

# Web Application Pentesting



Vivek Ramachandran

SWSE, SMFE, SPSE, SISE, SLAE, SGDE Course Instructor

Certifications: <http://www.securitytube-training.com>

Pentester Academy: <http://www.PentesterAcademy.com>

# CSRF Trigger Tags

# CSRF Trigger Tags

- ``
- `<iframe src="XXX" />`
- `<script src="YYY" />`

# XMLHttpRequest based Triggering

- Most handy if XSS is found on the Victim website
- Can still work from the Attackers Website with a favorable CORS Policy
  - CORS to be discussed later in great detail

# Demo

- OWASP WebGoat

[https://github.com/WebGoat/WebGoat/wiki/Installation-\(WebGoat-6.0\)](https://github.com/WebGoat/WebGoat/wiki/Installation-(WebGoat-6.0))

# Pentester Academy

PentesterAcademy

a SecurityTube.net initiative



TOPICS

PRICING

WHY SUBSCRIBE

TESTIMONIALS

MEMBER ACCESS



## Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

**Start Learning Today!**

## Latest Videos

New content added weekly!

### Dumping Passwords from Browser Memory

- Identify strings or data structures around the "secret information"
- Verify multiple times by varying conditions
  - Different versions of the Browser
  - Different OS
  - Different versions of the OS
  - Across Reboots (might not matter too much)
- Create search strings or regex for the pattern you identify
- Welcome to the world on Memory Analysis!
  - Volatility
  - Minikatz etc.

### Memory Dumping and Analysis

- Memory Dumping
  - Per Process
  - Full System
- Why Memory Dumping?
  - Trajectory trace of information!
    - Passwords, Keys, Secrets, etc.
  - No need to run multiple commands!
  - Limit running privileges commands on the system
- Requires Admin Privileges for system wide dumping

### Post/windows/gather/enum\_prefetch

```
root@kali:~# cat /etc/ansible/hosts
[windows]
192.168.1.100:ansible_port=5022
192.168.1.101:ansible_port=5022
192.168.1.102:ansible_port=5022
192.168.1.103:ansible_port=5022
192.168.1.104:ansible_port=5022
192.168.1.105:ansible_port=5022
192.168.1.106:ansible_port=5022
192.168.1.107:ansible_port=5022
192.168.1.108:ansible_port=5022
192.168.1.109:ansible_port=5022
192.168.1.110:ansible_port=5022
192.168.1.111:ansible_port=5022
192.168.1.112:ansible_port=5022
192.168.1.113:ansible_port=5022
192.168.1.114:ansible_port=5022
192.168.1.115:ansible_port=5022
192.168.1.116:ansible_port=5022
192.168.1.117:ansible_port=5022
192.168.1.118:ansible_port=5022
192.168.1.119:ansible_port=5022
192.168.1.120:ansible_port=5022
192.168.1.121:ansible_port=5022
192.168.1.122:ansible_port=5022
192.168.1.123:ansible_port=5022
192.168.1.124:ansible_port=5022
192.168.1.125:ansible_port=5022
192.168.1.126:ansible_port=5022
192.168.1.127:ansible_port=5022
192.168.1.128:ansible_port=5022
192.168.1.129:ansible_port=5022
192.168.1.130:ansible_port=5022
192.168.1.131:ansible_port=5022
192.168.1.132:ansible_port=5022
192.168.1.133:ansible_port=5022
192.168.1.134:ansible_port=5022
192.168.1.135:ansible_port=5022
192.168.1.136:ansible_port=5022
192.168.1.137:ansible_port=5022
192.168.1.138:ansible_port=5022
192.168.1.139:ansible_port=5022
192.168.1.140:ansible_port=5022
192.168.1.141:ansible_port=5022
192.168.1.142:ansible_port=5022
192.168.1.143:ansible_port=5022
192.168.1.144:ansible_port=5022
192.168.1.145:ansible_port=5022
192.168.1.146:ansible_port=5022
192.168.1.147:ansible_port=5022
192.168.1.148:ansible_port=5022
192.168.1.149:ansible_port=5022
192.168.1.150:ansible_port=5022
192.168.1.151:ansible_port=5022
192.168.1.152:ansible_port=5022
192.168.1.153:ansible_port=5022
192.168.1.154:ansible_port=5022
192.168.1.155:ansible_port=5022
192.168.1.156:ansible_port=5022
192.168.1.157:ansible_port=5022
192.168.1.158:ansible_port=5022
192.168.1.159:ansible_port=5022
192.168.1.160:ansible_port=5022
192.168.1.161:ansible_port=5022
192.168.1.162:ansible_port=5022
192.168.1.163:ansible_port=5022
192.168.1.164:ansible_port=5022
192.168.1.165:ansible_port=5022
192.168.1.166:ansible_port=5022
192.168.1.167:ansible_port=5022
192.168.1.168:ansible_port=5022
192.168.1.169:ansible_port=5022
192.168.1.170:ansible_port=5022
192.168.1.171:ansible_port=5022
192.168.1.172:ansible_port=5022
192.168.1.173:ansible_port=5022
192.168.1.174:ansible_port=5022
192.168.1.175:ansible_port=5022
192.168.1.176:ansible_port=5022
192.168.1.177:ansible_port=5022
192.168.1.178:ansible_port=5022
192.168.1.179:ansible_port=5022
192.168.1.180:ansible_port=5022
192.168.1.181:ansible_port=5022
192.168.1.182:ansible_port=5022
192.168.1.183:ansible_port=5022
192.168.1.184:ansible_port=5022
192.168.1.185:ansible_port=5022
192.168.1.186:ansible_port=5022
192.168.1.187:ansible_port=5022
192.168.1.188:ansible_port=5022
192.168.1.189:ansible_port=5022
192.168.1.190:ansible_port=5022
192.168.1.191:ansible_port=5022
192.168.1.192:ansible_port=5022
192.168.1.193:ansible_port=5022
192.168.1.194:ansible_port=5022
192.168.1.195:ansible_port=5022
192.168.1.196:ansible_port=5022
192.168.1.197:ansible_port=5022
192.168.1.198:ansible_port=5022
192.168.1.199:ansible_port=5022
192.168.1.200:ansible_port=5022
```

### Prefetch Settings

```
Configuration:
  The Prefetcher's configuration is stored in the Windows Registry at
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory
  Management\PrefetchParameters. The EnablePrefetcher value can be one of the following:
  * 0 - Disabled
  * 1 - Application prefetching enabled
  * 2 - Boot prefetching enabled (default on Windows 2003 only)
  * 3 - Application and boot prefetching enabled (default)
  The recommended value is 3. If values higher than 3 are not necessary performance, and changing the value to 2 will not
  make Windows boot faster.
  http://en.wikipedia.org/wiki/Prefetcher
```