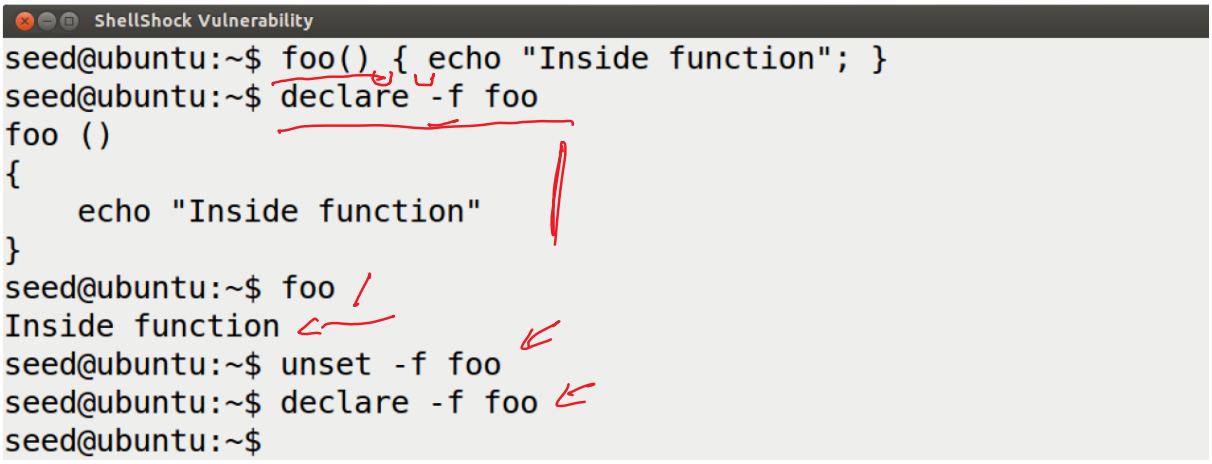
Shellshock Vulnerability

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

Introduction and Overview

- September 24, 2014
- Vulnerability in Bash
- Related to
  - Environment variables
  - CGI and web

Defining Functions in Shell

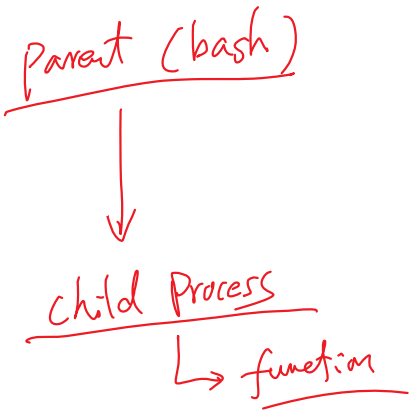


Passing Function to Child Process

❖ Passing function definition explicitly

Shellshock Vulnerability

```
seed@ubuntu:$ foo() { echo "hello world"; }
seed@ubuntu:$ declare -f foo
foo ()
{
    echo "hello world"
}
seed@ubuntu:$ foo
hello world
seed@ubuntu:$ export -f foo
seed@ubuntu:$ bash
seed@ubuntu(child):$ declare -f foo
foo ()
{
    echo "hello world"
}
seed@ubuntu(child):$ foo
hello world
seed@ubuntu(child):$
```



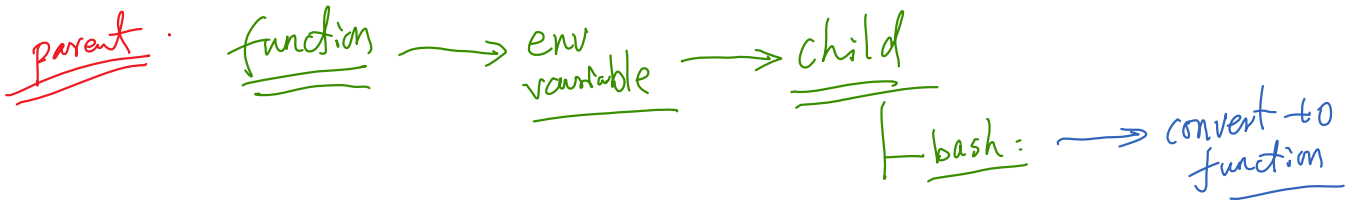
bash: shell variables

❖ Passing function definition via shell variable

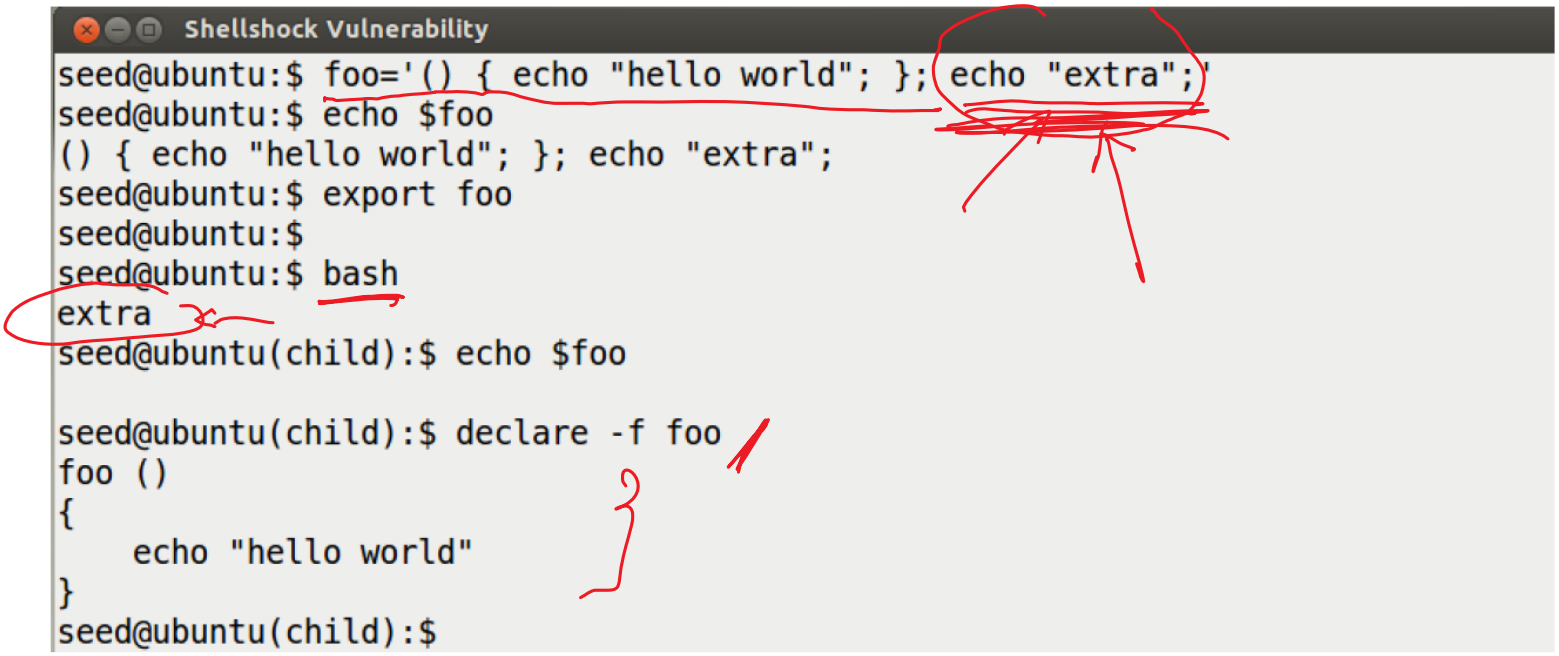
Shellshock Vulnerability

```
seed@ubuntu:$ foo='() { echo "hello world"; }'
seed@ubuntu:$ echo $foo
() { echo "hello world"; }
seed@ubuntu:$ declare -f foo
seed@ubuntu:$ export foo
seed@ubuntu:$ bash
seed@ubuntu(child):$ echo $foo

seed@ubuntu(child):$ declare -f foo
foo ()
{
    echo "hello world"
}
seed@ubuntu(child):$ foo
hello world
seed@ubuntu(child):$
```



Shellshock Vulnerability



Mistake in the Source Code

```
1  void initialize_shell_variables (env, privmode)
2      char **env;
3      int privmode;
4  {
5    [...]
6    for (string_index = 0; string = env[string_index++]; )
7      {
8        [...]
9        /* If exported function, define it now. Don't import functions from
10       the environment in privileged mode. */
11       if (privmode == 0 && read_but_dont_execute == 0 && STREQN ("() {",
             string, 4))
12       {
13         [...]
14         // Shellshock vulnerability is inside:
15         parse_and_execute (temp_string, name, SEVAL_NONINT|SEVAL_NOHIST);
16         [...]
17       }
18 }
```

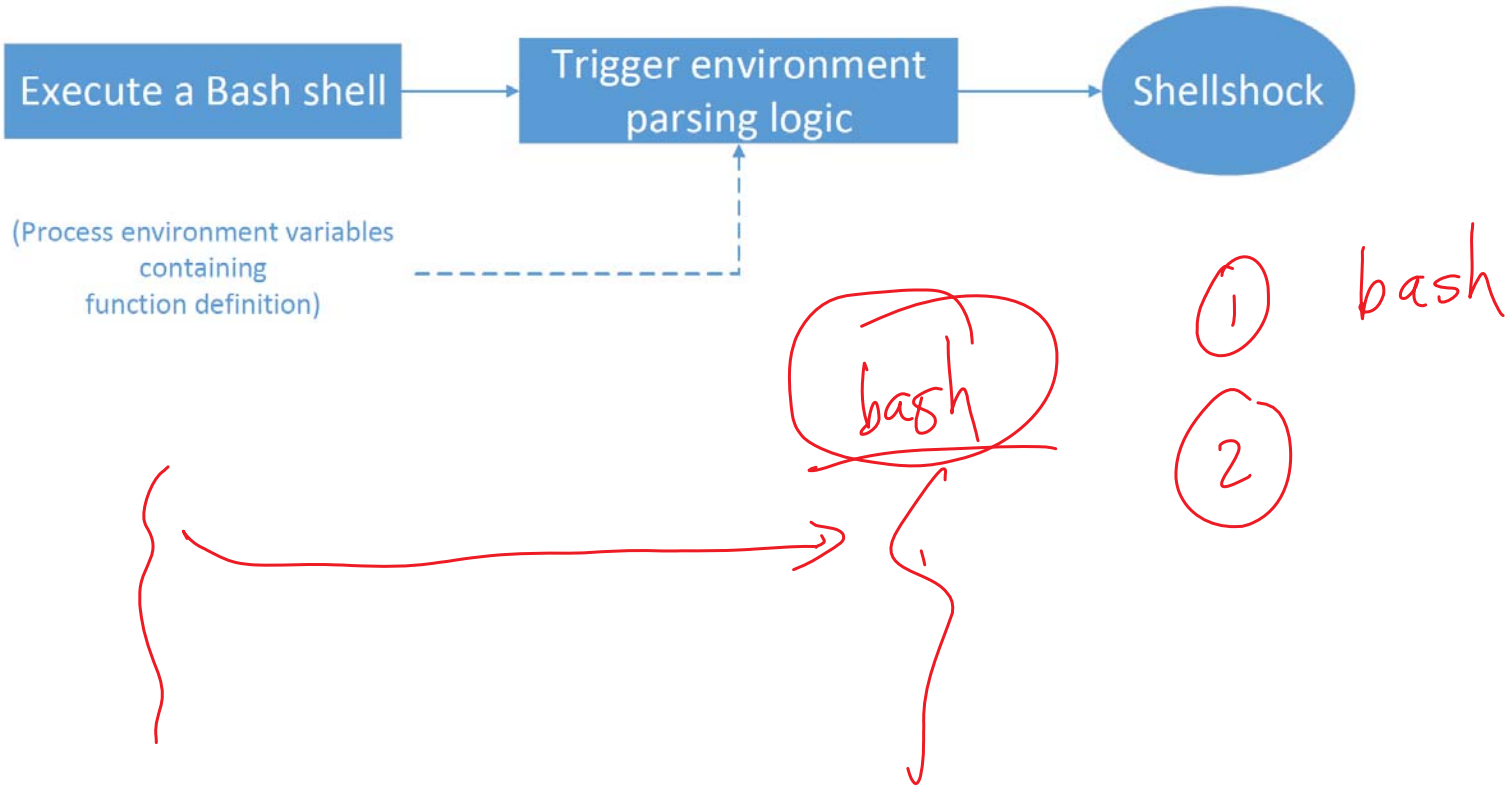
```
Line A: foo() { echo "hello world"; }; echo "extra";
Line B: foo () { echo "hello world"; }; echo "extra";
```

parsed

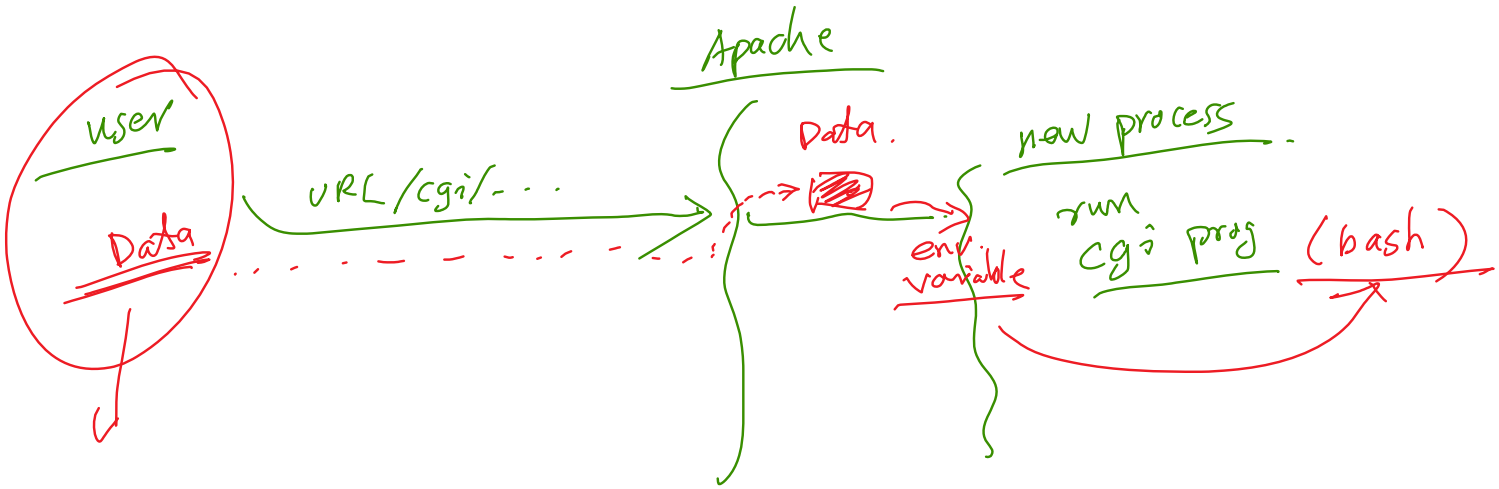
Exploiting Shellshock Vulnerability

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

Exploiting Shellshock Vulnerability



Shellshock Attack on CGI: How CGI Works

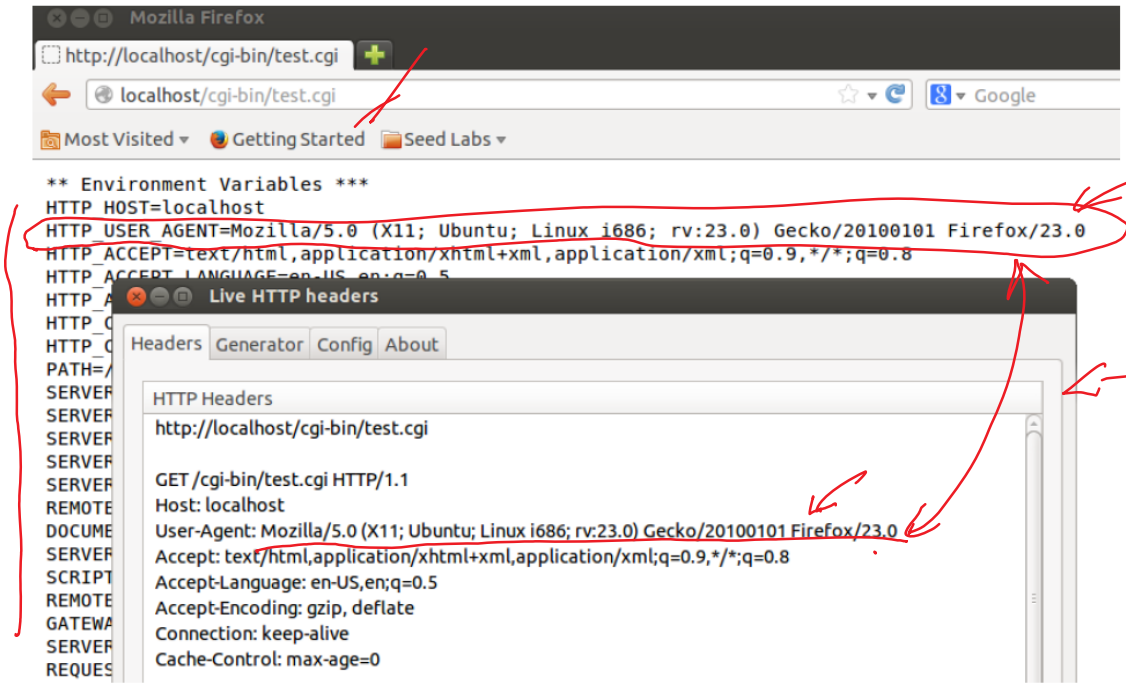


Passing Environment Variables to CGI

❖ The CGI program

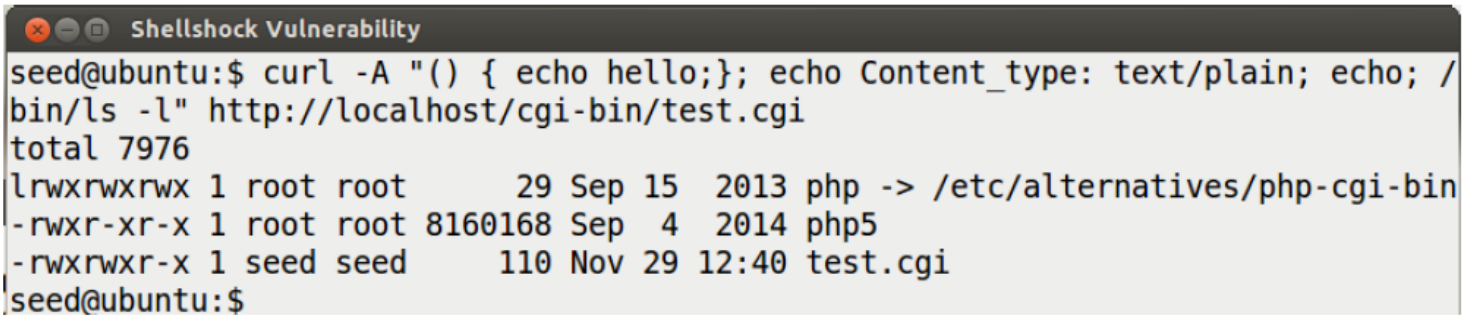
```
echo "Content-type: text/plain"
echo
echo "** Environment Variables *** "
strings /proc/$$/environ
```

❖ From browser



❖ From command line

Run a Command on the Server

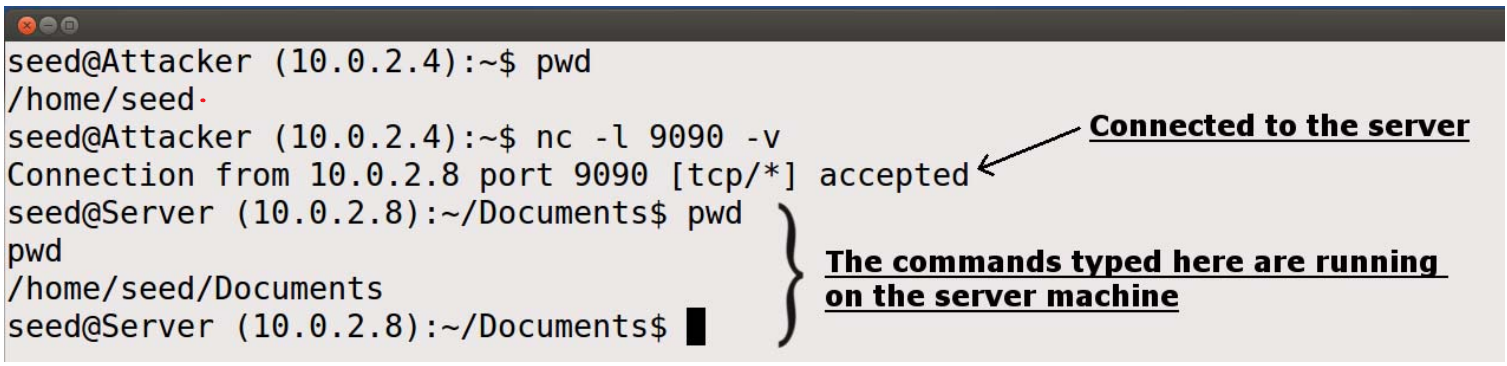


Reverse Shell

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

What Command to Inject: Reverse Shell

Reverse Shell



Summary

- How Shellshock attack works
- Conduct Shellshock attack
- Reverse shell