

Intrusion Detection System

An intrusion detection system (IDS) is a software application that monitors a network or systems for malicious activity or policy violations. An IDS specifically does not aim to prevent malicious actions but instead to monitor and log every event, and in cases where a rule has been defined, take a predefined action.* As of [Tiki 18](#), [Exposé](#) is available as a [package](#) to provide website threat identification for Tiki.

*From <https://en.wikipedia.org/wiki/PHPIDS>

Introduction

"An IDS system should not be relied upon for sole protection in your environment! It should only be used in the first level of threat identification. Please read up on [Defense in Depth](#) for more information on a layered security approach" (from <https://github.com/enygma/expose>).

"Here's a quick list (of features):

- A queue system that lets you do offline processing (store on request, cron to check or something similar)
- Notifications of results (just email right now)
- Setting thresholds for notifications


Since it was based on the PHPIDS system, it also has features in common with it:

- Setting exceptions
- Setting restrictions ("only look at...")
- Uses the same filter definitions

I tried to make it so that anyone that's used PHPIDS will feel pretty at home using Expose."

From https://www.reddit.com/r/PHP/comments/1iydsm/expose_a_php_ids/cb9a6z4/

Installation

Exposé isn't bundled with Tiki as an external library by default. Instead, it can be installed "on demand" via the  [Packages](#) feature.

Packages

External packages installation and management

Packages Installed

Install Other Packages

Packages Bundled

Diagnose

No Tabs

Composer Packages These packages have been identified as required by one or more features.

Package Name	Version	Licence	Required by	Install
jerome-breton/casperjs-installer	dev-master	MIT	wikiplugin_casperjs	<div>Install Package</div>
enygma/expose	^3.0	MIT	ids_enabled	<div>Install Package</div>
mpdf/mpdf	^6.1	GPL	Tiki Print	<div>Install Package</div>
onelogin/php-saml	^2.10	MIT	saml_auth_enabled	<div>Install Package</div>

There appear to be some optional packages that can be installed

In the list above, there are optional packages that may be installed in order to use the Tiki features that require the package.

Install packages from the administrator interface

Composer was not detected. Please follow the manual instructions.

Install packages manually

Make sure `composer` is installed.

Composer can be installed manually, in the host machine, by following the instructions from the [Composer](#) website.

The script `setup.sh` that is included in the Tiki distribution can be run to make sure composer is installed. In this case, composer will be installed as `temp/composer.phar`. Below is an example of how to do this in a Linux-like operating system:

```
bash ./setup.sh composer
```

Make sure there is a `composer.json` file in the root of the website.

If there is not already a `composer.json` file, then create one. The sample `composer.json.dist` that comes with Tiki can be used as a starting point. Below is an example of how to do this in a Linux-like operating system:

```
cp composer.json.dist composer.json
```

Install the package.

After all the steps above (that only need to be performed once), packages can be installed by issuing a command `composer require package:version` for each package that is to be installed. Below is an example of how to do this in a Linux-like operating system:

```
php temp/composer.phar require --update-no-dev --prefer-dist psr/log:^1.0
```

Apply

No Tabs

General Security

Spam Protection

Search results


Site Access

Tokens

OpenPGP


Close site

☐




Close site when server load is above the threshold

☐



Enable intrusion detection system

☐



Apply

Please follow the standard [instructions](#) for package installation. Note: in some edge cases, there may be a problem with the package installation GUI. For example, currently (pre-Tiki 17 release) in a Windows WAMP localhost server, there's an error that Composer can't be found. In this case, Exposé may be successfully fetched and installed via the command line:



```
php temp/composer.phar
require enygma/expose
```

Configuration and use

After the Exposé package is installed, go to Site Access tab on the Security Admin page (tiki-admin.php?page=security#content_admin1-4).

When the feature is activated, relevant options are displayed.


Enable intrusion detection system

☒  

Admin IDS custom rules


Custom rules file

temp/ids_custom_rules.json




Intrusion detection system mode

Log only




Intrusion detection system threshold

0



Log to file

ids.log



Apply

After activating the feature, you will notice that for every activity done in Tiki on all pages (requests, modifications, openings, etc.), a file named `ids.log` will be generated. In this file, for each request, the different vulnerability rules are evaluated on the entire content of your page, with an ID number for each rule to differentiate the various vulnerability rules.

Here is an example: After activating the feature, I visited my home page, and the first two lines were generated in the `ids.log` file. Then, I reloaded the page, and the next two lines were generated, and so on. After a while, I modified my home page, and you can see the in-depth analysis that was done below with the content of the page.

Exposé uses the PHPIDS project's ruleset for detecting potential threats. This can be extended with custom rules. The default location and name of the custom rules file is *temp/ids custom rules.json*.

The IDS operation mode needs to be defined, and there are two choices here: *Log only* and *Log and block requests*. Log and block requests will block an intrusion whose impact is over a given threshold. "As the impact scores in Expose are numeric (0 through whatever, depending on the rules matched) you can easily set a threshold to prevent low-level, annoying notifications being delivered" (<https://expose.readthedocs.io/en/latest/>).

[illegible]

Add a new rule

No Tab

Rule Id

Rule Regex

Description

Tags

Impact

Add

Intrusion detection system threshold

notifications are the only thing that setting a threshold changes. Logging and other processing is unchanged" (ibid).

Log to file

Events are logged to a file the default name of which is "ids.log".

History of this Tiki feature:

[+]

Related links

- <https://github.com/enygma/expose>
- <https://expose.readthedocs.io/>
- <http://websec.io/2012/10/12/Core-Concepts-Defense-in-Depth.html>
- <https://www.openhub.net/p/expose>
- <https://www.awnage.com/2014/01/06/ids-showdown-phpids-vs-expose/>
- <https://en.wikipedia.org/wiki/PHPIDS>

alias

- [PHPIDS](#)
- [Expose](#)
- [Exposé](#)
- [Intrusion Detection System](#)
- [IDS](#)