

# SOFTWARE SECURITY ASSURANCE SUMMIT

June 9, 2011 | The Broadmoor | Colorado Springs, CO

## Web Scanning Challenges

The Pro's and Con's of Remote Dynamic Application Security Testing

Matt Fisher, AppSec SME



*presented by*



# SOFTWARE SECURITY ASSURANCE SUMMIT

June 9, 2011 | The Broadmoor | Colorado Springs, CO

## Introduction

HP Software US Public Sector organization  
Report to Robert Roy, CTO of Fortify Federal

Application security since 2002  
Early member of SPI Dynamics  
Industry builder – primary research, assessment and exploit techniques,  
strong product drivers

Spoken at countless conferences, published multiple times.

Piscis – Expert Boutique in Washington DC area



*presented by*



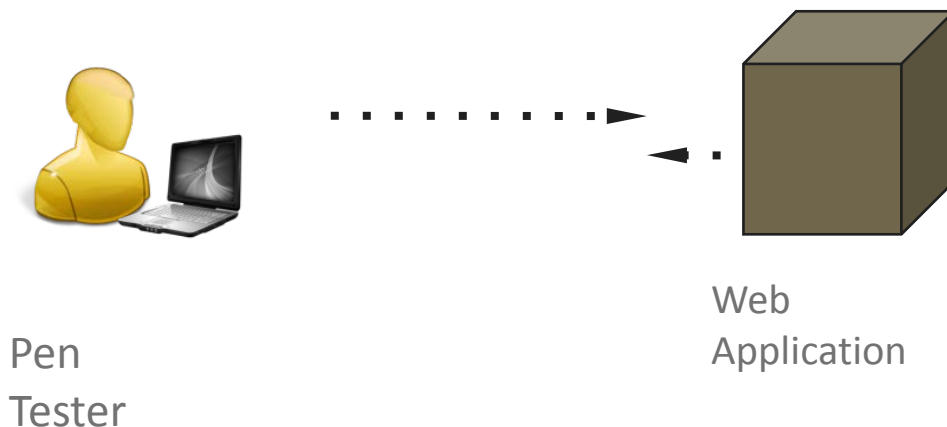


June 9, 2011 | The Broadmoor | Colorado Springs, CO

## Dynamic Application Security Testing

Web Application Scanning, Pen-testing, Black-box testing, DAST

- Test the software from the hackers point of view
  - Outside-in point of view
- Origins in automating the actions of ethical hacking



presented by





June 9, 2011 | The Broadmoor | Colorado Springs, CO

## DAST Methodology

- Works remotely over HTTP or SSL
- Crawls and indexes site as a search engine would.
- Performs additional discovery on the site (extraneous content, known vulnerabilities, etc).
- Wide variety of testing performed – known vulnerabilities, protocol, malformed packets, known framework issues, injection testing
- Parses out input fields for injection testing



*presented by*





June 9, 2011 | The Broadmoor | Colorado Springs, CO

## Web Application – Hacker's View

The screenshot shows a Mozilla browser window titled "iTrade : Login - Mozilla" with the URL `http://www.itrade.com/index.shtml?sessionId=02341751341342`. The page content includes a navigation menu with "CONTACT US" and "LOGIN" links, a "LOGIN to iTRADE" form with "User Name:" and "Password:" fields, and a "Submit" button. Several security vulnerabilities are highlighted with orange callouts:

- Session Hijacking**: Points to the `sessionId` parameter in the URL.
- Parameter Manipulation**: Points to the `sessionId` parameter in the URL.
- Insufficient Authorization**: Points to the "Forgot your Password?" link.
- Brute Force**: Points to the "Submit" button on the login form.
- Week Password Recovery**: Points to the "Forgot your Password?" link.
- SQL Injection**: Points to the "User Name:" input field.
- Account Enumeration**: Points to the "Forgot your Password?" link.
- Cross-site scripting**: Points to the "CONTACT US" link.



presented by





June 9, 2011 | The Broadmoor | Colorado Springs, CO

## Advantages of DAST

- Easily deployed
- Test the environment in addition to the pure app
- “Net Result” unaffected by typical source code challenges
- Definitive results via exploitable vulnerabilities



presented by





# SOFTWARE SECURITY ASSURANCE SUMMIT

June 9, 2011 | The Broadmoor | Colorado Springs, CO

## Popular Adoption

- Remote nature lent itself to security teams and penetrations testers.
- Very commonly used in independent verifications and security test and evaluations.
- Allows a “non-developer” to quickly and easily test software
- Great for continuous monitoring of web spaces



*presented by*





June 9, 2011 | The Broadmoor | Colorado Springs, CO

## Two Separate Worlds



*presented by*





# SOFTWARE SECURITY ASSURANCE SUMMIT

June 9, 2011 | The Broadmoor | Colorado Springs, CO



*presented by*



# SOFTWARE SECURITY ASSURANCE SUMMIT

June 9, 2011 | The Broadmoor | Colorado Springs, CO

## You Can't Shoot What You Can't See

Internal use of cryptography ?

Config (Global vars, RFI )

Publishing to other sources ?

Consuming from other sources ?

Interface-orphaned code



*presented by*





June 9, 2011 | The Broadmoor | Colorado Springs, CO

## Efficiency in Testing

Complex injections

Password Strength requirements ?

Password aging ? History aging ?

Vulnerable REQUIREMENTS !



*presented by*



# SOFTWARE SECURITY ASSURANCE SUMMIT

June 9, 2011 | The Broadmoor | Colorado Springs, CO

What is the goal of a web app assessment ?

~~Brush up on your data extraction skills~~

~~Learn a new hacking technique~~

~~Bring shock and awe to the system owner.~~

Find the bugs efficiently and effectively



*presented by*





June 9, 2011 | The Broadmoor | Colorado Springs, CO

## “Source Code Available” Testing



Blind SQL Injection  
Additional functionality  
Vulnerable REQUIREMENTS  
Unknown Interconnections



*presented by*





# SOFTWARE SECURITY



# ASSURANCE SUMMIT

June 9, 2011 | The Broadmoor | Colorado Springs, CO

## The Bridge



*presented by*

