Vulnerability Assessment Report Template

**Ime i prezime:** Vasilije Zeković **Tim:** 7 **Datum:** 28.10.2024. **Scan Tool:** Nessus (10.8.3)  
**Test okruženje:** Metasploitable3

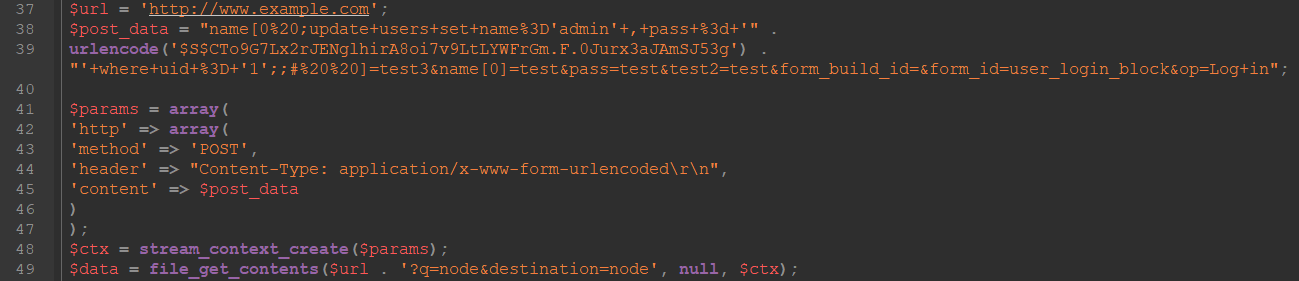
### **1. Enumeracija CVE-a**

* **CVE ID:** CVE-2014-3704
* **Opis:**  
  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.

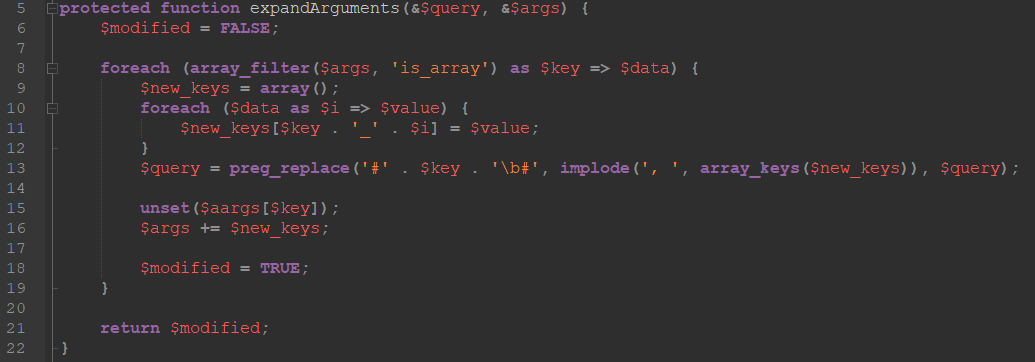
### **2. CVSS skor**

* **CVSS skor (numerička vrednost):** 7.5
* **Vektor:** AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H  
  **AV** je *Network* što predstavlja mogućnost eksploatacije ranjivosti putem mreže. Ova osobina je očekivana, jer se SQLi ostvaruje upotrebom *HTTP* zahteva upućenom ranjivom veb servisu.  
  **AC** je *Low* što predstavlja nizak stepen tehničkog znanja za potrebe eksploatacije ranjivosti. Delom je ovo slučaj jer je SQLi jedna od najpoznatijih ranjivosti u svetu sajber bezbednosti.  
  **PR** je *None* što govori da su nepotrebne ikakve privilegije radi uspešne eksploatacije ranjivosti. Korišćenjem samo pristupne tačke koja je vezana za formu prijavljivanja se može izvršiti eksploatacija ove ranjivosti.   
  **UI** je *None* što govori da je nepotrebna bilo kakva interakcija od strane korisnika (administratora) za potrebe ostvarivanja ranjivosti. Korisnik može poslati zahtev ka veb servisu sa proizvoljnim vrednostima čime se potencijalno izvršava upit zle namere, bez ikakvog dodatnog angažmana od strane administratora.   
  **S** je *Unchanged* predstavlja osobinu ranjivosti koja govori da se eksploatacija sistema obavlja nad istim opsegom koji je i bio cilj napada. Dakle, sve vreme će to biti najčešće baza podataka nad kojom se izvršava veb servis, čime se napad neće proširivati na druge delove servera ili druge sisteme. Ipak, moguće je uz neke eksploite obezbediti RCE i kasnije proširivanje opsega napada.  
  **C** je *High* što predstavlja mogućnost da napadač dobije pristup poverljivim informacijama. Zahvaljujući mogućnosti pokretanja proizvoljnih upita se takođe može izvršiti i upit kreiranja naloga admina i zahvaljujući samo jednom upitu se dobija pristup svim poverljivim informacijama. Svakako je moguće i iz samih upita zle namere narušiti poverljivost informacija.   
  **I** je *High* što predstavlja negativnu posledicu u kojoj napadač može narušiti integritet podataka. Zahvaljujući mogućnosti pokretanja proizvoljnih upita se takođe može izvršiti i upit operacija ažuriranja čime se ugrožava integritet podataka.   
  **A** je *High* što govori da se delovanjem napadača dostupnost sistema može narušiti. Na vrlo jednostavan način se može sabotirati rad čitavog veb servisa, praktično sa pokretanjem samo jednog upita, kao što je na primer upit brisanja svih podataka iz baze podataka.
* **Opravdanje:**  
  Ranjivost ima prilično visok *CVSS* skor zahvaljujući nepovoljnosti faktora opisanih u nastavku. Eksploatacije ranjivosti sa udaljene pozicije govori da svaki pripadnik mreže može biti napadač čime se ostvaruje velika numerička vrednost potencijalnih napadača. Velika većina napadača u svetu sajber sigurnosti su upoznati sa ovim tipom napada, jer je prilično karakterističan i jednostavan za izvođenje. Ozbiljnost eksploatacije ranjivosti se ogleda u mogućnosti eksploatacije putem mreže, pre svega interneta, uz minimalno tehničkog znanja, kao i lake penetracije usled nedostatka interakcije od strane administratora i potrebnih permisija. Kod ovakvog tipa napada najčešće se ne ostvaruje *RCE* što dalje utiče i na sam opseg delovanja napada. Poverljivost, integritet i dostupnost mogu biti u potpunosti narušeni, dok je opseg napada limitiran čime se umanjuje *CVSS* skor. Zanimljivo je da su se eksploiti povezani s ovom ranjivošću veoma brzo proširili unutar brojne hakerske zajednice nakon objave u vezi postojanja ranjivosti.

### **3. Dostupnost eksploita**

* **Postoji javno dostupan eksploit (Da/Ne):**  
  Da. Postoji više javno dostupnih eksploita koji su različitog tipa.   
  Odabrani eksploit: <https://www.exploit-db.com/exploits/34993>
* **Opis eksploita:**  
  Eksploit se nadovezuje na dosadašnju priču. Potrebno je podesiti *URL* adresu sajta koju napadač cilja. Slanjem *HTTP POST* zahteva sa malicioznim parametrima na *login* stranicu se resetuju kredencijali administratorskog naloga na *username = admin* i *password = admin.* U slučaju uspešne eksploatacije ranjivosti, napadač ima pristup administratorskom nalogu. Maliciozni parametri predstavljaju zapravo nastavak upita koji se generiše u metodi *expandArguments*. Što je detaljnije objašnjeno u tački 4.
* **Kod eksploita (ukoliko postoji):**  
    
  Srž eksploita je samo slanje *HTTP POST* zahteva na vešt način. Upit koristi *URL* kodiranje pa nije pregledan. Suština upita je izmena korisničkog imena i lozinke korisnika sa *UID* = 1 koji obično predstavlja administratorski nalog. Lozinka sa vrednošću *admin* je unapred hešovana prema poznatom načinu heširanja za *Drupal 7*. Na kraju se parametri zahteva pakuju u kontekst za *HTTP* zahtev i pokreće proces slanja zahteva.

### **4. Analiza uzroka (root cause)**

* **Uvođenje Greške (Commit/Verzija):**  
  Ranjivost je uvedena od verzije 7.0 i postojala je sve do verzije 7.31. Konkretnije datum uvođenja ranjivosti je 15.4.2010. na osnovu *commit-a* sa identifikatorom [c27d663](https://github.com/drupal/drupal/commit/c27d66307c2d395a5e071d2b9c1d8665f6dc952d). Datum saniranja ranjivosti je 15.10.2014 na osnovu *commit-a* sa identifikatorom [26a7752](https://github.com/drupal/drupal/commit/26a7752c34321fd9cb889308f507ca6bdb777f08). Sama ranjivost se ogleda u neadekvatnoj validaciji ulaznih parametara u funkciji *expandArguments* (pogledati kod ispod). Razlog za uvođenje funkcije predstavljaju forme čiji su ulazi ponovljivi, a koje je potrebno proslediti bazi podataka. Primer takve forme je forma za izmenu lozinke korisnika, pri čemu je staru lozinku potrebno uneti dva puta. Dakle, cilj funkcije je priprema parametara za potrebe formiranje upita, tačnije, ukoliko postoje u rečniku neke vrednosti ključeva koje su nizovi potrebno ih je isparsirati. Primer takvog slučaja je postojanje ključa *pass* u rečniku čija je vrednost zapravo niz sa dva elementa, lozinka uneta u prvom *input* poljui lozinka uneta u drugom *input* polju. Za sve vrednosti elemenata niza unutar rečnika će se parametri formirati na osnovu ključa rečnika ***$key*** uz konkatenaciju sa rednim brojem elementa ugnježdenog niza ***$i***. Zatim će se svi novonastali parametri zameniti sa starim parametrom ***$key*** unutar same promenljive upita ***$query***. Ista logika se primenjuje i za niz argumenata ***$args***, što predstavlja niz ključeva rečnika. Ključ rečnika čija je vrednost niz će biti zamenjen sa mnoštvom novih ključeva elemenata niza. U slučaju sa ponovljivim unosom lozinke bi se umesto ‘*pass: [‘string1’, ‘string2’]’* našle vrednosti *pass1: ‘string1’* i *pass2: ‘string2’*. Glavni krivac ove funkcije leži u činjenici da se nigde ne validira sama vrednost promenljive ***$i***, čime se potencijalno mogu uneti *string-ovi* (umesto *integer-i*) zle namere koji se dalje propagiraju u samom upitu. Ako se na stranici za prijavu napravi još jedno *input* polje, tako da je vrednost atributa *name = name[0; maliciozni upit;; # sve ostalo postaje komentar]* i vrednost atributa postojećeg *input* polja je *name = name[0]*. Tada će se ***$query*** evaluirati u *“SELECT \* FROM [users] WHERE name = :name\_0; maliciozni upit;; # , :name\_0 AND status = 1”* što dovodi do uspešne eksploatacije ranjivosti.
* **Primer Koda (ako je primenljivo):**  
  

### **5. Preporuke za mitigaciju**

* **Da li je dostupan Vendor Fix ili patch (Da/Ne):**Da, *patch* je dostupan u verziji 7.32.
* **Mitigation Strategy:**  
  Ažuriranje *Drupal-a* na 7.32 verziju otklanja ranjivost, pri čemu je potrebno obratiti pažnju da li su se u međuvremenu, kao posledica ranjivosti, pojavili *backdoors* programi. Razvojni tim *Drupal* platforme je izjavio da je 7h nakon objave o postojanju ranjivosti većina veb sajtova kompromitovana. Dakle, za svaki slučaj je neophodno izvršiti oporavak i resetovanje čitave aplikacije na osnovu čiste verzije *backup* podataka.  
  Ukoliko administrator iz nekog razloga nije u stanju da izvrši ažuriranje verzije, otklanjanje ranjivosti se može uraditi izmenom sledeće linije u *expandArguments* metodi.  
  **stara linija:** *foreach ($data as $i => $value) {*  
  **nova linija:** *foreach (array\_values($data) as $i => $value) {*Potrebno je ručno izvršiti primenu *patch-a,* izmenom već opisane linije koda ili izvršavanjem procesa ažuriranja.
* **Alternativni fix (ukoliko ne postoji vendorski):**