«From XSS to Ring 0»
Felix Gröbert <groebert@google.com>
12. November 2010
Handout zum eingeladenen Vortrag zum Hackerpraktikum an der Ruhr-Universität Bochum

Google Infografik
http://goo.gl/m7hln

Google Online Security Blog (Vulnerability Reward Program)
http://googleonlinesecurity.blogspot.com/

Google Web-Security Hands-on
http://google-gruyere.appspot.com/

zzuf Multi-Purpose Fuzzer Hands-on
http://caca.zoy.org/wiki/zzuf

CSS-based cross-origin theft and IE8 forced tweeting by Chris Evans
http://websec.sv.cmu.edu/css/css.pdf
http://scarybeastsecurity.blogspot.com/2010/09/ie8-css-based-forced-tweeting.html

Twitter's onMouseOver worm 2010-09-21
https://github.com/mzsanford/twitter-text-rb/commit/cffce8e60b7557e9945fc0e8b4383e5a66b1558f?tag=mncol;txt
http://news.ycombinator.com/item?id=1712275
http://stackoverflow.com/questions/3762746/todays-xss-onmouseover-exploit-on-twitter-com

IE8 XSS Protection Vulnerabilities
https://media.blackhat.com/bh-eu-10/presentations/Lindsay_Nava/BlackHat-EU-2010-Lindsay-Nava-IE8-XSS-Filters-slides.pdf
http://p42.us/ie8xss/Abusing_IE8s_XSS_Filters.pdf
http://www.collinjackson.com/research/xssauditor.pdf

Cross-site script inclusion (XSSI)
http://en.wikipedia.org/wiki/JSON#Cross-site_request_forgery

Mixed content
http://blogs.msdn.com/b/askie/archive/2009/05/14/mixed-content-and-internet-explorer-8-0.aspx
http://www.adambarth.com/papers/2009/barth-caballero-song.pdf

Typo3 shortMD5() Vulnerability by Gregor Kopf from Recurity Labs
http://typo3.org/teams/security/security-bulletins/typo3-sa-2010-020/

Joomla genRandomPassword() CRC32 Vulnerability by Gregor Kopf from Recurity Labs
http://goo.gl/NN9SE

Tavis Ormandy's «GNU C library dynamic linker expands $ORIGIN in setuid library search path» CVE-2010-3847
http://seclists.org/fulldisclosure/2010/Oct/257