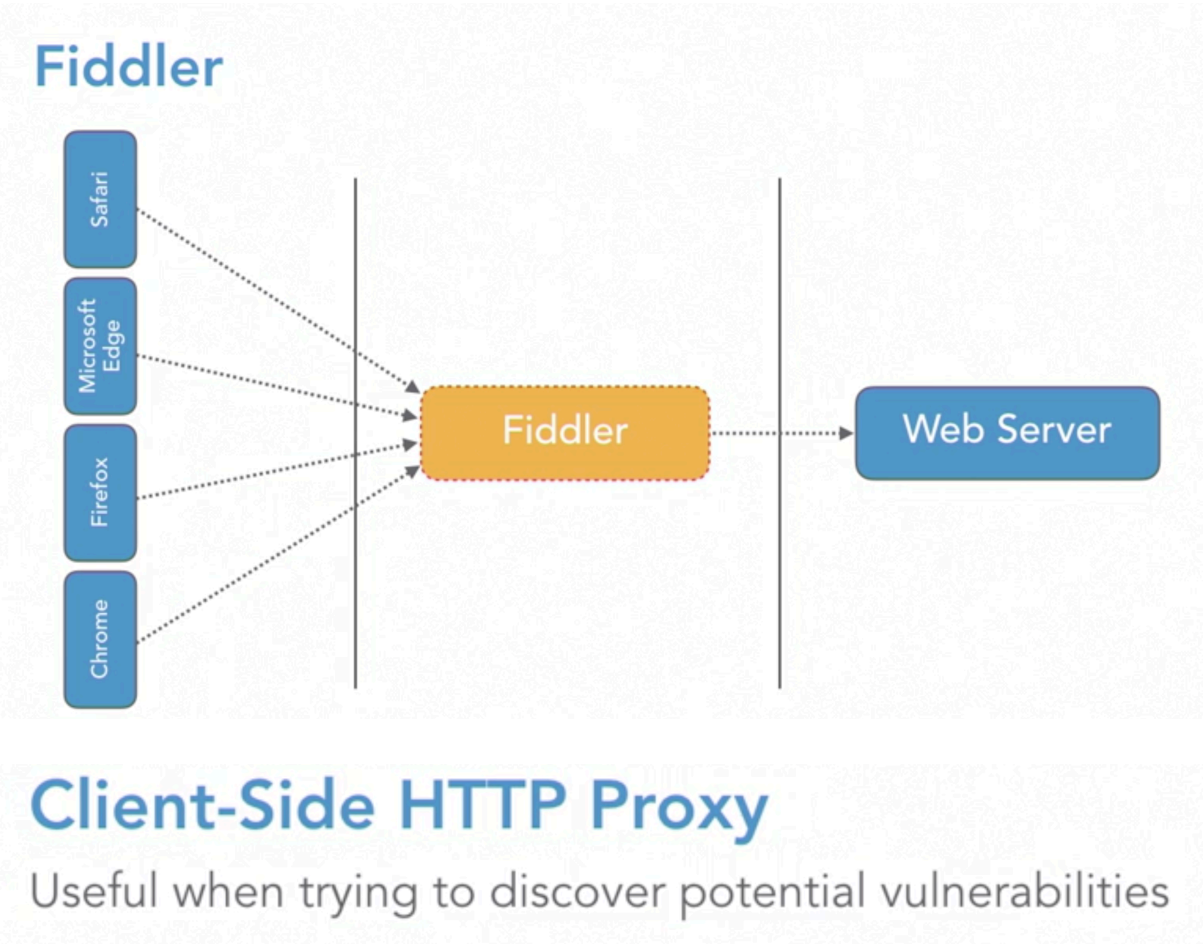
Http proxies

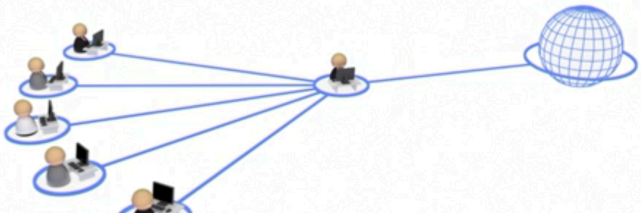
Tool to intercept client side potential vulnerabilities which might result to cybercrime

- Fiddler
- Squid



Server-Side Solutions: HTTP Proxy Server

- Acts more like a server
- Impersonates a web client when facing a target web server

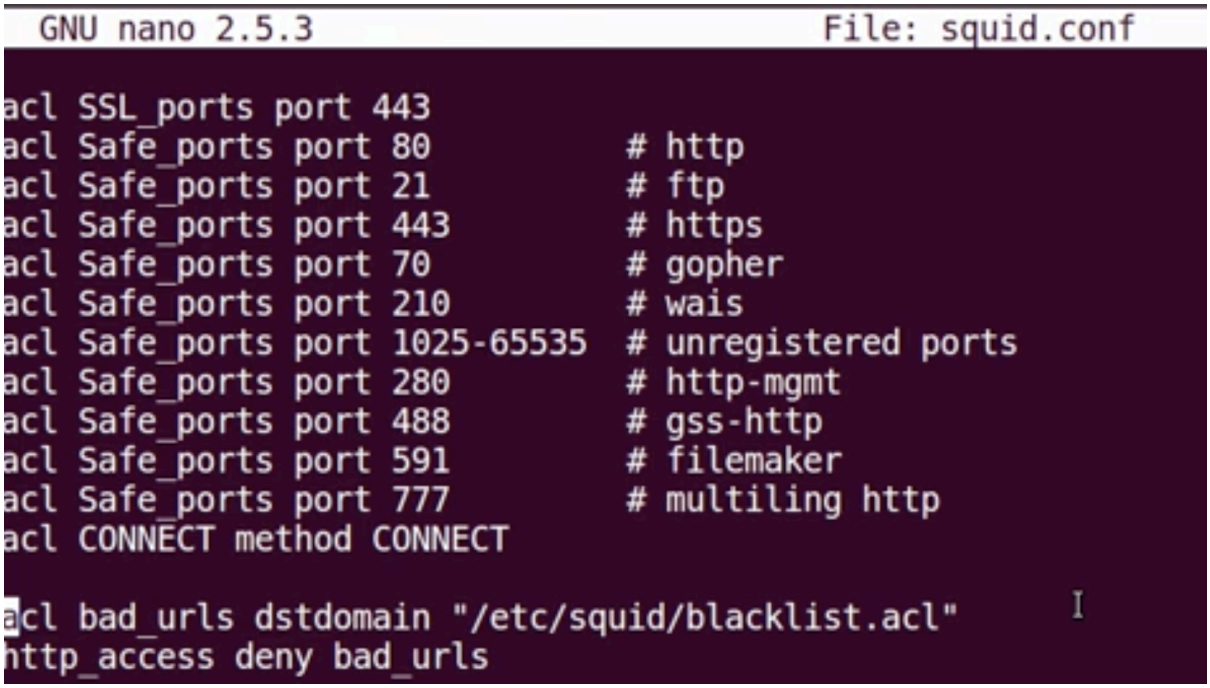


Squid

```
instructor@ubuntud2:~$ sudo service squid status
[sudo] password for instructor:
● squid.service - LSB: Squid HTTP Proxy version 3.x
   Loaded: loaded (/etc/init.d/squid; bad; vendor preset: enabled)
   Active: active (running) since Sat 2019-02-09 12:06:48 PST; 28min ago
     Docs: man:systemd-sysv-generator(8)
  Process: 9123 ExecStop=/etc/init.d/squid stop (code=exited, status=0/SUCC
  Process: 9156 ExecStart=/etc/init.d/squid start (code=exited, status=0/SU
```

- Change config '/etc/squid/squid.conf' for customization
  - 'Http_access allow all'
  - 'acl bad_urls dstdomain "<filename>"' settings

```
instructor@ubuntud2:~$ cd /etc/squid/
instructor@ubuntud2:/etc/squid$ ls
blacklist.acl  errorpage.css  squid.conf
instructor@ubuntud2:/etc/squid$ more blacklist.acl
.linkedin.com
instructor@ubuntud2:/etc/squid$
```


GNU nano 2.5.3 File: squid.conf
acl SSL_ports port 443
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 # https
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT
acl bad_urls dstdomain "/etc/squid/blacklist.acl"
http_access deny bad_urls