

## 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.



GEODIS



### 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".

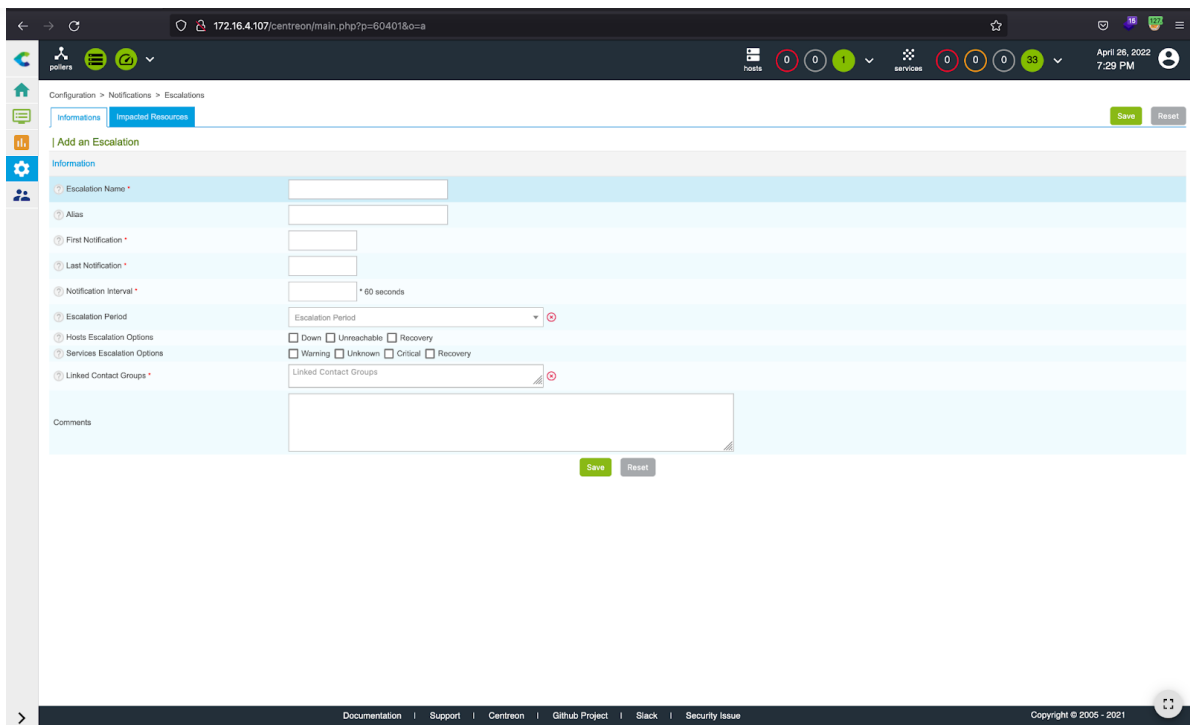
### About SQL Injection:

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

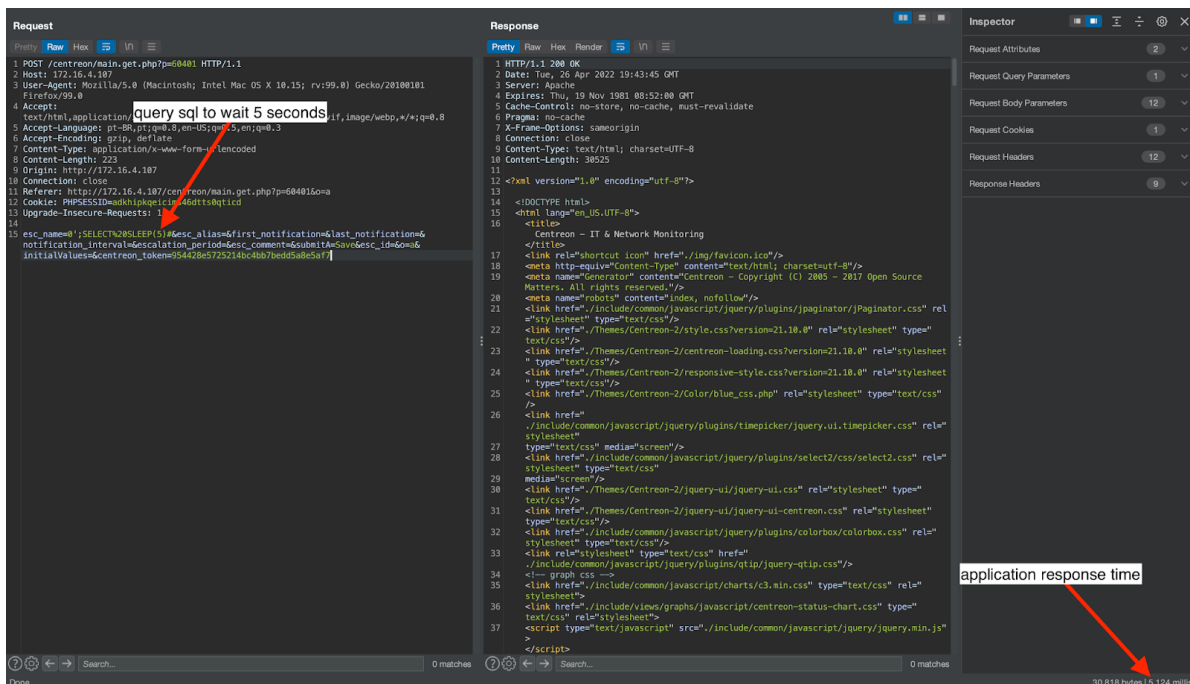
We use cookies on our website to give you the most relevant experience by remembering your preferences and repeat visits. By clicking "Accept All", you consent to the use of ALL the cookies. However, you may visit "Cookie Settings" to provide a controlled consent.

[Cookie Settings](#)

[Accept All](#)



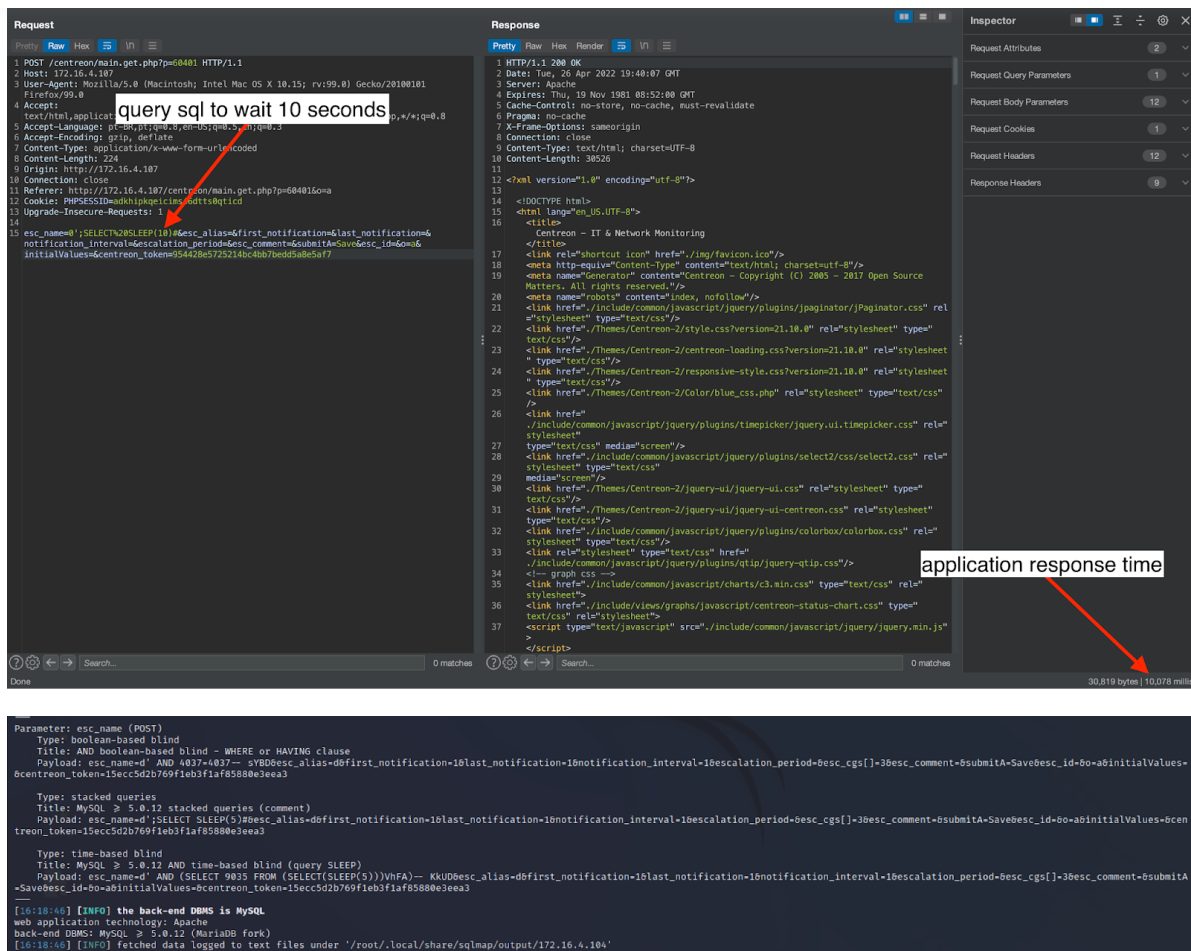
When analyzing the requests, it was possible to notice that it was a blind-sql (a type of SQL Injection attack that asks the database true or false questions and determines the answer based on the applications response) more specifically a time-based attack in which the application's response time is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



We use cookies on our website to give you the most relevant experience by remembering your preferences and repeat visits. By clicking "Accept All", you consent to the use of ALL the cookies. However, you may visit "Cookie Settings" to provide a controlled consent.

[Cookie Settings](#)

[Accept All](#)



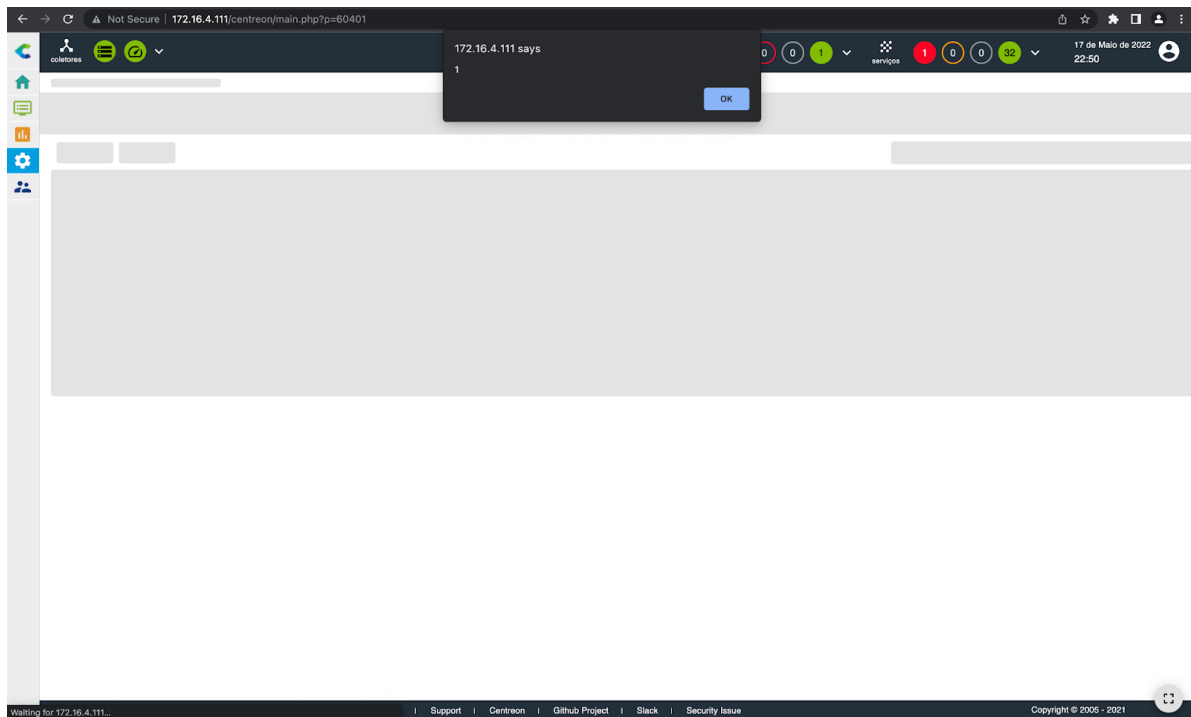
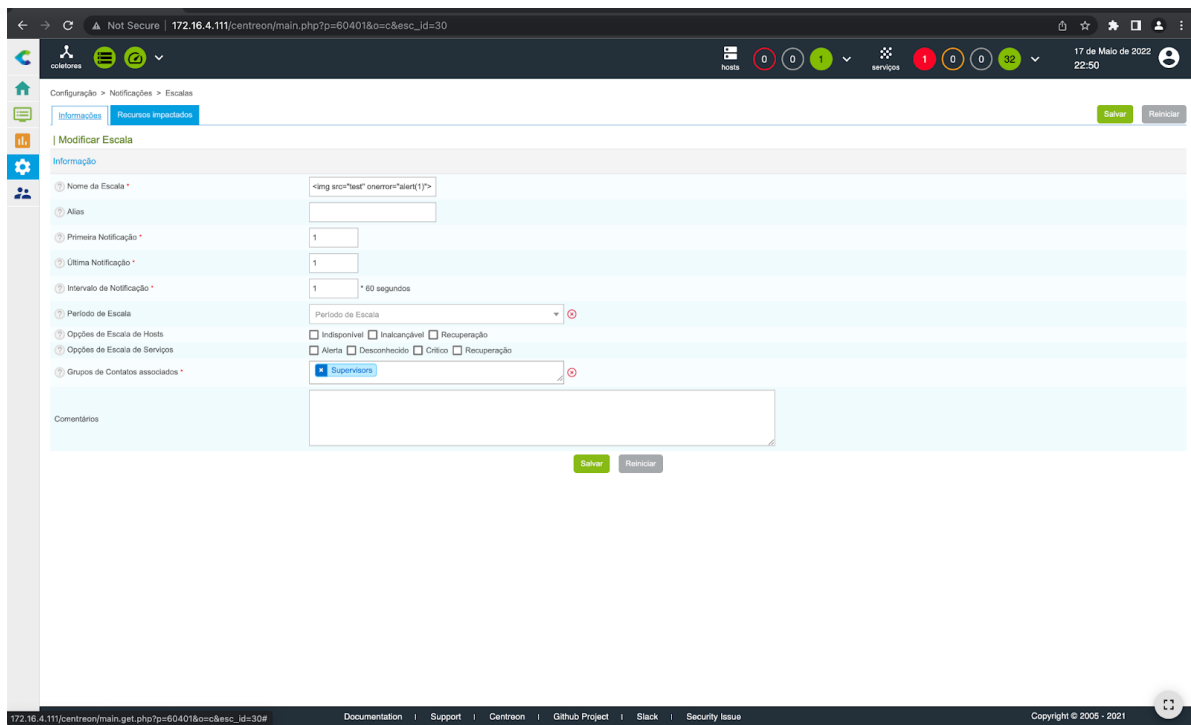
It is also possible to exploit Cross-Site Scripting (XSS) in the same field explored for SQLi, thus making it possible to insert malicious javascript into the application..

## 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.

We use cookies on our website to give you the most relevant experience by remembering your preferences and repeat visits. By clicking "Accept All", you consent to the use of ALL the cookies. However, you may visit "Cookie Settings" to provide a controlled consent.

Cookie Settings Accept All



## Fixed versions:

– centreon-web-22.04.1

We use cookies on our website to give you the most relevant experience by remembering your preferences and repeat visits. By clicking “Accept All”, you consent to the use of ALL the cookies. However, you may visit "Cookie Settings" to provide a controlled consent.

[Cookie Settings](#)

[Accept All](#)

24-05 – Vendor acknowledged disclosure.

04-08 – New versions of software released with patches

26-08 – Blog post release

<input type="text"/>	Pesquisar
----------------------	-----------

## Posts recentes

Centreon SQLi and XSS Vulnerability

Vulnerabilidades Publicadas (CVE)

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

## Comentários

Hakai Offensive Security

We use cookies on our website to give you the most relevant experience by remembering your preferences and repeat visits. By clicking "Accept All", you consent to the use of ALL the cookies. However, you may visit "Cookie Settings" to provide a controlled consent.

[Cookie Settings](#)

[Accept All](#)