Referenzen Bug Bounty Programme/ Schwachstellensuche in (Web)-Anwendungen

Security Advisories 2015

* Bug Bounty - login.microsoftonline.com - Cross-site Scripting vulnerability
* Bug Bounty – blogs.yandex.ru – Mixed Content
* Bug Bounty – events.yandex.ru – Mixed Content
* Bug Bounty – tech.yandex.ru – Mixed Content*
* Bug Bounty – browser.yandex.ru – Cross-site Scripting vulnerability
* Bug Bounty – statyandex.ru – Cross-site Scripting vulnerability

Security Advisories 2014

* Bug Bounty - regiobank.nl - Cross-site Scripting vulnerability
* Bug Bounty - forums.att.com - Cross-site Scripting vulnerability
* Bug Bounty - ecommerce.wireless.att.com - Cross-site Scripting vulnerability
* Bug Bounty - celebrity.yahoo.com - Cross-site Scripting vulnerability
* Bug Bounty - movies.yahoo.com - Cross-site Scripting vulnerability
* Bug Bounty - music.yahoo.com - Cross-site Scripting vulnerability
* Bug Bounty - ebs13.telekom.de - Cross-site Scripting vulnerability

Security Advisories 2013

===== Cross-Site Scripting (XSS) =====

* SSCHADV2013-001 - Websitebaker Add-on 'Concert Calendar 2.1.4' XSS & SQLi vulnerability
* SSCHADV2013-002 - heise.de - Cross-site Scripting vulnerability
* SSCHADV2013-004 - WordPress Plugin 'Feedweb 1.8.8' Cross-site Scripting vulnerability
* SSCHADV2013-005 - WordPress Plugin 'Types 1.2.1.1' CSRF & Stored Cross-site scripting vulnerability
* SSCHADV2013-006 - WordPress Plugin 'AJAX Comment Page 3.25' Cross-site scripting vulnerability
* SSCHADV2013-007 - Ligatus Advertising - DOM Based Cross-site Scripting vulnerability
* SSCHADV2013-008 - www.netcraft.com - Search Form Cross-site Scripting vulnerability
* SSCHADV2013-009 - store.apple.com - DOM based Cross-site Scripting vulnerability
* SSCHADV2013-010 - developer.mozilla.org - DOM based Cross-site Scripting vulnerability
* SSCHADV2013-011 - pages.ebay.de - DOM based Cross-site Scripting vulnerability

===== Open Redirection =====

* SSCHADV2013-003 - Omniture web analytics (Adobe) - Open Redirection vulnerability

Security Advisories 2012

===== Cross-Site Scripting (XSS) =====

* SSCHADV2012-001 - BoltWire 3.4.16 Multiple XSS vulnerabilities
* SSCHADV2012-002 - ATutor 2.0.3 Multiple XSS vulnerabilities
* SSCHADV2012-003 - WebsiteBaker 2.8.2 SP2 HTTP-Referer XSS vulnerability
* SSCHADV2012-004 - ContentLion Alpha 1.3 XSS vulnerability
* SSCHADV2012-006 - WikyBlog 1.7.3RC2 XSS vulnerability
* SSCHADV2012-008 - CMSimple_XH 1.5.2 Cross-site Scripting vulnerability
* SSCHADV2012-010 - WordPress plugin 'WordPress Integrator 1.32' XSS vulnerability
* SSCHADV2012-012 - Baby Gekko v1.2.0 Multiple XSS vulnerabilities
* SSCHADV2012-014 - Joomla 2.5.6 Multiple Cross-site scripting vulnerabilities
* SSCHADV2012-015 - WordPress Plugin 'Count Per Day' 3.1.1 Multiple Cross-site scripting vulnerabilities
* SSCHADV2012-016 - WordPress Plugin 'Quick Post Widget' 1.9.1 Multiple Cross-site scripting vulnerabilities
* SSCHADV2012-018 - SaltOS 3.1 Cross-Site Scripting vulnerability
* SSCHADV2012-020 - PHPExcel 1.7.7 Cross-Site Scripting vulnerability
* SSCHADV2012-021 - Zen cart v1.5.0 & v1.51 Cross-Site Scripting vulnerability
* SSCHADV2012-022 - Piwigo 2.4.3 Cross-Site Scripting vulnerability
* SSCHADV2012-023 - Hero Framework 3.76 Multiple Cross-site Scripting vulnerabilities

* SSCHADV2012-024 - www.elitepartner.de - Cross-site Scripting vulnerability
* SSCHADV2012-027 - www.datingcafe.de - Cross-site Scripting vulnerability

===== DoS =====

* SSCHADV2012-011 - KnFTPd 1.0.0 'FEAT' DoS vulnerability

===== Multiple security vulnerabilities =====

* SSCHADV2012-005 - Wikidforum 2.10 Multiple security vulnerabilities
* SSCHADV2012-007 - PHP Address Book 6.2.12 Multiple security vulnerabilities
* SSCHADV2012-009 - Star Wars Old Republic - SWTOR Char DB 1.8b Multiple security vulnerabilities
* SSCHADV2012-013 - PHP Address Book 7.0.0 Multiple security vulnerabilities
* SSCHADV2012-017 - MGB OpenSource Guestbook 0.6.9.1 Multiple security vulnerabilities
* SSCHADV2012-019 - Admidio 2.3.5 Multiple security vulnerabilities
* KORAMIS-ADV2012-001 - Serendipity 1.6 Backend Cross-Site Scripting and SQL-Injection vulnerability
* KORAMIS-ADV2012-002 - Alienvault OSSIM Open Source SIEM 3.1 Multiple security vulnerabilities
* SSCHADV2012-099 - t-online.de eMail Center - Cross-Site Request Forgery & Cross-site Scripting vulnerability

Security Advisories 2011

===== Cross-Site Scripting (XSS) =====

* SSCHADV2011-001 - Cross-Site Scripting vulnerabilities in Icinga
* SSCHADV2011-002 - Cross-Site Scripting vulnerability in Nagios - [CVE-2011-1523]
* SSCHADV2011-003 - Cross-Site Scripting vulnerability in Icinga
* SSCHADV2011-004 - Cross-Site Scripting vulnerability in Serendipity Plugin "serendipity_event_freetag"
* SSCHADV2011-005 - Cross-Site Scripting vulnerability in Icinga
* SSCHADV2011-006 - Cross-Site Scripting vulnerability in Nagios
* SSCHADV2011-007 - Multiple Cross-Site Scripting vulnerabilities in BLOGCMS
* SSCHADV2011-008 - Multiple Cross-Site Scripting vulnerabilities in WebCalendar
* SSCHADV2011-009 - Multiple XSS vulnerabilities on www.netto-travel.de
* SSCHADV2011-011 - XSS vulnerability in FortiMail Messaging Security Appliance
* SSCHADV2011-013 - Multiple XSS vulnerabilities in LightNEasy
* SSCHADV2011-014 - Multiple XSS vulnerabilities in Papoo Light Version
* SSCHADV2011-015 - Serendipity 'serendipity[filter][bp.ALT]' XSS vulnerability - [CVE-2011-4090]
* SSCHADV2011-016 - Serendipity freetag plugin 'serendipity[tagview]' Cross-Site Scripting vulnerability
* SSCHADV2011-017 - Serendipity Plugin 'Karma Ranking' Multiple XSS vulnerabilities - [CVE-2011-4090]
* SSCHADV2011-020 - Active CMS 1.2.0 'mod' Cross-site Scripting Vulnerability
* SSCHADV2011-021 - Bitweaver 2.8.1 Multiple Cross-site Scripting Vulnerabilities
* SSCHADV2011-022 - phpFK 7.2.5 Multiple Cross-site Scripting Vulnerabilities
* SSCHADV2011-023 - Phorum 5.2.18 Cross-site scripting vulnerability
* SSCHADV2011-024 - SilverStripe 2.4.5 Multiple backend Cross-site scripting vulnerabilities
* SSCHADV2011-025 - Contao 2.10.1 Cross-site scripting vulnerability
* SSCHADV2011-028 - FreeSMS (Free Student Management System) Multiple Cross-site Scripting Vulnerabilities
* SSCHADV2011-029 - PHP Booking Calendar Multiple Cross-Site Scripting Vulnerabilities
* SSCHADV2011-033 - Metasploit 4.1.0 Web UI "project[name]" XSS vulnerability
* SSCHADV2011-035 - PHP-SCMS 1.6.8 "lang" parameter XSS vulnerability
* SSCHADV2011-037 - Achievo 1.4.5 Multiple XSS vulnerabilities
* SSCHADV2011-038 - Ariadne 2.7.6 Multiple XSS vulnerabilitie
* SSCHADV2011-041 - phpVideoPro Multiple XSS vulnerabilities
* SSCHADV2011-042 - Beehive Forum 101 Multiple XSS vulnerabilities

* INFOSERVE-ADV2011-01 - Tiki Wiki CMS Multiple XSS vulnerabilities - [CVE-2011-4454, CVE-2011-4455]
* INFOSERVE-ADV2011-03 - Multiple Cross-Site-Scripting vulnerabilities in Dolibarr 3.1.0 - [CVE-2011-4329]
* INFOSERVE-ADV2011-04 - Multiple Cross-Site-Scripting vulnerabilities in x3cms
* INFOSERVE-ADV2011-07 - Tiki Wiki CMS Groupware Stored Cross-Site-Scripting - [CVE-2011-4551]
* INFOSERVE-ADV2011-11 - VertrigoServ 2.25 Cross-Site-Scripting vulnerability
* INFOSERVE-ADV2011-12 - SQLiteManager 1.2.4 Multiple Cross-Site-Scripting vulnerabilities

===== SQL Injection =====

* SSCHADV2011-019 - openEngine 2.0 'id' Blind SQL Injection vulnerability
* SSCHADV2011-026 - openEngine 2.0 'key' Blind SQL Injection vulnerability
* SSCHADV2011-039 - Meditate Web Content Editor 'username_input' SQL-Injection vulnerability

* INFOSERVE-ADV2011-06 - Seotoaster SQL-Injection Admin Login Bypass

* INFOSERVE-ADV2011-08 - PHP Inventory 1.3.1 Remote (Auth Bypass) SQL Injection Vulnerability

===== Full Path Disclosure =====

* SSCHADV2011-032 - Piwik 1.6 Full Path Disclosure

===== Local File Inclusion =====

* SSCHADV2011-034 - osCSS2 "_ID" parameter Local file inclusion

===== Buffer Overflow =====

* SSCHADV2011-040 - Nagios Plugin 'check_ups' Local Buffer Overflow

===== Multiple security vulnerabilities =====

* SSCHADV2011-010 - Multiple vulnerabilities on www.salue.de
* SSCHADV2011-012 - Multiple vulnerabilities in Zimplit CMS
* SSCHADV2011-018 - AdaptCMS 2.0.1 Multiple Security vulnerabilities
* SSCHADV2011-027 - KaiBB 2.0.1 XSS and SQL Injection vulnerabilities
* SSCHADV2011-030 - Site@School 2.4.10 SQL Injection & XSS vulnerabilities
* SSCHADV2011-031 - Yet Another CMS 1.0 SQL Injection & XSS vulnerabilities

* INFOSERVE-ADV2011-02 - Multiple security vulnerabilities in Ashop

===== Directory Traversal =====

* INFOSERVE-ADV2011-09 - zFTPServer Suite 6.0.0.52 'rmdir' Directory Traversal – [CVE-2011-4717]

“Bug Bounty” - Programme

http://www.telekom.com/sicherheit/danke
http://support.apple.com/kb/ht1318
http://pages.ebay.com/securitycenter/ResearchersAcknowledgement.html
http://helpx.adobe.com/security/acknowledgements.html
http://company.yandex.com/security/hall-of-fame.xml
https://hackerone.com/sschurtz
http://technet.microsoft.com/en-in/security/cc308589.aspx

Weitere Referenzen

http://packetstormsecurity.org/files/author/8812/
http://www.exploit-db.com/author/?a=3427