Web server reconnaissance
Reconnaissance and fingerprinting

- Finding information about a target web server/web site
  - May be illegal to perform reconnaissance on a web server and web site without prior approval/permission.
  - Simulate via war games to demonstrate issues with trusting clients with URLs and filenames
- Fingerprinting information
  - Name and version of server
  - Database backend
  - Use of reverse proxy (nginx)
  - Programming language and web application server
Viewing HTTP headers

$ nc vulnerable 80
GET / HTTP/1.1
Host: vulnerable

HTTP/1.1 200 OK
Date: Sun, 03 Mar 2013 10:56:20 GMT
Server: Apache/2.2.16 (Debian)
X-Powered-By: PHP/5.3.3-7+squeeze14
Content-Length: 6988
Content-Type: text/html

$ nc oregonctf.org 80
HEAD / HTTP/1.1
Host: foobar

$ nc cs410.oregonctf.org 80
HEAD / HTTP/1.1
Host: cs410.oregonctf.org
Viewing source content

- Look for comments, links, or directory structure

- Wikipedia (en.wikipedia.org)

- Mercedes-Benz (www.mercedes-benz.com/en)
Viewing source content

- **Hyatt.com**

```html
<div class="menu">
<ul>
<li><a href="/hyatt/reservations/reservation.jsp">My Reservations</a></li>
<li><a href="/hyatt/specials/offers-landing.jsp">Offers</a></li>
<li><a href="/hyatt/meetings/index.jsp">Meetings &amp; Events</a></li>
<li><a href="/hyatt/about/index.jsp">About Us</a></li>
</ul>
</div>
```

- **GitHub**
  - **Hint: Asset cache busting pipeline**

```html
<link crossorigin="anonymous" href="https://assets-cdn.github.com/assets/frameworks-4242846376d46c90f210115e62415cbb46cdaaf46291ec9fff638250c75f1ce30.css" integrity="sha256-QkKEYzbjDyEBFeAkFc0DNr0YPs9n/9jglDUXzja=" media="all" rel="stylesheet"/>

<link crossorigin="anonymous" href="https://assets-cdn.github.com/assets/github-9077fcc535b78561667f9bddd5347613c61c84be261b295fd421da92d8b25c6e.css" integrity="sha256-kHfBxTW3hWFMf5vdXTR2E8AcjGy1fRCHekiyXGd=" media="all" rel="stylesheet"/>
```
Viewing source content

- Blackboard
  
  <li><a href="/mobile-learning/index.aspx" target="_self" title="Mobile Learning">Mobile Learning</a></li>
  <li><a href="/moodlerooms.aspx" target="_self" title="Open Source Learning">Open Source Learning</a></li>
  <li><a href="/education-analytics/index.aspx" target="_self" title="Education Analytics">Education Analytics</a></li>
  <li><a href="/campus-access-card/cashless-campus.aspx" target="_self" title="Cashless Campus">Cashless Campus</a></li>
  <li><a href="/higher-education/marketing-and-recruiting-services/student-recruitment.aspx" target="_self" title="Student Recruitment">Student Recruitment</a></li>
Search engine signals

• Google, Yahoo, Bing, will crawl everything on your site unless you tell them otherwise.
  • Prevent via use of **robots.txt** file
  • Instructs search engine spiders how to interact with your content.
  • Can also reveal sensitive information
Search engine signals

- For hacker, robots.txt can contain interesting folders, files, and data to investigate.
  - Sometimes even passwords, usernames, ...
- Example
  - Specifies that no robots should visit any URL starting with "/cyberworld/map/" or "/tmp/", or /foo.html.

```plaintext
# robots.txt for http://www.example.com/
User-agent: *
Disallow: /cyberworld/map/ # This is an infinite virtual URL space
Disallow: /tmp/ # these will soon disappear
Disallow: /foo.html
```
# If the Joomla site is installed within a folder such as at
# e.g. www.example.com/joomla/ the robots.txt file MUST be
# moved to the site root at e.g. www.example.com/robots.txt
# AND the joomla folder name MUST be prefixed to the disallowed
# path, e.g. the Disallow rule for the /administrator/ folder
# MUST be changed to read Disallow: /joomla/administrator/
#
# For more information about the robots.txt standard, see:
# http://www.robotstxt.org/orig.html
#
# For syntax checking, see:
# http://tool.motoricerca.info/robots-checker.phtml

User-agent: *
Disallow: /administrator/
Disallow: /cache/
Disallow: /cli/
Disallow: /components/
Disallow: /images/
Disallow: /includes/
Disallow: /installation/
Disallow: /language/
Disallow: /libraries/
Disallow: /logs/
Disallow: /media/
Disallow: /modules/
Disallow: /plugins/
Disallow: /templates/
Disallow: /tmp/
Artifacts

- favicon.ico
  - Default icons indicate software package being used
  - Which package?

- Search-engine worms (Santy worm 2004)
  - phpBB
Fuzzing

- Brute-force common directory names
  - (e.g. admin, config, conf, src)
  - Brute-force admin pages with default admin credentials
- `wfuzz` tool
  - Detect directories and pages on the web server using wordlists of common resource names.

```
$ wfuzz -c -z file,wordlist/general/common.txt --hc 404 http://vulnerable/FUZZ
```
Examine error pages

- Application-specific 404 pages
  - Tomcat

HTTP Status 404 - /randomlongstring

Status report
Message /randomlongstring
Description The requested resource (/randomlongstring) is not available.

Apache Tomcat/6.0.35

- Ruby on Rails

The page you were looking for doesn’t exist.
You may have mistyped the address or the page may have moved.
Generate specific errors

- Stack trace of web application
- Inject %00, %22, %27 to check for injection vulnerabilities

---

HTTP Status 500

Description: The server encountered an internal error () that prevented it from fulfilling this request.

```
org.apache.jasper.JasperException: The absolute uri: http://java.sun.com/jsp/jstl/functions cannot be resolved in either web.xml or the jar files de;
  org.apache.jasper.compiler.DefaultErrorHandler.jspError(DefaultValueHandler.java:51)
  org.apache.jasper.compiler.ErrorDispatcher.dispatch(ErrorDispatcher.java:409)
  org.apache.jasper.compiler.ErrorDispatcher.jspError(ErrorDispatcher.java:116)
  org.apache.jasper.compiler.TagLibraryInfoImpl.generateTLDLocation(TagLibraryInfoImpl.java:316)
  org.apache.jasper.compiler.TagLibraryInfoImpl.<init>(TagLibraryInfoImpl.java:149)
  org.apache.jasper.compiler.Parser.parseTaglibDirective(Parser.java:386)
  org.apache.jasper.compiler.Parser.parseElements(Parser.java:1397)
  org.apache.jasper.compiler.Parser.parse(Parser.java:120)
  org.apache.jasper.compiler.ParserController.doParse(ParserController.java:255)
  org.apache.jasper.compiler.Compiler.parse(Compiler.java:103)
  org.apache.jasper.compiler.Compiler.generateJava(Compiler.java:185)
  org.apache.jasper.compiler.Compiler.compile(Compiler.java:354)
  org.apache.jasper.compiler.Compiler.compile(Compiler.java:334)
  org.apache.jasper.compiler.Compiler.compile(Compiler.java:321)
  org.apache.jasper.JspCompilationContext.compile(JspCompilationContext.java:592)
  org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:328)
  org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:313)
  org.apache.jasper.servlet.JspServlet.service(JspServlet.java:260)
  javax.servlet.http.HttpServlet.service(HttpServlet.java:717)
```

Note: The full stack trace of the root cause is available in the Apache Tomcat/6.0.35 logs.

Apache Tomcat/6.0.35