



6. Identificarea vulnerabilităților



Vulnerabilități

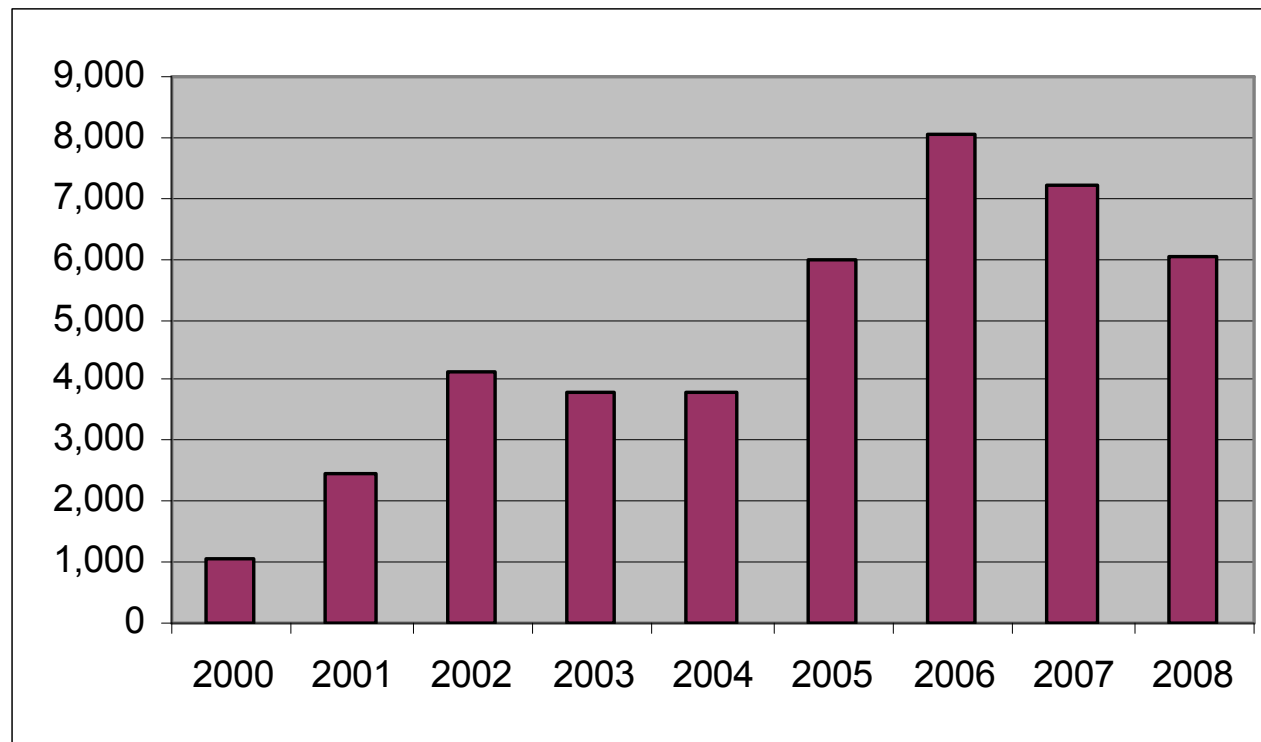
- Eroare de programare sau greșeală de configurare ce poate crea breșe în securitatea sistemelor
- Dacă nu sunt corectate la timp pot fi exploatare de către un eventual atacator
- Metode de corecție
 - instalare de patch-uri recomandate de producător
 - securizarea sistemelor (hardening)

Vulnerabilități (cont.)

Total vulnerabilități raportate (1995-Q3,2008): 44,074

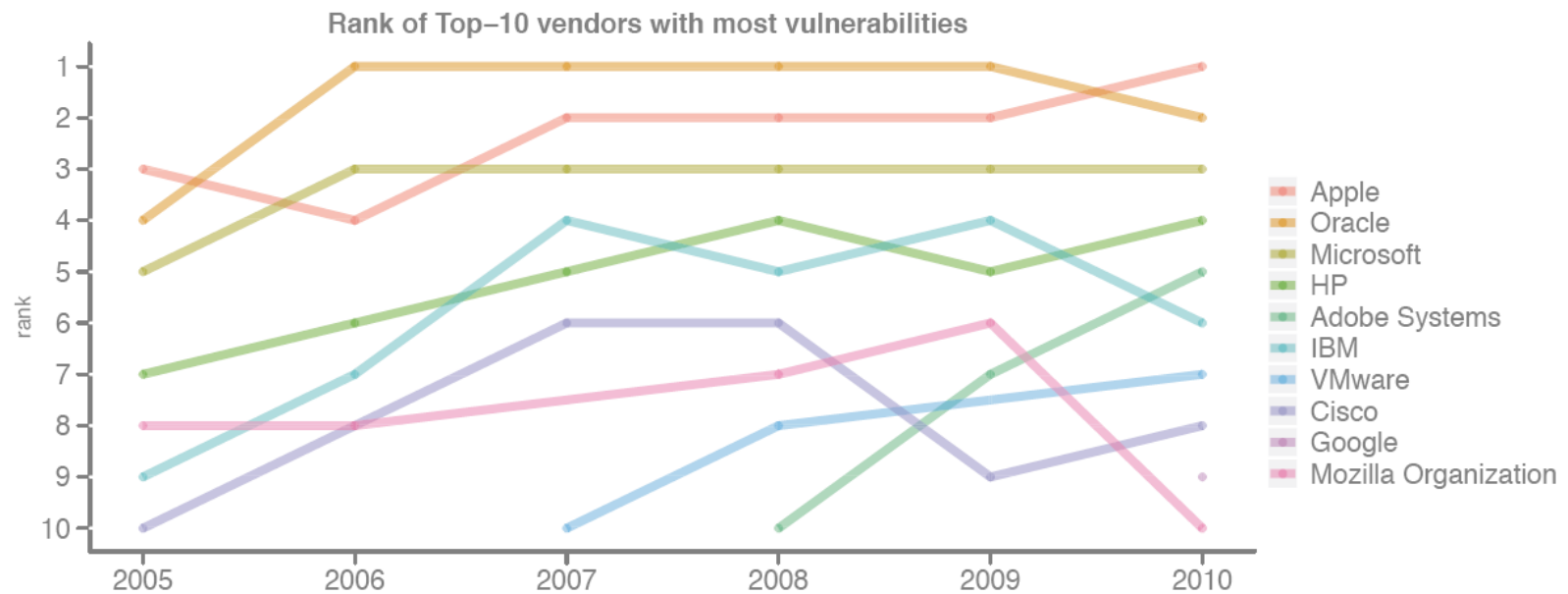
Sursa: CERT (<http://www.cert.org>)

Year	2000	2001	2002	2003	2004	2005	2006	2007
Vulnerabilities	1,090	2,437	4,129	3,784	3,780	5,990	8,064	7,236



Vulnerabilități (cont.)

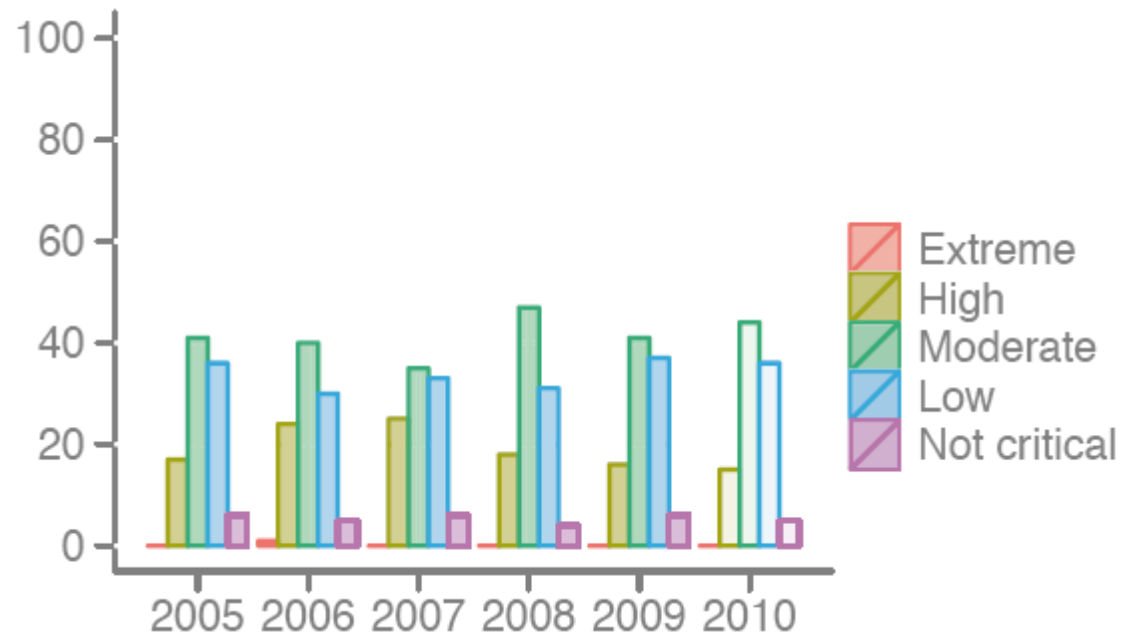
10 firme sunt responsabile pentru 38% din vulnerabilitățile dintr-un an!



Sursa: Secunia (<http://www.secunia.com>)

Vulnerabilități (cont.)

Numai 20% din vulnerabilități sunt critice!



Sursa: Secunia (<http://www.secunia.com>)

Vulnerabilități (cont.)

- **Common Vulnerabilities and Exposures (CVE)**
 - lista cu denumirile standardizate ale tuturor vulnerabilităților cunoscute public
 - dicționar de vulnerabilități (nu bază de date)
 - <http://cve.mitre.org/>
- **Open Vulnerability and Assessment Language (OVAL)**
 - standard ce descrie modul în care poate fi verificată existența unei vulnerabilități pe un sistem de calcul
 - <http://oval.mitre.org/>

Scannere de vulnerabilități

- **Automatizarea procesului de identificare și corectare a vulnerabilităților**
- **Clasificare**
 - funcție de locație de unde se face scanarea
 - network based
 - host based
 - funcție de credențialele folosite pe parcursul scanării
 - cu drepturi administrative
 - fără drepturi administrative
 - funcție de tipul de sisteme / aplicații testate
 - de uz general
 - pentru aplicații web

Scannere de vulnerabilități de uz general

- Nessus (<http://www.nessus.org>)
 - the best security tool!
- SARA - Security Auditor's Research Assistant (<http://www-arc.com/sara/>)
- X-scan (<http://www.xfocus.com>)
- MBSA (<http://www.microsoft.com>)

- GFI LANGuard (<http://www.gfi.com>)
- Retina (<http://www.eeye.com>)
- CORE IMPACT (<http://www.coresecurity.com>)
- Proventia Network Enterprise Scanner (<http://www.ibm.com>)
- QualysGuard (<http://www.qualys.com/>)
- SAINT - System Administrator's Integrated Network Tool (<http://www.saintcorporation.com/>)
- ...

Nessus

- **Arhitectură client / server**
 - server (scanning engine)
 - client (user interface)
 - autentificare utilizatori + criptare conexiune (SSL)
- **Modular**
 - funcționalități implementate sub forma de plugin-uri (script-uri)
 - aproximativ 40.000 de plugin-uri de scanare a vulnerabilităților
 - NASL (Nessus Attack Scripting Language)
- **Detectarea serviciilor active de pe calculatorul țintă se face prin port scanning**
 - ping, TCP connect(), SYN scan
- **Metode de scanare safe / distructive**
- **Generare de rapoarte (HTML)**
- **Compatibil CVE**
- **2 tipuri de abonamente**
 - ProfessionalFeed (1200 USD / year)
 - HomeFeed (free)

Nessus (cont.)

1. **Conectare în sistem (autentificare)**
2. **Definire ținte (calculator / subrețea)**
3. **Selectare politică de scanare (plugin-uri)**
4. **Scanare sisteme**
5. **Interpretare rezultate**

Nessus (cont.)

TENABLE
NESSUS 4

File Help

Scan Report

Report: 10/01/05 04:48:10 PM - Policy [Delete] [Export...]

10.254.40.71

- netbios-ns (137/udp)
- microsoft-ds (445/tcp)
- netbios-ssn (139/tcp)

MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (uncredentialed check)

Synopsis :
Arbitrary code can be executed on the remote host due to a flaw in the 'Server' service.

Description :
The remote host is vulnerable to a buffer overrun in the 'Server' service that may allow an attacker to execute arbitrary code on the remote host with the 'System' privileges.

Solution :
Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008 :
<http://www.microsoft.com/technet/security/bulletin/ms08-067.msp>

Risk factor :
Critical / CVSS Base Score : 10.0
(CVSS2#AV:N|AC:L|Au:N|C:C|I:C|A:C)
CVE : CVE-2008-4250
BID : 31874
Other references : OSVDB:49243
Nessus ID : [34477](#)

Filter... Stylesheet: Sort By CVE [View template...]

Disconnect

MBSA

- **Microsoft Baseline Security Analyzer**
- **Detectează vulnerabilități specifice produselor Microsoft:**
 - Security updates
 - Weak passwords
 - Windows configuration
 - IIS vulnerabilities
 - SQL vulnerabilities
- **Necesită drepturi administrative pe calculatorul țintă**
- **Generare de rapoarte**

MBSA (cont.)

The screenshot displays the Microsoft Baseline Security Analyzer (MBSA) interface. The window title is "Microsoft Baseline Security Analyzer". The main area is titled "View security report" and includes a "Sort Order" dropdown set to "Score (worst first)".

Scanned with MBSA version: 1.2.4013.0
Security update database version: 2006.5.9.0
Office update database version: 11.0.0.8903
Security assessment: Severe Risk (One or more critical checks failed.)

Security Update Scan Results

Score	Issue	Result
✖	Windows Security Updates	4 critical security updates are missing. 1 security updates could not be confirmed. What was scanned Result details How to correct this
✖	Office Updates	7 updates are missing. What was scanned Result details How to correct this
✘	MSXML Security Updates	1 products are using a service pack not at the latest version or have other warnings. What was scanned Result details How to correct this
✔	Microsoft VM Security Updates	No critical security updates are missing. What was scanned
✔	IIS Security	No critical security updates are missing.

Navigation buttons: Previous security report, Next security report

Footer: © 2002-2004 Microsoft Corporation. © 2002-2004 Shavlik Technologies, LLC. All rights reserved.

Notification: A new version of MBSA is available! Click [here](#) to go to the download page

Vulnerabilități specifice aplicațiilor Web

**“Over 70% of security vulnerabilities exist at the application layer,
not the network or system layer.”**

– Gartner 2004-2006



Vulnerabilități specifice aplicațiilor Web (cont.)

- **Unvalidated Input**
- **Cookie Poisoning**
- **CGI Parameters**
- **SQL Injection**
- **Cross site scripting (XSS)**
- **Directory Traversal**
- **Buffer Overflow**
- ...

Scannere de vulnerabilități pentru aplicații Web

- Nikto (<http://www.cirt.net/nikto2>)
- Paros proxy (<http://www.parosproxy.org>)
- Burpsuite (<http://portswigger.net/suite/>)

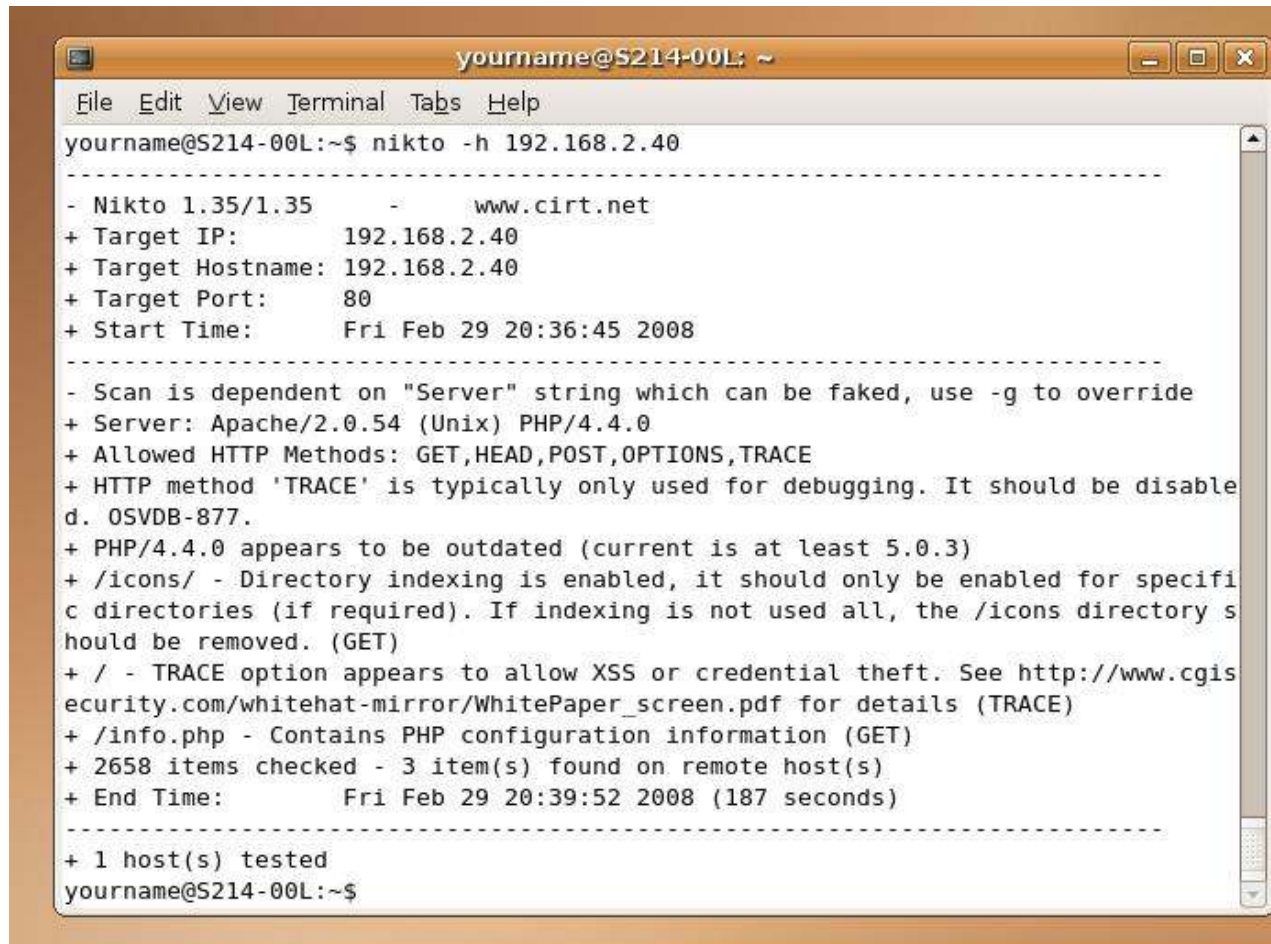
- WebInspect (<http://www.spidynamics.com>)
- Acunetix WVS (<http://www.acunetix.com>)
- Rational AppScan (<http://www.ibm.com>)
- N-Stealth (<http://www.nstalker.com/nstealth/>)

- Open Web Application Security Project (OWASP)
 - <http://www.owasp.org/>

Nikto

- **Open Source (GPL)**
- **Utilitar în linie de comandă**
- **Verificări efectuate:**
 - server and software misconfigurations
 - default files and programs
 - insecure files and programs
 - outdated servers and programs
- **Asigură identificarea modulelor software instalate pe serverul de Web (php, perl, etc)**
- **Suport pentru SSL, LibWhisker2 (anti IDS)**
- **Generare rapoarte în diverse formate (text, CSV, HTML, XML, NBE)**
- **Permite integrarea cu Nessus**
 - lansarea automată a programului nikto atunci când Nessus detectează un server de Web

Nikto (cont.)

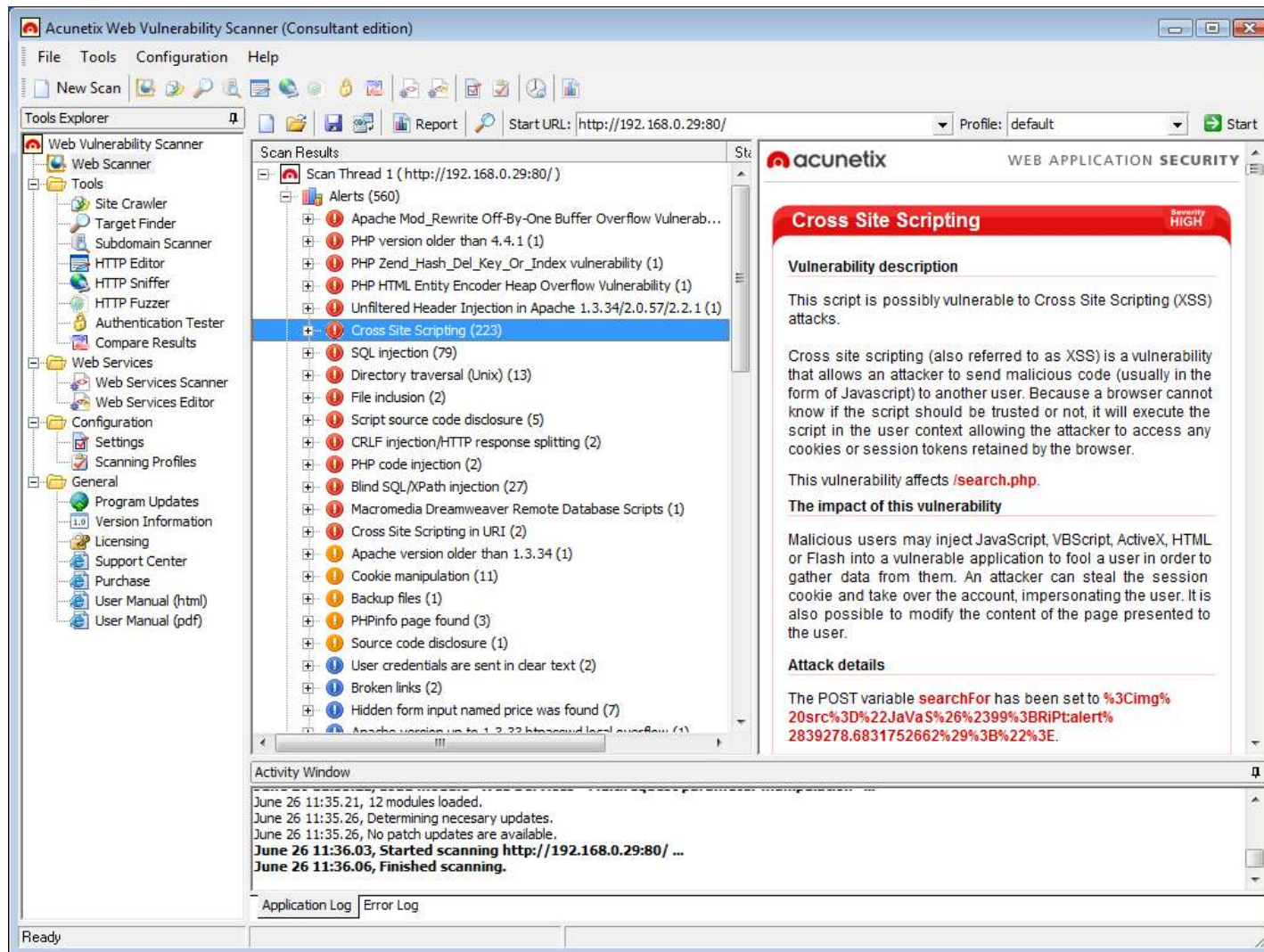


```
yourname@S214-00L: ~
File Edit View Terminal Tabs Help
yourname@S214-00L:~$ nikto -h 192.168.2.40
-----
- Nikto 1.35/1.35      -      www.cirt.net
+ Target IP:          192.168.2.40
+ Target Hostname:    192.168.2.40
+ Target Port:        80
+ Start Time:         Fri Feb 29 20:36:45 2008
-----
- Scan is dependent on "Server" string which can be faked, use -g to override
+ Server: Apache/2.0.54 (Unix) PHP/4.4.0
+ Allowed HTTP Methods: GET,HEAD,POST,OPTIONS,TRACE
+ HTTP method 'TRACE' is typically only used for debugging. It should be disabled. OSVDB-877.
+ PHP/4.4.0 appears to be outdated (current is at least 5.0.3)
+ /icons/ - Directory indexing is enabled, it should only be enabled for specific directories (if required). If indexing is not used all, the /icons directory should be removed. (GET)
+ / - TRACE option appears to allow XSS or credential theft. See http://www.cgisecurity.com/whitehat-mirror/WhitePaper_screen.pdf for details (TRACE)
+ /info.php - Contains PHP configuration information (GET)
+ 2658 items checked - 3 item(s) found on remote host(s)
+ End Time:          Fri Feb 29 20:39:52 2008 (187 seconds)
-----
+ 1 host(s) tested
yourname@S214-00L:~$
```

Acunetics WVS

- **Verificări efectuate:**
 - CGI testing
 - parameter manipulation (SQL Injection, XSS, ...)
 - text search
 - port scanning
 - Google Hacking Database
- **Generare de rapoarte personalizate**
- **Suport pentru AJAX / Web 2.0**
- **Suport pentru CAPTCHA, Single Sign-On și mecanisme de autentificare bazate pe doi factori**
- **Unelte auxiliare**
 - HTTP Editor, HTTP Sniffer, HTTP Fuzzer, Scripting tool, Blind SQL Injector
- **1500 USD (Single User Single URL Perpetual License)**

Acunetics WVS (cont.)



The screenshot displays the Acunetics Web Vulnerability Scanner (WVS) interface. The main window is titled "Acunetics Web Vulnerability Scanner (Consultant edition)". The interface is divided into several sections:

- Tools Explorer:** A tree view on the left showing various tools like Site Crawler, Target Finder, Subdomain Scanner, HTTP Editor, HTTP Sniffer, HTTP Fuzzer, Authentication Tester, Compare Results, Web Services, Web Services Scanner, Web Services Editor, Configuration, Settings, Scanning Profiles, and General.
- Scan Results:** A central pane showing a list of alerts. The "Cross Site Scripting (223)" alert is selected and highlighted in blue. Other alerts include Apache Mod_Rewrite Off-By-One Buffer Overflow Vulnerability, PHP version older than 4.4.1, PHP Zend_Hash_Del_Key_Or_Index vulnerability, PHP HTML Entity Encoder Heap Overflow Vulnerability, Unfiltered Header Injection in Apache, SQL injection, Directory traversal, File inclusion, Script source code disclosure, CRLF injection/HTTP response splitting, PHP code injection, Blind SQL/XPath injection, Macromedia Dreamweaver Remote Database Scripts, Cross Site Scripting in URI, Apache version older than 1.3.34, Cookie manipulation, Backup files, PHPinfo page found, Source code disclosure, User credentials are sent in clear text, Broken links, and Hidden form input named price was found.
- Alert Detail View:** A pane on the right showing the details for the selected "Cross Site Scripting" alert. It includes a red header with "Cross Site Scripting" and "Security HIGH". The "Vulnerability description" section explains that the application is vulnerable to XSS attacks. The "The impact of this vulnerability" section states that malicious users can inject JavaScript, VBScript, ActiveX, HTML, or Flash into the application to steal session cookies and impersonate users. The "Attack details" section shows a sample payload: `The POST variable searchFor has been set to %3Cimg%20src%3D%22JaVaS%26%2399%3BRiPt>alert%2839278.6831752662%29%3B%22%3E.`
- Activity Window:** A log window at the bottom showing system messages, including "June 26 11:35.21, 12 modules loaded.", "June 26 11:35.26, Determining necessary updates.", "June 26 11:35.26, No patch updates are available.", "June 26 11:36.03, Started scanning http://192.168.0.29:80/ ...", and "June 26 11:36.06, Finished scanning."

