Vulnerability and exploit repositories

For many years, a number of vulnerabilities have been reported in the public domain. Some of these were disclosed with the PoC exploit code to prove the feasibility and viability of a vulnerability found in the specific software or application. And, many still remain unaddressed. This competitive era of finding the publicly available exploits and vulnerability information makes it easier for penetration testers to quickly search and retrieve the best available exploit that may suit their target system environment. You can also port one type of exploit to another type (for example, Win32 architecture to Linux architecture) provided that you hold intermediate programming skills and a clear understanding of OS-specific architecture. We have provided a combined set of online repositories that may help you to track down any vulnerability information or its exploit by searching through them.

Note

Not every single vulnerability found has been disclosed to the public on the Internet. Some are reported without any PoC exploit code, and some do not even provide detailed vulnerability information. For this reason, consulting more than one online resource is a proven practice among many security auditors.

The following is a list of online repositories:

Repository name	**Website URL**
Bugtraq SecurityFocus	http://www.securityfocus.com
OSVDB Vulnerabilities	http://osvdb.org
Packet Storm	http://www.packetstormsecurity.org
VUPEN Security	http://www.vupen.com
National Vulnerability Database	http://nvd.nist.gov
ISS X-Force	http://xforce.iss.net
US-CERT Vulnerability Notes	http://www.kb.cert.org/vuls
US-CERT Alerts	http://www.us-cert.gov/cas/techalerts/
SecuriTeam	http://www.securiteam.com
Government Security Org	http://www.governmentsecurity.org
Secunia Advisories	http://secunia.com/advisories/historic/
Security Reason	http://securityreason.com
XSSed XSS-Vulnerabilities	http://www.xssed.com
Security Vulnerabilities Database	http://securityvulns.com
SEBUG	http://www.sebug.net
BugReport	http://www.bugreport.ir

Repository name	Website URL
MediaService Lab	http://lab.mediaservice.net
Intelligent Exploit Aggregation Network	http://www.intelligentexploit.com
Hack0wn	http://www.hack0wn.com

Although there are many other Internet resources available, we have listed only a few reviewed ones. Kali Linux comes with an integration of exploit database from Offensive Security. This provides an extra advantage of keeping all archived exploits to date on your system for future reference and use. To access `Exploit-DB` , execute the following commands on your shell:

```
# cd /usr/share/exploitdb/
# vim files.csv
```

This will open a complete list of exploits currently available from `Exploit-DB` under the `/usr/share/exploitdb/platforms/` directory. These exploits are categorized in their relevant subdirectories based on the type of system (Windows, Linux, HP-UX, Novell, Solaris, BSD, IRIX, TRU64, ASP, PHP, and so on). Most of these exploits were developed using C, Perl, Python, Ruby, PHP, and other programming technologies. Kali Linux already comes with a handful set of compilers and interpreters that support the execution of these exploits.

Tip

How to extract particular information from the exploits list?

Using the power of Bash commands, you can manipulate the output of any text file in order to retrieve the meaningful data. You can either use `searchsploit` , or this can also be accomplished by typing `cat files.csv |cut -d"," -f3` on your console. It will extract the list of exploit titles from a `files.csv` file. To learn the basic shell commands, refer to http://tldp.org/LDP/abs/html/index.html.