Blog



TRENDING NOW

INDUSTRY SOLUTIONS
Podcast

THOUGHT LEADERSHIP
Industry Observations

SECURITY RESEARCH
Aviator
Technical Insight
Tools And Applications
True Stories Of The TRC
Unsung Heroes
Vulnerabilities
WhiteHat HackerKast

WHITEHAT SENTINEL
Events
Web Application Security

VULNERABILITIES - WEB APPLICATION SECURITY

Top Ten Web Hacking Techniques of 2012

Jeremiah Grossman | December 06, 2012

Every year the security community produces a stunning amount of new Web hacking techniques that are published in various white papers, blog posts, magazine articles, mailing list emails, conference presentations, etc. Within the thousands of pages are the latest ways to attack websites, Web browsers, Web proxies, and their mobile platform equivilents. Beyond individual vulnerabilities with CVE numbers or system compromises, here we are solely focused on new and creative methods of Web-based attack. Now it its seventh year, The Top Ten Web Hacking Techniques list encourages information sharing, provides a centralized knowledge-base, and recognizes researchers who contribute excellent work. Past Top Tens and the number of new attack techniques discovered in each year: 2006 (65), 2007 (83), 2008 (70), 2009 (82), 2010 (69), 2011 (51)

The Top Ten

1. CRIME (1, 2, 3 4) by *Juliano Rizzo* and *Thai Duong*
2. Pwning via SSRF (memcached, php-fastcgi, etc) (2, 3, 4, 5)
3. Chrome addon hacking (2, 3, 4, 5)
4. Bruteforce of PHPSESSID
5. Blended Threats and JavaScript
6. Cross-Site Port Attacks
7. Permanent backdooring of HTML5 client-side application
8. CAPTCHA Re-Riding Attack
9. XSS: Gaining access to HttpOnly Cookie in 2012
10. Attacking OData: HTTP Verb Tunneling, Navigation Properties for Additional Data Access, System Query Options ($select)

Honorable Mention

11. Using WordPress as a intranet and internet port scanner

12. .Net Cross Site Scripting – Request Validation Bypassing (1)

13. Bruteforcing/Abusing search functions with no-rate checks to collect data

14. Browser Event Hijacking (2, 3)

15. ~~Bypassing Flash's local-with-filesystem Sandbox~~ Process oversight. Due to the original discovery date, January 4th, 2011, the technique should not have been included in this years list. How the winners are selected...

Phase 2: Panel of Security Experts [CLOSED]

Judges: Ryan Barnett, Robert Auger, Robert Hansen **(CEO,** Falling Rock Networks**)** Dinis Cruz, Jeff Williams **(CEO,** Aspect Security**),** Peleus Uhley, Romain Gaucher **(Lead Researcher,** Coverity**),** Giorgio Maone, Chris Wysopal, Troy Hunt, Ivan Ristic **(**Director of Engineering, Qualys**), and** Steve Christey **(MITRE).**

From the result of the open community voting, the final 15 Web Hacking Techniques will be voted upon by panel of security experts. Using the exact same voting process as phase 1, the judges will rank the final twenty based of novelty, impact, and overall pervasiveness. Once tabulation is completed, we'll have the Top Ten Web Hacking Techniques of 2012!

Phase 1: Open community voting for the final 15 [CLOSED]

Each attack technique (listed alphabetically) receives a certain amount of points depending on how highly the entry is ranked in each ballot. For example, an entry in position #1 will be given 15 points, position #2 will get 14 points, position #3 gets 13 points, and so on down to 1 point. At the end all points from all ballots will be tabulated to ascertain the top fifteen overall.

Final 15 List (In no particular order):

- Chrome addon hacking (2, 3, 4, 5)
- Browser Event Hijacking (2, 3)
- Attacking OData: HTTP Verb Tunneling, Navigation Properties for Additional Data Access, System Query Options ($select)
- Cross-Site Port Attacks
- CRIME (2)
- Blended Threats and JavaScript
- Pwning via SSRF (memcached, php-fastcgi, etc) (2, 3)
- Bruteforcing/Abusing search functions with no-rate checks to collect data

- Permanent backdooring of HTML5 client-side application
- .Net Cross Site Scripting – Request Validation Bypassing (1)
- Bruteforce of PHPSESSID
- XSS: Gaining access to HttpOnly Cookie in 2012
- CAPTCHA Re-Riding Attack
- Bypassing Flash's local-with-filesystem Sandbox
- Using WordPress as a intranet and internet port scanner

Prizes

1) The winner of this years top ten will receive an updated Web security book library! If any really good books have been recently published and missing, please let me know. I'll add it! Violent Python, Clickjacking und UI-Redressing,Web Application Defender's Cookbook, Seven Deadliest Web Application Attacks, A Bug Hunter's Diary, The Tangled Web, The Web Application Hacker's Handbook, Web Application Obfuscation, XSS Attacks, Hacking Web Apps. 2) After the open community voting process, two survey respondents will be chosen at random and given a $50 Amazon gift card.

Complete 2012 List

- CSRF token disclosure via iFRAME and CAPTCHA trickery (2)
- Parasitic computing using 'Cloud Browsers' (2)
- Browser Event Hijacking (2, 3)
- Cross-Site Port Attacks
- How I Hacked StackOverflow
- Visitor Tracking Without Cookies (or How To Abuse HTTP 301s)
- The "I Know..." series. What websites know about you
- Hyperlink Spoofing and the Modern Web
- Pwning via SSRF (memcached, php-fastcgi, etc) (2, 3)
- Using the HTML5 Fullscreen API for Phishing Attacks
- Steam Browser Protocol Insecurity
- Content Smuggling
- Using HTTP headers pollution for mobile networks attacks (2)
- CRIME (2)

- Top-Level Universal XSS
- Blended Threats and JavaScript
- Exploiting XSS in Ajax Web Applications
- .Net Cross Site Scripting – Request Validation Bypassing
- Stuffing Javascript into DNS names
- Clickjacking Rootkits for Android (2)
- How Facebook lacked X-Frame-Options and what I did with it
- IE9 Self-XSS Blackbox Protection bypass
- Bruteforce of PHPSESSID
- File System API with HTML5 – Juice for XSS
- How to upload arbitrary file contents cross-domain
- Bypassing HTTP Basic Authenitcation in PHP Applications (** **potential rediscovery of**: HTExploit – Bypassing .htaccess restrictions **)
- XSS: Gaining access to HttpOnly Cookie in 2012
- CSS-Only Clickjacking
- X-Frame-Options (XFO) Detection from Javascript
- Fun with data: URLs
- Browsers Anti-XSS methods in ASP (classic) have been defeated!
- Yes, you can have fun with downloads
- Stiltwalker, exploits weaknesses in the audio version of reCAPTCHA
- CSS :visited may be a bit overrated
- "ASPXErrorPath in URL" Technique in Scanning a .Net Web Application
- Cursorjacking again
- Chrome addon hacking (2, 3, 4, 5)
- Jumping out of Touch Screen Kiosks
- Using POST method to bypass IE-browser protected XSS
- Password extraction from Ajax/DOM/HTML5 routine
- Random Number Security in Python
- Bypassing Flash's local-with-filesystem Sandbox

- RCE through mangled WAR upload into Tomcat App Manager using PUT-in-Gopher-over-XXE (1)
- Using WordPress as a intranet and internet port scanner
- UI Redressing Mayhem: Firefox 0-Day And The LeakedIn Affair
- UI Redressing Mayhem: HTTPOnly Bypass PayPwn Style
- NTLM Relay via HTTP to internet or stealing windows user hashes while using java client
- Bypassing CAPTCHAs by Impersonating CAPTCHA Providers (1,2)
- CAPTCHA Re-Riding Attack
- Attacking CAPTCHAs for Fun and Profit
- Permanent backdooring of HTML5 client-side application [Apture example]
- Cracking Ruby on Rails Sessions
- Bruteforcing/Abusing search functions with no-rate checks to collect data
- Cross Context Scripting from within the Browser (1)
- Attacking OData: HTTP Verb Tunneling, Navigation Properties for Additional Data Access, System Query Options ($select)
- Same Origin Spoofing to Attack Client Certificate Sessions



Related Articles

INDUSTRY OBSERVATIONS - TECHNICAL INSIGHT

Top 10 Website Hacking Techniques of 2014

Matt Johansen | March 19, 2015

Most Recent Articles

INDUSTRY OBSERVATIONS

TECHNICAL INSIGHT - TOOLS AND APPLICATIONS - VULNERABILITIES - WEB APPLICATION SECURITY

Top 10 Web Hacking Techniques of 2015

Kuskos | January 12, 2016

PRESS RELEASES

WhiteHat Security Announces the Tenth Annual Top 10 Web Hacking Techniques for 2015

WhiteHat Security | April 20, 2016

The New York Cyber Security Regulation: An Application Security Perspective

Jeannie Warner | August 28, 2017

BREAKING NEWS - EVENTS

"Alexa, Who is WhiteHat Security?" Voice Search Now Available!

Avi B | August 22, 2017

BREAKING NEWS - INDUSTRY OBSERVATIONS - TOOLS AND APPLICATIONS

The Total Cost of Ownership of an Application Security Solution

Ruchika Mishra | August 14, 2017

October is National Cyber Security Awareness Month

October is National Cyber Security Awareness Month. NCSAM is designed to engage, educate, and raise awareness about cyber security.

As the Citizen Development Movement Grows, So Does Security Risk

Largely driven by the ready availability of low-code tools, the need for agility, and the ever-present shortage of IT resources, citizen developers are helping enterprises develop apps more quickly, a...

Complying with PCI DSS 3.1 Guidelines

If your business deals with credit cards, mobile and online payments, learn more about complying with PCI DSS guidelines.

General Data Protection Regulation

The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU).

Static Application Security Testing: Challenges and Benefits

Static application security testing allows you to build security into the software development lifecycle. Read this article to learn about its challenges and benefits.

The 4 Fundamental Cyber Security Strategies Every Financial Services Company Needs to Use

Cyber security in the financial services organizations to secure their business across current and emerging threat vectors.

https://web.archive.org/web/20170903113359/https://www.whitehatsec.com/blog/top-ten-web-hacking-techniques-of-2012/

WhiteHat Security © 2017

The front line of application security.

Terms & Conditions | Safe Harbor Privacy Policy

WEBSITE SECURITY BY WhiteHat SECURITY.