



Fast Innovation for Commerce Unified Systems

Software Test Documentation

Version 1.0

Date: October 29, 2009

Francis J. Hayes Vélez (48269)

Signature: _____

José M. Lecumberry Jimenez (42441)

Signature: _____

Norberto R. Reyes Díaz (50738)

Signature: _____

Jose H. Torres Torres (43645)

Signature: _____



Revision History

Date	Version	Description	Author
10/26/2009	0.1.1	First draft of SDD	Francis J. Hayes Vélez
10/28/2009	0.1.2	SDD Formatting	Norberto R. Reyes Díaz
10/29/2009	1.0	FICUS SDD Revised and Completed	Norberto R. Reyes Díaz



Table of Contents

1. Introduction	5
1.1 System Overview	5
1.2 Test Approach	5
2. Test Plan	6
2.1 Features to be Tested	6
2.1.1 Validation.....	6
2.1.2 Flexibility.....	7
2.1.3 Speed	7
2.1.4 Browser independence	7
2.2 Features not to be Tested	7
2.2.1 Security	7
2.3 Testing Tools and Environment	7
2.3.1 Markup Validation Service (http://validator.w3.org/)	7
2.3.2 CSS Validation Service (http://jigsaw.w3.org/css-validator/)	7
2.3.3 Link Checker (http://validator.w3.org/checklink)	7
2.3.4 Browser Shots (http://browsershots.org).....	7
2.3.5 Website Pulse: (http://www.websitepulse.com/help/tools.php).....	7
3. Test Cases	7
3.1 HTML (Code Stability)	7
3.1.1 Purpose	7
3.1.2 Inputs.....	8
3.1.3 Expected Outputs & Pass/Fail criteria	8
3.1.4 Test Procedure.....	8
3.2 CSS (Style Sheet Language)	8
3.2.1 Purpose	8
3.2.2 Inputs.....	9
3.2.3 Expected Outputs & Pass/Fail criteria	9
3.2.4 Test Procedure.....	9
3.3 Links	9
3.3.1 Purpose	9
3.3.2 Inputs.....	9
3.3.3 Expected Outputs & Pass/Fail criteria	9
3.3.4 Test Procedure.....	9
3.4 Browser Independence	9
3.4.1 Purpose	9



3.4.2	Inputs.....	10
3.4.3	Expected Outputs & Pass/Fail criteria	10
3.4.4	Test Procedure.....	10
3.5	Speed and Performance	10
3.5.1	Purpose	10
3.5.2	Inputs.....	10
3.5.3	Expected Outputs & Pass/Fail criteria	10
4.	Additional Material.....	10
4.1	Joomla Security Checklist.....	11
Appendix A.	Test Logs	19
A.1	Log for test 1: HTML (Code Stability).....	19
A.1.1	Test Results.....	19
A.1.2	Incident Report	20
A.2	Log for test 2: CSS (Code Stability)	21
A.2.1	Test Results.....	21
A.2.2	Incident Report	42
A.3	Log for test 3: Links.....	42
A.3.1	Test Results.....	42
A.3.2	Incident Report	44
A.4	Log for test 4: Browser Independence	45
A.4.1	Test Results.....	45
A.4.2	Incident Report	51
A.5	Log for test 5: Speed and Performance	52
A.5.1	Test Results.....	52
A.5.2	Incident Report	53



Software Test Documentation (STD)

1. Introduction

Software Testing Documentation (STD) is an empirical investigation conducted to provide stakeholders with information about the quality of Fast Innovation for Commerce Unified Systems (FICUS) under test, with respect to the context in which it is intended to operate. STD also provides an objective, independent view of FICUS allowing L.O. Classic Gym managers to appreciate and understand the risks at implementation of the Web Application (WebApp). Test techniques include, but not limited to, the process of executing the WebApp with the intent of finding software bugs. STD can also be stated as the process of validating and verifying that FICUS (1) meets the business and technical requirements that guided its design and development; (2) works as expected; and (3) can be implemented with the same characteristics as described.

Depending on the testing method employed, STD can be implemented at any time in the development process, however most of the test effort occurs after the requirements have been defined and the coding process has been completed. At JJFN Group we are very concerned that our products exceed the quality the client demands. FICUS has been scheduled to heavy testing and monitoring to prove its high quality, performance and reliability. A superior product quality defines the experience of your customers. On JJFN Group, we define high quality products

1.1 System Overview

Testing can never completely identify all the defects within software. Instead, it furnishes a criticism or comparison that compares the state and behavior of the product against principles or mechanisms by which someone might recognize a problem. These principles may include, but not limited to, specifications, contracts, comparable products, past versions of the same product, inferences about intended or expected purpose, user or customer expectations, relevant standards, applicable laws, or other criteria.

Every software product has a target audience. FICUS is targeted to L.O. Classic Gym's customers and management. Therefore, when JJFN Group develops or otherwise invests in a software product, it can evaluate whether the software product will be acceptable to its end users. Software testing is the process of attempting to make this evaluation.

1.2 Test Approach

FICUS testing will be made by different methods and tools. These tools will approach the system by testing its speed, performance, determining broken links and efficiency. Testing can be done by unit tests of the minimal WebApp's component, or modules. Each unit, or basic component, of the system is tested to verify that the detailed design for these units has been correctly implemented. In an object-oriented environment, this is done at the class level, and includes the constructors and destructors.



Then, integration testing exposes defects in the interfaces and interaction between integrated modules, where larger groups of tested FICUS components, corresponding to elements of the architectural design, are integrated and tested until it works as a system. The system tests, analyze the completely integrated system to verify that it meets its requirements. Integration testing verifies that it is integrated to any external or third party systems defined in the system requirements.

Before shipping the final version of software, alpha and beta testing are often done additionally: Alpha testing is simulated or actual operational testing by potential users or an independent test team at JJFN Group. Alpha testing is often employed as a form of internal acceptance testing, before the software goes to beta testing. These versions of the WebApp, known as beta versions, are released to a limited audience outside of the programming team, allowing that further testing can ensure the product has few faults or bugs. Sometimes, beta versions are made available to the open public to increase the feedback field to a maximal number of future users. Finally, acceptance testing can be conducted by the end-user, customer to validate whether or not to accept FICUS. Acceptance testing may be performed as part of the hand-off process between any two phases of development.

2. Test Plan

Tests coverage in the STD states what requirements will be verified during what stages of the product life. Test coverage is derived from design specifications and other requirements, such as safety standards or regulatory codes, where each requirement or specification of the design will have one or more corresponding means of verification. Test coverage for different product life stages may overlap, but will not necessarily be exactly the same for all stages.

These tests methods in the STD states how the coverage will be implemented. Test methods may be determined by standards, regulatory agencies, contractual agreement, and JJFN Group own quality regulations. This also specifies the equipment to be used in the performance of the tests and establish Pass or Fail criteria. These methods used to verify software design requirements can range from very simple steps, such as visual inspection, to elaborate test procedures that are documented separately.

Our tests responsibilities include what section of the organization will perform the test methods and at each stage of the product life. This allows an organized plan structure, a plan of what test's equipment will be acquire or develop and other what other resources necessary to implement the test methods are needed. Test responsibility includes, the data that will be collected, and how that data will be stored and reported, also known as deliverables. One outcome of a successful test plan should be a record or report of the verification of all design specifications and requirements as agreed upon by all parties.

2.1 Features to be Tested

2.1.1 Validation



Testing will be done to validate the HTML, CSS and Broken Links.

2.1.2 Flexibility

Testing will be done by varying window-sizes and trying different fonts.

2.1.3 Speed

Testing will be done by accessing the site with a 56k modem and by verifying all images sizes.

2.1.4 Browser independence

Testing will be done by accessing the site using different browsers and disable add-ons.

2.2 Features not to be Tested

2.2.1 Security

Testing has already been done by the Joomla Group. Documentation will be provided.

2.3 Testing Tools and Environment

2.3.1 Markup Validation Service (<http://validator.w3.org/>)

This validation checks the markup validity of Web documents in HTML, XHTML, SMIL, MathML, etc.

2.3.2 CSS Validation Service (<http://jigsaw.w3.org/css-validator/>)

Check Cascading Style Sheets (CSS) and (X)HTML documents with style sheets

2.3.3 Link Checker (<http://validator.w3.org/checklink>)

Check links and anchors in Web pages or full Web sites

2.3.4 Browser Shots (<http://browsershots.org>)

Browsershots.org is an online service that automatically captures full page screenshot images of your website in various browsers across all different OS platforms. You also have the option to preview the website design in browsers with or without Flash, Java and JavaScript. Browsershots.org is extremely popular and you may therefore have to wait a few minutes for this service to render screenshots of your website.

2.3.5 Website Pulse: (<http://www.websitepulse.com/help/tools.php>)

The Website test verifies the server status, downloads the full HTML content and measures the response time of the test website. The test results display the times for DNS lookup, connect, download the first byte and download the complete HTML of the tested website.

3. Test Cases

3.1 HTML (Code Stability)

3.1.1 Purpose

HTML, which stands for Hyper Text Markup Language, is the predominant markup language for



web pages. It provides a means to create structured documents by denoting structural semantics for text such as headings, paragraphs, lists etc as well as for links, quotes, and other items. It allows images and objects to be embedded and can be used to create interactive forms. It is written in the form of HTML elements consisting of "tags" surrounded by angle brackets within the web page content. It can include or can load scripts in languages such as JavaScript which affect the behavior of HTML processors like Web browsers; and Cascading Style Sheets (CSS) to define the appearance and layout of text and other material. The W3C, maintainer of both HTML and CSS standards, encourages the use of CSS over explicit presentational markup. If the HTML code fails, the website won't work as expected.

3.1.2 Inputs

<http://ficus.xtilos.com>

3.1.3 Expected Outputs & Pass/Fail criteria

JJFN expect of FICUS at least less than 10 errors in the HTML to be launched and delivered. Then it will fix on scheduled maintenance and patches.

3.1.4 Test Procedure

This will be tested using Markup Validation Service: <http://validator.w3.org/>. The procedure will be online and results are given immediately.

3.2 CSS (Style Sheet Language)

3.2.1 Purpose

Cascading Style Sheets (CSS) is a style sheet language used to describe the presentation semantics (that is, the look and formatting) of a document written in a markup language. Its most common application is to style web pages written in HTML and XHTML, but the language can be applied to any kind of XML document, including SVG and XUL.

CSS is designed primarily to enable the separation of document content (written in HTML or a similar markup language) from document presentation, including elements such as the layout, colors, and fonts. This separation can improve content accessibility, provide more flexibility and control in the specification of presentation characteristics, enable multiple pages to share formatting, and reduce complexity and repetition in the structural content (such as by allowing for table less web design). CSS can also allow the same markup page to be presented in different styles for different rendering methods, such as on-screen, in print, by voice (when read out by a speech-based browser or screen reader) and on Braille-based, tactile devices. While the author of a document typically links that document to a CSS style sheet, readers can use a different style sheet, perhaps one on their own computer, to override the one the author has specified.

CSS specifies a priority scheme to determine which style rules apply if more than one rule matches against a particular element. In this so-called cascade, priorities or weights are calculated and



assigned to rules, so that the results are predictable. If the CSS code fails, the website won't work as expected.

3.2.2 Inputs

<http://ficus.xtilos.com>

3.2.3 Expected Outputs & Pass/Fail criteria

JJFN Group expect of FICUS at least less than 5 errors in the CSS to be launched and delivered. Then it will fix on scheduled maintenance and patches.

3.2.4 Test Procedure

This will be tested using CSS Validation Service: <http://jigsaw.w3.org/css-validator/>. The procedure will be online and results are given immediately.

3.3 Links

3.3.1 Purpose

Links is an open source text and graphic web browser with a pull-down menu system. It renders complex pages, has partial HTML 4.0 support (including tables and frames and support for multiple character sets such as UTF-8), supports color and monochrome terminals and allows horizontal scrolling.

It is oriented toward visual users who want to retain many typical elements of graphical user interfaces (pop up windows, menus etc.) in a text-only environment. The focus on intuitive usability makes it suitable as a web browser for low-end terminals in libraries, Internet cafes etc. If the links fails, the website won't work as expected.

3.3.2 Inputs

<http://ficus.xtilos.com>

3.3.3 Expected Outputs & Pass/Fail criteria

JJFN expect of FICUS at least less than 0 errors in the CSS to be launched and delivered.

3.3.4 Test Procedure

This will be tested using Link Checker: <http://validator.w3.org/checklink>. The procedure will be online and results are given immediately.

3.4 Browser Independence

3.4.1 Purpose

A Web browser is a software application for retrieving, presenting, and traversing information resources on the World Wide Web. An information resource is identified by a Uniform Resource Identifier (URI) and may be a web page, image, video, or other piece of content. Hyperlinks present in resources enable users to easily navigate their browsers to related resources.



Although browsers are primarily intended to access the World Wide Web, they can also be used to access information provided by Web servers in private networks or files in file systems. The major web browsers are Internet Explorer, Mozilla Firefox, Apple Safari, Google Chrome, and Opera. FICUS must work in different browsers and environments because it will access by different users in different operating systems and different web browsers.

3.4.2 Inputs

<http://ficus.xtilos.com>

3.4.3 Expected Outputs & Pass/Fail criteria

JJFN expect of FICUS at least to run on 80% or more to be launched and delivered.

3.4.4 Test Procedure

This will be tested using Browsershots: <http://browsershots.org/>. The procedure will be online and results are given immediately.

3.5 Speed and Performance

3.5.1 Purpose

Speed on a website is very important, the less time a person need to wait for the website to open and reload, the more information and interaction can be expected from the user. Performance on a website is always expected to be high, and the less time the webpage need to communicate with the browser, the faster it will be displayed on the browser. If the speed and performance is low as expected, the website won't work as expected.

3.5.2 Inputs

<http://ficus.xtilos.com>

3.5.3 Expected Outputs & Pass/Fail criteria

JJFN expect of FICUS at least less than 0 errors in the Speed and Performance to be launched and delivered.

3.5.4 Test Procedure

This will be tested using Website Pulse: <http://www.websitepulse.com/help/tools.php>. The procedure will be online and results are given immediately.

4. Additional Material



4.1 Joomla Security Checklist

Security Checklist 1 - Getting Started

Read Me First

Security is always a concern

On the Internet, security is a fast evolving and ever present challenge. There is no one right way to secure a site, and all security methods are subject to improvement, revision, and obsolescence at any time. Luckily, there are many well-established principles that can help. The following checklist points you toward current best practices for Joomla security.

The most important guidelines

This checklist is long because the full plot is thick and complex. But don't despair! Here are the essential guidelines for securing any Web site. Following these few pointers will protect your site from most catastrophes.

Backup Early and Often: Setup (and use and test!) a regular backup and recovery process. When done well, this one practice ensures that you can recover from almost any imaginable disaster.

Update Early and Often: Promptly update to the latest *stable* version of Joomla! and any installed third-party extensions. This one step ensures that your site is protected from all new vulnerabilities as soon as a fix is released, and from all new attacks methods as soon as a defense is developed.

Use a secure host Of course the above advice applies to your entire infrastructure. Proper Web security is largely a Web hosting issue. Therefore, if security matters to you, use a high-quality Web host.

Consider hiring professional assistance if you have no experience or knowledge in this area. If you wish to ask questions of the community regarding security issues, please do so using the appropriate board (ex., Installation, Migration and Updating, Administration, etc) in the [Joomla! Forums](#).

There are many other important security considerations that you can learn about in this checklist and in the Security FAQ's.

There is no Web security!

There's no free lunch!

Don't be fooled by Joomla's award winning ease-of-use. Maintaining a secure Web site on the open Internet is not easy. Adequate security requires a range skills and knowledge, constant watchfulness, and a very solid backup and recovery process.

There's no one right way!

Due to the variety and complexity of modern web systems, security issues can't be resolved with simple, one-size-fits-all solutions. You (or someone you trust) must learn enough about your server infrastructure to make valid security decisions. Strong security is a moving target. Today's expert might be tomorrow's victim. Welcome to the game...

There's no substitute for experience!

To secure your Web site, you must gain real experience (some of which will be bitter), or get experienced help from others. If you haven't invested the considerable time it takes to learn how to maintain a secure Web site, be sure you can consult with someone who has. Read this tongue-in-cheek description of the [Top 10 Stupidest Administrator Tricks](#) which illustrates typical, blow-by-blow examples of how to learn Web security the hard way.

Encouragements

Start at the head of the herd

The Security Forums are filled with "Help! I've been hacked" posts by people who did NOT follow standard security practices. If you decided to study this checklist before your site is attacked, congrats, you're already ahead of the herd.

It's not as hard as it looks

If this is one of your first Web sites, security considerations may seem intimidating, but you don't have to deal with all of it at once. As you become familiar with tools of modern Open Source Web development, such as [GNU/Linux](#), [Apache](#), [MySQL](#), [SQL](#), [PHP](#), [HTTP](#), [CSS](#), [XML](#), [RSS](#), [TCP/IP](#), [FTP](#), [Subversion](#), [JavaScript](#), [Joomla!](#), you'll add refinements to your set of security tactics.

How to get help

If you believe your Web site was attacked, **do not** post in the Joomla! forums. If there is a vulnerability,





publishing that information could put other Web sites at risk. Instead, report possible security vulnerabilities to the [Joomla! Security Task Force](#).

How to read these documents

Not all techniques are appropriate for every level of user. Apply the techniques you understand and read up on the ones you don't.

Not all techniques are appropriate for every server. If you use a shared server, you will need to depend on the settings established by your hosting provider. If you are using a virtual or dedicated server, you will be able to apply more creative and exotic techniques.

Not all techniques are appropriate for all Joomla! versions. Where a technique applies to only one version, an image is added, such as  1.0 Native or  1.5 Native.

Getting Started

Are you ready?

Can you administer a dynamic, 24x7, world-accessible, database-driven, interactive, user-authenticated web server?

Do you have the time and resources to respond to the flow of emerging Internet security issues? The [Top 10 Stupidest Administrator Tricks](#) is a comic/tragic look at what can go wrong. Don't learn these tricks the hard way! Depending on your recent experience, reading the *Stupidest Tricks* will either make you laugh or cry.

Stay informed of security issues

Given the complexity of web servers, new vulnerabilities and conflicts are discovered all the time. To receive all security announcements, just subscribe to Joomla Security News. There are several ways to subscribe:

[Automatic Email Notification](#)

[RSS feed](#).

Check the FAQs.

The most helpful posts in the Joomla! Security Forum are converted into [Security and Performance FAQs](#). Many of the items on this list are explained in much greater detail in the FAQs.

Learn from the pros

Read the excellent [Absolute Beginners Guide to Joomla!](#) It has wealth of tips and tricks presented in an easy to understand format. Even experienced Joomlaists find great ideas here.

Hunt down the many nuggets of wisdom found in the [Joomla! Forums](#), in particular the [Joomla! 1.5 Security Forum](#) and the [Joomla! 1.0 Security Forum](#).

Security Checklist 2 - Hosting and Server Setup

Choose a Qualified Hosting Provider

The most important decision

Probably no decision is more critical to site security than the choice of hosts and servers. However, due to the wide variety of hosting options and configurations, it's not possible to provide a complete list for all situations. Check this unbiased [list of recommended hosts](#) who fully meet the security requirements of a typical Joomla site. ([FAQ](#))

Shared server risks

If you are on a tight budget and your site does not process highly confidential data, you can probably get by with a shared server, but you must understand the unavoidable risks. Most of the tips listed below are appropriate for securing sites on shared server environments.

Avoid sloppy server configurations

For a real eye-opener, [read this report](#) on thousands of sites that allowed Google to index the results of `phpinfo()`. Don't make this mistake on your site! The report includes alarming statistics on the percentage of site that use deprecated settings such as `register_globals` ON or that don't have `open_basedir` set at all: By the way, if *phpini* and *register_globals* are unfamiliar terms you are probably not ready to securely manage your own site.

Configuring Apache

Use Apache `.htaccess`

See also [.htaccess examples](#)



Block typical exploit attempts with local Apache `.htaccess` files. This option is not enabled on all servers. Check with your host if you run into problems. Using `.htaccess`, you can password protect sensitive directories, such as administrator, restrict access to sensitive directories by IP Address, and depending on your server's configuration, you may be able to increase security by switching from PHP4 to PHP5. Joomla ships with a [preconfigured .htaccess](#) file but *you* need to choose to use it. The file is called `htaccess.txt` to use it rename it to `.htaccess` and place it in the root of your webpage.

Consider following the "Least Privilege" principle for running PHP using tools such as PHPsuExec, `php_suexec` or suPHP. (Note: These are advanced methods that require agreement and coordination with your hosting provider. Such options are enabled or disabled on a server-wide bases, and are not individually adjustable on shared servers.)

Use Apache `mod_security`

Configure Apache `mod_security` and `mod_rewrite` filters to block PHP attacks. See [Google search for mod_security](#) and [Google search for mod_rewrite](#). (Note: These are advanced methods that usually require agreement and coordination with your hosting provider. Such options are enabled or disabled on a server-wide bases, and are not individually adjustable on shared servers.)

Configuring MySQL

Secure the database

Be sure MySQL accounts are set with limited access. The initial install of MySQL is insecure and careful configuration is required. (See the [MySQL Manuals](#)) Note: This item applies only to those administering their own servers, such as dedicated servers. Users of shared servers are dependent on their hosting provider to set proper database security.)

Configuring PHP

Understand how PHP works

Understand how to work with the `php.ini` file, and how PHP configurations are controlled. Study the [Official List of php.ini Directives](#) at <http://www.php.net>, and the well-documented default `php.ini` file included with every PHP install. Here is the [latest default php.ini file](#) on the official PHP site.

Use PHP5

Currently, both PHP4 and PHP5 are maintained, and both are often available on servers. Before PHP4 becomes obsolete, upgrade your custom scripts to PHP5. Don't worry about core Joomla code; all current versions are PHP5 compatible. (See [PHP News](#))

Use local `php.ini` files

On shared servers you can't edit the main `php.ini` file, but you may be able to add custom, local `php.ini` files. If so, you'll need to copy the `php.ini` files to every sub-directory that requires custom settings. Luckily a [set of scripts at B & T Scripts and Tips](#) can do the hard work for you.

There are a few important things to keep in mind.

Local `php.ini` files **only** have an effect if your server is configured to use them. This includes a `php.ini` file in your `http_root` directory. You can test whether or not these file affect your site by setting an obvious directive in the local `php.ini` file to see if it affects your site.

Local `php.ini` files only effect `.php` files that are located within the same directory (or included() or required() from those files). This means that there are normally only two Joomla! directories in which you would want to place a `php.ini` file. They are your `http_root`(your actual directory name may vary), which is where Joomla's Front-end `index.php` file is located, and the Joomla! `administrator` directory, which is where the Back-end administrator `index.php` file is located. Other directories that don't have files called via the Web do not need local `php.ini` files.

If you have a `php.ini` file in every directory, some script probably did this for you. If you didn't intend it to happen, you probably should root them out, but given #2 above, you probably only have to panic about the `php.ini` files in `http_root` and the `administrator` directories.

Use PHP `disable_functions`

Use `disable_functions` to disable dangerous PHP functions that are not needed by your site. Here is a typical setup for a Joomla! site:

`disable_functions = show_source, system, shell_exec, passthru, exec, phpinfo, popen, proc_open`

Use PHP `open_basedir`



`open_basedir` should be enabled and correctly configured. This directive limits the files that can be opened by PHP to the specified directory-tree. This directive is NOT affected by whether Safe Mode is ON or OFF.

The restriction specified with `open_basedir` is a prefix, not a directory name. This means that `open_basedir = /dir/incl` allows access to `/dir/include` and `/dir/incls` if they exist. To restrict access to only the specified directory, end with a slash. For more information, see [PHP Security and Safe Mode Configuration Directives](#).

```
open_basedir = /home/users/you/public_html
```

In some system configurations, at least with PHP 4.4.8, the use of the trailing slash to restrict the access to only the specified directory may cause Joomla to warn *JFolder::create: Infinite loop detected* when saving the Back-End Global Configuration. This warning is triggered because PHP `file_exists()` function fails, for example, when asked if `/home/user/public_html/joomla_demo` exists and `open_basedir` is set to `/home/user/public_html/joomla_demo/` (see the trailing slash).

Additionally, if `open_basedir` is set it may be necessary to set PHP `upload_tmp_dir` configuration directive to a path that falls within the scope of `open_basedir` or, alternatively, add the `upload_tmp_dir` path to `open_basedir` using the appropriate path separator for the host system.

```
open_basedir = /home/users/you/public_html:/tmp
```

PHP will use the system's temporary directory when `upload_tmp_dir` is not set or when it is set but the directory does not exist, therefore it may be necessary to add it to `open_basedir` as above to avoid uploading errors within Joomla.

Adjust `magic_quotes_gpc`

Adjust the `magic_quotes_gpc` directive as needed for your site. The recommended setting for Joomla! 1.0.x is ON to protect against poorly-written third-party extensions. The safest method is to turn `magic_quotes_gpc` off and avoid all poorly-written extensions, period.

Joomla! 1.5 ignores this setting and works fine either way. For more information, see [PHP Manual, Chapter 31. Magic Quotes](#).

```
magic_quotes_gpc = 1
```

Don't use PHP `safe_mode`

Avoid the use of PHP `safe_mode`. This is a valid but incomplete solution to a deeper problem and provides a false sense of security. See the official PHP site for an explanation of this issue.

```
safe_mode = 0
```

Don't use PHP `register_globals`

Automatically registering global variables was probably one of the dumbest decisions the developers of PHP made. This directive determines whether or not to register the EGPCS (Environment, GET, POST, Cookie, Server) variables as global variables where they become immediately available to all PHP scripts, and where they can easily overwrite your own variable if you're not careful. Luckily, the PHP developers long since realized the mistake and have depreciated this 'feature'.

If your site is on a shared server with a hosting provider that insists `register_globals` must be on, you should be very worried. Although you can often turn `register_globals` off for your own site with a local `php.ini` file, this adds little security as other sites on the same server remain vulnerable to attacks which can then launch attacks against your site from within the server. For more information, see [ZEND Chapter 29. Using Register Globals](#).

```
register_globals = 0
```

Don't use PHP `allow_url_fopen`

Don't use PHP `allow_url_fopen`. This option enables the URL-aware fopen wrappers that enable accessing URL object like files. Default wrappers are provided for the access of remote files using the ftp or http protocol, some extensions like zlib may register additional wrappers. Note: This can only be set in `php.ini` due to security reasons.

```
allow_url_fopen = 0
```

Setup a backup and recovery process

The most important rule:

Thou shalt at all time be able to return your site to a previous working state through regular use of a



strong, off-site backup and recovery process. Be sure your backup and recovery process is in place and tested BEFORE you go live. This is the single best way (and often the only way) to recover from such inevitable catastrophes as:

A compromised/cracked site.

Broken site due to a faulty upgrade.

Hardware failure, such as dead hard drives, power failures, server theft, etc.

Authoritarian government intervention. (More common than some think.)

Needing to quickly relocate to a new server or hosting provider.

Security Checklist 3 - Testing and Development

Secure Testing and Development

Develop locally, deploy globally

Develop and test your site on a local machine first. Installing Joomla locally is not as hard as it may sound, and the exercise will greatly boost your confidence.

Use an IDE

Consider using an Integrated Development Environment (IDE). One free IDE that many Joomla! developers use is [Eclipse](#). See [Setting up your workstation for Eclipse development](#) for instructions on installing Eclipse.

Use a versioning system

Be able to roll back to an earlier version of your site using a modern version control system, such as CVS, [Subversion](#), or [git](#). The Eclipse IDE indicated above includes a Subversion plugin. This allows you to work with the Joomla! source repository as well as other projects hosted on [JoomlaCode](#).

More suggested tools

Check out the Joomla! community's list of popular [Developer Software and Tools](#).

Setup a backup process first

The most important rule

Thou shalt at all time be able to return your site to a previous working state through regular use of a strong, off-site backup and recovery process.

Be sure your backup and recovery process is ready and tested BEFORE your site goes live.

This is the single best way (and often the only way) to recover from such inevitable catastrophes as:

A compromised/cracked site.

Broken site due to a faulty upgrade.

Hardware failure, such as dead hard drives, power failures, server theft, etc.

Authoritarian government intervention. (More common than some think.)

Needing to quickly relocate to a new server or hosting provider.

Security Checklist 4 - Joomla Setup

Configuring Joomla!

Install official versions of Joomla!

To avoid breaking your site, search the forums for reports of incompatible extensions before upgrading to a new version of Joomla.

Upgrade to the [latest stable version of Joomla!](#) as soon as possible.

Download Joomla! from official sites only, such as [JoomlaCode.org](#), and check the [MD5 hash](#).

Use [Joomla Diagnostics](#) to ensure that all files were installed correctly. (Note: the version of Joomla Diagnostics made for the initial release of 1.5 does not work for 1.5.3.)

Change the default administrator username

Change the user name of the default admin user. This simple step effectively increases the security of this critical account 50% by modifying one of the two variables attackers must know to gain access. The password is the other variable. Change it early and often. ([FAQ](#))

Protect directories and files


Increase the security of the critical *configuration.php* file by moving it outside of the *public_html* directory.


For more information visit ([FAQ](#))

Ensure that all configurable paths to writable or uploadable directories (document repositories, image



galleries, caches) are outside of public_html. Check third party extensions such as DOCMan and Gallery2 for editable paths to writable directories.

 **1.5 Native** In the Back-End Global Configuration, change the log path. Some extensions use the built in JLog class. This will, by default write logs to <http://yoursite/logs>. Change this to a place that a casual browser cannot find (and don't pick /tmp/), or lock it down with http authentication. Because we are dealing Open Source software, attackers can read the code of third-party extensions and may be able to guess log file names.

 **1.5 Native** In the Back-End Global Configuration, change the temp folder path. If the log and temp paths are changed and PHP `open_basedir` configuration directive is set, make sure that the new paths fall within the scope of `open_basedir`. There is currently no easy way to move the Joomla! /image and /media directories. This is because thousands of third party extensions expect to find these important directories at the current location. The best plan is to make sure `open_basedir` is properly set for all the user accounts on your server. Check with your host if unsure.


Adjust file and directory permissions

Once your site is configured and stable, write-protect critical directories and files by changing directory permissions to 755, and file permissions to 644. There is a feature in Site --> Global Configuration --> Server to set all folder and file permissions at once. Test third party extensions afterwards, and carefully review the code of any extension that has trouble with such settings. Note: Depending on your server's permissions, you may need to temporarily reset to more open permissions when installing more extensions with the Joomla! installer.

This option no longer appears in Joomla.

Remove unneeded files


Remove all design templates not needed by your site. Never put security logic into template files.


 **1.5 Native** Remove the XML-RPC server if you don't need it.

Clean up after installs. The installation process will require you to delete the installation directory and all its contents. Do this; do not simply rename it. If you upload files to your site as compressed archives (xxxx.zip for example), don't forget to remove the compressed file. Check the /temp/ directory as temporary files may remain there after a failed installation attempt.

In general, do not leave any unneeded files (compressed or otherwise) on a public server. Each unused (and perhaps long forgotten) file is a potential security hole.

Turn Register Globals Emulation OFF

 **1.0 Native** Turn Joomla's Register Globals Emulation OFF. Although this setting is somewhat safer than PHP `register_globals`, you are much better off avoiding such settings all together (as well as any applications that require them). On pre-1.0.13 versions of Joomla, this setting is found in the `globals.php` file. As of version 1.0.13, it can be turned off in the Back-end, under Global Settings.

 **1.5 Native** Joomla 1.5 and greater, does not use register globals, and in fact has smart code to defeat this setting even if it's turned on at the PHP level. Note that although this makes Joomla itself safer, any server with register globals turned on is potentially vulnerable. Any shared server with register globals turned on is more than likely a sitting duck. Any hosting provider that insists register globals should be turned on is ignorant, incompetent, or worse. Was that blunt enough?

For more information on `register_globals`, please see [Security Checklist: PHP: register_globals](#).

Installing Joomla! Extensions

Backup before installing

Before installing extensions, always backup your site's files and database. This follows a very basic principle:

Thou shalt at all times be able to return your site to a previous working state.

Therefore, it's smart to set up a simple and fast backup script to automated this task. If you don't set up an easy process in advance, you'll be sorely tempted to do a quick upgrade without backing up first. This very understandable tendency is however one of the chief causes of premature hair loss, sudden career changes, and even death.



Check for extension vulnerabilities

Most security vulnerabilities are caused by third party extensions. Before installing extensions, check the Official List of Vulnerable 3rd Party/Non Joomla! Extensions. There's an entire forum dedicated to vulnerable third part extensions. Subscribe to it.

Download from trusted sites

The fully qualified and official definition of a "trusted site" is one that **YOU** trust.

User beware! Check the code quality

Third party extensions come in all flavors of quality and age. Although Joomla! coding standards exist, third party developers are not required to follow them. Extensions listed on the official Joomla! site are not reviewed for compliance, however if verified vulnerabilities are reported, they will be removed from the list until they are fixed.

Test, test, test...

Test all extensions on a development site before installing on a production site. Then test on the production site. Don't forget to check the logs for runtime errors and warnings.

Remove junk files

Remove all unused extensions and double check that related folders and files were actually removed by uninstall scripts. Note that during uninstall, many third party extensions will leave related files on your site, and related database tables complete with data. This is either a feature or a bug depending on your point of view. Any files left on your server remain accessible from the Web via direct URLs, such as

http://yousite.com/modules/bad_module.

Avoid encrypted code

Joomla is (and despite disinformation campaigns, always has been) a GNU GPL project. This means that all extensions to Joomla must also be free (as in freedom) and open (as in readable code). Encrypted code may be safe, but you can't determine this for yourself, and so you must trust the developers. Using others' encrypted code puts you back in the world of proprietary software where you must wait for security patches from the developer, hoping that attackers don't find your site first before a fix is released.

You are often not free to modify, improve, or share encrypted code. These restrictions make encrypted code less valuable to the community as a whole, and reduce the overall viability of the Joomla project which depends on open sharing among all participants.

Of course, code that is not distributed to others is exempt from GNU GPL distribution requirements. Thus you can encrypt Joomla-related code your own servers providing you do not share it with others.

Additional Joomla! Hardening Tips and Tricks

Avoid shared servers if possible

For maximum security, avoid a shared server on which you don't know or can't trust all the other users or their code quality.

Use an SSL server

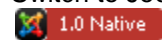
SSL servers are currently the only way to securely process confidential transactions and secure user authentication. SSL works by encrypting all HTTP communications between the Web server and Web clients. Thus, even if a transmission is intercepted, it can not be read.

Joomla! 1.0.x does not allow you to assign an SSL server to individual sub-directories. Search the forums for "Tommy Hack" for one way to deal with this. Joomla! 1.5 has greatly improved SSL options.

Use Apache's .htaccess

For an additional layer of password protection, you can use .htaccess to password protect critical directories. This is usually adequate for blocking the typical script kiddie, but be aware that .htaccess password protection alone is not a highly secure method. It **MUST** be combined with an SSL server for maximum protection. An SSL server is required for protecting your site from more sophisticated attacks, such as packet sniffing.

Switch to Joomla! 1.5



The most significant upgrade in Joomla!'s history includes powerful security and performance enhancements.

[Joomla 1.5 Overview](#)

[Joomla Downloads](#)



Add Joomla! Security Announcements to your site

The Joomla! Security Team supports and RSS feed that provides the latest Joomla security information. The following FAQ explains how to add this feed to your site.

Security Checklist 5 - Site Administration

Site Administration

Use well-formed passwords

Change passwords regularly and keep them unique. Use a random combination of letters, numbers, or symbols and avoid using single names or words found in a dictionary. Never use the names of your relatives, pets, etc. Search the forums for a script supplied by Wizzie that automatically changes passwords. This is a great tool for administrators or multiple sites.

Follow a password leveling scheme

Most users may not need more than three levels of passwords and webmasters no more than five. Each level must be completely unrelated to the others in terms of which usernames and passwords are used.

Maintain a strong site backup process

Never rely on others' backups. Take responsibility for your backup procedures. Many ISPs state in their contract that you can not rely solely on their backups.

Monitor crack attempts

VPS and dedicated server users can run TripWire or SAMHAIN. These applications provide exhaustive file checking and reporting functionality, and can be installed in a stealthy manner to help protect themselves in the event of a serious infiltration. (Note: Users of shared servers can not use this technique.)

Perform automated intrusion detection

Use an Intrusion Prevention/Detection Systems to block/alert on malicious HTTP requests.

[Google search](#)

Perform manual intrusion detection

Regularly check raw logs for suspicious activity. Don't rely on summaries and graphs.

Stay current with security patches and upgrades

Apply vendor-released security patches ASAP.

Proactively seek site vulnerabilities

Perform frequent web scanning.

[Google Search](#)

Proactively seek SQL injections vulnerabilities

Use tools such as Paros Proxy for conducting automated SQL Injection tests against your PHP applications.

Use shell scripts to automate security tasks

Search the forums for these popular scripts:

Joomla! Version Checking

Joomla! Component/Module Version Checking

Exploit Checking

Learn about security software

There is not a single tool that can protect your site. If there were, it would be so heavily targeted that it would probably become a liability.

Don't reinvent every wheel

Every now and then hire a professional Joomla! security consultant to review your configurations. Do you remember the adage, *"Anyone who acts as their own lawyer has a fool for a client."* The same goes for Web development. Don't expect to catch all of your own security mistakes.

Security Checklist 6 - Site Recovery

Site Recovery

Get help the right way

If you believe your Web site was attacked, **do not** create yet another oh-so-boring post in the Joomla! forums with the title, *"Help! I've been hacked."* This tells us nothing of importance. The vast majority of



compromised sites were not setup correctly or were using obsolete versions of Joomla! or third-party extensions. This is what you need to investigate.

If you discover a real vulnerability, publishing the information could put other Web sites at risk. Instead, report possible security vulnerabilities to the [Joomla! Security Task Force](#).

Follow a logical and rigorous recovery process

Know the important steps to follow when your site has been compromised. Once you've gotten to this point, there are few shortcuts. ([FAQ](#))

Reset your administrator password

Many attackers take pleasure in locking you out of your site. They do this by 'changing the key', or changing your administrator password. If you are locked out, don't panic! There is a simple procedure for resetting your administrator password. ([FAQ](#))

Find exploit attempts using the *NIX shell


Know how to check for suspicious and/or modified files. Know how to check the raw Apache logs for suspicious activity on your site.


Appendix A. Test Logs

A.1 Log for test 1: HTML (Code Stability)


A.1.1 Test Results


Validation Output: 13 Errors

1.  *Line 38, Column 70:* required attribute "alt" not specified
... src="http://ficus.xtilos.com/images/gym1.jpg"></center>
The attribute given above is required for an element that you've used, but you have omitted it. For instance, in most HTML and XHTML document types the "type" attribute is required on the "script" element and the "alt" attribute is required for the "img" element.
Typical values for type are type="text/css" for <style> and type="text/javascript" for <script>.


2.  Line 38, Column 79: end tag for "img" omitted, but OMITTAG NO was specified
....xtilos.com/images/qym1.jpg"></center> </div>

You may have neglected to close an element, or perhaps you meant to "self-close" an element, that is, ending it with `</>` instead of `>`.

3.  *Line 38, Column 19: start tag was here*
- `<center></center>`


4.  Line 49, Column 69: required attribute "alt" not specified
...mg src="http://ficus.xtilos.com/images/gym.jpg"></center>











The attribute given above is required for an element that you've used, but you have omitted it. For instance, in most HTML and XHTML document types the "type" attribute is required on the "script" element and the "alt" attribute is required for the "img" element. Typical values for type are type="text/css" for <style> and type="text/javascript" for <script>.

5.  Line 49, Column 78: end tag for "img" omitted, but OMITTAG NO was specified
...us.xtilos.com/images/gym.jpg"></center> </div>



You may have neglected to close an element, or perhaps you meant to "self-close" an element, that is, ending it with ">" instead of ">".

6.  *Line 49, Column 19:* start tag was here

```
<center></center>
```
7.  *Line 163, Column 99:* required attribute "alt" not specified
...order="0" width="500" height="333" /></p></td>
The attribute given above is required for an element that you've used, but you have omitted it. For instance, in most HTML and XHTML document types the "type" attribute is required on the "script" element and the "alt" attribute is required for the "img" element. Typical values for type are type="text/css" for <style> and type="text/javascript" for <script>.
8.  *Line 38, Column > 80:* XML Parsing Error: Opening and ending tag mismatch: img line 38 and center
...tilos.com/images/gym1.jpg"></center> </div>...
9.  *Line 38, Column > 80:* XML Parsing Error: Opening and ending tag mismatch: center line 38 and div
...tilos.com/images/gym1.jpg"></center> </div>...
10.  *Line 49, Column 78:* XML Parsing Error: Opening and ending tag mismatch: img line 49 and center
...us.xtilos.com/images/gym.jpg"></center> </div>
11.  *Line 49, Column > 80:* XML Parsing Error: Opening and ending tag mismatch: center line 49 and div
...tilos.com/images/gym.jpg"></center> </div>...
12.  *Line 193, Column 7:* XML Parsing Error: Opening and ending tag mismatch: div line 25 and body
</body>
13.  *Line 194, Column 7:* XML Parsing Error: Opening and ending tag mismatch: div line 20 and html
</html>
14.  *Line 194, Column 7:* XML Parsing Error: Premature end of data in tag body line 19
</html>

15.  *Line 194, Column 7:* XML Parsing Error: Premature end of data in tag html line 2
</html>

A.1.2 Incident Report



Results showed 13 errors and 2 warnings. They will be fix on maintenance.

A.2 Log for test 2: CSS (Code Stability)

A.2.1 Test Results

W3C CSS Validator results for <http://ficus.xtilos.com> (CSS level 2.1)

Congratulations! No Error Found.

This document validates as [CSS level 2.1](#) !

To show your readers that you've taken the care to create an interoperable Web page, you may display this icon on any page that validates. Here is the XHTML you could use to add this icon to your Web page:



```
<p>
  <a href="http://jigsaw.w3.org/css-validator/check/referer">
    
  </a>
</p>
```



```
<p>
  <a href="http://jigsaw.w3.org/css-validator/check/referer">
    
  </a>
</p>
```

(close the img tag with > instead of /> if using HTML <= 4.01)



The W3C validators rely on community support for hosting and development.

[Donate](#) and help us build better tools for a better web.

If you like, you can download a copy of this image to keep in your local web directory, and change the XHTML fragment above to reference your local image rather than the one on this server.

If you would like to create a link to this page (i.e., this validation result) to make it easier to re-validate this page in the future or to allow others to validate your page, the URI is:

<http://jigsaw.w3.org/css-validator/validator?uri=http%3A%2F%2Fficus.xtilos.com&profile=css21&usermedium=all&warning=1>

or

<http://jigsaw.w3.org/css-validator/check/referer> (for HTML/XML document only)

(Or, you can just add the current page to your bookmarks or hotlist.)

[↑ Top](#)

Warnings (4)

URI : <http://ficus.xtilos.com/templates/siteground-j15-82/css/template.css>

137 #pillmenu li In (x)HTML+CSS, floated elements need to have a width declared. Only elements with an intrinsic width (html, img, input, textarea, select, or object) are not affected

142 #pillmenu li In (x)HTML+CSS, floated elements need to have a width declared. Only elements with an intrinsic width (html, img, input, textarea, select, or object) are not affected



- 625 a.readon In (x)HTML+CSS, floated elements need to have a width declared. Only elements with an intrinsic width (html, img, input, textarea, select, or object) are not affected
- 1253 .tool-tip In (x)HTML+CSS, floated elements need to have a width declared. Only elements with an intrinsic width (html, img, input, textarea, select, or object) are not affected

Valid CSS information

```
input.system-openid, input.com-system-openid {
background : url(http://openid.net/images/login-bg.gif) no-repeat;
background-color : #fff;
background-position : 0 50%;
color : #000;
padding-left : 18px;
}
.system-unpublished {
background : #e8edf1;
border-top : 4px solid #c4d3df;
border-bottom : 4px solid #c4d3df;
}
#system-message {
margin-bottom : 10px;
padding : 0;
}
#system-message dt {
font-weight : bold;
}
#system-message dd {
margin : 0;
font-weight : bold;
text-indent : 30px;
}
#system-message dd ul {
color : #0055bb;
margin-bottom : 10px;
list-style : none;
padding : 10px;
border-top : 3px solid #84a7db;
border-bottom : 3px solid #84a7db;
}
#system-message dt.message {
display : none;
}
#system-message dt.error {
display : none;
}
#system-message dd.error ul {
color : #c00;
background-color : #e6c0c0;
border-top : 3px solid #de7a7b;
border-bottom : 3px solid #de7a7b;
}
#system-message dt.notice {
display : none;
}
#system-message dd.notice ul {
color : #c00;
```



```
background : #efe7b8;
border-top : 3px solid #f0dc7e;
border-bottom : 3px solid #f0dc7e;
}
#system-debug {
color : #ccc;
background-color : #fff;
padding : 10px;
margin : 10px;
}
#system-debug div {
font-size : 11px;
}
body {
font-family : Tahoma, Verdana, Arial, sans-serif;
line-height : 1.3em;
margin : 0;
padding : 0;
font-size : 11px;
color : #666;
background : #fff;
}
body.contentpane {
background : #fdfefe;
}
form {
margin : 0;
padding : 0;
}
img, table {
border : none;
}
p {
margin : 5px 0;
text-align : justify;
}
a {
font-weight : 400;
color : #666666;
outline : none;
}
a:link {
text-decoration : underline;
}
a:visited {
text-decoration : underline;
color : #999;
}
a:hover {
text-decoration : none;
}
input {
color : #ccc;
outline : none;
margin : 0;
```



```
}
input:focus {
outline : none;
}
button {
color : #fff;
font-size : 11px;
border : none;
background : #696969;
cursor : pointer;
}
.search .inputbox {
float : left;
border : none;
color : #000;
font-size : 11px;
line-height : 15px;
width : 130px;
height : 17px;
padding : 3px 10px 1px 10px;
background : transparent url(../images/inputbox.png) no-repeat top left;
}
#modIgn_remember.inputbox {
background : none;
border : none;
width : auto;
vertical-align : middle;
}
input.button, .validate {
color : #fefefe;
font-size : 11px;
cursor : pointer;
font-weight : 700;
border : none;
height : 23px;
line-height : 19px;
padding : 1px 4px 4px;
margin : 6px 0 0 0;
background : transparent url(../images/but.png) repeat-x top left;
}
input.button:hover, .validate:hover {
color : #fe8300;
}
#page_bg {
background : #f1f2f2 url(../images/page_bg.png) repeat-x top left;
}
#top_bg {
background : transparent url(../images/page_bg.png) repeat-x top center;
}
#footer_bg {
background : transparent url(../images/footer_bg.png) no-repeat bottom center;
}
#pillmenu {
margin : 0 auto;
width : 960px;
}
```




```
height : 40px;
overflow : hidden;
background : transparent url(..images/t_menu.png) no-repeat top center;
}
#pillmenu ul {
margin : 0;
padding : 0;
list-style : none;
}
#pillmenu li {
float : left;
background : transparent url(..images/t_menu_divider.png) no-repeat right center;
}
#pillmenu li a {
float : left;
color : #f9f9f8;
text-decoration : none;
text-transform : uppercase;
font-weight : 700;
height : 40px;
line-height : 39px;
padding : 0 16px;
cursor : pointer;
}
#pillmenu li a:hover {
color : #81cc0a;
background : transparent url(..images/t_menu_hover.gif) repeat top right;
}
#pillmenu li a#active_menu-nav {
color : #81cc0a;
background : transparent url(..images/t_menu_hover.gif) repeat top right;
}
#top h1 {
position : absolute;
top : 0;
left : 0;
margin : 0;
width : 319px;
text-align : left;
}
#top h1 a, #top h1 a:link, #top h1 a:hover {
display : block;
font-size : 28px;
font-family : Tahoma, Verdana, Arial, sans-serif;
line-height : normal;
color : #c0220d;
text-decoration : none;
font-weight : 700;
}
#search {
position : absolute;
top : 190px;
right : 0;
height : 20px;
width : 180px;
```



```
margin : 0;
}
.search {
height : 20px;
}
.search .button {
float : right;
margin : 0;
width : 24px;
height : 20px;
padding : 0;
text-indent : -9999px;
background : transparent url(..images/search_but.gif) no-repeat top right;
}
#logo {
position : absolute;
top : 70px;
right : 0;
width : 500px;
}
#logo h1 {
text-align : center;
font-size : 25px;
margin : 0;
line-height : normal;
}
#logo a {
color : #ff7302;
font-weight : 700;
text-transform : uppercase;
text-decoration : none;
}
#header_wrapper {
height : 358px;
}
#header_img {
position : relative;
margin : 0 auto;
width : 960px;
height : 358px;
background : transparent url(..images/headerimg.jpg) no-repeat top center;
}
#flashnews {
position : absolute;
top : 234px;
right : 0;
width : 648px;
height : 112px;
overflow : hidden;
}
.cpathway {
margin : 0 auto;
width : 960px;
background : transparent url(..images/pathway.png) no-repeat top center;
}
```



```
span.breadcrumbs.pathway {
display : block;
height : 20px;
line-height : 13px;
padding : 4px 10px 0;
color : #223307;
}
span.breadcrumbs.pathway a.pathway {
text-decoration : none;
color : #248600;
text-decoration : underline;
}
span.breadcrumbs.pathway a.pathway:hover {
text-decoration : none;
}
#content {
width : 960px;
margin : 20px auto;
}
.c_middle {
background : transparent url(../images/content.gif) repeat-y top center;
}
.c_left {
background : transparent url(../images/content_left.gif) repeat-y top center;
}
.c_right {
background : transparent url(../images/content_right.gif) repeat-y top center;
}
.c_full {
background : #f1f2f2;
}
.bboxes {
position : absolute;
right : 0;
bottom : 20px;
width : 641px;
background : url(../images/boxes_bg.png) repeat-x center left;
}
.bboxes_r_bg {
padding : 5px 6px 6px 5px;
background : url(../images/boxes_r_bg.png) no-repeat center right;
}
.bboxes_bg {
background : #f9f9f9;
height : 157px;
}
.bboxes ul {
overflow : hidden;
text-align : left;
margin : 0;
padding : 4px 10px;
list-style : none;
}
.bboxes ul li a, .bboxes ul li a:link, .bboxes ul li a:visited {
display : block;
```



```
color : #666;
padding : 0 0 0 23px;
height : 22px;
line-height : 20px;
background : url(../images/boxes_li_bg.png) no-repeat center left;
text-decoration : none;
}
.bboxes ul.latestnews li a, .bboxes ul.latestnews li a:link, .bboxes ul.latestnews li a:visited {
background : url(../images/boxes_li_r_bg.png) no-repeat center left;
}
.bboxes ul li a:hover {
color : #888;
background : url(../images/boxes_li_hover_bg.png) no-repeat center left;
}
.bboxes ul.latestnews li a:hover {
background : url(../images/boxes_li_r_hover_bg.png) no-repeat center left;
}
.popular .module, .latest .module {
float : left;
width : 45%;
}
.popular .module {
width : 50%;
}
.latest .module {
margin : 0;
padding : 0 0 0 30px;
background : url(../images/module_divider.png) no-repeat center left;
}
.bboxes .latest h3, .bboxes .popular h3 {
height : 30px;
line-height : 29px;
font-weight : 700;
color : #fbfbfb;
font-size : 11px;
padding : 0 10px 2px;
margin : 0;
background : url(../images/boxes_h3_bg.png) repeat-x center left;
}
.bboxes .popular h3 {
margin : 0;
background : url(../images/boxes_popular_h3_bg.png) no-repeat top right;
}
.popular a, .popular a:link, .popular ul li a:visited, .latest a, .latest a:link, .latest ul li a:visited {
color : #d1d3d4;
text-decoration : none;
padding : 0 0 0 14px;
background : url(../images/module_bullet.gif) no-repeat top left;
}
.popular ul li a:hover, .latest ul li a:hover {
color : #efefef;
}
.popular ul li a:visited, .latest ul li a:visited {
color : #223307;
}
```



```
.onlyone {
width : 321px;
}
.bboxes .only .module {
width : 100%;
}
.bboxes .only h3 {
background : url(../images/boxes_h3_bg.png) repeat-x center left;
}
.bboxes div.module {
float : left;
background : none;
height : 157px;
width : 50%;
}
.bboxes div.module div, .bboxes div.module div div {
margin : 0;
}
.bboxes div.module div div div {
width : auto;
}
#leftcolumn, #rightcolumn {
float : left;
width : 210px;
margin : 0 10px 0 0;
}
#rightcolumn {
margin : 0 0 0 10px;
}
div#maincolumn {
float : left;
width : 498px;
padding : 10px;
}
div#maincolumn_full {
float : left;
width : 940px;
padding : 10px;
}
div#maincolumn_left {
float : left;
width : 720px;
padding : 10px;
}
div#maincolumn_right {
float : left;
width : 720px;
padding : 10px;
}
div.nopad {
overflow : hidden;
padding : 0;
}
div.nopad ul {
clear : both;
}
```



```
}
td.middle_pad {
width : 20px;
}
#banner_l {
text-align : left;
padding : 0 0 0 24px;
}
#footer {
width : 920px;
margin : 0 auto;
height : 28px;
text-align : center;
font-size : 11px;
color : #919191;
padding : 6px 0;
}
#footer a {
color : #4a4a4a;
font-size : 11px;
text-decoration : none;
}
#footer p {
margin : 0;
}
#footer a:hover {
text-decoration : underline;
}
#footer #sgf a.sgfooter:link, #footer #sgf a.sgfooter:visited {
color : #8e8e8e;
font-family : Tahoma, Arial, sans-serif;
text-decoration : none;
background : none;
padding : 0;
}
#footer #sgf a.sgfooter:hover {
color : #8e8e8e;
font-family : Tahoma, Arial, sans-serif;
text-decoration : none;
background : none;
padding : 0;
}
#sgf {
font-size : 11px;
text-align : center;
margin : 0 auto;
color : #8e8e8e;
font-family : Tahoma, Arial, sans-serif;
}
.sgf {
text-align : right;
font-size : 12px;
font-family : Tahoma, Arial, sans-serif;
color : #8e8e8e;
text-decoration : none;
}
```



```
}  
.sgf1 {  
font-size : 12px;  
font-family : Tahoma, Arial, sans-serif;  
color : #8e8e8e;  
text-align : left;  
}  
a.sglink:link, a.sglink:visited {  
color : #8e8e8e;  
font-size : 12px;  
font-family : Tahoma, Arial, sans-serif;  
text-decoration : none;  
}  
a.sglink:hover {  
color : #8e8e8e;  
font-family : Tahoma, Arial, sans-serif;  
text-decoration : none;  
}  
div.offline {  
background : #fffebb;  
width : 100%;  
position : absolute;  
top : 0;  
left : 0;  
font-size : 1.2em;  
padding : 5px;  
}  
div.componentheading {  
height : 22px;  
margin : 0;  
color : #586a3d;  
}  
h1 {  
padding : 0;  
font-family : Tahoma, Arial, sans-serif;  
font-size : 1.3em;  
font-weight : 700;  
vertical-align : bottom;  
color : #153a71;  
text-align : left;  
width : 100%;  
}  
h2, .contentheading {  
padding : 0;  
font-family : Tahoma, Verdana, Arial, sans-serif;  
font-size : 11px;  
vertical-align : middle;  
color : #fe8300;  
text-align : left;  
font-weight : 700;  
}  
h2, a.contentheading {  
background : none;  
border : none;  
margin : 6px 0;
```



```
}
table.contentpaneopen h3 {
margin-top : 25px;
}
h4 {
font-family : Tahoma, Arial, sans-serif;
color : #333;
}
table.contentpaneopen h3 {
color : #586a3d;
}
h3, .componentheading, table.moduletable th, legend {
margin : 0 0 10px 0;
font-family : Tahoma, Arial, sans-serif;
font-size : 11px;
font-weight : 700;
text-align : left;
text-transform : uppercase;
color : #fbfbfb;
padding : 0;
}
.small {
font-size : 10px;
color : #999;
font-weight : 700;
text-align : left;
}
.modifydate {
height : 20px;
vertical-align : bottom;
font-size : 10px;
color : #666;
text-align : right;
}
.createdate {
vertical-align : top;
font-size : 11px;
color : #999;
padding-bottom : 8px;
}
a.readon {
float : right;
background : url(../images/readon.png) no-repeat center left;
line-height : normal;
font-size : 11px;
padding : 0 0 0 14px;
color : #7c7c7c;
text-transform : lowercase;
text-decoration : none;
}
a.readon:hover {
text-decoration : underline;
}
.invalid {
border-color : #ff0000;
```




```
}
label.invalid {
color : #ff0000;
}
.ol-foreground {
background-color : #f1f1f1;
color : #333;
}
.ol-background {
background-color : #f1f1f1;
color : #333;
}
.ol-textfont {
font-family : Tahoma, Arial, sans-serif;
font-size : 10px;
}
.ol-captionfont {
font-family : Tahoma, Arial, sans-serif;
font-size : 12px;
color : #f6f6f6;
font-weight : 700;
}
.ol-captionfont a {
background-color : #f1f1f1;
color : #333;
text-decoration : none;
font-size : 12px;
}
a.mainlevel:link, a.mainlevel:visited {
padding-left : 5px;
}
span.article_separator {
display : block;
height : 20px;
}
td.buttonheading {
text-align : right;
width : 0;
}
.clr {
clear : both;
}
table.blog span.article_separator {
display : block;
height : 20px;
}
table.contenttoc {
margin : 5px;
padding : 5px;
background : none;
}
table.contenttoc td {
padding : 0 5px;
}
td.sectiontableheader {
```



```
color : #999;
font-weight : 700;
padding : 4px;
}
tr.sectiontableentry1 td {
padding : 4px;
}
tr.sectiontableentry1 {
background : #e5e6e7;
}
tr.sectiontableentry0 td, tr.sectiontableentry2 td {
padding : 4px;
}
td.sectiontableentry0, td.sectiontableentry1, td.sectiontableentry2 {
padding : 3px;
font-size : 11px;
}
.contentpaneopen, table.contentpane {
margin : 0;
padding : 0;
}
table.contentpane td {
text-align : left;
}
table.contentpane td.contentdescription {
width : 100%;
}
table.contentpane {
text-align : left;
float : left;
width : 100%;
}
table.contentpane ul li a .category {
color : #ff8800;
}
table.contentpane ul li {
color : #666;
}
table.contentpaneopen {
margin : 0 4px;
border-collapse : collapse;
}
table.contentpaneopen li {
margin-bottom : 5px;
}
table.contentpaneopen fieldset {
border : 0;
border-top : 1px solid #669933;
}
table.contentpaneopen h3 {
margin-top : 25px;
}
table.contentpaneopen h4 {
font-family : Tahoma, Arial, sans-serif;
color : #669933;
```



```
}
.highlight {
background-color : #fffebb;
}
ul.latestnews, ul.mostread {
list-style : none;
padding : 0;
margin : 0;
text-align : left;
}
table.user1user2 div.moduletable {
margin-bottom : 0;
}
div.moduletable, div.module {
margin-bottom : 25px;
}
div.module_menu, div.module, div.module_text {
margin : 0;
padding : 0;
}
div.module_menu div div div, div.module div div div, div.module_text div div div {
margin : 0 auto 10px;
padding : 0;
text-align : center;
}
div.module div div div div {
width : 160px;
color : #767676;
}
div.module_menu div div div div, div.module div div div div, div.module_text div div div div {
background : none;
margin : 0 auto;
padding : 0;
}
div.module_text div div div div {
text-align : left;
}
div.module_text div div div div.bannergroup_text {
padding : 10px 10px 10px 20px;
width : 174px;
}
div.module_text div div div div.bannergroup_text div {
color : #767676;
width : auto;
padding : 0 0 4px;
}
div.module div div div form {
margin : 0 auto;
padding : 0 0 0 20px;
text-align : left;
width : 188px;
}
div.module_menu ul {
list-style : none;
padding : 0;
```



```
}
div.module_menu ul#mainlevel {
margin : 0 auto;
text-align : center;
}
div.module_menu ul li {
margin : 0;
padding : 0;
}
div.module_menu ul li a:link, div.module_menu ul li a:visited {
font-weight : 700;
background : transparent url(../images/blue/bullet2.jpg) no-repeat top left;
padding : 2px 0;
line-height : 24px;
}
#leftcolumn div.module table td, #rightcolumn div.module table td {
margin : 0;
padding : 0 6px 0 0;
height : 20px;
color : #6d6e71;
text-align : left;
line-height : 13px;
vertical-align : middle;
}
#leftcolumn div.module table.poll td {
text-align : left;
}
#leftcolumn h3, #rightcolumn h3 {
width : 182px;
height : 26px;
line-height : 25px;
padding : 0 14px;
margin : 0 0 10px 0;
color : #e6e7e8;
font-size : 11px;
text-align : left;
text-transform : uppercase;
font-weight : 700;
overflow : hidden;
background : url(../images/box_h3.png) no-repeat top left;
}
#leftcolumn .moduletable_menu, #leftcolumn .moduletable, #leftcolumn .moduletable_text, #leftcolumn .c,
#rightcolumn .moduletable_menu, #rightcolumn .moduletable, #rightcolumn .moduletable_text,
#rightcolumn .c {
margin : 0 0 16px 0;
padding : 0 0 8px 0;
}
#leftcolumn ul.menu, #rightcolumn ul.menu {
width : 210px;
list-style : none;
text-align : left;
margin : 0;
}
#rightcolumn ul.menu {
margin : 0 10px 0 0;
```



```
}
#leftcolumn ul.menu li, #rightcolumn ul.menu li {
margin : 0 0 1px 0;
}
#leftcolumn ul.menu li:hover {
background : #e5e6e7;
}
#leftcolumn ul.menu li ul li, #rightcolumn ul.menu li ul li {
border-bottom : none;
}
#leftcolumn ul.menu li a, #leftcolumn ul.menu li a:link, #rightcolumn ul.menu li a, #rightcolumn ul.menu li
a:link {
display : block;
font-weight : 700;
font-size : 11px;
line-height : 21px;
height : 22px;
padding : 0 0 0 24px;
text-decoration : none;
color : #6d6e71;
background : url(..images/menu_arrow.gif) no-repeat 10px center;
}
#rightcolumn ul.menu li a, #rightcolumn ul.menu li a:link {
background : transparent url(..images/menu_arrow_r.gif) no-repeat 10px center;
}
#leftcolumn ul.menu li a:hover, #rightcolumn ul.menu li a:hover {
color : #fe8300;
background : #e5e6e7 url(..images/menu_arrow_hover.gif) no-repeat 10px center;
}
#leftcolumn ul.menu li#current a, #leftcolumn ul.menu li#current a:link, #rightcolumn ul.menu li#current a,
#rightcolumn ul.menu li#current a:link {
display : block;
color : #fe8300;
background : #e5e6e7 url(..images/menu_arrow_hover.gif) no-repeat 10px center;
}
#leftcolumn ul.menu li#current {
background : #e5e6e7;
}
#leftcolumn ul.menu li#current a:hover, #rightcolumn ul.menu li#current a:hover {
color : #fe8300;
background : url(..images/menu_arrow_hover.gif) no-repeat 10px center;
}
#leftcolumn ul.menu li#current ul li a, #leftcolumn ul.menu li#current ul li a:link, #rightcolumn ul.menu
li#current ul li a, #rightcolumn ul.menu li#current ul li a:link {
font-weight : 700;
font-size : 11px;
height : 22px;
line-height : 21px;
padding : 0 0 0 38px;
text-decoration : none;
color : #6d6e71;
background : url(..images/menu_arrow.gif) no-repeat 24px center;
}
#rightcolumn ul.menu li#current ul li a, #rightcolumn ul.menu li#current ul li a:link {
background : url(..images/menu_arrow_r.gif) no-repeat 24px center;
```



```
}
#leftcolumn ul.menu li ul li#current a, #leftcolumn ul.menu li ul li#current a:link, #leftcolumn ul.menu li ul
li#current a:visited, #leftcolumn ul.menu li ul li#current a:hover, #rightcolumn ul.menu li ul li#current a,
#rightcolumn ul.menu li ul li#current a:link, #rightcolumn ul.menu li ul li#current a:visited, #rightcolumn
ul.menu li ul li#current a:hover {
padding : 0 0 0 38px;
color : #fe8300;
font-weight : 700;
background : url(../images/menu_arrow_hover.gif) no-repeat 24px center;
}
#leftcolumn ul.menu li.parent ul li a, #rightcolumn ul.menu li.parent ul li a {
font-size : 11px;
font-weight : 700;
line-height : 18px;
height : 22px;
line-height : 21px;
padding : 0 0 0 38px;
color : #6d6e71;
text-decoration : none;
background : url(../images/menu_arrow.gif) no-repeat 24px center;
}
#rightcolumn ul.menu li.parent ul li a {
background : url(../images/menu_arrow_r.gif) no-repeat 24px center;
}
#leftcolumn ul.menu li.parent ul li a:hover {
color : #fe8300;
background : url(../images/menu_arrow_hover.gif) no-repeat 24px center;
}
#leftcolumn ul.menu li#current ul {
margin : 0;
padding : 0;
}
#leftcolumn ul.menu li#current ul li {
margin : 0;
padding : 0;
}
#leftcolumn ul.menu li ul {
margin : 0;
padding : 0;
}
#leftcolumn ul.menu li#current ul li a:hover {
color : #fe8300;
background : url(../images/menu_arrow_hover.gif) no-repeat 24px center;
}
#leftcolumn ul.menu li ul, #rightcolumn ul.menu li ul {
list-style : none;
margin : 0;
}
#leftcolumn .moduletable ul, #rightcolumn .moduletable ul {
margin : 6px 0;
padding : 0;
list-style : none;
}
#leftcolumn .moduletable ul li, #rightcolumn .moduletable ul li {
margin : 0;
```



```
padding : 0 2px;
}
table.adminform textarea {
width : 540px;
height : 400px;
font-size : 1em;
color : #000099;
}
form#form-login fieldset {
border : 0 none;
padding : 0;
margin : 0;
color : #767676;
text-align : left;
}
form#form-login ul {
padding : 0;
list-style : none;
text-align : left;
width : 180px;
margin : 10px auto 0;
}
form#form-login ul li {
padding : 0;
}
form#form-login ul li a {
text-align : left;
padding : 0;
font-size : 11px;
color : #767676;
text-decoration : none;
}
form#form-login ul li a:hover {
text-decoration : underline;
}
#form-login input {
border : 1px solid #b9b9ba;
color : #767676;
font-size : 11px;
height : 16px;
line-height : 15px;
padding : 2px 10px;
background : #e5e6e7 none repeat scroll 0 0;
}
input#modlgn_passwd, input#modlgn_username {
width : 150px;
}
input.button, #form-login input.button {
height : 22px;
color : #e6e7e8;
line-height : 21px;
padding : 0 6px 4px;
border : none;
background : transparent url(../images/but.gif) repeat-x top left;
}
```



```
input.button:hover, #form-login input.button:hover {
color : #409622;
}
div.mosimage {
margin : 5px;
}
div.mosimage_caption {
font-size : 0.9em;
color : #333;
}
div.caption {
padding : 0 10px 0 10px;
}
div.caption img {
border : 1px solid #ccc;
}
div.caption p {
font-size : 0.9em;
color : #333;
text-align : center;
}
table.paramlist {
margin-top : 5px;
}
table.paramlist td.paramlist_key {
width : 128px;
text-align : left;
height : 30px;
}
div.message {
font-family : Tahoma, Arial, sans-serif;
font-weight : 700;
font-size : 14px;
color : #c30;
text-align : center;
width : auto;
background-color : #f9f9f9;
border : 1px solid #d5d5d5;
margin : 3px 0 10px;
padding : 3px 20px;
}
.banneritem_text {
padding : 4px;
font-size : 11px;
}
.banneritem_text a {
color : #fe8300;
}
.bannerfooter_text {
padding : 4px;
font-size : 11px;
text-align : right;
}
.pagination span {
padding : 2px;
```




```
}
.pagination a {
padding : 2px;
}
.pollstableborder td {
text-align : left;
}
fieldset {
border : 1px solid #ccc;
margin-top : 15px;
padding : 4px;
}
legend {
margin : 0;
padding : 0 10px;
}
td.key {
border-bottom : 1px solid #eee;
color : #333;
}
.tool-tip {
float : left;
background : #ffc;
border : 1px solid #d4d5aa;
padding : 5px;
max-width : 200px;
}
.tool-title {
padding : 0;
margin : 0;
font-size : 100%;
font-weight : 700;
margin-top : -15px;
padding-top : 15px;
padding-bottom : 5px;
background : url(../system/images/selector-arrow.png) no-repeat;
}
.tool-text {
font-size : 100%;
margin : 0;
}
#system-message dd.message ul {
padding : 0;
margin : 0;
background : none;
border : none;
}
#system-message dd.error ul {
color : #c00;
background : none;
border : none;
padding : 0;
margin : 0;
}
#system-message dd.notice ul {
```



```
color : #c00;
background : none;
border : none;
padding : 0;
margin : 0;
}
#system-message dd {
text-indent : 0;
}
#system-message dd ul {
list-style-type : none;
color : #c00;
background : none;
border : none;
}
#system-message {
margin-top : 5px;
}
```

A.2.2 Incident Report

No error found. Everything working as expected.

A.3 Log for test 3: Links

A.3.1 Test Results

Processing <http://ficus.xtilos.com>

List of broken links and other issues

There are issues with the URLs listed below. The table summarizes the issues and suggested actions by HTTP response status code.

Code	Occurrences	What to do
(N/A)	10	The link was not checked due to robots exclusion rules . Check the link manually, and see also the link checker documentation on robots exclusion .



Line: 14 <http://ficus.xtilos.com/media/system/js/caption.js>

Status: (N/A) Forbidden by robots.txt

The link was not checked due to robots exclusion rules. Check the link manually.



Line: 16 <http://ficus.xtilos.com/templates/system/css/system.css>

Status: (N/A) Forbidden by robots.txt

The link was not checked due to robots exclusion rules. Check the link manually.



Line: 49 <http://ficus.xtilos.com/images/gym.jpg>

Status: (N/A) Forbidden by robots.txt

The link was not checked due to robots exclusion rules. Check the link manually.



Line: 132 http://ficus.xtilos.com/images/M_images/pdf_button.png

Status: (N/A) Forbidden by robots.txt

The link was not checked due to robots exclusion rules. Check the link manually.



Line: 13 <http://ficus.xtilos.com/media/system/js/mootools.js>

Status: (N/A) Forbidden by robots.txt

The link was not checked due to robots exclusion rules. Check the link manually.



Line: 38 <http://ficus.xtilos.com/images/gym1.jpg>

Status: (N/A) Forbidden by robots.txt

The link was not checked due to robots exclusion rules. Check the link manually.



Line: 138 http://ficus.xtilos.com/images/M_images/emailButton.png

Status: (N/A) Forbidden by robots.txt

The link was not checked due to robots exclusion rules. Check the link manually.



Line: 17 <http://ficus.xtilos.com/templates/siteground-j15-82/css/template.css>

Status: (N/A) Forbidden by robots.txt

The link was not checked due to robots exclusion rules. Check the link manually.



Line: 135 http://ficus.xtilos.com/images/M_images/printButton.png

Status: (N/A) Forbidden by robots.txt



The link was not checked due to robots exclusion rules. Check the link manually.



Line: 12 <http://ficus.xtilos.com/templates/siteground-j15-82/favicon.ico>

Status: (N/A) Forbidden by robots.txt

The link was not checked due to robots exclusion rules. Check the link manually.

List of redirects

The links below are not broken, but the document does not use the exact URL, and the links were redirected. It may be a good idea to link to the final location, for the sake of speed.



Line: 22 http://ficus.xtilos.com/index.php?option=com_virtuemart&Itemid=54 redirected to http://ficus.xtilos.com/index.php?option=com_virtuemart&Itemid=54&vmcchk=1&Itemid=54

Status: 301 -> 200 OK

This is a permanent redirect. The link should be updated.

Anchors

Found 21 anchors.

Valid anchors!

Checked 1 document in 24.54 seconds.

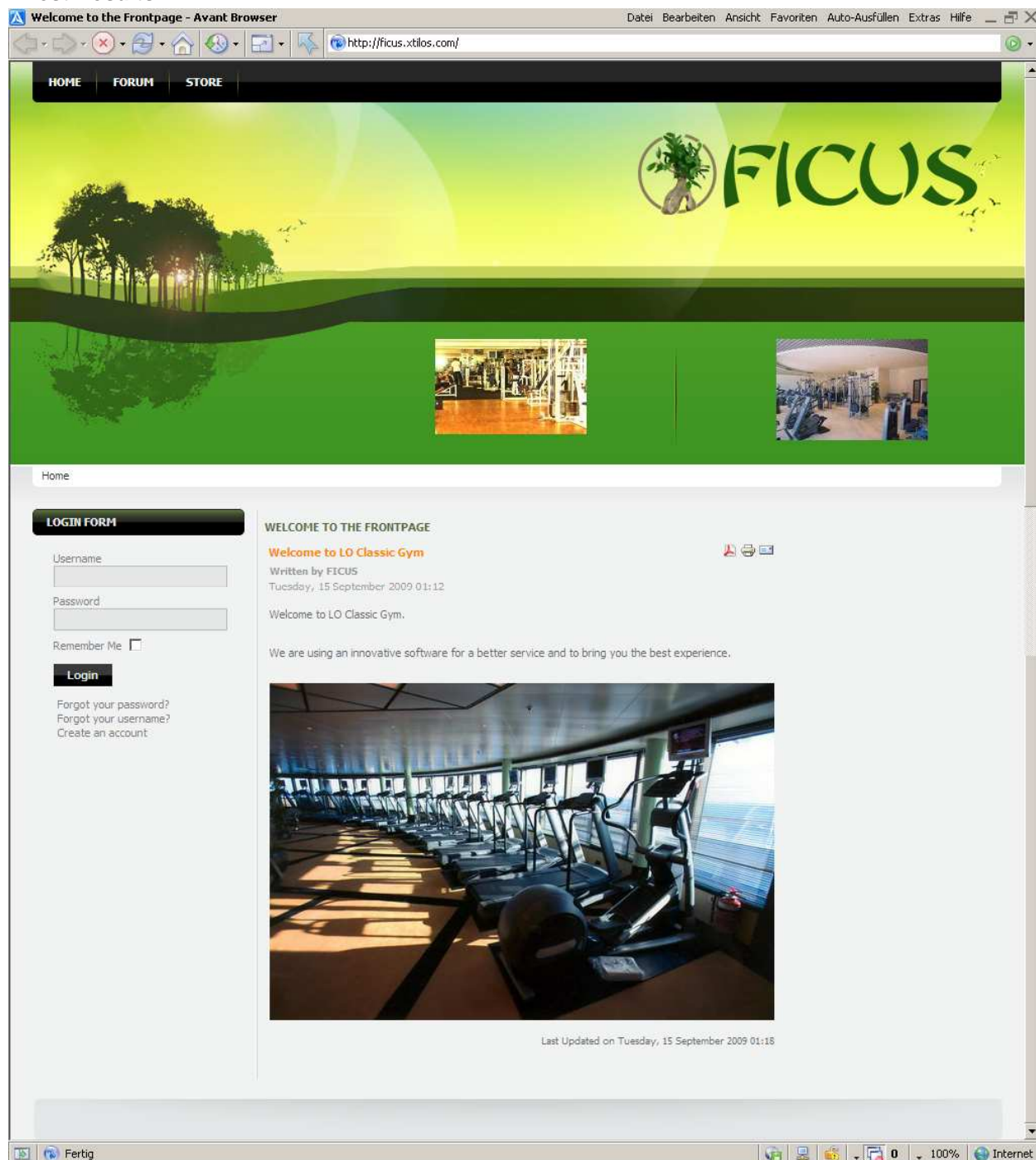
A.3.2 Incident Report

No Error Found. Warnings will be fix on maintenance.



A.4 Log for test 4: Browser Independence

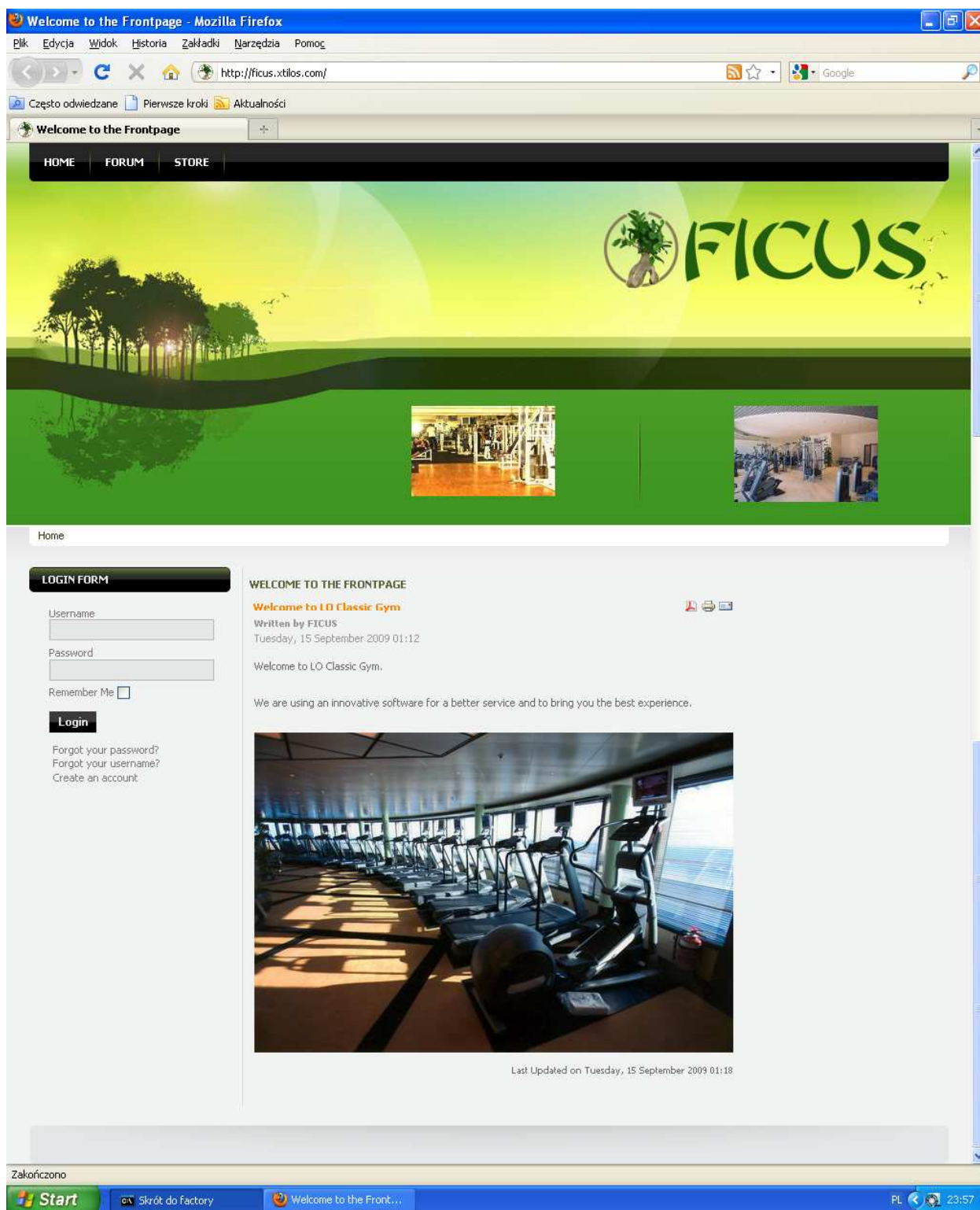
A.4.1 Test Results



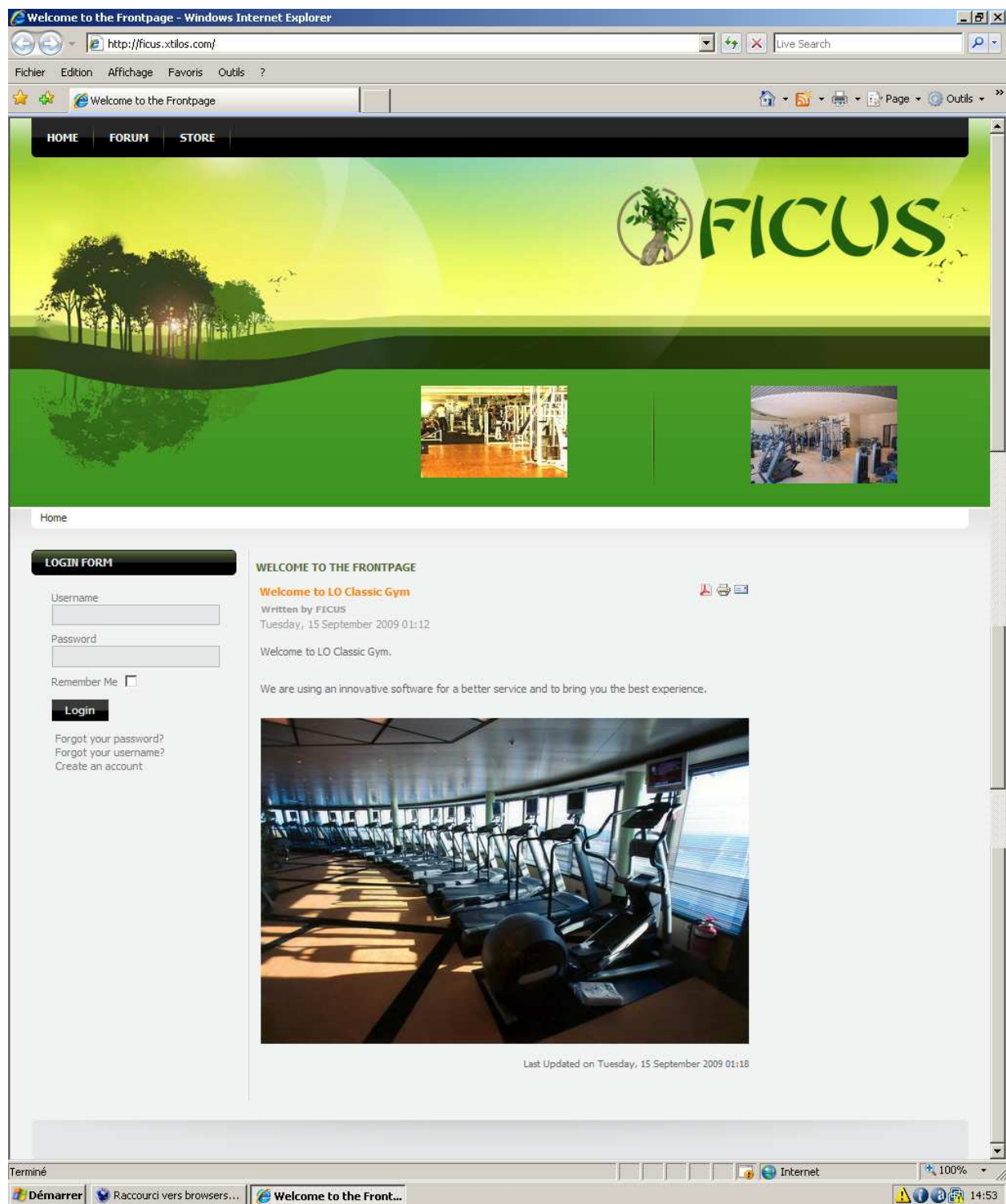
Avant 11.7 on Windows XP



Google Chrome 3.0 on Windows XP



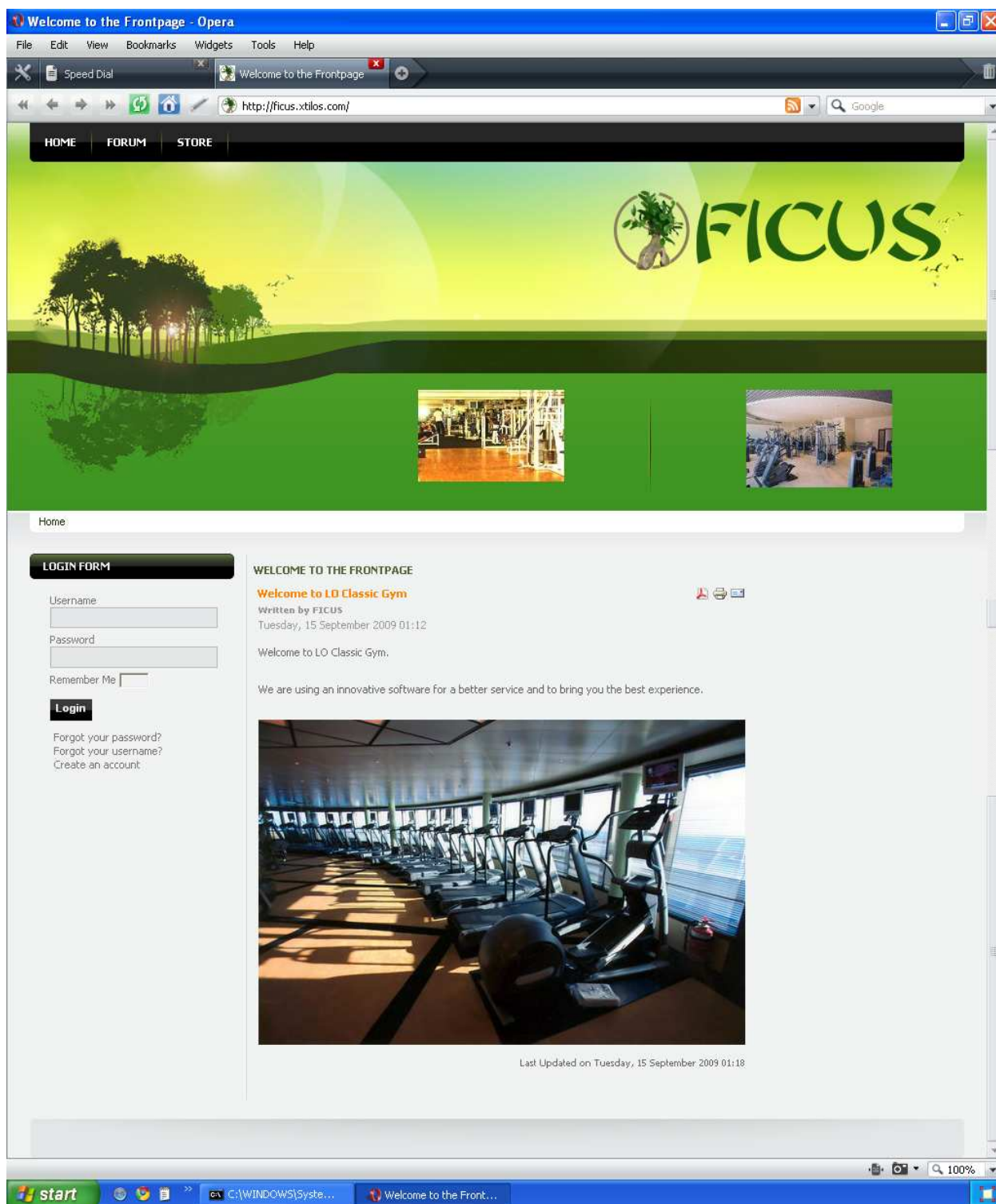
Firefox 3.5 on Windows XP



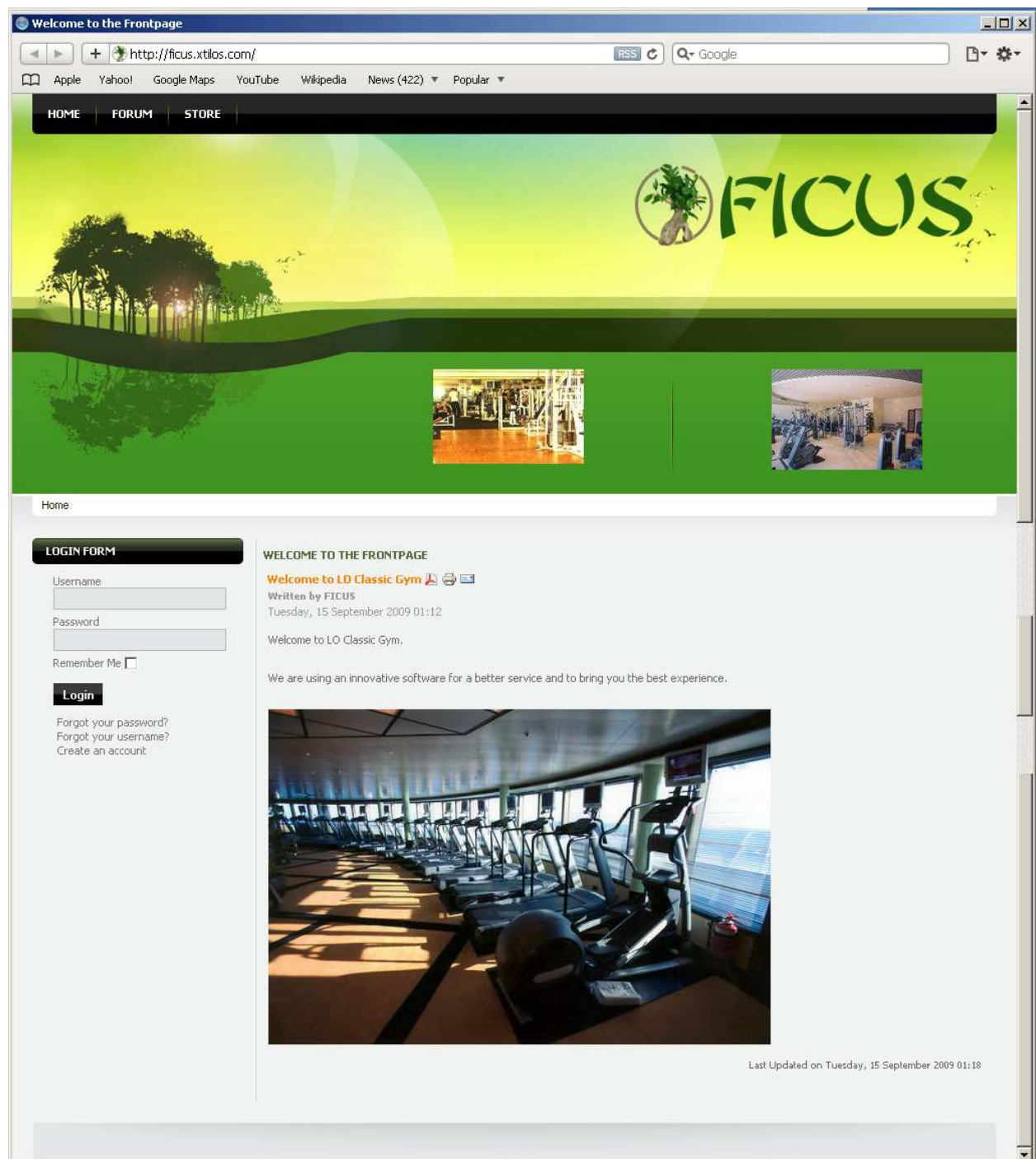
Microsoft Internet Explorer 7.0 on Windows XP



Microsoft Internet Explorer 8.0 on Windows XP



Opera 10.0 on Windows XP



Safari 4.0.3 on Windows XP

A.4.2 Incident Report

The webpage performed as expected in the different browsers: Avant, Chrome, Firefox, Flock, MSIE, Opera & Safari



A.5 Log for test 5: Speed and Performance

A.5.1 Test Results

Website test results

URL tested: http://ficus.xtilos.com
Test performed from: Seattle, WA
Test performed at: 2009-10-26 18:41:47 (GMT -04:00)
Resolved As: 68.171.208.148
Status: OK
Response Time: 0.616 sec
DNS: 0.158 sec
Connect: 0.058 sec
Redirect: 0.000 sec
First byte: 0.341 sec
Last byte: 0.059 sec
Size: 6796 bytes

Web Page Test results

URL tested: <http://ficus.xtilos.com>
Test performed from: Seattle, WA
Test performed at: 2009-10-26 15:42:34 (GMT -07:00)

#	URL	Status	Time	DNS (sec)	Conn ect (sec)	Redir ect (sec)	First (sec)	Last (sec)	Tota l (sec)	Size (Kb)
1	http://ficus.xtilos.com/	OK	15:42:34	0.00 10	0.05 80	0.00 00	0.32 21	0.06 04	0.44 14	6.64
2	ficus.xtilos.com/templates/sitegroup-j15-82/favicon.ico	OK	15:42:35	0.00 00	0.00 00	0.00 00	0.08 05	0.11 66	0.19 71	17.7 5
3	ficus.xtilos.com/media/system/js/mootools.js	OK	15:42:35	0.00 00	0.00 00	0.00 00	0.13 51	0.17 90	0.31 41	72.6 6
4	ficus.xtilos.com/media/system/js/caption.js	OK	15:42:35	0.00 00	0.00 00	0.00 00	0.06 14	0.00 00	0.06 15	1.68
5	ficus.xtilos.com/templates/system/css/system.css	OK	15:42:35	0.00 00	0.00 00	0.00 00	0.05 92	0.00 01	0.05 93	1.35
6	ficus.xtilos.com/templates/sitegroup-j15-82/css/template.css	OK	15:42:35	0.00 00	0.00 00	0.00 00	0.05 98	0.00 28	0.06 26	23.0 2
7	ficus.xtilos.com/images/gym1.jpg	OK	15:42:35	0.00 00	0.00 00	0.00 00	0.07 27	0.00 04	0.07 31	5.14



8	ficus.xtilos.com/images/gym.jpg	OK	15:42:35	0.00 00	0.00 00	0.00 00	0.07 23	0.00 03	0.07 26	4.07
9	ficus.xtilos.com/images/M_images/pdf_button.png	OK	15:42:36	0.00 00	0.00 00	0.00 00	0.07 68	0.00 01	0.07 68	0.57
10	ficus.xtilos.com/images/M_images/printButton.png	OK	15:42:36	0.00 00	0.00 00	0.00 00	0.07 49	0.00 01	0.07 50	0.37
11	ficus.xtilos.com/images/M_images/emailButton.png	OK	15:42:36	0.00 00	0.00 00	0.00 00	0.05 93	0.00 01	0.05 94	0.42
12	z.about.com/d/cruises/1/0/2/k/3/Gym.jpg	OK	15:42:36	0.32 68	0.01 96	0.00 00	0.08 14	0.06 11	0.48 88	60.8 2
Total		-	-	0.32 78	0.07 76	0.00 00	1.15 55	0.42 10	1.98 17	194. 48

HTTP Headers Test

Domain tested: ficus.xtilos.com
Test performed from: Seattle, WA
Test performed at: 2009-10-26 15:44:51 (GMT -07:00)
Status: OK
Response Time: 0.394 sec
DNS: 0.001 sec
Connect: 0.058 sec
Redirect: 0.000 sec
First byte: 0.335 sec
Last byte: 0.000 sec

HTTP Header:

HTTP/1.1 200 OK
Date: Mon, 26 Oct 2009 22:44:31 GMT
Server: Apache/2.0.63 (Unix) mod_ssl/2.0.63 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1
mod_bwlimited/1.4
FrontPage/5.0.2.2635
X-Powered-By: PHP/5.2.8
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Expires: Mon, 1 Jan 2001 00:00:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: d157b0d011c92187f7ec5eee84130266=6b9598798467bfa525d71b1048692d44
Last-Modified: Mon, 26 Oct 2009 22:44:31 GMT
Transfer-Encoding: chunked
Content-Type: text/html

A.5.2 Incident Report

The webpage and all of it's components have an excellent performance.

