

# 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, ExposÃ© 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:

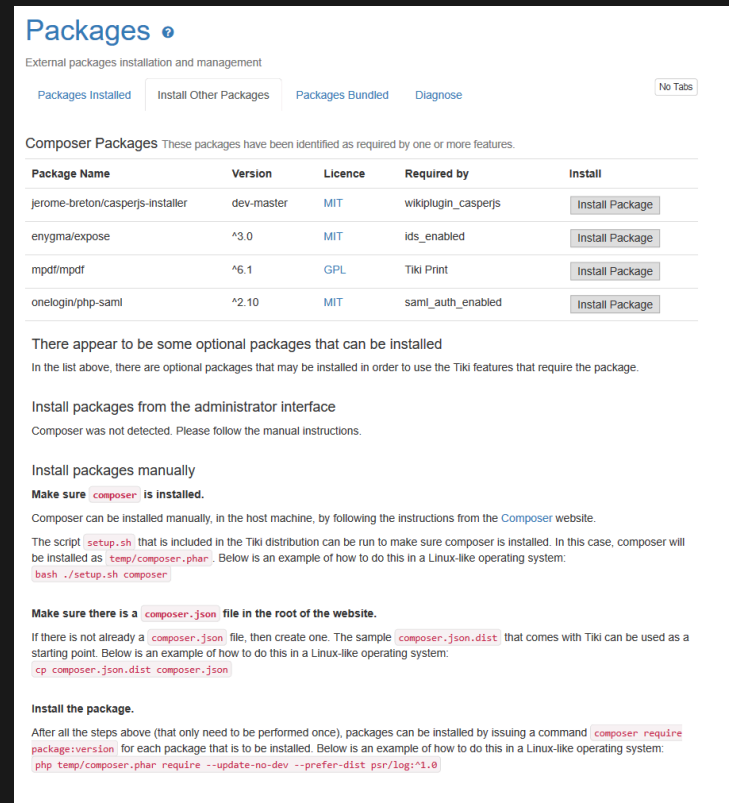
- Setting exceptions
- Setting restrictions ("only look at...")
- Uses the same filter definitions


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/](https://www.reddit.com/r/PHP/comments/1iydsm/expose_a_php_ids/cb9a6z4/)

# INSTALLATION

ExposÃ© 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	<a href="#">Install Package</a>
enigma/expose	^3.0	MIT	ids_enabled	<a href="#">Install Package</a>
mpdf/mpdf	^6.1	GPL	Tiki Print	<a href="#">Install Package</a>
onelogin/php-saml	^2.10	MIT	saml_auth_enabled	<a href="#">Install Package</a>

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
```

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, ExposÃ© may be successfully fetched and installed via the command line:

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

## CONFIGURATION AND USE

After the ExposÃ© package is installed, go to Site Access tab on the Security Admin page (tiki-admin.php?page=security#content\_admin1-4).

Apply

General Security Spam Protection Search results **Site Access** Tokens OpenPGP No Tabs

**Close site** ⓘ

**Close site when server load is above the threshold** ⓘ

**Enable intrusion detection system** ⓘ

Apply

When the feature is activated, relevant options are displayed.

Enable intrusion detection system  [i](#) [✓](#)

[Admin IDS custom rules](#)

Custom rules file  [i](#)

Intrusion detection system mode  [i](#)

Intrusion detection system threshold  [i](#)

Log to file  [i](#)

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.

## EXAMPLE

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.

```
ndar.tpl JS tiki-calendar.js JS wikiplugin-trackercalendar.js ids.log U X trackerlib.php tiki-view_tracker.tpl tracker_filter.tpl Filter.ph ...
ids.log
1 [(2024-10-31 14:32:08] IDS.INFO: Executing on data a4ac2b4473f06935a8e9c95eb5002200 [] []
2 [(2024-10-31 14:32:08] IDS.INFO: Executing on data a4ac2b4473f06935a8e9c95eb5002200 [] []
3 [(2024-10-31 14:33:37] IDS.INFO: Executing on data a4ac2b4473f06935a8e9c95eb5002200 [] []
4 [(2024-10-31 14:33:42] IDS.INFO: Executing on data f6a85803f96b88823ba808337eb50d8e [] []
5 [(2024-10-31 14:34:10] IDS.INFO: Executing on data 24ac4406a03596f9687d77f758e487a0 [] []
6 [(2024-10-31 14:34:20] IDS.INFO: Executing on data 63ef77cf6fca2bb0fa7d047fb16e8d61 [] []
7 [(2024-10-31 14:34:57] IDS.INFO: Executing on data 5b25d3e3bb16c97ff94fa02657b51170 [] []
8 [(2024-10-31 14:34:59] IDS.INFO: Executing on data 20ef404e39131c62f6754f1e2242bc73 [] []
9 [(2024-10-31 14:35:00] IDS.INFO: Executing on data cea7cf0557720e2604b0704ac3425ffb [] []
10 [(2024-10-31 14:35:01] IDS.INFO: Executing on data 26fdd069cb188a555c371a2bd4451cb4 [] []
11 [(2024-10-31 14:35:22] IDS.INFO: Executing on data a4ac2b4473f06935a8e9c95eb5002200 [] []
12 [(2024-10-31 14:35:22] IDS.INFO: Executing on data a4ac2b4473f06935a8e9c95eb5002200 [] []
13 [(2024-10-31 14:35:27] IDS.INFO: Executing on data 3a8b7c6aa5cb8916af2dbde6547efee0 [] []
14 [(2024-10-31 14:35:38] IDS.INFO: Executing on data 39e1f72610fc43d711adfa6f21a4463f [] []
15 [(2024-10-31 14:35:38] IDS.INFO: Match found on Filter ID 1 [{"id": "1", "rule": "(?:\\\"[^\"]*~?>)|(?:[^\w\\s]\\s*\\/>)|(?:>\\\")", "description": "
16 [(2024-10-31 14:35:38] IDS.INFO: Match found on Filter ID 8 [{"id": "8", "rule": "(?:\\\"[^\"]*~?>)|(?:[^\w\\s]\\s*\\/>)|(?:>\\\")|(?:\\\"[^\"]*~?>)|(?:[^\w\\s]\\s*\\/>)|(?:>\\\")", "description": "
17 [(2024-10-31 14:35:38] IDS.INFO: Match found on Filter ID 16 [{"id": "16", "rule": "(?:\\\"[^\"]*~?>)|(?:[^\w\\s]\\s*\\/>)|(?:>\\\")|(?:\\\"[^\"]*~?>)|(?:[^\w\\s]\\s*\\/>)|(?:>\\\")", "description": "
18 [(2024-10-31 14:35:38] IDS.INFO: Match found on Filter ID 20 [{"id": "20", "rule": "(?:\\\"[^\"]*~?>)|(?:[^\w\\s]\\s*\\/>)|(?:>\\\")|(?:\\\"[^\"]*~?>)|(?:[^\w\\s]\\s*\\/>)|(?:>\\\")", "description": "
19 [(2024-10-31 14:35:38] IDS.INFO: Match found on Filter ID 21 [{"id": "21", "rule": "(?:\\\"[^\"]*~?>)|(?:[^\w\\s]\\s*\\/>)|(?:>\\\")|(?:\\\"[^\"]*~?>)|(?:[^\w\\s]\\s*\\/>)|(?:>\\\")", "description": "
20 [(2024-10-31 14:35:38] IDS.INFO: Match found on Filter ID 38 [{"id": "38", "rule": "(?:\\\"[^\"]*~?>)|(?:[^\w\\s]\\s*\\/>)|(?:>\\\")|(?:\\\"[^\"]*~?>)|(?:[^\w\\s]\\s*\\/>)|(?:>\\\")", "description": "
21 [(2024-10-31 14:35:38] IDS.INFO: Match found on Filter ID 43 [{"id": "43", "rule": "(?:\\\"[^\"]*~?>)|(?:[^\w\\s]\\s*\\/>)|(?:>\\\")|(?:\\\"[^\"]*~?>)|(?:[^\w\\s]\\s*\\/>)|(?:>\\\")", "description": "
22 [(2024-10-31 14:35:38] IDS.INFO: Impact: 31, Report: Variable: data | Value: !Congratulations This is the default homepage for your Tiki. If you
23 [(2024-10-31 14:35:38] IDS.INFO: Executing on data cf9f9b4cef828477d95c03237cb60edd [] []
24 [(2024-10-31 14:35:38] IDS.INFO: Executing on data a0f07095da6a54e15ffb8ab25c542516 [] []
25 [(2024-10-31 14:35:38] IDS.INFO: Match found on Filter ID 1 [{"id": "1", "rule": "(?:\\\"[^\"]*~?>)|(?:[^\w\\s]\\s*\\/>)|(?:>\\\")", "description": "
```

## CUSTOM RULES FILE

ExposÃ© 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*.

# IDS Rules

Add a new rule No Tabs

**Rule Id**

**Rule Regex**

**Description**

**Tags**

**Impact**

## INTRUSION DETECTION SYSTEM MODE

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/>).

## INTRUSION DETECTION SYSTEM THRESHOLD

This is to define the IDS threshold as a numerical value, when in the "Log and block requests" mode. "Some applications know for a fact that theyâ€™ll always be getting a certain amount of traffic thatâ€™s in the 1-2 impact score range. Getting notifications for every one of these requests would get annoying pretty quickly, so you can set your threshold a bit higher." Setting the threshold to 8 means that Expose will only send notifications when the score is greater than or equal to 8. Thereâ€™s no concept of "high", "medium" or "low" in Expose as the meanings of these terms vary greatly by environment and application. "NOTE: Currently notifications are the only thing that setting a threshold changes. Logging and other processing is unchanged" (ibid).

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
- ExposÃ©
- Intrusion Detection System
- IDS