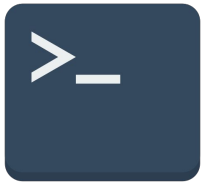
# ShellShock

LA RIVIERE-GILLET Thibaud
GITTON Marine
GIRARDET Maxence
GOT-BOUTET Flavien
CHALLET Nathan

# Présentation

Septembre 2014

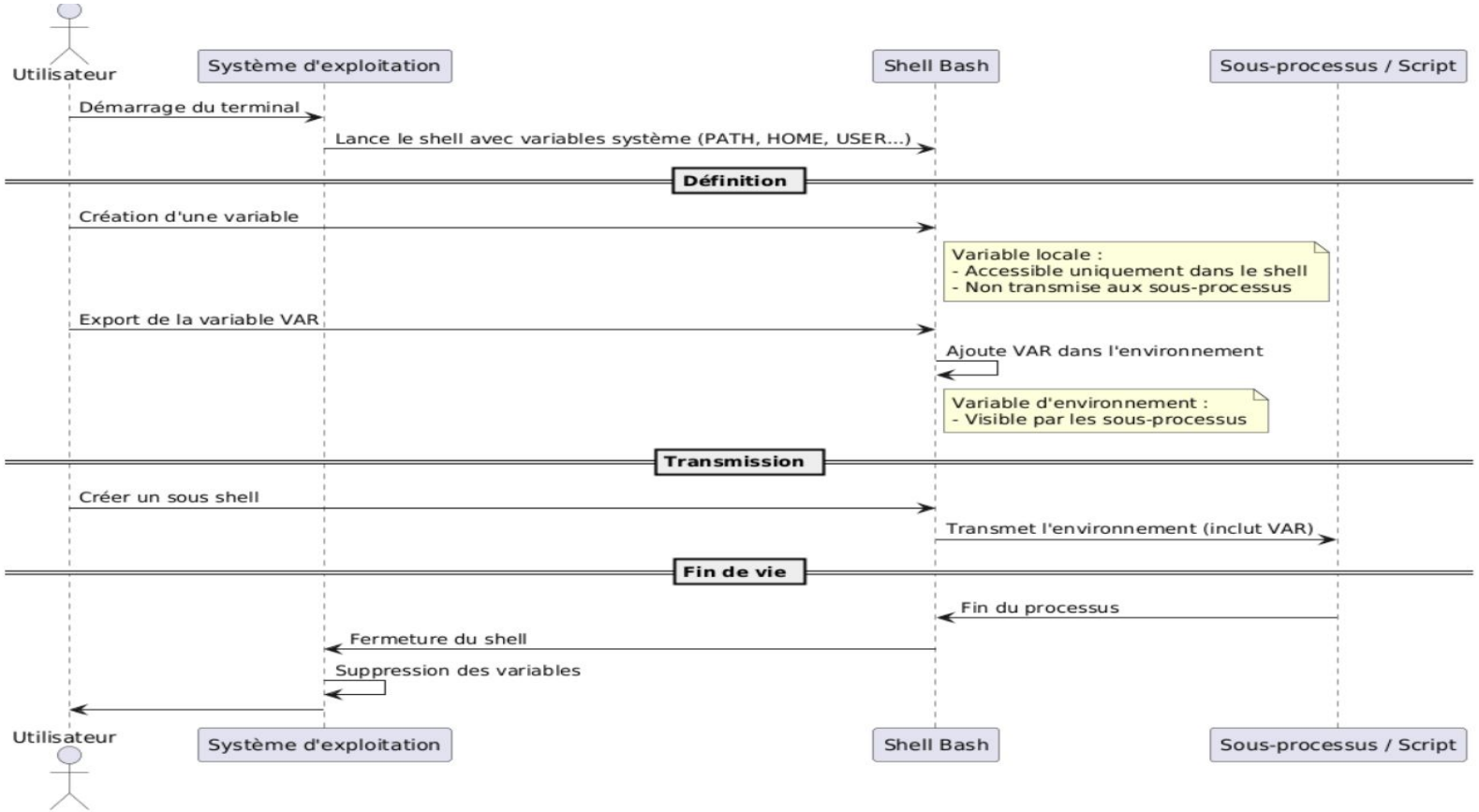


⚠ Bash ⚠

Stéphane Chazelas

CVSS
COMMON VULNERABILITY SCORING SYSTEM

# Fonctionnement des variables d'environnements



# Exemple

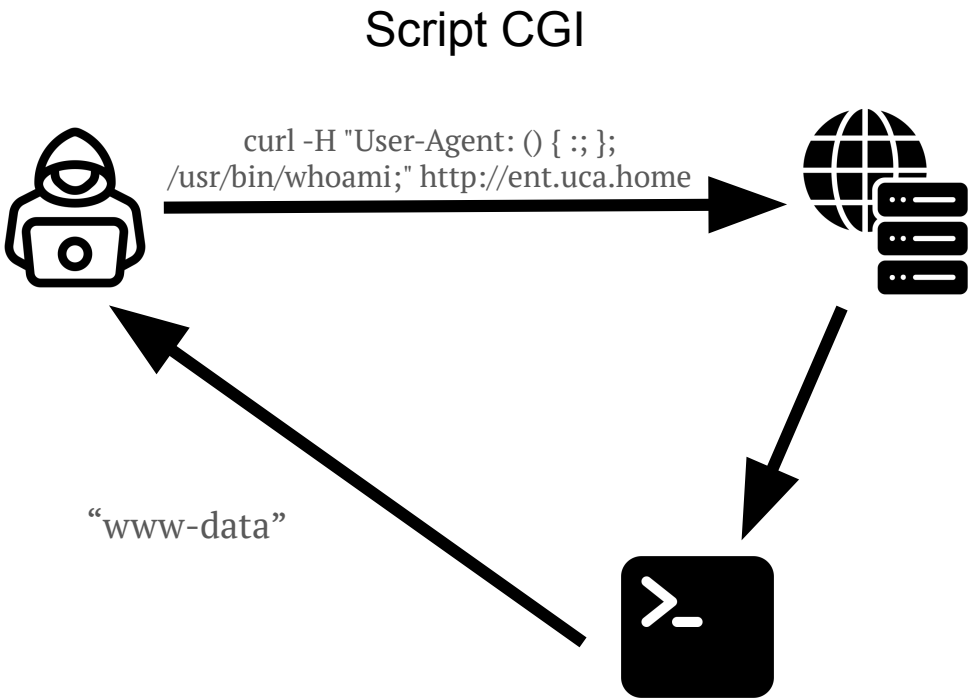
```
$ export X='() { :;}'

$ bash -c "type X"
X is a function
X ()
{
        :
}
```

```
$ export X='() { :;}; echo HACKED'

$ bash -c "type X"
HACKED
X is a function
X ()
{
    :
}
```

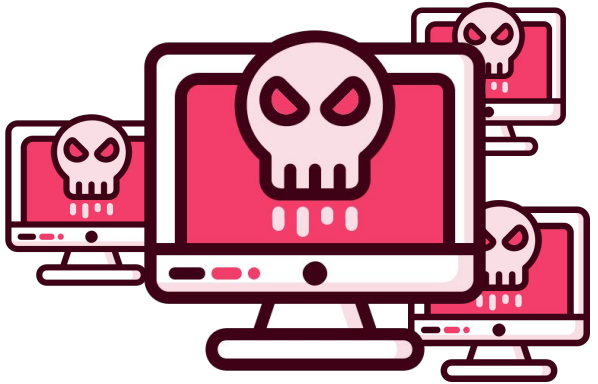
# Exploitations web




Autres exploitations :

- Clients DHCP
- Service SSH

# Exploitations web



500 millions

- Botnet
- DDoS
- Récupération de données

# Correctifs


- mise à jour Bash
- limiter usage Bash

- filtrer les en-têtes HTTP
- désactiver l’export de fonctions

systemd (ClearEnvironment=yes)

- WAF/firewall

# Conclusion

- Problèmes :
  - Parseur :
    - accepte et reconstruit des définitions de fonction
  - Interpréteur :
    - exécute du code après les définitions

- Faille critique :
  - Faut-il continuer à dépendre massivement des mêmes technologies sans en réévaluer régulièrement la sécurité ?