

滲透測試實務應用

Code Review & HostVA tools

洪峻宸, 邵靖翔

Code Review: Bearer

- Bearer CLI 是一種靜態應用程式安全測試 (SAST) 工具，可掃描原始程式碼並分析資料流，以發現、過濾安全性和隱私風險並確定其優先順序。
- 目前支援：JavaScript/TypeScript (GA)、Ruby (GA)、PHP (GA)、Java (Beta)、Go (Beta)、Python (Alpha)
- Pros: 安裝快速、CLI
- Cons: 沒有好看的report

Code Review: Bearer

檢測出多種風險、歸類並依照風險等級排序

以檢測Vulnerable-Code-Snippets為例，共檢測出87個風險

其中0個為critical、49個為high、18個為low、17個warning

```
G: Leakage of information in logger message [CWE-532]
//docs.bearer.com/reference/rules/javascript_lang_logger_leak
ore this finding, run: bearer ignore add 0b9521f380cb436411d674d135bc4cc9_1

SQL Injection/example2.js:34
system console.log('GENERATED id: ' + result.id);

G: Leakage of information in logger message [CWE-532]
//docs.bearer.com/reference/rules/javascript_lang_logger_leak
ore this finding, run: bearer ignore add 992b386b457207fe628516a6848fad4c_0

SSRF/express.js:21
.on('error', (err) => console.log(err, 'controller.url.download.error'))

G: Unsanitized non-literal filename detected [CWE-73]
//docs.bearer.com/reference/rules/javascript_lang_non_literal_fs_filename
ore this finding, run: bearer ignore add 13284aa93353bdf02b5fd98352f354d8_0

Path Traversal/eq.js:56
result = fs.readFileSync(path)

G: Usage of dangerous 'eval' function [CWE-95]
//docs.bearer.com/reference/rules/ruby_lang_eval_linter
ore this finding, run: bearer ignore add 74c856744e327b5b7a0d7e7f831ca890_0

Code Injection/example1.rb:7
nt eval(first_number+" "+second_number)

ecks, 87 findings

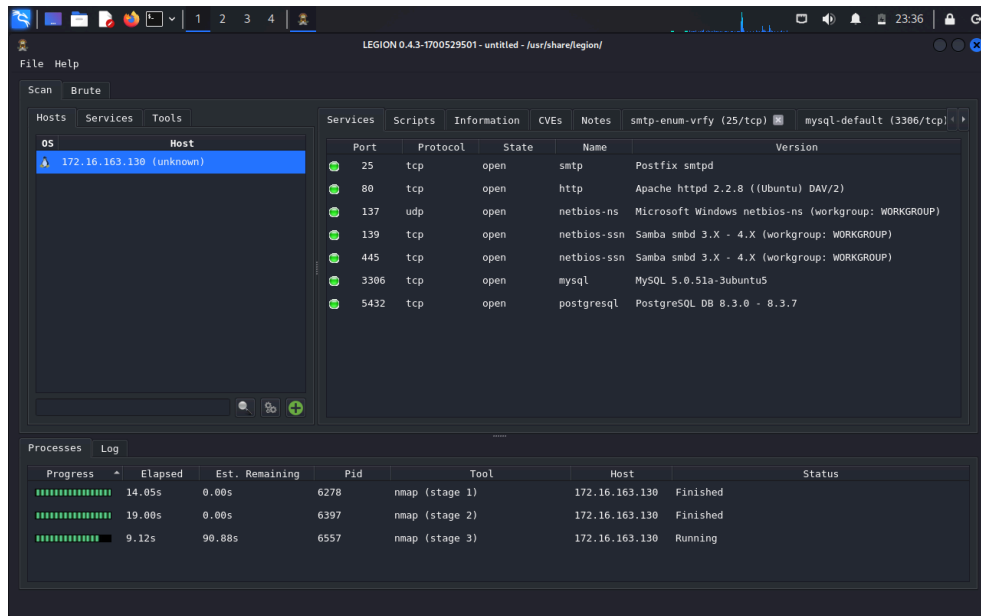
AL: 0
49 (CWE-611, CWE-73, CWE-78, CWE-79, CWE-798, CWE-89, CWE-918, CWE-95, CWE-98)
: 3 (CWE-346, CWE-601)
8 (CWE-693, CWE-79)
G: 17 (CWE-532, CWE-73, CWE-78, CWE-95)
```

elp or want to discuss the output? Join the Community <https://discord.gg/eahZBJU>

Host VA: Legion

Legion是一個開源的半自動網路滲透測試工具，適合用來進行探索 可以識別網路中的設備並對暴露出的目標設備進行攻擊

會利用Nikto、whataweb、sslyzer、vulners、SMBenum、NMAP、THC Hydra、Shodan的自動化程序來進行掃描



Host VA: Legion

The screenshot shows the Legion Host VA interface. The title bar reads "LEGION 0.3.7-1596220187 - untitled - /usr/share/legion/". The menu bar includes "File" and "Help". The main window has tabs for "Scan" and "Brute". Under "Scan", there are sub-tabs for "Hosts", "Services", and "Tools". The "Hosts" tab is active, displaying a list of hosts. The host "10.0.2.4 (unknown)" is selected. Below the host list is a search bar and three icons: a magnifying glass, a gear, and a green plus sign. The "Services" tab is also visible, showing a table of CVEs for the selected host. The table has columns for "CVE Id", "CVSS Score", "Product", "Version", "CVE URL", "Source", and "E". The "Processes" tab is active at the bottom, showing a log of activities.

LEGION 0.3.7-1596220187 - untitled - /usr/share/legion/

File Help

Scan Brute

Hosts Services Tools

OS	Host
?	10.0.2.1 (unknown)
?	10.0.2.2 (unknown)
?	10.0.2.3 (unknown)
?	10.0.2.4 (unknown)
?	10.0.2.5 (unknown)
?	10.0.2.6 (unknown)
?	10.0.2.15 (unknown)

Services Scripts Information CVEs Notes screenshot (80/tcp) smtp-enum-vrfy (25/tcp) mysql

CVE Id	CVSS Score	Product	Version	CVE URL	Source	E
EDB-ID:21018	10.0	openssh	4.7p1	https://vulners.com/exploitdb/EDB-ID:21018	openbsd	un
CVE-2001-0554	10.0	openssh	4.7p1	https://vulners.com/cve/CVE-2001-0554	openbsd	21
PACKETSTORM:101052	7.8	openssh	4.7p1	https://vulners.com/packetstorm/PACKETSTORM:101052	openbsd	un
PACKETSTORM:105078	7.8	openssh	4.7p1	https://vulners.com/packetstorm/PACKETSTORM:105078	openbsd	un
MSF:ILITIES/OPENBSD-OP...	7.5	openssh	4.7p1	https://vulners.com/metasploit/MSF:ILITIES/OPENBSD-OP...	openbsd	un
SECURITYVULNS:VULN:81...	7.5	openssh	4.7p1	https://vulners.com/securityvulns/SECURITYVULNS:VULN:81...	openbsd	un
CVE-2010-4478	7.5	openssh	4.7p1	https://vulners.com/cve/CVE-2010-4478	openbsd	un
MSF:ILITIES/LINUXRPM-EL...	7.5	openssh	4.7p1	https://vulners.com/metasploit/MSF:ILITIES/LINUXRPM-EL...	openbsd	un

Processes Log

'os_nodes' to process: 0
'ports' to process: 0
Finished in 3.779820203781128 seconds.
Scheduler started!
Running tools for: http on 10.0.2.2:34027
Running tools for: status on 10.0.2.4:32818
Running tools for: java-rmi on 10.0.2.4:36689
Running tools for: mountd on 10.0.2.4:39037

Thanks for Listening