АКТИВНОЕ СКАНИРОВАНИЕ

```
C:\Users\leksadin\Desktop
> wpscan http://www.[redacted].ru
_______________________________________________________________

        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.9.1
          Sponsored by Sucuri - https://sucuri.net
   @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________

[+] URL: http://www[redacted]ru/
[+] Started: Thu Mar 30 01:58:28 2017

[+] robots.txt available under: 'http://www.[redacted]/robots.txt'
[+] Interesting entry from robots.txt: http://www.[redacted].ru/wp-login.php
[+] Interesting entry from robots.txt: http://www.[redacted].ru/wp-register.php
[+] Interesting entry from robots.txt: http://www.[redacted].ru/feed/
    Reference: https://wpvulndb.com/vulnerabilities/6012
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-5296
[i] Fixed in: 3.0.2

[!] Title: WordPress 2.0 - 3.0 Remote Authenticated Administrator Add Action Bypass
    Reference: https://wpvulndb.com/vulnerabilities/6013
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-5297
[i] Fixed in: 3.0

[!] Title: WordPress 2.0 - 2.7.1 admin.php Module Configuration Security Bypass
    Reference: https://wpvulndb.com/vulnerabilities/6019
    Reference: http://www.securityfocus.com/bid/35584/

[!] Title: WordPress <= 4.0 - Long Password Denial of Service (DoS)
    Reference: https://wpvulndb.com/vulnerabilities/7681
    Reference: http://www.behindthefirewalls.com/2014/11/wordpress-denial-of-service-responsible-d
    Reference: https://wordpress.org/news/2014/11/wordpress-4-0-1/
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9034
    Reference: https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_long_password_dos
    Reference: https://www.exploit-db.com/exploits/35413/
    Reference: https://www.exploit-db.com/exploits/35414/
[i] Fixed in: 4.0.1

[!] Title: WordPress <= 4.0 - Server Side Request Forgery (SSRF)
    Reference: https://wpvulndb.com/vulnerabilities/7696
    Reference: http://www.securityfocus.com/bid/71234/
    Reference: https://core.trac.wordpress.org/changeset/30444
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9038
[i] Fixed in: 4.0.1

[!] Title: WordPress <= 4.7 - Post via Email Checks mail.example.com by Default
    Reference: https://wpvulndb.com/vulnerabilities/8719
    Reference: https://github.com/WordPress/WordPress/commit/061e8788814ac87706d8b95688df276fe3c85
    Reference: https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5491
[i] Fixed in: 4.7.1
```

```
C:\Users\leksadin\Desktop
> nmap login.[redacted].ru -sV -Pn -p 1-65535

Starting Nmap 7.10 ( https://nmap.org ) at 2017-03-30 02:08 RTZ 2 (ceia)
Nmap scan report for login.[redacted].ru (195.245.205.104)
Host is up (0.023s latency).
Not shown: 65523 filtered ports
PORT      STATE  SERVICE      VERSION
21/tcp    open   ftp?
25/tcp    open   smtp
80/tcp    open   http
143/tcp   open   imap?
443/tcp   open   https?
465/tcp   open   ssl/smtp
993/tcp   open   ssl/imaps?
5222/tcp  open   xmpp-client?
5223/tcp  closed hpvirtgrp
5269/[redacted]
21401[redacted]
21451[redacted]
```

view-source:http://www[redacted].au/internal/

```
.tc-rectangular-thumb {
            max-height: 250px;
            height :250px
          }

          .single .tc-rectangular-thumb {
            max-height: 250px;
            height :250px
          }


</style>
<link rel='stylesheet' id='customizr-style-css'  href='http://www.elite-electronics.com.au/internal/wp-content/themes
<link rel='stylesheet' id='fancyboxcss-css'  href='http://www.elite-electronics.com.au/internal/wp-content/themes/cus
ver=4.3.6' type='text/css' media='all' />
<link rel='stylesheet' id='ws-plugin--s2member-css'  href='http://www.elite-electronics.com.au/internal/wp-content/pl
ws_plugin__s2member_css=1&#038;qcABC=1&#038;ver=150203-1657412487' type='text/css' media='all' />
<link rel='stylesheet' id='wp-members-css'  href='http://www.elite-electronics.com.au/internal/wp-content/plugins/wp-
media='all' />
<script type='text/javascript' src='http://www.elite-electronics.com.au/internal/wp-includes/js/jquery/jquery.js?ver=
<script type='text/javascript' src='http://www.elite-electronics.com.au/internal/wp-includes/js/jquery/jquery-migrate
<script type='text/javascript'>
/* <![CDATA[ */
var TCParams =
{"FancyBoxState":"1","FancyBoxAutoscale":"1","SliderName":"0","SliderDelay":"5000","SliderHover":"1","SmoothScroll":"
eftSidebarClass":".span3.left.tc-sidebar","RightSidebarClass":".span3.right.tc-
sidebar","LoadModernizr":"1","stickyCustomOffset":"0","stickyHeader":"1","dropdowntoViewport":"","timerOnScrollAllBrc
ed":"1","dropcapWhere":{"post":"","page":"1"},"dropcapMinWords":"50","skipSelectors":{"tags":["IMG","IFRAME","H1","H2
/* ]]> */
</script>
<script type='text/javascript' src='http://www.elite-electronics.com.au/internal/wp-content/themes/customizr/inc/asse
<link rel="EditURI" type="application/rsd+xml" title="RSD" href="http://www.elite-electronics.com.au/internal/xmlrpc.
<link rel="wlwmanifest" type="application/wlwmanifest+xml" href="http://www.elite-electronics.com.au/internal/wp-incl
<meta name="generator" content="WordPress 4.3.6" />
<!-- WP-Members version 2.9.9.1, available at http://rocketgeek.com/wp-members -->
```