Resources

- Whitepapers
- Webinars & Presentations
- Jeremiah Grossman Blog
- Statistics Report
- Website Security Glossary
- Sentinel Videos

WEBSITE SECURITY TOPICS :: JEREMIAH GROSSMAN BLOG

TOP TEN WEB HACKING TECHNIQUES OF 2011 FEBRUARY 21, 2012

Every year the Web security community produces a stunning amount of new hacking techniques published in various white papers, blog posts, magazine articles, mailing list emails, etc. Within the thousands of pages are the latest ways to attack websites, Web browsers, Web proxies, and so on. Beyond individual vulnerability instances with CVE numbers or system compromises, we're talking about actual new and creative methods of Web-based attack. The Top Ten Web Hacking Techniques list encourages information sharing, provides a centralized knowledge-base, and recognizes researchers who contribute excellent work.

The Top Ten

1. BEAST (by: Thai Duong and Juliano Rizzo)
2. Multiple vulnerabilities in Apache Struts2 and property oriented programming with Java (by: Johannes Dahse)
3. DNS poisoning via Port Exhaustion (by: Roee Hay and Yair Amit)
4. DOMinator – Finding DOMXSS with dynamic taint propagation (by: Stefano Di Paola)
5. Abusing Flash-Proxies for client-side cross-domain HTTP requests (by: Martin Johns and Sebastian Lekies)
6. Expression Language Injection (by: Stefano Di Paola and Arshan Dabirsiaghi)
7. Java Applet Same-Origin Policy Bypass via HTTP Redirect (by: Neal Poole)
8. CAPTCHA Hax With TesserCap (by: Gursev Kalra)
9. Bypassing Chrome's Anti-XSS filter (by: Nick Nikiforakis)
10. CSRF: Flash + 307 redirect = Game Over (by: Phillip Purviance)

How the winners were selected...

Phase 1: Open community voting (Ballot) [COMPLETE]

From of the field of 51 total entries received listed below, each voter (open to everyone) ranks their fifteen favorite Web Hacking Techniques using a survey. Each entry (listed alphabetically) get a certain amount of points depending on how highly they are individually ranked in each ballot. For example, an each entry in position #1 will be given 15 points, position #2 will get 14 point, 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. And NO selecting the same attack multiple times! (they'll be deleted).

Voting will close at the end of the day this Monday, February 20.

[CLOSED] The more people who vote, the better the results! Vote Now!

Phase 2: Panel of Security Experts [COMPLETE]

From the result of the open community voting, the top fifteen Web Hacking Techniques will be voted upon by panel of security experts (to be announced soon). Using the exact same voting process as phase 1, the judges will rank the final fifteen based of novelty, impact, and

overall pervasiveness. Once tabulation is completed, we'll have the Top Ten Web Hacking Techniques of 2011!

Voting will close at the end of the day on Sunday, February 26.

Soon after the winners will be announced!

Good luck everyone.

The Final 15:

Hundreds of votes were cast during the open vote — a great turn out. Thank you everyone for taking the time! 44% of the respondents were self-described "Breakers," follow by 22% "Defenders," 16% "Builders," and 17% did not specify. There was a very smooth distribution of points totals across the range of entries. Clearly everyone had their favorites. Of course we saw a lot of ballot stuffing action, which required a substantive amount of clean-up, but when ranking a Web hacking techniques' its kind of what you expect This is exactly why we have a final 15 process first, so the top ten outcome isn't negatively affected. Any entries that obviously don't belong in the top ten are easily eliminated during the "Panel of Security Experts" phase. Now it's the judges turn to have their say!

1. Abusing Flash-Proxies for client-side cross-domain HTTP requests
2. Abusing HTTP Status Codes to Expose Private Information
3. Autocomplete..again?!
4. BEAST
5. Bypassing Chrome's Anti-XSS filter
6. CAPTCHA Hax With TesserCap
7. Cookiejacking
8. CSRF: Flash + 307 redirect = Game Over
9. DNS poisoning via Port Exhaustion
10. DOMinator – Finding DOMXSS with dynamic taint propagation
11. Expression Language Injection
12. Java Applet Same-Origin Policy Bypass via HTTP Redirect
13. JSON-based XSS exploitation
14. Multiple vulnerabilities in Apache Struts2 and property oriented programming with Java
15. Session Puzzling (aka Session Variable Overloading)

The Big List:

1. Abusing Flash-Proxies for client-side cross-domain HTTP requests [slides]
2. Abusing HTTP Status Codes to Expose Private Information
3. Autocomplete..again?!
4. BEAST
5. Bypassing Chrome's Anti-XSS filter
6. Bypassing Flash's local-with-filesystem Sandbox
7. CAPTCHA Hax With TesserCap
8. CSRF with JSON – leveraging XHR and CORS
9. CSRF: Flash + 307 redirect = Game Over
10. Close encounters of the third kind (client-side JavaScript vulnerabilities)
11. Cookiejacking
12. Cross domain content extraction with fake captcha
13. Crowd-sourcing mischief on Google Maps leads customers astray
14. DNS poisoning via Port Exhaustion
15. DOMinator – Finding DOMXSS with dynamic taint propagation
16. Double eval() for DOM based XSS
17. Drag and Drop XSS in Firefox by HTML5 (Cross Domain in frames)
18. Excel formula injection in Google Docs
19. Exploitation of "Self-Only" Cross-Site Scripting in Google Code
20. Exploiting the unexploitable XSS with clickjacking
21. Expression Language Injection
22. Facebook: Memorializing a User
23. Filejacking: How to make a file server from your browser (with HTML5 of course)

24. Google Chrome/ChromeOS sandbox side step via owning extensions
25. HOW TO: Spy on the Webcams of Your Website Visitors
26. Hidden XSS Attacking the Desktop & Mobile Platforms
27. How To Own Every User On A Social Networking Site
28. How to get SQL query contents from SQL injection flaw
29. How to upload arbitrary file contents cross-domain (2)
30. JSON-based XSS exploitation
31. Java Applet Same-Origin Policy Bypass via HTTP Redirect
32. Kindle Touch (5.0) Jailbreak/Root and SSH
33. Launch any file path from web page
34. Lotus Notes Formula Injection
35. Multiple vulnerabilities in Apache Struts2 and property oriented programming with Java
36. NULLs in entities in Firefox
37. Rapid history extraction through non-destructive cache timing (v8)
38. Session Puzzling (aka Session Variable Overloading) Video 1, 2, 3, 4
39. SpyTunes: Find out what iTunes music someone else has
40. Stealth Cookie Stealing (new XSS technique)
41. Stripping Referrer for fun and profit
42. SurveyMonkey: IP Spoofing
43. Temporal Session Race Conditions Video 2
44. Text-based CAPTCHA Strengths and Weaknesses
45. The Failure of Noise-Based Non-Continuous Audio Captchas
46. Timing Attacks on CSS Shaders
47. Tracking users that block cookies with a HTTP redirect
48. Using Cross-domain images in WebGL and Chrome 13
49. XSS in Skype for iOS
50. XSS-Track as a HTML5 WebSockets traffic sniffer
51. HashDOS: Effective Denial of Service attacks against web application platforms



2014 © Copyright I WhiteHat Security