

CodeCat



CodeCat manual tool for codereview

Antonio Costa - CoolerVoid - coolerlair[aT]gmail[DOT]com

November 11, 2019

Whoami

Author:

- Antonio Costa "CoolerVoid" an ordinary Developer.



(a)

Introduction

Software Information:

- CodeCat is a Open Source Tool, focused to help code review.
- CodeCat held by GPL v3 license

Introduction

Motivations

- Track untrusted user input
- Track dangerous functions
- Save sinks in cache and show syntax highlight to study all codes.
- Options to save custom rule to search new sinks

Introduction

Requirements:

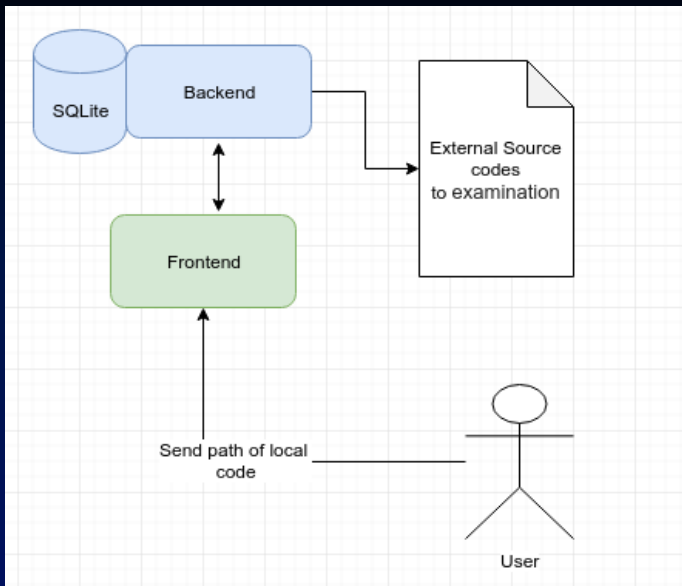
- Python3
- Current version tested only in Linux.
- Current version run well, but is a BeTa version, you can report bug...

How you can use it

Following this to get, decompress and install:

- `git clone https://github.com/CoolerVoid/codecat`
- Follow steps of `readme.md` file

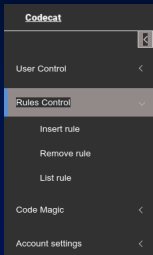
The Overview



Explanation

Following left menu you have options to custom rules.


- You can create, list, remove your custom rules...



Explanation

Insert your custom rule ex 1

- Example to detect simple XSS



User Control <

Rules Control <

Code Magic <

Account settings <

Title

Simple XSS

Description:

Put description of warning or vuln here.XSS occurs when an attacker is capable of injecting a script, often Javascript, into the output of a web application in such a way that it is executed in the client browser. This ordinarily happens by locating a means of breaking out of a data context in HTML into a scripting context - usually by injecting new HTML, Javascript strings or CSS markup.

Language

Impact

match1

(echo|print|display|render|write|send)

match2

(\\$_GET|\\$_POST|\\$_REQUEST|\\$_COOKIE)

Explanation

Insert your custom rule ex 2

- Note, form with value zero, not find match


Codecat

User Control <

Rules Control <

Code Magic <

Account settings <



Title

Java SQL tracks

Description:

Uses of SQL queries is interesting to find SQL points...

Language Java

Impact Low

match1

(SELECT|DELETE|INSERT|DROP|WHERE|JOIN|UPDATE|hq|createQuery)

match2

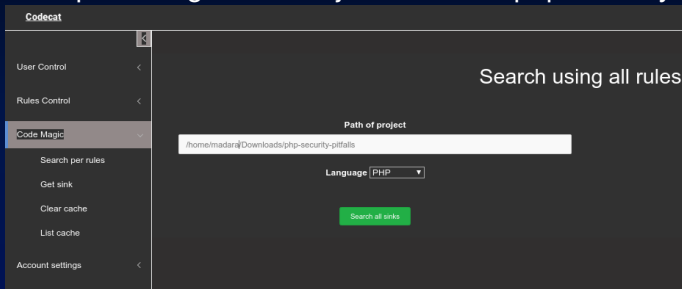
0

Insert Rule in database

Explanation

Recursive search by rules in path

- example from github.com/joostvanveen/php-security-pitfalls



Explanation

The results will appear in cache

- If you click in ID Rule you can view rule descriptions...

Cache of result

Show entries

Search:

Rule_ID ▲	Title ↕	Path ↕	Lines ↕	Ext ↕	View ↕
1	Simple XSS	/home/madara/Downloads/php-security-pitfalls/public_html/xss/views/comment.php	10,12	php	
2	Code injection PHP	/home/madara/Downloads/php-security-pitfalls/public_html/osinjection/index.php	62	php	
2	Code injection PHP	/home/madara/Downloads/php-security-pitfalls/public_html/sqlinjection/reset.php	33	php	
2	Code injection PHP	/home/madara/Downloads/php-security-pitfalls/public_html/codeinjection/eval.php	10	php	
2	Code injection PHP	/home/madara/Downloads/php-security-pitfalls/public_html/codeinjection/preg.php	11	php	
Rule_ID	Title	Path	Lines	Ext	View

Showing 1 to 5 of 5 entries

[Previous](#)[Next](#)

Explanation

You can view source of match, when you click view icon

Path: /home/madara/Downloads/php-security-pitfalls/public_html/xss/views/comment.php

Lines: 10,12

```
1  <?php
2  /**
3   * This code is part of the Tutsplus course PHP Security Pitfalls.
4   * It is meant for demonstration purposes only.
5   * Do not use this code in a production environment!
6   */
7
8  if (!empty($_POST['comment'])) {
9      echo '<h1>Your name</h1>';
10     echo escape($_POST['name']);
11     echo '<h1>Your comment</h1>';
12     echo escape($_POST['comment']);
13 }
14
15 // plain text
16 // html text from CMS
```

The End ?



Greetings

- contact: coolerlair[at]gmail[dot]com
- coolerlair[at]gmail[dot]com
- my parents and friends...
- github.com/CoolerVoid

at construction...