

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>

Mitigating CSRF with Tokens

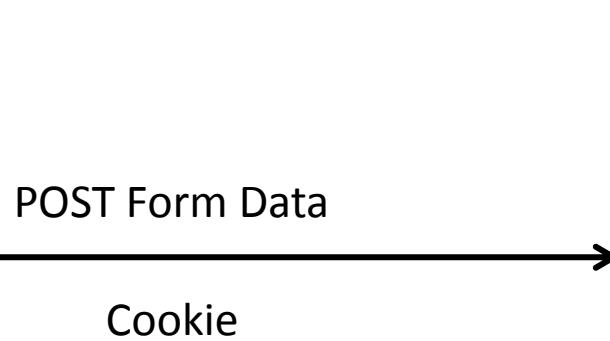
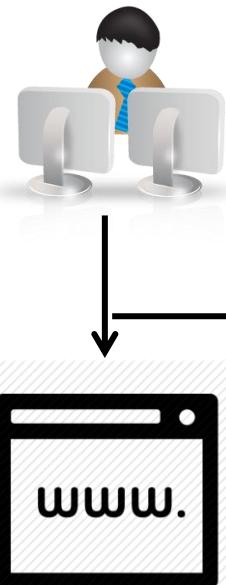
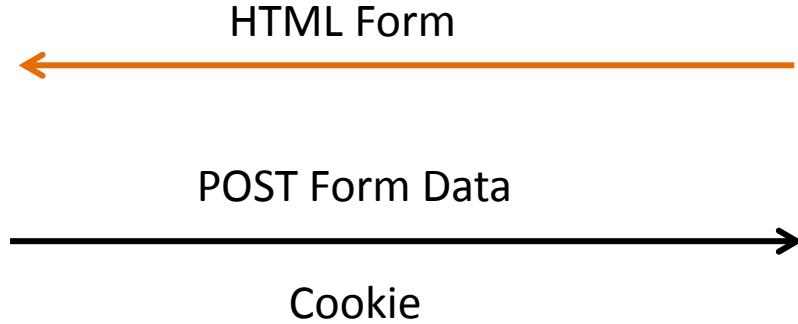
Why does CSRF work?

- What is the problem?
 - Cookie is sent automatically with requests
 - Attacker need not know the value of the cookie
 - No other “session” or “operation” validation
 - How do we know the user is logged in and using the website?

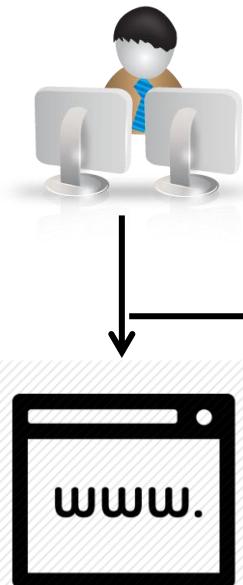
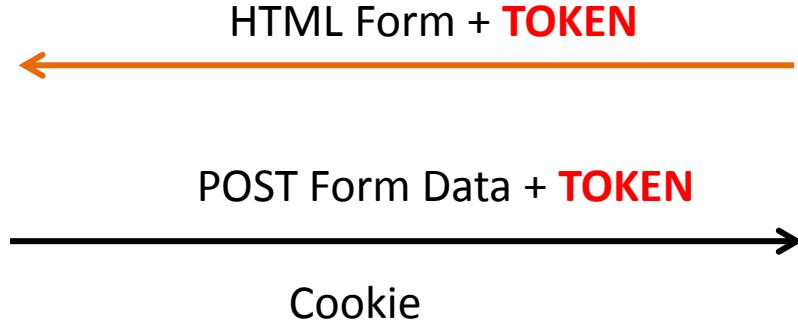
Tokens: Per Session / Request

- Solution to CSRF
 - Identify critical operations in the Application
 - Basically URLs / API endpoints
 - Each critical operation request must be accompanied with a “token”
 - Token is
 - Long, Random, not repeated for application lifetime
 - Unique per session or even per operation
 - Part of URL in GET
 - Hidden Field in POST (forms)
 - Attacker cannot know / predict this token and hence cannot create requests to exploit the operation

User Interaction without Tokens



User Interaction with Tokens



TOKEN Missing! REJECT!



Demo

- OWASP WebGoat

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

What could go wrong? Token Security

- Is the token long enough?
- Is it random enough? Entropy?
 - Should not be derived from known / predictable data
- Never repeated or reused?
- Stored insecurely
 - GET requests in history files, server logs etc.
- Is sent over a secure medium? HTTPS?
 - Sniffing and MITM

OWASP CSRF Guides

- [https://www.owasp.org/index.php/Cross-Site Request Forgery \(CSRF\)](https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF))
- [https://www.owasp.org/index.php/Cross-Site Request Forgery \(CSRF\) Prevention Cheat Sheet](https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet)
- [https://www.owasp.org/index.php/Reviewing code for Cross-Site Request Forgery issues](https://www.owasp.org/index.php/Reviewing_code_for_Cross-Site_Request_Forgery_issues)

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!
 - Volatile
 - Mimikatz etc.

Memory Dumping and Analysis

- Memory Dumping
 - Per Process
 - Full System
- Why Memory Dumping?
 - Treasure trove 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

The Prefetch configuration is stored in the Windows Registry at KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Gestion\Prefetch. The EnablePrefetcher value can set to be one of the following:^[1]

- 0 = Disabled
- 1 = Application prefetching enabled
- 2 = Boot prefetching enabled (default on Windows 2003 only)^[2]
- 3 = Application and Boot prefetching enabled (default)^[3]

The recommended value is 3^[3]. Values higher than 3 do not increase performance, and changing the value to 2 will not make Windows boot faster.^[3]

Prefetch Settings

Configuration

The Prefetch configuration is stored in the Windows Registry at KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Gestion\Prefetch. The EnablePrefetcher value can set to be one of the following:^[1]

- 0 = Disabled
- 1 = Application prefetching enabled
- 2 = Boot prefetching enabled (default on Windows 2003 only)^[2]
- 3 = Application and Boot prefetching enabled (default)^[3]

The recommended value is 3^[3]. Values higher than 3 do not increase performance, and changing the value to 2 will not make Windows boot faster.^[3]

<http://en.wikipedia.org/wiki/Prefetcher>