Wisec - The WIse SECurity

Wisec - The WIse SECurity - Stefano Di Paola, wisec.it.

- Published: date not stated
- Original: <http://www.wisec.it/sectou.php?id=4698ebdc59d15>
- Preserved from: http://www.wisec.it/sectou.php?id=4698ebdc59d15 (stored) on 2026-08-16
- Licence: unknown

Content

> UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

Wisec - The WIse SECurity

THP Wisec USH DigitalBullets TheHackersPlace network

|

[image: image]

The ***WI***se ***SEC***urity

| .italian .english | |

Wisec Home SecSearch Projects Papers Security Thoughts

| News

Flash Application Testing: A New Vector for XSS and Cross Site Flashing.

IE and Firefox Digest Authentication Request Splitting.

Php import_req_var globals overwrite Advisory.

Subverting Ajax - The Paper.

Adobe Plugin Multiple Vulnerabilities.

Wisec@23rd.CCC Congress in Berlin - 29th Dec. 2006 - Subverting Ajax.

SecSearch. Search Engine for Security Community.

Mysql COM_TABLE_DUMP Flaws.

Mysql Anonymous login Flaw.

A new project to stop embed passwords in Php scripts: PassBroker.

MySQL new three vulnerabilities unleashed

PHP shmop safemode bypass

PHP RFC1867 Vuln - POC Released!

Search on Wisec

[image: Google]

|

Security Thoughts

[Back]

Saturday, July 14, 2007, 17:26

Multiviews Apache, Accept Requests and free listing

This is a small post about a way to easily get backup files on Apache web servers with MultiViews option enabled. I really don't know if this is a known attack technique, but IMO it should be implemented in every web scanner and it should be added in the OWASP Testing Guide - section Information Gathering.

Let's start:

MultiViews is an Apache option which acts with the following rules:

> if the server receives a request for /some/dir/foo, if /some/dir has MultiViews enabled, and /some/dir/foo does not exist, then the server reads the directory looking for files named foo.*, and effectively fakes up a type map which names all those files, assigning them the same media types and content-encodings it would have if the client had asked for one of them by name. It then chooses the best match to the client's requirements.

How the best match is chosen by Apache? It depends on several Accept* headers in the client Request.**

> Accept Accept-Language Accept-Encoding

Let's see how it works:

Let's suppose i just saved an backup copy of my index.php on a Web Server with the MultiView option enabled.

If an attacker requests "index" without any extension:

> GET /index HTTP/1.1 Host: myhost Accept: /

the web server will reply with:

> HTTP/1.1 200 OK Date: Sat, 14 Jul 2007 14:46:22 GMT Server: Apache/2.0.55 (Ubuntu) Content-Location: index.php Vary: negotiate,accept TCN: choice Last-Modified: Sat, 14 Jul 2007 10:58:38 GMT ETag: "8d15d-0-1c1d5380;498a0540" Accept-Ranges: bytes Content-Length: #ofBytes Content-Type: text/html; charset=UTF-8

Now, it could be noticed that in the server response several interesting headers are out:

> Content-Location: index.php Vary: negotiate,accept TCN: choice

This means there is MultiViews enabled on / directory.

Let's see if in the request we use a "Accept:" header with an inexistent mime type:

> GET /index HTTP/1.1 Host: myhost Accept: application/whatever; q=1.0

the server will reply with:

> HTTP/1.1 406 Not Acceptable Date: Sat, 14 Jul 2007 14:51:29 GMT Server: Apache/2.0.55 (Ubuntu) Alternates: {"index.bak" 1 {type application/x-trash} {length 3}}, {"index.php" 1 {type application/x-httpd-php} {length 3}} Vary: negotiate,accept TCN: list Content-Length: NNNN Content-Type: text/html; charset=iso-8859-1 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"> <html><head> <title>406 Not Acceptable</title> </head><body> <h1>Not Acceptable</h1> An appropriate representation of the requested resource /index could not be found on this server. Available variants: <ul> index.php , type text/html index.bak , type application/x-trash <hr>

aha! With a single request we get a listing of all the files! And for free..as in free speech ;)

Well, ok. Not really *all* the files but every file with the same name requested and with an extension listed in mime-types file.

This means that if index.whatever is on the server it won't be listed.

Obviously an attacker could request every known extension for index.* but it would be a bit noisy, isn't it?

As usual i prefer to leave discussion open than give everything i think on the subject...so feel free to leave a comment. ...as in free beer :)

Tim Brown, Saturday, July 14, 2007, 18:40

nEUrOO, Monday, July 16, 2007, 22:12

Bunyamin Demir, Tuesday, July 17, 2007, 13:02

Comments are disabled

Wisec is brought to you by...

Wisec is written and mantained by Stefano Di Paola.

Wisec uses open standards, including XHTML, CSS2, and XML-RPC.

| |