# Controlling the Browser to Protect Against Cross Site Scripting (XSS) and Click-jacking Attacks


**Roland Guijt**

MICROSOFT MVP, CONSULTANT, AUTHOR AND SPEAKER

@rolandguijt  rolandguijt.com

# Module Overview

Cross Site Scripting (XSS) attacks

Content Security Policy (CSP)

Click-jacking attacks

CSP Frame Source and the x-frame-options header

The Feature-policy header

# XSS = JavaScript injection attack

# X-XSS-Protection

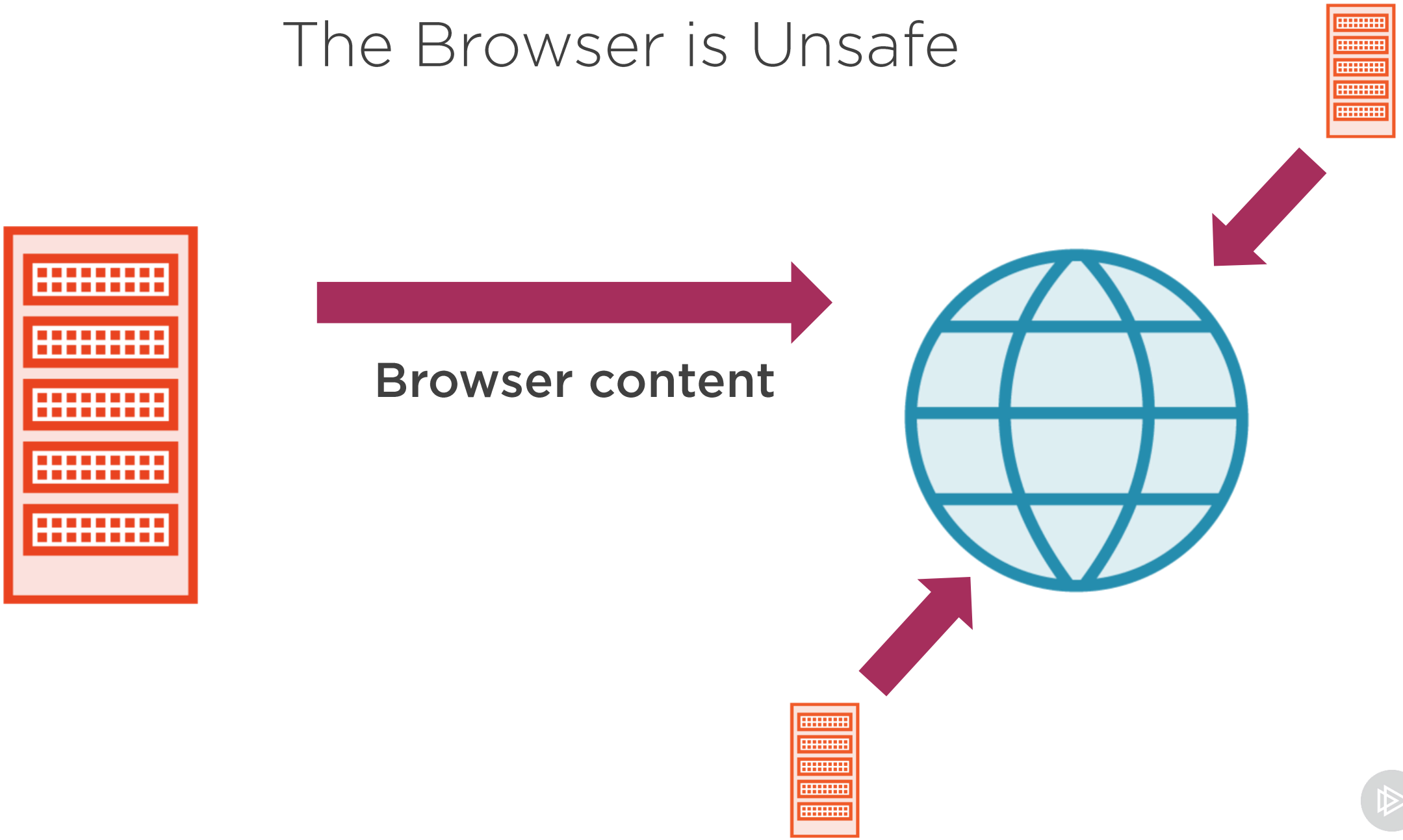
```
X-XSS-Protection: 1; mode=block
```

# XSS Consequences

Attacker can access everything in the browser

External JavaScript files can be downloaded that automate further attacks

# The Browser is Unsafe



# Content Security Policy (csp)

```
Content-Security-Policy: style-src ‘none’
```

Content Security Policy Options

*

'self'

'none'

<origin(s)>

# CSP Content Types

- script-src
- style-src
- img-src
- media-src
- frame-src
- font-src
- default-src

# Content Security Policy (csp)

```
Content-Security-Policy: style-src ‘none’ ‘unsafe inline’
```

https://4sh.nl/cspcreate

# Click-jacking

# Click-jacking

```
<form action="https://bank.com/api/transfer" method="post">
  <input type="hidden" name="Amount" value="1000000"/>
  <input type="hidden" name="AccountNumber" value="4356283"/>
  <input type="submit"/>
</form>
```

frame-ancestors in CSP prevents your site to be shown in IFrames on other sites

# X-Frame-Options

```
X-Frame-Options: DENY
X-Frame-Options: SAMEORIGIN
X-Frame-Options: ALLOW-FROM https://example.com/
```

# CSP: Controlling the Showing of IFrames

**frame-src**

**child-src**

# Feature Policy

```
Feature-Policy: camera ‘none’
```

# Feature Policy Supported Features

- accelerometer
- ambient-light-sensor
- autoplay (auto start playing video/audio)
- camera
- fullscreen
- gyroscope
- magnetometer
- microphone
- midi
- payment (payment requests)
- sync-xhr (synchronous HTTP requests from js)
- usb (web usb)

# Feature Policy Options

*

**‘self’**

**‘none’**

**<origin(s)>**

# Summary

Restricting the browser =
reducing the attack surface

Done by sending specific HTTP headers