



Content Security Policy (CSP)

PRESENTED BY : SUSHMITA POUDEL

Agenda



Introduction to CSP



Why is it Used ?



How does it work ?



Demo



Impact



Conclusion

Content Security Policy



A mechanism to define allowed resources for a web page

Can be understood as a policy for scripts, images and iframes

Implemented via response headers or HTML meta elements

Implementation of CSP

Implemented via Response Header:

```
Content-Security-policy: default-src 'self'; script-src 'self'  
allowed.com; img-src 'self' allowed.com; style-src 'self';
```

Implemented via meta tag:

```
<meta http-equiv="Content-Security-Policy" content="default-src  
'self'; img-src https://*; child-src 'none';">
```

Directives

default-src - Default directive for loading resources and is used to verify if a resource is allowed to load when no specific directive is specified for its type.

script-src - This directive specifies the sources wherefrom JavaScript scripts can be loaded and executed.

style-src / img-src / font-src / media-src - These directives specify from which locations CSS stylesheets, images, fonts and media files (audio/video) respectively can be loaded

Sources

'self' - This source allows you to load resources that are hosted on the same protocol (http/https), hostname (example.com), and port (80/443) as the website.

'*' - This source is a wildcard, which means content for that specific directive can be loaded from anywhere.

'none' - This is the opposite of the wildcard (*) source as it fully disallows loading resources of the specified directive type from anywhere.



How Does
it Work ?

How Does CSP Work ?



Restricts origins for active and passive content loading

Restrict certain aspects of active content like inline JavaScript, eval()

Developers need to define allowed origins for each resource type used on website

Website "owaspkathmandu.com" loads resources from "localhost" and "wannagethacked.com"

Why
CSP is
used ?



Why CSP is used ??



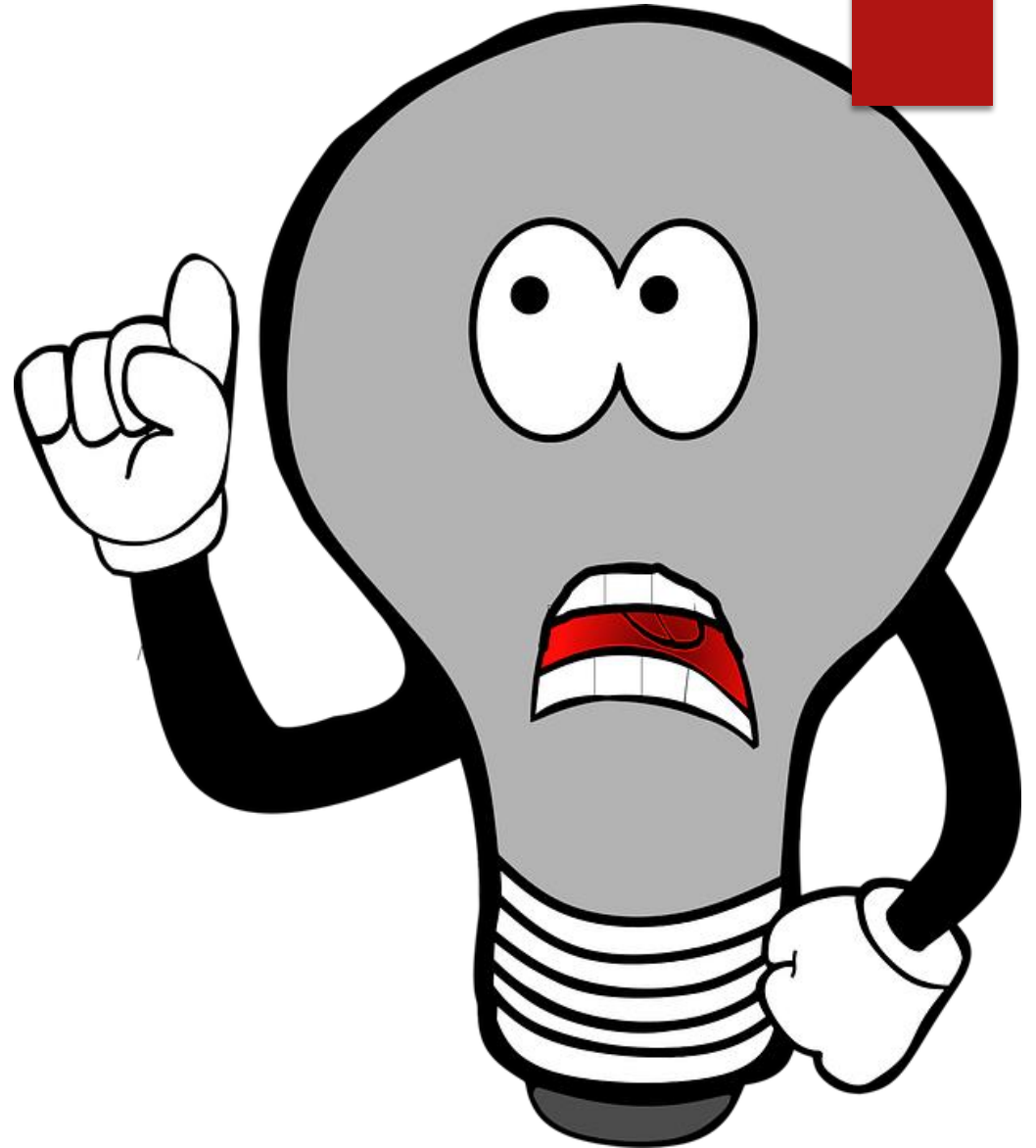
Secure web applications against content injection attacks, such as XSS

Provides an additional layer of security and can also provide information about blocked attacks

CSP provides a way for website owners to define a whitelist of trusted sources for different types of content

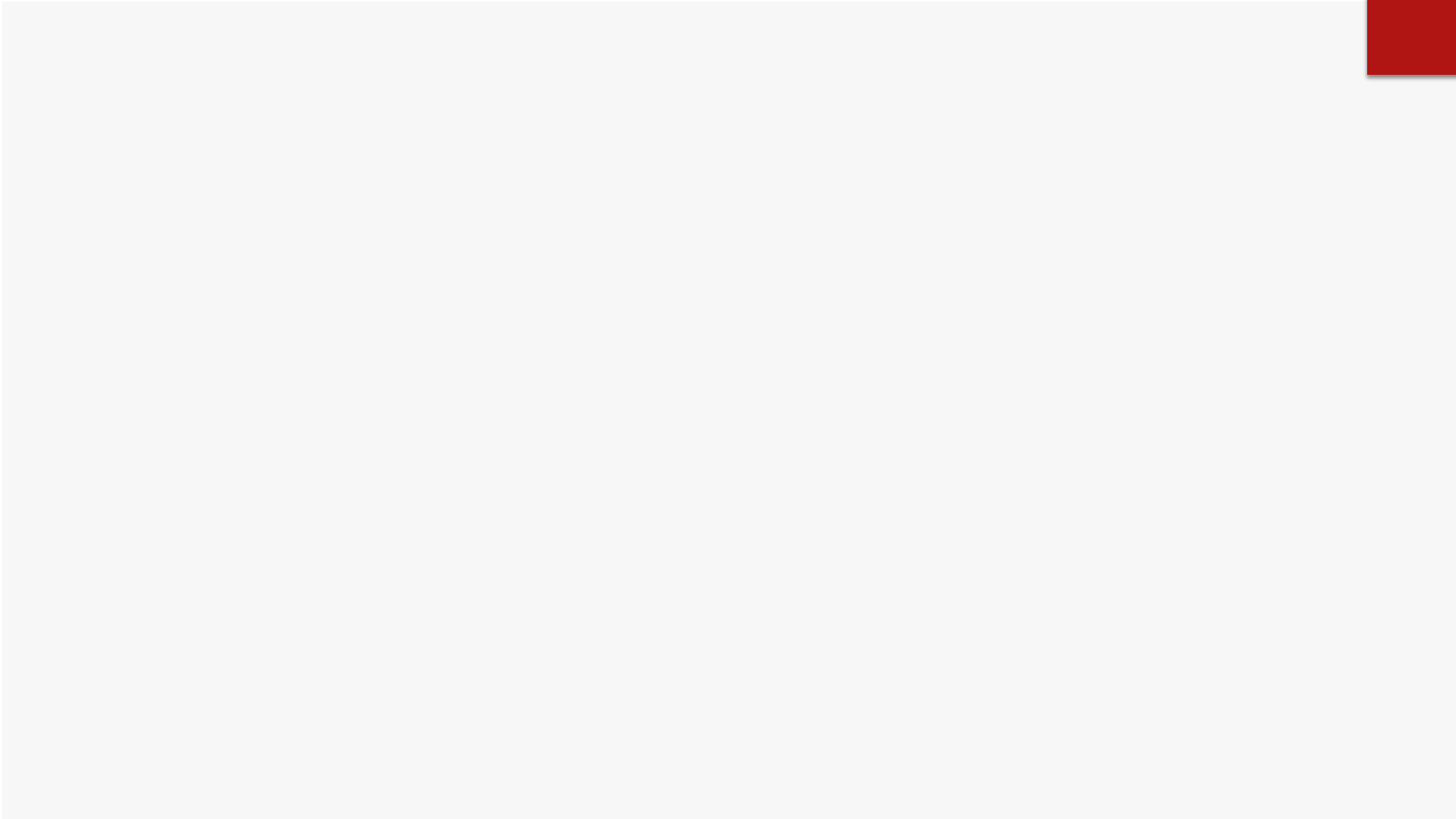
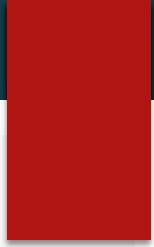
Can we think CSP
as mitigation of
XSS?

The answer is no!

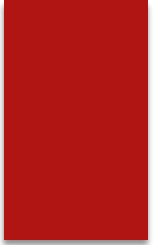




DEMO



IMPACT



Improves the security of a website by limiting the types of content that can be loaded and executed by a web browser.

CSPs can also provide a way to monitor and track the effectiveness of security measures and improve website security over time.

Implementing a Content Security Policy (CSP) can help a website meet compliance requirements such as PCI-DSS and OWASP.

Conclusion

We saw the importance of CSP as a defence in-depth strategy against XSS attack

However, poor implementation of CSP can be bypassed easily.



Thank You

ANY QUESTION ???