OWASP

The Open Web Application Security Project

About Me

OWASP
The Open Web Application Security Project

- Maty Siman
- Founder and CTO of Checkmarx – Static Application Security Testing (AKA – Source Code Analysis)

CHECKMARX

Agenda

OWASP
The Open Web Application Security Project

- New Tricks, Old Dog
- New Tricks, New Dog
- Too Good

New Tricks, Old Dog

OWASP
The Open Web Application Security Project

- Super-charged XSS
  - Just an XSS
    - http://localhost/bookstore/Login.aspx?name=<script>alert('hi')</script>
  - Sticky
    - http://localhost/bookstore/Login.aspx?Name=<iframe src="http://localhost/bookstore/login.aspx" width="100%" height="100%“>
  - Now, we can use a component called HTML2Canvas to take screenshots
    - http://localhost/bookstore/TakePicture.js
  - This gives the following:
    - http://localhost/bookstore/Login.aspx?Name=<script src='http://localhost/bookstore/hijackpage.js'></script>
  - But we can further manipulate the component to even…. (Login page)

New Tricks, Old Dog

OWASP
The Open Web Application Security Project

- Super-charged XSS
  - Advanced port scanning (WebSockets)
    - http://www.andlabs.org/tools/jsrecon.html

Sandbox – why?

OWASP
The Open Web Application Security Project

- SOP -> 3rd party markets

Sandbox – pitfalls?

OWASP
The Open Web Application Security Project

Syntax

```
<iframe sandbox="value">
```

Attribute Values

Value	Description
""	Applies all restrictions below
allow-same-origin	Allows the iframe content to be treated as being from the same origin as the containing document
allow-top-navigation	Allows the iframe content to navigate (load) content from the containing document
allow-forms	Allows form submission
allow-scripts	Allows script execution

Source	Demo	Action	Pe
Host Embedded	Click	Alert	IFra
Host Embedded	Click	Alert	IFrame + Full SB
Host Embedded	Click	Alert	Iframe + SB allowing Scripts and SameOrigin
Host Embedded	Click	Top Navigation	Iframe + SB allowing Scripts and SameOrigin
Host Embedded	Click	Tricky”“ top navigation	Iframe + SB allowing Scripts and SameOrigin

Too Good

OWASP
The Open Web Application Security Project

- Pacman
  - http://worldsbiggestpacman.com/play/#-14,-25
  - Database
  - Cookies
  - Business logic
    - Breakpoint at Level.min.js : 131
    - if(b!=GhostState.DEATH){b=GhostState.FRIGHT; i.currBehavior.name=GhostState.FRIGHT;}

New Tricks, New Dogs

OWASP
The Open Web Application Security Project

- Demo

http://localhost/bookstore/k2.html