SHELLSHOCK Module 2

SHELLSHOCK EXAMPLE

SUMMERY

| | |
|---|---|
| Matched Branch: | 0 |
| Partially Matched Branch: | 6 |
| Mismatched Branch: | 0 |
| Extra Branch: | 69 |
| Total Match: | 60.0 % |
| Concept Match: | 70.0 % |
| Link. Phr. Match: | 40.0 % |
| Misconception: | 50.0 % |
| Hierarchy Match: | 65.56 % |

Grade: 58.59%

with the example of

related to

curl -i -X HEAD "http://192.168.160.134/cgi-bin/test.sh" -A '() { :;}; echo $(</etc/passwd)'

Common Gateway Interface (CGI) use bash to run executable programs

SHELLSHOCK BUG

with possible result of

illustrated by

SHELLSHOCK ATTACK

Bash executes code after function definition without the function being executed

Security bug in bash or bourne-again shell, which was first disclosed in Sept 2014

Many applications and services use bash shell

depicted by

Allows an attacker to run an arbitrary command on a victim's machine