Web Applications: The New Threat

Joe Klemencic
Fermilab Computer Security
InterLab Oct 2006

Out with the old…

- System vulnerabilities
- Protocol vulnerabilities
- Service vulnerabilities

In with the new…

- Web application frameworks
- Web 2.0
- CGI handlers
- Custom scripts
- Input Injection
- Malformed URL’s
- XSS
- Redirects

Goals

- Exploit users connecting to your web site
  - Redirects
  - XSS
  - Cookie/session stealing
- Read system files on web server
  - Directory traversal
  - Obtain access to sensitive files
- SQL Injection
- Abusing PHP Includes
- Run commands
- Deface!
- Get a shell!!!

Enough talking, let’s demonstrate

Recap

- Your users can be compromised simply by accessing your web site
- Sensitive files can be stolen from the web server
- Bypass ‘controls’ to gain access to the raw database
- Frameworks are often vulnerable

All of these are risks of embarrassment and possible legal liability and should be considered in your Risk Assessment

Mitigation

- Keep current on ALL patches
  - Operating System
  - Web Server
  - Scripting interpreters
  - Frameworks
- Remove dormant applications

INPUT VALIDATION!!!!