AS Lab 3 - Application Security Threats Modeling

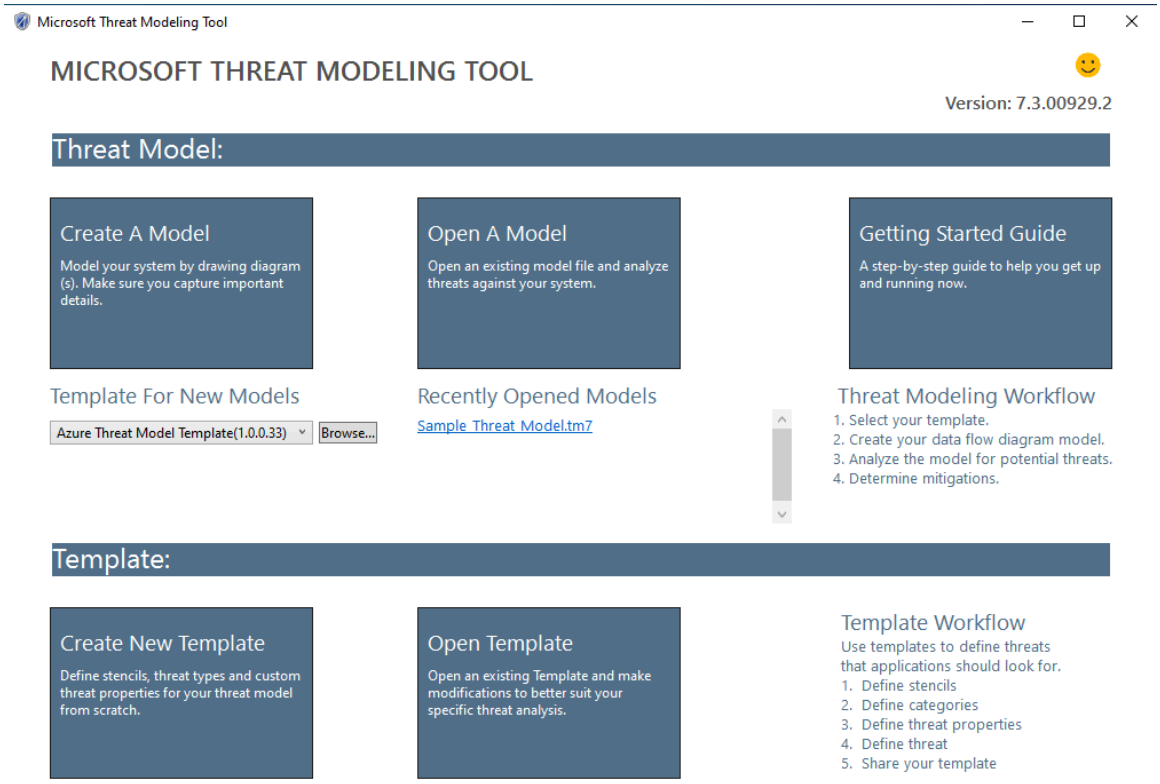
Lab Member1: *Nadezhda Syutkina*
Lab Member2: *Ahmed Elkashef*

Task 1 - The definition of object for threat modeling

Chosen Project URL: https://vocabstock.com/de/

Task 2 - Select the tool for threat modeling

Microsoft Threat Modeling Tool (default choice for STRIDE)



Task 3 - DFD model creation

The goal:

- Asses a virtual appliance with zero initial knowledge
- Map its attack surface
- Develop a threat model

Steps:

1) Enumeration / Discovery
2) Dataflow
3) Threat model

1) Enumeration / Discovery

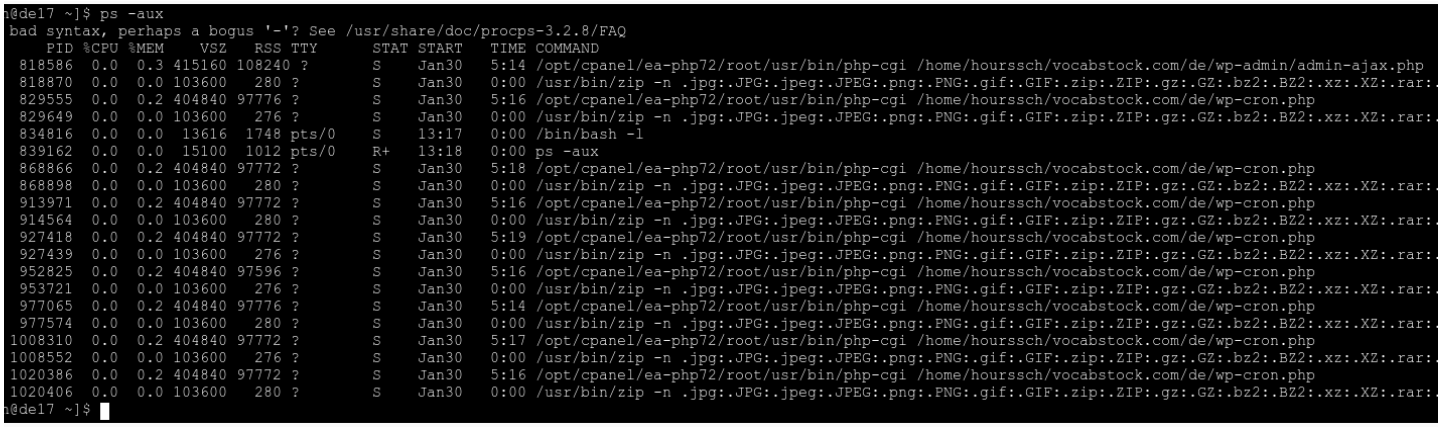
- Product functionality
- Processes
- Listening ports
- Process to port mappings
- Users processes are running as
- Mooch around the interfaces (*scientific)
- Dig into the database (if there is one)

Product functionality:

VocabStock is a website for learning German Vocabulary. It provides the following

- A website interface
- A web administration interface (wp-admin)
- An Email Gateway (Sendmail) - /usr/sbin/sendmail

Processes:



The full contents is as follows:

```
[hourssch@de17 ~]$ ps -aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
hourssch  818586  0.0  0.3 415160 108240 ?       S    Jan30   5:14 /opt/cpanel/ea-php72/root/usr/bin/php-cgi
/home/hourssch/vocabstock.com/de/wp-admin/admin-ajax.php
hourssch  818870  0.0  0.0 103600   280 ?        S    Jan30   0:00 /usr/bin/zip -n
.jpg:.JPG:.jpeg:.JPEG:.png:.PNG:.gif:.GIF:.zip:.ZIP:.gz:.GZ:.bz2:.BZ2:.xz:.XZ:.rar:.RAR:.mp3:.MP3:.mp4:.MP4:.mp
hourssch  829555  0.0  0.2 404840 97776 ?        S    Jan30   5:16 /opt/cpanel/ea-php72/root/usr/bin/php-cgi
/home/hourssch/vocabstock.com/de/wp-cron.php
hourssch  829649  0.0  0.0 103600   276 ?        S    Jan30   0:00 /usr/bin/zip -n
.jpg:.JPG:.jpeg:.JPEG:.png:.PNG:.gif:.GIF:.zip:.ZIP:.gz:.GZ:.bz2:.BZ2:.xz:.XZ:.rar:.RAR:.mp3:.MP3:.mp4:.MP4:.mp
hourssch  834816  0.0  0.0  13616  1748 pts/0    S    13:17   0:00 /bin/bash -l
```

```
hourssch  839162  0.0  0.0  15100  1012 pts/0    R+   13:18   0:00 ps -aux
hourssch  868866  0.0  0.2 404840 97772 ?        S    Jan30   5:18 /opt/cpanel/ea-php72/root/usr/bin/php-cgi
/home/hourssch/vocabstock.com/de/wp-cron.php
hourssch  868898  0.0  0.0 103600   280 ?        S    Jan30   0:00 /usr/bin/zip -n
.jpg:.JPG:.jpeg:.JPEG:.png:.PNG:.gif:.GIF:.zip:.ZIP:.gz:.GZ:.bz2:.BZ2:.xz:.XZ:.rar:.RAR:.mp3:.MP3:.mp4:.MP4:.mp
hourssch  913971  0.0  0.2 404840 97772 ?        S    Jan30   5:16 /opt/cpanel/ea-php72/root/usr/bin/php-cgi
/home/hourssch/vocabstock.com/de/wp-cron.php
hourssch  914564  0.0  0.0 103600   280 ?        S    Jan30   0:00 /usr/bin/zip -n
.jpg:.JPG:.jpeg:.JPEG:.png:.PNG:.gif:.GIF:.zip:.ZIP:.gz:.GZ:.bz2:.BZ2:.xz:.XZ:.rar:.RAR:.mp3:.MP3:.mp4:.MP4:.mp
hourssch  927418  0.0  0.2 404840 97772 ?        S    Jan30   5:19 /opt/cpanel/ea-php72/root/usr/bin/php-cgi
/home/hourssch/vocabstock.com/de/wp-cron.php
hourssch  927439  0.0  0.0 103600   276 ?        S    Jan30   0:00 /usr/bin/zip -n
.jpg:.JPG:.jpeg:.JPEG:.png:.PNG:.gif:.GIF:.zip:.ZIP:.gz:.GZ:.bz2:.BZ2:.xz:.XZ:.rar:.RAR:.mp3:.MP3:.mp4:.MP4:.mp
hourssch  952825  0.0  0.2 404840 97596 ?        S    Jan30   5:16 /opt/cpanel/ea-php72/root/usr/bin/php-cgi
/home/hourssch/vocabstock.com/de/wp-cron.php
hourssch  953721  0.0  0.0 103600   276 ?        S    Jan30   0:00 /usr/bin/zip -n
.jpg:.JPG:.jpeg:.JPEG:.png:.PNG:.gif:.GIF:.zip:.ZIP:.gz:.GZ:.bz2:.BZ2:.xz:.XZ:.rar:.RAR:.mp3:.MP3:.mp4:.MP4:.mp
hourssch  977065  0.0  0.2 404840 97776 ?        S    Jan30   5:14 /opt/cpanel/ea-php72/root/usr/bin/php-cgi
/home/hourssch/vocabstock.com/de/wp-cron.php
hourssch  977574  0.0  0.0 103600   280 ?        S    Jan30   0:00 /usr/bin/zip -n
.jpg:.JPG:.jpeg:.JPEG:.png:.PNG:.gif:.GIF:.zip:.ZIP:.gz:.GZ:.bz2:.BZ2:.xz:.XZ:.rar:.RAR:.mp3:.MP3:.mp4:.MP4:.mp
hourssch 1008310  0.0  0.2 404840 97772 ?        S    Jan30   5:17 /opt/cpanel/ea-php72/root/usr/bin/php-cgi
/home/hourssch/vocabstock.com/de/wp-cron.php
hourssch 1008552  0.0  0.0 103600   276 ?        S    Jan30   0:00 /usr/bin/zip -n
.jpg:.JPG:.jpeg:.JPEG:.png:.PNG:.gif:.GIF:.zip:.ZIP:.gz:.GZ:.bz2:.BZ2:.xz:.XZ:.rar:.RAR:.mp3:.MP3:.mp4:.MP4:.mp
hourssch 1020386  0.0  0.2 404840 97772 ?        S    Jan30   5:16 /opt/cpanel/ea-php72/root/usr/bin/php-cgi
/home/hourssch/vocabstock.com/de/wp-cron.php
hourssch 1020406  0.0  0.0 103600   280 ?        S    Jan30   0:00 /usr/bin/zip -n
.jpg:.JPG:.jpeg:.JPEG:.png:.PNG:.gif:.GIF:.zip:.ZIP:.gz:.GZ:.bz2:.BZ2:.xz:.XZ:.rar:.RAR:.mp3:.MP3:.mp4:.MP4:.mp
```

The following processes:
818586, 818870, 829555, 829649, 834816, 839162, 868866, 868898, 913971, 914564, 927418, 927439, 952825, 953721, 977065, 977574, 1008310, 1008552, 1020386, 1020406

Listening ports:
We use the following script, which does the same job as **netstat**

```
awk 'function hextodec(str,ret,n,i,k,c){
    ret = 0
    n = length(str)
    for (i = 1; i <= n; i++) {
        c = tolower(substr(str, i, 1))
        k = index("123456789abcdef", c)
        ret = ret * 16 + k
    }
    return ret
}
function getIP(str,ret){
    ret=hextodec(substr(str,index(str,":")-2,2));
    for (i=5; i>0; i-=2) {
        ret = ret"."hextodec(substr(str,i,2))
    }
    ret = ret":"hextodec(substr(str,index(str,":")+1,4))
    return ret
}
NR > 1 {{if(NR==2)print "Local - Remote";local=getIP($2);remote=getIP($3)}{print local" -
"remote}}' /proc/net/tcp
```

```
Local - Remote
0.0.0.0:31337 - 0.0.0.0:0
0.0.0.0:6025 - 0.0.0.0:0
0.0.0.0:3369 - 0.0.0.0:0
0.0.0.0:2121 - 0.0.0.0:0
0.0.0.0:1353 - 0.0.0.0:0
0.0.0.0:60521 - 0.0.0.0:0
0.0.0.0:60201 - 0.0.0.0:0
0.0.0.0:32778 - 0.0.0.0:0
0.0.0.0:31338 - 0.0.0.0:0
0.0.0.0:5802 - 0.0.0.0:0
0.0.0.0:5226 - 0.0.0.0:0
0.0.0.0:3050 - 0.0.0.0:0
0.0.0.0:60522 - 0.0.0.0:0
0.0.0.0:6667 - 0.0.0.0:0
0.0.0.0:1131 - 0.0.0.0:0
0.0.0.0:60523 - 0.0.0.0:0
0.0.0.0:587 - 0.0.0.0:0
0.0.0.0:1164 - 0.0.0.0:0
0.0.0.0:60524 - 0.0.0.0:0
0.0.0.0:5357 - 0.0.0.0:0
0.0.0.0:5101 - 0.0.0.0:0
0.0.0.0:1357 - 0.0.0.0:0
0.0.0.0:60525 - 0.0.0.0:0
```

```
172.105.94.109:80 - 66.249.66.205:45433
172.105.94.109:443 - 162.158.94.237:18898
172.105.94.109:993 - 151.56.209.36:53624
172.105.94.109:80 - 66.249.66.203:36786
172.105.94.109:443 - 162.158.88.213:54764
172.105.94.109:443 - 199.36.223.241:53237
172.105.94.109:993 - 188.2.151.241:64345
172.105.94.109:54528 - 40.67.211.166:443
172.105.94.109:443 - 162.158.92.83:23110
127.0.0.1:143 - 127.0.0.1:58830
172.105.94.109:443 - 162.158.91.6:24230
172.105.94.109:80 - 66.249.66.209:37333
172.105.94.109:80 - 66.249.66.213:57312
172.105.94.109:80 - 66.249.66.205:56928
172.105.94.109:80 - 103.26.85.68:53555
172.105.94.109:443 - 162.158.90.35:20724
172.105.94.109:993 - 90.167.51.253:42552
172.105.94.109:993 - 176.127.155.132:50387
172.105.94.109:993 - 176.127.155.132:50389
172.105.94.109:443 - 162.158.89.144:59680
127.0.0.1:51180 - 127.0.0.1:2082
172.105.94.109:80 - 66.249.66.201:37309
172.105.94.109:80 - 66.249.66.213:37873
172.105.94.109:80 - 66.249.66.205:35864
```

The full list of open ports on our machine looks as follows:

```
Open Ports:
17/tcp - qotd
21/tcp - ftp
23/tcp - telnet
25/tcp - smtp
53/tcp - domain ISC BIND
79/tcp - dovecot pop3
80/tcp - http
84/tcp - smtp
88/tcp - open kerberos-sec
110/tcp - pop3
119/tcp - ftp
125/tcp - smtp
139/tcp - open netbios-ssn
143/tcp - imap
199/tcp - smux
264/tcp - smtp
311/tcp - dovecot pop3
443/tcp - ssl/https
465/tcp - smtps
513/tcp - login
543/tcp - pop3
555/tcp - ftp
563/tcp - snews
587/tcp - exim smtpd
666/tcp - FTP(ProFTPD)
700/tcp - FTP(ProFTPD)
808/tcp - ccproxy-http
993/tcp - imaps
995/tcp - pop3s
1001/tcp - webpush
1002/tcp - ftp(ProFTPD)
1025/tcp - pop3
1026/tcp - ftp(ProFTPD)
1028/tcp - unknown
1031/tcp - pop3(dovecot pop3d)
1032/tcp - pop3(dovecot pop3d)
1044/tcp - ftp(ProFTPD)
1050/tcp - smtp
1055/tcp - ansyslmd
```

The full nmap scan shows the following information:

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-10 15:36 MSK
Nmap scan report for de17.fcomet.com (172.105.94.109)
Host is up (0.064s latency).
Not shown: 896 closed ports
PORT      STATE SERVICE       VERSION
17/tcp    open  qotd?
| fingerprint-strings:
```

```
|   GenericLines, GetRequest:
|     OK [CAPABILITY LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN] Dovecot ready.
|     Error in IMAP command : Unknown command.
|   NULL:
|_    OK [CAPABILITY LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN] Dovecot ready.
21/tcp    open  ftp           Pure-FTPd
23/tcp    open  telnet?
| fingerprint-strings:
|   GenericLines, tn3270:
|     This is an unrestricted telnet server.
|     Please do not user for production purposes
|     bash: command not found
|   NULL:
|     This is an unrestricted telnet server.
|_    Please do not user for production purposes
25/tcp    open  smtp?
|_smtp-commands: Couldn't establish connection on port 25
53/tcp    open  domain        ISC BIND 9.8.2rc1 (RedHat Enterprise Linux 6)
| dns-nsid:
|_  bind.version: 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6_10.8
79/tcp    open  pop3          Dovecot pop3d
|_finger: ERROR: Script execution failed (use -d to debug)
80/tcp    open  http          Apache httpd 2.4.46 ((cPanel) OpenSSL/1.1.1h mod_bwlimited/1.4
Phusion_Passenger/5.3.7)
84/tcp    open  smtp?
| fingerprint-strings:
|   GenericLines, GetRequest:
|     220 ESMTP Postfix (Debian/GNU)
|     5.5.2 Error: command not recognized
|   NULL:
|_    220 ESMTP Postfix (Debian/GNU)
|_smtp-commands: Couldn't establish connection on port 84
88/tcp    open  kerberos-sec?
| fingerprint-strings:
|   GetRequest, Kerberos:
|     This is an unrestricted telnet server.
|     Please do not user for production purposes
|     bash: command not found
|   NULL:
|     This is an unrestricted telnet server.
|_    Please do not user for production purposes
110/tcp   open  pop3          Dovecot pop3d
119/tcp   open  ftp           ProFTPD 1.3.1
125/tcp   open  smtp?
| fingerprint-strings:
|   GenericLines, GetRequest:
|     220 ESMTP Postfix (Debian/GNU)
|     5.5.2 Error: command not recognized
|   NULL:
|_    220 ESMTP Postfix (Debian/GNU)
|_smtp-commands: Couldn't establish connection on port 125
139/tcp   open  netbios-ssn?
| fingerprint-strings:
|   GetRequest, SMBProgNeg:
|     OK [CAPABILITY LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN] Dovecot ready.
```

```
|     Error in IMAP command : Unknown command.
|   NULL:
|_    OK [CAPABILITY LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN] Dovecot ready.
143/tcp   open  imap          Dovecot imapd
199/tcp   open  smux?
| fingerprint-strings:
|   GenericLines, RPCCheck:
|     This is an unrestricted telnet server.
|     Please do not user for production purposes
|     bash: command not found
|   NULL:
|     This is an unrestricted telnet server.
|_    Please do not user for production purposes
264/tcp   open  smtp?
| fingerprint-strings:
|   GenericLines, GetRequest:
|     220 ESMTP Postfix (Debian/GNU)
|     5.5.2 Error: command not recognized
|   NULL:
|_    220 ESMTP Postfix (Debian/GNU)
|_smtp-commands: Couldn't establish connection on port 264
311/tcp   open  pop3          Dovecot pop3d
443/tcp   open  ssl/https?
465/tcp   open  smtps?
|_smtp-commands: Couldn't establish connection on port 465
513/tcp   open  login?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP:
|     This is an unrestricted telnet server.
|     Please do not user for production purposes
|     bash: command not found
|   NULL:
|     This is an unrestricted telnet server.
|_    Please do not user for production purposes
543/tcp   open  pop3          Dovecot pop3d
555/tcp   open  ftp           ProFTPD 1.3.1
563/tcp   open  snews?
| fingerprint-strings:
|   GenericLines, SSLSessionReq:
|     This is an unrestricted telnet server.
|     Please do not user for production purposes
|     bash: command not found
|   NULL:
|     This is an unrestricted telnet server.
|_    Please do not user for production purposes
587/tcp   open  smtp          Exim smtpd 4.93
|_smtp-commands: Couldn't establish connection on port 587
666/tcp   open  ftp           ProFTPD 1.3.1
700/tcp   open  ftp           ProFTPD 1.3.1
808/tcp   open  ccproxy-http?
| fingerprint-strings:
|   GenericLines:
|     OK [CAPABILITY LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN] Dovecot ready.
|     Error in IMAP command : Unknown command.
|   NULL:
```

```
|_    OK [CAPABILITY LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN] Dovecot ready.
993/tcp   open  imaps?
995/tcp   open  pop3s?
1001/tcp  open  webpush?
| fingerprint-strings:
|   GenericLines:
|     This is an unrestricted telnet server.
|     Please do not user for production purposes
|     bash: command not found
|   NULL:
|     This is an unrestricted telnet server.
|_    Please do not user for production purposes
1002/tcp  open  ftp           ProFTPD 1.3.1
1025/tcp  open  pop3          Dovecot pop3d
1026/tcp  open  ftp           ProFTPD 1.3.1
1028/tcp  open  unknown
| fingerprint-strings:
|   NULL:
|     This is an unrestricted telnet server.
|     Please do not user for production purposes
|   TerminalServer:
|     This is an unrestricted telnet server.
|     Please do not user for production purposes
|_    bash: command not found
1031/tcp  open  pop3          Dovecot pop3d
1032/tcp  open  pop3          Dovecot pop3d
1044/tcp  open  ftp           ProFTPD 1.3.1
1050/tcp  open  smtp?
| fingerprint-strings:
|   GenericLines, NULL:
|_    220 ESMTP Postfix (Debian/GNU)
|_giop-info: TIMEOUT
|_smtp-commands: Couldn't establish connection on port 1050
1055/tcp  open  ansyslmd?
| fingerprint-strings:
|   GenericLines, NULL:
|_    OK [CAPABILITY LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN] Dovecot ready.
9 services unrecognized despite returning data. If you know the service/version, please submit the
following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port17-TCP:V=7.80%I=7%D=2/10%Time=6023D345%P=x86_64-pc-linux-gnu%r(NULL
SF:,4A,"OK\x20\[CAPABILITY\x20LOGIN-REFERRALS\x20ID\x20ENABLE\x20IDLE\x20A
SF:UTH=PLAIN\]\x20Dovecot\x20ready\.\r\n")%r(GenericLines,78,"OK\x20\[CAPA
SF:BILITY\x20LOGIN-REFERRALS\x20ID\x20ENABLE\x20IDLE\x20AUTH=PLAIN\]\x20Do
SF:vecot\x20ready\.\r\nBAD\x20Error\x20in\x20IMAP\x20command\x20:\x20Unkno
SF:wn\x20command\.\r\n")%r(GetRequest,78,"OK\x20\[CAPABILITY\x20LOGIN-REFE
SF:RRALS\x20ID\x20ENABLE\x20IDLE\x20AUTH=PLAIN\]\x20Dovecot\x20ready\.\r\n
SF:BAD\x20Error\x20in\x20IMAP\x20command\x20:\x20Unknown\x20command\.\r\n"
SF:);
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port23-TCP:V=7.80%I=7%D=2/10%Time=6023D345%P=x86_64-pc-linux-gnu%r(NULL
SF:,58,"This\x20is\x20an\x20unrestricted\x20telnet\x20server\.\r\nPlease\x
SF:20do\x20not\x20user\x20for\x20production\x20purposes\r\n\r\n#\x20")%r(G
SF:enericLines,74,"This\x20is\x20an\x20unrestricted\x20telnet\x20server\.\
SF:r\nPlease\x20do\x20not\x20user\x20for\x20production\x20purposes\r\n\r\n
```

```
SF:#\x20\x20bash:\x20command\x20not\x20found\r\n#\x20")%r(tn3270,74,"This\
SF:x20is\x20an\x20unrestricted\x20telnet\x20server\.\r\nPlease\x20do\x20no
SF:t\x20user\x20for\x20production\x20purposes\r\n\r\n#\x20\x20bash:\x20com
SF:mand\x20not\x20found\r\n#\x20");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port84-TCP:V=7.80%I=7%D=2/10%Time=6023D345%P=x86_64-pc-linux-gnu%r(NULL
SF:,20,"220\x20ESMTP\x20Postfix\x20\(Debian/GNU\)\r\n")%r(GetRequest,49,"2
SF:20\x20ESMTP\x20Postfix\x20\(Debian/GNU\)\r\n502\x205\.5\.2\x20Error:\x2
SF:0command\x20not\x20recognized\r\n")%r(GenericLines,49,"220\x20ESMTP\x20
SF:Postfix\x20\(Debian/GNU\)\r\n502\x205\.5\.2\x20Error:\x20command\x20not
SF:\x20recognized\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port88-TCP:V=7.80%I=7%D=2/10%Time=6023D345%P=x86_64-pc-linux-gnu%r(NULL
SF:,58,"This\x20is\x20an\x20unrestricted\x20telnet\x20server\.\r\nPlease\x
SF:20do\x20not\x20user\x20for\x20production\x20purposes\r\n\r\n#\x20")%r(G
SF:etRequest,74,"This\x20is\x20an\x20unrestricted\x20telnet\x20server\.\r\
SF:nPlease\x20do\x20not\x20user\x20for\x20production\x20purposes\r\n\r\n#\
SF:x20\x20bash:\x20command\x20not\x20found\r\n#\x20")%r(Kerberos,74,"This\
SF:x20is\x20an\x20unrestricted\x20telnet\x20server\.\r\nPlease\x20do\x20no
SF:t\x20user\x20for\x20production\x20purposes\r\n\r\n#\x20\x20bash:\x20com
SF:mand\x20not\x20found\r\n#\x20");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port125-TCP:V=7.80%I=7%D=2/10%Time=6023D345%P=x86_64-pc-linux-gnu%r(NUL
SF:L,20,"220\x20ESMTP\x20Postfix\x20\(Debian/GNU\)\r\n")%r(GenericLines,49
SF:,"220\x20ESMTP\x20Postfix\x20\(Debian/GNU\)\r\n502\x205\.5\.2\x20Error:
SF:\x20command\x20not\x20recognized\r\n")%r(GetRequest,49,"220\x20ESMTP\x2
SF:0Postfix\x20\(Debian/GNU\)\r\n502\x205\.5\.2\x20Error:\x20command\x20no
SF:t\x20recognized\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port139-TCP:V=7.80%I=7%D=2/10%Time=6023D345%P=x86_64-pc-linux-gnu%r(NUL
SF:L,4A,"OK\x20\[CAPABILITY\x20LOGIN-REFERRALS\x20ID\x20ENABLE\x20IDLE\x20
SF:AUTH=PLAIN\]\x20Dovecot\x20ready\.\r\n")%r(GetRequest,78,"OK\x20\[CAPAB
SF:ILITY\x20LOGIN-REFERRALS\x20ID\x20ENABLE\x20IDLE\x20AUTH=PLAIN\]\x20Dov
SF:ecot\x20ready\.\r\nBAD\x20Error\x20in\x20IMAP\x20command\x20:\x20Unknow
SF:n\x20command\.\r\n")%r(SMBProgNeg,78,"OK\x20\[CAPABILITY\x20LOGIN-REFER
SF:RALS\x20ID\x20ENABLE\x20IDLE\x20AUTH=PLAIN\]\x20Dovecot\x20ready\.\r\nB
SF:AD\x20Error\x20in\x20IMAP\x20command\x20:\x20Unknown\x20command\.\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port199-TCP:V=7.80%I=7%D=2/10%Time=6023D345%P=x86_64-pc-linux-gnu%r(NUL
SF:L,58,"This\x20is\x20an\x20unrestricted\x20telnet\x20server\.\r\nPlease\
SF:x20do\x20not\x20user\x20for\x20production\x20purposes\r\n\r\n#\x20")%r(
SF:GenericLines,74,"This\x20is\x20an\x20unrestricted\x20telnet\x20server\.
SF:\r\nPlease\x20do\x20not\x20user\x20for\x20production\x20purposes\r\n\r\
SF:n#\x20\x20bash:\x20command\x20not\x20found\r\n#\x20")%r(RPCCheck,74,"Th
SF:is\x20is\x20an\x20unrestricted\x20telnet\x20server\.\r\nPlease\x20do\x2
SF:0not\x20user\x20for\x20production\x20purposes\r\n\r\n#\x20\x20bash:\x20
SF:command\x20not\x20found\r\n#\x20");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port264-TCP:V=7.80%I=7%D=2/10%Time=6023D345%P=x86_64-pc-linux-gnu%r(NUL
SF:L,20,"220\x20ESMTP\x20Postfix\x20\(Debian/GNU\)\r\n")%r(GenericLines,49
SF:,"220\x20ESMTP\x20Postfix\x20\(Debian/GNU\)\r\n502\x205\.5\.2\x20Error:
SF:\x20command\x20not\x20recognized\r\n")%r(GetRequest,49,"220\x20ESMTP\x2
SF:0Postfix\x20\(Debian/GNU\)\r\n502\x205\.5\.2\x20Error:\x20command\x20no
SF:t\x20recognized\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
```

```
SF-Port513-TCP:V=7.80%I=7%D=2/10%Time=6023D345%P=x86_64-pc-linux-gnu%r(NUL
SF:L,58,"This\x20is\x20an\x20unrestricted\x20telnet\x20server\.\r\nPlease\
SF:x20do\x20not\x20user\x20for\x20production\x20purposes\r\n\r\n#\x20")%r(
SF:DNSVersionBindReqTCP,74,"This\x20is\x20an\x20unrestricted\x20telnet\x20
SF:server\.\r\nPlease\x20do\x20not\x20user\x20for\x20production\x20purpose
SF:s\r\n\r\n#\x20\x20bash:\x20command\x20not\x20found\r\n#\x20")%r(DNSStat
SF:usRequestTCP,74,"This\x20is\x20an\x20unrestricted\x20telnet\x20server\.
SF:\r\nPlease\x20do\x20not\x20user\x20for\x20production\x20purposes\r\n\r\
SF:n#\x20\x20bash:\x20command\x20not\x20found\r\n#\x20");
Device type: firewall
Running (JUST GUESSING): Fortinet embedded (87%)
OS CPE: cpe:/h:fortinet:fortigate_100d
Aggressive OS guesses: Fortinet FortiGate 100D firewall (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OSs: Linux, Unix; CPE: cpe:/o:redhat:enterprise_linux:6

Host script results:
|_smb2-security-mode: SMB: Couldn't find a NetBIOS name that works for the server. Sorry!
|_smb2-time: ERROR: Script execution failed (use -d to debug)

TRACEROUTE (using port 22/tcp)
HOP RTT      ADDRESS
1   0.10 ms  _gateway (10.1.1.1)
2   0.50 ms  188.130.155.33
3   2.36 ms  1.123.18.84.in-addr.arpa (84.18.123.1)
4   2.56 ms  212.44.137.165
5   49.86 ms mx01.Frankfurt.gldn.net (79.104.235.74)
6   62.29 ms ipv4.de-cix.fra.de.as63949.linode.com (80.81.194.193)
7   65.44 ms 139.162.129.17
8   ... 30

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 902.22 seconds
```

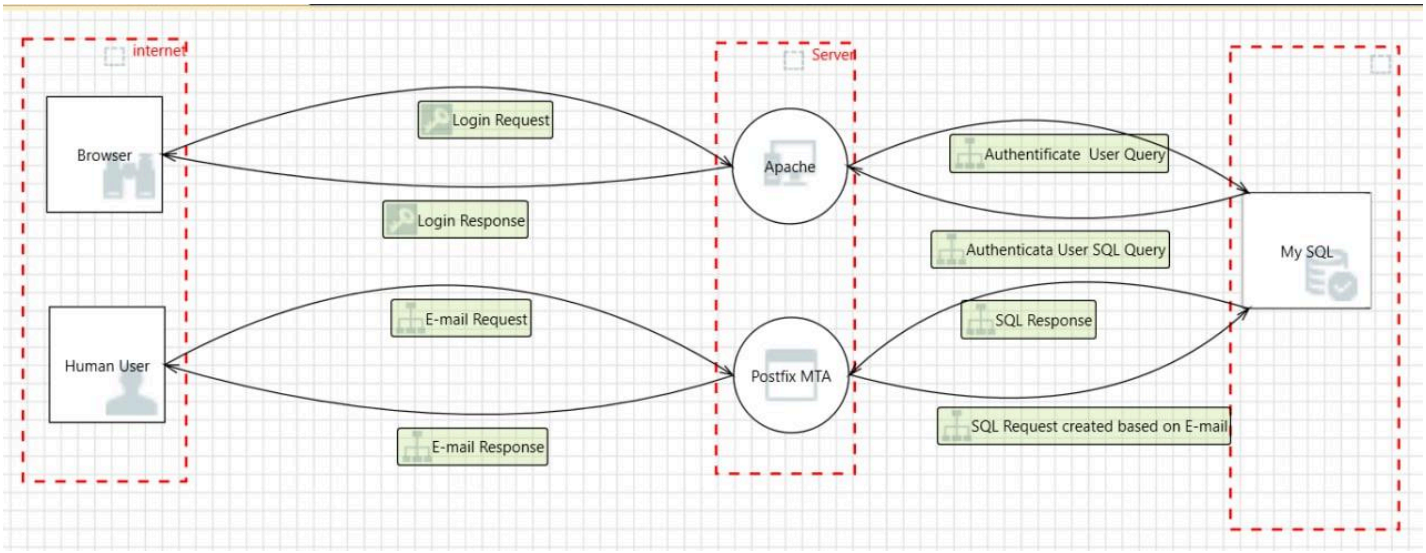
Process to port mappings:

```
[hourssch@de17 ~]$ ps -p 818586 -f
UID          PID    PPID  C STIME TTY          TIME CMD
hourssch  818586  457025  0 Jan30 ?        00:05:16 /opt/cpanel/ea-php72/root/usr/bin/php-cgi /home/hourssch/vocabstock.com/de/wp-admin/admin-ajax.php
[hourssch@de17 ~]$ ps -p 829555 -f
UID          PID    PPID  C STIME TTY          TIME CMD
hourssch  829555  457105  0 Jan30 ?        00:05:18 /opt/cpanel/ea-php72/root/usr/bin/php-cgi /home/hourssch/vocabstock.com/de/wp-cron.php
[hourssch@de17 ~]$ ps -p 868866 -f
UID          PID    PPID  C STIME TTY          TIME CMD
hourssch  868866  486373  0 Jan30 ?        00:05:20 /opt/cpanel/ea-php72/root/usr/bin/php-cgi /home/hourssch/vocabstock.com/de/wp-cron.php
[hourssch@de17 ~]$ ps -p 913971 -f
UID          PID    PPID  C STIME TTY          TIME CMD
hourssch  913971  456881  0 Jan30 ?        00:05:18 /opt/cpanel/ea-php72/root/usr/bin/php-cgi /home/hourssch/vocabstock.com/de/wp-cron.php
[hourssch@de17 ~]$ ps -p 927418 -f
UID          PID    PPID  C STIME TTY          TIME CMD
hourssch  927418  456750  0 Jan30 ?        00:05:20 /opt/cpanel/ea-php72/root/usr/bin/php-cgi /home/hourssch/vocabstock.com/de/wp-cron.php
[hourssch@de17 ~]$ ps -p 952825 -f
UID          PID    PPID  C STIME TTY          TIME CMD
hourssch  952825  530954  0 Jan30 ?        00:05:18 /opt/cpanel/ea-php72/root/usr/bin/php-cgi /home/hourssch/vocabstock.com/de/wp-cron.php
[hourssch@de17 ~]$ ps -p 977065 -f
UID          PID    PPID  C STIME TTY          TIME CMD
hourssch  977065  456881  0 Jan30 ?        00:05:16 /opt/cpanel/ea-php72/root/usr/bin/php-cgi /home/hourssch/vocabstock.com/de/wp-cron.php
[hourssch@de17 ~]$
```

The full content is here:

```
[hourssch@de17 ~]$ ps -p 818586 -f
UID          PID    PPID  C STIME TTY          TIME CMD
hourssch  818586  457025  0 Jan30 ?        00:05:16 /opt/cpanel/ea-php72/root/usr/bin/php-cgi
/home/hourssch/vocabstock.com/de/wp-admin/admin-ajax.php
[hourssch@de17 ~]$ ps -p 829555 -f
UID          PID    PPID  C STIME TTY          TIME CMD
```

```
hourssch  829555  457105  0 Jan30 ?        00:05:18 /opt/cpanel/ea-php72/root/usr/bin/php-cgi
/home/hourssch/vocabstock.com/de/wp-cron.php
[hourssch@de17 ~]$ ps -p 868866 -f
UID          PID    PPID  C STIME TTY          TIME CMD
hourssch  868866  486373  0 Jan30 ?        00:05:20 /opt/cpanel/ea-php72/root/usr/bin/php-cgi
/home/hourssch/vocabstock.com/de/wp-cron.php
[hourssch@de17 ~]$ ps -p 913971 -f
UID          PID    PPID  C STIME TTY          TIME CMD
hourssch  913971  456881  0 Jan30 ?        00:05:18 /opt/cpanel/ea-php72/root/usr/bin/php-cgi
/home/hourssch/vocabstock.com/de/wp-cron.php
[hourssch@de17 ~]$ ps -p 927418 -f
UID          PID    PPID  C STIME TTY          TIME CMD
hourssch  927418  456750  0 Jan30 ?        00:05:20 /opt/cpanel/ea-php72/root/usr/bin/php-cgi
/home/hourssch/vocabstock.com/de/wp-cron.php
[hourssch@de17 ~]$ ps -p 952825 -f
UID          PID    PPID  C STIME TTY          TIME CMD
hourssch  952825  530954  0 Jan30 ?        00:05:18 /opt/cpanel/ea-php72/root/usr/bin/php-cgi
/home/hourssch/vocabstock.com/de/wp-cron.php
[hourssch@de17 ~]$ ps -p 977065 -f
UID          PID    PPID  C STIME TTY          TIME CMD
hourssch  977065  456881  0 Jan30 ?        00:05:16 /opt/cpanel/ea-php72/root/usr/bin/php-cgi
/home/hourssch/vocabstock.com/de/wp-cron.php
```



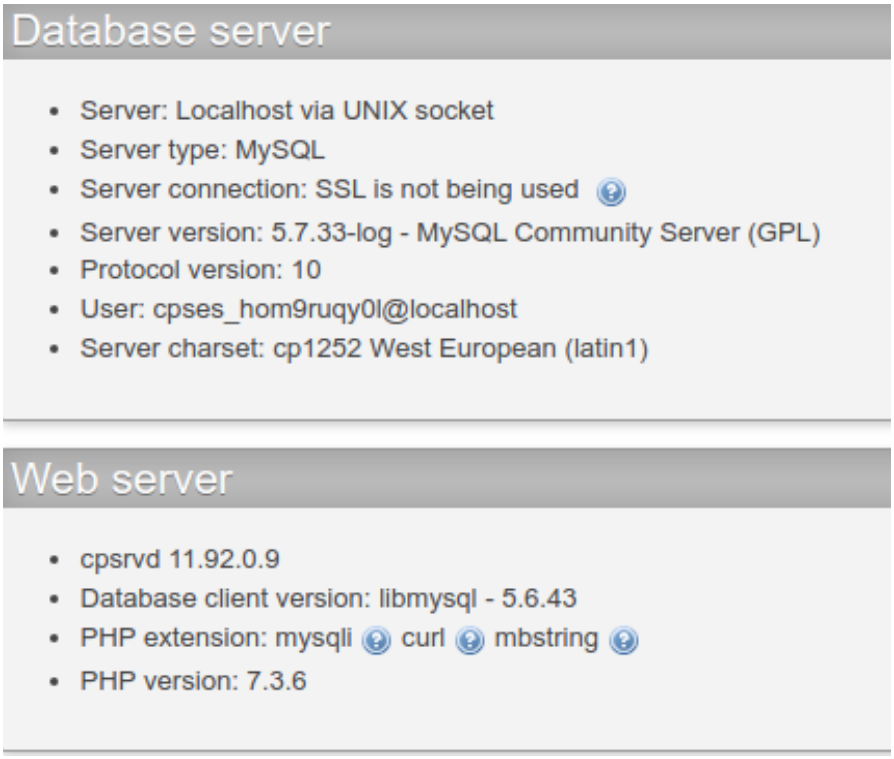
All interactions and data flows are specified in the attached report. It is generated from the Microsoft threat modeling tool.

Task 4 - The definition of assets

Technologies in use:

LAMP Stack:

- Linux - 2.6.32-954.3.5.lve1.4.77.el6.x86_64
- Apache Web Server 2.4.46
- Database (MySQL) 5.7.33
- PHP 7.2.33



Server Information

Item	Detail
Hosting Package	FastCloudPlus
Server Name	de17
cPanel Version	92.0 (build 9)
Apache Version	2.4.46
PHP Version	7.2.33
MySQL Version	5.7.33
Architecture	x86_64
Operating System	linux
Shared IP Address	172.105.94.109
Path to Sendmail	/usr/sbin/sendmail
Path to Perl	/usr/bin/perl
Perl Version	5.10.1
Kernel Version	2.6.32-954.3.5.lve1.4.77.el6.x86_64

Plugins:

- AddToAny Share Buttons (1.7.42), version 1.7.43 available.
- Advanced Custom Fields (5.9.3), Version 5.9.4 available.
- Ajax Search Lite (4.8.4), Version 4.8.6 available.
- Anywhere Elementor (1.2.2), Version 1.2.3 available.
- ARI Stream Quiz (1.2.21), Version 1.2.22 available.
- Contact Form 7 (5.3), Version 5.3.2 available.
- Contact Form CFDB7 (1.2.5.3), Version 1.2.5.8 available.
- Custom Post Type UI (1.8.1), Version 1.8.2 available.
- Elementor (3.0.14), Version 3.1.1 available.
- Essential Addons for Elementor (4.3.7), Version 4.5.0 available.
- Feed Them Social - for Twitter feed, Youtube, Pinterest and more (2.9.0), Version 2.9.3 available.
- Official Facebook Pixel (2.2.1), Version 3.0.2 available.
- Really Simple SSL (4.0.3), Version 4.0.8 available.
- Sucuri Security - Auditing, Malware Scanner and Hardening (1.8.24), Version 1.8.25 available.
- Unlimited Elements for Elementor (1.4.55), Version 1.4.65 available.
- UpdraftPlus - Backup/Restore (1.16.41), Version 1.16.47 available.
- Wordfence Security (7.4.12), Version 7.4.14 available.
- Yoast SEO (15.3), Version 15.8 available.

Themes:

- Twenty Nineteen (1.7), Version 1.9 available.

WordPress Users:

- Alic, admin user

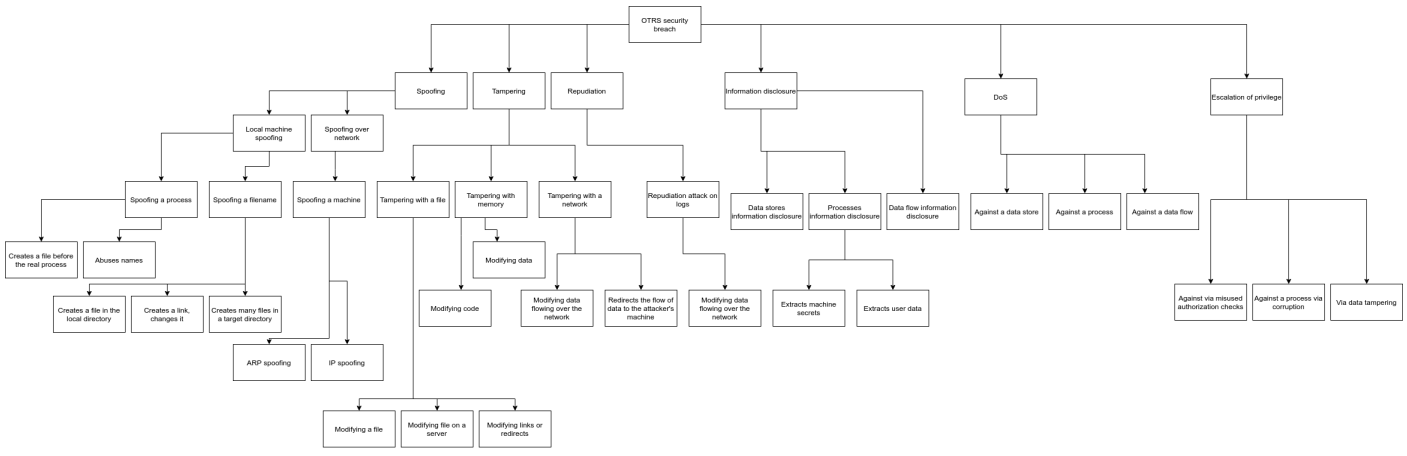
Task 5 - Select threat modeling technique

STRIDE (default choice)

STRIDE:

- Spoofing of user identity
- Tampering
- Repudiation
- Information disclosure (privacy breach or data leak)
- Denial of service (D.o.S)
- Elevation of privilege

We use the Microsoft Threat Modeling Tool to explore potential STRIDE security threats, we put all the model on the software



1) **AddToAny Share Buttons <= 1.7.14 - Conditional Host Header Injection**

This will take the following path on the tree:
OTRS security breach > Tampering > Tampering with a file > Modifying links or redirects

2) **Contact Form 7 < 5.3.2 - Unrestricted File Upload**

This will take the following path on the tree:
OTRS security breach > Tampering > Tampering with a file > Modifying file on a server

Task 6 - The definition of threats

Through the use of the threat modeling technique (STRIDE), the following threats have been identified:

1) **AddToAny Share Buttons <= 1.7.14 - Conditional Host Header Injection**
   There is a possibility to inject a custom Host-Header. Which can poison the website's cache and be shared instead of the legitimate website.
   The vulnerable code is in **add-to-any/trunk/add-to-any.php**

```
Vulnerable: ( is_ssl() ? 'https://' : 'http://' ) . $_SERVER['HTTP_HOST'] .
$_SERVER['REQUEST_URI']
Not-Vulnerable: home_url( $_SERVER['REQUEST_URI'] )
```

2) **Title: Contact Form 7 < 5.3.2 - Unrestricted File Upload**
   A form submitter can bypass Contact Form 7's filename sanitization, and upload a file which can be executed as a script file on the host server.
   The vulnerable code is in **includes/formatting.php**

```
Add: $filename = preg_replace( '/[\pC\pZ]+/i', '', $filename );
To the wpcf7_antiscript_file_name() function
```

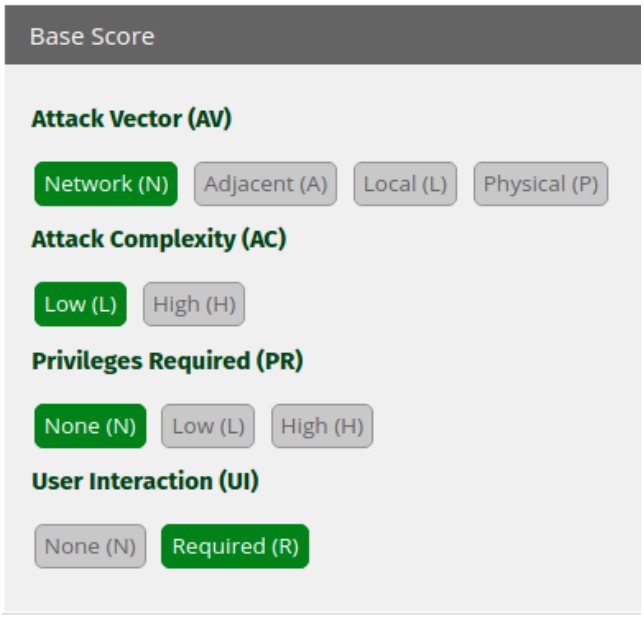
   And in **modules/akismet.php**

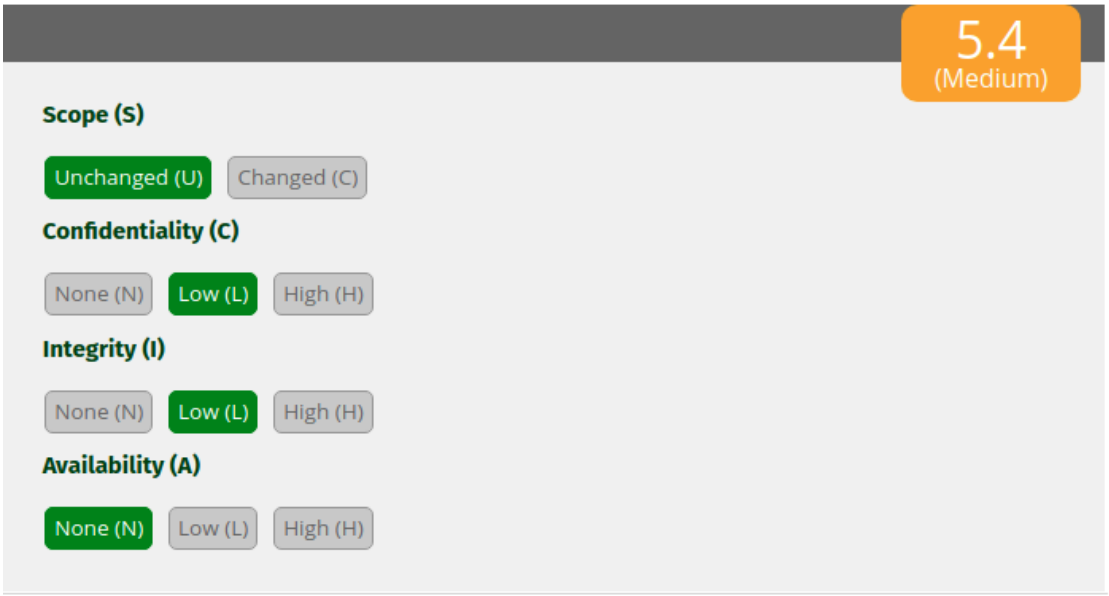
```
Delete: $c['comment_date_gmt'] = $submission->get_meta( 'timestamp' );

Add:  $datetime = date_create_immutable(
            '@' . $submission->get_meta( 'timestamp' )
      );

      if ( $datetime ) {
            $c['comment_date_gmt'] = $datetime->format( DATE_ATOM );
      }
```

Task 7 - The potential attacks severity calculation

1) AddToAny Share Buttons <= 1.7.14 - Conditional Host Header Injection

CVSS Score: 5.4 (Medium)





Attack Vector(AV) - Network(N): A vulnerability exploitable with network access means the vulnerable component is bound to the network stack and the attacker's path is through OSI layer 3 (the network layer). Such a vulnerability is often termed "remotely exploitable" and can be thought of as an attack being exploitable one or more network hops away.

Attack Complexity(AC) - Low(L): Specialized access conditions or extenuating circumstances do not exist. An attacker can expect repeatable success against the vulnerable component.

Privileges Required(PR) - None(N): The attacker is unauthorized prior to attack, and therefore does not require any access to settings or files to carry out an attack.

User Interaction(UI) - Required(R): Successful exploitation of this vulnerability requires a user to take some action before the vulnerability can be exploited.

Scope(S) - Unchanged(U): An exploited vulnerability can only affect resources managed by the same authority. In this case the vulnerable component and the impacted component are the same.

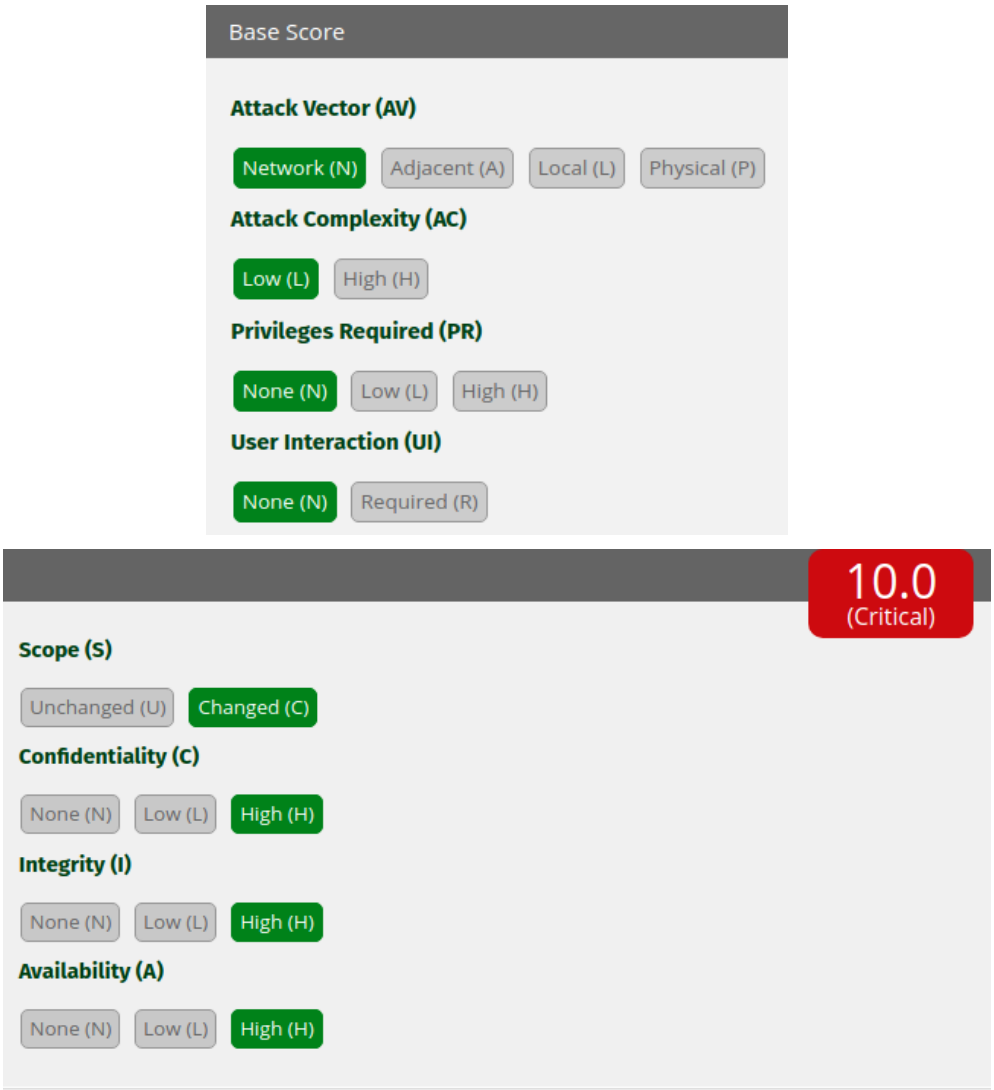
Confidentiality(C) - Low(L): There is some loss of confidentiality. Access to some restricted information is obtained, but the attacker does not have control over what information is obtained, or the amount or kind of loss is constrained. The information disclosure does not cause a direct, serious loss to the impacted component.

Integrity(I) - Low(L): Modification of data is possible, but the attacker does not have control over the consequence of a modification, or the amount of modification is constrained. The data modification does not have a direct, serious impact on the impacted component.

Availability(A) - None(N): There is no impact to availability within the impacted component.

1) Contact Form 7 < 5.3.2 - Unrestricted File Upload

CVSS Score: 10 (Critical)



Task 8 - Countermeasures definition

3) AddToAny Share Buttons <= 1.7.14 - Conditional Host Header Injection

The vulnerable code is in **add-to-any/trunk/add-to-any.php**

```
Vulnerable: ( is_ssl() ? 'https://' : 'http://' ) . $_SERVER['HTTP_HOST'] .
$_SERVER['REQUEST_URI']
Not-Vulnerable: home_url( $_SERVER['REQUEST_URI'] )
```

Changes include using the `home_url()` instead of the Host header when generating the current URL to be shared.
The advised countermeasure is to update to the latest version.

4) Contact Form 7 < 5.3.2 - Unrestricted File Upload

The vulnerable code is in **includes/formatting.php**

```
Add: $filename = preg_replace( '/[\pC\pZ]+/i', '', $filename );
To the wpcf7_antiscript_file_name() function
```

And in **modules/akismet.php**

```
Delete: $c['comment_date_gmt'] = $submission->get_meta( 'timestamp' );

Add:  $datetime = date_create_immutable(
            '@' . $submission->get_meta( 'timestamp' )
      );

      if ( $datetime ) {
            $c['comment_date_gmt'] = $datetime->format( DATE_ATOM );
      }
```

The advised countermeasure is to update to the latest version.

Task 9 - Threat modeling summarization

Asset	Threat	Impact	CVSS	Countermeasure
AddToAny Share Buttons (Plugin)	Conditional Host Header Injection	Medium	5.4	Update to the latest version
Contact Form 7 (Plugin)	Unrestricted File Upload	Critical	10	Update to the latest version

- **References:**

1. https://wpscan.com/vulnerability/469e8aa7-b689-438c-8421-fba8ae5972fb
2. https://plugins.trac.wordpress.org/changeset/1713858/add-to-any
3. https://github.com/takayukister/contact-form-7/compare/v5.3.1...v5.3.2
4. https://wpscan.com/vulnerability/7ea1de5f-6073-4fb7-9211-b36d977c5577