SANS Institute
InfoSec Reading Room

Security Strengths and Weaknesses of Two Popular Web Servers

As the mediator between your business and the world the Web Server that you choose must be completely sound in regards to security. You do have many options when choosing which Web Server package you will use to transmit your company's on-line presence to the rest of the world. There are two Web Server packages in particular that dominate the market for Web Servers. These two Web Server packages are Microsoft's Internet Information Server, and Apache.

Brad Bell
August 19, 2001

Security Strengths and Weaknesses of Two Popular Web Servers

As the mediator between your business and the world the Web Server that you choose must be completely sound in regards to security. You do have many options when choosing which Web Server package you will use to transmit your company's on-line presence to the rest of the world. There are two Web Server packages in particular that dominate the market for Web Servers. These two Web Server packages are Microsoft's Internet Information Server, and Apache.

What is a Web Server?

The definition and purpose of a web server is a software package that serves either static content to a Web browser at a basic level, or dynamic content that require end-user interaction. For example, a web server may receive a request for a Web page such as www.amazon.com/index.html. The Web Server would then map the Uniform Resource Locator (URL) to a local file on the host server. In this case the file, index.html is somewhere on the host file system. The server then loads this file from disk and serves it out across the network to the user's Web browser. The browser and the server are talking to each other using Hypertext Transfer Protocol (HTTP) which controls this entire exchange.

How does a Web Server transmit dynamic content?

Web Servers don't just send static documents and files across the network they also transmit dynamic content. This could be done through web pages created in response to a user input, which is done directly or indirectly by the user. An example of the user directly influencing the output of a web page could be through the use of on-page forms backed by some sort of executable program or code. Also, an example of a user indirectly influencing the results of a web page may be through the use of "cookies." Cookies are short pieces of data used by Web Servers to help identify web users.

Common Gateway Interface (CGI), and JavaScript for Dynamic Content

With CGI an end-user can visit your site and perform specified tasks with the CGI programs you have. The Common Gateway Interface (CGI) is a frequently used technique of interfacing external applications with Web Servers. A standard HTML document that a Web Server retrieves is static and will never change. However, with a CGI program the Web Server will send the results for the web page upon receipt of the criteria for the page. This allows for the output of dynamic information. For example, let's say that you wanted to connect your Stamp Collection database to the Internet, to allow people from all over the world to look through it based upon whatever criteria they set. Basically, you need to create a CGI program that the Web Server will execute to transmit information to the database software, and receive the results back again and provide them to the end-user. A CGI program can be written in several languages such as Visual Basic, PERL, or C++ that allows it to be executed on the system. CGI programs are one way of making Internet content dynamic, but there are other methods of doing this. For example, simply adding a few lines of JavaScript code to an HTML file will make the web page very dynamic. The JavaScript could all be within the HTML thus making the program execute on the host side rather than the server. An example of some JavaScript would be a program that pulls the local date of the user machine and

displays it on the user's screen. Here is the code for such a program:

```
<SCRIPT LANGUAGE="JavaScript">
function displaydatetime() {
if (!document.layers && !document.all)        return;
var today;
var timeLocal;
var timeUTC;
today = new Date();
timeLocal = today.toLocaleString() + " " + "Local"; //Convert to current locale.
timeUTC = today.toUTCString(); //Convert to UTC.
if (document.layers) {
document.layers.clockLocal.document.write(timeLocal);
document.layers.clockLocal.document.close();
document.layers.clockUTC.document.write(timeUTC);
document.layers.clockUTC.document.close();}
else if (document.all) {
clockLocal.innerHTML = timeLocal;
clockUTC.innerHTML = timeUTC;}
setTimeout("displaydatetime()", 500)
}
window.onload = displaydatetime;
// End -->
</script>
```

The above JavaScript would display the following results on your web browser:

08/02/2001 09:31:08 Local
Thu, 02 Aug 2001 14:31:08 UTC

Security Issues Related to Serving Information via Web Servers (Static and Dynamic content)

Serving data and information to people all over the world is a grand task. However when coupled with the related security issues and needs this task becomes monumental. Serving information over the internet securely was brought about with the introduction of Hypertext Transmission Protocol, Secure (HTTPS). This protocol allows for secure communication to go on between the browser and Web server. Basically this means that it is safe for a user and a server to transmit sensitive data to each other over what might be considered an insecure network. What either of the counterparts in this transmission does with the data is another story however.

More about HTTPS

The secure hypertext transfer protocol (HTTPS) is a communications protocol designed to transfer encrypted information between computers over the Internet. HTTPS is just HTTP using a Secure Socket Layer (SSL). A secure socket layer is an encryption protocol invoked on a Web Server that uses HTTPS. The main reasons for using HTTPS are online purchasing and the exchange of private information over the internet. An example of online purchasing would be something like

purchasing a best-selling novel on amazon.com. Also, an example of exchanging private information might be the transmission of the credit card number used to purchase the novel off amazon.com.

IIS vs. Apache
Given the current environment of the Internet and how Web Servers interact with end-users we can begin to compare how two popular Web Servers, Microsoft Internet Information Server and Apache, perform. Specifically we can compare these two Web Servers in regards to the security they provide, and the problems and incidents that have occurred with these Web Servers since they have been in production.

IIS
Microsoft's flagship Internet product, Internet Information Server, is useful as both a first time Web Server for those comfortable and familiar with Microsoft products and as a high-end Web Server for hosting a large e-commerce web site. Since the vast majority of computer users are accustomed to using Microsoft based products and the similar interfaces that exist on these applications it is not a surprise that many people choose to use Microsoft's IIS for their Web Server. This alone is not an adequate reason to choose IIS as your web server, but it definitely accounts for some of Microsoft's market share of Web Server sales.

The Wrong Reason to choose IIS
When asked why a company is using IIS as it's web server application many times the appropriate IT employee will answer one of the following responses:

"It came with the Operating System"
"We're a "Microsoft Shop. So we use MS products"
"We're not familiar with other options"
"Our consultants told us to use IIS"

These are all reasons or excuses you would expect to hear in any standard organization for choosing IIS. However, none of the reason listed above are strong enough to justify choosing the software that will run your Web Server. For a decision of this magnitude more research is necessary.

Weaknesses of IIS
One of the major weaknesses of using IIS as your web server is that being a Microsoft product IIS automatically becomes a target for the software hacking community. There are many hackers around the world who would love to terrorize any piece of software produced by Microsoft. The notoriety of the company basically puts a target on any of its products for hackers. The level of testing of the software is also questionable when you consider the number of patches and updates that have been released by Microsoft for IIS. This brings into doubt the quality of the product that was developed in the first place. With all of the money available to Microsoft for Research and Development it is very surprising that so many patches have been released for IIS. This makes one wonder if IIS was a rushed product quickly put out by Microsoft with the sole intention of fixing any problem they encountered later on down the road. In fact, if you take this view point it is easy to see IIS as more of a money making scheme rather than a polished piece of software developed

with pride.

IIS Code Red Virus

One example of an incident involving Microsoft's IIS web server was the Code Red virus that infiltrated systems all over the world in July and August of 2001. This virus worked by taking advantage of a ubiquitous software bug within IIS. The reason the Code Red virus worked was a buffer-overflow vulnerability in Microsoft's IIS web servers. This allowed system-level execution of code and thus presented a major security weakness. The virus ignored all physical and political boundaries and quickly spread all over the world. Luckily there was no real harm done from the virus. Its main purpose was to perform a denial of service attack on www.whitehouse.gov. The virus attacked based upon the IP address of the White House serve so the Denial of Service attack was easily fixed. This is just one example of how a web server can be vulnerable without the proper configurations or updates installed. Had the hacker's decided to they could have created much more havoc with this virus.

Reasons why companies are using IIS

When making a decision of this nature the person responsible should choose IIS as their Web Server package for the appropriate reasons. Many organizations and businesses do in fact choose IIS as their Web Server, and are very satisfied with the results that they have seen. A reason for this is the fact that many people are familiar with the Microsoft style graphical user interface, and can easily apply this to using and learning IIS. In fact, this interface can even remove the need for companies to hire expert help thus saving them money. Another reason why IIS would be a good choice is the fact that Microsoft offers downloadable tools to ensure that all of the latest software updates and patches are installed on your Web Server. Microsoft has also made available an IIS Security Configuration tool that will ease the process of securing any Web Server running off IIS. Additionally, with all of the security patches that Microsoft has released recently should cause more relief than concern. This is because with each additional security patch IIS becomes that much more "secure" as a product. In theory as these patches and updates are released the number of vulnerabilities should decrease.

Apache

Apache is a powerful, flexible web server that implements the latest protocols, including HTTP/1.1. Apache is highly configurable and extensible with third-party modules, and the custom modules that can be created using the Apache module API. Apache also functions on every major computer platform in existence including Windows NT/9x, Netware 5.x, OS/2, and most versions of Unix, as well as several other operating systems.

How did Apache come about?

Apache was first developed as a result of the National Center for Supercomputing Applications httpd project. Today Apache is one of the most functional and efficient web servers in existence. The name Apache is not a tribute to the native people of North America, but rather a direct representation of how the software was developed. The software was first known as "A PatCHy server" because it was based on some existing code and a series of patch files. There are some developers out there however who prefer to believe that the software was named Apache because of the superior skills in warfare strategy and inexhaustible endurance of the Apache Indian tribe of North America.

Weaknesses of Apache

Even with all of the strengths of Apache it is not the web server for all users. Setup of the server is performed through a command-line interface. Typical Microsoft users will have trouble navigating this interface. Apache does not have the user-friendly tools you would expect to see in a Microsoft product like Wizards, or other visuals. For some developers this is advantageous, but for others it can translate into expensive deployment and maintenance costs. Also, the technical support given through newsgroups may not be adequate for many users. You could imagine the scenario of an inexperienced user who is accustomed to graphical user interfaces trying to setup Apache as their web server with a command-line interface and hardly any technical help. It would be nearly impossible for this user to get the server up and running, and even if they did it definitely would not be configured correctly.

Strengths of Apache

One of the primary reasons people begin using Apache in the first place is the fact that it is a free and open-source product. All of the source code for Apache is freely distributed to any person or organization that wants it along with an unrestrictive license. The Apache Group also strongly encourages user feedback through new ideas, bug reports and patches. Apache's overall security performance is unquestionable. This is obvious when you consider the fact that many of the most accessed web sites in the world run Apache or Apache variants. The public distribution of the source code results in quick distribution of patches and updates for the software. This public scrutiny also ensures that any security hole is truly fixed according to the differing viewpoints of anyone investigating the software's security issue. As a result of this Apache's large base of users have ensured that its developers have created a package that is extremely stable and secure. Apache users also have the benefit of accessing technical support via Usenet newsgroups from anywhere in the world.

Conclusion

When it comes to deciding on which web server is right for your organization there is no clear-cut answer. Your basis for making this decision could be based upon many different sets of criteria. For instance you may choose Apache because it's free, or you may choose Microsoft's IIS because you have a large amount of faith in Microsoft products and their technical support. These are both good reason to choose a web server. No matter which web server you choose you must do several things in order to ensure that you have the security your organization needs. Any web server software package must be setup properly for the needs of your business. You must also continuously make certain that you have all of the most current updates and patches installed to defend against any security weakness that has been discovered within your web server of choice. Also, as incidents occur around the world you must have a designated employee or set of employees who stays in tune with all of this to make sure that your business will be safe and unaffected by any newly found security weakness. Both Microsoft's IIS and Apache can be secure if the proper configuration is done. Many of the weaknesses in IIS and Apache are from features in the software that are useful for one reason or another but they may present a security weakness if not configured properly. You would be well served by both of these web servers, but you must educate yourself and take the necessary precautions with either web server to ensure that your organization is safe and secure.

Bibliography

Honeycutt, Jerry. "Microsoft IIS: safe or sorry?." 29 Jan. 2001.
URL: http://enterprise.cnet.com/enterprise/0-9566-7-4561136.html (19 Aug. 2001).

Madigan, Andrew. "LINUX / Apache versus Windows NT / IIS."
URL: http://homepage.tinet.ie/~designmad/Linux-v-NT.htm (19 Aug. 2001).

Meloni, Julie. " Apache 1.3.14 - CNET Linux Center - CNET.com." 18 Jan. 2001.
URL: http://linux.cnet.com/linux/0-2136889-7-4513044.html?tag=st.it.9566-7-4561136.pptxt.2136889-7-4513044 (19 Aug. 2001).

Moore, David. "CAIDA Analysis of Code-Red" 24 July 2001.
URL: http://www.caida.org/analysis/security/code-red/ (19 Aug. 2001).

Park, Barry. "IIS leaves cracker's door wide open." 02 May 2001.
URL: http://it.mycareer.com.au/breaking/20010502/A39778-2001May2.html (19 Aug. 2001).

Sol, Selena. "Secured Transmission (SSL, HTTPS)." 20 Sep. 2001.
URL: http://www.wdvl.com/Authoring/Tools/Tutorial/secure.html (19 Aug. 2001).

Steinberger, Ric. "IIS: Time to Just Say No." 21 May 2001.
URL: http://securityportal.com/articles/iis20010521.html (19 Aug. 2001).

Viejo, Aliso. "Exploit Puts Pressure On For IIS Web Server Patch." 04 May 2001.
URL: http://www.newsbytes.com/news/01/165322.html (19 Aug. 2001).

Wittmann, Art. "Who's the Best?." 18 Oct. 1999.
URL: http://www.networkcomputing.com/1021/1021colwittmann.html (19 Aug. 2001).

"CGI City - One of the biggest WWW Resources for CGI and Perl materials."
URL: http://www.icthus.net/CGI-City/ (19 Aug. 2001).

"JavaScript.com (TM) - The Definitive JavaScript Resource: JavaScript Tutorials and Free Java Scripts."
URL: http://www.javascript.com/ (19 Aug. 2001).

Last Updated: July 20th, 2018

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Riyadh July 2018	Riyadh, SA	Jul 28, 2018 - Aug 02, 2018	Live Event
SANS Pittsburgh 2018	Pittsburgh, PAUS	Jul 30, 2018 - Aug 04, 2018	Live Event
Security Operations Summit & Training 2018	New Orleans, LAUS	Jul 30, 2018 - Aug 06, 2018	Live Event
SANS Hyderabad 2018	Hyderabad, IN	Aug 06, 2018 - Aug 11, 2018	Live Event
Security Awareness Summit & Training 2018	Charleston, SCUS	Aug 06, 2018 - Aug 15, 2018	Live Event
SANS Boston Summer 2018	Boston, MAUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS San Antonio 2018	San Antonio, TXUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS August Sydney 2018	Sydney, AU	Aug 06, 2018 - Aug 25, 2018	Live Event
SANS New York City Summer 2018	New York City, NYUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Northern Virginia- Alexandria 2018	Alexandria, VAUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Krakow 2018	Krakow, PL	Aug 20, 2018 - Aug 25, 2018	Live Event
Data Breach Summit & Training 2018	New York City, NYUS	Aug 20, 2018 - Aug 27, 2018	Live Event
SANS Chicago 2018	Chicago, ILUS	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Prague 2018	Prague, CZ	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Virginia Beach 2018	Virginia Beach, VAUS	Aug 20, 2018 - Aug 31, 2018	Live Event
SANS San Francisco Summer 2018	San Francisco, CAUS	Aug 26, 2018 - Aug 31, 2018	Live Event
SANS Copenhagen August 2018	Copenhagen, DK	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS SEC504 @ Bangalore 2018	Bangalore, IN	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS Wellington 2018	Wellington, NZ	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Amsterdam September 2018	Amsterdam, NL	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Tokyo Autumn 2018	Tokyo, JP	Sep 03, 2018 - Sep 15, 2018	Live Event
SANS Tampa-Clearwater 2018	Tampa, FLUS	Sep 04, 2018 - Sep 09, 2018	Live Event
SANS MGT516 Beta One 2018	Arlington, VAUS	Sep 04, 2018 - Sep 08, 2018	Live Event
Threat Hunting & Incident Response Summit & Training 2018	New Orleans, LAUS	Sep 06, 2018 - Sep 13, 2018	Live Event
SANS Baltimore Fall 2018	Baltimore, MDUS	Sep 08, 2018 - Sep 15, 2018	Live Event
SANS Alaska Summit & Training 2018	Anchorage, AKUS	Sep 10, 2018 - Sep 15, 2018	Live Event
SANS Munich September 2018	Munich, DE	Sep 16, 2018 - Sep 22, 2018	Live Event
SANS London September 2018	London, GB	Sep 17, 2018 - Sep 22, 2018	Live Event
SANS Network Security 2018	Las Vegas, NVUS	Sep 23, 2018 - Sep 30, 2018	Live Event
SANS DFIR Prague Summit & Training 2018	Prague, CZ	Oct 01, 2018 - Oct 07, 2018	Live Event
Oil & Gas Cybersecurity Summit & Training 2018	Houston, TXUS	Oct 01, 2018 - Oct 06, 2018	Live Event
SANS Brussels October 2018	Brussels, BE	Oct 08, 2018 - Oct 13, 2018	Live Event
SANS Pen Test Berlin 2018	OnlineDE	Jul 23, 2018 - Jul 28, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced