به نام خدا

دوره تست نفوذ و امنیت وب

مدرس: فرهاد علی‌محمدی

ارائه شده توسط آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران

دانشگاه تهران

آزمایشگاه پژوهشی فضای سایبر

جلسه دوم

برنامه‌های مورد نیاز:

- Vmware workstation
- Metasploitable 2
- Burp Suite

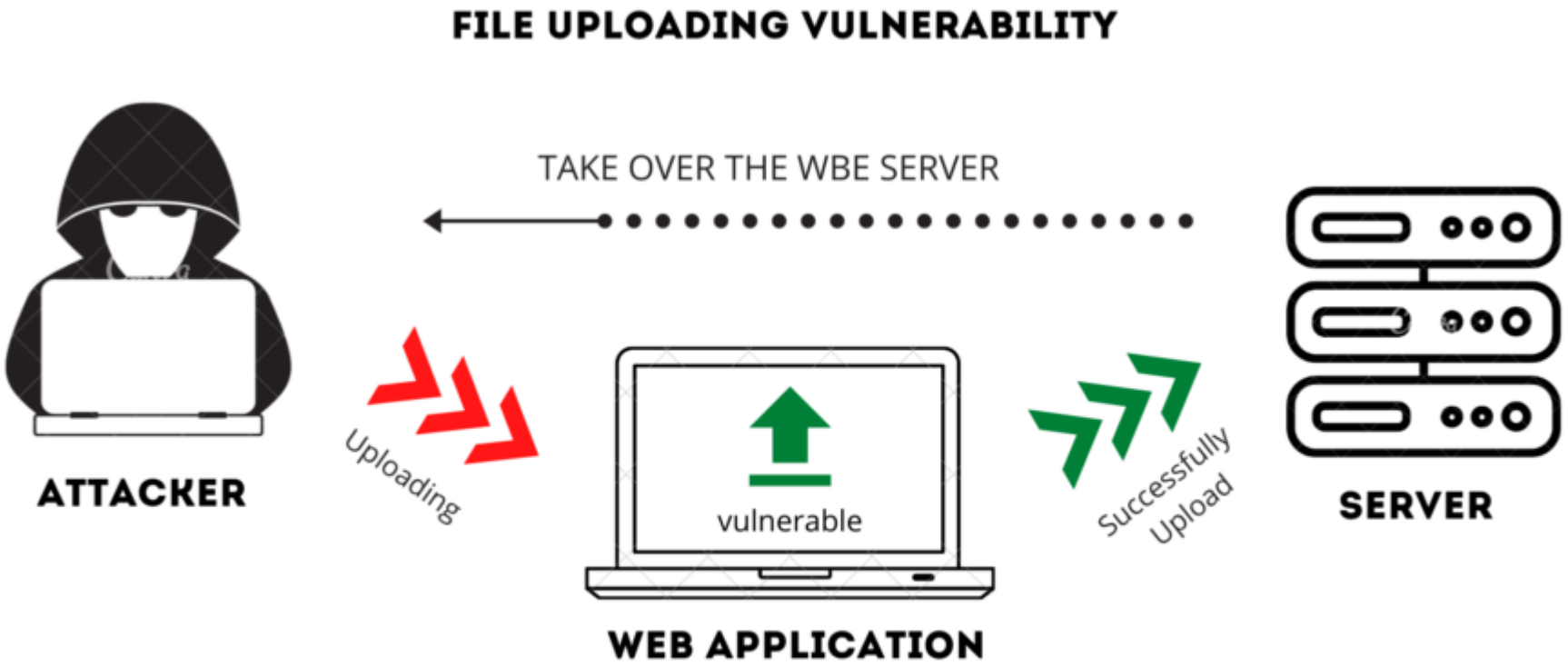
منابع دانلود:

https://soft98.ir/os/virtual-machine/1232-vmware-workstation.html

https://sourceforge.net/projects/metasploitable/files/Metasploitable2/

https://soft98.ir/internet/network/17745-Burp.html

File Upload Vulnerability



File Upload Vulnerability

راه‌های بررسی این باگ:

Content-Type Modification

File Extension Manipulation

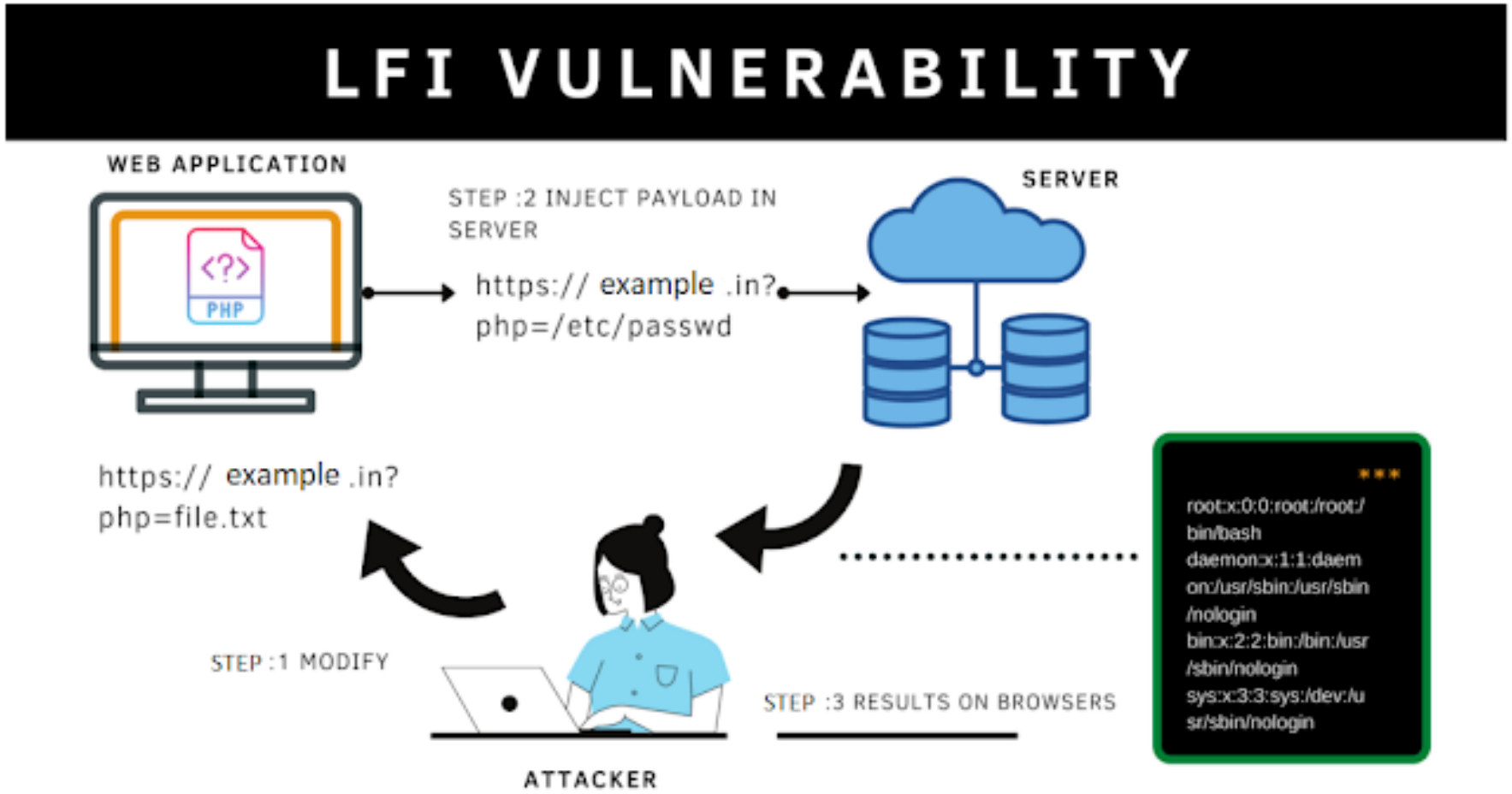
راه‌های جلوگیری از این باگ:

File type verification

Malware prevention

Randomize uploaded file names

LFI Vulnerability



LFI Vulnerability

LFI Payloads:

/etc/issue
/etc/passwd
/etc/shadow
/etc/group
/etc/hosts
/etc/motd
/etc/mysql/my.cnf
/proc/self/environ
/proc/version
/proc/cmdline

LFI to RCE:

/proc/self/environ -> Inject code to headers

LFI Vulnerability

راه‌های بررسی این باگ:

URL parameter checking

راه‌های جلوگیری این باگ:

Set allow_url_include=off

Using selection for pages instead pass the page