# 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=472f952d79293>
- Preserved from: http://www.wisec.it/sectou.php?id=472f952d79293 (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 ]

Monday, November 05, 2007, 22:54

Bursting Performances in Blind SQL Injection - Take 2 (Bandwidth)

Today my colleague Giorgio Fedon of Minded Security, talked me about an idea regarding how to save bandwidth while exploiting blind SQL Injection. His question was:

> "When a pentester is trying to get the content of a DB by exploiting a blind injection how can s/he get the content-length header without effectively getting all the response body, so that s/he can save time and bandwidth?"

My answer was: "use HEAD! (in both senses :)" It came out that RFC says it's not possible to use it. Infact, Apache doesn't satisfy a HEAD request with Content-Length header in response.

> HEAD /index.php HTTP/1.1 Host: 127.0.0.1 Accept: / HTTP/1.1 200 OK Date: Mon, 05 Nov 2007 21:00:07 GMT Server: Apache Content-Type: text/html

See? no Content-Length in response even if my localhost home page is 90 bytes long (as Rfc suggests). Let's try it with Range header:

> GET /index.php HTTP/1.1 Host: 127.0.0.1 Accept: / Range: bytes=-1 HTTP/1.1 206 Partial Content Date: Mon, 05 Nov 2007 21:03:15 GMT Server: Apache Content-Range: bytes 89-89/90 Content-Length: 1 Content-Type: text/html

Ahhhh, so the Range header in a request will fullfill my request without sending me the whole body but with a Content-Range which shows me how big would be the body itself.

Unfortunately, not all Web Servers acts the same. IIS 6.0 doesn't follow HTTP 1.1 Rfc and simply sends the whole body in response to GET or POST requests. But..Yes there is a but. HEAD requests are fullfilled with the right Content-Length:

> HEAD /search.aspx HTTP/1.1 Host: 127.0.0.1 Accept: / Content-Length: 22 search=all'+AND+'1'='1 HTTP/1.1 200 OK Date: Mon, 05 Nov 2007 21:14:00 GMT Server: Microsoft-IIS/6.0 X-Powered-By: ASP.NET Content-Length: 4790 Content-Type: text/html Expires: Mon, 05 Nov 2007 21:14:00 GMT Set-Cookie: ASPSESSIONIDSQTCRTQA=XXXXXXXXXXXXXXXXXXX; path=/ Cache-control: private

This means that we get the length of the response body even when there's no body in response.

How to use these infos? By improving blind sql injection tools.

Often blind sql injection tools use the differences in response bodies to understand if the sql injection accomplishes a true or false response. Using Content-Length or Content-Range could improve performances a lot.

The following look up table is for server and method:

```
SERVER     METHOD   RANGE

IIS 6.0    HEAD

APACHE     GET/POST  X

IBM HTTP   GET/POST  X

WEBSPHERE  GET/POST  X
```

We (me and Giorgio) hope some reader will provide informations about other web servers.

**Giorgio**, Monday, November 05, 2007, 23:16

**Stefano**, Monday, November 05, 2007, 23:29

**floyd**, Thursday, September 16, 2010, 15:17

**Stefano**, Thursday, September 16, 2010, 16:25

**Comments are disabled**

Admin login | This weblog is from www.mylittlehomepage.net

# 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.

| |