ChaoticOnyx / **OnyxForum** Public

fix(hub): absolute Path Traversal due to incorrect use of `send_file` …

Browse files

… call

A path traversal attack (also known as directory traversal) aims to access files and directories that are stored outside the web root folder. By manipulating variables that reference files with “dot-dot-slash (../)” sequences and its variations or by using absolute file paths, it may be possible to access arbitrary files and directories stored on file system including application source code or configuration and critical system files. This attack is also known as “dot-dot-slash”, “directory traversal”, “directory climbing” and “backtracking”.

## Root Cause Analysis

The `os.path.join` call is unsafe for use with untrusted input. When the `os.path.join` call encounters an absolute path, it ignores all the parameters it has encountered till that point and starts working with the new absolute path. Please see the example below.

```
>>> import os.path
>>> static = "path/to/mySafeStaticDir"
>>> malicious = "/../../../../../etc/passwd"
>>> os.path.join(t,malicious)
'/../../../../../etc/passwd'
```

Since the "malicious" parameter represents an absolute path, the result of `os.path.join` ignores the static directory completely. Hence, untrusted input is passed via the `os.path.join` call to `flask.send_file` can lead to path traversal attacks.

In this case, the problems occurs due to the following code :
https://github.com/ChaoticOnyx/OnyxForum/blob/4077b499a1ca213f3eb55b8321a4733d83531750/modules/hub/hub/views.py#L493

Here, the `path` parameter is attacker controlled. This parameter passes through the unsafe `os.path.join` call making the effective directory and filename passed to the `send_file` call attacker controlled. This leads to a path traversal attack.

## Remediation

This can be fixed by preventing flow of untrusted data to the vulnerable `send_file` function. In case the application logic necessiates this behaviour, one can either use the `flask.safe_join` to join untrusted paths or replace `flask.send_file` calls with `flask.send_from_directory` calls.

## References

* [OWASP Path Traversal](https://owasp.org/www-community/attacks/Path_Traversal)
* github/securitylab#669

```
### This bug was found using *[CodeQL by Github](https://codeql.github.com/)*

Co-authored-by: Porcupiney Hairs <porucpiney.hairs@protonmail.com>
PR #63
```

master (#63)

porcupineyhairs committed on May 4

1 parent 4077b49   commit f25543dfc62a9694d7e4f67eebfa45e3de916053

Showing **1 changed file** with **3 additions** and **1 deletion**.

Split | Unified

4 🟩🟩🟩🟥⬜ modules/hub/hub/views.py

```
  from flaskbb.extensions import allows, db, celery
  from flaskbb.user.models import User, Group
  from flaskbb.forum.models import Post
+ from werkzeug.utils import safe_join
+

  from hub.forms import ConfigEditForm, BanSearchForm, ConnectionSearchForm
  from hub.permissions import CanAccessServerHub, CanAccessServerHubAdditional, CanAccessSe
          if server is None:
              abort(404)

-         file_path = os.path.join(server.logs_path, path)
+         file_path = safe_join(server.logs_path, path)
          return send_file(file_path, as_attachment=True)


```

0 comments on commit f25543d

Please sign in to comment.