Identifying Web Servers

"A first-look into Web Server Fingerprinting."
Send the same HTTP Request and get different Responses

Perform a single or standard set of HTTP request towards a web server. The varied differences in the responses will allow for accurate fingerprinting.
Why Fingerprint?

- Determine the specific version and possibly service pack installed.
- Determine the configuration settings.
- Develop countermeasures to fingerprinting.

“If ignorant both of your enemy and yourself, you are certain to be in peril. “

Sun Tzu – "Art of war"
## The Common Web Servers

<table>
<thead>
<tr>
<th>Developer</th>
<th>July 2002</th>
<th>Percent</th>
<th>August 2002</th>
<th>Percent</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache</td>
<td>21453498</td>
<td>57.62</td>
<td>22859123</td>
<td>63.51</td>
<td>5.89</td>
</tr>
<tr>
<td>Microsoft</td>
<td>11866718</td>
<td>31.87</td>
<td>9139785</td>
<td>25.39</td>
<td>-6.48</td>
</tr>
<tr>
<td>Zeus</td>
<td>787071</td>
<td>2.11</td>
<td>765115</td>
<td>2.13</td>
<td>0.02</td>
</tr>
<tr>
<td>iPlanet</td>
<td>494567</td>
<td>1.33</td>
<td>486868</td>
<td>1.35</td>
<td>0.02</td>
</tr>
</tbody>
</table>
The Server Banner

HEAD / HTTP/1.1
Host: www.host.com

Server: Apache/1.3.26 (Unix)
Server: Microsoft-IIS/5.0
Server: Netscape-Enterprise/4.1
WhiteHat Banner Grabber

$ wh_banner.pl http://host.com

Server: Apache/1.3.26 (Unix)

“Know your enemy and know yourself and you can fight a hundred battles without disaster.”

Sun Tzu – "Art of war"
HTTP/1.1 RFC 2616

http://www.ietf.org/rfc/rfc2616.txt
Apache with no Server Banner

"...paranoid so you don't have to be"
Apache with no Server Banner

[jeremiah@localhost jeremiah]$ telnet www.wiretrip.net 80
Trying 66.21.117.200...
Connected to www.wiretrip.net.
Escape character is `^]`.
OPTIONS * HTTP/1.1
Host: www.wiretrip.net

HTTP/1.1 200 OK
Date: Thu, 12 Sep 2002 01:55:09 GMT
Content-Length: 0
Allow: GET, HEAD, OPTIONS, TRACE
OPTIONS *

HTTP Request:
OPTIONS * HTTP/1.1
Host: www.host.com

HTTP Response:
Allow: GET, HEAD, POST
Apache 1.3.x

```
[jeremiah@localhost jeremiah]$ telnet www.netcraft.com 80
Trying 195.92.95.5...
Escape character is "^]".
OPTIONS * HTTP/1.1
Host: www.netcraft.com

HTTP/1.1 200 OK
Date: Thu, 12 Sep 2002 01:49:01 GMT
Server: Apache/1.3.26 (Unix) mod_perl/1.27
Content-Length: 0
Allow: GET, HEAD, OPTIONS, TRACE
Connection: close
```
Apache 1.3.x
Welcome!

The Apache Software Foundation provides support for the Apache community of open-source software projects. The Apache projects are characterized by a collaborative, consensus based development process, an open and pragmatic software license, and a desire to create high quality software that leads the way in its field. We consider ourselves not simply a group of projects sharing a server, but rather a community of developers and users.

You are invited to participate in The Apache Software Foundation. We welcome contributions in many forms. Our membership consists of those individuals who have demonstrated a commitment to collaborative open-source software development through sustained participation and contributions within the Foundation's projects.

Apache News by Email

If you would like to keep up with news and announcements from the foundation and all its projects, you can subscribe to the new Apache Announcements List.

Featured Projects

Below we feature a few of the many Apache projects.

Apache FOP

http://xml.apache.org/fop/

As part of the Apache XML Project, Apache FOP (Formatting Objects Processor) is the middle-ware component driving the XSLT tool kit.
Apache 2.0.x

[jeremiah@localhost jeremiah]$ telnet www.apache.org 80
Trying 63.251.56.142...
Connected to www.apache.org.
Escape character is "^]".
OPTIONS * HTTP/1.1
Host: www.apache.org

HTTP/1.1 200 OK
Date: Thu, 12 Sep 2002 01:11:24 GMT
Server: Apache/2.0.41-dev (Unix)
Cache-Control: max-age=86400
Expires: Fri, 13 Sep 2002 01:11:24 GMT
Allow: GET,HEAD,POST,OPTIONS,TRACE
Content-Length: 0
Content-Type: text/plain
Microsoft IIS 4.0

[jeremiah@localhost jeremiah]$ telnet www8.compaq.com 80
Trying 161.114.19.218...
Connected to www8.compaq.com.
Escape character is `^]`.
OPTIONS * HTTP/1.1
Host: www8.compaq.com

HTTP/1.1 200 OK
Server: Microsoft-IIS/4.0
Date: Thu, 12 Sep 2002 02:11:12 GMT
Public: OPTIONS, TRACE, GET, HEAD, POST, PUT, DELETE
Content-Length: 0
Microsoft IIS 5.0/6.0

[jeremiah@localhost jeremiah]# telnet www.dell.com 80
Trying 143.166.83.63...
Escape character is `^]`.
OPTIONS * HTTP/1.1
Host: www.dell.com

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Thu, 12 Sep 2002 02:02:24 GMT
P3P: CP="BUS CAO CNT COM CUR DEV DSP INT NAV OUR PSA PSD SAM STA TAI UNI"
PICS-Label: (pics-1.1 "http://www.icra.org/ratingsv02.html" 1 r (cb 1 lz 1 nz 1 oz 1 vz 1) "http://www.rsac.org/ratingsv01.html" 1 r (n 0 s 0 v 0 i 0))
P3P: policyref="http://www.dell.com/w3c/p3p.xml", CP="BUS CAO CNT COM CUR DEV DSP INT NAV OUR PSA PSD SAM STA TAI UNI"
Expires: Thu, 01 Dec 1994 8:00:00 GMT
Set-Cookie: SITESERVER=ID=538382e81a644ec3b74519d300cf567d; domain=.dell.com; path=/; expires=Wed, 12-Sep-2007 02:02:24 GMT;
Set-Cookie: SITESERVER_SESSION=ID=538382e81a644ec3b74519d300cf567d; domain=.dell.com; path=/
Content-Length: 0
Accept-Ranges: bytes
DAVL: <DAV:sql>
DAV: 1, 2
Public: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
Allow: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
Cache-Control: private
Oracle 9i

Customers: McData Saves US$1 Million in First Year With Oracle
- Technology: McData Streamlines Growth From US$100-million to US$300-million
- Banking: Wells Fargo Sees Business Data 400% Faster
- Automotive: Vector SCM Saves US$1.5 Million with Oracle9i Real Application Clusters

Database: Linux Powered and Enterprise Ready
- Unbreakable Linux: New Clustering Capabilities Mean Mainframe Quality at Lower Prices
- Grow Your Small to Mid-Sized Business: Deploy Oracle9i Database on Windows and Linux
- Performance: Oracle Sets New World Records--Faster With Half the Processors

Application Server: Oracle #1 in ECperf Benchmarks
- Performance: Run Java Faster
- Enterprise Application Integration: Consolidate All Your Applications in Just Four Weeks
- Toplink: Download the #1 Java-to-Relational Persistence Software--Free

Collaboration Suite: Improve Your Outlook
- Email: Keep Your Microsoft Outlook Email--But Make It Unbreakable
- Files: Consolidate Your File Servers and Save
- Wireless & Voice: Be More Productive with Wireless & Voice Access to Messages, Files, and

E-Business Suite: Complete. Manage By Fact With Oracle and Fr...
Oracle 9i
iPlanet 3.6

[jeremiah@localhost jeremiah]$ telnet central.sun.net 80
Trying 192.18.97.198...
Connected to central.sun.net.
Escape character is "^]".
OPTIONS * HTTP/1.1
Host: central.sun.net

HTTP/1.1 200 OK
Server: Netscape-Enterprise/3.6 SP2
Date: Thu, 12 Sep 2002 02:22:43 GMT
Content-length: 0
Public: HEAD, GET, PUT, POST
iPlanet 4.0
iPlanet 4.1

[jeremiah@localhost jeremiah]$ telnet www.sun.com 80
Trying 64.124.140.181...
Escape character is "^]".
OPTIONS * HTTP/1.1
Host: www.sun.com

HTTP/1.1 200 OK
Server: Netscape-Enterprise/4.1
Date: Thu, 12 Sep 2002 01:08:21 GMT
Allow: HEAD, GET, PUT, POST, DELETE, TRACE, OPTIONS, MOVE, INDEX, MKDIR, RMDIR
Content-length: 0
iPlanet 6.0

```
[jeremiah@localhost jeremiah]$ telnet www.iplanet.com 80
Trying 128.11.159.93...
Escape character is '^]'.
OPTIONS * HTTP/1.1
Host: www.iplanet.com

HTTP/1.1 200 OK
Server: Netscape-Enterprise/6.0
Date: Thu, 12 Sep 2002 01:19:05 GMT
Allow: HEAD, GET, PUT, POST, DELETE, TRACE, OPTIONS, MOVE, INDEX, MKDIR, RMDIR
Content-length: 0
```
We've Moved!

On March 17, 2002, Sun officially concluded its original Alliance agreement with AOL. iPlanet is now a division of Sun and is a core component of the Sun Open Net Environment (Sun ONE). We retain the intellectual property rights for all of the products and the product engineering and support organizations are now fully staffed by Sun employees. Visit us at sun.com/software.

Find Sun ONE Software (formerly iPlanet)
Application/Integration Servers & Messaging Software
Directory Servers/Identity Management Software
Internet Software
E-Mail, Calendar, & Collaboration Software
Portal Servers
Web Servers

Now's a good time to update your bookmarks!

Evaluate
Product Info
Trial Downloads
Case Studies
White Papers
Solutions

Get
Get the Software
Partners
Training
Contact Sales: 1-888-786-8111

Use
Documentation
Sun Software Forum

Maintain
Support
Services
OPTIONS Results

Server: Apache/1.3.26 (Unix)
Allow: GET, HEAD, OPTIONS, TRACE

Server: Apache/2.0.41-dev (Unix)
Allow: GET,HEAD,POST,OPTIONS,TRACE

Server: Microsoft-IIS/4.0
Public: OPTIONS, TRACE, GET, HEAD, POST, PUT, DELETE

Server: Microsoft-IIS/5.0
Public: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
Allow: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH

Allow: GET, HEAD, OPTIONS, TRACE
Server: Oracle9iAS/9.0.2 Oracle HTTP Server Oracle9iAS-Web-Cache/9.0.2.0.0 (N)

Server: Netscape-Enterprise/3.6 SP2
Public: HEAD, GET, PUT, POST

Server: Netscape-Enterprise/4.0
Allow: HEAD, GET, PUT, POST

Server: Netscape-Enterprise/4.1
Allow: HEAD, GET, PUT, POST, DELETE, TRACE, OPTIONS, MOVE, INDEX, MKDIR, RMDIR

Server: Netscape-Enterprise/6.0
Allow: HEAD, GET, PUT, POST, DELETE, TRACE, OPTIONS, MOVE, INDEX, MKDIR, RMDIR
Adequate Entropy

The results from the sampling of HTTP output using only “OPTIONS *” provided enough data to start fingerprinting.
OPTIONS * Conclusions

If the server allows and supports the “OPTIONS” HTTP Request Method, then with a reasonable level of certainty, we can conclude what the major version number is for a popular web server.

The “Server” response header is no longer necessary to determine what a web server is running.
Tell Apache Apart

The Major Versions:

Server: Apache/1.3.26 (Unix)
Allow: GET, HEAD, OPTIONS, TRACE

Server: Apache/2.0.41-dev (Unix)
Allow: GET, HEAD, POST, OPTIONS, TRACE
Tell IIS Apart

Server: Microsoft-IIS/4.0
Public: OPTIONS, TRACE, GET, HEAD, POST, PUT, DELETE

Server: Microsoft-IIS/5.0
Public: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
Allow: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
Tell iPlanet Apart

Server: Netscape-Enterprise/4.0
Allow: HEAD, GET, PUT, POST

Server: Netscape-Enterprise/4.1
Allow: HEAD, GET, PUT, POST, DELETE, TRACE, OPTIONS, MOVE, INDEX, MKDIR, RMDIR

Server: Netscape-Enterprise/6.0
Allow: HEAD, GET, PUT, POST, DELETE, TRACE, OPTIONS, MOVE, INDEX, MKDIR, RMDIR
The Research is not complete!

Apache Version identifiers are not consistent

RedHat Apache, Apache Stronghold and other have no exhibited the same behavior as a standard Apache distribution has.
Fingerprinting Countermeasures

Microsoft Internet Information Server (IIS)
- URL Scan
- IIS Lockdown
- SecureIIS

Apache
- Mod_Rewrite
- http.conf Configurations
- Source code modifications