

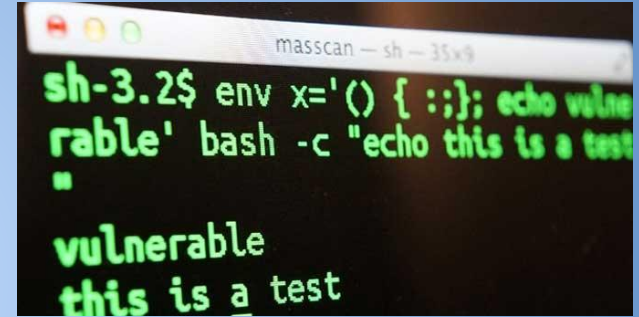
# The Shellshock Bug

Emily McCorry, Jenn Collins, Erica Wivagg

*“The new vulnerability in the Bash shell is the worst we’ve seen in many years. No software on critical systems can be assumed as safe.” ~ Larry Zeltzer*

# Shellshock in the media

- programming bug: “Bash bug”
- compared with Heartbleed
- potential threat to:
  - computers, servers
  - power plants, municipal water systems
  - common object like refrigerators, cameras



```
masscan - sh - 35x9
sh-3.2$ env x='() { :; }; echo vulnerable' bash -c "echo this is a test"
vulnerable
this is a test
```

# What is it?

- family of bugs from CVE-201406271
- vulnerability in Bash
  - shell used in Linux, Unix, Mac OS X
- adversary can send harmful commands to machine
  - type of arbitrary code execution attack



# Normal Execution vs Shellshock

## Normal execution:

env testcode= '() {echo "Here I am.";}' bash -c :

```
testcode= '() {echo "Here I am.";}'
```

- restart the shell and read/load in variable



-calling our  
code:

```
$testcode
```

```
Here I am
```



# Shellshock vulnerability in action:

env testcode= '() {echo "Here I am.";} echo MUAHAHA' bash -c

```
testcode= '() {echo "Here I am.";}  
echo MUAHAHA'
```



-load with new shell/evaluate variables BUT  
execute extra text as command??

```
MUAHAHA
```

```
without prompt  
from user!
```



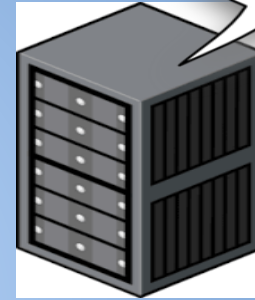
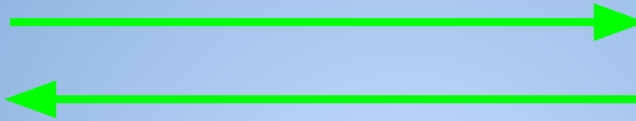
# An Overview



Sounds good



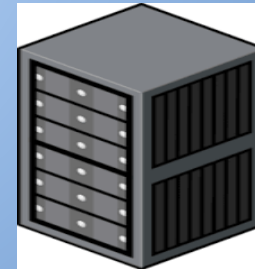
I'm using a  
Firefox Brower



Here's the web page info you  
want to view



{ ::}; show me  
all your files



\*return all the  
files

# Who's at risk for attack?

- web servers → use CGI (Common Gateway Interface) to create dynamic content
- if the CGI content uses bash at any point, can be exploited
  - ie content is executed, variables created
- SSH, DHCP clients

# How do Shellshock and CGI work?

```
HTTP_ACCEPT_ENCODING=  
HTTP_ACCEPT_LANGUAGE=  
HTTP_CACHE_CONTROL=  
HTTP_PRAGMA=no-cache  
HTTP_USER_AGENT=Mozilla/5.0  
HTTP_HOST=cloudflare.com
```





F12

DOM Explorer

Console ✖ 3

Debugger

Network

UI Responsiveness

Profiler

Memory

Emulation



### Mode

Document mode

Edge (Default) ▼ ⓘ

Browser profile

Default

### Display

Orientation

Landscape ▼

Resolution

Default ▼

### Geolocali

Simulate G

Latitude

Longitude

User agen

User agent string

Custom ▼

Enter a custom user agent string

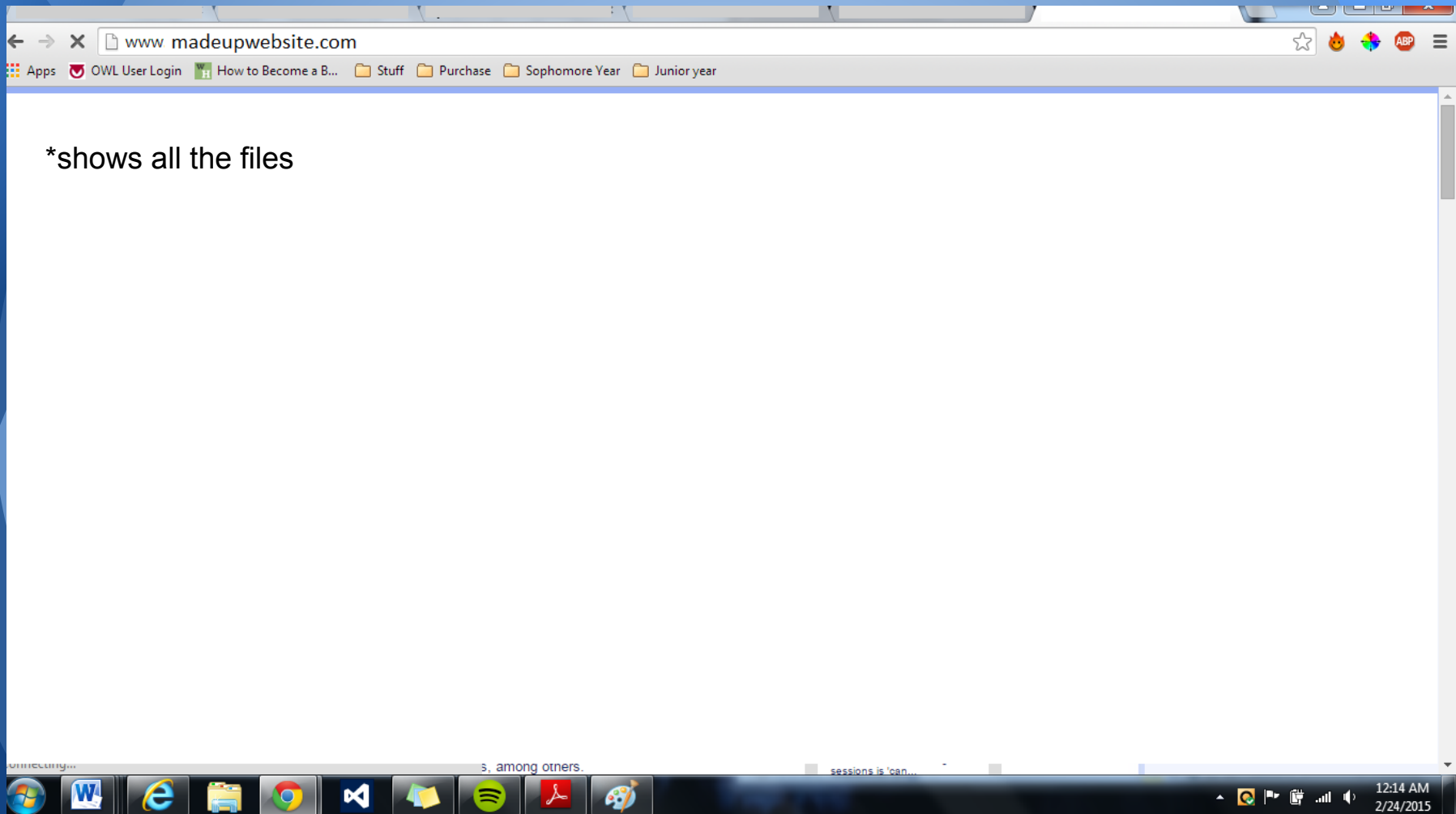
Custom string

() { ::}; \*show me your files ✕

http://comcast.kaya

Custom

U59/2015-03-20/2015-03-23/-1,-1/2/0,0,0/-



\*shows all the files

# What caused the bug (and could we have stopped it)?

- Bash maintained by Chet Ramey
- bug existed since 1989
- discovered: September 2014  
--> 25 years!
- only way to stop it? **catch it sooner**



# How has it been exploited?

- Botnet and DDOS attacks
  - Romanian hackers attacked Yahoo Games
  - group used botnet against Akamai
  - scans for vulnerable machines by botnet
- Possibly more attacks before Shellshock was discovered?

# Legal Consequences?

- HIPAA: companies must protect against threats to security of information
- Companies required to tell customers about vulnerabilities, patches

# References:

<http://www.jonesday.com/shellshock-the-perfect-10-exploit-easy-to-use-devastating-impact-09-30-2014/>

[http://en.wikipedia.org/wiki/Shellshock\\_%28software\\_bug%29](http://en.wikipedia.org/wiki/Shellshock_%28software_bug%29)

<http://fedoramagazine.org/shellshock-how-does-it-actually-work/>

<https://www.youtube.com/watch?v=ArEOVHQu9nk>

<http://www.symantec.com/connect/blogs/shellshock-all-you-need-know-about-bash-bug-vulnerability>

<http://mashable.com/2014/09/26/what-is-shellshock/>

<http://www.howtogeek.com/113439/how-to-change-your-browsers-user-agent-without-installing-any-extensions/>

<https://blog.cloudflare.com/inside-shellshock/>



**Any Questions?**