# ОТНОСНО ПРОВЕРКА ЗА УЯЗВИМОСТ ПРИ ПУБЛИКУВАНЕ НА ДАННИ В БАЗА ДАННИ НА ЦЕНТЪР ЗА УПРАВЛЕНИЕ НА КРИЗИ

**Веселина Александрова, доц. д-р*, Виолета Василева, д-р**, инж. Елица Павлова д-р*****
***Военна академия "Г. С. Раковски", v.gagamova@rndc.bg, **Future Innovation Labs, violetta.ziv@gmail.com, *** УНСС, epavlova@unwe.bg**

# REGARDING CRISIS MANAGEMENT CENTER DATABASE POSTING VULNERABILITY CHECK

**Veselina Aleksandrova, Assoc. Prof., PhD*, Violeta Vasileva, PhD** , Elitsa Pavlova, PhD*****
***Rakovski National Defence College, v.gagamova@rndc.bg,**Future Innovation Labs, violetta.ziv@gmail.com, ** University of National and World Economy /UNWE/, epavlova@unwe.bg**

***ABSTRACT***
*In the proposed paper, the authors present a study on some aspects of security related to the management and storage of information in automated crisis management information systems. The process is analyzed in which a potential threat of theft and/or possible replacement of a file prepared for publication in a crisis database hosted on a web server arises.*

## Въведение

Постоянното развитие на информационните технологии и навлизането на интернет приложенията във всички сфери на обществения живот оказват огромно отражение върху работата на бизнеса, правителствените институции, науката и образованието. Използването на уеб-базираните информационни системи от една страна има редица предимства и създава нови възможности, но от друга страна се превръща и в инструмент и цел за извършване на кибератаки. Свидетели сме на нарастващ брой компютърни атаки срещу важни системи, които създават заплаха за обществото и причиняват милионни загуби. Информационните и комуникационни технологии се използват и за събиране на информация и за улесняване на комуникациите при извършване на редица престъпления. Киберпрестъпността се явява сериозен проблем за съвременното общество, който непрекъснато се разраства. Във връзка с това се обединяват усилията на редица институции за създаването на платформа, която да стимулира и подпомага обмяна на добрите практики в това направление.

Целта на авторите е да разкрият някои аспекти на сигурността свързани с проникване и нарушаване защитеността на уеб базираните информационни системи за мениджмънт на кризи. За целта се анализира технологията на публикуване на информация в база данни на уеб сървър на Център за управление на кризи (ЦУК), при което възниква потенциална заплаха за откраднване или евентуална подмяна на файл, подготвен за публикуване на сървъра. Предлага се и вариант за решение на проблема свързан с прилагането на препоръчителни практики за изпълнение при публикуването на данни в информационната система.

## Изследване на потенциални уязвимости при публикуване на файлове

При публикуването на файл на WEB сървър, той се запазва в стандартна временна директория. Файлът се изтрива, ако не бъде преместен или преименуван преди обработващият сървърен скрипт да приключи своето изпълнение. При положение, че формата, написана на езика HTML съдържа поле с име userfile, то на обработващия сървърен скрипт разработен на езика PHP ще бъдат предадени пет променливи. Достъпът до тях може да се осъществи по няколко начина. В разработката се разглежда начина с използването на супер глобалните масиви $_FILES и $HTTP_POST_FILES.

Със средствата на HTML и PHP става възможно да се заобиколи забраната за обмен на файлове по протокол File Transfer Protocol (FTP). Това представлява сериозен проблем и потенциална уязвимост, която би позволява неконтролируемо предаване на важна информация към външни за информационната система злонамерени потребители или нелегални складове за данни. Динамично променящата се среда за сигурност налага съсредоточаване на вниманието и върху изследванията на технологиите предизвикващи такива атаки. Такива изследвания са в съответствие на съвременната концепция за интелигентна отбрана на НАТО и биха подпомогнали решаването на проблеми на сигурността на информацията в киберпространството с цел постигане на по-голямо равнище на сигурност.

Няколко събития от историята на Военна академия "Георги Стойков Раковски" я превърнаха в едно от водещите звена за изследване, изграждане и развитие на способности за управление на кризи и реагиране при бедствия. С най-съвременни средства и технологии в рамките на военна академия беше създаден Център "Обучение при извънредни ситуации". Той беше тържествено открит на 15 октомври 2011 г. от тогавашните Европейския комисар по "Международно сътрудничество, хуманитарна помощ и реакция при кризи" госпожа Кристалина Георгиева и министърът на отбраната Аню Ангелов. С финансовата помощ на Генерална дирекция „Вътрешни работи" на Европейската комисия, Програма „Превенция, готовност и ликвидиране на последствията от тероризъм и други заплахи за сигурността", Военна академия „Г. С. Раковски" участва в европейски проект „Разработване на необходими инструменти за координиране на вътрешно-секторните дейности за защита на критична инфраструктура в ситуация на многостранна терористична заплаха. Повишаване способността за защита на ключови обекти от критичната инфраструктура в България". Референтния номер е HOME/2010/CIPS/AG/019. Водеща организация е Институт по металознание, съоръжения и технологии "Акад. А.Балевски" с център по хидроаеродинамика при Българска академия на науките – БАН. Партньори са Военна академия „Г. С. Раковски", Главна дирекция „Пожарна безопасност и защита на населението"; Академия на министерство на вътрешните работи; Русенски университет "Ангел Кънчев". Продължителността на проекта е за периода 08.06.2011 г. – 08.06.2013 г.

Изграждането на автоматизирана информационна система за мениджмънт на кризи е свързано с развитието на способностите за управление при кризи и реагиране при бедствия. Това отговаря на изпълнението на една от мисиите на Въоръжените сили - Принос към националната сигурност в мирно време, което включва поддържане на способности за ранно предупреждение за потенциални рискове и заплахи; дейности по контрола на въздушното и морското пространство; операции по сдържане и неутрализиране на терористични, екстремистки и престъпни групи; защита на стратегически обекти; защита и подпомагане на населението при природни бедствия, аварии и екологични катастрофи; неутрализиране на невзривени боеприпаси; оказване на хуманитарна помощ; съдействие за контрола на миграцията; спасителни и евакуационни дейности; помощ, при необходимост, на други държавни органи, организации и местни власти за предотвратяване и преодоляване на последствията от терористични атаки, природни бедствия, екологични и индустриални катастрофи и опасно разпространение на инфекциозни заболявания [[1]].

Като етап в развитието на автоматизирана информационна система за мениджмънт на кризи във Военна академия се проектира, алгоритмизира, програмира и пуска в опитна, а в последствие и редовна експлоатация централизирана база данни за регистриране и съхраняване на информация, свързана с широк спектър кризи, класифицирани с техните параметри и характеристики. Системата е с отворена архитектура, което е предпоставка за бъдещо взаимодействие с автоматизираните информационни системи по управление на кризи на съюзно ниво.

Като бъдещо направление за развитието на базата данни е тя постепенно да се надгражда до банка с експертни знания за оценка на риска, прогнозиране на бъдещи кризи, както и оценка на вече възникнали неблагоприятни обстоятелства. Целта е да се генерира спектър от възможни решения за преодоляване на конкретна ситуация. По този начин базата данни се явява част от системата за поуки от практиката при мениджмънта на кризи и представлява част от цялостната информационна инфрасструктура на ЦУК. Друг аспект при изграждането на базата данни е тя да бъде проектирана

така, че да бъде съвмесима с базите данни по мениджмънт на кризи на други системи от национален или съюзен формат. За целта е необходимо да се предложат и приемат съвместими формализовани документи за съхранение в базата данни.]

Един от аспектите на сигурността при управление и съхранение на информацията е свързан с необходимостта предварително да бъдат изградени, независими от чужди системи и решения, три специализирни модула със сигурен код. Те са следните:

1. Модул за защита от кибератака, реализирана чрез вграждане на скрит код с отместено разрушително действие в определен бъдещ момент, (това е атака от типа на Стухнет, блокирал работата на Иранската ядрена централа);

2. Независим софтуерен модул за проследяване, статистика на трафика и противодействие на кибератаки по време на активна връзка с базата данни, включително в системата за дистанционно управление на екипите, както и за целите на дистанционното обучение в областта на мениджмънта на кризи;

3. Модул за откриване, противодействие и ликвидиране на кибератака срещу забрана за използване на протокол FTP в домейните, сайтовете и информационните системи в сферата на сигурността и отбраната, и в частност в центъра за управление на кризи.

След успешното сертифициране на тези модули, необходими за сигурността на информацията, се пристъпва към поетапното изграждане на базата от данни.

Скрипт за проверка “upload.php”.

Един от аспектите на сигурността при управление и съхранение на информацията в автоматизираните информационни системи за мениджмънт на кризи е свързан с изследване на възможността за заобикаляне на защитата чрез регламентирана забрана за достъп по FTP протокол. За целта се предлагат разработените специализиран код за качване на файлове в HTML (HyperText Markup Language) форма за публикуване (“UploadForm.html”), както и скрипт за проверка “upload.php”, представляващ PHP код за обработка на файловете посочени в HTML формата. Детайлното съдържание на тези специализирани кодове е разгледано в други публикации [[2]]. При публикуването на даден файл на уеб сървъра, той се запазва в стандартна временна директория на сървъра. След това скриптът “upload.php” се изпълнява, при което се извършват съответни проверки за сигурността по отношение на:

- името на файла
- откъде (от какъв компютър или сървър) е качен файла във временната директория.

След тези проверки файлът се запазва в съответната директория на уеб сървъра и се изтрива от временната директория на сървъра, където се е извършила проверката.

HTML формата съдържа поле с името на файла - userfile. На PHP скрипта ще бъдат предадени пет променливи. Достъп до тях може да се осъществи чрез масива $HTTP_POST_FILES.

По-голямата част от скрипта се състои от проверка на грешки поради необходимостта да бъдат намалени потенциалните рискове за сигурността при качване на файловете, да се види дали каченият файл може да се покаже на потребителите, а също да се провери дали файлът е качен във временната директория от потребителския компютър или от външен за средата компютър. Целта е да се намалят потенциалните рискове за сигурността при качване на файловете.

Част от проверката се състои в това, да се установи дали каченият файл може да се покаже на браузера на посетителите.

Проверката започва с определянето на кода за грешка, върнат в променлива $HTTP_POST_FILES[‘userfile’][‘error’]. Този код за проверка е достъпен във версия на езика PHP 4.2.0. От версия PHP 4.3. и нагоре се въвеждат съответстващи на всеки връщан код на грешка константи [[3], 4].

Възможните константи и стойностите им са следните:

- UPLOAD_ERROR_OK = 0

- UPLOAD_ERR_INI_SIZE = 1 – означава, че размерът на качения файл надвишава максималната стойност, указана във файла PHP.INI чрез директивата UPLOAD_MAX_FILESIZE.
- UPLOAD_ERR_FORM_SIZE = 2 - означава, че размерът на качения файл надвишава максималната стойност, указана в MAX_FILE_SIZE елемента на HTML формата.
- UPLOAD_ERR_PARTIAL = 3 - означава, че файлът е качен частично.
- UPLOAD_ERR_NO_file = 4 - означава, че не е качен никакъв файл.

Ако се използва по-стара версия на PHP, някои от тези проверки може да се извършат ръчно. Може да се провери дали променливата с името на качвания файл $userfile е със стойност равна на "none". Тази стойност се установява от PHP, ако няма качен файл. Може също да се провери дали файлът има някакво съдържание (т.е. дали $userfile е по-голямо от 0).

Накрая, независимо от версията, може да се провери MIME типа на файла, като се тества $userfile_type (например в разглеждания случай може да е необходимо да се качват само текстови файлове).

След това се проверява дали файлът, който се опитваме да отворим, наистина се е качил и дали не е локален файл за сървъра, т.е. дали не е качен там от злонамерен потребител. Подобно действие представлява предпоставка за особено опасна заплаха.

След изпълнението на скрипта за проверка „upload.php", ако няма съобщения за грешка, файлът е копира в съответната *include* директория на сървъра (Фиг. 1).


*Фиг. 1. Показване на съдържание на директория include на сървъра*

След това е необходимо да се отвори файла, чрез функцията strip_tags(),да се премахват всички евентуално съдържащи се в него HTML и PHP тагове и да се запише отново на същото място.

Накрая се извежда съдържанието на файла, за да може потребителят да се увери, че качването е завършило успешно. След като се копира и преформатира, само при изрично указване в кода, каченият файл се извежда като потвърждение, че качването е протекло успешно.

Още през септември на далечната 2000 г. е открито слабо място в сигурността, което позволява на хакерите да накарат скрипта да обработи локален файл, все едно че е качен.

Проверка за местоположението на файла

За да се провери, че се обработва качен, а не локален файл се използват функциите: is_uploaded_file() и move_ uploaded_file(), които са достъпни от PHP версия 4.0.3, както и по-високи. Съществува и еквивалентен код за по-ранните версии на PHP.

Ако не се приложат тези две функции в скрипта, той може да се използва от злонамерен клиент, посетител или друг потребител, който да подмени временното име на файл с друго. По този начин той може да обработи (види, снеме, манипулира) важен файл, като например такъв с паролите за достъп до бази данни, данни от изпитни материали, данни за личните акаунти на личния състав, данни за бъдещи дейности, политики, ценен сорс код и др.

Като препоръчителни практики за приложение при разгледаната технология за качване на файлове могат да се посочат следните:

- Необходима е задължителна автентификация на потребителите.
- Наблюдаване и автоматизирано проверяване, чрез програмен код/ скрипт) на имената на качваните файлове. При съвпадение с файл от системните, конфигурационните, и пр., е налице кибератака срещу същността на съответния сайт, система, портал или сървър с данни по мениджмънт на кризи.
- Ако даден потребител качва непрекъснато файлове, задължително трябва да преименува качените файлове с имена, които се считат за безопасни.
- Да се контролира зоната, в която се качват файлове, чрез PHP.INI. Трябва да се установи директивата UPLOAD_TMP_DIR, така, че да сочи към директория, към която са приложени съответните права за достъп.
- Да се контролира големината на качваните файлове чрез директивата MEMORY_LIMIT. Тя определя максималния размер в байтове на файловете, които могат да се качват.

При последните версии на скриптовия език PHP, ако той е настроен да работи в безопасен режим, ще се получи съобщение за грешка, ако не съществува достъп до временната директория или файл. Това може да се избегне единствено, ако не се работи в безопасен режим. Също така може да се напише друг скрипт, не на PHP, който копира файла на достъпно място. След това този друг скрипт да се изпълни от нашия PHP със съответната технология на зареждане и изпълнение, която може да бъде предмет на друго изследване.

Заключение

В заключение може да се обобщи, че с изграждането и внедряването на автоматизирана информационна система и база данни в център за управление на кризи съответства на концепцията за прилагане на организационно - архитектурното моделиране на отбраната. По този начин се дава възможност на по-голям брой потребители да ползват информацията за мениджмънта на кризите, както поуките от практиката, свързани с участието на формирования от Българската армия при провеждането на операции от невоенен характер, при бедствия, аварии и катастрофи, както на наша територия, така и извън страната. Като перспективно направление за по-нататъшна работа може да се посочи необходимостта от разработването на информационно-справочна система по мениджмънт на кризи и поуки от практиката, като приложно програмно осигуряване на автоматизирана информационна система за мениджмънт на кризи.

**Благодарности.** Докладът е написан благодарение на финансиране от Министерство на образованието и науката в изпълнение на Националната стратегия за развитие на научните изследвания 2017 – 2030 по Национална научна програма „Сигурност и отбрана“, приета с решение на Министерски съвет № 731 от 21 октомври 2021 г.

Литература

[1] Бяла книга за отбраната и въоръжените сили на Република България, 2010 г.
[2] Веселина Гагъмова, Виолета Василева, Относно сценарий за пробив в сигурността на системи за електронно обучение и облачни информационни системи за съвместна работа при публикуване на съдържание на уеб сървъри. Десетата национална конференция за електронно обучение във висшите училища, 26-27.09. 2024 г. във Великотърновски университет "Св. св. Кирил и Методий" в гр. Велико Търново, сп. Дигитални образователни технологии, Изд. Великотърновския университет „Св. св. Кирил и Методий“, Том 1, 2/2024, стр. 125-132, ISSN: 3033-2044 (Online), ISSN: 3033-2036 (Print), COBISS.BG-ID - 72344328, DOI: https://doi.org/10.54664/AGKR8106 България. Налично на: https://www.uni-vt.bg/bul/pages/?page=6894&zid=150
[3] Люк Уелинг, Лаура Томсън, Разработване на проекти за Web с PHP и MySQL, СофтПрес, 2003.
[4] Лари Улман, Php и MySql за динамични Web сайтове, Алекс Софт; 2019.