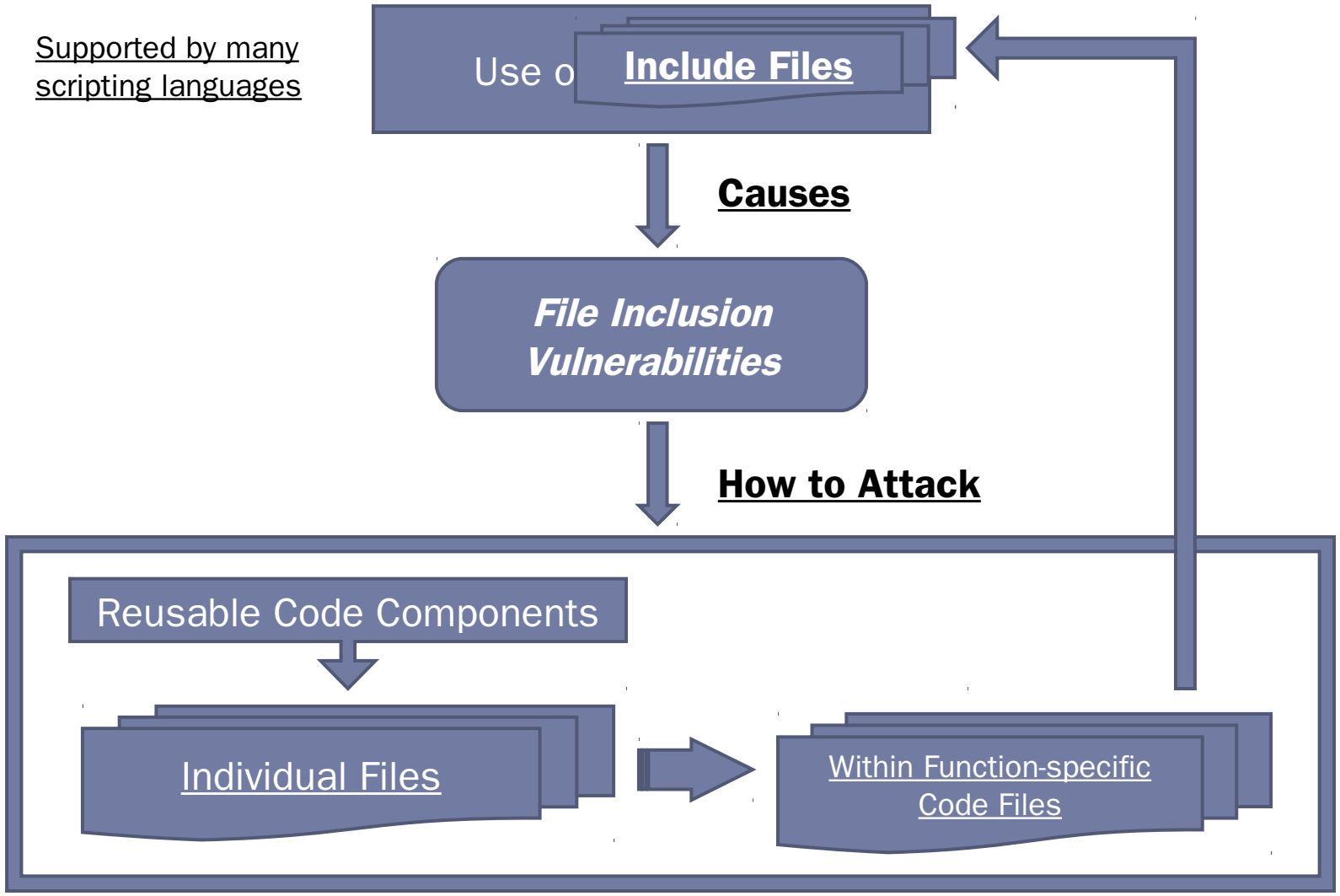
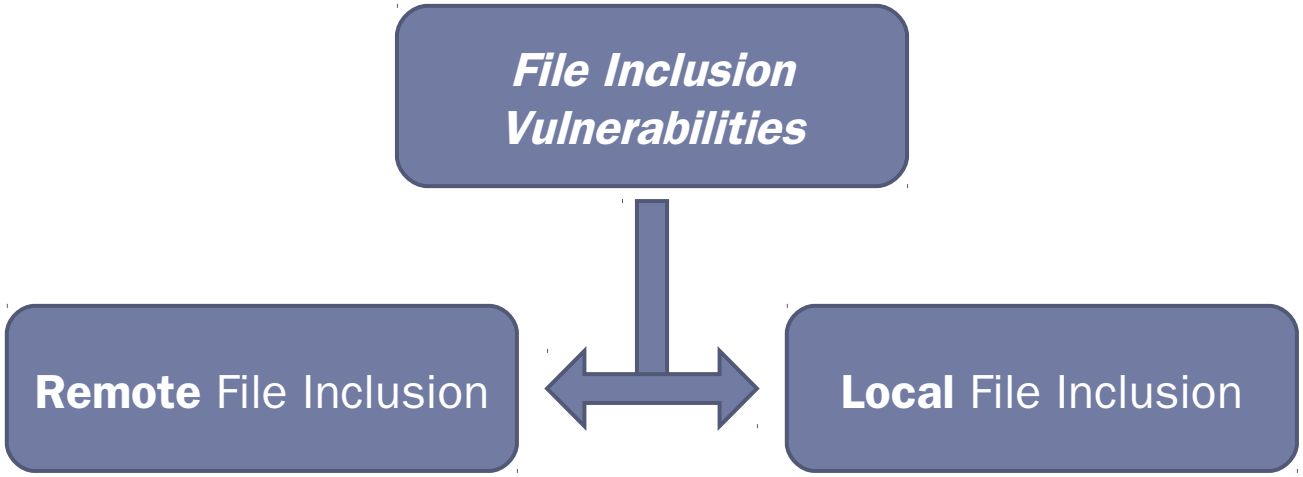
File Inclusion Vulnerabilities

Luyao Cui 2009553330
PAV Lab

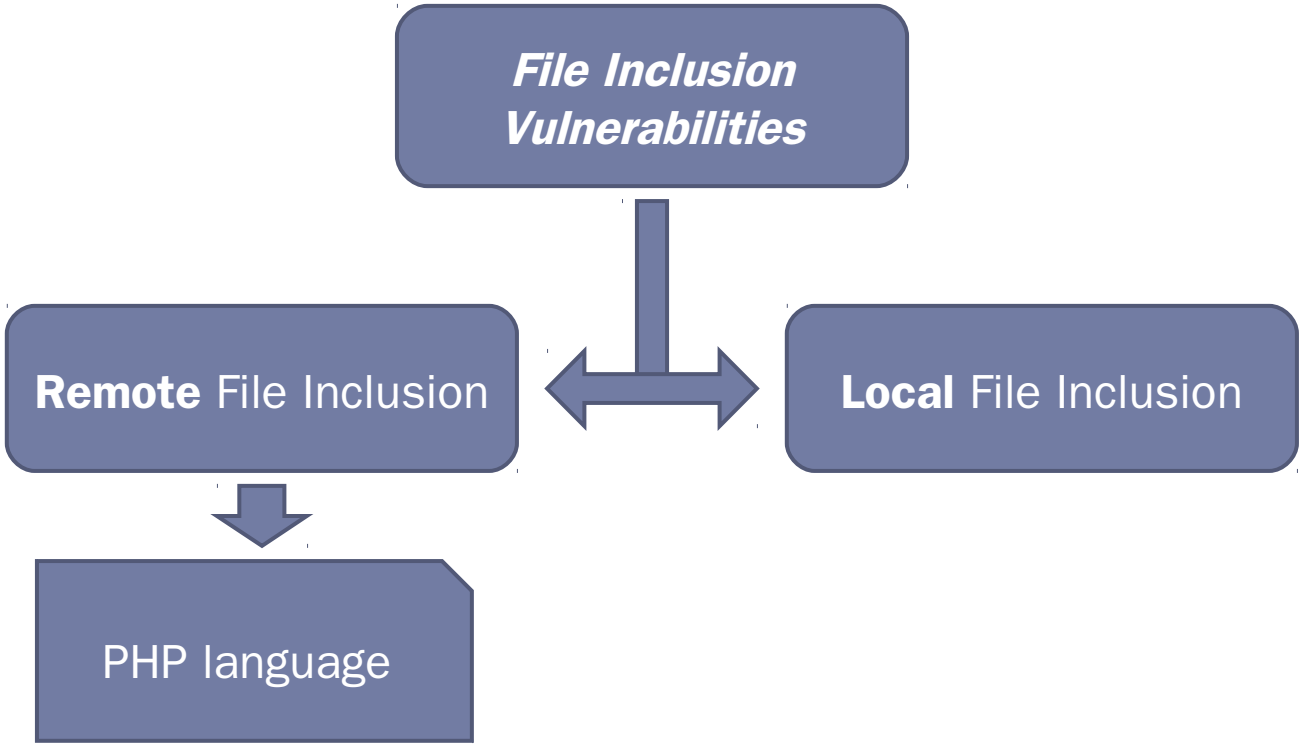
Introduction



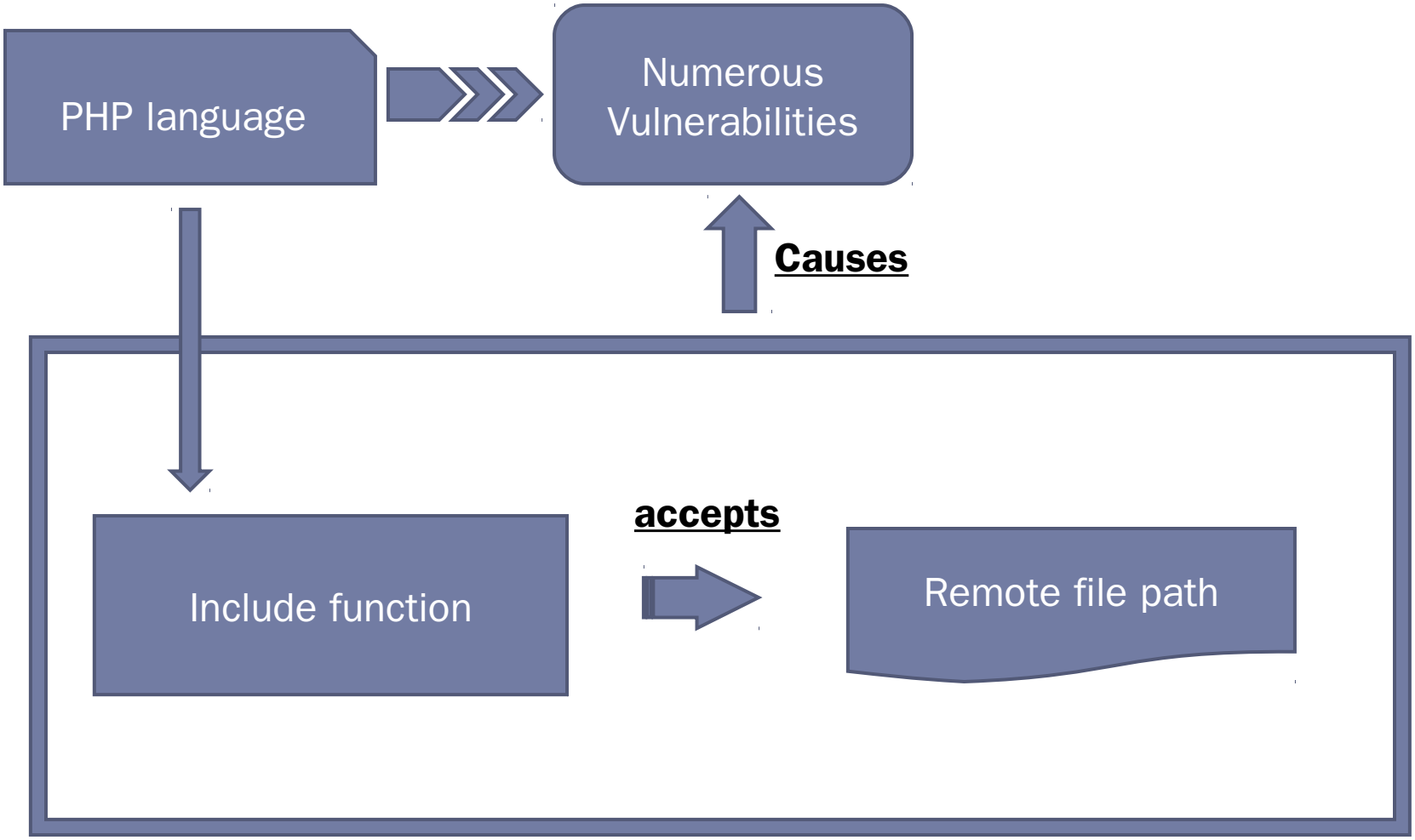
Introduction



Introduction



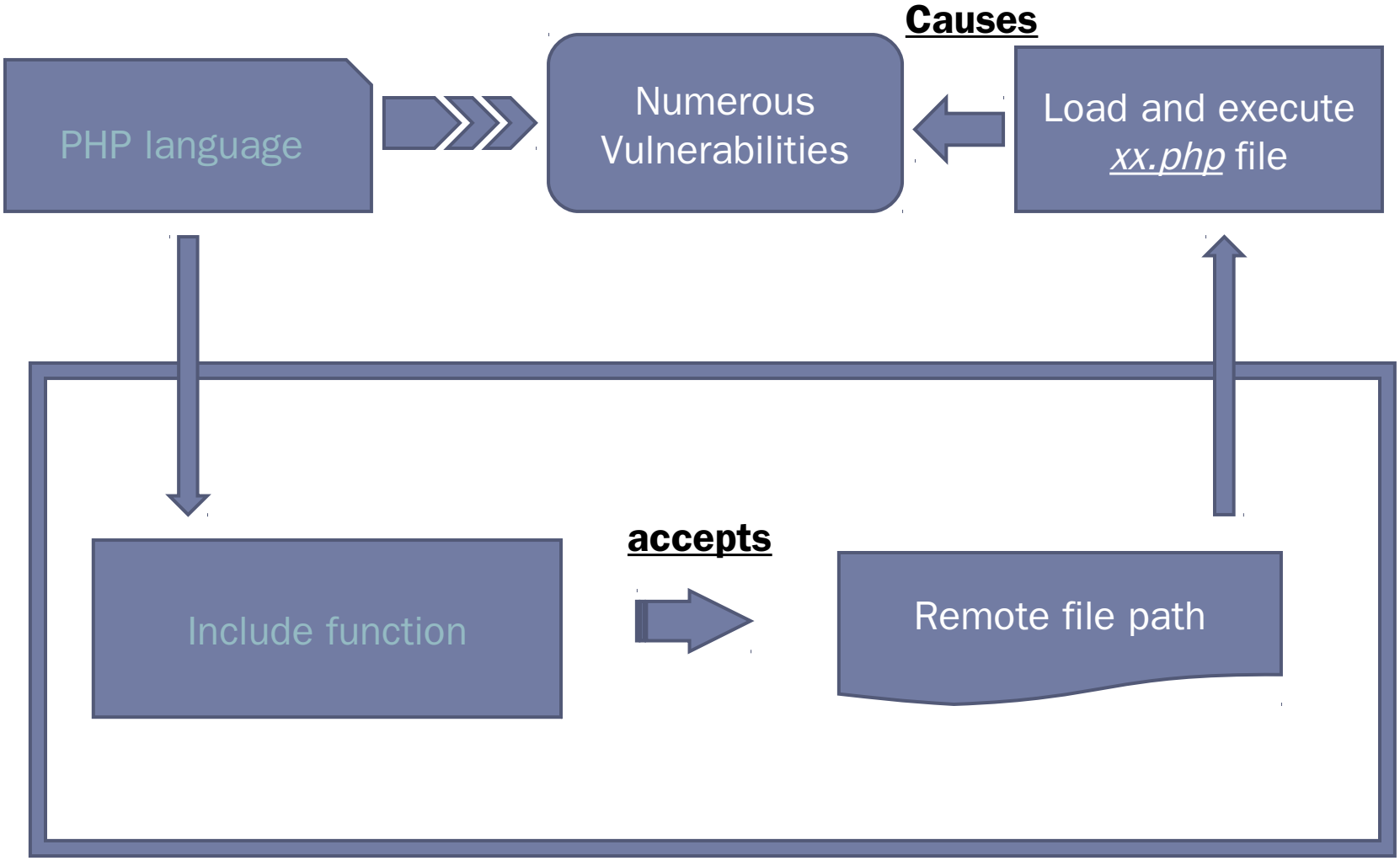
Remote File Inclusion (PHP)



Remote File Inclusion

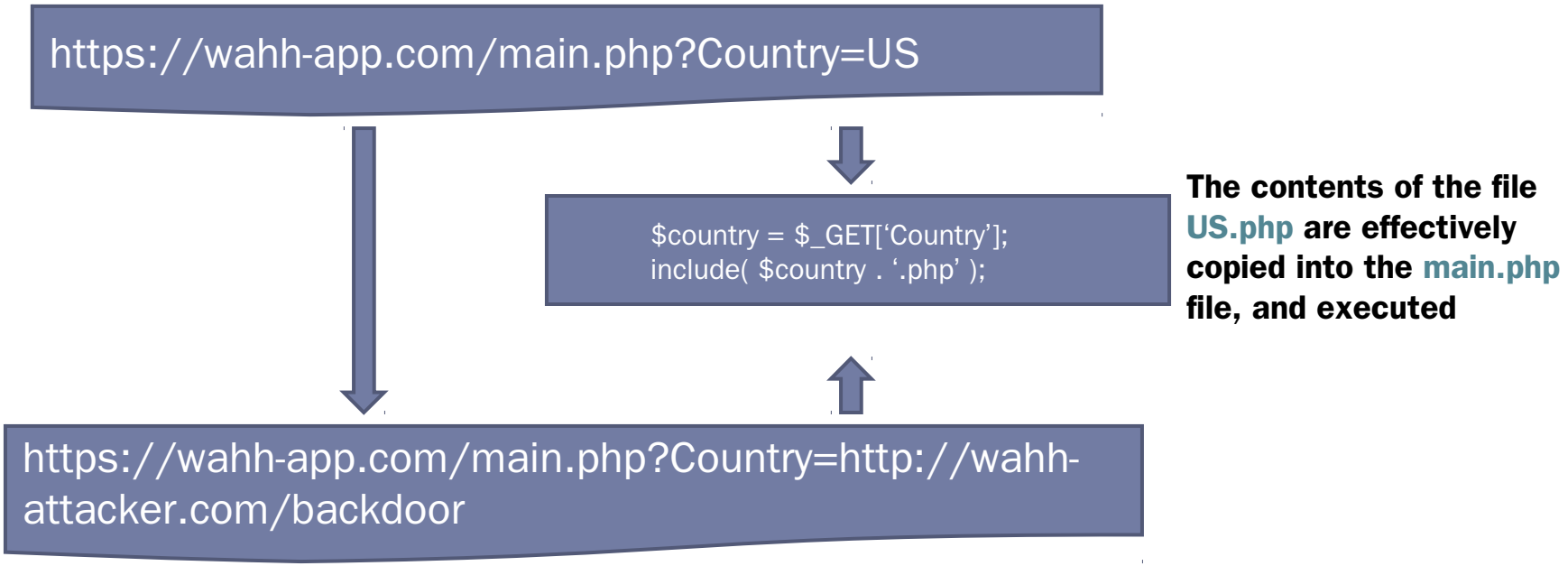
- Example
  - Microsoft Homepage
  - Others…
    - HYU Homepage

Remote File Inclusion (PHP)



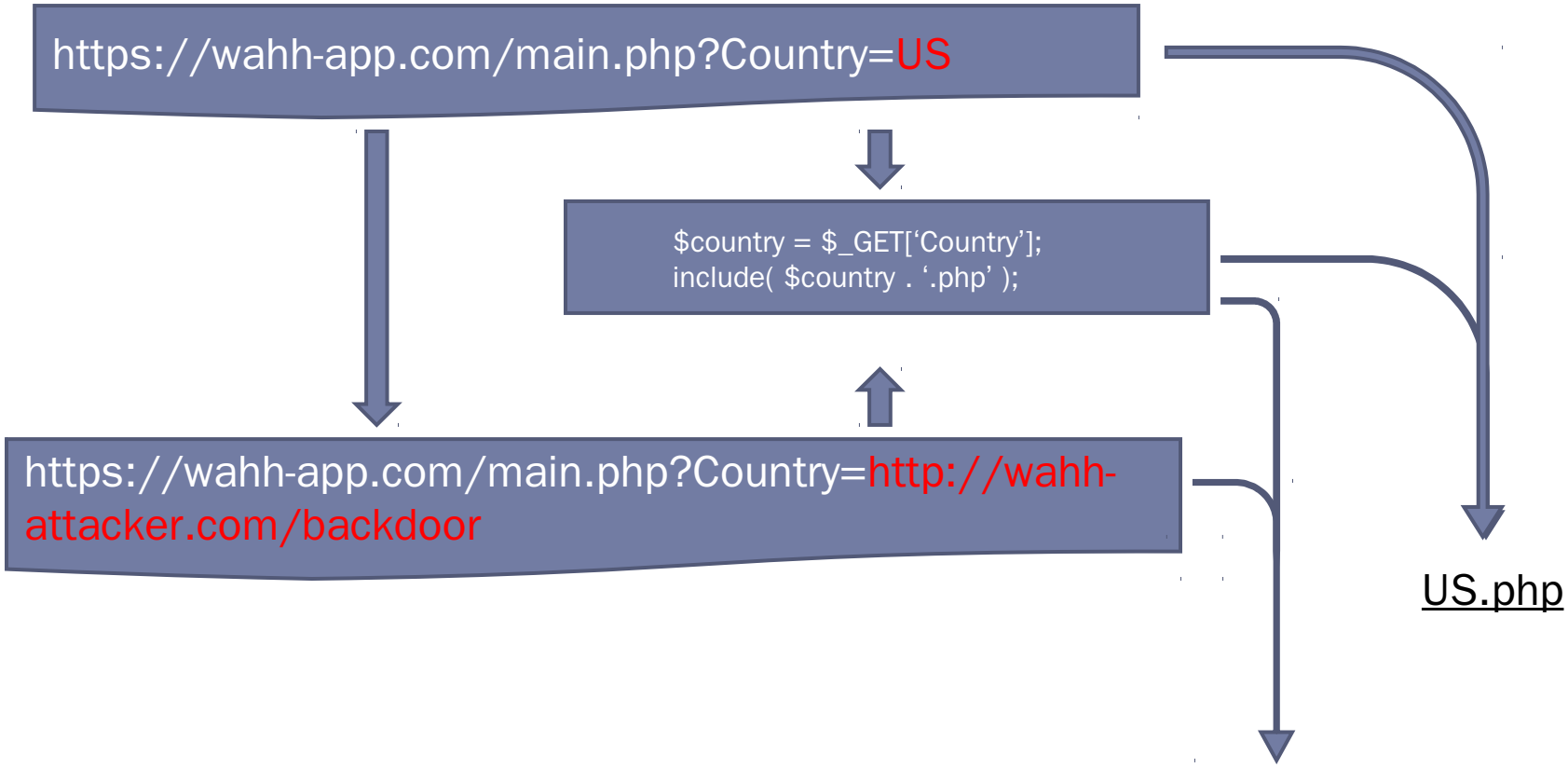
Remote File Inclusion (attack)

Different ways to attack.
Most serious – to specify an external URL as the location of the include file



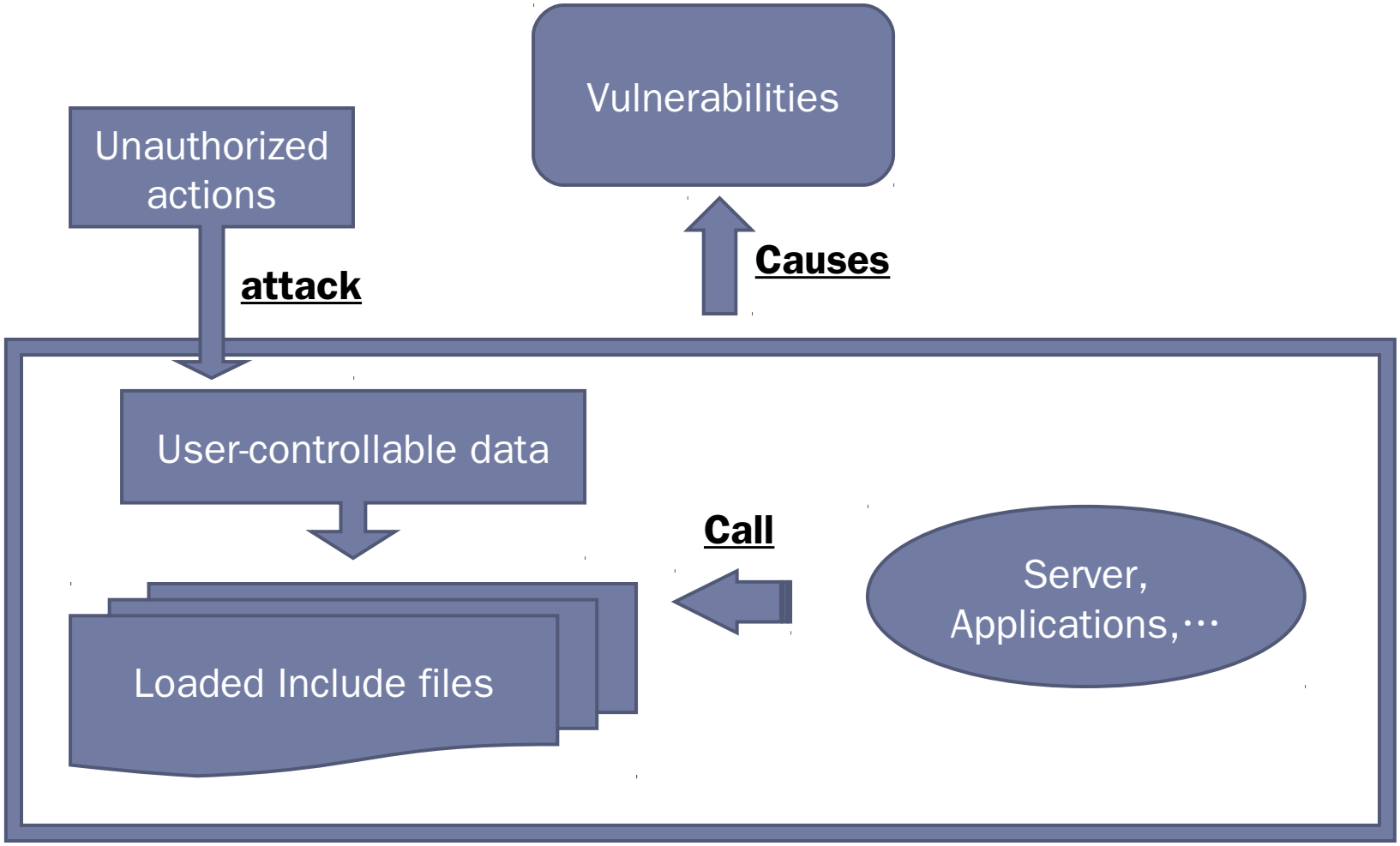
The contents of the file US.php are effectively copied into the main.php file, and executed

Remote File Inclusion (attack)

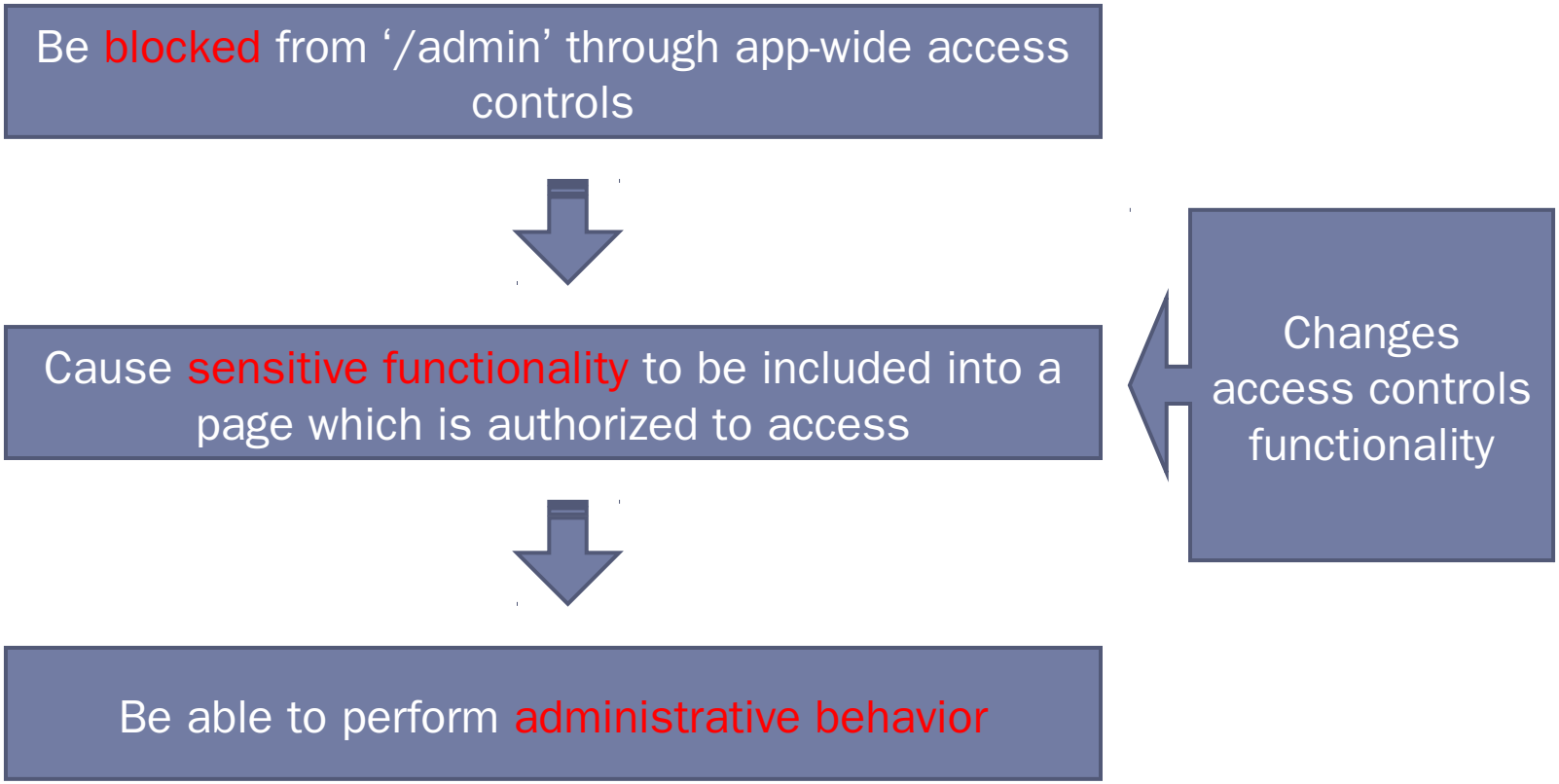


With a malicious script containing arbitrarily complex content

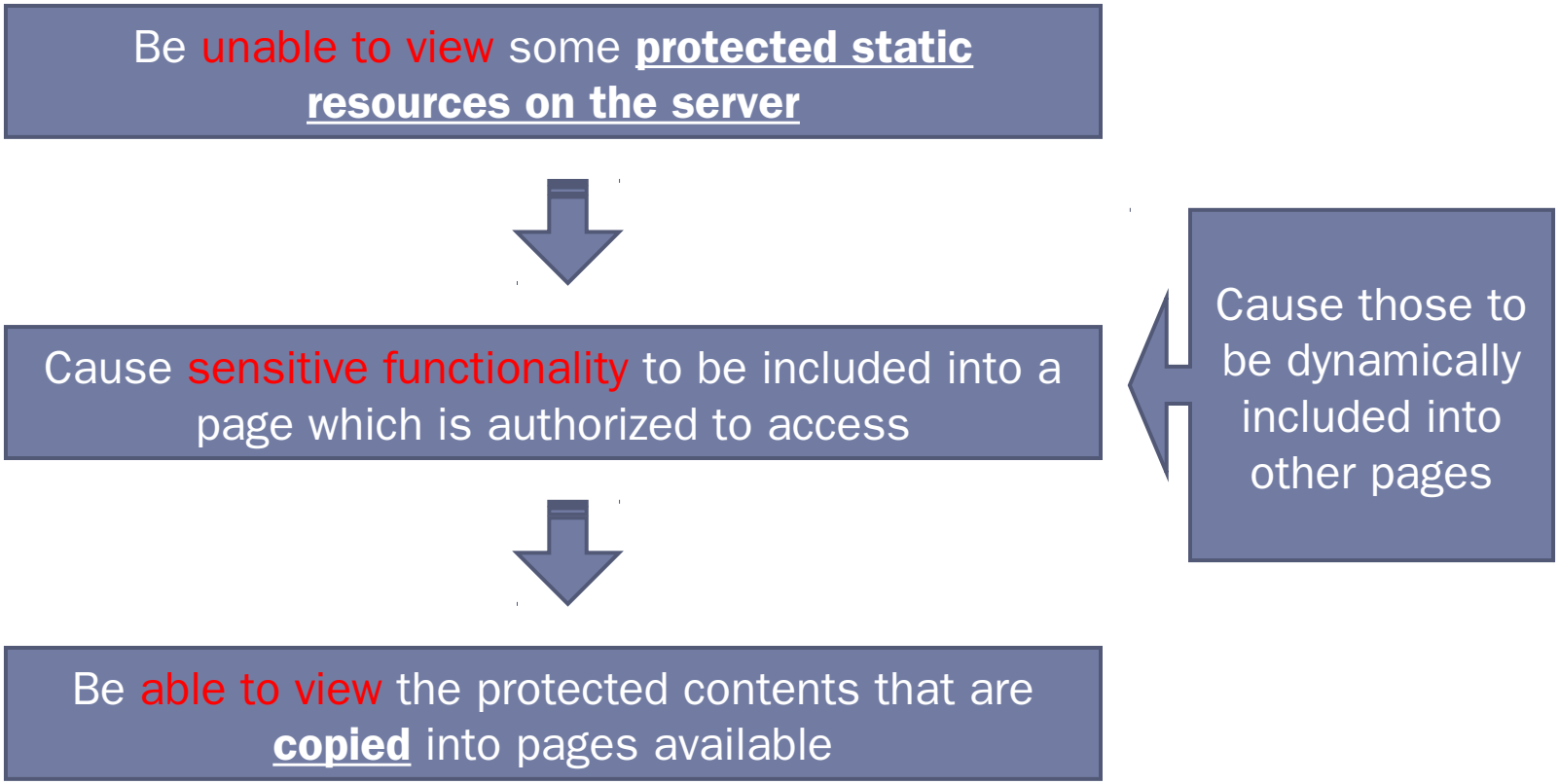
Local File Inclusion



Local File Inclusion (attack 1)



Local File Inclusion (attack 2)



How to Find File Inclusion Vulnerability

- Request user-supplied data
  - Request parameters that specify a language or location
- Parameter using names of a server-side file

How to Find File Inclusion Vulnerability

- Remote File Inclusion
  - ***Step 1***. **Control** a web server (be external to the target web-app)
  - ***Step 2***. **Submit a URL** (of your server) in each parameter of the web-app, and see if your server **receives any requests** from the target web-app (if so, proved)
  - ***Step 3***. **Submit a URL** containing a **nonexistent IP** address to see if a **timeout** occurs(if so, proved)
  - ***Step 4***. Do **attacks** as described before

How to Find File Inclusion Vulnerability

- Local File Inclusion(wider range than RFI)
  - ***Step 1***. Get to know the **information about resources** on the target web-app server
  - ***Step 2***. Submit the name of a known **executable resource** on the server, and watch the behavior (**changes**)
  - ***Step 3***. Submit the name of a known **static resource** on the server, and watch the behavior (**copied contents**)
  - ***Step 4***. Record **protected resources**, and do **attacks** as described before to watch the behavior.(if succeed in access, proved)

Preventing Script Injection Vulnerability

- Concerning any dynamic execution or include functions --
  - No user-supplied input or derived data
  - Strictly validated input
    - White list of good input
    - White list of harmful input

Thank You!!