<get_results_response status="200" status_text="OK"><result id="346f02b4-8fd9-460e-b41f-ce6dde3a4982"><name>
creation_time>2024-08-04T09:43:10Z</creation_time><modification_time>2024-08-04T09:43:10Z</modification_time
29-4cce-a699-5265b947c89a"><name>metasploit</name></task><user_tags><count>0</count></user_tags><host>
t>general/CPE-T</port><nvt oid="1.3.6.1.4.1.25623.1.0.810002"><type>nvt</type><name>CPE Inventory</name><fa
bid>NOBID</bid><xref>URL:http://cpe.mitre.org/</xref><tags>cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:N|summ
CPE identities of operating systems, services and
applications detected during the scan.|qod_type=remote_banner</tags><cert></cert></nvt><scan_nvt_version>$R
verity><qod><value>80</value><type>remote_banner</type></qod><description>192.168.1.14|cpe:/a:apache:http_
192.168.1.14|cpe:/a:beasts:vsftpd:2.3.4
192.168.1.14|cpe:/a:isc:bind:9.4.2
192.168.1.14|cpe:/a:jquery:jquery
192.168.1.14|cpe:/a:mysql:mysql:5.0.51a
192.168.1.14|cpe:/a:openbsd:openssh:4.7p1
192.168.1.14|cpe:/a:php:php:5.2.4
192.168.1.14|cpe:/a:phpmyadmin:phpmyadmin:3.1.1
192.168.1.14|cpe:/a:postfix:postfix
192.168.1.14|cpe:/a:postgresql:postgresql:8.3.1
192.168.1.14|cpe:/a:proftpd:proftpd:1.3.1
192.168.1.14|cpe:/a:samba:samba:3.0.20
192.168.1.14|cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
192.168.1.14|cpe:/a:twiki:twiki:01.Feb.2003
192.168.1.14|cpe:/a:unrealircd:unrealircd:3.2.8.1
192.168.1.14|cpe:/a:x.org:x11:11.0
192.168.1.14|cpe:/o:canonical:ubuntu_linux:8.04</description><original_threat>Log</original_threat><original_seve
result><result id="58601023-5005-4e38-bd55-838a2c6c27c9"><name>SSH Brute Force Logins With Default Credenti
reation_time>2024-08-04T09:43:10Z</creation_time><modification_time>2024-08-04T09:43:10Z</modification_time
9-4cce-a699-5265b947c89a"><name>metasploit</name></task><user_tags><count>0</count></user_tags><host>1
>22/tcp</port><nvt oid="1.3.6.1.4.1.25623.1.0.103239"><type>nvt</type><name>SSH Brute Force Logins With Defau
se>7.5</cvss_base><cve>NOCVE</cve><bid>NOBID</bid><xref>NOXREF</xref><tags>cvss_base_vector=AV:N/AC:L/A
ing default credentials.

As the NVT 'SSH Brute Force Logins with default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013) might
timeout the actual reporting of this vulnerability takes place in this NVT instead. The script preference 'Repor
allows you to configure if such an timeout is reported.|solution=Change the password as soon as possible.|vuldete
SSH protocol.|solution_type=Mitigation|qod_type=remote_active</tags><cert></cert></nvt><scan_nvt_version>$Re
verity><qod><value>95</value><type>remote_active</type></qod><description>It was possible to login with the fol

msfadmin:msfadmin
user:user</description><original_threat>High</original_threat><original_severity>7.5</original_severity><notes></n
-925e-6077ab317528"><name>Possible Backdoor: Ingreslock</name><owner><name>admin</name></owner><co
me>2024-08-04T09:39:01Z</modification_time><report id="42a0103d-ec5d-4ea9-8c29-b5c401e78851"/><task id="f8
s><count>0</count></user_tags><host>192.168.1.14<asset asset_id="89b2b59d-c441-4a26-a817-8db895e501db"/><
</type><name>Possible Backdoor: Ingreslock</name><family>Gain a shell remotely</family><cvss_base>10.0</cvss
vector=AV:N/AC:L/Au:N/C:C/I:C/A:C|summary=A backdoor is installed on the remote host|impact=Attackers can exp
context of the application. Successful attacks will compromise the affected isystem.|qod_type=remote_vul|solution
ion: 11327 $</scan_nvt_version><threat>High</threat><severity>10.0</severity><qod><value>99</value><type>rem
' command with the following response: uid=0(root) gid=0(root)</description><original_threat>High</original_
errides></overrides></result><result id="05aee266-dee5-4d07-8312-b8d86c02e5ad"><name>Distributed Ruby (dRu
dmin</name></owner><comment></comment><creation_time>2024-08-04T09:37:57Z</creation_time><modificatio
29-b5c401e78851"/><task id="f834aeb1-6b29-4cce-a699-5265b947c89a"><name>metasploit</name></task><user_t
41-4a26-a817-8db895e501db"/></host><port>8787/tcp</port><nvt oid="1.3.6.1.4.1.25623.1.0.108010"><type>nvt</
nerabilities</name><family>Gain a shell remotely</family><cvss_base>10.0</cvss_base><cve>NOCVE</cve><bid>47
rtId=22750, URL:http://www.securityfocus.com/bid/47071, URL:http://blog.recurity-labs.com/archives/2011/05/12/dr
3/libdoc/drb/rdoc/DRb.html</xref><tags>cvss_base_vector=AV:N/AC:L/Au:N/C:C/I:C/A:C|summary=Systems using Di
and later, may permit unauthorized systems to execute distributed commands.|vuldetect=Send a crafted comman
via the instance_eval or syscall requests.|impact=By default, Distributed Ruby does not impose restrictions on allow
$SAFE environment variable to prevent privileged activities. If other controls are not in place, especially if the
Distributed Ruby process runs with elevated privileges, an attacker could execute arbitrary system commands or Ru
scripts on the Distributed Ruby server. An attacker may need to know only the URI of the listening Distributed Ruby
server to submit Ruby commands.|solution=Administrators of environments that rely on Distributed Ruby should e

appropriate controls are in place. Code-level controls may include:

- Implementing taint on untrusted input

- Setting $SAFE levels appropriately (>=2 is recommended if untrusted hosts are allowed to submit Ruby comma

- Including drb/acl.rb to set ACLEntry to restrict access to trusted hosts|solution_type=Mitigation|qod_type=remote
$</scan_nvt_version><threat>High</threat><severity>10.0</severity><qod><value>99</value><type>remote_vul</t
ver it is still possible to run arbitrary syscall commands on the remote host. Sending an invalid syscall the service ret

Flo:Errno::ENOSYS:bt["3/usr/lib/ruby/1.8/drb/drb.rb:1555:in `syscall'"0/usr/lib/ruby/1.8/drb/drb.rb
send__'"A/usr/lib/ruby/1.8/drb/drb.rb:1555:in `perform_without_block'"3/usr/lib/ruby/1.8/d
9:in `main_loop&apos;&quot;0/usr/lib/ruby/1.8/drb/drb.rb:1585:in `loop'"5/usr/lib/ruby/1.8/drb/drb.rb
start'"5/usr/lib/ruby/1.8/drb/drb.rb:1581:in `main_loop'"//usr/lib/ruby/1.8/drb/drb.rb:1430:
"//usr/lib/ruby/1.8/drb/drb.rb:1427:in `run&apos;&quot;6/usr/lib/ruby/1.8/drb/drb.rb:1347:in `initialize&apos
lib/ruby/1.8/drb/drb.rb:1627:in `start_service'"%/usr/sbin/druby_timeserver.rb:12:errnoi+:mesg"F
hreat><original_severity>10.0</original_severity><notes></notes><overrides></overrides></result><result id="5f9d
Only' Cookie Information Disclosure Vulnerability</name><owner><name>admin</name></owner><commer
e>2024-08-04T09:37:52Z</modification_time><report id="42a0103d-ec5d-4ea9-8c29-b5c401e78851"/><task id="f834
><count>0</count></user_tags><host>192.168.1.14<asset asset_id="89b2b59d-c441-4a26-a817-8db895e501db"/></
ype><name>Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability</name><family
d>51706</bid><xref>URL:http://secunia.com/advisories/47779, URL:http://www.exploit-db.com/exploits/18442, URL
he.org/security/vulnerabilities_22.html, URL:http://svn.apache.org/viewvc?view=revision&revision=1235454, UR
26.html</xref><tags>cvss_base_vector=AV:N/AC:M/Au:N/C:P/I:N/A:N|impact=Successful exploitation will allow attack
that may aid in further attacks.|affected=Apache HTTP Server versions 2.2.0 through 2.2.21|insight=The flaw is due
status code 400 when no custom ErrorDocument is configured, which can be
exploited to expose 'httpOnly' cookies.|solution=Upgrade to Apache HTTP Server version 2.2.22 or lat
ookie
information disclosure vulnerability.|solution_type=VendorFix|qod_type=remote_vul</tags><cert><cert_ref type="
05"/><cert_ref type="CERT-Bund" id="CB-K14/0608"/><cert_ref type="DFN-CERT" id="DFN-CERT-2015-0082"/><cert_r
"DFN-CERT-2014-0635"/><cert_ref type="DFN-CERT" id="DFN-CERT-2013-1307"/><cert_ref type="DFN-CERT" id="DFN
ref type="DFN-CERT" id="DFN-CERT-2012-0928"/><cert_ref type="DFN-CERT" id="DFN-CERT-2012-0758"/><cert_ref ty
CERT-2012-0568"/><cert_ref type="DFN-CERT" id="DFN-CERT-2012-0425"/><cert_ref type="DFN-CERT" id="DFN-CERT
ype="DFN-CERT" id="DFN-CERT-2012-0343"/><cert_ref type="DFN-CERT" id="DFN-CERT-2012-0332"/><cert_ref type=
2012-0264"/><cert_ref type="DFN-CERT" id="DFN-CERT-2012-0203"/><cert_ref type="DFN-CERT" id="DFN-CERT-2012
><threat>Medium</threat><severity>4.3</severity><qod><value>99</value><type>remote_vul</type></qod><desc
rity>4.3</original_severity><notes></notes><overrides></overrides></result><result id="adebe468-c2e8-4882-ab61-
me></owner><comment></comment><creation_time>2024-08-04T09:37:45Z</creation_time><modification_time>2
1e78851"/><task id="f834aeb1-6b29-4cce-a699-5265b947c89a"><name>metasploit</name></task><user_tags><cou
a817-8db895e501db"/></host><port>80/tcp</port><nvt oid="1.3.6.1.4.1.25623.1.0.80110"><type>nvt</type><name
ase>0.0</cvss_base><cve>NOCVE</cve><bid>NOBID</bid><xref>NOXREF</xref><tags>cvss_base_vector=AV:N/AC:L
web security issues.

Make sure to have wapiti 2.x as wapiti 1.x is not supported.

See the preferences section for wapiti options.

Note that the scanner is using limited set of wapiti options. Therefore, for more complete web
assessment, you should use standalone wapiti tool for deeper/customized checks.

Note: The plugin needs the 'wapiti' binary found within the PATH of the user running the scanner and
needs to be executable for this user. The existence of this binary is checked and reported separately
within 'Availability of scanner helper tools' (OID: 1.3.6.1.4.1.25623.1.0.810000).|qod_type=remote_app
n_nvt_version><threat>Log</threat><severity>0.0</severity><qod><value>98</value><type>remote_app</type></q
wrong version of wapiti is used or tmp dir is not accessible. Make sure to have wapiti 2.x as wapiti 1.x is not support
In short: Check the installation of wapiti and the scanner.</description><original_threat>Log</original_threat><origi
overrides></result><result id="ce7fe3e2-be8c-4d29-bf31-81fd30af71c0"><name>Multiple Vendors STARTTLS Implem
<name>admin</name></owner><comment></comment><creation_time>2024-08-04T09:37:43Z</creation_time><m
4ea9-8c29-b5c401e78851"/><task id="f834aeb1-6b29-4cce-a699-5265b947c89a"><name>metasploit</name></task>
b59d-c441-4a26-a817-8db895e501db"/></host><port>25/tcp</port><nvt oid="1.3.6.1.4.1.25623.1.0.103935"><type>

ry Command Injection Vulnerability</name><family>SMTP problems</family><cvss_base>6.8</cvss_base><cve>CVE
2011-1575, CVE-2011-1926, CVE-2011-2165</cve><bid>46767</bid><xref>URL:http://www.securityfocus.com/bid/46
tp://bugzilla.cyrusimap.org/show_bug.cgi?id=3424, URL:http://cyrusimap.org/mediawiki/index.php/Bugs_Resolved_in
es.kolab.org/server/release/kolab-server-2.3.2/sources/release-notes.txt, URL:http://www.postfix.org/CVE-2011-0411
://www.watchguard.com/support/release-notes/xcs/9/en-US/EN_ReleaseNotes_XCS_9_1_1/EN_ReleaseNotes_WG_XC
URL:http://datatracker.ietf.org/doc/draft-josefsson-kerberos5-starttls/?include_text=1, URL:http://www.securityfocus
ents/100134676, URL:http://support.avaya.com/css/P8/documents/100141041, URL:http://www.oracle.com/technetw
vu555316.patch, URL:http://www.kb.cert.org/vuls/id/555316</xref><tags>cvss_base_vector=AV:N/AC:M/Au:N/C:P/I:P/
ands in
the context of the user running the application. Successful exploits
can allow attackers to obtain email usernames and passwords.|vuldetect=Send a special crafted 'STARTTLS&
Please see the references for more information.|summary=Multiple vendors' implementations of 'STAR
vulnerability that lets attackers inject arbitrary commands.|affected=The following vendors are affected:

Ipswitch

Kerio

Postfix

Qmail-TLS

Oracle

SCO Group

spamdyke

ISC|qod_type=remote_vul|solution_type=VendorFix</tags><cert><cert_ref type="CERT-Bund" id="CB-K15/1514"/><
T" id="DFN-CERT-2011-0912"/><cert_ref type="DFN-CERT" id="DFN-CERT-2011-0897"/><cert_ref type="DFN-CERT" id=
<cert_ref type="DFN-CERT" id="DFN-CERT-2011-0808"/><cert_ref type="DFN-CERT" id="DFN-CERT-2011-0771"/><cert
="DFN-CERT-2011-0712"/><cert_ref type="DFN-CERT" id="DFN-CERT-2011-0673"/><cert_ref type="DFN-CERT" id="DF
_ref type="DFN-CERT" id="DFN-CERT-2011-0519"/><cert_ref type="DFN-CERT" id="DFN-CERT-2011-0516"/><cert_ref t
-CERT-2011-0434"/><cert_ref type="DFN-CERT" id="DFN-CERT-2011-0393"/><cert_ref type="DFN-CERT" id="DFN-CERT
ersion><threat>Medium</threat><severity>6.8</severity><qod><value>99</value><type>remote_vul</type></qod>
l_severity>6.8</original_severity><notes></notes><overrides></overrides></result><result id="b27a75cc-0281-4ec3-
</name></owner><comment></comment><creation_time>2024-08-04T09:37:35Z</creation_time><modification_tim
5c401e78851"/><task id="f834aeb1-6b29-4cce-a699-5265b947c89a"><name>metasploit</name></task><user_tags>
a26-a817-8db895e501db"/></host><port>80/tcp</port><nvt oid="1.3.6.1.4.1.25623.1.0.103079"><type>nvt</type><
s_base>0.0</cvss_base><cve>NOCVE</cve><bid>NOBID</bid><xref>NOXREF</xref><tags>cvss_base_vector=AV:N/A
s on web
applications via brute forcing. See the preferences section for configuration options.

Note: The plugin needs the 'dirb' binary found within the PATH of the user running the scanner and
needs to be executable for this user. The existence of this binary is checked and reported separately
within 'Availability of scanner helper tools' (OID: 1.3.6.1.4.1.25623.1.0.810000).|qod_type=remote_app
n_nvt_version><threat>Log</threat><severity>0.0</severity><qod><value>98</value><type>remote_app</type></q

http://192.168.1.14:80/
http://192.168.1.14:80/cgi-bin/
http://192.168.1.14:80/dav/
http://192.168.1.14:80/doc/
http://192.168.1.14:80/icons/
http://192.168.1.14:80/index
http://192.168.1.14:80/index.php
http://192.168.1.14:80/index/
http://192.168.1.14:80/phpMyAdmin/</description><original_threat>Log</original_threat><original_severity>0.0</or
t id="fa6f0c1a-3a36-4424-9198-96eab7ac574a"><name>phpMyAdmin 'error.php' Cross Site Scripting Vu
tion_time>2024-08-04T09:37:35Z</creation_time><modification_time>2024-08-04T09:37:35Z</modification_time><r
cce-a699-5265b947c89a"><name>metasploit</name></task><user_tags><count>0</count></user_tags><detection>

ct</name><value>cpe:/a:phpmyadmin:phpmyadmin:3.1.1</value></detail><detail><name>location</name><value>
25623.1.0.900129</value></detail><detail><name>source_name</name><value>phpMyAdmin Detection</value></
9d-c441-4a26-a817-8db895e501db"/></host><port>80/tcp</port><nvt oid="1.3.6.1.4.1.25623.1.0.801660"><type>nv
ability</name><family>Web application abuses</family><cvss_base>4.3</cvss_base><cve>CVE-2010-4480</cve><bi
//www.vupen.com/english/advisories/2010/3133</xref><tags>cvss_base_vector=AV:N/AC:M/Au:N/C:N/I:P/A:N|qod_t
t arbitrary
HTML code within the error page and conduct phishing attacks.|affected=phpMyAdmin version 3.3.8.1 and prior.|in
.php'
script when processing crafted BBcode tags containing '@' characters, which
could allow attackers to inject arbitrary HTML code within the error page
and conduct phishing attacks.|solution=No known solution was made available for at least one year since the disclo
of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer
release, disable respective features, remove the product or replace the product by another one.|summary=The hos
Scripting Vulnerability.|solution_type=WillNotFix</tags><cert><cert_ref type="DFN-CERT" id="DFN-CERT-2011-0467"/
FN-CERT" id="DFN-CERT-2011-0016"/><cert_ref type="DFN-CERT" id="DFN-CERT-2011-0002"/></cert></nvt><scan_nv
rity>4.3</severity><qod><value>99</value><type>remote_vul</type></qod><description></description><original_th
notes></notes><overrides></overrides></result><result id="f3be588d-fd59-4dea-8fa1-ff1f160c7a35"><name>PHP-C
p files.</name><owner><name>admin</name></owner><comment></comment><creation_time>2024-08-04T09:37
ort id="42a0103d-ec5d-4ea9-8c29-b5c401e78851"/><task id="f834aeb1-6b29-4cce-a699-5265b947c89a"><name>me
4<asset asset_id="89b2b59d-c441-4a26-a817-8db895e501db"/></host><port>80/tcp</port><nvt oid="1.3.6.1.4.1.256
hen parsing query string parameters from php files.</name><family>Web application abuses</family><cvss_base>7
-2335</cve><bid>53388</bid><xref>URL:http://www.h-online.com/open/news/item/Critical-open-hole-in-PHP-create
RL:http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/, URL:https://bugs.php.net/bug.php?id=61910, URL
urityfocus.com/bid/53388</xref><tags>cvss_base_vector=AV:N/AC:L/Au:N/C:P/I:P/A:P|summary=PHP is prone to an
ased setup (such as Apache's mod_cgid), the
php-cgi receives a processed query string parameter as command line
arguments which allows command-line switches, such as -s, -d or -c to be
passed to the php-cgi binary, which can be exploited to disclose source
code and obtain arbitrary code execution.

An example of the -s command, allowing an attacker to view the source code
of index.php is below:

http://example.com/index.php?-s|impact=Exploiting this issue allows remote attackers to view the source code of f
context of the server process. This may allow the attacker to obtain sensitive information and to run arbitrary PHP
on the affected computer. Other attacks are also possible.|solution=PHP has released version 5.4.3 and 5.3.13 to a
PHP is recommending that users upgrade to the latest version of PHP.|qod_type=remote_active|solution_type=Ver
<cert_ref type="DFN-CERT" id="DFN-CERT-2012-1316"/><cert_ref type="DFN-CERT" id="DFN-CERT-2012-1276"/><cert
="DFN-CERT-2012-1267"/><cert_ref type="DFN-CERT" id="DFN-CERT-2012-1266"/><cert_ref type="DFN-CERT" id="DF
_ref type="DFN-CERT" id="DFN-CERT-2012-0994"/><cert_ref type="DFN-CERT" id="DFN-CERT-2012-0993"/><cert_ref t
-CERT-2012-0920"/><cert_ref type="DFN-CERT" id="DFN-CERT-2012-0915"/><cert_ref type="DFN-CERT" id="DFN-CERT
type="DFN-CERT" id="DFN-CERT-2012-0907"/><cert_ref type="DFN-CERT" id="DFN-CERT-2012-0906"/><cert_ref type=
-2012-0880"/><cert_ref type="DFN-CERT" id="DFN-CERT-2012-0878"/></cert></nvt><scan_nvt_version>$Revision: 13
><value>95</value><type>remote_active</type></qod><description>Vulnerable url: http://192.168.1.14/cgi-bin/php
>7.5</original_severity><notes></notes><overrides></overrides></result><filters id=""><term>min_qod=70 apply_o
s><keyword><column>min_qod</column><relation>=</relation><value>70</value></keyword><keyword><column>
><column>autofp</column><relation>=</relation><value>0</value></keyword><keyword><column>rows</column
/column><relation>=</relation><value>created</value></keyword><keyword><column>first</column><relation>=<
d<order>descending</order></field></sort><results start="1" max="10"/><result_count>381<filtered>136</filtered>