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

T.E.N. presented by FORTIFY An HP Company

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

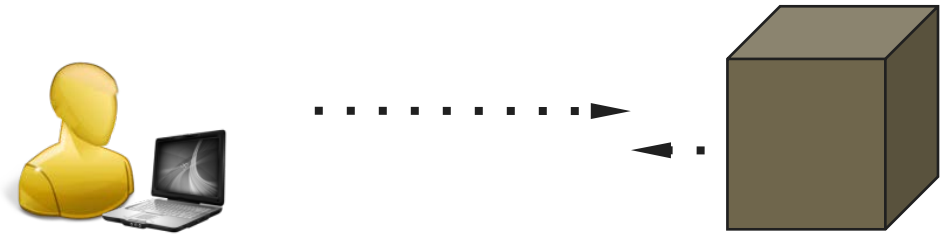
Spoken at countless conferences, published multiple times.

Piscis – Expert Boutique in Washington DC area

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



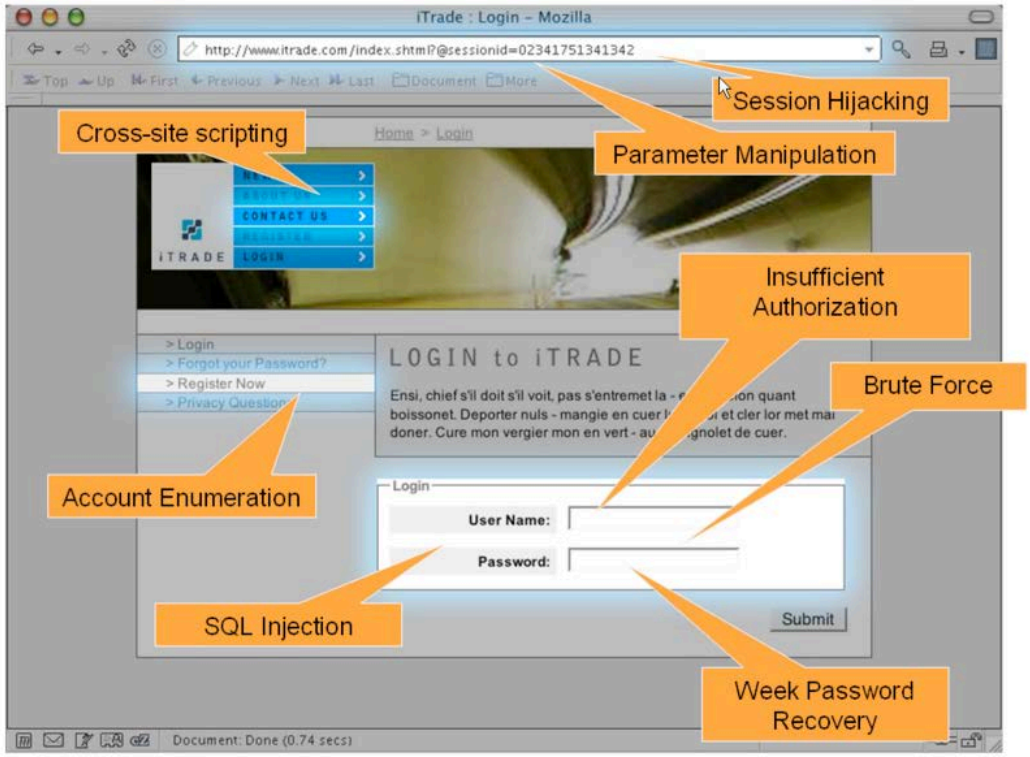
Pen Tester

Web Application

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

Web Application – Hacker's View



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

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

Two Separate Worlds

Software Security Assurance Summit

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

T.E.N. TECH EXEC NETWORKS

presented by

FORTIFY® An HP Company

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

Efficiency in Testing

Complex injections
Password Strength requirements ?
Password aging ? History aging ?
Vulnerable REQUIREMENTS !

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

"Source Code Available" Testing

Blind SQL Injection
Additional functionality
Vulnerable REQUIREMENTS
Unknown Interconnections

The Bridge