

**JÉRI Tamás**

[jeri.tamas@bv.gov.hu](mailto:jeri.tamas@bv.gov.hu)

## THE SECURITY OF DATABASES IN CRITICAL INTERNET SERVICES

### *Abstract*

*Database management systems are essential subsystems of Critical Internet Services. They store data in rendering data sets or databases to operate the service. Without existing database security is however its confidentiality, integrity and accessibility cannot be realised. This paper focuses on these issues and analyses how safety and security can be retained in databases of Critical Internet Service.*

*A kritikus internetes szolgáltatások nélkülözhetetlen alrendszerei az adatbázis-kezelők, amelyek rendezett halmazban, adatbázisban tárolják a szolgáltatás működéséhez szükséges adatokat. Az adatbázis biztonsága létfontosságú a bizalmasság, a sértetlenség és a rendelkezésre állás megvalósulásához. Jelen írás arra keresi a választ, hogy miként tartható fenn a kritikus internetes szolgáltatások adatbázisainak biztonsága.*

**Keywords:** *Internet, service, database, database management system, security ~ Internet, szolgáltatás, adatbázis-kezelő, adatbázis, biztonság*

## INTRODUCTION

For Critical Internet Services (CISs) a database management system functions as an essential sub-system [1] fulfilling all the necessary duties of CIS to process data. As mentioned before, when operating and network relations are being regarded, positions of CIS and of database management system compared to each other, they self play a crucial role in data storage security. Beyond potentialities of position current study rather aims to analyse circumstances of operation and safety. This time research has been focused on data disposability, since role of database managers had already been examined and described in one author's former studies [2]. At the same time, existence of a close relationship between the two approaches must be highlighted since database management system needs to manage data while data cannot be provided without a database management system. Therefore, missing any of them can disable CIS operation. Therefore a database management system and the managed data should always be analysed together from the view-point of Critical Internet Service, namely, how transactions influence CIS. Although effects of missing database management system as an essential sub-system are known, but how databases and database-related transactions could affect CIS. This research was carried out along with the expectation that a database management system was standing at dispose constantly, therefore, able to complete various transactions. Moreover, databases could also have been accessed from it. It is said, that the greater life and soul of CIS stored data are or, from the point of view of the operation, the more valid they are the larger impact they will have on CIS. Referring complexity to data, confidentiality, integrity and disposability or accessibility can guarantee an appropriate CIS-operation. Therefore, compromising the system is most likely to lead to total failure of CIS as one of the main hazards.

In general, database management systems arrange write and read operations in databases, where read operations are meant for data reading while write operations assist new data processing or manipulating or deleting the already registered ones. From view-point of CIS, data mainly including dynamically changeable information are originally stored in databases they need to be uploaded first. The condition of uploading is that access points to database management systems just as necessary authorities are disposable and available. In most cases, Critical Internet Services provide different information based on data sets standing behind, but several times it also has to ensure enlargement, manipulation or deleting operations in terms of data-circle so, write operations must be carried out with database management system. To be able to select between user roles and make a decision, CIS need to know either one of the following two things: who were given access to what kind of data sets or what kinds of authorities are being possessed and by whom. In general, the decision itself is also based on user's data sets stored in the database. After a positive verification process, data become modifiable. Because of this protocol, it is easy to understand how a user with criminal intent could access to data verification providing rights to data manipulating transactions. If they would have the opportunity, they could access those data by carrying out read operations in a database management system. It is easily conceivable, that compromising a database needs two steps only if a user with criminal intent is able to access to the database management system operating behind the Critical Internet Service. As a result, default operation should already be reviewed to explore actual risks. No matter how excellent a system seems to be, it can always contain vulnerable points and they lead to damages of Critical Internet Service.

# 1. DATABASE MANAGEMENT IN CRITICAL INTERNET SERVICES

Success of database management is based on three fundamental things: realising accessibility, disposability of sufficient accesses to the database and finally, the absolving as many write operations as needed. Thereby, it can be divided in three equally important units. CIS-users can also be divided into groups depending on what kind of intentions they are using the service, whether they turn to the system with intention of a normal, proper use or they interfere with not-proper, even criminal purposes, like data compromising would be.

## 1.1 Database availability

Database availability means a connecting ability via the relevant interface, regardless the transfer media.

According to researcher's basic expectation, a database management system forms an inevitable sub-system of CIS which also involves necessity of certain conditions such as data-permeability and a constant correlation among the services. In favour of effective interworking, CIS needs to be able to access the database management system and through it relevant data which are necessary to its operation. In addition, system administrators also need to have a direct access to database management system to maintain databases. In conclusion of CIS' definition [3], database management is a constantly disposable system through which databases just as its data are also constant available. So, an accessible database management system also means database accessibility at the same time. Direct or indirect access to databases or data can be realised depending on user's position. Under indirect accession is meant when someone can have connection to database management system via an intermediate permeable programme only.

If the database management system also operates as a CIS sub-system, data transfer will be arranged by CIS itself as it has a mediator function between users and stored data. There is one adjustment only that a permanent connection must exist because of CIS default function. Therefore, all CIS users a direct access to database management system just as to databases.

## 1.2 Database accessibility

To get access to a database or to a database management system means to get connected via the disposable availabilities and to be able to manage data according to received authorities. Interworking between CIS and database management system needs to be configured and defining the accessions just as setting the authorities to relevant database transactions play parts in it. Practically, CIS has access to the database management system with a database account and all necessary database management authorities demanded in CIS' operation must be assigned to it. This account might include both write and read operations at the same time, depending on type of CIS. Taking CIS itself into consideration, the service is available and, as per its definition, it has access to the database, but it delivers indirect so, limited rights and authorities only to other users. As the matter of fact, according to a program code users are able to carry out different database transactions depending on their potentials to interfere. (Figure 1)

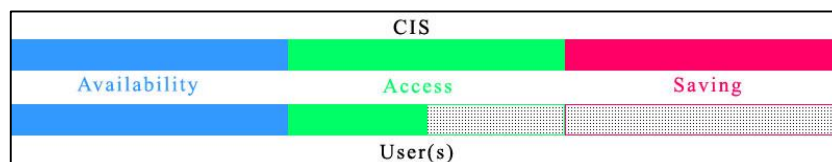


Figure 1: Users' discriminative database-use via CIS

Naturally, a CIS programme code does not involve such a part which would provide a unjustified larger scope for action to gain data, at the same time users with criminal intent want

to obtain protected database information in the short run, while data manipulating are their targets in the long run. Taking advantage of that a database account possesses authorities to the largest amount of database-transactions [4] necessary to CIS-operation, they try to make use of CIS and extend access into protected data of database.

For extension of an access CIS can be employed under the following circumstances:

- Information coming from server program, incorrect settings, error messages, programme errors, defaults, and informer signals can be collected and can contain data or information they are meant to be safe and might enable user to extend access.
- Through unverified or less monitored input interfaces, after injecting SQL<sup>1</sup> commands [5], queries can be extended and a CIS-provided access can be converted into a full access of user, against the original intent of programmer.
- While entering operating system, access to the database at layer of files becomes available exploiting the bug of server program.

Of course, it depends on type of CIS, whether it allows interactive interferes or not. If yes, the exploiting possibility of SQL on the basis of its linguistic characteristics<sup>2</sup> should also be considered. In case CIS-operator would run a user-board for users to have more rights and authorities to the service than the average after a successful verification, access could also be extended with injected quires, after obtaining top users data.

### 1.3 Write transactions in a database

This topic involves database transactions either in database structure or in stored data they are bound by authorisations of writing. Final stage of a compromising activity just as its main goal involves activities of deleting modifying or registering on database. It depends on type of CIS whether it only reads database data or also completes write operations as it is more common. It must be mentioned that data must be uploaded once even in case of a CIS carrying out read operations exclusively. It definitely means write operations at a certain point.

CIS must have authorities to complete write operations in its database while users demanding the service should be given rights and opportunities to data registering subject to certain conditions, according to a fix protocol of programme. Users with criminal intent aim to validate their rights to write operations that they obtained through extension of access as explained in more details before.

CIS administration is in close connection with database security since a user name-password matching specified in text boxes is applied to verify service administrator. As mentioned before, through an injection, users with criminal intent can reach access to stored user names and passwords first and then, misusing the already available information, they can enter CIS as system administrators and complete saving operations.

Depending on CIS' security system, attackers might apply brute-force<sup>3</sup> techniques based on repeatedly try-outs, or steal data as a result of data flow's play back. However, program code-given functions mainly determine what impacts database-compromising actions completed via CIS will have, it must be pointed out that these acts make both partial and full service failures possible.

---

SQL - Structured Query Language  
SELECT - UNION [4]

<sup>3</sup> „brute force”, also known as the full try-out method/ pattern

## 2. MAINTANANCE OF CIS-DATABASE

### 2.1 Indirect access

Because of practical reasons, system administrators install an intermediate, from the Internet accessible program onto CIS server that is applied for database management and its maintenance. In this way database managers can remain in the background of databases not being exposed to direct accessibility or attacks while doing maintenance work. In addition, database administration can be provided on the Internet. Use of this intermediate program is usually assigned to a less prominent, IP<sup>4</sup> based service of server. Beside of a sufficient invisibility, it can provide a decent service administration with a moderate amount of risks. As a matter of fact, there are applications of default or transpired accesses they mainly jeopardize the system, and use of links not being encrypted weakens it even more. In this way, users with criminal intent are given targets to attack.

### 2.2 Direct access

Having a direct access to the database management system means, that system can directly be linked with a client program across an established interface. It can be realized in both a file system and a network. Neither the intermediate program nor CIS itself do participate in accession to database management system. In this case the beforehand established connection is missing, therefore, users cannot obtain data with injection. Database management systems with direct access involve more risks since users able to access to transfer media can also connect them. It depends on what way of verification a database management system possesses. A database-access is carried out in accordance of users' rights and authorities and this way a user with criminal intent will be able to complete CIS' database-transactions after having obtained CIS' database-account.

An overloading attack (DoS<sup>5</sup>, DDoS<sup>6</sup>) is very harmful to a from the Internet open database management system with a network connection and, depending on its duration, it can also jeopardize CIS operation.

At the same time databases are protected or unprotected in a file system. Their protection level depends on accession authorities to the general transaction files. Concerning their structures and contents, they can be read or manipulated via any client programs of the database management system. In case of having authorities to read-operations, access at file-system level is suitable for data-obtaining, but authorities to write operations make serious damage-causing also possible.

## 3. EXPERIENCE OF THE AUTHOR

With the aim of experiment the author of this paper has tested a very popular media portal on the Internet. It is known that information-updating on the portal happens fast and regularly, the site wants to report on the most current news. This should mean that the portal is constantly maintained. This paper will not mention domain name of the website, because it is still operating using the same configuration as it was experienced at time of testing.

First, the generally used administrative URL<sup>7</sup> of interactive websites (<http://domain.name/admin>) was tested. To author's great surprise, an error message (Figure 2) was received sharing a number of important data about website's operation, such as

---

<sup>4</sup> Internet Protocol

<sup>5</sup> Denial of Service: attack in company of denial service

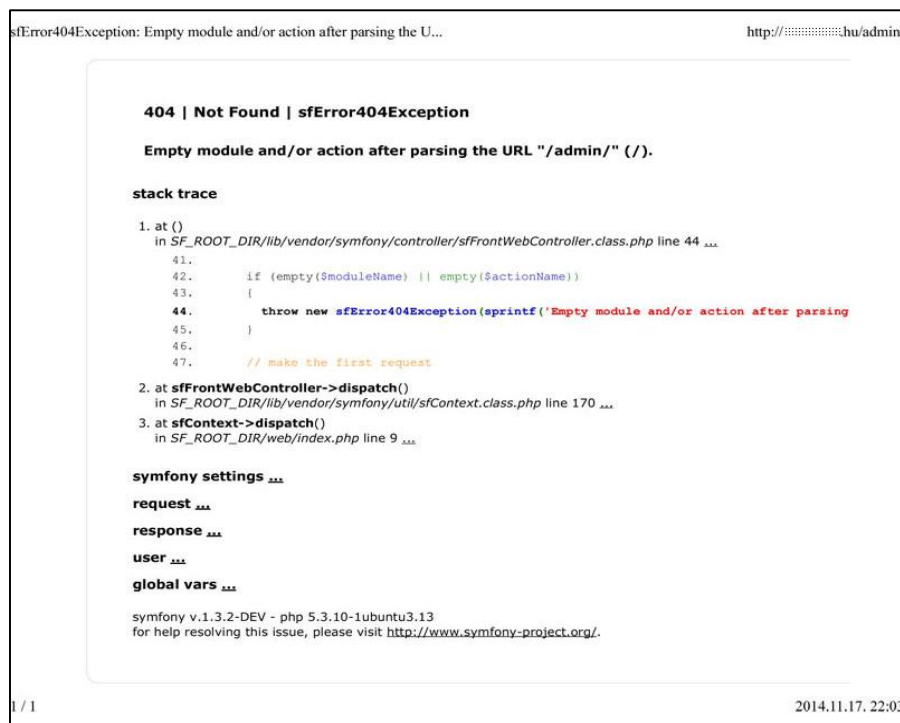
<sup>6</sup> Distributed Denial of Service: attack in company of distributed denial of service

<sup>7</sup> Uniform Resource Locator

information on operating system, web server, programming language, and content-producer engine.

Website operator has made a great mistake leaving error message management of the frame system in debug mode, namely in a communicative mode of operation. This has delivered information on self while completing all the given instructions.

Examination the source code of received error message led to even more surprises as it has contained all settings of the portal, even the name and password they enabled user(s) to access database. Thus, database account used by the service became known and so, as the next step, researcher had to find a direct link to MySQL<sup>8</sup> database management system that frame system applied. It was also tested whether server operators were using a direct database administration or not. The most popular administrative program is "phpMyAdmin"<sup>9</sup> which can be used with a PHP pre-processor on web server. Therefore research has begun in this direction aiming to find its signs. Behind the server's IP address located URL [/phpmyadmin](#) was better looked at while default settings formed test targets when the following log-in window appeared with the function of database-maintenance.



```
sfError404Exception: Empty module and/or action after parsing the U... http://:hu/admin

404 | Not Found | sfError404Exception

Empty module and/or action after parsing the URL "/admin/" (/).

stack trace
1. at ()
   in SF_ROOT_DIR/lib/vendor/symfony/controller/sfFrontWebController.class.php line 44 ...
   41.
   42.     if (empty($moduleName) || empty($actionName))
   43.     {
   44.         throw new sfError404Exception(sprintf('Empty module and/or action after parsing
   45.     }
   46.
   47.     // make the first request

2. at sfFrontWebController->dispatch()
   in SF_ROOT_DIR/lib/vendor/symfony/util/sfContext.class.php line 170 ...

3. at sfContext->dispatch()
   in SF_ROOT_DIR/web/index.php line 9 ...

symfony settings ...
request ...
response ...
user ...
global vars ...

symfony v.1.3.2-DEV - php 5.3.10-1ubuntu3.13
for help resolving this issue, please visit http://www.symfony-project.org/.
```

Figure 2: An informer error message

The previously obtained user name and password were correct and they enabled researcher to access database management system giving him unlimited authorities, as it was shown in Figure 3. Free access to all tables and data in portal's database were available. Through the database, even total data-asset of media portal and, therefore, the media portal itself were in researcher's hands. Of course, researcher did not abuse service and database remained untouched. Although operator had made fatal mistakes and the operation became attackable because of numerous inattention, the portal is still operating without deface. The only reason why this is possible is that the portal has not been targeted by users with criminal intent yet. During the experiment, no interference with need of strong skills was applied by the researcher, only a few default settings were tested that operator left open.

<sup>8</sup> <https://www.mysql.com>

<sup>9</sup> [http://www.phpmyadmin.net/home\\_page/index.php](http://www.phpmyadmin.net/home_page/index.php)

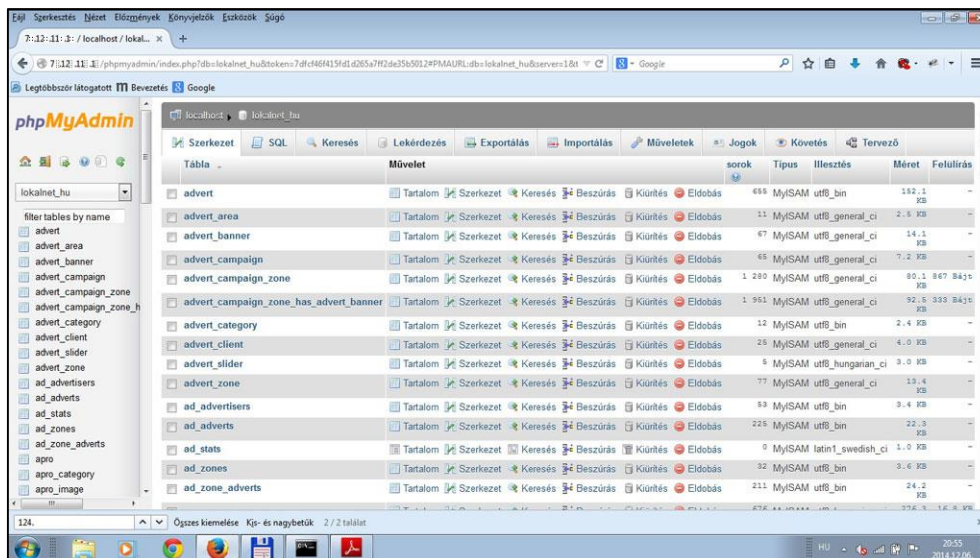


Figure 3: Gaining a database

## SUMMARY AND CONCLUSIONS

This study has analysed security of databases standing behind CIS from the view-points of availability, accessibility and data saving. Researcher wanted to find answers for two important questions: what effects of database compromising could have on CIS' default functions and what activities would lead to its influencing.

It is verifiable that initial expectation of research as CIS equals a constantly available Internet service already enables availability of database management system operating behind the service with constant links, as well as it makes a partial accessibility to the database also possible. CIS-related faults, careless attitude in its operation and even automatism may open up some opportunities to extend access to the database and, as a result, to compromise it. With criminal intent, the via CIS gained accesses to all the operating system, file system, database management system, and database could lead to a total service-crash.

Experience of the author was described to confirm that mal-configured online service systems without an appropriate database-security can easily end up as targets of attackers getting control over it.

## References:

- [1] Tamás Jéri: A kritikus internetes szolgáltatások alrendszerai (Subsystems of Critical Internet Services). Társadalom és Honvédelem, issue 2013/3-4, NKE Budapest, ISSN 1417-7293
- [2] Tamás Jéri: Az adatbázis-kezelők szerepe a kritikus internetes szolgáltatásokban (Roles of database management systems in Critical Internet Services). Hadmérnök, volume X, issue 1, March 2015, NKE Budapest, ISSN 1788- 1919.  
[http://hadmernok.hu/151\\_19\\_jerit\\_1.pdf](http://hadmernok.hu/151_19_jerit_1.pdf) - letöltve 2015.05.04
- [3] Tamás Jéri: Kritikus Internetes Szolgáltatások (Critical Internet Services). Hadmérnök, volume VIII, issue 1, March 2013, NKE Budapest, ISSN 1788- 1919.  
[http://hadmernok.hu/2013\\_1\\_jerit.pdf](http://hadmernok.hu/2013_1_jerit.pdf) - letöltve 2014.01.25
- [4] János Szelezsán: Adatbázisok (Databases), ISBN 963 577 189 4. LSI Oktatóközpont (LSI Training Centre)

- [5] Rita Fleiner: SQL injekcióra épülő támadások és védekezési lehetőségek. SQL injection attacks and defence opportunities. Hadmérnök, issue 2008 (III.)/4, pages 117-128, ISSN 1788- 1919. [http://hadmernok.hu/archivum/2008/4/2008\\_4\\_fleiner.pdf](http://hadmernok.hu/archivum/2008/4/2008_4_fleiner.pdf) - letöltve 2015.05.04
- [6] Andrew S. Tanenbaum: Számítógép-hálózatok (Andrew S. Tanenbaum: Computer Networks), ISBN 963 545 384 1. Panem Könyvkiadó Kft., Budapest 2004.