Intrusion Detection System

onclick=role="">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.

onclick=role=""> *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 evel of threat identification. Please read up on Defense in Depth for more information on a layered security approach

(from https://github.com/enygma/expose).

onclick=role="">

onclick=role="">

onclick=role="">

onclick=role="">

"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."

onclick=role="">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.

onclick=role="">

onclick=role="">

Plugin Image

The "id" parameter is not allowed unless "file_galleries_redirect_from_image_gallery" preference is enabled.

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 Acccess tab on the Security Admin page (tiki-admin.php?page=security#content_admin1-4).

onclick=role="">

onclick=role="">

Plugin Image

The "id" parameter is not allowed unless "file_galleries_redirect_from_image_gallery" preference is enabled.

When the feature is activated, relevant options are displayed.

onclick=role="">

onclick=role="">

Plugin Image

The "id" parameter is not allowed unless "file_galleries_redirect_from_image_gallery" preference is enabled.

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.

onclick=role="">

onclick=role="">

Plugin Image

The "id" parameter is not allowed unless "file_galleries_redirect_from_image_gallery" preference is enabled.

Custom rules file

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*.

onclick=role="">

onclick=role="">

Plugin Image

The "id" parameter is not allowed unless "file_galleries_redirect_from_image_gallery" preference is enabled.

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 re numeric (0 through whatever, depending on the rules matched) you can easily set a threshold to prevent low-leve 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 they’ll always be getting a certain amount of traffic that’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. There’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 threshol 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:

[+]

PHPIDS (PHP-Intrusion Detection System)

This is somewhat similar to ModSecurity but in PHP, and thus configurable via Tiki.

PHPIDS (PHP-Intrusion Detection System) is a simple to use, well structured, fast and state-of-the-art security layer fo your PHP based web application. The IDS neither strips, sanitizes nor filters any malicious input, it simply recognizes when an attacker tries to break your site and reacts in exactly the way you want it to. Based on a set of approved and heavily tested filter rules any attack is given a numerical impact rating which makes it easy to decide what kind of action should follow the hacking attempt. This could range from simple logging to sending out an emergency mail to the development team, displaying a warning message for the attacker or even ending the user's session.

PHPIDS enables you to see who's attacking your site and how and all without the tedious trawling of logfiles or searching hacker forums for your domain. Last but not least it's licensed under the LGPL!"

- http://phpids.org/
- http://www.ohloh.net/p/phpids
- http://forum.itratos.de/showthread.php?37550-PHPIDS-now-part-of-Tiki-Wiki-CMS-Group ware-(tiki.org)

This improves Security and Performance

To configure, visit tiki-admin.php?page=security -> PHPIDS

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