Integrating Web Application Penetration Testing into Your Vulnerability Management Program

Rich Mogull
Securosis, L.L.C.

Top Threats

Web Applications

Clientside

Why Web Applications Are Such a Problem

- Rapid development with limited QA
- Eternal beta cycles
- Un(security)trained developers
- New vulnerability classes
- Insecure browsers
- Inherent insecurity of web model

Major Webapp Attacks

Breaking Trust Relationships

Browser

Cross Site Scripting

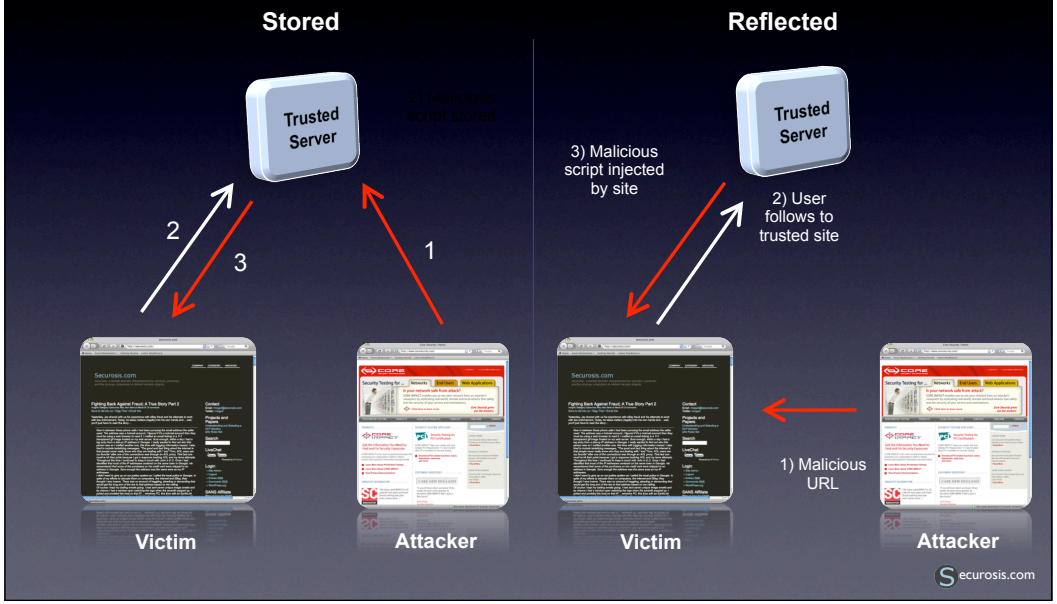
Cross Site Request Forgery

SQL Injection

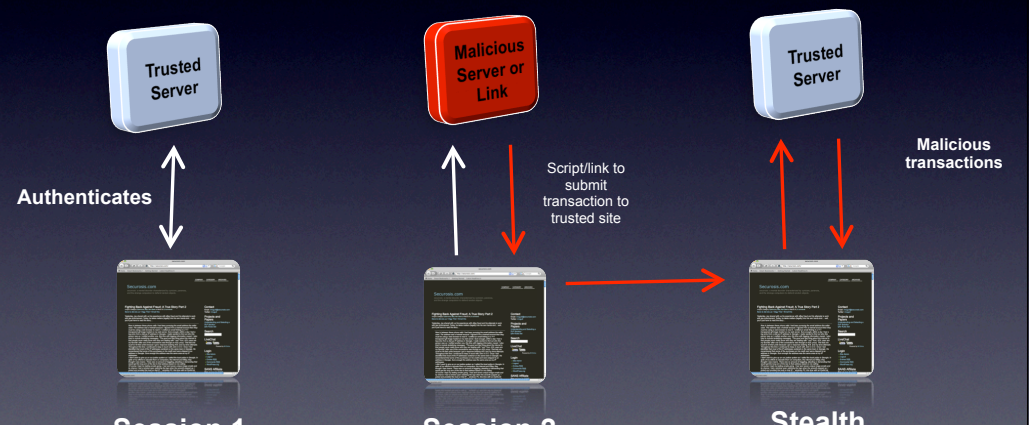
Server

Securosis.com

Cross Site Scripting



Cross Site Request Forgery



Securosis.com

SQL Injection

```
admin'--
```

Attack Input

```
Statement: "SELECT * FROM users WHERE
name = '" + uName + "' AND password =
'" + upass + "';"
```

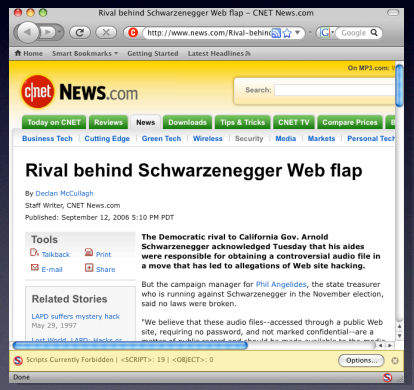
SQL Statement

```
SELECT * FROM users WHERE name =
'admin'-- "' AND password = '" + upass
+ "';"
```

Executed Statement

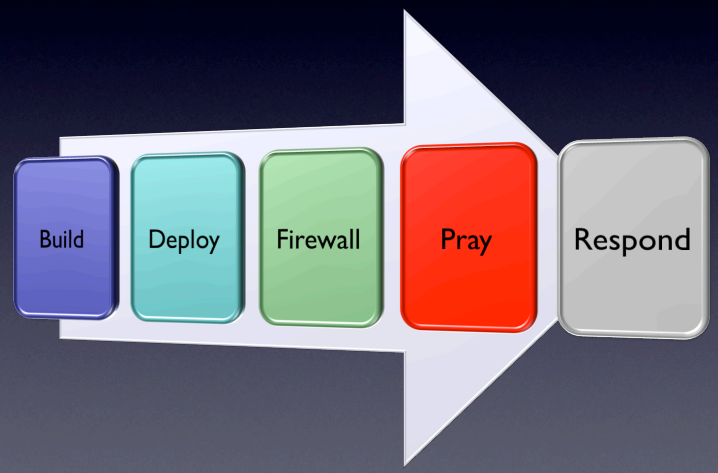
Accidental/Directory Traversal

+ Or - “/” =



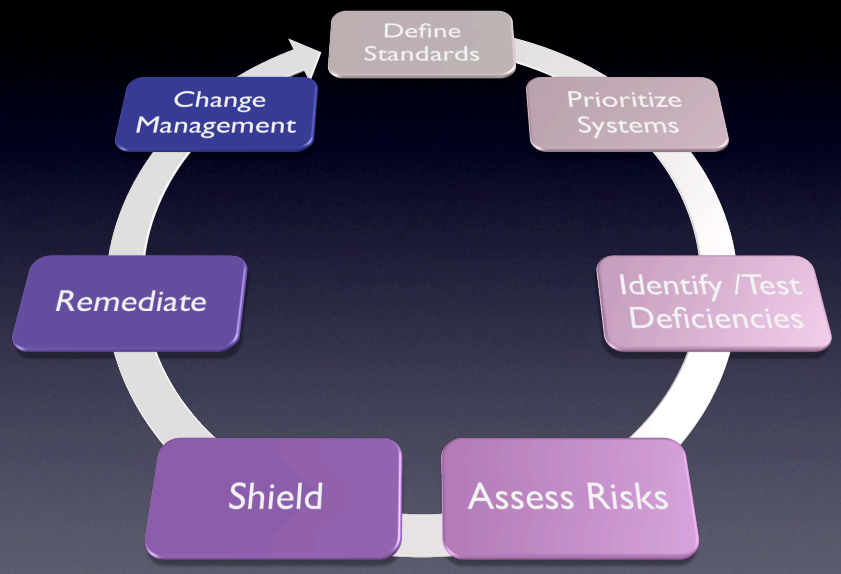
Securosis.com

How we used to manage web applications



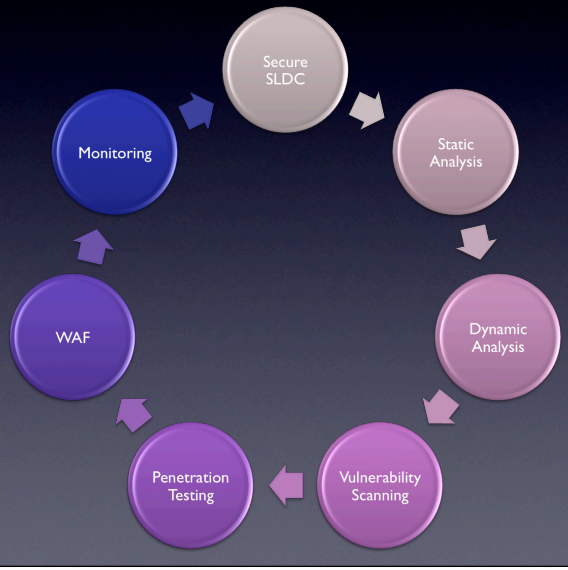
Securosis.com

Vulnerability Management



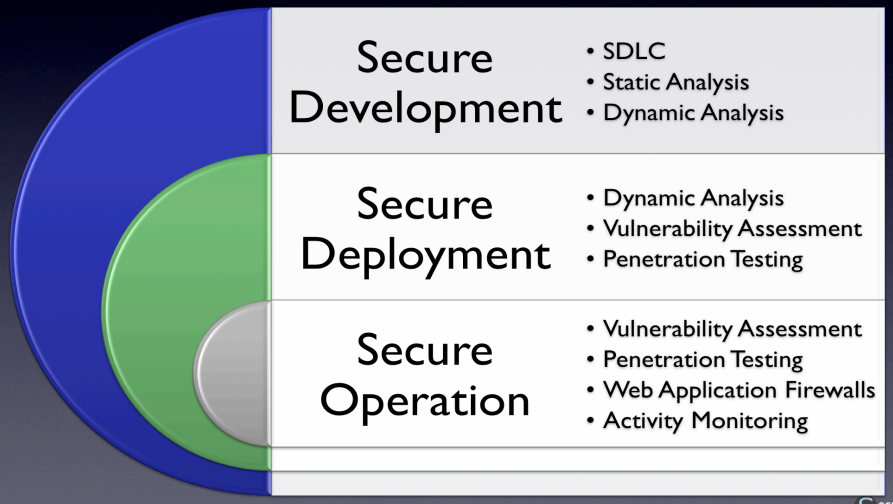
Securosis.com

Web Application Security Program Overview



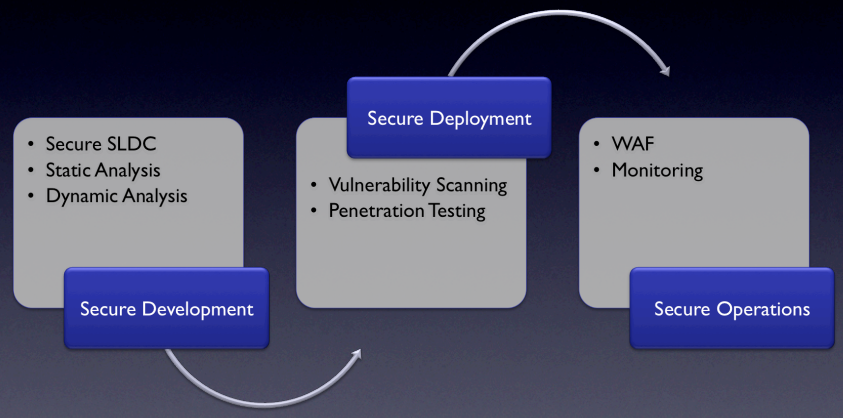
Securosis.com

Application Security Lifecycle

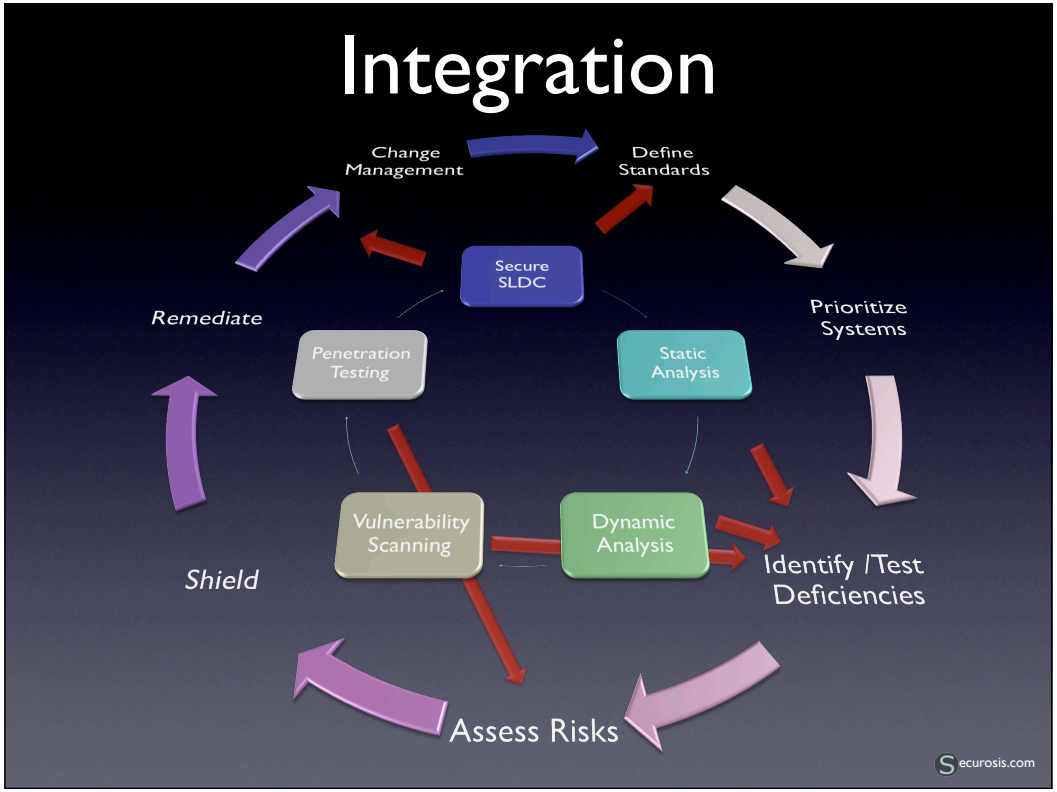


Securosis.com

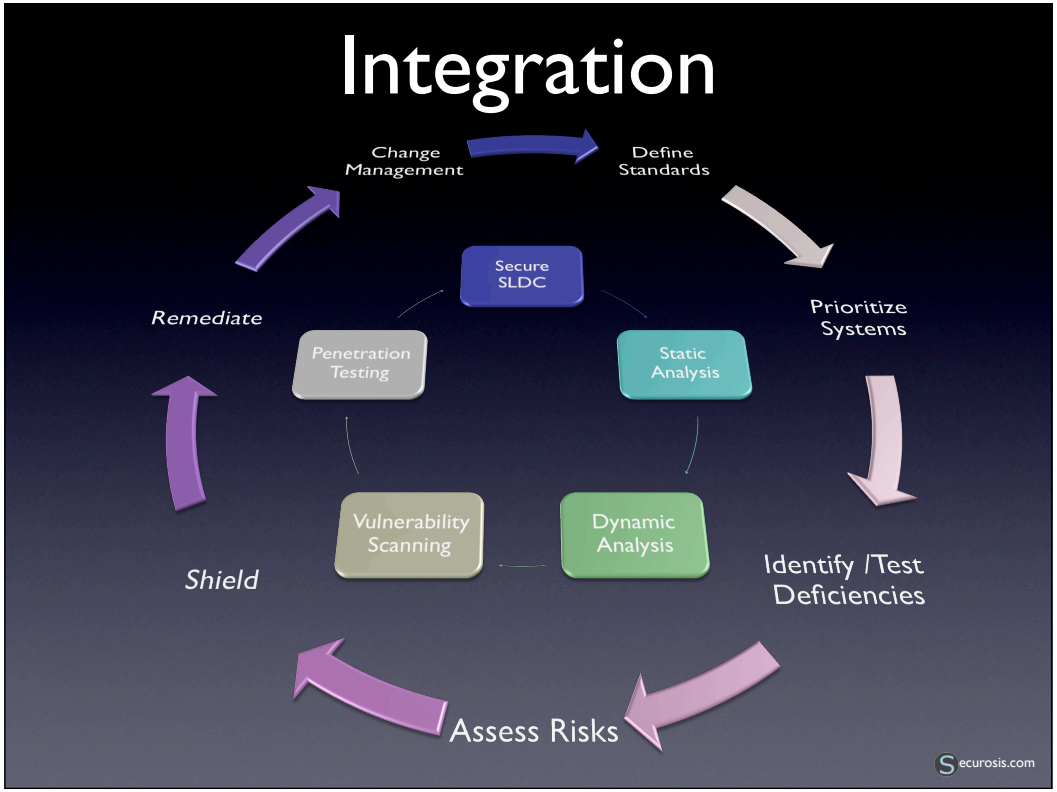
Development Phases



Securosis.com



Platform vulns



Platform vulns

Limitations of static analysis/scanning

- Can't catch everything
- No validation
- No exploitability/Impact
- Miss logic flaws
- Fire and forget
- The bad guys don't use them

Best Practices for Web App Pen Testing

- Begun testing in the development process.
- Use a combination of tools and manual process.
- Include traditional pen testing of the underlying platform.
- Perform periodic testing post-deployment, especially as new exploits appear.

Adapting your program for the long term

- Understand the different requirements of web application vulnerability management.
- Establish web application configuration standards and begin enforcement during development.
- Include code and vulnerability scanning, but you cannot skip penetration testing.

Integrating Web Application Penetration Testing into Your Vulnerability Management Program

Rich Mogull
Securosis, L.L.C.
http://securosis.com
rmogull@securosis.com