Creation and implementation of the Intruders module for security improvement from logs files generated in systems developed in Yii2 Framework

Jonathan De La Cruz Álvarez, José Ángel Jesús Magaña, José Manuel Gómez Zea, José Ney Garrido Vázquez, José Alejandro Hernández Cadena

National Technological Institute of Mexico / Technological Institute of Villahermosa. Systems and Computing Department. Highway Villahermosa - Frontera Km. 3.5 Ciudad Industrial Villahermosa, Tabasco, Mexico. C.P. 86010.

Abstract

Each time computer attackers are looking for how to get hold of the valuable information that companies' web systems have; Today, this has become a laborious task for administrators. Due to the above, it is necessary that these systems not only prevent attacks, but also have mechanisms for identifying and stopping intruders.

In this article, we will have the opportunity to learn about the "Intruders" module, created based on the data obtained from the use of logging in systems developed in Yii2 Framework, the information generated by this framework is a primary source in the error analysis and stopping processes, as well as user behavior.

Keywords: *Logs, Yii, Logging, Vulnerabilities.*

1. INTRODUCTION

"The COVID-19 pandemic has highlighted the need for more security in the digital world. People have increased their online presence to maintain personal and professional relationships, while cybercriminals have taken advantage of this situation…" (ENISA)

Faced with such a situation, all systems are under constant attack by intruders, locally or remotely; Therefore, their security not only lies in prevention but also in identification, the less time has passed since the intrusion identification, the less damage will be; To achieve this, it is important to constantly monitor the system.

"Web systems are in the focus of cybercriminals. For the detection of these attacks, log file analysis is often preferred, as anomalies in user requests and related server responses could be clearly identified. Two main reasons for this preference are that log files are readily available, and there is no need for expensive hardware for analysis, although server log files are an alternative source of identification for website attacks that are not being exploited." (Chinguel-Tineo, Arcila-Diaz, Tuesta-Monteza, & Mejia-Cabrera, 2018)

There are several types of log files that have different functions, among the main ones are:

- Help solve errors.
- Early stopping of system abuses.
- Show us the traceability of the records (What? Who? When? Through what means?).

This article proposes the use of the "Intruders" module, which uses the information generated by the logging in systems developed with Yii2 Framework, to identify and stop intruders, as well as to view user income statistics.

2. RECORD OF ANNOTATIONS

Yii2 Framework, according to the official website of the framework tells us that "Yii is a generic web programming framework, which means that it can be used to develop all kinds of web applications in PHP. Due to its component-based architecture and sophisticated cache support, it is especially suitable for the development of large applications, such as web pages, forums, content management systems (CMS), e-commerce projects, compatible web services. REST architecture and many more. " (yiiframework)

Yii2 is a framework, which includes among its main characteristics the use of the MVC architecture pattern, from this pattern we can highlight:

a) "Allow substitution of user interfaces.
b) Generate components of the interfaces.
c) Design simultaneous views of the same model.
d) Easily apply changes to the interfaces." (Camarena Sagredo, Trueba Espinosa, Martínez Reyes, & López García, 2012)

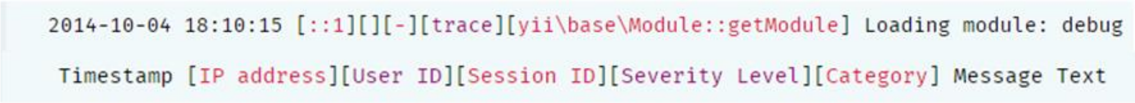
"Yii2 provides us with a powerful framework dedicated to logging that is highly customizable and extensible. Using this framework, you can easily save annotations (logs) of various types of messages, filter them, and unify them in different destinations that can be files, databases or emails. " (yiiframework)

The information obtained from the log is processed in 2 ways:

- Insertion of the main data collected in a MySQL table.
- Creation of the logs files, which are physical files, saved in the / runtime / logs folder, in our project.

"A log file (commonly known as Log file) arises from the need, on the part of the administrator, to maintain control over the system and can be defined as a file in which all the activity carried out by a system during a specific period of time. Therefore, it allows us to know information about What? - Who? - When? - Where? - How? - Why?" of a certain event. " (Mateos Mohino, 2017)

The log files generated by the log file have the following format:



```
2014-10-04 18:10:15 [::1][][-][trace][yii\base\Module::getModule] Loading module: debug

 Timestamp [IP address][User ID][Session ID][Severity Level][Category] Message Text
```

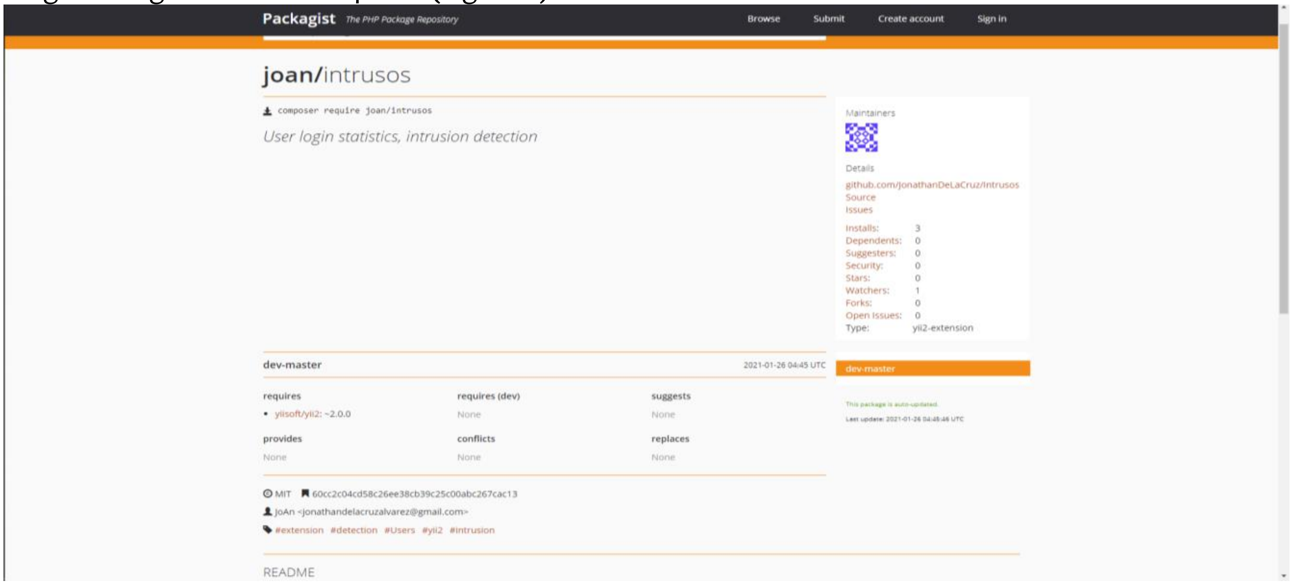
Figure 1. Yiiframework, 2020, Message Formatting [Image]. Recover from https://www.yiiframework.com/doc/guide/2.0/en/runtime-logging

The "Intruders" module takes as a base the information processed from the log; It is divided into three sub-modules that are responsible for identifying:

i. The number of users who successfully log in.
ii. The IPs that are trying to look for some type of computer vulnerability or security hole typical of web applications.
iii. Isolated errors that can be corrected in a timely manner.

3. LOG PROCESSING

The module was created and saved as a repository available online for any user, downloadable through the package manager for PHP Composer (Figure 2).



joan/intrusos

composer require joan/intrusos

User login statistics, intrusion detection

Maintainers

Details

github.com/JonathanDeLaCruz/Intrusos
Source
Issues

Installs:	3
Dependents:	0
Suggesters:	0
Security:	0
Stars:	0
Watchers:	1
Forks:	0
Open Issues:	0
Type:	yii2-extension

dev-master 2021-01-26 04:45 UTC

requires	requires (dev)	suggests
yiisoft/yii2: ~2.0.0	None	None
provides	**conflicts**	**replaces**
None	None	None

MIT 60cc2c04cd58c26ee38cb39c25c00abc267cac13
JoAn <jonathandelacruzalvarez@gmail.com>
#extension #detection #Users #yii2 #intrusion

README

dev-master

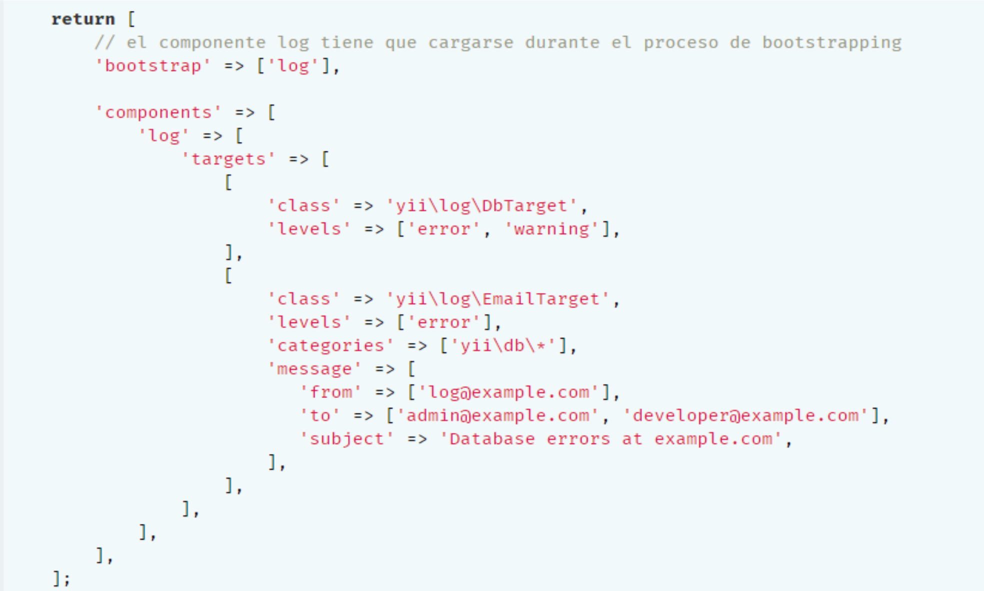
This package is auto-updated.

Last update: 2021-01-26 04:45:46 UTC

Figure 2. Packagist, 2020, joan/intruders [Image]. Recover from https://packagist.org/packages/joan/intrusos

The "Intruders" module processes the log files in real time. By obtaining the data provided by the log records, the security of the system is controlled and improved in a positive and efficient way. For the commissioning of the module, the following stages were required:

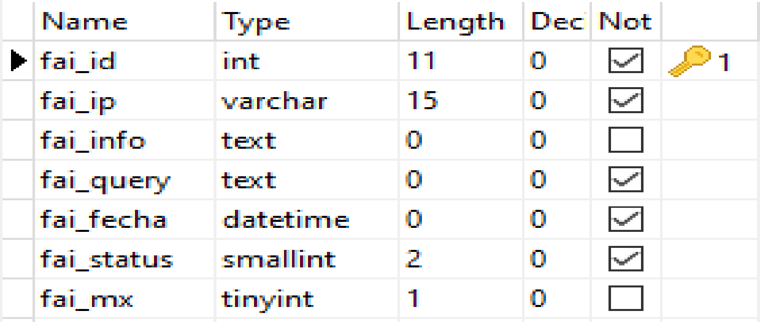
1.- The framework configurations are made in the /config/web.php file (figure 3), which allow the saving of the most important and necessary information to identify the IPs that are trying to search for vulnerabilities; Through the record destination we save the data in the structure of a MySQL table, see figure 4.



```
return [
    // el componente log tiene que cargarse durante el proceso de bootstrapping
    'bootstrap' => ['log'],

    'components' => [
        'log' => [
            'targets' => [
                [
                    'class' => 'yii\log\DbTarget',
                    'levels' => ['error', 'warning'],
                ],
                [
                    'class' => 'yii\log\EmailTarget',
                    'levels' => ['error'],
                    'categories' => ['yii\db\*'],
                    'message' => [
                       'from' => ['log@example.com'],
                       'to' => ['admin@example.com', 'developer@example.com'],
                       'subject' => 'Database errors at example.com',
                    ],
                ],
            ],
        ],
    ],
];
```

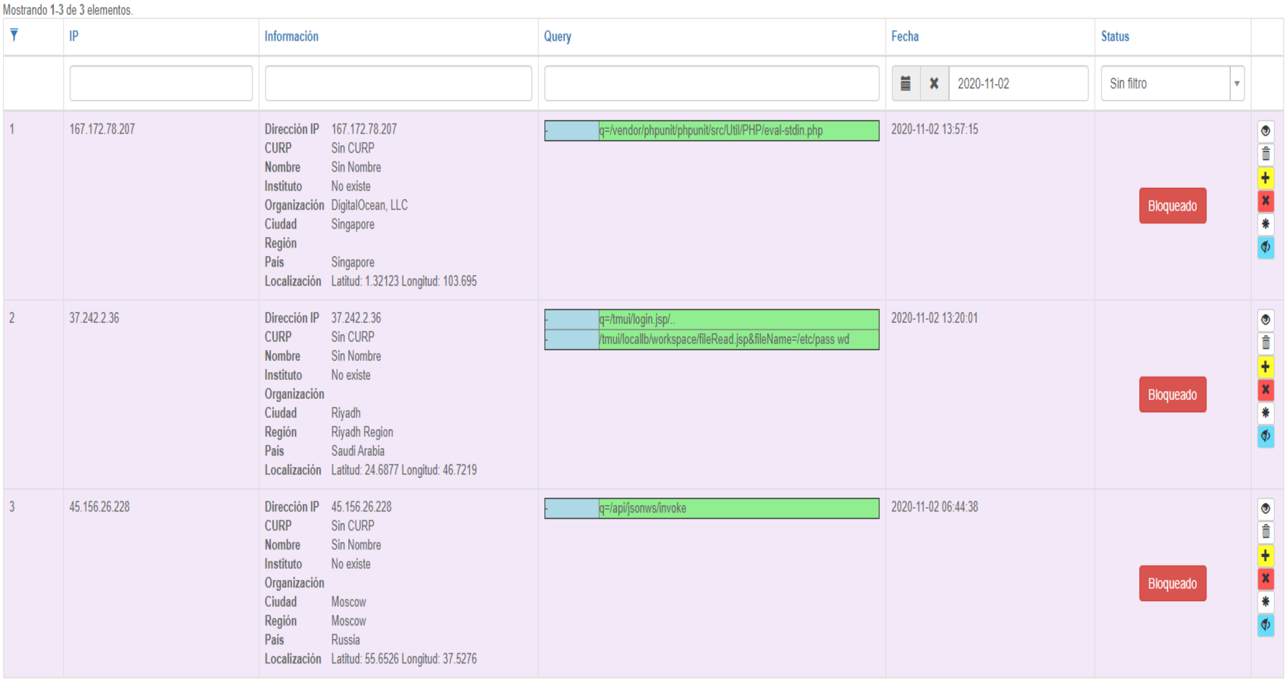
Figure 3. yiiframework, 2020, Log Targets [Image]. Recover from https://www.yiiframework.com/doc/ guide / 2.0 / en / runtime-logging



	Name	Type	Length	Dec	Not	
▶	fai_id	int	11	0	☑	🔑 1
	fai_ip	varchar	15	0	☑	
	fai_info	text	0	0	□	
	fai_query	text	0	0	☑	
	fai_fecha	datetime	0	0	☑	
	fai_status	smallint	2	0	☑	
	fai_mx	tinyint	1	0	□	

Figure 4. Own elaboration, 2020, Description of MySQL table [Image].

2.- With the data stored in the table, the first sub-module is built, dedicated to preventing malicious attacks from unknown users. An algorithm dedicated to identifying users who tried to enter different suspicious routes was developed and, with more interest, when the IP is not from the interior of Mexico, said IP is blocked and thus access to the system is denied (figure 5). The system provides the administration of the detected IPs, the administrator can review the detailed location information and other data that an IP can provide us. Among the allowed options: 🗑 Delete, + give an opportunity in case we notice that it was not the intention of the user, ✖ block, ✱ give recursive opportunities to test parts of the system and 👁 hide the registry.

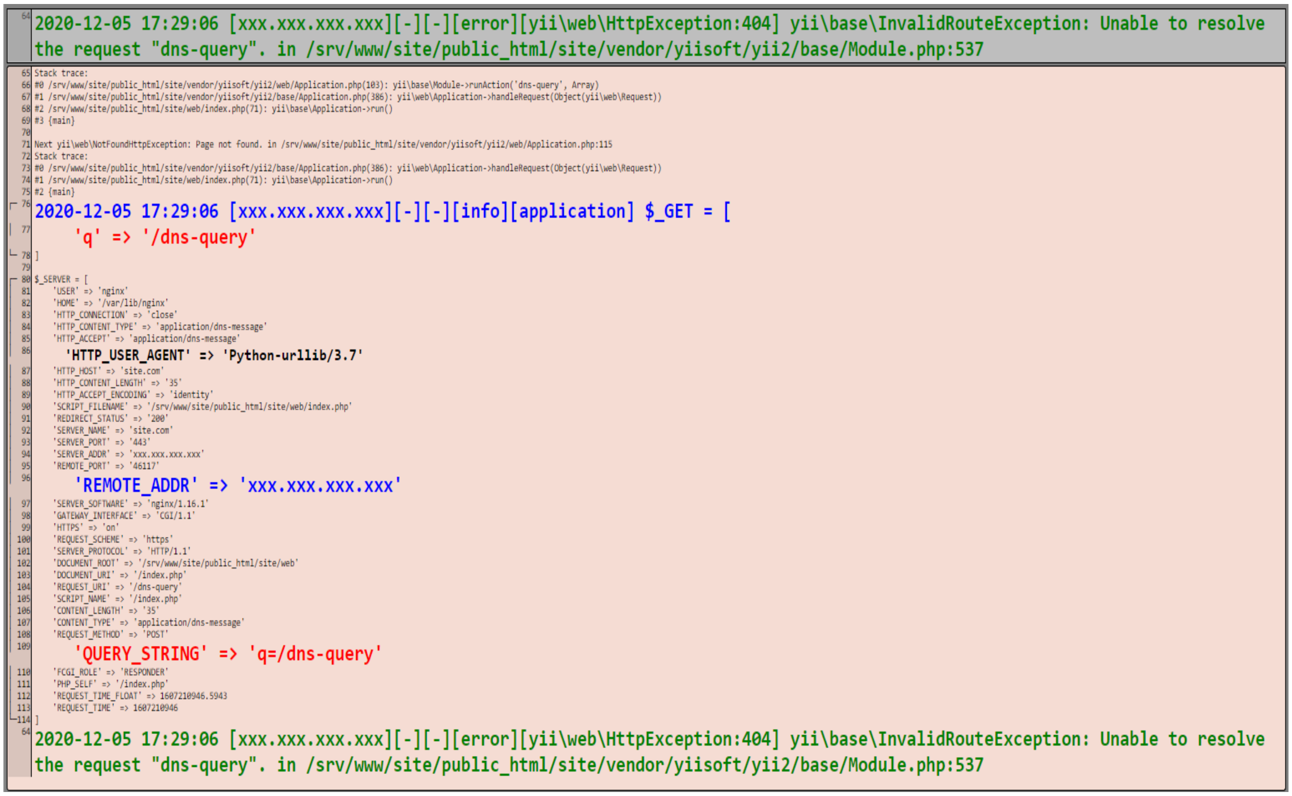


Mostrando 1-3 de 3 elementos.

	IP	Información	Query	Fecha	Status	
				2020-11-02	Sin filtro	
1	167.172.78.207	Dirección IP 167.172.78.207 CURP Sin CURP Nombre Sin Nombre Instituto No existe Organización DigitalOcean, LLC Ciudad Singapore Región País Singapore Localización Latitud: 1.32123 Longitud: 103.695	q=/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php	2020-11-02 13:57:15	Bloqueado	👁 🗑 + ✖ ✱ 👁
2	37.242.2.36	Dirección IP 37.242.2.36 CURP Sin CURP Nombre Sin Nombre Instituto No existe Organización Ciudad Riyadh Región Riyadh Region País Saudi Arabia Localización Latitud: 24.6877 Longitud: 46.7219	q=/tmui/login.jsp/.. /tmui/locallb/workspace/fileRead.jsp&fileName=/etc/pass wd	2020-11-02 13:20:01	Bloqueado	👁 🗑 + ✖ ✱ 👁
3	45.156.26.228	Dirección IP 45.156.26.228 CURP Sin CURP Nombre Sin Nombre Instituto No existe Organización Ciudad Moscow Región Moscow País Russia Localización Latitud: 55.6526 Longitud: 37.5276	q=/api/jsonws/invoke	2020-11-02 06:44:38	Bloqueado	👁 🗑 + ✖ ✱ 👁

Figure 5. Own elaboration, 2020, Intruder administration submodule [Image].

3.- By default, the logs files include the values of the following PHP global variables: $ _GET, $ _POST, $ _FILES, $ _COOKIE, $ _SESSION and $ _SERVER, this information is of great importance. Many of these variables provide data that helps us detect attacks. The log file viewer submodule, which displays the files generated by the log records on the screen, is configured to highlight the following important variables:



```
2020-12-05 17:29:06 [xxx.xxx.xxx.xxx][-][-][error][yii\web\HttpException:404] yii\base\InvalidRouteException: Unable to resolve
the request "dns-query". in /srv/www/site/public_html/site/vendor/yiisoft/yii2/base/Module.php:537
Stack trace:
#0 /srv/www/site/public_html/site/vendor/yiisoft/yii2/web/Application.php(103): yii\base\Module->runAction('dns-query', Array)
#1 /srv/www/site/public_html/site/vendor/yiisoft/yii2/base/Application.php(386): yii\web\Application->handleRequest(Object(yii\web\Request))
#2 /srv/www/site/public_html/site/web/index.php(71): yii\base\Application->run()
#3 {main}

Next yii\web\NotFoundHttpException: Page not found. in /srv/www/site/public_html/site/vendor/yiisoft/yii2/web/Application.php:115
Stack trace:
#0 /srv/www/site/public_html/site/vendor/yiisoft/yii2/base/Application.php(386): yii\web\Application->handleRequest(Object(yii\web\Request))
#1 /srv/www/site/public_html/site/web/index.php(71): yii\base\Application->run()
#2 {main}
2020-12-05 17:29:06 [xxx.xxx.xxx.xxx][-][-][info][application] $_GET = [
    'q' => '/dns-query'
]

$_SERVER = [
    'USER' => 'nginx'
    'HOME' => '/var/lib/nginx'
    'HTTP_CONNECTION' => 'close'
    'HTTP_CONTENT_TYPE' => 'application/dns-message'
    'HTTP_ACCEPT' => 'application/dns-message'
    'HTTP_USER_AGENT' => 'Python-urllib/3.7'
    'HTTP_HOST' => 'site.com'
    'HTTP_CONTENT_LENGTH' => '35'
    'HTTP_ACCEPT_ENCODING' => 'identity'
    'SCRIPT_FILENAME' => '/srv/www/site/public_html/site/web/index.php'
    'REDIRECT_STATUS' => '200'
    'SERVER_NAME' => 'site.com'
    'SERVER_PORT' => '443'
    'SERVER_ADDR' => 'xxx.xxx.xxx.xxx'
    'REMOTE_PORT' => '46117'
    'REMOTE_ADDR' => 'xxx.xxx.xxx.xxx'
    'SERVER_SOFTWARE' => 'nginx/1.16.1'
    'GATEWAY_INTERFACE' => 'CGI/1.1'
    'HTTPS' => 'on'
    'REQUEST_SCHEME' => 'https'
    'SERVER_PROTOCOL' => 'HTTP/1.1'
    'DOCUMENT_ROOT' => '/srv/www/site/public_html/site/web'
    'DOCUMENT_URI' => '/index.php'
    'REQUEST_URI' => '/dns-query'
    'SCRIPT_NAME' => '/index.php'
    'CONTENT_LENGTH' => '35'
    'CONTENT_TYPE' => 'application/dns-message'
    'REQUEST_METHOD' => 'POST'
    'QUERY_STRING' => 'q=/dns-query'
    'FCGI_ROLE' => 'RESPONDER'
    'PHP_SELF' => '/index.php'
    'REQUEST_TIME_FLOAT' => 1607210946.5943
    'REQUEST_TIME' => 1607210946
]
2020-12-05 17:29:06 [xxx.xxx.xxx.xxx][-][-][error][yii\web\HttpException:404] yii\base\InvalidRouteException: Unable to resolve
the request "dns-query". in /srv/www/site/public_html/site/vendor/yiisoft/yii2/base/Module.php:537
```

Figure 6. Own elaboration, 2020, Sub-module reading logs files [Image].

- The query string that is sent by the GET method to the system.
- The source IP address from which the user is viewing the system ('REMOTE_ADDR').
- Address of the source page (if any) used by the user agent for system query ('HTTP_REFERER').
- The string that indicates the user agent used to access the system ('HTTP_USER_AGENT').
- If it exists, the system query string ('QUERY_STRING').

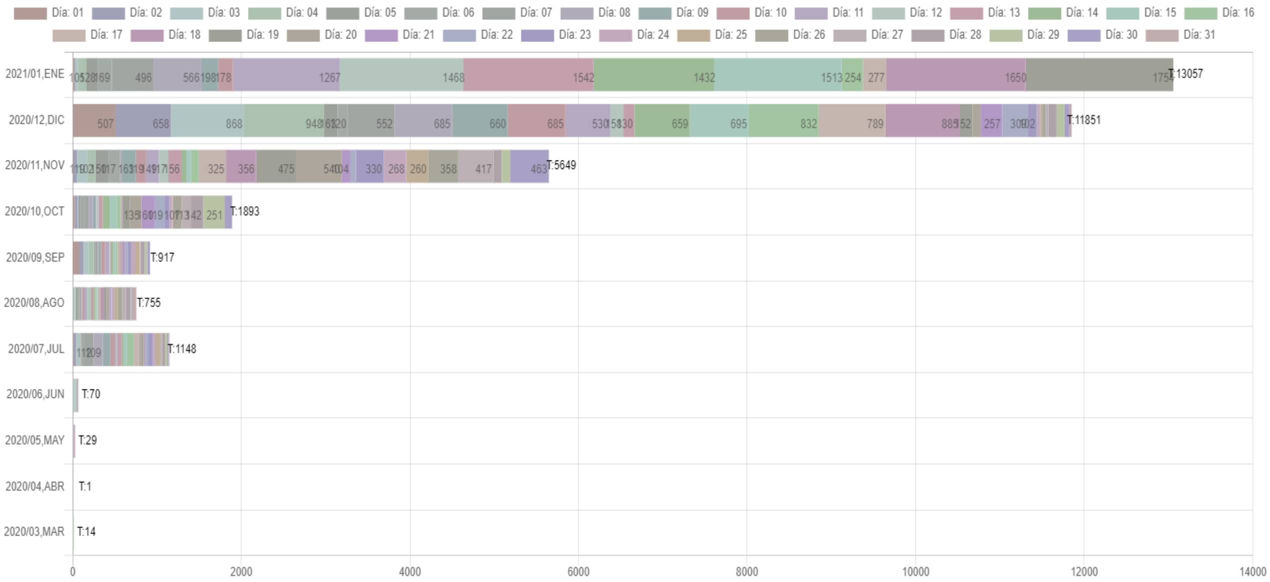


Figure 7. Own elaboration, 2021, Successful visits per month [Image].

4.- The third sub-module in charge of visualizing the successful entry of users, so that we can see how the system is being visited and used more frequently since its launch, generating graphs for hours, days, weeks, fortnights, months and years. See figure 7 and 9.

The "Intruders" module allows the system to carry out additional control over security, controlling unwanted visiting users and verifying the statistics of authorized use.

4. CONCLUSION

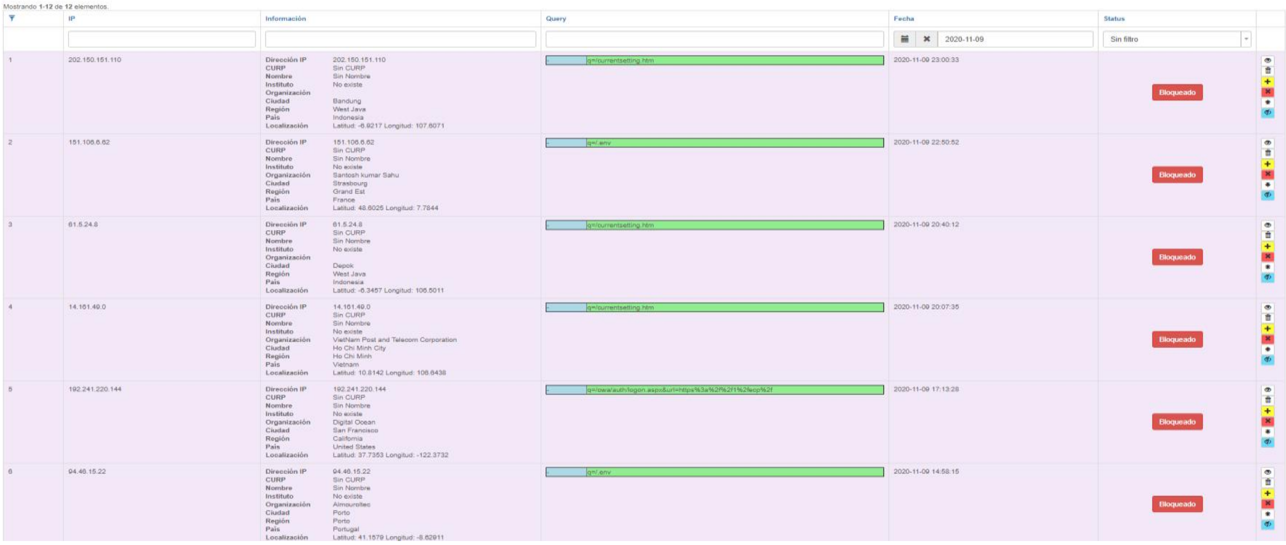
In conclusion, the information that the Yii2 framework annotations record offers us is very useful for early stopping of attack attempts and thus reducing them, correcting errors and displaying successful logins to the system.

The intruder module provides us with three sub-modules:

- Intruder management: In charge of verifying if users are really attackers, since many times they are errors caused by wrong typing, access tests from other systems, etc., thus allowing the ease of unlocking, deleting, giving another chance, hide or give recursion to user access.
- Log file viewer: Highlights the most important data in the log file, which is plain text; allows us to save the log file in a separate folder and, thanks to this, a new file is generated so as not to have all the information in just one; All of this helps to have quick non-physical access to the file, since many times only administrators are allowed access, thus allowing developers or support personnel to review the file and identify errors and / or security problems.
- Statistics: Provides access graphs in time periods (hours, days, weeks, fortnights, months and yearly).

Among the results obtained from the implementation of the "Intruders" module, we can visualize the following behaviors:

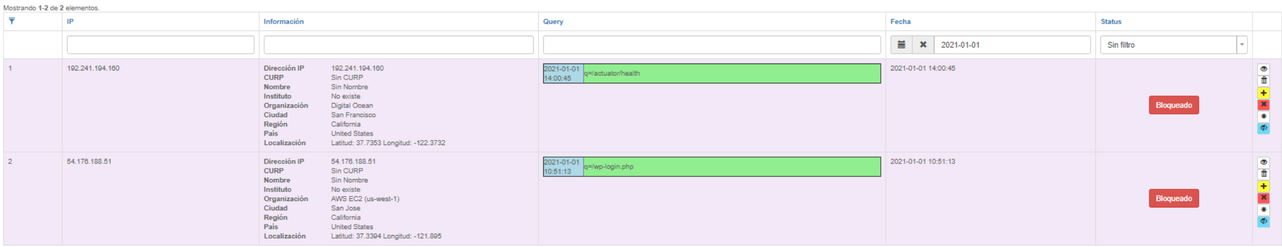
1.- 70% reduction in errors and attempts to search for vulnerabilities in the system.



Mostrando 1-12 de 12 elementos.

	IP	Información	Query	Fecha	Status	
				✖ 2020-11-09	Sin filtro	
1	202.150.151.110	Dirección IP 202.150.151.110 CURP Sin CURP Nombre Sin Nombre Instituto No existe Organización Ciudad Bandung Región West Java País Indonesia Localización Latitud: -6.9217 Longitud: 107.6071	- q=/currentsetting.htm	2020-11-09 23:00:33	Bloqueado	
2	151.106.6.62	Dirección IP 151.106.6.62 CURP Sin CURP Nombre Sin Nombre Instituto No existe Organización Santosh kumar Sahu Ciudad Strasbourg Región Grand Est País France Localización Latitud: 48.6025 Longitud: 7.7844	- q=/.env	2020-11-09 22:50:52	Bloqueado	
3	61.5.24.8	Dirección IP 61.5.24.8 CURP Sin CURP Nombre Sin Nombre Instituto No existe Organización Ciudad Depok Región West Java País Indonesia Localización Latitud: -6.3457 Longitud: 106.5011	- q=/currentsetting.htm	2020-11-09 20:40:12	Bloqueado	
4	14.161.49.0	Dirección IP 14.161.49.0 CURP Sin CURP Nombre Sin Nombre Instituto No existe Organización VietNam Post and Telecom Corporation Ciudad Ho Chi Minh City Región Ho Chi Minh País Vietnam Localización Latitud: 10.8142 Longitud: 106.6438	- q=/currentsetting.htm	2020-11-09 20:07:35	Bloqueado	
5	192.241.220.144	Dirección IP 192.241.220.144 CURP Sin CURP Nombre Sin Nombre Instituto No existe Organización Digital Ocean Ciudad San Francisco Región California País United States Localización Latitud: 37.7353 Longitud: -122.3732	- q=/owa/auth/logon.aspx&url=https%3a%2f%2f1%2fecp%2f	2020-11-09 17:13:28	Bloqueado	
6	94.46.15.22	Dirección IP 94.46.15.22 CURP Sin CURP Nombre Sin Nombre Instituto No existe Organización Almouroltec Ciudad Porto Región Porto País Portugal Localización Latitud: 41.1579 Longitud: -8.62911	- q=/.env	2020-11-09 14:58:15	Bloqueado	

Figure 8a. Author's elaboration, 2021, Intruders 2020-11-09 [Image].



Mostrando **1-2** de **2** elementos.

	IP	Información	Query	Fecha	Status	
				2021-01-01	Sin filtro	
1	192.241.194.160	**Dirección IP** 192.241.194.160 **CURP** Sin CURP **Nombre** Sin Nombre **Instituto** No existe **Organización** Digital Ocean **Ciudad** San Francisco **Región** California **País** United States **Localización** Latitud: 37.7353 Longitud: -122.3732	2021-01-01 14:00:45 q=/actuator/health	2021-01-01 14:00:45	Bloqueado	
2	54.176.188.51	**Dirección IP** 54.176.188.51 **CURP** Sin CURP **Nombre** Sin Nombre **Instituto** No existe **Organización** AWS EC2 (us-west-1) **Ciudad** San Jose **Región** California **País** United States **Localización** Latitud: 37.3394 Longitud: -121.895	2021-01-01 10:51:13 q=/wp-login.php	2021-01-01 10:51:13	Bloqueado	

Figure 8b. Author's elaboration, 2021, Intruders 2021-01-01 [Image].

2.- Positive increase in the use of the system, showing on which days of the week it is most used.

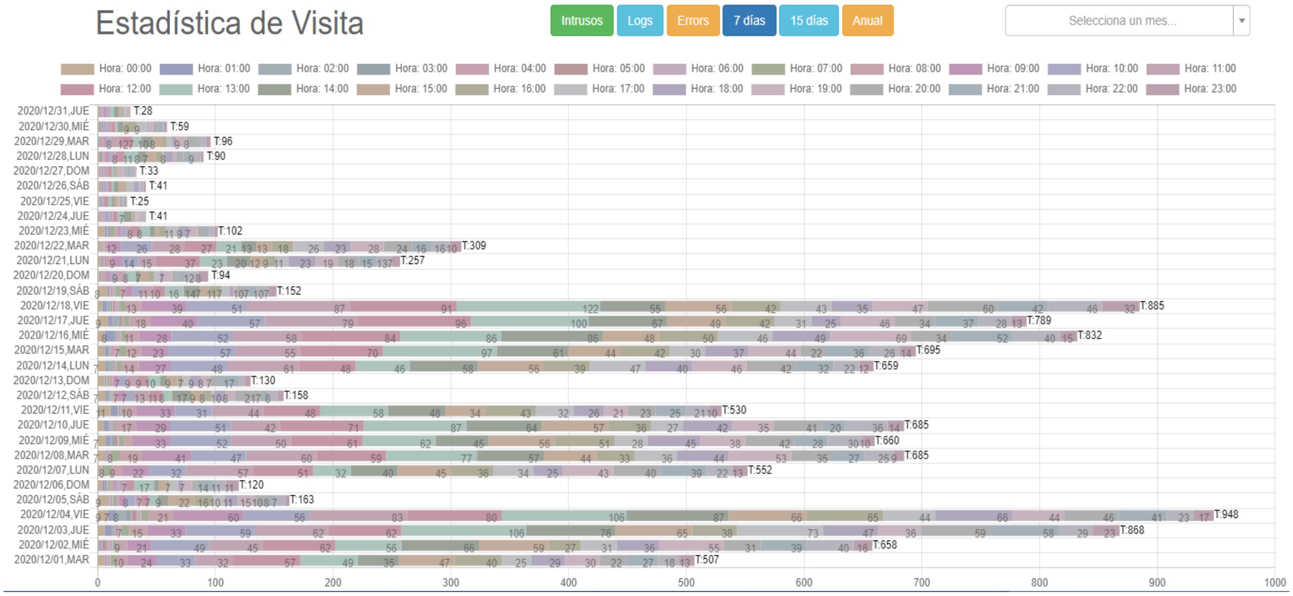


Figure 9a. Author's elaboration, 2021, Successful visits by days of the month of December 2020 [Image].

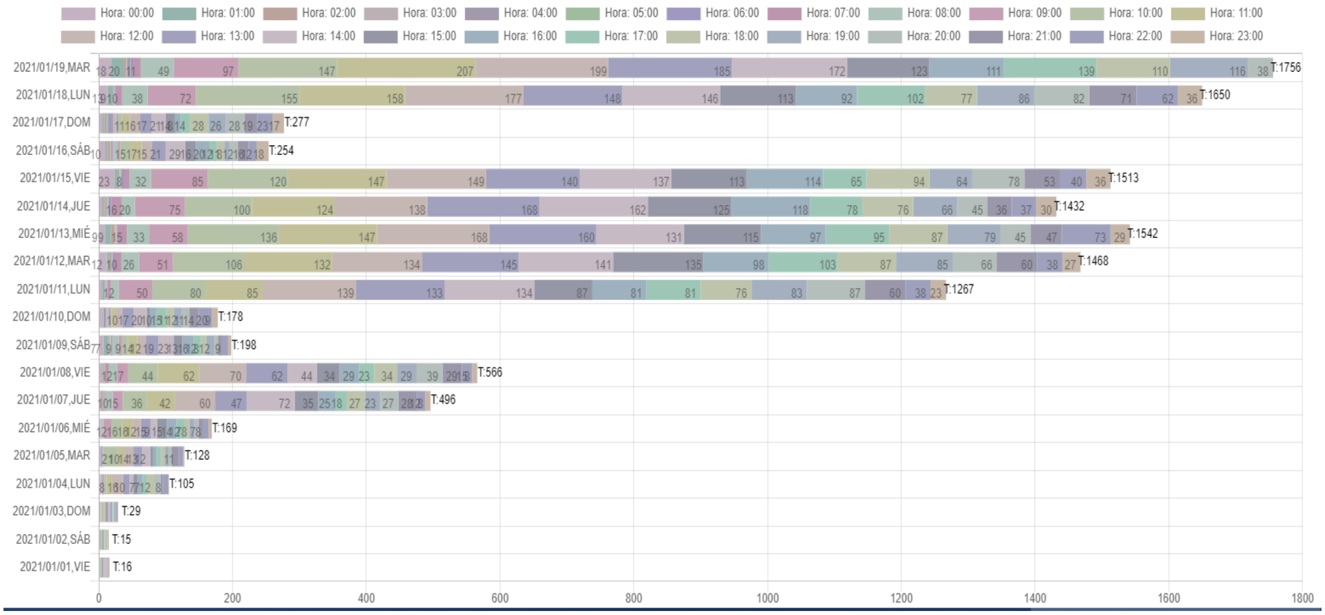
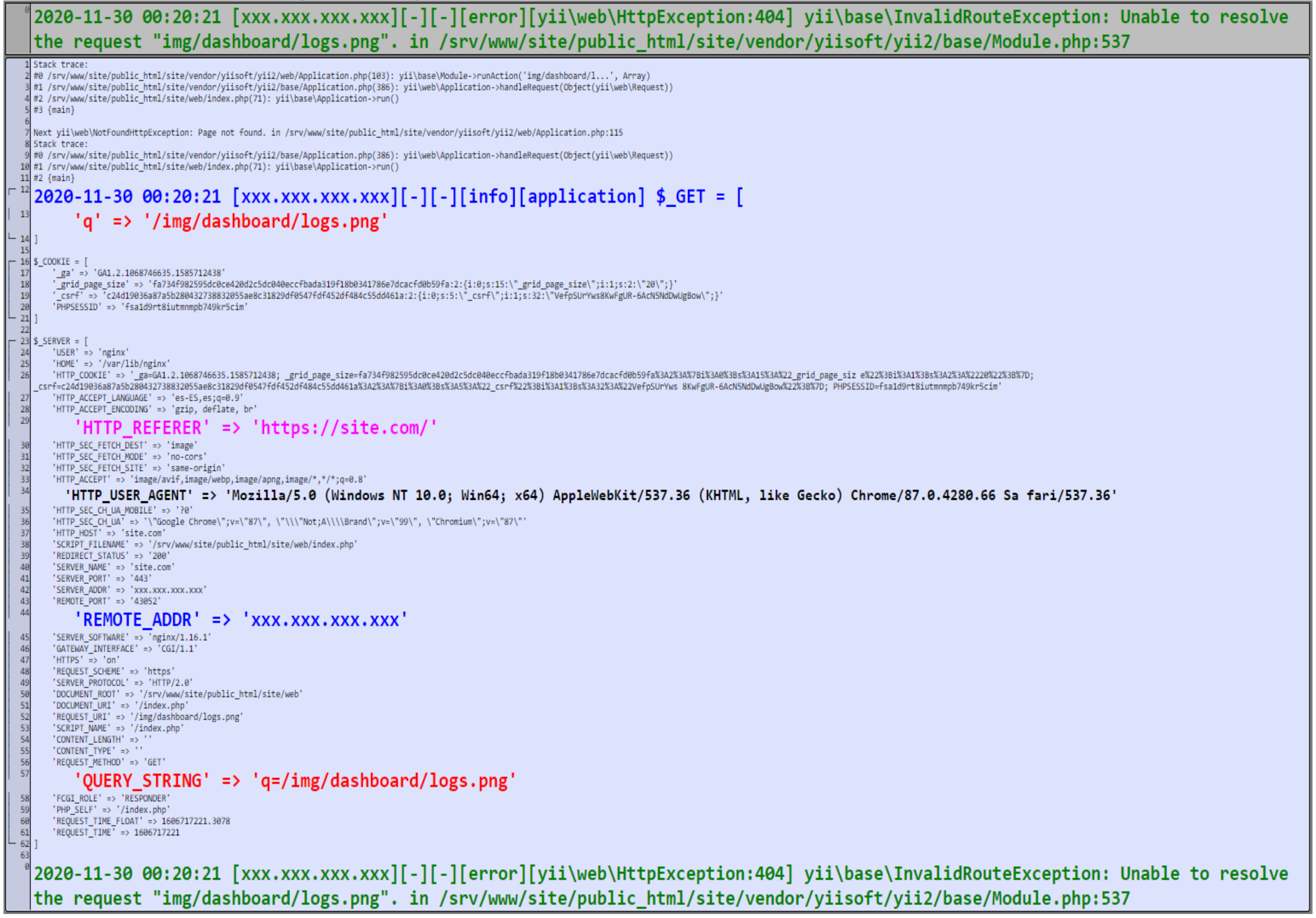


Figure 9b. Author's elaboration, 2021, Successful visits by days of the month of January 2021 [Image].

3.- Detention of 85% of failures in the algorithms of the system that, in a timely manner, solutions were provided. For example, see in figure 10, where the log warns us that an image is missing in a view that, although it is a failure that allows the process to continue, being able to interact with the file allowed us to solve it by placing the image in the correct path to its use.



```
2020-11-30 00:20:21 [xxx.xxx.xxx.xxx][-][-][error][yii\web\HttpException:404] yii\base\InvalidRouteException: Unable to resolve
the request "img/dashboard/logs.png". in /srv/www/site/public_html/site/vendor/yiisoft/yii2/base/Module.php:537

Stack trace:
#0 /srv/www/site/public_html/site/vendor/yiisoft/yii2/web/Application.php(103): yii\base\Module->runAction('img/dashboard/l...', Array)
#1 /srv/www/site/public_html/site/vendor/yiisoft/yii2/base/Application.php(386): yii\web\Application->handleRequest(Object(yii\web\Request))
#2 /srv/www/site/public_html/site/web/index.php(71): yii\base\Application->run()
#3 {main}

Next yii\web\NotFoundHttpException: Page not found. in /srv/www/site/public_html/site/vendor/yiisoft/yii2/web/Application.php:115
Stack trace:
#0 /srv/www/site/public_html/site/vendor/yiisoft/yii2/base/Application.php(386): yii\web\Application->handleRequest(Object(yii\web\Request))
#1 /srv/www/site/public_html/site/web/index.php(71): yii\base\Application->run()
#2 {main}
2020-11-30 00:20:21 [xxx.xxx.xxx.xxx][-][-][info][application] $_GET = [
    'q' => '/img/dashboard/logs.png'
]

$_COOKIE = [
    '_ga' => 'GA1.2.1068746635.1585712438'
    '_grid_page_size' => 'fa734f982595dc0ce420d2c5dc040eccfbada319f18b0341786e7dcacfd0b59fa:2:{i:0;s:15:\"_grid_page_size\";i:1;s:2:\"20\";}'
    '_csrf' => 'c24d19036a87a5b280432738832055ae8c31829df0547fdf452df484c55dd461a:2:{i:0;s:5:\"_csrf\";i:1;s:32:\"VefpSUrYws8KwFgUR-6AcN5NdDwUgBow\";}'
    'PHPSESSID' => 'fsa1d9rt8iutmnmpb749kr5cim'
]

$_SERVER = [
    'USER' => 'nginx'
    'HOME' => '/var/lib/nginx'
    'HTTP_COOKIE' => '_ga=GA1.2.1068746635.1585712438; _grid_page_size=fa734f982595dc0ce420d2c5dc040eccfbada319f18b0341786e7dcacfd0b59fa%3A2%3A%7Bi%3A0%3Bs%3A15%3A%22_grid_page_siz e%22%3Bi%3A1%3Bs%3A2%3A%2220%22%3B%7D;
_csrf=c24d19036a87a5b280432738832055ae8c31829df0547fdf452df484c55dd461a%3A2%3A%7Bi%3A0%3Bs%3A5%3A%22_csrf%22%3Bi%3A1%3Bs%3A32%3A%22VefpSUrYws 8KwFgUR-6AcN5NdDwUgBow%22%3B%7D; PHPSESSID=fsa1d9rt8iutmnmpb749kr5cim'
    'HTTP_ACCEPT_LANGUAGE' => 'es-ES,es;q=0.9'
    'HTTP_ACCEPT_ENCODING' => 'gzip, deflate, br'
    'HTTP_REFERER' => 'https://site.com/'
    'HTTP_SEC_FETCH_DEST' => 'image'
    'HTTP_SEC_FETCH_MODE' => 'no-cors'
    'HTTP_SEC_FETCH_SITE' => 'same-origin'
    'HTTP_ACCEPT' => 'image/avif,image/webp,image/apng,image/*,*/*;q=0.8'
    'HTTP_USER_AGENT' => 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Sa fari/537.36'
    'HTTP_SEC_CH_UA_MOBILE' => '?0'
    'HTTP_SEC_CH_UA' => '\"Google Chrome\";v=\"87\", \"\\\"Not;A\\\\Brand\";v=\"99\", \"Chromium\";v=\"87\"'
    'HTTP_HOST' => 'site.com'
    'SCRIPT_FILENAME' => '/srv/www/site/public_html/site/web/index.php'
    'REDIRECT_STATUS' => '200'
    'SERVER_NAME' => 'site.com'
    'SERVER_PORT' => '443'
    'SERVER_ADDR' => 'xxx.xxx.xxx.xxx'
    'REMOTE_PORT' => '43052'
    'REMOTE_ADDR' => 'xxx.xxx.xxx.xxx'
    'SERVER_SOFTWARE' => 'nginx/1.16.1'
    'GATEWAY_INTERFACE' => 'CGI/1.1'
    'HTTPS' => 'on'
    'REQUEST_SCHEME' => 'https'
    'SERVER_PROTOCOL' => 'HTTP/2.0'
    'DOCUMENT_ROOT' => '/srv/www/site/public_html/site/web'
    'DOCUMENT_URI' => '/index.php'
    'REQUEST_URI' => '/img/dashboard/logs.png'
    'SCRIPT_NAME' => '/index.php'
    'CONTENT_LENGTH' => ''
    'CONTENT_TYPE' => ''
    'REQUEST_METHOD' => 'GET'
    'QUERY_STRING' => 'q=/img/dashboard/logs.png'
    'FCGI_ROLE' => 'RESPONDER'
    'PHP_SELF' => '/index.php'
    'REQUEST_TIME_FLOAT' => 1606717221.3078
    'REQUEST_TIME' => 1606717221
]

2020-11-30 00:20:21 [xxx.xxx.xxx.xxx][-][-][error][yii\web\HttpException:404] yii\base\InvalidRouteException: Unable to resolve
the request "img/dashboard/logs.png". in /srv/www/site/public_html/site/vendor/yiisoft/yii2/base/Module.php:537
```

Figure 10. Author's elaboration, 2020, Error detected [Image].

REFERENCIAS

[1] Camarena Sagredo, J. G., Trueba Espinosa, A., Martínez Reyes, M., & López García, M. d. (2012). Automatización de la codificación del patrón modelo vista controlador (mvc) en proyectos orientados a la Web. Ciencia Ergo Sum, 239-250.

[2] Chinguel-Tineo, S. F., Arcila-Diaz, J. C., Tuesta-Monteza, V. A., & Mejia-Cabrera, H. I. (2018). Evaluación de algoritmos SMO, BayesNet y J48 para la identificación de ataques a sitios web utilizando log de servidor. PERSPECTIV@S. Revista de Tecnología e Información, 88-91.

[3] ENISA. (n.d.). enisa. Retrieved January 18, 2021, from https://www.enisa.europa.eu/

[4] Mateos Mohino, J. C. (2017). LogsAnalizer: Herramienta para la evaluación en tiempo real de registros log con tecnología Big Data. Universidad de Castilla-La Mancha: Escuela Superior de Informática.

[5] yiiframework. (n.d.). Retrieved January 1, 2021, from https://www.yiiframework.com/doc/guide/2.0/en/intro-yii

Correo electrónico autor: *jonathandelacruzalvarez@gmail.com*