INTRO TO ETHICAL HACKING

MIS 5211.701
Week 12
Site:
http://community.mis.temple.edu/mis5211sec701fall2018/

Tonight's Plan

- Sample Pen Test Reports
- Web Services

Example Pen Test Reports

- http://www.offensive-security.com/penetration-testing-sample-report.pdf
- http://resources.infosecinstitute.com/writing-penetration-testing-reports/
- http://www.niiconsulting.com/services/security-assessment/NII_Sample_PT_Report.pdf

Vocabulary

- XML – Structured data that can be exchanged between applications and platforms
- SOAP – messaging protocol for transporting information and instructions between applications (uses XML)
- WSDL – a standard method of describing web services and their specific capabilities (XML)
- UDDI – defines XML-based rules for building directories in which companies advertise themselves and their web services

More Vocabulary

- REST - Representational State Transfer – Describes a architectural framework for web applications that includes:
  - Client–server
  - Stateless
  - Cacheable
  - Layered system
  - Code on demand (optional)
  - Uniform interface
- WADL – Web Application Description Language (Replaces WSDL in REST Applications)

Still More Vocabulary

- JSON - JavaScript Object Notation
- WS-Security – An extension to SOAP to apply security to Web services. It is a member of the Web service specifications and was published by OASIS.
- SAML – Security Assertion Markup Language

Web Services

- From OWASP
  - At the simplest level, web services can be seen as a specialized web application that differs mainly at the presentation tier level. While web applications typically are HTML-based, web services are XML-based.
  - Web services are employed as building blocks used by other web applications using the so-called SOA model.
  - Web services typically present a public functional interface, callable in a programmatic fashion.

Web Services

- Web services, like other distributed applications, require protection at multiple levels:
  - SOAP messages that are sent on the wire should be delivered confidentially and without tampering
  - The server needs to be confident who it is talking to and what the clients are entitled to
  - The clients need to know that they are talking to the right server, and not a phishing site.
  - System message logs should contain sufficient information to reliably reconstruct the chain of events and track those back to the authenticated callers

Advantages

- Open, text-based standards
- Modular approach
- Inexpensive to implement (relatively)
- Reduce the cost of enterprise application integration
- Incremental implementation

XML

- Developed from Standard Generalized Markup Method (SGML)
- XML widely supported by W3C
- Essential characteristic is the separation of content from presentation
- XML describes only data
- Any application that understands XML can exchange data

XML

- XML parser checks syntax
- If syntax is good the document is *well-formed*
- XML document can optionally reference a *Document Type Definition (DTD),* also called a *Schema*
- If an XML document adheres to the structure of the schema it is *valid*

SOAP

- SOAP – Simple Object Access Protocol
- SOAP enables between distributed systems
- SOAP message has three parts
  - *envelope* – wraps entire message and contains header and body
  - *header* – optional element with additional info such as security or routing
  - *body* – application-specific data being communicated

WSDL

- WSDL – Web Services Description Language
- Web services are self-describing
- Description is written in WSDL, an XML-based language through which a web service conveys to applications the methods that the service provides and how those methods are accessed
- WSDL is meant to be read by applications (not humans)

UDDI

- UDDI – Universal Description, Discovery, and Integration
- UDDI defines an XML-based format that describes electronic capabilities and business processes
- Entries are stored in a UDDI registry
- UDDI Business Registry (UBR)
  - "white pages" – contact info, description
  - "yellow pages" – classification info, details
  - "green pages" – technical data
  - uddi.microsoft.com

REST

- REST – Representational State Transfer
- SOAP is a heavy weight protocol
- REST uses simple HTML operations GET, PUT, POST, DELETE for carrying out web operations/activity
- It is an architectural style not a protocol
- REST has become the favored style for web services to communicate
- REST-based APIs provided by many applications

WADL

- WADL – Web Application Description Language
- WADL models the resources provided by a service and the relationships between them.
- WADL is intended to simplify the reuse of web services that are based on the existing HTTP architecture of the Web.
- WADL is platform and language independent and aims to promote reuse of applications beyond the basic use in a web browser.

JSON

- JSON - An open standard format that uses human-readable text to transmit data objects consisting of attribute–value pairs. Used primarily to transmit data between a server and web application, as an alternative to XML.

WS-Security

- WS-Security describes three main mechanisms:
  - How to sign SOAP messages to assure integrity. Signed messages also provide non-repudiation.
  - How to encrypt SOAP messages to assure confidentiality.
  - How to attach security tokens to ascertain the sender's identity.
- The specification allows a variety of signature formats, encryption algorithms and multiple trust domains, and is open to various security token models, such as:
  - X.509 certificates
  - Kerberos tickets
  - UserID/Password credentials
  - SAML Assertions
  - Custom-defined tokens.

SAML

- XML-based open standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider.
- SAML is a product of the OASIS Security Services Technical Committee.
- Even with this, best practice is to only transmit inside of an SSL protected channel

Why is this Important

- Web services are built to be reusable
- As a result, they typically make a lot of data available, more then the specific application they support needs
- Often, but not always, this means an attacker can gather data that was not intended to be made available
- Also, developers creating later applications may include similar data in their applications believing it's OK because why else would it have been provided

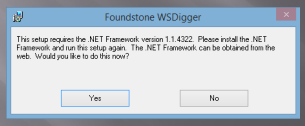
Where Do We Start

- WSDigger - WSDigger is a free open source tool designed by McAfee Foundstone to automate black-box web services security testing.
- Version one of this framework contains sample attack plug-ins for SQL injection, cross site scripting and XPATH injection attacks.
- A web service vulnerable to XPATH injection is provided as an example with the tool.

http://www.mcafee.com/us/downloads/free-tools/wsdigger.aspx

Where to get WSDigger

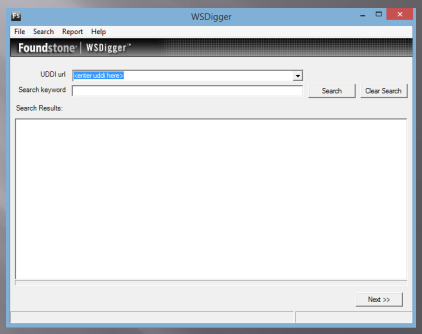
- Available at:
- http://www.mcafee.com/us/downloads/free-tools/wsdigger.aspx
- After launching you will likely get this



More on Installing

- You will need to do a search. This is an old package.
- Use for testing, but delete afterwards

Eventually



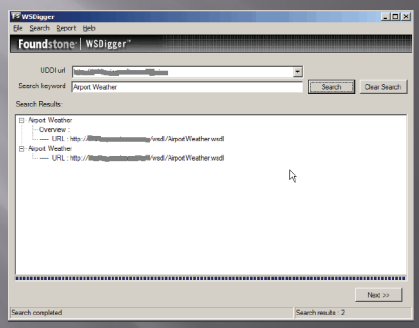
Uses for WSDigger

- Tool covers the following:
  - Service Discovery
  - Attack Vector Discovery
  - Exploit Testing
  - Analysis

Examples from Foundstone

- Target public UDDI from drop down
- Target private UDDI by typing over public
- Then search

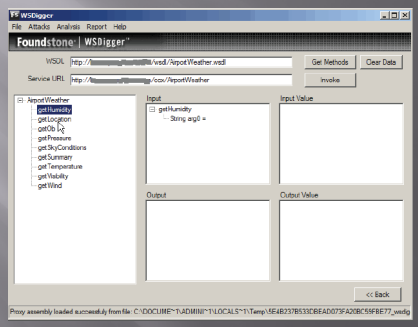
Examples from Foundstone



Examples from Foundstone

- Previous capture shows list of WSDLs
- Pick one and explore

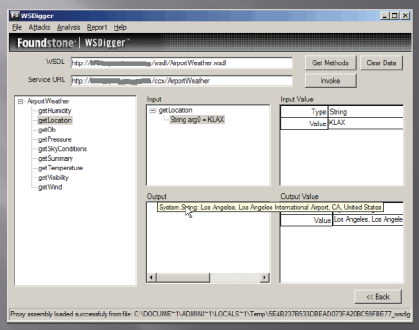
Examples from Foundstone



Examples from Foundstone

- Then, similar to Intercepting Proxies, we can enter or own values
- In the following example "KLAX"

Examples from Foundstone



Final Notes on WSDigger

- Obviously, only target systems you own or have permission
- These examples came out of the Foundstone documentation
- Documentation is included with the download

Alternatives

- Burp Suite has it's own plug in for Web Services via Burp Extender in the Pro version
  - See: http://portswigger.net/burp/extender/
  - And
  - https://pro.portswigger.net/bappstore/ShowBappDetails.aspx?uuid=ef2f3f1a593d417987bb2ddded760aee

More Alternatives

- WebScarab also has Web Services Functionality
- WebScarab replaced by ZED Attack Proxy
- Please note: Download only from owasp.org if you want to play with either. Lots of "Free" software sites offering copies that are likely malware.

More Alternatives

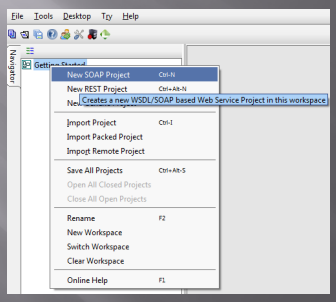
- Microsoft has a "Web Performance Test Editor" in Visual Studio
- Directions for use are here: http://msdn.microsoft.com/en-us/library/ms182557.aspx

Visual Studio is available from the software repository

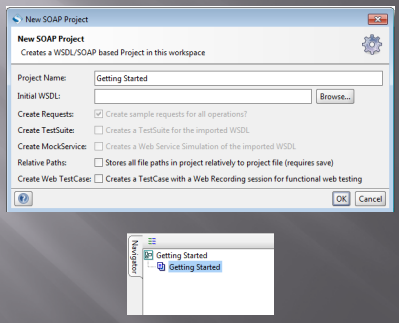
More Alternatives

- SOAPUI
  - Supports SOAP and REST

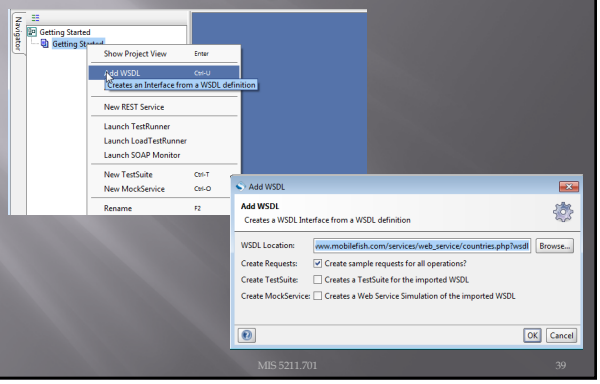
Using SOAPUI



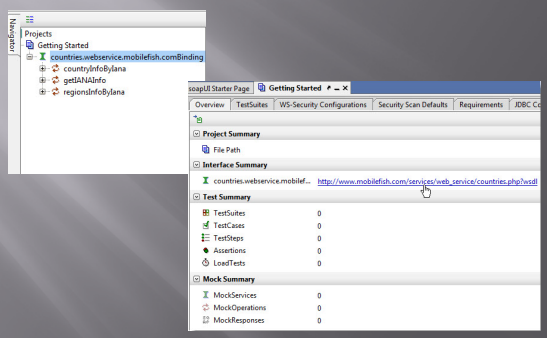
Using SOAPUI



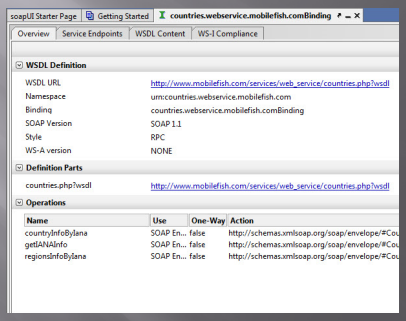
Adding a WSDL



Navigating



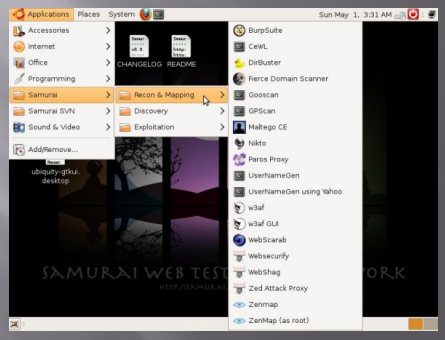
Eventually You Get Here



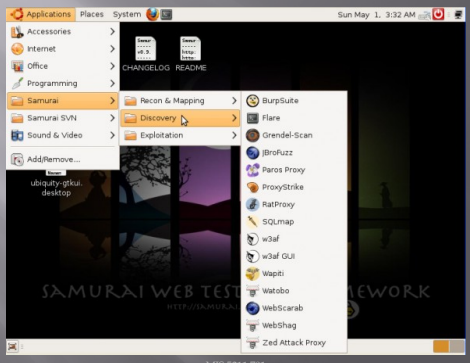
Final Option

- Samurai WTF (Web Testing Framework)
- Available Here: http://samurai-wtf.org/
- Similar to KALI, but focused entirely on Web Applications
- If you do want to play with it, remember the password for Samurai is "samurai".
- Asking this question in a help forum will garner a lot of abuse

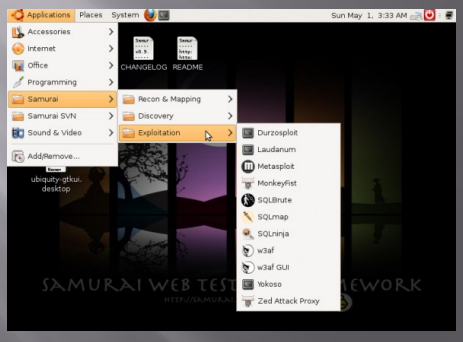
Samurai Features



Samurai Features

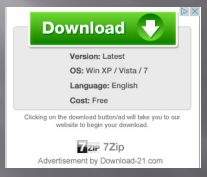


Samurai Features



Warning On Sourceforge

- DO NOT click on anything that looks like this!



- These are advertisers that are trying to trick you in to installing adware at best, or worse!

Interesting Item

- Kali is available via Amazon Web Services
- https://aws.amazon.com/marketplace/pp/B01M26MMTT
- Free for up to 750 hrs/month for first year after signup
- As low as $.02/hr with a paid account

Next Week

- Evasion
- Odds and Ends

Questions

?