IN5290 Ethical Hacking

Lecture 11: Vulnerability scanners

Laszlo Erdödi

laszloe@ifi.uio.no

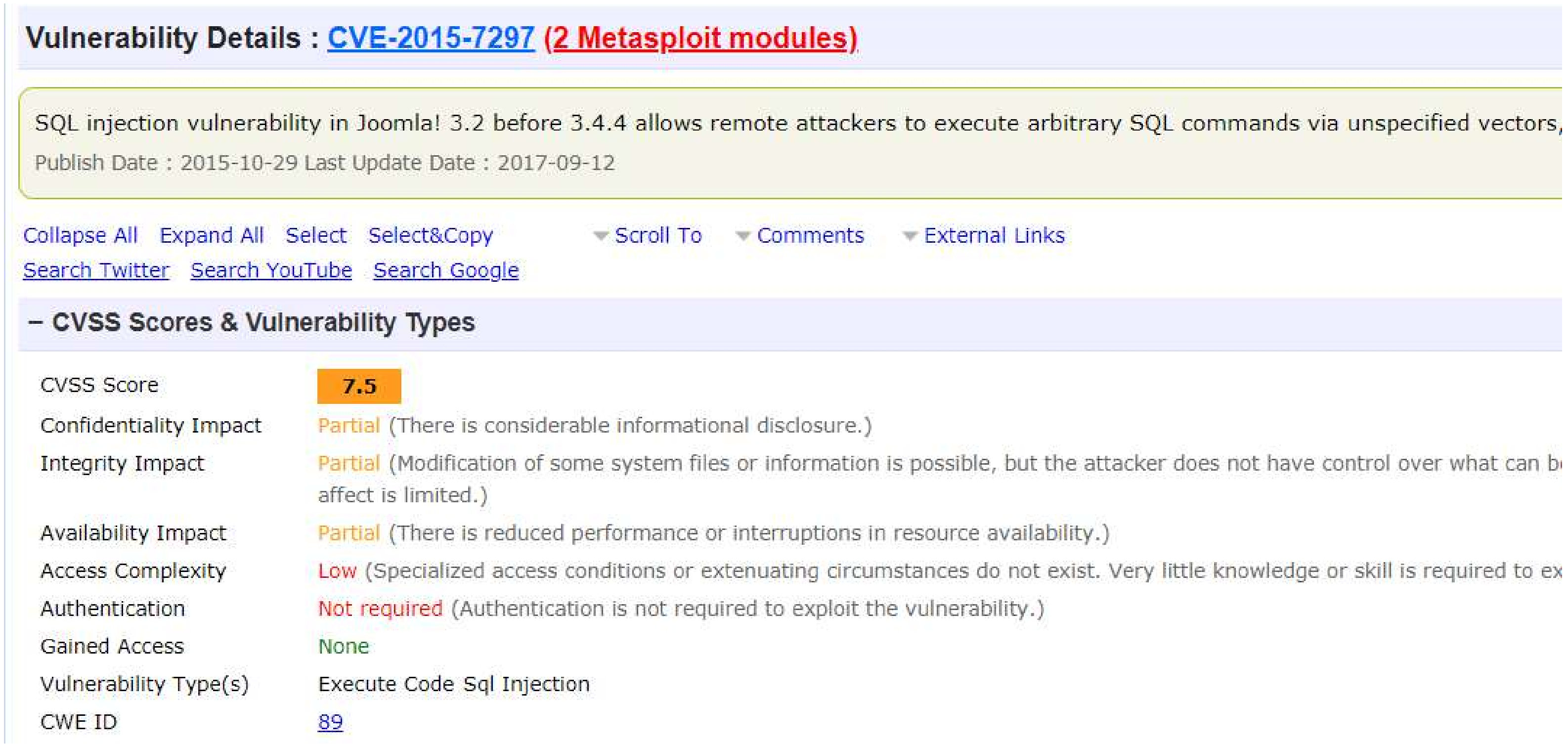
Lecture Overview

- Vulnerability databases
- Characteristics and application of automatic web security scanners

Vulnerability databases

Vulnerabilities are registered in a database, each vulnerability has a unique identification number.

Common Vulnerabilities and Exposures (CVE) E.g.: CVE-2015-7297



Vulnerability Details : CVE-2015-7297 (2 Metasploit modules)

SQL injection vulnerability in Joomla! 3.2 before 3.4.4 allows remote attackers to execute arbitrary SQL commands via unspecified vectors,

Publish Date : 2015-10-29 Last Update Date : 2017-09-12

Collapse All Expand All Select Select&Copy ▾ Scroll To ▾ Comments ▾ External Links
Search Twitter Search YouTube Search Google

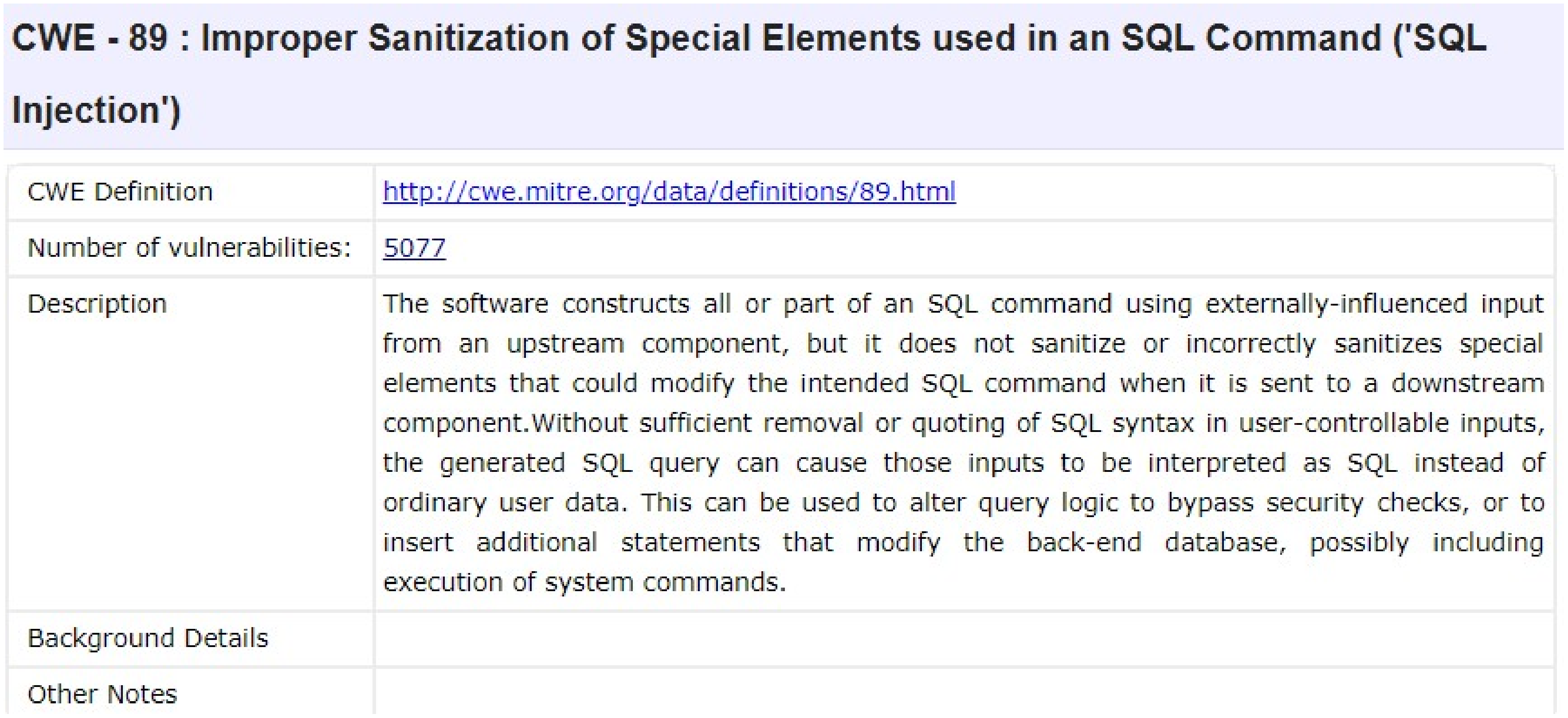
– CVSS Scores & Vulnerability Types

CVSS Score	7.5
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can b affect is limited.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to ex
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code Sql Injection
CWE ID	89

Vulnerability databases

Common Weakness Enumeration (CWE)

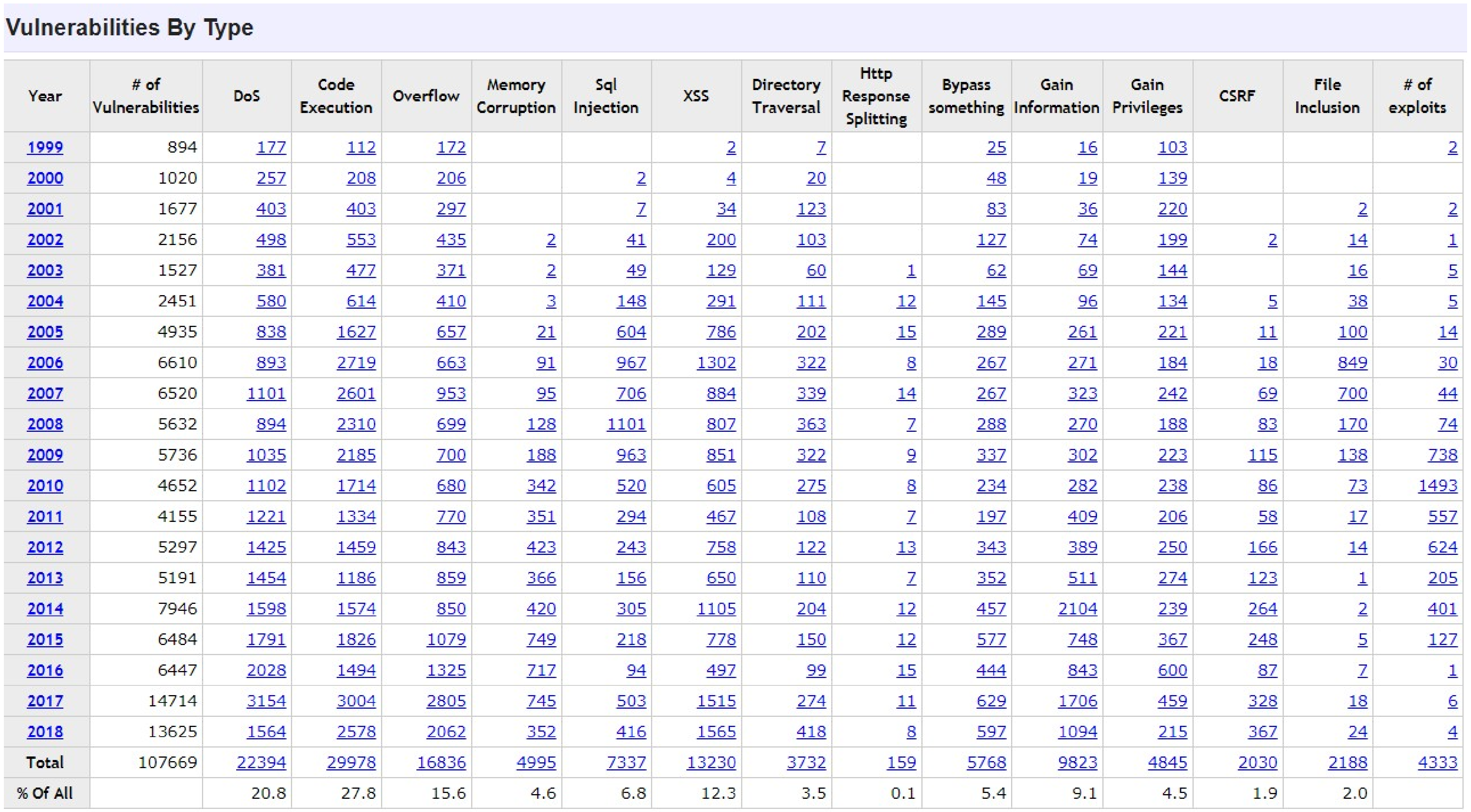
It contains vulnerability types, e.g. CWE-89



CWE - 89 : Improper Sanitization of Special Elements used in an SQL Command ('SQL Injection')

CWE Definition	http://cwe.mitre.org/data/definitions/89.html
Number of vulnerabilities:	5077
Description	The software constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not sanitize or incorrectly sanitizes special elements that could modify the intended SQL command when it is sent to a downstream component.Without sufficient removal or quoting of SQL syntax in user-controllable inputs, the generated SQL query can cause those inputs to be interpreted as SQL instead of ordinary user data. This can be used to alter query logic to bypass security checks, or to insert additional statements that modify the back-end database, possibly including execution of system commands.
Background Details	
Other Notes	

Vulnerability categories



Vulnerabilities By Type

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
1999	894	177	112	172			2	7		25	16	103			2
2000	1020	257	208	206		2	4	20		48	19	139			
2001	1677	403	403	297		7	34	123		83	36	220		2	2
2002	2156	498	553	435	2	41	200	103		127	74	199	2	14	1
2003	1527	381	477	371	2	49	129	60	1	62	69	144		16	5
2004	2451	580	614	410	3	148	291	111	12	145	96	134	5	38	5
2005	4935	838	1627	657	21	604	786	202	15	289	261	221	11	100	14
2006	6610	893	2719	663	91	967	1302	322	8	267	271	184	18	849	30
2007	6520	1101	2601	953	95	706	884	339	14	267	323	242	69	700	44
2008	5632	894	2310	699	128	1101	807	363	7	288	270	188	83	170	74
2009	5736	1035	2185	700	188	963	851	322	9	337	302	223	115	138	738
2010	4652	1102	1714	680	342	520	605	275	8	234	282	238	86	73	1493
2011	4155	1221	1334	770	351	294	467	108	7	197	409	206	58	17	557
2012	5297	1425	1459	843	423	243	758	122	13	343	389	250	166	14	624
2013	5191	1454	1186	859	366	156	650	110	7	352	511	274	123	1	205
2014	7946	1598	1574	850	420	305	1105	204	12	457	2104	239	264	2	401
2015	6484	1791	1826	1079	749	218	778	150	12	577	748	367	248	5	127
2016	6447	2028	1494	1325	717	94	497	99	15	444	843	600	87	7	1
2017	14714	3154	3004	2805	745	503	1515	274	11	629	1706	459	328	18	6
2018	13625	1564	2578	2062	352	416	1565	418	8	597	1094	215	367	24	4
Total	107669	22394	29978	16836	4995	7337	13230	3732	159	5768	9823	4845	2030	2188	4333
% Of All		20.8	27.8	15.6	4.6	6.8	12.3	3.5	0.1	5.4	9.1	4.5	1.9	2.0	

Automatic vulnerability scanners

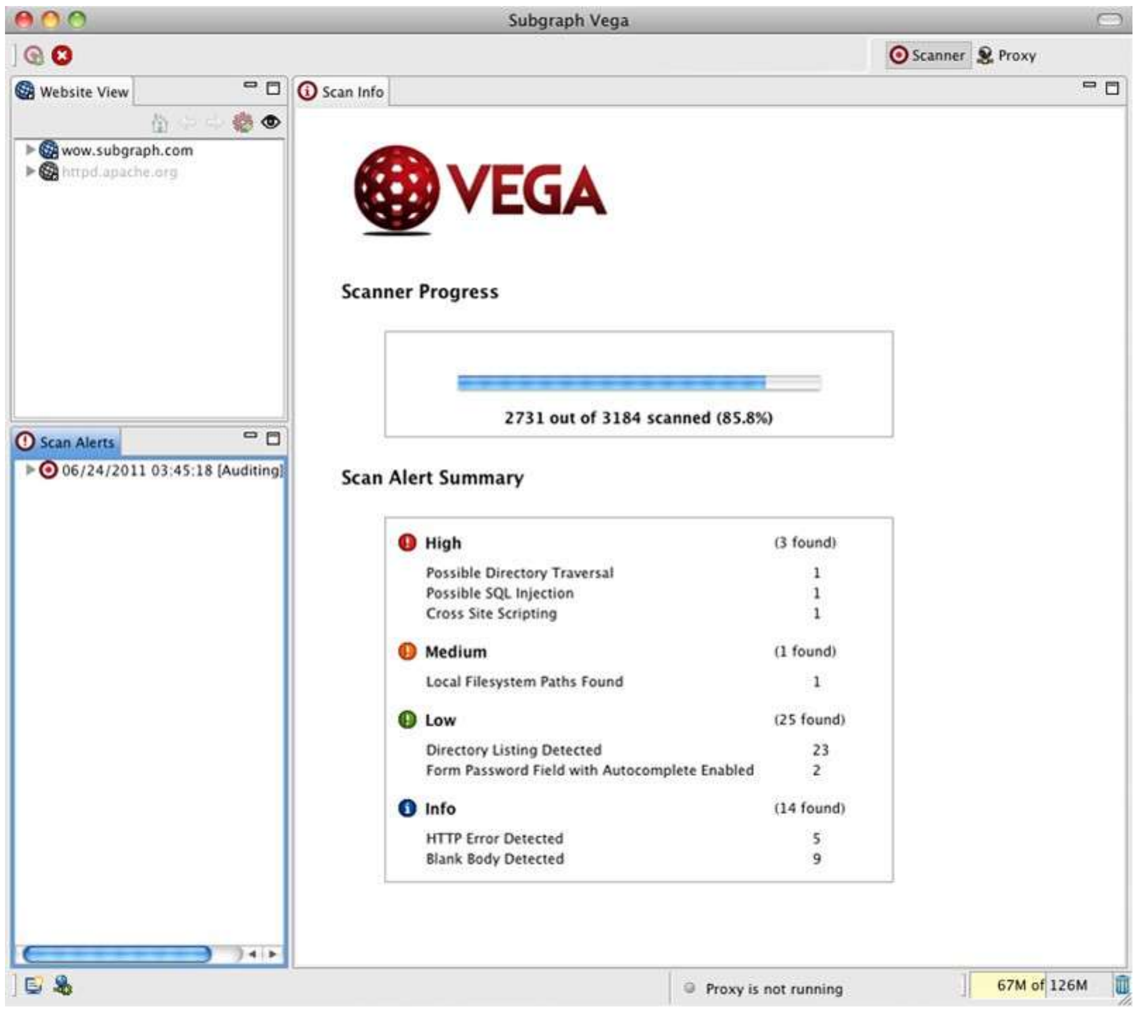
Automatic tools can carry out fast vulnerability identification. They have huge vulnerability databases that contain the requests that have to be sent for checking a vulnerability. Based on the answer the scanner decides wheter the vulneraility exists or not. The main characteristics of the scanners are:

- working with predifened web requests,
- since the complexity is not too high (they cannot really find connections between actions), usually they have several false positives,
- the identified vulnerabilities are categorized according to the severity (critical, high, medium, low, information disclosure),
- scans usually can be customized (which scripts to run),
- tools can be trained how to login to a password protected web area.

Web vulnerability scanners - VEGA

Vega is a free and open source web security scanner and web security testing platform to test the security of web applications.

DEMO…



06/24/2011 03:45:18 [Auditing]

Scanner Progress

2731 out of 3184 scanned (85.8%)

Scan Alert Summary

High	(3 found)
Possible Directory Traversal	1
Possible SQL Injection	1
Cross Site Scripting	1
Medium	(1 found)
Local Filesystem Paths Found	1
Low	(25 found)
Directory Listing Detected	23
Form Password Field with Autocomplete Enabled	2
Info	(14 found)
HTTP Error Detected	5
Blank Body Detected	9

Proxy is not running

67M of 126M

End of lecture