ABillS - Улучшение #560

Анализатор логов апача на взлом

22-02-2017 13:52 - AsmodeuS Asm

Статус:	Закрыта	**Дата начала:**	22-02-2017
Приоритет:	Нормальный	**Дата завершения:**	
Назначена:	Юрій Климюк	**Готовность:**	100%
Категория:		**Оценка трудозатрат:**	6.00 часов
Версия:	167 20.03.2023 09:00:00	**Трудозатраты:**	6.00 часов
Важность:	100	**Применение:**	
Сложность:	13	**Время на тест:**	
Цель:			

Описание

billd плугин

проверяющий лог на SELECT UPDATE INSERT

История

#1 - 29-06-2021 09:44 - AsmodeuS Asm

- Параметр Назначена изменился на AsmodeuS Asm

- Параметр Версия изменился на 122 28.06.2021 09:00:00

- Параметр Оценка трудозатрат изменился на 6.00 ч

- Параметр Сложность изменился с 1 на 13

pm для плагина и для update.pl

#2 - 12-07-2021 09:57 - Андрей Собчинский

- Параметр Версия изменился с 122 28.06.2021 09:00:00 на 123 12.07.2021 09:00:00

#3 - 23-07-2021 17:19 - Андрей Собчинский

- Параметр Версия изменился с 123 12.07.2021 09:00:00 на 124 26.07.2021 09:00:00

#4 - 09-08-2021 09:46 - Андрей Собчинский

- Параметр Версия изменился с 124 26.07.2021 09:00:00 на 125 09.08.2021 09:00:00

#5 - 23-08-2021 09:54 - Андрей Собчинский

- Параметр Версия изменился с 125 09.08.2021 09:00:00 на 126 23.08.2021 09:00:00

#6 - 06-09-2021 09:53 - AsmodeuS Asm

- Параметр Версия изменился с 126 23.08.2021 09:00:00 на 127 06.09.2021 09:00:00

#7 - 08-08-2022 09:58 - AsmodeuS Asm

- Значение 127 06.09.2021 09:00:00 параметра Версия удалено

#8 - 06-02-2023 09:43 - AsmodeuS Asm

- Параметр Версия изменился на 164 06.02.2023 09:00:00

название скрипта bills.plugins/secure.pm

фильтрация логов апача

на появления IP или запросов из списка

список вести в файле libexec/secure.txt (в будущем перенести в базу)

одна строка один параметр

выводить все строки которые содержат искаемое значение

billd secure

Вывод:
Парамтер:
- списко строк с выделением искаемых значений

Расположение логов вебсеверар указывать в сонфиге через точку с запаятой, потом по ни проходиться парсером

лучший вариант парсить так

open(my $program, '|-', "grep 'parameters' logfile")

#9 - 06-02-2023 09:47 - AsmodeuS Asm

- Параметр Назначена изменился с AsmodeuS Asm на Юрій Климюк

#10 - 06-02-2023 16:41 - Юрій Климюк

- Параметр Статус изменился с Новая на В работе

#11 - 08-02-2023 13:25 - Юрій Климюк

- Параметр Статус изменился с В работе на На тестировании

- Параметр Готовность изменился с 0 на 90

http://abills.net.ua:8090/pages/viewpage.action?pageId=3211314#billd%D0%BA%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D1%8C%D1%81%D0%BE%D1%81%D1%82%D0%BE%D1%8F%D0%BD%D0%B8%D1%8F%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B-%D0%90%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7%D0%B0%D1%82%D0%BE%D1%80%D0%BB%D0%BE%D0%B3%D0%BE%D0%B2Apache%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80%D0%B0

#12 - 20-03-2023 14:05 - Віталій Андрусяк

- Параметр Статус изменился с На тестировании на Обратная связь

Функціонал не зовсім робочий.

1. Не повідомляє, чи вказаний файл в конфігурації взагалі існує.

2. При введенні нового рядка чи пробіла - billd зупиняється намертво.
Методом білого ящика було вияснено, що команда grep очікує на аргумент, а цей же аргумент це і є пробіл, який відповідно розпізнає.

Можливі рекомендації для покращення (не обов'язково для виконання, і не є компетенцію в рамках тестування)
1. Додати в лог дату тестування, коли був проведений пошук.

#13 - 23-03-2023 12:30 - Віталій Андрусяк

- Параметр Версия изменился с 164 06.02.2023 09:00:00 на 167 20.03.2023 09:00:00

#14 - 23-03-2023 17:41 - Юрій Климюк

- Параметр Статус изменился с Обратная связь на На тестировании

1. *Не повідомляє, чи вказаний файл в конфігурації взагалі існує.* - Якщо файлу або параметрів пошуку немає, то виводиться повідомлення **Error. Please add search parameters to libexec/secure.txt**

2. *При введенні нового рядка чи пробіла - billd зупиняється намертво.* - Тут не зрозуміло. В документації прописано як запускати програму **/usr/abills/libexec/billd secure**

3. Дату логування можна добавити

#15 - 08-04-2024 12:45 - Віктор Дудаль

- Параметр Статус изменился с На тестировании на Решена

#16 - 08-04-2024 12:45 - Віктор Дудаль

- Параметр Статус изменился с Решена на Закрыта

- Параметр Готовность изменился с 90 на 100