

# 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>

# Cross Site Request Forgery (CSRF/XSRF)

# CSRF

- Malicious website exploits trust between Browser and a Vulnerable Website the user is authenticated to
- Unauthorized commands are run on behalf of the user on the vulnerable website

# 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

```
msf5 > post/windows/gather/enum_prefetch
msf5 post/windows/gather/enum_prefetch > run
[*] Prefetch gathering started...
[*] Local Machine: 10.10.10.100, Host OS: windows
[*] Local Machine: 10.10.10.100, Host OS: windows and local machine default user: user1, WORKST.
[*] Remote Machine: 10.10.10.101, Host OS: windows
[*] Local OS: 10.10.10.100, Host OS: windows
[*] Local OS: 10.10.10.101, Host OS: windows
[*] Gathering information from remote system. This will take awhile...
[*] Done.

Remote Information
-----
Local Information:
Host: 10.10.10.100, Host OS: windows, Local User: user1, Local OS: windows
Host: 10.10.10.101, Host OS: windows, Local User: user1, Local OS: windows
Host: 10.10.10.101, Host OS: windows, Local User: user1, Local OS: windows
```

### Prefetch Settings

```
Configuration:
-----
The Prefetcher configuration is stored in the Windows Registry at:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurEm\Manager\Memory
Management\PrefetchParameters. The EnablePrefetcher value can be one of the following:
+0 - Disabled
+1 - Application prefetching enabled
+2 - Data prefetching enabled (default on Windows 2003 only)
+3 - Application and Data prefetching enabled (default)
The recommended value is 3. If values higher than 3 is not increase performance, and changing the value to 2 will not
Make Windows boot faster.

http://en.wikipedia.org/wiki/Prefetcher
```