#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Java floating point number denial of service - via POST"; flow:to\_server,established; content:"2.2250738585072012e-308"; nocase; http\_client\_body; metadata:policy security-ips drop, service http; reference:cve,2010-4476; reference:url,www.oracle.com/technetwork/topics/security/alert-cve-2010-4476-305811.html; classtype:attempted-dos; sid:18471; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP System variable directory traversal attempt - %WINDIR%"; flow:to\_server,established; content:"%WINDIR%"; fast\_pattern:only; http\_uri; metadata:service http; classtype:attempted-recon; sid:21836; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ion-p access"; flow:to\_server,established; content:"/ion-p"; nocase; http\_uri; metadata:service http; reference:bugtraq,6091; reference:cve,2002-1559; reference:nessus,11729; classtype:web-application-activity; sid:1969; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP everythingform.cgi access"; flow:to\_server,established; content:"/everythingform.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,2101; reference:bugtraq,4579; reference:cve,2001-0023; reference:nessus,11748; classtype:web-application-activity; sid:2203; rev:16;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Joomla invalid token administrative password reset attempt"; flow:to\_server,established; content:"task=confirmreset"; nocase; http\_uri; content:"option=com\_user"; http\_uri; content:"token=%27&"; nocase; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,30667; reference:cve,2008-3681; reference:url,developer.joomla.org/security/news/241-20080801-core-password-remind-functionality.html; classtype:attempted-admin; sid:14610; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP SWEditServlet access"; flow:to\_server,established; content:"/SWEditServlet"; http\_uri; metadata:service http; reference:bugtraq,2868; classtype:attempted-recon; sid:1259; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Invision Board ipchat.php file include"; flow:to\_server,established; content:"/ipchat.php"; nocase; http\_uri; content:"root\_path="; content:"conf\_global.php"; fast\_pattern:only; metadata:service http; reference:bugtraq,6976; classtype:web-application-attack; sid:2359; rev:10;)

alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP MKCOL Webdav Stack Buffer Overflow attempt"; flow:to\_server,established; content:"MKCOL"; depth:5; nocase; isdataat:200,relative; pcre:"/^MKCOL\s+[^\s]{200}/smi"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,37874; reference:cve,2010-0361; classtype:attempted-admin; sid:21234; rev:2;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Oracle Fusion Middleware WebCenter selectedLocale parameter sql injection attempt"; flow:to\_server,established; content:"POST"; http\_method; content:"/cs/ContentServer"; fast\_pattern:only; http\_uri; content:"selectedLocale="; nocase; http\_client\_body; pcre:"/(^|&)selectedLocale=[^&]+?([\x22\x27]|%22|%27)/iP"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,55984; reference:cve,2012-3186; reference:url,www.oracle.com/technetwork/topics/security/cpuoct2012-1515893.html; classtype:web-application-attack; sid:24629; rev:1;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Lizard Cart CMS SQL injection in detail.php id attempt"; flow:to\_server,established; content:"detail.php"; fast\_pattern:only; http\_uri; content:"id"; nocase; http\_uri; pcre:"/id=[^\r\n\x26]\*?([\x22\x27]|%2[27])/i"; metadata:service http; reference:bugtraq,16140; reference:cve,2006-0087; classtype:web-application-attack; sid:20644; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP envout.bat access"; flow:to\_server,established; content:"/envout.bat"; http\_uri; metadata:service http; reference:bugtraq,762; reference:cve,1999-0947; reference:nessus,10016; classtype:web-application-activity; sid:1517; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 8028 (msg:"SERVER-WEBAPP Novell eDirectory HTTP redirection buffer overflow attempt"; flow:to\_server,established; content:"Host|3A|"; nocase; isdataat:63,relative; content:!"|0A|"; within:63; pcre:"/^(GET|POST)\s+[^\s]\*(\x2fnds|\x2fdhost)[^\n]\*\nHost\x3a\s\*[^\n]{63}/i"; metadata:service http; reference:bugtraq,20655; reference:cve,2006-5478; classtype:attempted-admin; sid:8711; rev:9;)

alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP UNLOCK Webdav Stack Buffer Overflow attempt"; flow:to\_server,established; content:"UNLOCK"; depth:6; nocase; isdataat:200,relative; pcre:"/^UNLOCK\s+[^\s]{200}/smi"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,37874; reference:cve,2010-0361; classtype:attempted-admin; sid:21236; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP chipcfg.cgi access"; flow:to\_server,established; content:"/chipcfg.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,2767; reference:cve,2001-1341; reference:url,archives.neohapsis.com/archives/bugtraq/2001-05/0233.html; classtype:web-application-activity; sid:2116; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 8300 (msg:"SERVER-WEBAPP Novell Groupwise Messenger parameter memory corruption attempt"; flow:to\_server,established; content:"tag=NM\_A\_PARM1"; fast\_pattern:only; content:"POST"; http\_method; content:"/login"; depth:6; nocase; http\_uri; content:"|0D 0A 0D 0A|"; content:"type=12"; distance:0; content:"cmd="; nocase; metadata:policy security-ips drop, service http; reference:bugtraq,52056; reference:url,aluigi.altervista.org/adv/nmma\_1-adv.txt; classtype:attempted-admin; sid:23385; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Ecommerce checks.txt access"; flow:to\_server,established; content:"/orders/checks.txt"; nocase; http\_uri; metadata:service http; reference:bugtraq,2281; classtype:attempted-recon; sid:1155; rev:13;)

#alert tcp $EXTERNAL\_NET $FILE\_DATA\_PORTS -> $HOME\_NET any (msg:"SERVER-WEBAPP Netop Remote Control dws file buffer overflow attempt"; flow:to\_client,established; flowbits:isset,file.dws; file\_data; pcre:"/[^\x0d\x0a]{520}/smi"; metadata:service http, service imap, service pop3; reference:bugtraq,47631; reference:url,osvdb.org/72291; classtype:attempted-user; sid:24706; rev:1;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Bugzilla doeditvotes.cgi access"; flow:to\_server,established; content:"/doeditvotes.cgi"; http\_uri; metadata:service http; reference:bugtraq,3800; reference:cve,2002-0011; classtype:web-application-activity; sid:1617; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP tcsh access"; flow:to\_server,established; content:"/tcsh"; nocase; http\_uri; metadata:service http; reference:cve,1999-0509; reference:url,www.cert.org/advisories/CA-1996-11.html; classtype:attempted-recon; sid:872; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Ecommerce import.txt access"; flow:to\_server,established; content:"/config/import.txt"; nocase; http\_uri; metadata:service http; classtype:attempted-recon; sid:1146; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP iPlanet .perf access"; flow:to\_server,established; content:"/.perf"; http\_uri; metadata:service http; reference:nessus,11220; classtype:web-application-activity; sid:2062; rev:10;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP OpenView Network Node Manager cookie buffer overflow attempt"; flow:to\_server,established; content:"/OVCgi/webappmon.exe"; fast\_pattern:only; http\_uri; pcre:"/(OvJavaScript|OvTitleFrame|OvHelpWindow|OvMap|OvSession|OvJavaLocale|OvOSLocale|OvLogin|OvDebug|OvDeveloper|OvTreeControl|OvJavaScript|OvProduct|OvPort|OvLocale|OvWebSession)\s\*\x3D[^\x3B\x2C]{1024}/iC"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,42154; reference:cve,2010-2709; classtype:attempted-user; sid:17140; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 81 (msg:"SERVER-WEBAPP McAfee header buffer overflow attempt"; flow:to\_server,established; content:"AgentGuid="; nocase; isdataat:62,relative; pcre:"/^[^\x3e\x3f\x26]{63}/R"; content:"Source="; nocase; isdataat:50,relative; pcre:"/^[^\x3e\x3f\x26]{50}/R"; metadata:service http; reference:bugtraq,20288; reference:cve,2006-5156; classtype:attempted-admin; sid:8441; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Wordpress cache\_lastpostdate code injection attempt"; flow:to\_server,established; content:"wp\_filter"; pcre:"/cache\_lastpostdate\[[^\]]+\]=[^\x00\x3B\x3D]{30}/smi"; metadata:service http; reference:bugtraq,14533; reference:cve,2005-2612; classtype:attempted-admin; sid:8708; rev:6;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Majordomo2 http directory traversal attempt"; flow:to\_server,established; content:"mj\_wwwusr"; fast\_pattern; nocase; http\_uri; content:"extra="; distance:0; nocase; http\_uri; content:"../../.."; distance:0; http\_uri; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,46127; reference:cve,2011-0049; classtype:web-application-attack; sid:18761; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP pfdispaly.cgi arbitrary command execution attempt"; flow:to\_server,established; content:"/pfdispaly.cgi?'"; nocase; http\_uri; metadata:service http; reference:cve,1999-0270; reference:nessus,10174; classtype:web-application-attack; sid:1655; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP webcart access"; flow:to\_server,established; content:"/webcart/"; nocase; http\_uri; metadata:service http; reference:cve,1999-0610; reference:nessus,10298; classtype:attempted-recon; sid:1125; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP bizdbsearch access"; flow:to\_server,established; content:"/bizdb1-search.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,1104; reference:cve,2000-0287; reference:nessus,10383; classtype:web-application-activity; sid:1535; rev:19;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP bbs\_forum.cgi access"; flow:to\_server,established; content:"/bbs\_forum.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,2177; reference:cve,2001-0123; reference:url,www.cgisecurity.com/advisory/3.1.txt; classtype:web-application-activity; sid:1710; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ls%20-l"; flow:to\_server,established; content:"ls%20-l"; nocase; metadata:service http; classtype:attempted-recon; sid:1118; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP admin.php access"; flow:to\_server,established; content:"/admin.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,3361; reference:bugtraq,7532; reference:bugtraq,9270; reference:cve,2001-1032; classtype:attempted-recon; sid:1301; rev:21;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 443 (msg:"SERVER-WEBAPP SSLv2 OpenSSl KEY\_ARG buffer overflow attempt"; flow:to\_server,established; ssl\_version:sslv2; ssl\_state:client\_keyx; content:"|02|"; depth:1; offset:2; byte\_test:2,>,8,7,relative; metadata:service ssl; reference:bugtraq,5362; reference:cve,2002-0656; classtype:misc-attack; sid:10997; rev:8;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP flexform access"; flow:to\_server,established; content:"/flexform"; nocase; http\_uri; metadata:service http; reference:url,www.wiretrip.net/rfp/p/doc.asp/i2/d6.htm; classtype:attempted-recon; sid:883; rev:15;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP OpenView Network Node Manager cookie buffer overflow attempt"; flow:to\_server,established; content:"/OVCgi/nnmRptPresenter.exe"; fast\_pattern:only; http\_uri; pcre:"/(OvJavaScript|OvTitleFrame|OvHelpWindow|OvMap|OvSession|OvJavaLocale|OvOSLocale|OvLogin|OvDebug|OvDeveloper|OvTreeControl|OvJavaScript|OvProduct|OvPort|OvLocale|OvWebSession)\s\*\x3D[^\x3B\x2C]{1024}/iC"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,42154; reference:cve,2010-2709; classtype:attempted-user; sid:18911; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Oracle GlassFish Enterprise server cross site scripting attempt"; flow:to\_server,established; content:"/common/appServer/pswdAliasNew|2E|jsf"; fast\_pattern:only; http\_uri; pcre:"/aliasNameNew=[^\x26]+(script|onload|onmouseover|\x27|\x22|\x3c|\x3e|src)/smi"; metadata:policy security-ips drop, service http, service imap, service pop3; reference:cve,2012-0551; reference:url,osvdb.org/81250; reference:url,www.oracle.com/technetwork/topics/security/cpuapr2012-366314.html; classtype:web-application-attack; sid:23047; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP PayPal Storefront remote file include attempt"; flow:to\_server,established; content:"do=ext"; http\_uri; content:"page="; http\_uri; pcre:"/page=(https?|ftps?|php)/Ui"; metadata:service http; reference:bugtraq,8791; reference:nessus,11873; classtype:web-application-attack; sid:2307; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Symantec IM manager IMAdminReportTrendFormRun.asp sql injection attempt"; flow:to\_server, established; content:"|2F|IMManager|2F|admin|2F|IMAdminReportTrendFormRun|2E|asp|3F|"; nocase; http\_uri; pcre:"/groupList\x3d[^\x26]\*\x3b/Ui"; metadata:policy security-ips drop, service http; reference:bugtraq,44299; reference:cve,2010-0112; classtype:attempted-user; sid:18556; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP unify eWave ServletExec DOS"; flow:to\_server,established; content:"/servlet/ServletExec"; http\_uri; metadata:service http; reference:bugtraq,1868; reference:cve,2000-1025; classtype:web-application-activity; sid:1083; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ddicgi.exe access"; flow:to\_server,established; content:"/ddicgi.exe"; nocase; http\_uri; metadata:service http; reference:bugtraq,1657; reference:cve,2000-0826; reference:nessus,11728; classtype:web-application-activity; sid:2242; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP MatrikzGB privilege escalation attempt"; flow:to\_server,established; content:"new\_rights=admin"; nocase; http\_uri; metadata:service http; reference:bugtraq,8430; classtype:web-application-activity; sid:2331; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP smartsearch.cgi access"; flow:to\_server,established; content:"/smartsearch.cgi"; http\_uri; metadata:service http; reference:bugtraq,7133; classtype:web-application-activity; sid:2001; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP eXtropia webstore directory traversal"; flow:to\_server,established; content:"/web\_store.cgi"; http\_uri; content:"page=../"; metadata:service http; reference:bugtraq,1774; reference:cve,2000-1005; reference:nessus,10532; classtype:web-application-attack; sid:1088; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP hello.bat arbitrary command execution attempt"; flow:to\_server,established; content:"/hello.bat"; http\_uri; content:"&"; metadata:service http; reference:bugtraq,1002; reference:cve,2000-0213; reference:nessus,10246; classtype:web-application-attack; sid:1707; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP Data Protector GetPolicies SQL Injection attempt"; flow:to\_server,established; content:"POST"; nocase; http\_method; content:"/dpnepolicyservice/DPNECentral.asmx"; nocase; http\_uri; content:"GetPolicies"; nocase; http\_client\_body; content:"clientVersion"; distance:0; nocase; http\_client\_body; content:"|3B|"; distance:0; http\_client\_body; content:"/clientVersion"; distance:0; nocase; http\_client\_body; metadata:service http; reference:cve,2011-3157; reference:url,h20565.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr\_na-c03058866&ac.admitted=1321285525395.876444892.492883150; reference:url,osvdb.org/show/osvdb/76702; classtype:attempted-user; sid:20635; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Title.php access"; flow:to\_server,established; content:"/Title.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,9057; classtype:web-application-activity; sid:2280; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP System variable in URI attempt - %LOGONSERVER%"; flow:to\_server,established; content:"%LOGONSERVER%"; fast\_pattern:only; http\_uri; metadata:service http; classtype:attempted-recon; sid:21840; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Oracle Dynamic Monitoring Services dms access"; flow:to\_server,established; content:"/dms0"; http\_uri; metadata:service http; reference:nessus,10848; classtype:web-application-activity; sid:1872; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP csPassword password.cgi.tmp access"; flow:to\_server,established; content:"/password.cgi.tmp"; http\_uri; metadata:service http; reference:bugtraq,4889; reference:cve,2002-0920; classtype:web-application-activity; sid:1788; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Advanced Poll admin\_logout.php access"; flow:to\_server,established; content:"/admin\_logout.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,8890; reference:nessus,11487; classtype:web-application-activity; sid:2292; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP read\_body.php access attempt"; flow:to\_server,established; content:"/read\_body.php"; http\_uri; metadata:service http; reference:bugtraq,6302; reference:cve,2002-1341; reference:nessus,11415; classtype:web-application-activity; sid:1997; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Mambo upload.php access"; flow:to\_server,established; content:"/upload.php"; http\_uri; metadata:service http; reference:bugtraq,6572; reference:cve,2003-1204; reference:nessus,16315; classtype:web-application-activity; sid:2077; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cvsweb version access"; flow:to\_server,established; content:"/cvsweb/version"; http\_uri; metadata:service http; reference:cve,2000-0670; reference:nessus,10465; classtype:web-application-activity; sid:1552; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP csNews.cgi access"; flow:to\_server,established; content:"/csNews.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,4994; reference:cve,2002-0923; reference:nessus,11726; classtype:web-application-activity; sid:2223; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP way-board access"; flow:to\_server,established; content:"/way-board"; nocase; http\_uri; metadata:service http; reference:bugtraq,2370; reference:cve,2001-0214; reference:nessus,10610; classtype:web-application-activity; sid:896; rev:21;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP nessus 1.X 404 probe"; flow:to\_server,established; content:"/nessus\_is\_probing\_you\_"; depth:32; http\_uri; metadata:service http; classtype:web-application-attack; sid:1102; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP swc access"; flow:to\_server,established; content:"/swc"; nocase; http\_uri; metadata:service http; reference:nessus,10493; classtype:attempted-recon; sid:1478; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Oracle iSQLPlus login.uix username overflow attempt"; flow:to\_server,established; content:"/login.uix"; nocase; http\_uri; pcre:"/username=[^&\x3b\r\n]{250}/smi"; metadata:service http; reference:bugtraq,10871; reference:url,www.nextgenss.com/advisories/ora-isqlplus.txt; classtype:web-application-attack; sid:2703; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP backup access"; flow:to\_server,established; content:"/backup"; nocase; http\_uri; metadata:service http; classtype:attempted-recon; sid:1213; rev:11;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP OpenView Network Node Manager cookie buffer overflow attempt"; flow:to\_server,established; content:"/OVCgi/Title.exe"; fast\_pattern:only; http\_uri; pcre:"/(OvJavaScript|OvTitleFrame|OvHelpWindow|OvMap|OvSession|OvJavaLocale|OvOSLocale|OvLogin|OvDebug|OvDeveloper|OvTreeControl|OvJavaScript|OvProduct|OvPort|OvLocale|OvWebSession)\s\*\x3D[^\x3B\x2C]{1024}/iC"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,42154; reference:cve,2010-2709; classtype:attempted-user; sid:18924; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 9120 (msg:"SERVER-WEBAPP DiskPulseServer GetServerInfo request buffer overflow"; flow:to\_server,established; content:"GetServerInfo|02|"; nocase; isdataat:256,relative; content:!"|0D|"; within:256; metadata:policy security-ips drop; reference:bugtraq,43919; reference:url,xforce.iss.net/xforce/xfdb/62396; classtype:attempted-user; sid:20446; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Squid HTTP Proxy-Authorization overflow"; flow:to\_server,established; content:"TlRMTVNTUAADAAAA"; fast\_pattern:only; content:"Proxy-Authorization"; nocase; pcre:"/^\s\*\x3a\s\*[Nn][Tt][Ll][Mm]\s+TlRMTVNTUAADAAAA/R"; base64\_decode:relative; base64\_data; byte\_test:2,>,24,0,little; metadata:service http; reference:bugtraq,10500; reference:cve,2004-0541; classtype:attempted-user; sid:12362; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP setinfo.hts access"; flow:to\_server,established; content:"/setinfo.hts"; nocase; http\_uri; metadata:service http; reference:bugtraq,9973; reference:cve,2004-1857; reference:nessus,12120; classtype:web-application-activity; sid:2448; rev:9;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP OpenView NNM ovlogin.exe CGI userid parameter buffer overflow attempt"; flow:to\_server,established; content:"/OvCgi/ovlogin|2E|exe"; fast\_pattern:only; http\_uri; content:"userid|3D|"; nocase; http\_client\_body; isdataat:29,relative; pcre:"/userid\x3D[^\x26\x3F\x3B\x0D\x0A]{29}/iP"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:cve,2009-3846; reference:url,h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01950877; classtype:attempted-user; sid:20179; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP authentication\_index.php access"; flow:to\_server,established; content:"/authentication\_index.php"; nocase; http\_uri; metadata:service http; reference:cve,2004-0032; reference:nessus,11982; classtype:web-application-activity; sid:2328; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP OABoard forum script remote file injection attempt"; flow:to\_server,established; content:"oaboard"; nocase; http\_uri; content:"forum|2E|php|3F|"; nocase; http\_uri; content:"inc|3D|http:/"; distance:0; nocase; http\_uri; pcre:"/\/oaboard[^\r\n]\*?\/forum\.php[^\r\n]\*[\x26\x3F]inc\x3Dhttp\x3A\x2F/iU"; metadata:service http; reference:bugtraq,16105; reference:cve,2006-0076; classtype:attempted-user; sid:20826; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Novell iManager ClassName handling overflow attempt"; flow:to\_server,established; content:"/nps/servlet/webacc"; nocase; http\_uri; content:"ClassName="; fast\_pattern; nocase; http\_client\_body; pcre:"/^[^\x26]{512}/R"; metadata:policy security-ips drop, service http; reference:bugtraq,40480; reference:cve,2010-1929; classtype:attempted-admin; sid:18796; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Samba SWAT Authorization overflow attempt"; flow:to\_server,established; content:"Authorization|3A| Basic"; nocase; http\_header; pcre:"/^Authorization\x3a(\s\*|\s\*\r?\n\s+)Basic\s+=/smiH"; metadata:service http; reference:bugtraq,10780; reference:cve,2004-0600; classtype:web-application-attack; sid:2597; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Oracle XSQLConfig.xml access"; flow:to\_server,established; content:"/XSQLConfig.xml"; http\_uri; metadata:service http; reference:bugtraq,4290; reference:cve,2002-0568; reference:nessus,10855; classtype:web-application-activity; sid:1871; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 9090 (msg:"SERVER-WEBAPP Jive Software Openfire user-properties.jsp XSS attempt"; flow:to\_server,established; content:"/user-properties.jsp"; fast\_pattern:only; http\_uri; pcre:"/user-properties\.jsp\?.\*?=([^\x26]\*[\x22\x27\x3C\x3E\x28\x29\x3B]|script|src|location|document)/U"; metadata:policy security-ips drop, service http; reference:bugtraq,32935; reference:cve,2009-0496; classtype:web-application-attack; sid:20865; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP hello.bat access"; flow:to\_server,established; content:"/hello.bat"; http\_uri; metadata:service http; reference:bugtraq,1002; reference:cve,2000-0213; reference:nessus,10246; classtype:web-application-activity; sid:1708; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP simplestmail.cgi access"; flow:to\_server,established; content:"/simplestmail.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,2106; reference:bugtraq,4579; reference:cve,2001-0022; reference:nessus,11748; classtype:web-application-activity; sid:2220; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP faqmanager.cgi access"; flow:to\_server,established; content:"/faqmanager.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,3810; reference:nessus,10837; classtype:web-application-activity; sid:1591; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP xp\_regwrite attempt"; flow:to\_server,established; content:"xp\_regwrite"; nocase; metadata:service http; classtype:web-application-activity; sid:1977; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP /cgi-dos/ access"; flow:to\_server,established; content:"/cgi-dos/"; http\_uri; content:"/cgi-dos/ HTTP"; fast\_pattern:only; metadata:service http; classtype:web-application-attack; sid:1669; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP AlienForm af.cgi access"; flow:to\_server,established; content:"/af.cgi"; http\_uri; metadata:service http; reference:bugtraq,4983; reference:cve,2002-0934; reference:nessus,11027; classtype:web-application-activity; sid:1825; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP global.cgi access"; flow:to\_server,established; content:"/global.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,4579; reference:cve,2000-0952; reference:nessus,11748; classtype:web-application-activity; sid:2210; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP a1stats a1disp3.cgi directory traversal attempt"; flow:to\_server,established; content:"/a1disp3.cgi?/../../"; http\_uri; metadata:service http; reference:bugtraq,2705; reference:cve,2001-0561; reference:nessus,10669; classtype:web-application-attack; sid:1501; rev:14;)

alert tcp $HOME\_NET any -> $EXTERNAL\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Symantec Web Gateway PHP remote code execution attempt"; flow:established,to\_server; content:"/spywall/images/upload/"; fast\_pattern:only; http\_uri; content:".php"; nocase; http\_uri; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,53443; reference:cve,2012-0299; reference:url,osvdb.org/53443; reference:url,www.symantec.com/security\_response/securityupdates/detail.jsp?fid=security\_advisory&pvid=security\_advisory&year=2012&suid=20120517\_00; classtype:attempted-admin; sid:24519; rev:1;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP files.inc.php access"; flow:to\_server,established; content:"/files.inc.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,8910; classtype:web-application-activity; sid:2304; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP DCP-Portal remote file include editor script attempt"; flow:to\_server,established; content:"/library/editor/editor.php"; fast\_pattern; nocase; http\_uri; content:"root="; http\_uri; metadata:service http; reference:bugtraq,6525; classtype:web-application-attack; sid:2341; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP xmlrpc.php post attempt"; flow:to\_server,established; content:"/xmlrpc.php"; nocase; http\_uri; pcre:"/^POST\s/smi"; metadata:service http; reference:bugtraq,14088; reference:cve,2005-1921; classtype:web-application-attack; sid:3827; rev:11;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Cisco Unified Communications Manager sql injection attempt"; flow:to\_server,established; content:"/ccmcip/xmldirectorylist"; fast\_pattern:only; http\_uri; pcre:"/xmldirectorylist(\.utf-8|\.other)?\.jsp[^$\n]\*[\x3F\x26][lfn]=[^$\x26\n]\*[\x22\x27]/Ui"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:cve,2011-1610; classtype:web-application-attack; sid:21377; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP bb-hist.sh attempt"; flow:to\_server,established; content:"/bb-hist.sh?HISTFILE=../.."; nocase; http\_uri; metadata:service http; reference:bugtraq,142; reference:cve,1999-1462; reference:nessus,10025; classtype:web-application-attack; sid:1531; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Domino setup.nsf access"; flow:to\_server,established; content:"/setup.nsf"; nocase; http\_uri; metadata:service http; reference:nessus,10629; classtype:attempted-recon; sid:1577; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP commerce.cgi arbitrary file access attempt"; flow:to\_server,established; content:"/commerce.cgi"; http\_uri; content:"page="; content:"/../"; nocase; metadata:service http; reference:bugtraq,2361; reference:cve,2001-0210; reference:nessus,10612; classtype:attempted-recon; sid:1572; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP phf access"; flow:to\_server,established; content:"/phf"; nocase; http\_uri; metadata:service http; reference:bugtraq,629; reference:cve,1999-0067; classtype:web-application-activity; sid:886; rev:22;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP websitepro path access"; flow:to\_server,established; content:" /HTTP/1."; fast\_pattern:only; metadata:service http; reference:bugtraq,932; reference:cve,2000-0066; reference:nessus,10303; classtype:attempted-recon; sid:811; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP mmstdod.cgi access"; flow:to\_server,established; content:"/mmstdod.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,2063; reference:cve,2001-0021; reference:nessus,10566; classtype:attempted-recon; sid:819; rev:20;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Netscape Enterprise Server directory view"; flow:to\_server,established; content:"?wp-verify-link"; nocase; http\_uri; metadata:service http; reference:bugtraq,1063; classtype:attempted-recon; sid:1177; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Netscape Enterprise Server directory view"; flow:to\_server,established; content:"?wp-stop-ver"; nocase; http\_uri; metadata:service http; reference:bugtraq,1063; reference:cve,2000-0236; classtype:attempted-recon; sid:1189; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ws\_ftp.ini access"; flow:to\_server,established; content:"/ws\_ftp.ini"; nocase; http\_uri; metadata:service http; reference:bugtraq,547; reference:cve,1999-1078; classtype:attempted-recon; sid:1166; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP weblogic/tomcat .jsp view source attempt"; flow:to\_server,established; content:".jsp"; nocase; http\_uri; pcre:!"/^\w+\s+[^\n\s\?]\*\.jsp/smi"; metadata:service http; reference:bugtraq,2527; classtype:web-application-attack; sid:1054; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP input.bat arbitrary command execution attempt"; flow:to\_server,established; content:"/input.bat|7C|"; http\_uri; metadata:service http; reference:bugtraq,762; reference:cve,1999-0947; reference:nessus,10016; classtype:web-application-attack; sid:1512; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Netscape Enterprise Server directory view"; flow:to\_server,established; content:"?wp-start-ver"; nocase; http\_uri; metadata:service http; reference:bugtraq,1063; reference:cve,2000-0236; classtype:attempted-recon; sid:1188; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP PHP-Nuke index.php SQL injection attempt"; flow:to\_server,established; content:"insert"; fast\_pattern; nocase; http\_header; content:"index.php"; nocase; http\_uri; pcre:"/Referer\x3a[^\r\n]\*?[\x27\x22]\x29[^\r\n]\*?INSERT/Hi"; metadata:service http; reference:bugtraq,22638; reference:cve,2007-1061; classtype:web-application-attack; sid:23406; rev:4;)

alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Oracle Java Web Server Webdav Stack Buffer Overflow attempt"; flow:to\_server,established; content:"PROPPATCH"; depth:9; nocase; isdataat:200,relative; pcre:"/^PROPPATCH\s+[^\s]{200}/smi"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,37874; reference:cve,2003-0109; reference:cve,2010-0361; classtype:attempted-admin; sid:18613; rev:4;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 5555 (msg:"SERVER-WEBAPP HP OpenView Storage Data Protector directory traversal attempt"; flow:to\_server,established; content:"|2E 00 2F 00 2E 00 2E 00 2F 00|"; content:"|32 00 00 00|"; depth:4; offset:6; content:"1|00|7|00 00 00|"; distance:0; metadata:policy balanced-ips drop, policy security-ips drop; reference:cve,2011-1736; classtype:attempted-recon; sid:20530; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP php tiny shell upload attempt"; flow:to\_server,established; content:"<?=($\_=@$\_GET[2]).@$\_($\_GET[1])?>"; fast\_pattern:only; http\_client\_body; metadata:service http; reference:url,h.ackack.net/tiny-php-shell.html; classtype:misc-activity; sid:20533; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Domino mail.box access"; flow:to\_server,established; content:"/mail.box"; nocase; http\_uri; metadata:service http; reference:bugtraq,881; reference:nessus,10629; classtype:attempted-recon; sid:1586; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP calender\_admin.pl access"; flow:to\_server,established; content:"/calender\_admin.pl"; nocase; http\_uri; metadata:service http; reference:cve,2000-0432; reference:nessus,10506; classtype:attempted-recon; sid:1456; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP myPHPNuke chatheader.php access"; flow:to\_server,established; content:"/chatheader.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,6544; classtype:web-application-activity; sid:2346; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP alert.cgi access"; flow:to\_server,established; content:"/alert.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,4211; reference:bugtraq,4579; reference:cve,2002-0346; reference:nessus,11748; classtype:web-application-activity; sid:2195; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 1080 (msg:"SERVER-WEBAPP Oracle Java web proxy sockd buffer overflow attempt"; flow:to\_server,established; content:"|05 01|"; depth:2; content:"|03|"; within:1; distance:1; byte\_test:1,>,136,0,relative; metadata:policy security-ips drop; reference:bugtraq,24165; reference:cve,2007-2881; classtype:attempted-admin; sid:11680; rev:8;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cacti graph\_image.php access"; flow:to\_server,established; content:"/cacti/graph\_image.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,14042; classtype:web-application-activity; sid:4650; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP rcmd attempt"; flow:to\_server,established; content:"rcmd.exe"; nocase; http\_uri; metadata:service http; classtype:web-application-activity; sid:1065; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 8080 (msg:"SERVER-WEBAPP Trend Micro OfficeScan multiple CGI modules HTTP form processing buffer overflow attempt"; flow:to\_server,established; content:"POST"; nocase; http\_method; content:"/officescan/cgi/cgi"; nocase; http\_uri; content:"multipart/form-data"; nocase; content:"|0A|--"; distance:0; isdataat:270; content:!"|0A|--"; within:270; metadata:service http; reference:cve,2008-3862; classtype:attempted-admin; sid:15908; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP System variable directory traversal attempt - %APPDATA%"; flow:to\_server,established; content:"%APPDATA%"; fast\_pattern:only; http\_uri; metadata:service http; classtype:attempted-recon; sid:21820; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP System variable directory traversal attempt - %SystemDrive%"; flow:to\_server,established; content:"%SystemDrive%"; fast\_pattern:only; http\_uri; metadata:service http; classtype:attempted-recon; sid:21829; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Flashchat remote file include in aedating4CMS.php"; flow:to\_server,established; content:"/aedating4CMS.php"; nocase; http\_uri; content:"dir[inc]="; nocase; http\_uri; pcre:"/\x2Faedating4CMS\.php?[^\r\n]\*?dir\[inc\]=(https?|ftps?)/Ui"; metadata:service http; reference:bugtraq,19826; reference:cve,2006-4583; classtype:web-application-activity; sid:20680; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP FormHandler.cgi directory traversal attempt attempt"; flow:to\_server,established; content:"/FormHandler.cgi"; nocase; http\_uri; content:"reply\_message\_attach="; fast\_pattern:only; content:"/../"; metadata:service http; reference:bugtraq,798; reference:bugtraq,799; reference:cve,1999-1050; reference:nessus,10075; classtype:web-application-attack; sid:1628; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Sample\_showcode.html access"; flow:to\_server,established; content:"/Sample\_showcode.html"; nocase; http\_uri; content:"fname"; metadata:service http; reference:bugtraq,9555; classtype:web-application-activity; sid:2371; rev:8;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 3128 (msg:"SERVER-WEBAPP Squid authentication headers handling denial of service attempt"; flow:to\_server,established; content:"Proxy-Authorization: NTLM"; fast\_pattern:only; flowbits:set,ntlm\_authentication; flowbits:noalert; metadata:policy security-ips drop, service http; reference:bugtraq,14977; reference:cve,2005-2917; classtype:protocol-command-decode; sid:17370; rev:5;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 383 (msg:"SERVER-WEBAPP HP Operations Agent stack buffer overflow attempt"; flow:to\_server,established; flowbits:isset,hp\_openview\_coda; content:"|00 00 00 A0|"; depth:4; offset:18; byte\_jump:2,8,relative; byte\_jump:2,0,relative; byte\_jump:2,0,relative; byte\_jump:2,0,relative; byte\_test:2,>,1024,0,relative; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,54362; reference:cve,2012-2019; reference:url,h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03397769; classtype:attempted-admin; sid:24319; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP exif invalid tag data buffer overflow attempt"; flow:to\_server,established; content:"Exif|00 00|II|2A 00|"; depth:16; offset:6; http\_client\_body; content:"|05 02 05 00|"; within:1024; http\_client\_body; byte\_test:4,>,268435457,0,relative,little; metadata:service http; reference:bugtraq,46365; reference:cve,2011-0708; classtype:denial-of-service; sid:23796; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP FreePBX recording interface file upload code execution attempt"; flow:to\_server,established; content:"config.php"; nocase; http\_uri; content:"Content-Disposition"; nocase; content:"name=|22|ivrfile|22 3B|"; distance:0; fast\_pattern; nocase; content:"filename=|22|"; distance:0; nocase; pcre:!"/^\w+\.(wav|alaw|ulaw|sln|gsm)\x22/Ri"; metadata:service http; reference:bugtraq,43454; reference:cve,2010-3490; classtype:attempted-admin; sid:18465; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 8080 (msg:"SERVER-WEBAPP story.pl arbitrary file read attempt"; flow:to\_server,established; content:"/story.pl"; http\_uri; content:"next=../"; metadata:service http; reference:bugtraq,3028; reference:cve,2001-0804; reference:nessus,10817; classtype:default-login-attempt; sid:1868; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Vmist Downstat remote file include in stats.php art"; flow:to\_server,established; content:"downstat"; nocase; http\_uri; content:"stats.php"; nocase; http\_uri; content:"art="; nocase; http\_uri; pcre:"/\x2Fstats\.php\x3F[^\r\n]\*?art\x3Dhttp\x3A\x2F/Ui"; metadata:service http; reference:bugtraq,20007; reference:cve,2006-4827; classtype:web-application-activity; sid:20818; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS 80 (msg:"SERVER-WEBAPP vbulletin php code injection"; flow:to\_server,established; content:"misc.php"; http\_uri; pcre:"/template\s\*=\s\*\x7b\x24/sUmi"; metadata:service http; reference:cve,2005-0511; reference:url,marc.info/?l=bugtraq&m=110910899415763&w=2; classtype:attempted-user; sid:11668; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP htmlscript access"; flow:to\_server,established; content:"/htmlscript"; nocase; http\_uri; metadata:service http; reference:bugtraq,2001; reference:cve,1999-0264; reference:nessus,10106; classtype:attempted-recon; sid:826; rev:19;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP TikiWiki jhot.php script file upload attempt"; flow:to\_server,established; content:"/jhot.php"; nocase; http\_uri; content:"Content-Disposition|3A|"; nocase; content:"filename="; nocase; pcre:"/^Content-Disposition\x3A[^\r\n]\*filename=(?P<q1>\x22|\x27|)[^\r\n]\*?\x2Ephp(?P=q1)/smi"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,19819; reference:url,tikiwiki.org/tiki-read\_article.php?articleid=136; classtype:attempted-user; sid:17597; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ans.pl access"; flow:to\_server,established; content:"/ans.pl"; http\_uri; metadata:service http; reference:bugtraq,4147; reference:bugtraq,4149; reference:cve,2002-0306; reference:cve,2002-0307; reference:nessus,10875; classtype:web-application-activity; sid:1523; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ICQ Webfront HTTP DOS"; flow:to\_server,established; content:"??????????"; http\_uri; metadata:service http; reference:bugtraq,1463; reference:cve,2000-1078; classtype:web-application-attack; sid:1091; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Multiple Vendor server file disclosure attempt"; flow:to\_server,established; content:".jsp"; http\_uri; pcre:"/^[^\x3b]\*\x3b.\*\x2ejsp/Ui"; metadata:service http; reference:bugtraq,11245; reference:bugtraq,19106; reference:cve,2004-0928; reference:cve,2006-3853; classtype:web-application-attack; sid:15990; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP pajax call\_dispatcher remote exec attempt"; flow:to\_server,established; content:"pajax\_call\_dispatcher.php"; nocase; http\_uri; pcre:"/\x22method\x22\s\*?\x3a\s\*?\x22[^\x22]\*?\x3b\s\*?system\s\*?\x28/smi"; metadata:service http; reference:bugtraq,17519; reference:cve,2006-1551; reference:url,www.redteam-pentesting.de/advisories/rt-sa-2006-001.php; classtype:attempted-user; sid:9620; rev:8;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP SFNofitication.dll access"; flow:to\_server,established; content:"/SFNofitication.dll"; nocase; http\_uri; metadata:service http; reference:bugtraq,3327; reference:cve,2001-0958; reference:nessus,11747; classtype:web-application-activity; sid:2233; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP helpout.exe access"; flow:to\_server,established; content:"/helpout.exe"; http\_uri; metadata:service http; reference:bugtraq,6002; reference:cve,2002-1169; reference:nessus,11162; classtype:web-application-activity; sid:2057; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP htsearch access"; flow:to\_server,established; content:"/htsearch"; nocase; http\_uri; metadata:service http; reference:bugtraq,1026; reference:cve,2000-0208; reference:nessus,10105; classtype:web-application-activity; sid:1602; rev:19;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP PHP-Nuke remote file include attempt"; flow:to\_server,established; content:"/index.php"; fast\_pattern; nocase; http\_uri; content:"file="; pcre:"/file=(https?|ftps?|php)/i"; metadata:service http; reference:bugtraq,3889; reference:cve,2002-0206; classtype:web-application-attack; sid:1399; rev:21;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP SWSoft ASPSeek Overflow attempt"; flow:to\_server,established; content:"/s.cgi"; fast\_pattern; nocase; http\_uri; content:"tmpl="; metadata:service http; reference:bugtraq,2492; reference:cve,2001-0476; classtype:web-application-attack; sid:804; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP quickstore.cgi access"; flow:to\_server,established; content:"/quickstore.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,9282; reference:nessus,11975; classtype:web-application-activity; sid:2323; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 25 (msg:"SERVER-WEBAPP socket\_connect buffer overflow attempt"; flow:to\_server,established; file\_data; content:"$padd = str\_repeat(|22|A|22|, 196)"; content:"$evil = $padd.$payload"; distance:0; fast\_pattern; content:"socket\_create(AF\_UNIX, SOCK\_STREAM, 1)"; metadata:service smtp; reference:bugtraq,49241; reference:cve,2011-1938; classtype:attempted-user; sid:24195; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP WAnewsletter db\_type.php access"; flow:to\_server,established; content:"/sql/db\_type.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,6964; classtype:web-application-activity; sid:2399; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP textcounter.pl access"; flow:to\_server,established; content:"/textcounter.pl"; nocase; http\_uri; metadata:service http; reference:bugtraq,2265; reference:cve,1999-1479; reference:nessus,11451; classtype:attempted-recon; sid:836; rev:20;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Novell iManager getMultiPartParameters unauthorized file upload attempt"; flow:to\_server,established; content:"/nps/servlet/modulemanager"; nocase; http\_uri; content:"Content-Disposition"; nocase; pcre:"/^[^\n]\*filename[^\x3B]\*([\x5C\x2F]\x2E\x2E|\x2E\x2E[\x5C\x2F])/Ri"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,43635; classtype:attempted-admin; sid:18311; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cacti graph\_image SQL injection attempt"; flow:to\_server,established; content:"graph.php"; nocase; http\_uri; pcre:"/local\_graph\_id=(?!(\d+|)([\x26\s]|$))/smi"; metadata:service http; reference:bugtraq,14128; reference:bugtraq,14129; reference:cve,2005-2148; classtype:web-application-attack; sid:8716; rev:7;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP OpenView Network Node Manager cookie buffer overflow attempt"; flow:to\_server,established; content:"/OVCgi/ovsipexport.exe"; fast\_pattern:only; http\_uri; pcre:"/(OvJavaScript|OvTitleFrame|OvHelpWindow|OvMap|OvSession|OvJavaLocale|OvOSLocale|OvLogin|OvDebug|OvDeveloper|OvTreeControl|OvJavaScript|OvProduct|OvPort|OvLocale|OvWebSession)\s\*\x3D[^\x3B\x2C]{1024}/iC"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,42154; reference:cve,2010-2709; classtype:attempted-user; sid:18919; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Phorum authentication access"; flow:to\_server,established; content:"PHP\_AUTH\_USER=boogieman"; fast\_pattern:only; metadata:service http; reference:bugtraq,2274; classtype:attempted-recon; sid:1137; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP mailit.pl access"; flow:to\_server,established; content:"/mailit.pl"; nocase; http\_uri; metadata:service http; reference:nessus,10417; classtype:attempted-recon; sid:1475; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Trend Micro OfficeScan access"; flow:to\_server,established; content:"/officescan/cgi/jdkRqNotify.exe"; nocase; http\_uri; metadata:service http; reference:bugtraq,1057; classtype:attempted-recon; sid:1192; rev:12;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 383 (msg:"SERVER-WEBAPP HP Operations Agent stack buffer overflow attempt"; flow:to\_server,established; flowbits:isset,hp\_openview\_coda; content:"|00 00 00 6E|"; depth:4; offset:18; byte\_jump:2,16,relative; byte\_jump:2,0,relative; byte\_test:2,>,1024,0,relative; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,54362; reference:cve,2012-2019; reference:url,h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03397769; classtype:attempted-admin; sid:24314; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Talentsoft Web+ Source Code view access"; flow:to\_server,established; content:"/webplus.exe?script=test.wml"; http\_uri; metadata:service http; reference:bugtraq,1722; reference:url,archives.neohapsis.com/archives/ntbugtraq/2000-q3/0168.html; classtype:web-application-attack; sid:1095; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP System variable directory traversal attempt - %ALLUSERSPROFILE%"; flow:to\_server,established; content:"%ALLUSERSPROFILE%"; fast\_pattern:only; http\_uri; metadata:service http; classtype:attempted-recon; sid:21818; rev:3;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP CA Total Defense management.asmx sql injection attempt"; flow:to\_server,established; content:"POST"; http\_method; content:"/UNCWS/Management.asmx"; fast\_pattern:only; http\_uri; content:!"SOAP"; nocase; http\_header; pcre:"/(^|&)SelectedID=[^&]+?(\x3B|%3B)/miP"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,47355; reference:url,support.ca.com/irj/portal/anonymous/phpsupcontent?contentID={CD065CEC-AFE2-4D9D-8E0B-BE7F6E345866}; classtype:attempted-admin; sid:24704; rev:1;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP auktion.cgi directory traversal attempt"; flow:to\_server,established; content:"/auktion.cgi"; fast\_pattern; nocase; http\_uri; content:"menue=../../"; nocase; metadata:service http; reference:bugtraq,2367; reference:cve,2001-0212; reference:nessus,10638; classtype:web-application-attack; sid:1703; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP bigconf.cgi access"; flow:to\_server,established; content:"/bigconf.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,778; reference:cve,1999-1550; reference:nessus,10027; classtype:web-application-activity; sid:1172; rev:16;)

#alert tcp $HOME\_NET any -> $EXTERNAL\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Zend Framework Zend\_XmlRpc information disclosure attempt"; flow:to\_server,established; content:"POST"; http\_method; content:"<!ENTITY"; nocase; http\_client\_body; content:"SYSTEM"; distance:0; http\_client\_body; pcre:"/<!ENTITY[^>]\*?SYSTEM/smiP"; metadata:service http; reference:cve,2012-3363; reference:url,osvdb.org/83221; classtype:attempted-recon; sid:24339; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP sadmind worm access"; flow:to\_server,established; content:"GET x HTTP/1.0"; depth:15; metadata:service http; reference:url,www.cert.org/advisories/CA-2001-11.html; classtype:attempted-recon; sid:1375; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 3443 (msg:"SERVER-WEBAPP HP Openview NNM connectedNodes.ovpl port 3443 Unix command execution attempt"; flow:to\_server,established; content:"/connectedNodes.ovpl"; nocase; http\_uri; content:"node="; nocase; http\_uri; pcre:"/connectedNodes.ovpl[^\r\n]\*node=[^\r\n]\*[\x2c\x24\x7c\x3b\x22\x26\x3c\x3f]/Usmi"; metadata:service http; reference:bugtraq,14662; reference:cve,2005-2773; classtype:web-application-attack; sid:8085; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP win-c-sample.exe access"; flow:to\_server,established; content:"/win-c-sample.exe"; nocase; http\_uri; metadata:service http; reference:bugtraq,2078; reference:cve,1999-0178; reference:nessus,10008; classtype:attempted-recon; sid:875; rev:20;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 5555 (msg:"SERVER-WEBAPP HP OpenView Storage Data Protector get file buffer overflow attempt"; flow:to\_server,established; content:"|32 00 00 00|"; depth:4; offset:6; content:"1|00|7|00 00 00|"; distance:0; isdataat:514,relative; content:!"|00|"; within:514; metadata:policy balanced-ips drop, policy security-ips drop; reference:cve,2011-1729; classtype:attempted-user; sid:20532; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP alienform.cgi directory traversal attempt"; flow:to\_server,established; content:"/alienform.cgi"; http\_uri; content:".|7C|./.|7C|."; metadata:service http; reference:bugtraq,4983; reference:cve,2002-0934; reference:nessus,11027; classtype:web-application-attack; sid:1822; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP /cgi-bin/ls access"; flow:to\_server,established; content:"/cgi-bin/ls"; nocase; http\_uri; metadata:service http; reference:bugtraq,936; reference:cve,2000-0079; reference:nessus,10037; classtype:web-application-activity; sid:1539; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Novell Groupwise gwweb.exe attempt"; flow:to\_server,established; content:"/GWWEB.EXE?HELP="; nocase; http\_uri; metadata:service http; reference:bugtraq,879; reference:cve,1999-1005; reference:cve,1999-1006; reference:nessus,10877; classtype:attempted-recon; sid:1614; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP service.cgi access"; flow:to\_server,established; content:"/service.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,4211; reference:bugtraq,4579; reference:cve,2002-0346; reference:nessus,11748; classtype:web-application-activity; sid:2218; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP txt2html.cgi directory traversal attempt"; flow:to\_server,established; content:"/txt2html.cgi"; http\_uri; content:"/../../../../"; fast\_pattern:only; metadata:service http; classtype:web-application-attack; sid:1305; rev:13;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP OpenView Network Node Manager cookie buffer overflow attempt"; flow:to\_server,established; content:"/OVCgi/jovwreg.exe"; fast\_pattern:only; http\_uri; pcre:"/(OvJavaScript|OvTitleFrame|OvHelpWindow|OvMap|OvSession|OvJavaLocale|OvOSLocale|OvLogin|OvDebug|OvDeveloper|OvTreeControl|OvJavaScript|OvProduct|OvPort|OvLocale|OvWebSession)\s\*\x3D[^\x3B\x2C]{1024}/iC"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,42154; reference:cve,2010-2709; classtype:attempted-user; sid:18909; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP whois\_raw.cgi arbitrary command execution attempt"; flow:to\_server,established; content:"/whois\_raw.cgi?"; http\_uri; content:"|0A|"; metadata:service http; reference:bugtraq,304; reference:cve,1999-1063; reference:nessus,10306; classtype:web-application-attack; sid:809; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP IdeaBox notification.php file include"; flow:to\_server,established; content:"/index.php"; nocase; http\_uri; content:"gorumDir="; fast\_pattern:only; content:"notification.php"; nocase; metadata:service http; reference:bugtraq,7488; classtype:web-application-activity; sid:2354; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP Openview OvWebHelp.exe buffer overflow"; flow:to\_server, established; content:"POST"; http\_method; content:"/OvCgi/OvWebHelp.exe"; http\_uri; content:"Topic="; nocase; isdataat:500,relative; pcre:"/^[^&\x3b]{500}/Ri"; metadata:policy security-ips drop, service http; reference:bugtraq,37261; reference:bugtraq,37340; reference:cve,2009-4178; reference:url,h2000.ww2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01950877; classtype:attempted-admin; sid:18475; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP VEGO Web Forum SQL injection in login.php username attempt"; flow:to\_server,established; content:"login.php"; fast\_pattern:only; http\_uri; content:"username"; nocase; pcre:"/username=[^\r\n\x26]\*?([\x22\x27]|%2[27])/i"; metadata:service http; reference:bugtraq,16108; reference:cve,2006-0067; classtype:web-application-attack; sid:20640; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP musicat empower attempt"; flow:to\_server,established; content:"/empower?DB="; nocase; http\_uri; metadata:service http; reference:bugtraq,2374; reference:cve,2001-0224; reference:nessus,10609; classtype:web-application-attack; sid:1589; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP NetScreen SA 5000 delhomepage.cgi access"; flow:to\_server,established; content:"/delhomepage.cgi"; http\_uri; metadata:service http; reference:bugtraq,9791; reference:cve,2004-0347; classtype:web-application-activity; sid:3062; rev:8;)

alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Symantec Web Gateway blocked.php id parameter sql injection attempt"; flow:to\_server,established; content:"/spywall/blocked.php"; fast\_pattern:only; http\_uri; pcre:"/[?&]id=[^&]\*?[\x28\x29]/Ui"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,54424; reference:cve,2012-2574; classtype:web-application-attack; sid:23784; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP PhpGedView PGV authentication\_index.php base directory manipulation attempt"; flow:to\_server,established; content:"/authentication\_index.php"; nocase; http\_uri; content:"PGV\_BASE\_DIRECTORY"; fast\_pattern:only; metadata:service http; reference:bugtraq,9368; reference:cve,2004-0030; classtype:web-application-attack; sid:2366; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ustorekeeper.pl directory traversal attempt"; flow:to\_server,established; content:"/ustorekeeper.pl"; nocase; http\_uri; content:"file=../../"; fast\_pattern:only; metadata:service http; reference:bugtraq,2536; reference:cve,2001-0466; reference:nessus,10645; classtype:web-application-attack; sid:1730; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP AnyForm2 access"; flow:to\_server,established; content:"/AnyForm2"; nocase; http\_uri; metadata:service http; reference:bugtraq,719; reference:cve,1999-0066; reference:nessus,10277; classtype:attempted-recon; sid:892; rev:20;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP TheWebForum SQL injection in login.php username attempt"; flow:to\_server,established; content:"login.php"; fast\_pattern:only; http\_uri; content:"username"; nocase; pcre:"/username=[^\r\n\x26]\*?([\x22\x27]|%2[27])/i"; metadata:service http; reference:bugtraq,16161; reference:cve,2006-0135; classtype:web-application-attack; sid:20641; rev:6;)

#alert tcp $EXTERNAL\_NET $HTTP\_PORTS -> $HOME\_NET any (msg:"SERVER-WEBAPP server negative Content-Length attempt"; flow:to\_client,established; content:"Content-Length"; nocase; pcre:"/^Content-Length\s\*\x3a\s\*-\d+/mi"; metadata:service http; reference:bugtraq,10508; reference:cve,2004-0492; reference:url,www.guninski.com/modproxy1.html; classtype:attempted-admin; sid:2580; rev:10;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP OpenView Network Node Manager cookie buffer overflow attempt"; flow:to\_server,established; content:"/OVCgi/OpenView5.exe"; fast\_pattern:only; http\_uri; pcre:"/(OvJavaScript|OvTitleFrame|OvHelpWindow|OvMap|OvSession|OvJavaLocale|OvOSLocale|OvLogin|OvDebug|OvDeveloper|OvTreeControl|OvJavaScript|OvProduct|OvPort|OvLocale|OvWebSession)\s\*\x3D[^\x3B\x2C]{1024}/iC"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,42154; reference:cve,2010-2709; classtype:attempted-user; sid:18912; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP /.... access"; flow:to\_server,established; content:"/...."; metadata:service http; classtype:attempted-recon; sid:1142; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP sml3com access"; flow:to\_server,established; content:"/graphics/sml3com"; http\_uri; metadata:service http; reference:bugtraq,2721; reference:cve,2001-0740; classtype:web-application-activity; sid:1291; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP /cgi-bin/ access"; flow:to\_server,established; content:"/cgi-bin/"; http\_uri; content:"/cgi-bin/ HTTP"; fast\_pattern:only; metadata:service http; classtype:web-application-attack; sid:1668; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP fileseek.cgi access"; flow:to\_server,established; content:"/fileseek.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,4579; reference:bugtraq,6784; reference:cve,2002-0611; reference:nessus,11748; classtype:web-application-activity; sid:2207; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP webplus access"; flow:to\_server,established; content:"/webplus?script"; nocase; http\_uri; metadata:service http; reference:bugtraq,1174; reference:bugtraq,1720; reference:bugtraq,1722; reference:bugtraq,1725; reference:cve,2000-1005; classtype:attempted-recon; sid:1159; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP JBoss expression language actionOutcome remote code execution"; flow:to\_server,established; content:"actionOutcome=/"; nocase; http\_uri; content:"|23 7B|"; distance:0; nocase; http\_uri; pcre:"/actionOutcome=\x2F[^\x3F]+\x3F[^\x26]\*\x23\x7B/Ui"; metadata:service http; reference:bugtraq,41994; reference:cve,2010-1871; classtype:attempted-admin; sid:19558; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP bnbform.cgi access"; flow:to\_server,established; content:"/bnbform.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,2147; reference:cve,1999-0937; classtype:attempted-recon; sid:846; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP spamrule.dll access"; flow:to\_server,established; content:"/spamrule.dll"; nocase; http\_uri; metadata:service http; reference:bugtraq,3327; reference:cve,2001-0958; reference:nessus,11747; classtype:web-application-activity; sid:2236; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP alchemy http server NUL arbitrary command execution attempt"; flow:to\_server,established; content:"/NUL/../../"; http\_uri; metadata:service http; reference:bugtraq,3599; reference:cve,2001-0871; reference:nessus,10818; classtype:web-application-activity; sid:1506; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP .wwwacl access"; flow:to\_server,established; content:".www\_acl"; nocase; http\_uri; metadata:service http; classtype:attempted-recon; sid:1131; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP nph-publish.cgi access"; flow:to\_server,established; content:"/nph-publish.cgi"; http\_uri; metadata:service http; reference:cve,1999-1177; reference:nessus,10164; classtype:web-application-activity; sid:1876; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP PCCS mysql database admin tool access"; flow:to\_server,established; content:"pccsmysqladm/incs/dbconnect.inc"; depth:36; nocase; metadata:service http; reference:bugtraq,1557; reference:cve,2000-0707; reference:nessus,10783; classtype:web-application-attack; sid:509; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP System variable directory traversal attempt - %SystemRoot%"; flow:to\_server,established; content:"%SystemRoot%"; fast\_pattern:only; http\_uri; metadata:service http; classtype:attempted-recon; sid:21830; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP .bat? access"; flow:to\_server,established; content:".bat?"; nocase; http\_uri; metadata:service http; reference:bugtraq,2023; reference:bugtraq,4335; reference:cve,1999-0233; reference:cve,2002-0061; reference:url,support.microsoft.com/support/kb/articles/Q148/1/88.asp; reference:url,support.microsoft.com/support/kb/articles/Q155/0/56.asp; classtype:web-application-activity; sid:976; rev:18;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP OpenView Network Node Manager OvOSLocale parameter buffer overflow attempt"; flow:to\_server,established; content:"/OVCgi/Toolbar.exe"; nocase; http\_uri; content:"OvOSLocale"; nocase; http\_cookie; pcre:"/OvOSLocale\s\*\x3d\s\*[^\x3b\s]{249}/Cmi"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,34134; reference:cve,2008-0067; reference:cve,2009-0920; classtype:attempted-user; sid:15434; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP csh access"; flow:to\_server,established; content:"/csh"; nocase; http\_uri; metadata:service http; reference:cve,1999-0509; reference:url,www.cert.org/advisories/CA-1996-11.html; classtype:attempted-recon; sid:862; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Advanced Poll admin\_comment.php access"; flow:to\_server,established; content:"/admin\_comment.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,8890; reference:nessus,11487; classtype:web-application-activity; sid:2287; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP files.pl access"; flow:to\_server,established; content:"/files.pl"; nocase; http\_uri; metadata:service http; reference:cve,1999-1081; classtype:attempted-recon; sid:851; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Advanced Poll admin\_stats.php access"; flow:to\_server,established; content:"/admin\_stats.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,8890; reference:nessus,11487; classtype:web-application-activity; sid:2296; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP processit access"; flow:to\_server,established; content:"/processit.pl"; nocase; http\_uri; metadata:service http; reference:nessus,10649; classtype:web-application-activity; sid:2668; rev:12;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP OpenView Network Node Manager cookie buffer overflow attempt"; flow:to\_server,established; content:"/OVCgi/OvHelp.exe"; fast\_pattern:only; http\_uri; pcre:"/(OvJavaScript|OvTitleFrame|OvHelpWindow|OvMap|OvSession|OvJavaLocale|OvOSLocale|OvLogin|OvDebug|OvDeveloper|OvTreeControl|OvJavaScript|OvProduct|OvPort|OvLocale|OvWebSession)\s\*\x3D[^\x3B\x2C]{1024}/iC"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,42154; reference:cve,2010-2709; classtype:attempted-user; sid:18920; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 25 (msg:"SERVER-WEBAPP truncated crypt function attempt"; flow:to\_server,established; file\_data; content:"crypt("; fast\_pattern:only; content:"<?"; pcre:"/((?P<m1>\$\w+)\s\*=\s\*(?P<q1>[\x22\x27])\s\*[^(?P=q1)]+(\\x80|\x80).\*?crypt\(\s\*(?P=m1)|crypt\(\s\*(?P<q2>[\x22\x27])\s\*[^(?P=q1)]+(\\x80|\x80))/smi"; metadata:policy security-ips drop, service smtp; reference:cve,2012-2143; classtype:attempted-admin; sid:23894; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP DCShop orders.txt access"; flow:to\_server,established; content:"/orders/orders.txt"; nocase; http\_uri; metadata:service http; reference:bugtraq,2889; reference:cve,2001-0821; classtype:web-application-activity; sid:1556; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP search.dll directory listing attempt"; flow:to\_server,established; content:"/search.dll"; http\_uri; content:"query=%00"; metadata:service http; reference:bugtraq,1684; reference:cve,2000-0835; reference:nessus,10514; classtype:web-application-attack; sid:1766; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP lyris.pl access"; flow:to\_server,established; content:"/lyris.pl"; http\_uri; metadata:service http; reference:bugtraq,1584; reference:cve,2000-0758; classtype:web-application-activity; sid:2072; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP awstats.pl configdir command execution attempt"; flow:to\_server,established; content:"/awstats.pl?"; fast\_pattern; nocase; http\_uri; content:"configdir="; nocase; http\_uri; pcre:"/awstats.pl?[^\r\n]\*configdir=\x7C/Ui"; metadata:service http; reference:bugtraq,12298; reference:cve,2005-0116; reference:nessus,16189; classtype:attempted-user; sid:3813; rev:11;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP OpenView NNM getnnmdata.exe CGI MaxAge parameter buffer overflow attempt"; flow:to\_server,established; content:"/OvCgi/getnnmdata|2E|exe"; fast\_pattern:only; http\_uri; content:"MaxAge|3D|"; nocase; isdataat:300,relative; pcre:"/MaxAge\x3D[^\x26\x3F\x3B\x0D\x0A]{300}/i"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:cve,2010-1553; classtype:attempted-user; sid:19139; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP webadmin.dll access"; flow:to\_server,established; content:"/webadmin.dll"; nocase; http\_uri; metadata:service http; reference:bugtraq,7438; reference:bugtraq,7439; reference:bugtraq,8024; reference:cve,2003-0471; reference:nessus,11771; classtype:web-application-activity; sid:2246; rev:12;)

#alert tcp $HOME\_NET any -> $EXTERNAL\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP SurgeMail webmail.exe page format string exploit attempt"; flow:to\_server,established; content:"/scripts/webmail.exe"; fast\_pattern:only; http\_uri; pcre:"/[\x26\x3f]page=[^\x26]\*?\x25/Ii"; metadata:service http; reference:bugtraq,27990; reference:cve,2008-1055; reference:url,aluigi.altervista.org/adv/surgemailz-adv.txt; reference:url,www.osvdb.org/42981; classtype:web-application-attack; sid:21609; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Cyboards default\_header.php access"; flow:to\_server,established; content:"/default\_header.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,6597; classtype:web-application-activity; sid:2363; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP wsh attempt"; flow:to\_server,established; content:"wsh.exe"; nocase; metadata:service http; classtype:web-application-activity; sid:1064; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP plusmail access"; flow:to\_server,established; content:"/plusmail"; nocase; http\_uri; metadata:service http; reference:bugtraq,2653; reference:cve,2000-0074; reference:nessus,10181; classtype:attempted-recon; sid:1217; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP miniBB rss.php premodDir remote file include attempt"; flow:to\_server,established; content:"rss.php"; nocase; http\_uri; content:"premodDir="; nocase; http\_uri; pcre:"/premodDir=(ftp|https?)/Ui"; metadata:policy security-ips drop, service http; reference:url,osvdb.org/show/osvdb/51460; classtype:web-application-attack; sid:18478; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Web Shopper shopper.cgi attempt"; flow:to\_server,established; content:"/shopper.cgi"; fast\_pattern; nocase; http\_uri; content:"newpage=../"; nocase; metadata:service http; reference:bugtraq,1776; reference:cve,2000-0922; reference:nessus,10533; classtype:web-application-attack; sid:1468; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP SIX webboard generate.cgi attempt"; flow:to\_server,established; content:"/generate.cgi"; http\_uri; content:"content=../"; metadata:service http; reference:bugtraq,3175; reference:cve,2001-1115; reference:nessus,10725; classtype:web-application-attack; sid:1494; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP bsml.pl access"; flow:to\_server,established; content:"/bsml.pl"; nocase; http\_uri; metadata:service http; reference:bugtraq,9311; reference:nessus,11973; classtype:web-application-activity; sid:2327; rev:8;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP talkback.cgi access"; flow:to\_server,established; content:"/talkbalk.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,2547; reference:cve,2001-0420; classtype:web-application-activity; sid:1720; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP ACal Calendar Project cookie based authentication bypass attempt"; flow:to\_server,established; content:"login.php"; nocase; http\_uri; content:"ACalAuthenticate|3D|inside"; nocase; http\_cookie; metadata:policy security-ips drop, service http; reference:cve,2006-0182; classtype:attempted-user; sid:20819; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cached\_feed.cgi moreover shopping cart access"; flow:to\_server,established; content:"/cached\_feed.cgi"; http\_uri; metadata:service http; reference:bugtraq,1762; reference:cve,2000-0906; classtype:web-application-activity; sid:2051; rev:9;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET [1521,5560] (msg:"SERVER-WEBAPP Oracle Database Server buffer overflow attempt"; flow:to\_server,established; content:"DBMS\_AQELM"; pcre:"/SET\_(SENDFROM|MAILHOST)\x28\x27[^\x27]{256}/i"; metadata:policy balanced-ips drop, policy security-ips drop; reference:bugtraq,30177; reference:cve,2008-2607; classtype:misc-attack; sid:13951; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP nph-test-cgi access"; flow:to\_server,established; content:"/nph-test-cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,686; reference:cve,1999-0045; reference:nessus,10165; classtype:attempted-recon; sid:829; rev:22;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP mrtg.cgi directory traversal attempt"; flow:to\_server,established; content:"/mrtg.cgi"; http\_uri; content:"cfg=/../"; metadata:service http; reference:bugtraq,4017; reference:cve,2002-0232; reference:nessus,11001; classtype:web-application-attack; sid:1862; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP amazon 1-click cookie theft"; flow:to\_server,established; content:"ref%3Cscript%20language%3D%22Javascript"; nocase; metadata:service http; reference:bugtraq,1194; reference:cve,2000-0439; classtype:web-application-attack; sid:1082; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP client negative Content-Length attempt"; flow:to\_server,established; content:"Content-Length|3A|"; nocase; byte\_test:10,>,0x7FFFFFFF,1,relative,string,dec; metadata:policy security-ips drop, service http; reference:bugtraq,16354; reference:bugtraq,17879; reference:bugtraq,9098; reference:bugtraq,9476; reference:bugtraq,9576; reference:cve,2004-0095; reference:cve,2005-3653; reference:cve,2006-2162; reference:cve,2006-3655; classtype:misc-attack; sid:2278; rev:24;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 383 (msg:"SERVER-WEBAPP HP Operations Agent stack buffer overflow attempt"; flow:to\_server,established; flowbits:isset,hp\_openview\_coda; content:"|00 00 00 AA|"; depth:4; offset:18; byte\_jump:2,16,relative; byte\_jump:2,0,relative; byte\_test:2,>,1024,0,relative; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,54362; reference:cve,2012-2019; reference:url,h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03397769; classtype:attempted-admin; sid:23960; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Cisco Catalyst command execution attempt"; flow:to\_server,established; content:"/exec/show/config/cr"; nocase; http\_uri; metadata:service http; reference:bugtraq,1846; reference:cve,2000-0945; reference:nessus,10545; classtype:web-application-activity; sid:1544; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Netscape Enterprise DOS"; flow:to\_server,established; content:"REVLOG / "; depth:9; metadata:service http; reference:bugtraq,2294; reference:cve,2001-0251; classtype:web-application-attack; sid:1047; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Ecommerce check.txt access"; flow:to\_server,established; content:"/config/check.txt"; nocase; http\_uri; metadata:service http; classtype:attempted-recon; sid:1124; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP AHG search.cgi access"; flow:to\_server,established; content:"/publisher/search.cgi"; fast\_pattern; nocase; http\_uri; content:"template="; nocase; metadata:service http; reference:bugtraq,3985; classtype:web-application-activity; sid:1405; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Devellion CubeCart searchStr parameter SQL injection"; flow:to\_server,established; content:"searchStr='"; fast\_pattern; http\_uri; content:"/index.php?"; nocase; http\_uri; metadata:service http; reference:url,www.acunetix.com/blog/web-security-zone/articles/sql-injection-xss-cubecart-4-3-3/; classtype:web-application-attack; sid:21271; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP CCBill whereami.cgi arbitrary command execution attempt"; flow:to\_server,established; content:"/whereami.cgi?g="; nocase; http\_uri; metadata:service http; reference:bugtraq,8095; reference:url,secunia.com/advisories/9191/; classtype:web-application-attack; sid:2396; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP /wwwboard/passwd.txt access"; flow:to\_server,established; content:"/wwwboard/passwd.txt"; nocase; http\_uri; metadata:service http; reference:bugtraq,649; reference:cve,1999-0953; reference:cve,1999-0954; reference:nessus,10321; classtype:attempted-recon; sid:807; rev:22;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP iPlanet GETPROPERTIES attempt"; flow:to\_server,established; content:"GETPROPERTIES"; depth:13; metadata:service http; reference:bugtraq,2732; reference:cve,2001-0746; classtype:web-application-attack; sid:1050; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP phpBB viewtopic double URL encoding attempt"; flow:to\_server,established; content:"viewtopic.php"; http\_uri; content:"highlight="; http\_uri; content:"%25"; metadata:service http; reference:cve,2004-1315; classtype:web-application-attack; sid:12610; rev:8;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cart 32 AdminPwd access"; flow:to\_server,established; content:"/c32web.exe/ChangeAdminPassword"; nocase; http\_uri; metadata:service http; reference:bugtraq,1153; reference:cve,2000-0429; classtype:attempted-recon; sid:1162; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP PhpGedView search.php access"; flow:to\_server,established; content:"/search.php"; nocase; http\_uri; content:"action=soundex"; fast\_pattern; nocase; http\_uri; content:"firstname="; nocase; http\_uri; metadata:service http; reference:bugtraq,9369; reference:cve,2004-0032; classtype:web-application-activity; sid:2345; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Emumail init.emu access"; flow:to\_server,established; content:"/init.emu"; nocase; http\_uri; metadata:service http; reference:bugtraq,9861; reference:nessus,12095; classtype:web-application-activity; sid:2567; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP MDaemon form2raw.cgi access"; flow:to\_server,established; content:"/form2raw.cgi"; fast\_pattern:only; metadata:service http; reference:bugtraq,9317; reference:cve,2003-1200; reference:url,secunia.com/advisories/10512/; classtype:web-application-activity; sid:2434; rev:10;)

#alert tcp $EXTERNAL\_NET $FILE\_DATA\_PORTS -> $HOME\_NET any (msg:"SERVER-WEBAPP PECL zip URL wrapper buffer overflow attempt"; flow:to\_client,established; file\_data; content:"|3C 3F|"; content:"php"; distance:0; nocase; content:"zip|3A 2F 2F|"; distance:0; pcre:"/zip\x3a\x2f\x2f[^\x0A\x20\x09\x0B\x0C\x85\x3E\x3C]{400}/i"; metadata:policy security-ips drop, service http, service imap, service pop3; reference:bugtraq,22883; reference:cve,2007-1399; reference:url,php-security.org/MOPB/MOPB-16-2007.html; classtype:attempted-user; sid:21671; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP bizdbsearch attempt"; flow:to\_server,established; content:"/bizdb1-search.cgi"; fast\_pattern; nocase; http\_uri; content:"mail"; nocase; metadata:service http; reference:bugtraq,1104; reference:cve,2000-0287; reference:nessus,10383; classtype:web-application-attack; sid:1185; rev:21;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP DNSTools access"; flow:to\_server,established; content:"/dnstools.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,4617; reference:cve,2002-0613; classtype:web-application-activity; sid:1741; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Visuplay CMS news\_article.php unspecified SQL injection attempt "; flow:to\_server,established; content:"news\_article|2E|php"; fast\_pattern; nocase; http\_uri; content:"press\_id|3D|"; nocase; pcre:"/press\_id\x3D\d+[^\&\r\n]/i"; metadata:service http; reference:bugtraq,33209; classtype:web-application-activity; sid:18586; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Domino cersvr.nsf access"; flow:to\_server,established; content:"/cersvr.nsf"; nocase; http\_uri; metadata:service http; reference:nessus,10629; classtype:attempted-recon; sid:1576; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP multidiff.cgi access"; flow:to\_server,established; content:"/multidiff.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,4579; reference:bugtraq,5517; reference:cve,2003-0153; reference:nessus,11748; classtype:web-application-activity; sid:2199; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP test.cgi access"; flow:to\_server,established; content:"/test.cgi"; nocase; http\_uri; metadata:service http; classtype:web-application-activity; sid:1646; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Nucleus CMS action.php itemid SQL injection"; flow:to\_server,established; content:"action.php"; fast\_pattern; nocase; http\_uri; content:"itemid="; nocase; pcre:"/itemid=\d\*[^\d\&\;\r\n]/i"; metadata:service http; reference:bugtraq,10798; reference:cve,2004-2056; reference:nessus,14194; classtype:web-application-activity; sid:3690; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 2401 (msg:"SERVER-WEBAPP CVS remote file information disclosure attempt"; flow:established,to\_server; content:"Argument -X"; content:"history"; distance:0; metadata:policy security-ips drop; reference:bugtraq,10955; reference:cve,2004-0788; classtype:attempted-recon; sid:23402; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ftp.pl access"; flow:to\_server,established; content:"/ftp.pl"; nocase; http\_uri; metadata:service http; reference:bugtraq,1471; reference:cve,2000-0674; reference:nessus,10467; classtype:web-application-activity; sid:1107; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Domino collect4.nsf access"; flow:to\_server,established; content:"/collect4.nsf"; nocase; http\_uri; metadata:service http; reference:nessus,10629; classtype:attempted-recon; sid:1582; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP DatabaseFunctions.php access"; flow:to\_server,established; content:"/DatabaseFunctions.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,9057; classtype:web-application-activity; sid:2283; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP /doc/packages access"; flow:to\_server,established; content:"/doc/packages"; nocase; http\_uri; metadata:service http; reference:bugtraq,1707; reference:cve,2000-1016; reference:nessus,10518; reference:nessus,11032; classtype:web-application-activity; sid:1559; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 9090 (msg:"SERVER-WEBAPP Jive Software Openfire server-properties.jsp XSS attempt"; flow:to\_server,established; content:"/server-properties.jsp"; fast\_pattern:only; http\_uri; pcre:"/server-properties\.jsp\?.\*?=([^\x26]\*[\x22\x27\x3C\x3E\x28\x29\x3B]|script|src|location|document)/U"; metadata:policy security-ips drop, service http; reference:bugtraq,32935; reference:cve,2009-0496; classtype:web-application-attack; sid:20867; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP websendmail access"; flow:to\_server,established; content:"/websendmail"; nocase; http\_uri; metadata:service http; reference:bugtraq,2077; reference:cve,1999-0196; reference:nessus,10301; classtype:attempted-recon; sid:815; rev:20;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cpshost.dll access"; flow:to\_server,established; content:"/scripts/cpshost.dll"; nocase; http\_uri; metadata:service http; reference:bugtraq,1811; reference:bugtraq,4002; reference:cve,1999-0360; classtype:attempted-recon; sid:1128; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP emumail.cgi access"; flow:to\_server,established; content:"/emumail.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,5824; reference:cve,2002-1526; classtype:web-application-activity; sid:1724; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP BLNews objects.inc.php4 access"; flow:to\_server,established; content:"/objects.inc.php4"; http\_uri; metadata:service http; reference:bugtraq,7677; reference:cve,2003-0394; reference:nessus,11647; classtype:web-application-activity; sid:2148; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP System variable directory traversal attempt - %USERDATA%"; flow:to\_server,established; content:"%USERDATA%"; fast\_pattern:only; http\_uri; metadata:service http; classtype:attempted-recon; sid:21833; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Twiki rdiff rev command injection attempt"; flow:to\_server,established; content:"/rdiff/"; nocase; http\_uri; content:"twiki"; distance:0; nocase; http\_uri; content:"|7C|"; distance:0; nocase; http\_uri; metadata:service http; reference:bugtraq,14834; reference:cve,2005-2877; classtype:attempted-admin; sid:4985; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Netscape Enterprise Server directory view"; flow:to\_server,established; content:"?wp-ver-info"; nocase; http\_uri; metadata:service http; reference:bugtraq,1063; reference:cve,2000-0236; classtype:attempted-recon; sid:1184; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS 7777 (msg:"SERVER-WEBAPP WhatsUpGold configuration access"; flow:to\_server,established; content:"/\_maincfgret.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,11043; reference:cve,2004-0798; classtype:web-application-activity; sid:12057; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Lotus Domino directory traversal"; flow:to\_server,established; content:".nsf/"; http\_uri; content:"../"; nocase; http\_uri; metadata:service http; reference:bugtraq,2173; reference:cve,2001-0009; reference:nessus,12248; classtype:web-application-attack; sid:1072; rev:17;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP OpenView NNM snmpviewer.exe CGI parameter buffer overflow attempt"; flow:to\_server,established; content:"/OvCgi/snmpviewer|2E|exe"; fast\_pattern:only; http\_uri; content:"app|3D|"; nocase; isdataat:300,relative; content:"act|3D|"; nocase; isdataat:300,relative; pcre:"/act\x3D[^\x26\x3F\x3B\x0D\x0A]{300}/i"; pcre:"/app\x3D[^\x26\x3F\x3B\x0D\x0A]{300}/i"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:cve,2010-1552; classtype:attempted-user; sid:19140; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Sourceforge Gallery search engine cross-site scripting attempt"; flow:to\_server,established; content:"search.php?"; nocase; http\_uri; content:"<script>"; within:25; nocase; http\_uri; metadata:service http; reference:cve,2003-0614; reference:url,secunia.com/advisories/9376/; reference:url,www.securityfocus.com/bid/8288; classtype:attempted-admin; sid:20674; rev:3;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP OpenView Network Node Manager nnmRptConfig.exe multiple parameters buffer overflow attempt"; flow:to\_server,established; content:"nnmRptConfig.exe"; fast\_pattern:only; http\_uri; pcre:"/(data\_select1|nameParams|schdParams|text1|schd\_select1)=[^\x26]{512}/iU"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,45762; reference:cve,2011-0265; reference:cve,2011-0266; reference:cve,2011-0267; reference:cve,2011-0268; reference:cve,2011-0269; reference:url,osvdb.org/show/osvdb/70473; classtype:attempted-user; sid:24147; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Lotus Notes .csp script source download attempt"; flow:to\_server,established; content:".csp."; http\_uri; metadata:service http; classtype:web-application-attack; sid:2065; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP SGI InfoSearch fname attempt"; flow:to\_server,established; content:"/infosrch.cgi?"; fast\_pattern; nocase; http\_uri; content:"fname="; nocase; metadata:service http; reference:bugtraq,1031; reference:cve,2000-0207; reference:nessus,10128; classtype:web-application-attack; sid:1196; rev:21;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP inTouch SQL injection in index.php user attempt"; flow:to\_server,established; content:"index.php"; fast\_pattern:only; http\_uri; content:"user"; nocase; http\_uri; pcre:"/user=[^\r\n\x26]\*?([\x22\x27]|%2[27])/Ui"; metadata:service http; reference:bugtraq,16110; reference:cve,2006-0088; classtype:web-application-attack; sid:20647; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Symantec IM Manager Edituser cross site scripting attempt"; flow:to\_server,established; content:"/IMManager/Admin/IMAdminEdituser.asp"; nocase; http\_uri; content:"action="; distance:0; nocase; http\_uri; pcre:"/action=[^\x26\s]\*[\x3e\x3d\x26]/Ui"; metadata:service http; reference:bugtraq,49739; reference:cve,2011-0552; reference:url,osvdb.org/75981; classtype:attempted-user; sid:21065; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP IBM Lotus Domino cross site scripting attempt"; flow:established,to\_server; content:"/CitiPayPro.nsf"; fast\_pattern:only; http\_uri; pcre:"/[?&]BaseTarget=[^&]+?([\x22\x27\x3c\x3e\x28\x29]|script|onload|src)/Ui"; metadata:policy security-ips drop, service http; reference:bugtraq,14845; reference:cve,2005-3015; classtype:web-application-attack; sid:23433; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP mailview.cgi access"; flow:to\_server,established; content:"/mailview.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,1335; reference:bugtraq,4579; reference:cve,2000-0526; reference:nessus,11748; classtype:web-application-activity; sid:2214; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS 80 (msg:"SERVER-WEBAPP sphpblog install03\_cgi access attempt"; flow:to\_server,established; content:"sphpblog"; http\_uri; content:"install03\_cgi.php"; fast\_pattern; nocase; http\_uri; metadata:service http; reference:bugtraq,14667; reference:cve,2005-2733; classtype:attempted-user; sid:11665; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP xp\_regdeletekey attempt"; flow:to\_server,established; content:"xp\_regdeletekey"; nocase; metadata:service http; classtype:web-application-activity; sid:1978; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Sage SalesLogix admin authentication bypass attempt"; flow:to\_server,established; content:"teams=ADMIN!"; fast\_pattern:only; content:"slxweb=user=Admin"; nocase; http\_cookie; content:"teams=ADMIN!"; nocase; http\_cookie; content:"usertype=Administrator"; nocase; http\_cookie; metadata:service http; reference:bugtraq,11450; reference:cve,2004-1612; classtype:attempted-admin; sid:20617; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP db4web\_c directory traversal attempt"; flow:to\_server,established; content:"/db4web\_c"; nocase; http\_uri; pcre:"/db4web\_c(\.exe)?\/.\*(\.\.[\\\/]|[a-z]\:)/smiU"; metadata:service http; reference:bugtraq,5723; reference:cve,2002-1483; reference:nessus,11182; classtype:web-application-attack; sid:3674; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP file upload GLOBAL variable overwrite attempt"; flow:to\_server,established; content:"Content-Type|3A| multipart/form-data"; nocase; http\_header; content:"name="; nocase; content:"GLOBALS"; within:7; distance:1; metadata:service http; reference:bugtraq,15250; reference:cve,2005-3390; classtype:web-application-attack; sid:12221; rev:8;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Oracle Java Web Server Webdav Stack Buffer Overflow attempt"; flow:to\_server,established; content:"PROPFIND"; depth:8; nocase; isdataat:200,relative; pcre:"/^PROPFIND\s+[^\s]{200}/smi"; metadata:policy security-ips drop, service http; reference:bugtraq,37874; reference:cve,2003-0109; reference:cve,2010-0361; classtype:attempted-admin; sid:18612; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Advanced Poll admin\_tpl\_new.php access"; flow:to\_server,established; content:"/admin\_tpl\_new.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,8890; reference:nessus,11487; classtype:web-application-activity; sid:2300; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP RFC1867 file-upload implementation denial of service attempt"; flow:to\_server,established; content:"POST"; http\_method; content:"|0A|Content-Disposition|3A|"; fast\_pattern:only; http\_client\_body; pcre:"/\nContent-Disposition\x3a[^\n]\*?name\s\*=\s\*(?P<quote>[\x22\x27]).\*?\[(?P=quote)\x3b/Pims"; metadata:policy security-ips drop, service http; reference:cve,2012-1172; classtype:attempted-dos; sid:24093; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP phpBB mod shoutbox sql injection attempt"; flow:to\_server,established; content:"shoutbox\_view.php"; fast\_pattern; nocase; http\_uri; content:"mode="; nocase; http\_uri; content:"id="; nocase; http\_uri; pcre:"/shoutbox\_view\.php\x3F[^\r\n]\*mode\s\*=\s\*(delete|edit)[^\r\n]\*id\s\*=\s\*[^\r\n\x26]\*[^\d]+/Usmi"; metadata:policy security-ips alert, service http; reference:bugtraq,32123; reference:cve,2008-6301; classtype:web-application-attack; sid:15424; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP book.cgi access"; flow:to\_server,established; content:"/book.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,3178; reference:cve,2001-1114; reference:nessus,10721; classtype:web-application-activity; sid:1472; rev:19;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Allaire Pro Web Shell attempt"; flow:to\_server,established; content:"/authenticate.cgi?PASSWORD"; fast\_pattern; nocase; http\_uri; content:"config.ini"; metadata:service http; classtype:web-application-attack; sid:1090; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP content-disposition file upload attempt"; flow:to\_server,established; content:"Content-Disposition|3A|"; nocase; http\_header; content:"form-data|3B|"; fast\_pattern:only; metadata:service http; reference:bugtraq,4183; reference:cve,2002-0081; reference:nessus,10867; classtype:web-application-attack; sid:1425; rev:21;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP b2 cafelog gm-2-b2.php remote file include attempt"; flow:to\_server,established; content:"/gm-2-b2.php"; fast\_pattern; nocase; http\_uri; content:"b2inc="; pcre:"/b2inc=(https?|ftps?|php)/i"; metadata:service http; reference:nessus,11667; classtype:web-application-attack; sid:2143; rev:13;)

#alert tcp $EXTERNAL\_NET $FILE\_DATA\_PORTS -> $HOME\_NET any (msg:"SERVER-WEBAPP calendar conversion remote integer overflow attempt"; flow:to\_client,established; file\_data; content:"cal\_from\_jd"; fast\_pattern:only; pcre:"/cal\_from\_jd\x28\s\*\d{9,}/mi"; metadata:policy security-ips drop, service http, service imap, service pop3; reference:bugtraq,46967; reference:cve,2011-1466; classtype:attempted-user; sid:23975; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 389 (msg:"SERVER-WEBAPP OpenLDAP Modrdn utf-8 string code execution attempt"; flow:to\_server, established; content:"|30|"; depth:1; content:"|6C|"; within:20; content:"cn="; pcre:"/cn=[^\x00]\*\x23[^\x00]\*\x01\x01\x00/i"; metadata:policy security-ips drop, service ldap; reference:bugtraq,41770; reference:cve,2010-0211; classtype:attempted-admin; sid:18804; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP philboard\_admin.asp authentication bypass attempt"; flow:to\_server,established; content:"/philboard\_admin.asp"; http\_uri; content:"Cookie"; nocase; content:"philboard\_admin=True"; distance:0; metadata:service http; reference:bugtraq,7739; reference:nessus,11675; classtype:web-application-attack; sid:2136; rev:8;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 383 (msg:"SERVER-WEBAPP HP Operations Agent stack buffer overflow attempt"; flow:to\_server,established; flowbits:isset,hp\_openview\_coda; content:"|00 00 00 78|"; depth:4; offset:18; byte\_jump:2,12,relative; byte\_jump:2,0,relative; byte\_test:2,>,1024,0,relative; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,54362; reference:cve,2012-2019; reference:url,h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03397769; classtype:attempted-admin; sid:24315; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS 1220 (msg:"SERVER-WEBAPP streaming server view\_broadcast.cgi access"; flow:to\_server,established; content:"/view\_broadcast.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,8257; reference:cve,2003-0422; classtype:web-application-activity; sid:2388; rev:14;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Novell ZENworks Configuration Management UploadServlet code execution attempt"; flow:to\_server,established; content:"/zenworks/UploadServlet"; fast\_pattern; nocase; http\_uri; content:"filename="; nocase; pcre:"/^[^\x26]\*?\x2E\x2E/R"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,39914; reference:url,www.novell.com/support/viewContent.do?externalId=7005573; classtype:attempted-admin; sid:18792; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Trend Micro Control Manager Chunked overflow attempt"; flow:to\_server,established; isdataat:1420; content:"isaNVWRequest.dll"; nocase; http\_uri; content:"Transfer-Encoding|3A|"; nocase; http\_header; content:"chunked"; nocase; http\_header; metadata:policy security-ips drop, service http; reference:bugtraq,15865; reference:cve,2005-1929; classtype:attempted-admin; sid:17486; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP www-sql access"; flow:to\_server,established; content:"/www-sql"; nocase; http\_uri; metadata:service http; reference:url,marc.theaimsgroup.com/?l=bugtraq&m=88704258804054&w=2; classtype:attempted-recon; sid:887; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP empty zip file upload attempt"; flow:to\_server,established; content:"|50 4B 05 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00|"; fast\_pattern:only; metadata:service http; reference:bugtraq,46354; reference:cve,2011-0421; classtype:denial-of-service; sid:23944; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cybercop scan"; flow:to\_server,established; content:"/cybercop"; nocase; http\_uri; metadata:service http; classtype:web-application-activity; sid:1099; rev:13;)

alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP zend\_strndup null pointer dereference attempt"; flow:to\_server,established; content:"define|28|"; nocase; content:"str\_repeat|28|"; fast\_pattern:only; pcre:"/<\?(php)?.{1,256}define\s\*\x28\s\*str\_repeat\s\*\x28\s\*[\x22\x27][^\x22\x27]+[\x22\x27]\s\*\x2c\s\*\x24argv/ims"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:cve,2011-4153; classtype:attempted-dos; sid:23994; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS 443 (msg:"SERVER-WEBAPP SSLv2 Client\_Hello Challenge Length overflow attempt"; flow:to\_server,established; ssl\_version:sslv2; ssl\_state:client\_hello; content:"|01 00 02|"; depth:3; offset:2; byte\_test:1,>,127,0; byte\_test:2,>,32,9; metadata:service ssl; reference:bugtraq,11015; reference:cve,2004-0826; classtype:attempted-admin; sid:2656; rev:19;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ROADS search.pl attempt"; flow:to\_server,established; content:"/ROADS/cgi-bin/search.pl"; http\_uri; content:"form="; nocase; metadata:service http; reference:bugtraq,2371; reference:cve,2001-0215; reference:nessus,10627; classtype:attempted-recon; sid:1224; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP view-source access"; flow:to\_server,established; content:"/view-source"; nocase; http\_uri; metadata:service http; reference:bugtraq,2251; reference:bugtraq,8883; reference:cve,1999-0174; classtype:attempted-recon; sid:849; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP bad HTTP/1.1 request, Potentially worm attack"; flow:to\_server,established; content:"GET / HTTP/1.1|0D 0A 0D 0A|"; depth:18; metadata:service http; reference:url,securityresponse.symantec.com/avcenter/security/Content/2002.09.13.html; classtype:web-application-activity; sid:1881; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP tstisapi.dll access"; flow:to\_server,established; content:"tstisapi.dll"; nocase; http\_uri; metadata:service http; reference:bugtraq,2381; reference:cve,2001-0302; classtype:attempted-recon; sid:902; rev:19;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP info2www access"; flow:to\_server,established; content:"/info2www"; nocase; http\_uri; metadata:service http; reference:bugtraq,1995; reference:cve,1999-0266; reference:nessus,10127; classtype:attempted-recon; sid:827; rev:19;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP awstats access"; flow:to\_server,established; content:"/awstats.pl"; nocase; http\_uri; metadata:service http; reference:bugtraq,12572; reference:nessus,16456; classtype:web-application-activity; sid:3463; rev:12;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP OpenView NNM ovlogin.exe CGI passwd parameter buffer overflow attempt"; flow:to\_server,established; content:"/OvCgi/ovlogin|2E|exe"; fast\_pattern:only; http\_uri; content:"passwd|3D|"; nocase; http\_client\_body; isdataat:29,relative; pcre:"/passwd\x3D[^\x26\x3F\x3B\x0D\x0A]{29}/iP"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:cve,2009-3846; reference:url,h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01950877; classtype:attempted-user; sid:20180; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP newdesk access"; flow:to\_server,established; content:"/newdesk"; nocase; http\_uri; metadata:service http; classtype:web-application-activity; sid:1714; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP OpenView NNM webappmon.exe buffer overflow attempt"; flow:to\_server,established; content:"/OVCgi/webappmon.exe"; nocase; http\_uri; content:"&sel="; distance:0; nocase; isdataat:1023,relative; content:!"|0D|"; within:1023; metadata:service http; reference:bugtraq,41829; reference:cve,2010-2703; classtype:attempted-user; sid:18999; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Basic Authorization string overflow attempt"; flow:to\_server,established; content:"Authorization|3A|"; pcre:"/^Authorization\x3a(\s\*|\s\*\r?\n\s+)Basic\s[^\n]{512}/smi"; metadata:policy security-ips drop, service http; reference:bugtraq,3230; reference:bugtraq,8375; reference:cve,2001-1067; reference:cve,2003-0727; classtype:attempted-dos; sid:16681; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP envout.bat arbitrary command execution attempt"; flow:to\_server,established; content:"/envout.bat|7C|"; http\_uri; metadata:service http; reference:bugtraq,762; reference:cve,1999-0947; reference:nessus,10016; classtype:web-application-attack; sid:1516; rev:16;)

#alert tcp $HOME\_NET any -> $EXTERNAL\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP PHP use-after-free in substr\_replace attempt"; flow:to\_server,established; content:"substr\_replace("; fast\_pattern:only; http\_client\_body; content:"<?"; http\_client\_body; pcre:"/substr\_replace\((\s\*\$\w+\s\*,\s\*){3,}.\*?\)\x3b/Psmi"; metadata:service http; reference:cve,2011-1148; classtype:misc-activity; sid:23792; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP robots.txt access"; flow:to\_server,established; content:"/robots.txt"; nocase; http\_uri; metadata:service http; reference:nessus,10302; classtype:web-application-activity; sid:1852; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Symantec IM Manager Administrator console site injection attempt"; flow:to\_server,established; content:"POST"; nocase; http\_method; content:"/IMMAnager/User/IMUserEditKeywordAction.asp?action="; nocase; http\_uri; content:"KeywordValue="; http\_client\_body; pcre:"/KeywordValue=[^\x26\s]\*[\x2F\x5C\x5E\x24\x2A\x2B\x3F\x28\x29\x2E\x7C\x5B\x5D\x7E\x3E\x3C]/iP"; metadata:service http; reference:cve,2011-0554; classtype:attempted-user; sid:21060; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP System variable directory traversal attempt - %HOMEDRIVE%"; flow:to\_server,established; content:"%HOMEDRIVE%"; fast\_pattern:only; http\_uri; metadata:service http; classtype:attempted-recon; sid:21824; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP bb-rep.sh access"; flow:to\_server,established; content:"/bb-rep.sh"; nocase; http\_uri; metadata:service http; reference:bugtraq,142; reference:cve,1999-1462; classtype:attempted-recon; sid:1461; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Phorum read access"; flow:to\_server,established; content:"/read.php3"; nocase; http\_uri; metadata:service http; classtype:attempted-recon; sid:1178; rev:17;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Adobe ColdFusion locale directory traversal attempt"; flow:to\_server,established; content:"CFIDE"; fast\_pattern; http\_uri; content:"locale="; nocase; content:"../../../"; distance:0; content:"%00"; distance:0; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,42342; reference:cve,2010-2861; classtype:attempted-admin; sid:18464; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Cisco /%% DOS attempt"; flow:to\_server,established; content:"/%%"; metadata:service http; reference:bugtraq,1154; reference:cve,2000-0380; reference:nessus,10387; classtype:web-application-attack; sid:1546; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP glimpse access"; flow:to\_server,established; content:"/glimpse"; nocase; http\_uri; metadata:service http; reference:bugtraq,2026; reference:cve,1999-0147; reference:nessus,10095; classtype:attempted-recon; sid:825; rev:19;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP remote include path"; flow:to\_server,established; content:".php"; nocase; http\_uri; content:"path="; fast\_pattern:only; pcre:"/path=(https?|ftps?|php)/i"; metadata:service http; classtype:web-application-attack; sid:2002; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP tftp attempt"; flow:to\_server,established; content:"tftp.exe"; nocase; metadata:service http; classtype:web-application-activity; sid:1068; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Allaire JRUN DOS attempt"; flow:to\_server,established; content:"servlet/......."; nocase; http\_uri; metadata:service http; reference:bugtraq,2337; reference:cve,2000-1049; classtype:web-application-attack; sid:1084; rev:16;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP D-Link Wireless Router CAPTCHA data processing buffer overflow attempt"; flow:to\_server,established; content:"POST"; http\_method; content:"/goform/formLogin"; fast\_pattern:only; http\_uri; content:"FILECODE="; nocase; http\_client\_body; isdataat:96,relative; pcre:"/FILECODE=[^&]{96}/iP"; metadata:policy balanced-ips alert, policy security-ips drop, service http; reference:url,websecuritywatch.com/d-link-wireless-n300-cloud-router-captcha-processing-buffer-overflow-vulnerability; classtype:attempted-admin; sid:24647; rev:1;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Oracle Java System Web Server 7.0u7 authorization digest heap overflow"; flow:to\_server,established; content:!"GET"; nocase; http\_method; content:!"POST"; nocase; http\_method; content:"Authorization"; nocase; content:"Digest"; distance:0; fast\_pattern; nocase; pcre:"/^Authorization\s\*\x3A\s\*Digest\s+([^\n\x2C]\*\x2C){15}/im"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,37896; reference:cve,2010-0387; classtype:attempted-user; sid:16392; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP pfdispaly.cgi access"; flow:to\_server,established; content:"/pfdispaly.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,64; reference:cve,1999-0270; reference:nessus,10174; classtype:web-application-activity; sid:1656; rev:17;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Joomla Remote File Include upload attempt"; flow:to\_server,established; content:"POST"; http\_method; content:"/admin/addcontent.inc.php"; fast\_pattern:only; http\_uri; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:url,stopmalvertising.com/security/95.211.20.103-local-file-inclusion-attack.html; reference:url,www.mmleoni.net/sql-iniection-lfi-protection-plugin-for-joomla; classtype:attempted-user; sid:23828; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 8080 (msg:"SERVER-WEBAPP Squid content length cache poisoning attempt"; flow:to\_server,established; content:"Content-Length|3A|"; nocase; http\_header; content:"Content-Length|3A|"; nocase; http\_header; pcre:"/^Content-Length\x3a(?!\x0d\x0a\x0d\x0a).\*?^Content-Length\x3a/smiH"; metadata:service http; reference:bugtraq,12412; reference:bugtraq,13956; reference:cve,2005-0174; reference:cve,2005-1215; classtype:misc-attack; sid:3694; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 749 (msg:"SERVER-WEBAPP MIT Kerberos V% KAdminD klog\_vsyslog server overflow attempt"; flow:to\_server,established; content:"|90|D|FA A0 B1|^C|07|m'|1C|m|08 02 D0 C7 C0|q|EE|q|E3|R|B3 1C|}K|DE D2 C1 F8 5C|{"; fast\_pattern:only; metadata:policy security-ips drop; reference:bugtraq,23285; reference:cve,2007-0957; classtype:attempted-user; sid:16207; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP DCShop auth\_user\_file.txt access"; flow:to\_server,established; content:"/auth\_data/auth\_user\_file.txt"; nocase; http\_uri; metadata:service http; reference:bugtraq,2889; reference:cve,2001-0821; classtype:web-application-activity; sid:1557; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Twiki viewfile rev command injection attempt"; flow:to\_server,established; content:"/viewfile/"; nocase; http\_uri; content:"twiki"; distance:0; nocase; http\_uri; content:"|7C|"; distance:0; nocase; http\_uri; metadata:service http; reference:bugtraq,14834; reference:cve,2005-2877; classtype:attempted-admin; sid:4987; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP TRACE attempt"; flow:to\_server,established; content:"TRACE"; depth:5; metadata:service http; reference:bugtraq,9561; reference:cve,2003-1567; reference:cve,2004-2320; reference:cve,2010-0360; reference:nessus,11213; classtype:web-application-attack; sid:2056; rev:9;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP Power Manager remote code execution attempt"; flow:to\_server,established; content:"/goform/formLogin"; fast\_pattern:only; http\_uri; content:"Login="; nocase; http\_client\_body; isdataat:51; pcre:"/^[^\x26\x3b]{51}/R"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,36933; reference:cve,2009-2685; reference:cve,2010-4113; classtype:attempted-admin; sid:19826; rev:4;)

#alert tcp $EXTERNAL\_NET $HTTP\_PORTS -> $HOME\_NET any (msg:"SERVER-WEBAPP uTorrent announce buffer overflow attempt"; flow:to\_client,established; file\_data; content:"d8|3A|announce"; nocase; pcre:"/^(\d{5,}|390[1-9]|39[1-9][0-9]|[4-9][0-9]{3})\x3A/R"; metadata:service http; reference:bugtraq,22530; reference:cve,2007-0927; classtype:attempted-user; sid:10172; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Advanced Poll admin\_settings.php access"; flow:to\_server,established; content:"/admin\_settings.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,8890; reference:nessus,11487; classtype:web-application-activity; sid:2295; rev:14;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 38292 (msg:"SERVER-WEBAPP Symantec Alert Management System modem string buffer overflow attempt"; flow:to\_server,established; content:"|FF FF FF FF|"; depth:4; content:"PAGE"; depth:4; offset:30; content:"ModemString|00|"; distance:0; byte\_test:2,>,32,0,relative,little; metadata:policy balanced-ips drop, policy security-ips drop; reference:cve,2010-0110; reference:url,www.symantec.com/business/security\_response/securityupdates/detail.jsp?fid=security\_advisory&pvid=security\_advisory&year=2011&suid=20110126\_00; classtype:attempted-user; sid:19209; rev:2;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Oracle Virtual Server Agent command injection attempt"; flow:to\_server,established; content:"/RPC2"; fast\_pattern; nocase; http\_uri; content:"<?xml"; http\_client\_body; content:"params"; distance:0; pcre:"/\x3C\s\*param\s\*\x3E\s\*\x3C\s\*value\s\*\x3E\s\*\x3C\s\*string\s\*\x3E[^\x3C]\*[\x2C\x3B]/smiR"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,44031; reference:cve,2010-3582; classtype:attempted-admin; sid:19441; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Ruby on Rails SQL injection attempt"; flow:to\_server,established; content:"[mysql where "; http\_uri; metadata:service http; reference:cve,2012-2661; classtype:web-application-attack; sid:23216; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP /home/www access"; flow:to\_server,established; content:"/home/www"; nocase; http\_uri; metadata:service http; reference:nessus,11032; classtype:web-application-activity; sid:1671; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP System variable in URI attempt - %PATH%"; flow:to\_server,established; content:"%PATH%"; fast\_pattern:only; http\_uri; metadata:service http; classtype:attempted-recon; sid:21841; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP basilix sendmail.inc access"; flow:to\_server,established; content:"/inc/sendmail.inc"; http\_uri; metadata:service http; reference:bugtraq,2198; reference:cve,2001-1044; reference:nessus,10601; classtype:web-application-activity; sid:1526; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP UpdateClasses.php access"; flow:to\_server,established; content:"/UpdateClasses.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,9057; classtype:web-application-activity; sid:2279; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Mambo uploadimage.php access"; flow:to\_server,established; content:"/uploadimage.php"; http\_uri; metadata:service http; reference:bugtraq,6572; reference:cve,2003-1204; reference:nessus,16315; classtype:web-application-activity; sid:2076; rev:9;)

#alert tcp $EXTERNAL\_NET $FILE\_DATA\_PORTS -> $HOME\_NET any (msg:"SERVER-WEBAPP calendar conversion remote integer overflow attempt"; flow:to\_client,established; file\_data; content:"cal\_from\_jd"; fast\_pattern:only; pcre:"/\x24(?P<var>\w\*)\s\*=\s\*(rand\x28\d\x2c\s\*\d{9,}|\d{9,}).\*?cal\_from\_jd\x28\s\*\x24(?P=var)/smi"; metadata:policy security-ips drop, service http, service imap, service pop3; reference:bugtraq,46967; reference:cve,2011-1466; classtype:attempted-user; sid:23974; rev:2;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP OpenView Network Node Manager cookie buffer overflow attempt"; flow:to\_server,established; content:"/OVCgi/Toolbar.exe"; fast\_pattern:only; http\_uri; pcre:"/(OvJavaScript|OvTitleFrame|OvHelpWindow|OvMap|OvSession|OvJavaLocale|OvOSLocale|OvLogin|OvDebug|OvDeveloper|OvTreeControl|OvJavaScript|OvProduct|OvPort|OvLocale|OvWebSession)\s\*\x3D[^\x3B\x2C]{1024}/iC"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,42154; reference:cve,2010-2709; classtype:attempted-user; sid:18925; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP globals.jsa access"; flow:to\_server,established; content:"/globals.jsa"; http\_uri; metadata:service http; reference:bugtraq,4034; reference:cve,2002-0562; reference:nessus,10850; classtype:web-application-activity; sid:1873; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Admin\_files access"; flow:to\_server,established; content:"/admin\_files"; nocase; http\_uri; metadata:service http; classtype:attempted-recon; sid:1212; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP uploader.exe access"; flow:to\_server,established; content:"/uploader.exe"; nocase; http\_uri; metadata:service http; reference:bugtraq,1611; reference:cve,1999-0177; reference:cve,2000-0769; reference:nessus,10291; classtype:attempted-recon; sid:837; rev:20;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP calendar.php access"; flow:to\_server,established; content:"/calendar.php"; http\_uri; metadata:service http; reference:bugtraq,5820; reference:bugtraq,9353; reference:nessus,11179; classtype:web-application-activity; sid:1998; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 8004 (msg:"SERVER-WEBAPP Symantec Antivirus admin scan interface negative Content-Length attempt"; flow:to\_server,established; content:"Content-Length|3A| 4294967295"; fast\_pattern:only; reference:bugtraq,15001; reference:cve,2005-2758; classtype:attempted-admin; sid:21233; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Benders Calendar SQL injection in index.php this\_day attempt"; flow:to\_server,established; content:"index.php"; fast\_pattern:only; http\_uri; content:"this\_day"; nocase; pcre:"/this\_day=[^\r\n\x26]\*?([\x22\x27]|%2[27])/i"; metadata:service http; reference:bugtraq,16242; reference:cve,2006-0252; classtype:web-application-attack; sid:20646; rev:6;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET [8008,8010,8028,8030] (msg:"SERVER-WEBAPP Novell eDirectory HTTP request content-length heap buffer overflow attempt"; flow:to\_server,established; content:"POST /SOAP"; depth:10; nocase; pcre:"/^Content-Length\s\*\x3A\s/mi"; content:"-"; within:1; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:cve,2008-4478; classtype:attempted-user; sid:16195; rev:6;)

alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP LOCK Webdav Stack Buffer Overflow attempt"; flow:to\_server,established; content:"LOCK"; depth:4; nocase; isdataat:200,relative; pcre:"/^LOCK\s+[^\s]{200}/smi"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,37874; reference:cve,2010-0361; classtype:attempted-admin; sid:21235; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP bb-histsvc.sh access"; flow:to\_server,established; content:"/bb-histsvc.sh"; nocase; http\_uri; metadata:service http; reference:bugtraq,142; reference:cve,1999-1462; classtype:attempted-recon; sid:1460; rev:15;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 8080 (msg:"SERVER-WEBAPP Jboss default configuration unauthorized application add attempt"; flow:to\_server,established; content:"/jmx-console/HtmlAdaptor?"; nocase; http\_uri; content:"action=inspectMBean"; nocase; http\_uri; content:"name=jboss.deployment|3A|type=DeploymentScanner,flavor=URL"; nocase; http\_uri; content:"addURL|28|"; nocase; metadata:policy balanced-ips drop, policy connectivity-ips drop, policy security-ips drop, service http; reference:url,www.nruns.com/\_downloads/Whitepaper-Hacking-jBoss-using-a-Browser.pdf; classtype:web-application-attack; sid:18932; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP ME Download System remote file include in header.php Vb8878b936c2bd8ae0cab"; flow:to\_server,established; content:"header.php"; fast\_pattern:only; http\_uri; content:"Vb8878b936c2bd8ae0cab="; nocase; pcre:"/Vb8878b936c2bd8ae0cab=(https?|ftps?)/i"; metadata:service http; reference:bugtraq,19336; reference:cve,2006-4053; classtype:web-application-attack; sid:20652; rev:6;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP OpenView Network Node Manager ovalarm.exe Accept-Language buffer overflow attempt"; flow:to\_server,established; content:"/OVCgi/ovalarm.exe"; nocase; http\_uri; content:"OVABverbose="; nocase; pcre:"/^(?!false|off|no|0)/iR"; pcre:"/(OvAcceptLang|Accept-Language)\s\*[\x3D\x3A]\s\*[^\n]{69}/i"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,37261; reference:cve,2009-4179; classtype:attempted-user; sid:16604; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $SMTP\_SERVERS 25 (msg:"SERVER-WEBAPP use-after-free in substr\_replace attempt"; flow:to\_server,established; file\_data; content:"substr\_replace("; fast\_pattern:only; content:"<?"; pcre:"/substr\_replace\((\s\*\$\w+\s\*,\s\*){3,}.\*?\)\x3b/smi"; metadata:service smtp; reference:cve,2011-1148; classtype:misc-activity; sid:23793; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP album.pl access"; flow:to\_server,established; content:"/album.pl"; fast\_pattern:only; metadata:service http; reference:bugtraq,7444; reference:nessus,11581; classtype:web-application-activity; sid:2115; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Vmist Downstat remote file include in chart.php art"; flow:to\_server,established; content:"downstat"; nocase; http\_uri; content:"chart.php"; nocase; http\_uri; content:"art="; nocase; http\_uri; pcre:"/\x2Fchart\.php\x3F[^\r\n]\*?art\x3Dhttp\x3A\x2F/Ui"; metadata:service http; reference:bugtraq,20007; reference:cve,2006-4827; classtype:web-application-activity; sid:20815; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP HyperSeek hsx.cgi directory traversal attempt"; flow:to\_server,established; content:"/hsx.cgi"; http\_uri; content:"../../"; content:"%00"; distance:1; metadata:service http; reference:bugtraq,2314; reference:cve,2001-0253; reference:nessus,10602; classtype:web-application-attack; sid:803; rev:19;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Domino names.nsf access"; flow:to\_server,established; content:"/names.nsf"; nocase; http\_uri; metadata:service http; reference:nessus,10629; classtype:attempted-recon; sid:1154; rev:13;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP CA Total Defense management.asmx sql injection attempt"; flow:to\_server,established; content:"POST"; http\_method; content:"/UNCWS/Management.asmx"; fast\_pattern:only; http\_uri; content:"SOAP"; nocase; http\_header; pcre:"/<SelectedID>[^<]+?(\x3B|%3B)/miP"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,47355; reference:url,support.ca.com/irj/portal/anonymous/phpsupcontent?contentID={CD065CEC-AFE2-4D9D-8E0B-BE7F6E345866}; classtype:attempted-admin; sid:24705; rev:1;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Invision Power Board search.pl access"; flow:to\_server,established; content:"/search.pl"; http\_uri; content:"st="; nocase; metadata:service http; reference:bugtraq,9766; classtype:web-application-activity; sid:2408; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP /etc/passwd file access attempt"; flow:to\_server,established; content:"/etc/passwd"; fast\_pattern:only; nocase; http\_uri; metadata:service http; classtype:attempted-recon; sid:1122; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ads.cgi command execution attempt"; flow:to\_server,established; content:"/ads.cgi"; fast\_pattern; nocase; http\_uri; content:"file="; nocase; content:"../../"; content:"|7C|"; metadata:service http; reference:bugtraq,2103; reference:cve,2001-0025; reference:nessus,11464; classtype:web-application-attack; sid:1053; rev:21;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP file upload directory traversal"; flow:to\_server,established; content:"POST"; http\_method; content:"upload.php"; fast\_pattern; nocase; http\_uri; pcre:"/^Content-Type\x3A\s+multipart\/form-data/smiH"; content:"Content-Disposition|3A|"; nocase; http\_header; pcre:"/filename=\S\*\x2e\x2e\x2f/smiH"; content:"|0A|"; distance:0; metadata:service http; reference:url,bugs.php.net/bug.php?id=28456; classtype:misc-attack; sid:5709; rev:11;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP OpenView Network Node Manager cookie buffer overflow attempt"; flow:to\_server,established; content:"/OVCgi/ovlaunchreg.exe"; fast\_pattern:only; http\_uri; pcre:"/(OvJavaScript|OvTitleFrame|OvHelpWindow|OvMap|OvSession|OvJavaLocale|OvOSLocale|OvLogin|OvDebug|OvDeveloper|OvTreeControl|OvJavaScript|OvProduct|OvPort|OvLocale|OvWebSession)\s\*\x3D[^\x3B\x2C]{1024}/iC"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,42154; reference:cve,2010-2709; classtype:attempted-user; sid:18916; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cacti graph\_image arbitrary command execution attempt"; flow:to\_server,established; content:"graph\_image.php"; nocase; http\_uri; pcre:"/graph\_(start|end|height|width)=(?!(\d+|)[\x26\s])/smi"; metadata:service http; reference:bugtraq,14042; reference:bugtraq,14129; reference:cve,2005-1524; classtype:web-application-attack; sid:8712; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Advanced Poll admin\_edit.php access"; flow:to\_server,established; content:"/admin\_edit.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,8890; reference:nessus,11487; classtype:web-application-activity; sid:2288; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP aglimpse access"; flow:to\_server,established; content:"/aglimpse"; nocase; http\_uri; metadata:service http; reference:bugtraq,2026; reference:cve,1999-0147; reference:nessus,10095; classtype:attempted-recon; sid:842; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP IGeneric Free Shopping Cart page.php access"; flow:to\_server,established; content:"/page.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,9773; classtype:web-application-activity; sid:2410; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP squirrel mail theme arbitrary command attempt"; flow:to\_server,established; content:"/left\_main.php"; nocase; http\_uri; content:"cmdd="; fast\_pattern:only; metadata:service http; reference:bugtraq,4385; reference:cve,2002-0516; classtype:web-application-attack; sid:1737; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP a1stats a1disp3.cgi access"; flow:to\_server,established; content:"/a1disp3.cgi"; http\_uri; metadata:service http; reference:bugtraq,2705; reference:cve,2001-0561; reference:nessus,10669; classtype:web-application-activity; sid:1502; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP whisker HEAD/./"; flow:to\_server,established; content:"HEAD/./"; metadata:service http; reference:url,www.wiretrip.net/rfp/pages/whitepapers/whiskerids.html; classtype:attempted-recon; sid:1139; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP TikiWiki tiki-graph\_formula.php remote php code execution attempt"; flow:to\_server,established; content:"/tikiwiki/tiki-graph\_formula.php"; fast\_pattern:only; http\_uri; content:"f[]="; nocase; http\_uri; pcre:"/(^|&)f\[\]=([^&]+(eval|exec|system|passthru|info))|([^&]{50})/iU"; metadata:policy security-ips drop, service http; reference:bugtraq,26006; reference:cve,2007-5423; classtype:attempted-admin; sid:24502; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP snorkerz.cmd access"; flow:to\_server,established; content:"/snorkerz.cmd"; nocase; http\_uri; metadata:service http; classtype:attempted-recon; sid:870; rev:15;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP OpenView Performance Insight Server backdoor account code execution attempt"; flow:to\_server,established; content:"/reports"; nocase; http\_uri; content:"aGNoOTA4djp6NnQwaiQraQ=="; fast\_pattern:only; http\_header; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,46079; reference:cve,2011-0276; classtype:attempted-admin; sid:18559; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP PHP-Nuke index.php SQL injection attempt"; flow:to\_server,established; content:"select"; fast\_pattern; nocase; http\_header; content:"index.php"; nocase; http\_uri; pcre:"/Referer\x3a[^\r\n]\*?[\x27\x22]\x29[^\r\n]\*?SELECT/Hi"; metadata:service http; reference:bugtraq,22638; reference:cve,2007-1061; classtype:web-application-attack; sid:23405; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP rpm\_query access"; flow:to\_server,established; content:"/rpm\_query"; nocase; http\_uri; metadata:service http; reference:bugtraq,1036; reference:cve,2000-0192; reference:nessus,10340; classtype:attempted-recon; sid:1167; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP JBoss web console access attempt"; flow:to\_server,established; content:"/web-console/"; fast\_pattern:only; http\_uri; metadata:service http; reference:cve,2007-1036; reference:url,docs.jboss.org/jbossas/6/Admin\_Console\_Guide/en-US/pdf/Admin\_Console\_Guide.pdf; classtype:attempted-recon; sid:24342; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS 901 (msg:"SERVER-WEBAPP Samba SWAT Authorization port 901 overflow attempt"; flow:to\_server,established; content:"Authorization|3A| Basic"; nocase; pcre:"/^Authorization\x3a(\s\*|\s\*\r?\n\s+)Basic\s+=/smi"; reference:bugtraq,10780; reference:cve,2004-0600; classtype:web-application-attack; sid:2598; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP yabb access"; flow:to\_server,established; content:"/YaBB"; nocase; http\_uri; metadata:service http; reference:bugtraq,1668; reference:cve,2000-0853; reference:nessus,10512; classtype:attempted-recon; sid:1637; rev:19;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP BigBrother access"; flow:to\_server,established; content:"/bb-hostsvc.sh?HOSTSVC"; nocase; http\_uri; metadata:service http; reference:bugtraq,1455; reference:cve,2000-0638; reference:nessus,10460; classtype:attempted-recon; sid:1105; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Turba status.php access"; flow:to\_server,established; content:"/turba/status.php"; nocase; http\_uri; metadata:service http; reference:nessus,11646; classtype:web-application-activity; sid:2149; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cwmail.exe access"; flow:to\_server,established; content:"/cwmail.exe"; nocase; http\_uri; metadata:service http; reference:bugtraq,4093; reference:cve,2002-0273; reference:nessus,11727; classtype:web-application-activity; sid:2241; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP BugPort config.conf file access"; flow:to\_server,established; content:"/config.conf"; nocase; http\_uri; metadata:service http; reference:bugtraq,9542; classtype:attempted-recon; sid:2370; rev:8;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Domino mailw46.nsf access"; flow:to\_server,established; content:"/mailw46.nsf"; nocase; http\_uri; metadata:service http; reference:nessus,10629; classtype:attempted-recon; sid:1583; rev:12;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP Intelligent Management Center information disclosure attempt"; flow:to\_server,established; content:"/imc/report/DownloadReportSource"; nocase; http\_uri; content:"fileName"; http\_uri; pcre:"/fileName=.\*?\x2E\x2E(\x2F|\x5C)/sI"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,40298; reference:url,secunia.com/advisories/39891; classtype:misc-attack; sid:17137; rev:2;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Oracle Secure Backup Administration property\_box.php other variable command execution attempt"; flow:to\_server,established; content:"/property\_box.php"; fast\_pattern; nocase; http\_uri; content:"type=ListAttachment"; nocase; http\_uri; content:"other="; nocase; http\_uri; pcre:"/other=[^\x26]\*(%26|%7c)/siI"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,41616; reference:cve,2010-0899; classtype:attempted-admin; sid:18797; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP webspirs.cgi directory traversal attempt"; flow:to\_server,established; content:"/webspirs.cgi"; fast\_pattern; nocase; http\_uri; content:"../../"; nocase; metadata:service http; reference:bugtraq,2362; reference:cve,2001-0211; reference:nessus,10616; classtype:web-application-attack; sid:900; rev:20;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Pajax arbitrary command execution attempt"; flow:to\_server,established; content:"method"; nocase; pcre:"/\x22method\x22\s\*\x3a\s\*\x22[A-Z]\w\*[^\x22]/smi"; metadata:service http; reference:bugtraq,17519; reference:cve,2006-1551; reference:cve,2006-1789; classtype:web-application-attack; sid:8734; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP bb\_smilies.php access"; flow:to\_server,established; content:"/bb\_smilies.php"; nocase; http\_uri; metadata:service http; reference:url,www.securiteam.com/securitynews/Serious\_security\_hole\_in\_PHP-Nuke\_\_bb\_smilies\_.html; classtype:web-application-activity; sid:1774; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP store.cgi directory traversal attempt"; flow:to\_server,established; content:"/store.cgi"; fast\_pattern; nocase; http\_uri; content:"../"; metadata:service http; reference:bugtraq,2385; reference:cve,2001-0305; reference:nessus,10639; classtype:web-application-attack; sid:1488; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Oracle iSQL Plus cross site scripting attempt"; flow:to\_server,established; content:"/isqlplus"; nocase; http\_uri; content:"action="; nocase; http\_uri; pcre:"/action[\x3d\x3f][^\n\x26]\*\x3c[^\n\x26]+\x3e/Ui"; metadata:service http; reference:bugtraq,9484; reference:cve,2004-2115; classtype:web-application-attack; sid:11193; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP w3-msql access"; flow:to\_server,established; content:"/w3-msql/"; nocase; http\_uri; metadata:service http; reference:bugtraq,591; reference:bugtraq,898; reference:cve,1999-0276; reference:cve,1999-0753; reference:cve,2000-0012; reference:nessus,10296; classtype:attempted-recon; sid:861; rev:23;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Netscape Enterprise Server directory view"; flow:to\_server,established; content:"?wp-uncheckout"; nocase; http\_uri; metadata:service http; reference:bugtraq,1063; reference:cve,2000-0236; classtype:attempted-recon; sid:1190; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP htmlscript attempt"; flow:to\_server,established; content:"/htmlscript?../.."; nocase; http\_uri; metadata:service http; reference:bugtraq,2001; reference:cve,1999-0264; reference:nessus,10106; classtype:web-application-attack; sid:1608; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP System variable directory traversal attempt - %COMMONPROGRAMFILES%"; flow:to\_server,established; content:"%COMMONPROGRAMFILES%"; fast\_pattern:only; http\_uri; metadata:service http; classtype:attempted-recon; sid:21821; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP /doc/ access"; flow:to\_server,established; content:"/doc/"; nocase; http\_uri; metadata:service http; reference:bugtraq,318; reference:cve,1999-0678; classtype:web-application-activity; sid:1560; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP emumail.cgi NULL attempt"; flow:to\_server,established; content:"/emumail.cgi"; http\_uri; content:"type="; nocase; content:"%00"; metadata:service http; reference:bugtraq,5824; reference:cve,2002-1526; classtype:web-application-activity; sid:1723; rev:13;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP RedHat JBoss Enterprise Application Platform JMX code execution attempt"; flow:established,to\_server; content:"/jmx-console/HtmlAdaptor"; fast\_pattern:only; http\_uri; pcre:"/\x26?arg\d+\s\*=\s\*[^\x26]\*?(import|http)/i"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,39710; reference:cve,2010-0738; classtype:attempted-admin; sid:24642; rev:1;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP mailfile.cgi access"; flow:to\_server,established; content:"/mailfile.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,1807; reference:bugtraq,4579; reference:cve,2000-0977; reference:nessus,11748; classtype:web-application-activity; sid:2213; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP WebChat db\_mysql.php file include"; flow:to\_server,established; content:"/defines.php"; nocase; http\_uri; content:"WEBCHATPATH="; nocase; content:"db\_mysql.php"; fast\_pattern:only; metadata:service http; reference:bugtraq,7000; classtype:web-application-attack; sid:2356; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ultraboard access"; flow:to\_server,established; content:"/ultraboard"; nocase; http\_uri; metadata:service http; reference:bugtraq,1164; reference:bugtraq,1175; reference:nessus,11748; classtype:attempted-recon; sid:1220; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP whois\_raw.cgi access"; flow:to\_server,established; content:"/whois\_raw.cgi"; http\_uri; metadata:service http; reference:bugtraq,304; reference:cve,1999-1063; reference:nessus,10306; classtype:attempted-recon; sid:810; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cgitest.exe access"; flow:to\_server,established; content:"/cgitest.exe"; nocase; http\_uri; metadata:service http; reference:bugtraq,1313; reference:bugtraq,3885; reference:cve,2000-0521; reference:cve,2002-0128; reference:nessus,10040; reference:nessus,10623; reference:nessus,11131; classtype:web-application-activity; sid:1587; rev:20;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Oracle GlassFish Enterprise server cross site scripting attempt"; flow:to\_server,established; content:"/management/domain/create-password-alias"; fast\_pattern:only; http\_uri; pcre:"/id=[^\x26]+(script|onload|onmouseover|\x27|\x22|\x3c|\x3e|src)/i"; metadata:policy security-ips drop, service http, service imap, service pop3; reference:cve,2012-0551; reference:url,osvdb.org/81227; reference:url,www.oracle.com/technetwork/topics/security/cpuapr2012-366314.html; classtype:web-application-attack; sid:23046; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP test.bat access"; flow:to\_server,established; content:"/test.bat"; http\_uri; metadata:service http; reference:bugtraq,762; reference:cve,1999-0947; reference:nessus,10016; classtype:web-application-activity; sid:1511; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 8888 (msg:"SERVER-WEBAPP answerbook2 admin attempt"; flow:to\_server,established; content:"/cgi-bin/admin/admin"; reference:bugtraq,5383; reference:cve,2000-0696; classtype:web-application-activity; sid:1946; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP RiSearch show.pl proxy attempt"; flow:to\_server,established; content:"/show.pl"; fast\_pattern; nocase; http\_uri; content:"url="; nocase; metadata:service http; reference:bugtraq,10812; classtype:web-application-activity; sid:3465; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP sambar /search/results.stm access"; flow:to\_server,established; content:"POST"; nocase; content:"/search/results.stm"; nocase; metadata:service http; reference:bugtraq,7975; reference:bugtraq,9607; reference:cve,2004-2086; reference:nessus,18650; classtype:web-application-activity; sid:3629; rev:8;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP WAnewsletter newsletter.php file include attempt"; flow:to\_server,established; content:"newsletter.php"; nocase; http\_uri; content:"waroot"; fast\_pattern:only; content:"start.php"; nocase; metadata:service http; reference:bugtraq,6965; classtype:web-application-attack; sid:2398; rev:8;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP encoded cross site scripting HTML Image tag set to javascript attempt"; flow:to\_server,established; content:"img src=javascript"; nocase; http\_uri; metadata:service http; reference:bugtraq,4858; reference:cve,2002-0902; classtype:web-application-attack; sid:7071; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP filemail access"; flow:to\_server,established; content:"/filemail.pl"; nocase; http\_uri; metadata:service http; reference:cve,1999-1154; classtype:attempted-recon; sid:858; rev:17;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 383 (msg:"SERVER-WEBAPP HP OpenView Operations Agent request"; flow:to\_server,established; content:"GET /Hewlett-Packard/OpenView/Coda"; fast\_pattern:only; flowbits:set,hp\_openview\_coda; flowbits:noalert; classtype:misc-activity; sid:24313; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ttawebtop.cgi arbitrary file attempt"; flow:to\_server,established; content:"/ttawebtop.cgi"; nocase; content:"pg=../"; fast\_pattern:only; metadata:service http; reference:bugtraq,2890; reference:cve,2001-0805; reference:nessus,10696; classtype:web-application-attack; sid:1479; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP campas access"; flow:to\_server,established; content:"/campas"; nocase; http\_uri; metadata:service http; reference:bugtraq,1975; reference:cve,1999-0146; reference:nessus,10035; classtype:attempted-recon; sid:847; rev:20;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP OpenView Network Node Manager cookie buffer overflow attempt"; flow:to\_server,established; content:"/OVCgi/getcvdata.exe"; fast\_pattern:only; http\_uri; pcre:"/(OvJavaScript|OvTitleFrame|OvHelpWindow|OvMap|OvSession|OvJavaLocale|OvOSLocale|OvLogin|OvDebug|OvDeveloper|OvTreeControl|OvJavaScript|OvProduct|OvPort|OvLocale|OvWebSession)\s\*\x3D[^\x3B\x2C]{1024}/iC"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,42154; reference:cve,2010-2709; classtype:attempted-user; sid:18906; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Armada Style Master Index directory traversal"; flow:to\_server,established; content:"/search.cgi?keys"; http\_uri; content:"catigory=../"; metadata:service http; reference:bugtraq,1772; reference:cve,2000-0924; reference:nessus,10562; reference:url,www.synnergy.net/downloads/advisories/SLA-2000-16.masterindex.txt; classtype:web-application-attack; sid:1092; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP perl command attempt"; flow:to\_server,established; content:"/perl?"; nocase; http\_uri; metadata:service http; reference:cve,1999-0509; reference:nessus,10173; reference:url,www.cert.org/advisories/CA-1996-11.html; classtype:attempted-recon; sid:1649; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP pmachine remote file include attempt"; flow:to\_server,established; content:"lib.inc.php"; fast\_pattern; nocase; http\_uri; content:"pm\_path="; pcre:"/pm\_path=(https?|ftps?|php)/"; metadata:service http; reference:bugtraq,7919; reference:nessus,11739; classtype:web-application-attack; sid:2226; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP login.htm access"; flow:to\_server,established; content:"/login.htm"; nocase; http\_uri; metadata:service http; reference:bugtraq,665; reference:cve,1999-1533; classtype:web-application-activity; sid:1564; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Talentsoft Web+ internal IP Address access"; flow:to\_server,established; content:"/webplus.exe?about"; http\_uri; metadata:service http; reference:bugtraq,1720; reference:url,archives.neohapsis.com/archives/ntbugtraq/2000-q3/0168.html; classtype:web-application-activity; sid:1096; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Netscape Enterprise Server directory view"; flow:to\_server,established; content:"?wp-html-rend"; nocase; http\_uri; metadata:service http; reference:bugtraq,1063; reference:cve,2000-0236; classtype:attempted-recon; sid:1191; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP DirBuster brute forcing tool detected"; flow:to\_server,established; content:"User-Agent|3A| DirBuster"; fast\_pattern:only; http\_header; metadata:service http; reference:url,sourceforge.net/projects/dirbuster/; classtype:web-application-attack; sid:19933; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP .DS\_Store access"; flow:to\_server,established; content:"/.DS\_Store"; http\_uri; metadata:service http; reference:url,www.macintouch.com/mosxreaderreports46.html; classtype:web-application-activity; sid:1769; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Wordcircle SQL injection attempt"; flow:to\_server,established; content:"/index.php"; nocase; http\_uri; content:"password="; nocase; http\_uri; pcre:"/\x2Findex\.php?[^\r\n]\*?password=[^\r\n\x26]\*?[\x22\x27][^\r\n\x26]\*[\x22\x27]/Ui"; metadata:service http; reference:bugtraq,16227; reference:cve,2006-0205; classtype:web-application-activity; sid:20615; rev:4;)

#alert udp $HOME\_NET any -> $EXTERNAL\_NET 500 (msg:"SERVER-WEBAPP Openswan/Strongswan Pluto IKE daemon ISAKMP DPD malformed packet DOS attempt"; flow:to\_server; content:"|8D 28|"; depth:2; offset:38; isdataat:!41; reference:bugtraq,34296; reference:cve,2009-0790; classtype:attempted-dos; sid:21333; rev:2;)

alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Oracle Java Web Server Webdav Stack Buffer Overflow attempt"; flow:to\_server,established; content:"COPY"; depth:4; nocase; isdataat:200,relative; pcre:"/^COPY(?!\n)\s[^\n]{200}/smi"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,37874; reference:cve,2010-0361; classtype:attempted-admin; sid:17609; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP loadpage.cgi directory traversal attempt"; flow:to\_server,established; content:"/loadpage.cgi"; http\_uri; content:"file=../"; fast\_pattern:only; metadata:service http; reference:bugtraq,2109; reference:cve,2000-1092; reference:nessus,10065; classtype:web-application-attack; sid:1569; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 9090 (msg:"SERVER-WEBAPP Jive Software Openfire audit-policy.jsp XSS attempt"; flow:to\_server,established; content:"/audit-policy.jsp"; fast\_pattern:only; http\_uri; pcre:"/audit-policy\.jsp\?.\*?=([^\x26]\*[\x22\x27\x3C\x3E\x28\x29\x3B]|script|src|location|document)/U"; metadata:policy security-ips drop, service http; reference:bugtraq,32935; reference:cve,2009-0496; classtype:web-application-attack; sid:20866; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP ScozBook SQL injection in auth.php adminname attempt"; flow:to\_server,established; content:"auth.php"; fast\_pattern:only; http\_uri; content:"adminname"; nocase; pcre:"/adminname=[^\r\n\x26]\*?([\x22\x27]|%2[27])/i"; metadata:service http; reference:bugtraq,16115; reference:cve,2006-0079; classtype:web-application-attack; sid:20643; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP siteUserMod.cgi access"; flow:to\_server,established; content:"/.cobalt/siteUserMod/siteUserMod.cgi"; http\_uri; metadata:service http; reference:bugtraq,951; reference:cve,2000-0117; reference:nessus,10253; classtype:web-application-activity; sid:1870; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP rguest.exe access"; flow:to\_server,established; content:"/rguest.exe"; nocase; http\_uri; metadata:service http; reference:bugtraq,2024; reference:cve,1999-0287; classtype:attempted-recon; sid:833; rev:21;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Opt-X header.php remote file include attempt"; flow:to\_server,established; content:"/header.php"; nocase; http\_uri; content:"systempath="; fast\_pattern:only; pcre:"/systempath=(https?|ftps?|php)/i"; metadata:service http; reference:bugtraq,9732; classtype:web-application-attack; sid:2575; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ezadmin.cgi access"; flow:to\_server,established; content:"/ezadmin.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,4068; reference:bugtraq,4579; reference:cve,2002-0263; reference:nessus,11748; classtype:web-application-activity; sid:2204; rev:16;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP phpThumb fltr[] parameter remote command execution attempt"; flow:to\_server,established; content:"/phpThumb.php?"; nocase; http\_uri; content:"fltr[]="; nocase; http\_uri; content:"|3B|"; within:200; nocase; http\_uri; pcre:"/\x2FphpThumb\.php\x3F[^\r\n]\*fltr\[\]=[^\r\n\x26]+\x3B/Ui"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,39605; reference:cve,2010-1598; reference:url,blog.spiderlabs.com/2011/12/honeypot-alert-phpthumb-fltr-parameter-command-injection-detected.html; classtype:attempted-user; sid:20827; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP calendar\_admin.pl arbitrary command execution attempt"; flow:to\_server,established; content:"/calendar\_admin.pl?config=|7C|"; http\_uri; metadata:service http; reference:bugtraq,1215; reference:cve,2000-0432; reference:nessus,10506; classtype:web-application-attack; sid:1536; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS 7777 (msg:"SERVER-WEBAPP WhatsUpGold instancename overflow attempt"; flow:to\_server,established; content:"/\_maincfgret.cgi"; nocase; http\_uri; pcre:"/instancename=[^&\x3b\r\n]{513}/smi"; metadata:service http; reference:bugtraq,11043; reference:cve,2004-0798; classtype:web-application-attack; sid:12056; rev:11;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP Power Manager formExportDataLogs buffer overflow attempt"; flow:to\_server, established; content:"|2F|goform|2F|formExportDataLogs"; nocase; http\_uri; content:"fileName"; http\_client\_body; pcre:"/fileName\x3d[^\r\n&]{235}/iP"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,37866; reference:cve,2009-3999; classtype:attempted-user; sid:18745; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP pals-cgi access"; flow:to\_server,established; content:"/pals-cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,2372; reference:cve,2001-0216; reference:cve,2001-0217; reference:nessus,10611; classtype:attempted-recon; sid:897; rev:20;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Oracle Java System Web Server 7.0 WebDAV format string exploit attempt - PROPFIND method"; flow:to\_server,established; content:"PROPFIND"; depth:8; fast\_pattern; nocase; content:"<?xml"; content:"encoding"; within:30; pcre:"/\<\?xml[^\>]+encoding\s\*\=\s\*(\'|\")[^\'\"\>\%]\*\%/"; metadata:service http; reference:bugtraq,37910; reference:cve,2010-0388; classtype:attempted-user; sid:16426; rev:8;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP phptest.php access"; flow:to\_server,established; content:"/phptest.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,9737; classtype:web-application-activity; sid:2405; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ContentFilter.dll access"; flow:to\_server,established; content:"/ContentFilter.dll"; nocase; http\_uri; metadata:service http; reference:bugtraq,3327; reference:cve,2001-0958; reference:nessus,11747; classtype:web-application-activity; sid:2232; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Oracle Secure Backup Administration preauth variable command injection attempt"; flow:to\_server,established; content:"/index.php"; nocase; http\_uri; content:"button=Remove"; nocase; http\_uri; content:"op=Preauth"; nocase; http\_uri; content:"preauth="; nocase; http\_uri; pcre:"/preauth\x3d[\x26\x7c]/Ui"; metadata:service http; reference:bugtraq,41597; reference:cve,2010-0906; classtype:attempted-admin; sid:19228; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP SAP Crystal Reports crystalimagehandler.aspx access"; flow:to\_server,established; content:"/crystalimagehandler.aspx"; nocase; http\_uri; metadata:service http; reference:cve,2004-0204; reference:url,www.microsoft.com/security/bulletins/200406\_crystal.mspx; classtype:web-application-activity; sid:2581; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Advanced Poll admin\_license.php access"; flow:to\_server,established; content:"/admin\_license.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,8890; reference:nessus,11487; classtype:web-application-activity; sid:2291; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP rpc-nlog.pl access"; flow:to\_server,established; content:"/rpc-nlog.pl"; http\_uri; metadata:service http; reference:cve,1999-1278; reference:url,marc.theaimsgroup.com/?l=bugtraq&m=91470326629357&w=2; reference:url,marc.theaimsgroup.com/?l=bugtraq&m=91471400632145&w=2; classtype:web-application-activity; sid:1931; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP LANDesk Thinkmanagement Suite ServerSetup Directory Transversal attempt"; flow:to\_server,established; content:"POST"; http\_method; content:"/landesk/managementsuite/core/core.anonymous/ServerSetup.asmx"; fast\_pattern:only; http\_uri; content:"<RunAMTCommand"; nocase; http\_client\_body; content:"-RunEnhancedRemediation"; distance:0; nocase; http\_client\_body; metadata:service http; reference:bugtraq,52023; reference:cve,2012-1195; classtype:attempted-user; sid:23259; rev:2;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP OpenView Network Node Manager ovwebsnmpsrv.exe OVwSelection buffer overflow attempt - GET"; flow:to\_server,established; content:"|2F|OvCgi|2F|jovgraph.exe"; nocase; http\_uri; content:"OVwSelection"; nocase; http\_uri; pcre:"/(arg=[^\x26]\*?OVwSelection[^\x26]\*?\x26.\*?sel=[^\s\x26]{1023}|sel=[^\x26]{1023,}\x26.\*?arg=[^\s\x26]\*?OVwSelection)/sU"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,37343; reference:cve,2009-4181; classtype:attempted-user; sid:16712; rev:2;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP SiteScope APISiteScopeImpl information disclosure attempt"; flow:to\_server,established; content:"POST"; http\_method; content:"/APISiteScopeImpl"; http\_uri; content:"impl:getSiteScopeConfiguration"; fast\_pattern:only; http\_client\_body; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,55269; reference:cve,2012-3259; reference:url,osvdb.org/85120; classtype:web-application-activity; sid:24291; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Symantec Web Gateway timer.php cross site scripting attempt"; flow:to\_server,established; content:"/spywall/timer.php"; fast\_pattern:only; http\_uri; pcre:"/[?&](l|d|profile)=[^&]+?([\x22\x27\x3c\x3e\x28\x29]|script|onload|src)/U"; metadata:service http; reference:bugtraq,53396; reference:cve,2012-0296; reference:url,www.osvdb.org/show/osvdb/82022; classtype:web-application-attack; sid:23177; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP chatbox.php access"; flow:to\_server,established; content:"/chatbox.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,8930; classtype:web-application-activity; sid:2305; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 8090 (msg:"SERVER-WEBAPP TrackerCam ComGetLogFile.php3 log information disclosure"; flow:to\_server,established; content:"/ComGetLogFile.php3"; nocase; pcre:"/fn=Eye\d{4}\_\d{2}\.log/Rmsi"; reference:bugtraq,12592; reference:cve,2005-0481; reference:nessus,17160; classtype:web-application-activity; sid:3545; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP HP Network Node Manager cross site scripting attempt"; flow:to\_server,established; content:"/nnm/"; fast\_pattern:only; http\_uri; pcre:"/\x2Fnnm\x2F(mibdiscover|protected\x2Fconfigurationpoll\.jsp|protected\x2Fping\.jsp|protected\x2Fstatuspoll\.jsp|protected\x2Ftraceroute\.jsp|validate)/Ui"; pcre:"/(node|nodename|field)=[^\x26]+(script|onload|onmouseover|\x27|\x22|\x3c|\x3e|src)/i"; metadata:policy security-ips drop, service http; reference:cve,2011-4155; reference:url,h20566.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr\_na-c03035744; reference:url,osvdb.org/76962; classtype:web-application-attack; sid:20845; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP source.jsp access"; flow:to\_server,established; content:"/source.jsp"; nocase; http\_uri; metadata:service http; reference:nessus,12119; classtype:web-application-activity; sid:2484; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP webplus version access"; flow:to\_server,established; content:"/webplus?about"; nocase; http\_uri; metadata:service http; reference:bugtraq,1102; reference:cve,2000-0282; classtype:attempted-recon; sid:812; rev:20;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Checkpoint Firewall-1 HTTP parsing format string vulnerability attempt"; flow:to\_server,established; content:"|3A|/"; offset:11; http\_uri; pcre:"/^[^\x3a\x3f]{11,}\x3a\x2f/Usmi"; metadata:service http; reference:bugtraq,9581; reference:cve,2004-0039; reference:nessus,12084; classtype:attempted-admin; sid:2381; rev:17;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP OpenView Network Node Manager cookie buffer overflow attempt"; flow:to\_server,established; content:"/OVCgi/nnmRptConfig.exe"; fast\_pattern:only; http\_uri; pcre:"/(OvJavaScript|OvTitleFrame|OvHelpWindow|OvMap|OvSession|OvJavaLocale|OvOSLocale|OvLogin|OvDebug|OvDeveloper|OvTreeControl|OvJavaScript|OvProduct|OvPort|OvLocale|OvWebSession)\s\*\x3D[^\x3B\x2C]{1024}/iC"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,42154; reference:cve,2010-2709; classtype:attempted-user; sid:18910; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Lotus EditDoc attempt"; flow:to\_server,established; content:"?EditDocument"; nocase; http\_uri; metadata:service http; reference:url,www.securiteam.com/exploits/5NP080A1RE.html; classtype:attempted-recon; sid:1117; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP survey.cgi access"; flow:to\_server,established; content:"/survey.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,1817; reference:cve,1999-0936; classtype:attempted-recon; sid:871; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP phpBook date command execution attempt"; flow:established, to\_server; content:"/lwc/index.php"; nocase; http\_uri; pcre:"/index\.php\?.\*date=[^\r\n\x26]\*\x29\x3B/smiU"; metadata:policy security-ips drop, service http; reference:bugtraq,16229; reference:cve,2006-0206; classtype:attempted-admin; sid:18333; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cal\_make.pl directory traversal attempt"; flow:to\_server,established; content:"/cal\_make.pl"; nocase; http\_uri; content:"p0=../../"; fast\_pattern:only; metadata:service http; reference:bugtraq,2663; reference:cve,2001-0463; reference:nessus,10664; classtype:web-application-attack; sid:1704; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Invalid HTTP Version String"; flow:to\_server,established; content:"HTTP/"; nocase; pcre:"/^\w+\s+[^\x0D\x0A\s]+\s+HTTP\x2F[^\x0A]{5}/si"; metadata:service http; reference:bugtraq,34240; reference:bugtraq,9809; reference:cve,2009-0478; reference:nessus,11593; classtype:non-standard-protocol; sid:2570; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP sresult.exe access"; flow:to\_server,established; content:"/sresult.exe"; nocase; http\_uri; metadata:service http; reference:bugtraq,10837; reference:nessus,14186; classtype:web-application-activity; sid:2672; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ttforum remote file include attempt"; flow:to\_server,established; content:"forum/index.php"; http\_uri; content:"template="; pcre:"/template=(https?|ftps?|php)/i"; metadata:service http; reference:bugtraq,7542; reference:bugtraq,7543; reference:nessus,11615; classtype:web-application-attack; sid:2155; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP bsguest.cgi access"; flow:to\_server,established; content:"/bsguest.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,2159; reference:cve,2001-0099; classtype:web-application-activity; sid:1711; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 8022 (msg:"SERVER-WEBAPP Ipswitch WhatsUp Small Business directory traversal attempt"; flow:to\_server,established; content:"|2E 2E 5C 2E 2E 5C 2E 2E 5C|"; depth:100; pcre:"/^(GET|POST)\h+[^\n]\*?\x2E\x2E\x5C\x2E\x2E\x5C\x2E\x2E\x5C[^\n]\*?HTTP/i"; metadata:policy security-ips drop, service http; reference:bugtraq,15291; reference:cve,2005-1939; classtype:attempted-user; sid:17280; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP formmail arbitrary command execution attempt"; flow:to\_server,established; content:"/formmail"; fast\_pattern; nocase; http\_uri; content:"%0a"; nocase; metadata:service http; reference:bugtraq,1187; reference:bugtraq,2079; reference:cve,1999-0172; reference:cve,2000-0411; reference:nessus,10076; reference:nessus,10782; classtype:web-application-attack; sid:1610; rev:21;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP .cmd? access"; flow:to\_server,established; content:".cmd?"; nocase; http\_uri; metadata:service http; reference:bugtraq,4335; reference:cve,2002-0061; classtype:web-application-activity; sid:9791; rev:6;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Wordpress Invit0r plugin php upload attempt"; flow:to\_server,established; content:"/wp-content/plugins/invit0r/lib/php-ofc-library/ofc\_upload\_image.php"; fast\_pattern:only; http\_uri; content:"name="; http\_uri; content:"<?php "; nocase; http\_client\_body; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,53995; reference:url,osvdb.org/show/osvdb/82985; reference:url,www.opensyscom.fr/Actualites/wordpress-plugins-invit0r-arbitrary-file-upload-vulnerability.html; classtype:web-application-attack; sid:23485; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP SalesLogix Eviewer web command attempt"; flow:to\_server,established; content:"/slxweb.dll/admin?command="; nocase; http\_uri; metadata:service http; reference:bugtraq,1078; reference:bugtraq,1089; reference:cve,2000-0278; reference:cve,2000-0289; reference:nessus,10361; classtype:web-application-attack; sid:1187; rev:19;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP iPlanet Search directory traversal attempt"; flow:to\_server,established; content:"/search"; http\_uri; content:"NS-query-pat="; content:"../../"; metadata:service http; reference:bugtraq,5191; reference:cve,2002-1042; reference:nessus,11043; classtype:web-application-attack; sid:1828; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Domino statrep.nsf access"; flow:to\_server,established; content:"/statrep.nsf"; nocase; http\_uri; metadata:service http; reference:nessus,10629; classtype:attempted-recon; sid:1578; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP catgy.cgi access"; flow:to\_server,established; content:"/alert.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,3714; reference:bugtraq,4579; reference:cve,2001-1212; reference:nessus,11748; classtype:web-application-activity; sid:2196; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP calendar.pl access"; flow:to\_server,established; content:"calendar"; nocase; http\_uri; pcre:"/calendar(|[-\_]admin)\.pl/Ui"; metadata:service http; reference:bugtraq,1215; reference:cve,2000-0432; classtype:attempted-recon; sid:1455; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Phorum admin access"; flow:to\_server,established; content:"/admin.php3"; nocase; http\_uri; metadata:service http; reference:bugtraq,2271; classtype:attempted-recon; sid:1134; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP perl.exe command attempt"; flow:to\_server,established; content:"/perl.exe?"; nocase; http\_uri; metadata:service http; reference:cve,1999-0509; reference:nessus,10173; reference:url,www.cert.org/advisories/CA-1996-11.html; classtype:attempted-recon; sid:1648; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP filemail access"; flow:to\_server,established; content:"/filemail"; nocase; http\_uri; metadata:service http; reference:cve,1999-1154; reference:cve,1999-1155; reference:url,www.securityfocus.com/archive/1/11175; classtype:attempted-recon; sid:1216; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Akarru remote file include in main\_content.php bm\_content"; flow:to\_server,established; content:"main\_content.php"; fast\_pattern:only; http\_uri; pcre:"/\x2Fmain\_content\.php?[^\r\n]\*?bm\_content=(https?|ftps?)/Ui"; metadata:service http; reference:bugtraq,19870; reference:cve,2006-4645; classtype:web-application-activity; sid:20631; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP printenv access"; flow:to\_server,established; content:"/printenv"; http\_uri; metadata:service http; reference:bugtraq,1658; reference:cve,2000-0868; reference:nessus,10188; reference:nessus,10503; classtype:web-application-activity; sid:1877; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP mall log order access"; flow:to\_server,established; content:"/mall\_log\_files/order.log"; nocase; http\_uri; metadata:service http; reference:bugtraq,2266; reference:cve,1999-0606; classtype:attempted-recon; sid:1168; rev:14;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 8889 (msg:"SERVER-WEBAPP Openwsman HTTP basic authentication buffer overflow attempt"; flow:to\_server,established; content:"Authorization|3A|"; nocase; content:"Basic"; nocase; isdataat:256,relative; pcre:"/^Authorization\x3a\s\*Basic[^\n]{256}/mi"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,30694; reference:cve,2008-2234; classtype:attempted-user; sid:14992; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP shopping cart directory traversal"; flow:to\_server,established; content:"/shop.cgi"; http\_uri; content:"page=../"; metadata:service http; reference:bugtraq,1777; reference:cve,2000-0921; classtype:web-application-attack; sid:1089; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP dbman db.cgi access"; flow:to\_server,established; content:"/dbman/db.cgi"; http\_uri; metadata:service http; reference:bugtraq,1178; reference:cve,2000-0381; reference:nessus,10403; classtype:web-application-activity; sid:1554; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ans.pl attempt"; flow:to\_server,established; content:"/ans.pl?p=../../"; http\_uri; metadata:service http; reference:bugtraq,4147; reference:bugtraq,4149; reference:cve,2002-0306; reference:cve,2002-0307; reference:nessus,10875; classtype:web-application-attack; sid:1522; rev:16;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP OpenView NNM getnnmdata.exe CGI hostname parameter buffer overflow attempt"; flow:to\_server,established; content:"/OvCgi/getnnmdata|2E|exe"; fast\_pattern:only; http\_uri; content:"Hostname|3D|"; nocase; isdataat:300,relative; pcre:"/Hostname\x3D[^\x26\x3F\x3B\x0D\x0A\s]{300}/i"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:cve,2010-1555; classtype:attempted-user; sid:19138; rev:3;)

#alert tcp $HTTP\_SERVERS $HTTP\_PORTS -> $EXTERNAL\_NET any (msg:"SERVER-WEBAPP 407 Proxy Authentication Required"; flow:to\_client,established; content:"407"; http\_stat\_code; flowbits:set,http.stat\_code\_407; flowbits:noalert; metadata:service http; classtype:misc-activity; sid:17447; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP wwwadmin.pl access"; flow:to\_server,established; content:"/wwwadmin.pl"; nocase; http\_uri; metadata:service http; classtype:attempted-recon; sid:888; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP snork.bat access"; flow:to\_server,established; content:"/snork.bat"; nocase; http\_uri; metadata:service http; reference:bugtraq,2023; reference:cve,1999-0233; classtype:attempted-recon; sid:860; rev:20;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP RedHat JBoss Enterprise Application Platform JMX authentication bypass attempt"; flow:to\_server,established; content:"HEAD"; nocase; http\_method; content:"/jmx-console/HtmlAdaptor"; nocase; http\_uri; content:"import"; nocase; http\_uri; pcre:"/\x26arg\d+\s\*=\s\*[^\r\n\x26]\*import/Ui"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,39710; reference:cve,2010-0738; classtype:attempted-admin; sid:18794; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP modules.php access"; flow:to\_server,established; content:"/modules.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,9879; classtype:web-application-activity; sid:2565; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP YaBB SE packages.php file include"; flow:to\_server,established; content:"/packages.php"; fast\_pattern; nocase; http\_uri; content:"packer.php"; nocase; metadata:service http; reference:bugtraq,6663; classtype:web-application-attack; sid:2362; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Advanced Poll admin\_tpl\_misc\_new.php access"; flow:to\_server,established; content:"/admin\_tpl\_misc\_new.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,8890; reference:nessus,11487; classtype:web-application-activity; sid:2299; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP robot.txt access"; flow:to\_server,established; content:"/robot.txt"; nocase; http\_uri; metadata:service http; reference:nessus,10302; classtype:web-application-activity; sid:1857; rev:9;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP OpenView Network Node Manager cookie buffer overflow attempt"; flow:to\_server,established; content:"/OVCgi/OvWebHelp.exe"; fast\_pattern:only; http\_uri; pcre:"/(OvJavaScript|OvTitleFrame|OvHelpWindow|OvMap|OvSession|OvJavaLocale|OvOSLocale|OvLogin|OvDebug|OvDeveloper|OvTreeControl|OvJavaScript|OvProduct|OvPort|OvLocale|OvWebSession)\s\*\x3D[^\x3B\x2C]{1024}/iC"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,42154; reference:cve,2010-2709; classtype:attempted-user; sid:18921; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 8484 (msg:"SERVER-WEBAPP Ipswitch IMail Calendaring arbitrary file read attempt"; flow:to\_server,established; content:"GET /what.jsp?|5C|..|5C|.."; metadata:policy security-ips drop; reference:bugtraq,13727; reference:cve,2005-1252; classtype:attempted-recon; sid:15953; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP System variable directory traversal attempt - %TMP%"; flow:to\_server,established; content:"%TMP%"; fast\_pattern:only; http\_uri; metadata:service http; classtype:attempted-recon; sid:21832; rev:3;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Webmin show.cgi arbitrary command injection attempt"; flow:to\_server,established; content:"/file/show.cgi/bin/"; fast\_pattern:only; http\_uri; pcre:"/^\/file\/show\.cgi\/bin\/[^\s]+?\x7c/miI"; metadata:policy balanced-ips alert, policy security-ips drop, service http; reference:bugtraq,55446; reference:cve,2012-2982; reference:url,www.kb.cert.org/vuls/id/788478; classtype:web-application-attack; sid:24628; rev:1;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP sdbsearch.cgi access"; flow:to\_server,established; content:"/sdbsearch.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,1658; reference:cve,2001-1130; reference:nessus,10503; reference:nessus,10720; classtype:attempted-recon; sid:1476; rev:19;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Webnews.exe access"; flow:to\_server,established; content:"/Webnews.exe"; nocase; http\_uri; metadata:service http; reference:bugtraq,4124; reference:cve,2002-0290; reference:nessus,11732; classtype:web-application-activity; sid:2245; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP bb-histlog.sh access"; flow:to\_server,established; content:"/bb-histlog.sh"; nocase; http\_uri; metadata:service http; reference:bugtraq,142; reference:cve,1999-1462; reference:nessus,10025; classtype:attempted-recon; sid:1459; rev:17;)

alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Novell iManager buffer overflow attempt"; flow:to\_server,established; content:"POST"; http\_method; content:"/nps/servlet/webacc"; nocase; http\_uri; content:"EnteredAttrName="; fast\_pattern:only; http\_client\_body; pcre:"/EnteredAttrName=[^&]{32}/iP"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:cve,2011-4188; reference:url,novell.com/support/kb/doc.php?id=7002971; classtype:attempted-admin; sid:23354; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP directorypro.cgi access"; flow:to\_server,established; content:"/directorypro.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,2793; reference:cve,2001-0780; reference:nessus,10679; classtype:web-application-activity; sid:1467; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP miniBB rss.php pathToFiles remote file include attempt"; flow:to\_server,established; content:"rss.php"; nocase; http\_uri; content:"pathToFiles="; nocase; http\_uri; pcre:"/pathToFiles=(ftp|https?)/Ui"; metadata:policy security-ips drop, service http; reference:url,osvdb.org/show/osvdb/51460; classtype:web-application-attack; sid:18479; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP MsmMask.exe access"; flow:to\_server,established; content:"/MsmMask.exe"; http\_uri; metadata:service http; reference:nessus,11163; classtype:web-application-activity; sid:2059; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP post32.exe access"; flow:to\_server,established; content:"/post32.exe"; http\_uri; metadata:service http; reference:bugtraq,1485; classtype:web-application-activity; sid:2071; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP changepw.exe access"; flow:to\_server,established; content:"/changepw.exe"; nocase; http\_uri; metadata:service http; reference:bugtraq,1256; reference:cve,2000-0401; reference:nessus,11723; classtype:web-application-activity; sid:2240; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP webalizer access"; flow:to\_server,established; content:"/webalizer/"; nocase; http\_uri; metadata:service http; reference:bugtraq,3473; reference:cve,2001-0835; reference:nessus,10816; classtype:web-application-activity; sid:1847; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP RBS ISP /newuser access"; flow:to\_server,established; content:"/newuser"; http\_uri; metadata:service http; reference:bugtraq,1704; reference:cve,2000-1036; reference:nessus,10521; classtype:web-application-activity; sid:1493; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP CCBill whereami.cgi access"; flow:to\_server,established; content:"/whereami.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,8095; reference:url,secunia.com/advisories/9191/; classtype:web-application-activity; sid:2397; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP register.cgi access"; flow:to\_server,established; content:"/register.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,2157; reference:cve,2001-0076; classtype:web-application-activity; sid:1715; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP imagemap.exe overflow attempt"; flow:to\_server,established; content:"/imagemap.exe?"; nocase; http\_uri; metadata:service http; reference:bugtraq,739; reference:cve,1999-0951; reference:nessus,10122; classtype:web-application-attack; sid:821; rev:23;)

#alert tcp $HOME\_NET any -> $EXTERNAL\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP PHP 5.3.3 mt\_rand integer overflow attempt"; flow:to\_server,established; content:"mt\_getrandmax("; fast\_pattern:only; http\_client\_body; content:"<?"; pcre:"/(define\(\s\*(?P<q1>[\x22\x27])\s\*(?P<m1>\w+)(?P=q1)\s\*,\s\*mt\_getrandmax\(\)\s\*\+\d+\s\*\)\x3b.\*?mt\_rand\(\s\*0\s\*,\s\*(?P=m1)\s\*\)|(?P<m2>\$\w+)\s\*=\s\*mt\_getrandmax\(\)\s\*\+\s\*\d+\s\*\x3b.\*?mt\_rand\(\s\*0\s\*,\s\*(?P=m2)\s\*\)|mt\_rand\(\s\*0\s\*,\s\*mt\_getrandmax\(\)\s\*\+\s\*\d+\s\*\)\x3b)/smi"; metadata:service http; reference:cve,2011-0755; classtype:misc-activity; sid:24061; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP SGI InfoSearch fname access"; flow:to\_server,established; content:"/infosrch.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,1031; reference:cve,2000-0207; classtype:web-application-activity; sid:1727; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP System variable directory traversal attempt - %PROGRAMDATA%"; flow:to\_server,established; content:"%PROGRAMDATA%"; fast\_pattern:only; http\_uri; metadata:service http; classtype:attempted-recon; sid:21819; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP perlshop.cgi access"; flow:to\_server,established; content:"/perlshop.cgi"; nocase; http\_uri; metadata:service http; reference:cve,1999-1374; classtype:attempted-recon; sid:840; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 8080 (msg:"SERVER-WEBAPP Linksys router default username and password login attempt"; flow:to\_server,established; content:"YWRtaW46YWRtaW4"; pcre:"/^Authorization\x3a\s\*Basic\s+(?-i)YWRtaW46YWRtaW4[=\s]/smi"; reference:nessus,10999; classtype:default-login-attempt; sid:1861; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 3037 (msg:"SERVER-WEBAPP Novell File Reporter Agent XMLK parsing stack bugger overflow attempt"; flow:to\_server,established; content:"|3C|NAME|3E|"; isdataat:41; pcre:"/^[^\x3c\x2f]{41}/R"; reference:bugtraq,47144; reference:cve,2011-0994; classtype:attempted-admin; sid:19813; rev:4;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 383 (msg:"SERVER-WEBAPP HP Operations Agent stack buffer overflow attempt"; flow:to\_server,established; flowbits:isset,hp\_openview\_coda; content:"|00 00 00 32|"; depth:4; offset:18; byte\_jump:2,16,relative; byte\_jump:2,0,relative; byte\_test:2,>,1024,0,relative; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,54362; reference:cve,2012-2019; reference:url,h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03397769; classtype:attempted-admin; sid:23958; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cart32.exe access"; flow:to\_server,established; content:"/cart32.exe"; nocase; http\_uri; metadata:service http; reference:bugtraq,1153; reference:nessus,10389; classtype:web-application-activity; sid:1654; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP TextPortal admin.php default password admin attempt"; flow:to\_server,established; content:"/admin.php"; http\_uri; content:"op=admin\_enter"; content:"password=admin"; fast\_pattern:only; metadata:service http; reference:bugtraq,7673; reference:nessus,11660; classtype:web-application-activity; sid:2145; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 1761 (msg:"SERVER-WEBAPP Novell ZENworks Remote Management overflow attempt"; flow:to\_server,established; content:"|00 01|"; depth:2; offset:16; byte\_jump:2,0,relative,big; byte\_jump:2,0,relative,big; byte\_jump:2,0,relative,big; content:"|00 01 00 02|"; within:4; distance:2; byte\_test:2,>,28,0,relative; metadata:policy security-ips drop; reference:bugtraq,13678; reference:cve,2005-1543; classtype:attempted-admin; sid:15958; rev:4;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Microsoft Windows .NET Chart Control directory traversal attempt"; flow:to\_server,established; content:"charImg.axd?"; content:"i=/"; distance:0; http\_uri; content:".."; distance:0; http\_uri; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:cve,2011-1977; reference:url,technet.microsoft.com/en-us/security/bulletin/MS11-066; classtype:attempted-recon; sid:19694; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP rolis guestbook remote file include attempt"; flow:to\_server,established; content:"/insert.inc.php"; fast\_pattern; nocase; http\_uri; content:"path="; metadata:service http; reference:bugtraq,9057; classtype:web-application-attack; sid:2284; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP autohtml.php directory traversal attempt"; flow:to\_server,established; content:"/autohtml.php"; fast\_pattern; nocase; http\_uri; content:"name="; content:"../../"; distance:0; metadata:service http; reference:nessus,11630; classtype:web-application-attack; sid:2153; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Emumail emumail.fcgi access"; flow:to\_server,established; content:"/emumail.fcgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,9861; reference:nessus,12095; classtype:web-application-activity; sid:2568; rev:13;)

alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Symantec Web Gateway pbcontrol.php filename parameter command injection attempt"; flow:to\_server,established; content:"/spywall/pbcontrol.php"; fast\_pattern:only; http\_uri; pcre:"/[?&]filename=[^&]\*?[\x22\x27]\x3B/Ui"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,54426; reference:cve,2012-2953; classtype:attempted-admin; sid:23783; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP /fcgi-bin/echo.exe access"; flow:to\_server,established; content:"/fcgi-bin/echo.exe"; nocase; http\_uri; metadata:service http; reference:nessus,10838; classtype:web-application-activity; sid:1592; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP .nsconfig access"; flow:to\_server,established; content:"/.nsconfig"; http\_uri; metadata:service http; reference:url,www.osvdb.org/5709; classtype:attempted-recon; sid:1209; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Oracle GlassFish server REST interface cross site request forgery attempt"; flow:to\_server,established; content:"POST"; http\_method; content:"/management/domain/applications/application"; fast\_pattern:only; http\_uri; content:"Content-Disposition:"; http\_client\_body; content:".war"; http\_client\_body; pcre:"/Content-Disposition\x3a[^\n]+filename\s\*=\s\*[\x22\x27][^\x22\x27]\*?\.war[\x22\x27]/iP"; metadata:policy security-ips drop, service http; reference:cve,2012-0550; reference:url,osvdb.org/show/osvdb/81225; classtype:attempted-user; sid:23401; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP eXtropia webstore access"; flow:to\_server,established; content:"/web\_store.cgi"; http\_uri; metadata:service http; reference:bugtraq,1774; reference:cve,2000-1005; reference:nessus,10532; classtype:web-application-activity; sid:1611; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Amaya templates sendtemp.pl directory traversal attempt"; flow:to\_server,established; content:"/sendtemp.pl"; fast\_pattern; nocase; http\_uri; content:"templ="; nocase; metadata:service http; reference:bugtraq,2504; reference:cve,2001-0272; reference:nessus,10614; classtype:web-application-attack; sid:899; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP perl post attempt"; flow:to\_server,established; content:"POST"; depth:4; content:"/perl/"; http\_uri; metadata:service http; reference:bugtraq,5520; reference:cve,2002-1436; reference:nessus,11158; classtype:web-application-attack; sid:1979; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP admentor admin.asp access"; flow:to\_server,established; content:"/admentor/admin/admin.asp"; http\_uri; metadata:service http; reference:bugtraq,4152; reference:cve,2002-0308; reference:nessus,10880; reference:url,www.securiteam.com/windowsntfocus/5DP0N1F6AW.html; classtype:web-application-activity; sid:1503; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Invision Board emailer.php file include"; flow:to\_server,established; content:"/ad\_member.php"; fast\_pattern; nocase; http\_uri; content:"emailer.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,7204; classtype:web-application-activity; sid:2355; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 1111 (msg:"SERVER-WEBAPP F-Secure web console username overflow attempt"; flow:to\_server,established; content:"/authorise"; nocase; content:"userName"; fast\_pattern; nocase; isdataat:500,relative; pcre:"/userName\s\*=([^\x5C\x26]{500}|[^5C]+\x5C[^\x26]{500})/i"; metadata:policy security-ips drop; reference:bugtraq,18201; reference:cve,2006-2838; classtype:attempted-admin; sid:20726; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 1311 (msg:"SERVER-WEBAPP Dell OpenManage server application field buffer overflow attempt"; flow:to\_server,established; content:"Dell Computer Corporation"; fast\_pattern; nocase; content:"user|3D|"; distance:0; nocase; content:"password|3D|"; distance:0; nocase; content:"application|3D|"; distance:0; nocase; isdataat:194,relative; content:!"|26|"; within:194; reference:cve,2004-0331; classtype:attempted-user; sid:20740; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP windmail.exe access"; flow:to\_server,established; content:"/windmail.exe"; nocase; http\_uri; metadata:service http; reference:bugtraq,1073; reference:cve,2000-0242; reference:nessus,10365; classtype:attempted-recon; sid:1158; rev:17;)

alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP libtidy null pointer dereference attempt"; flow:to\_server,established; content:"<?"; content:"Tidy"; distance:0; content:"diagnose"; fast\_pattern:only; pcre:"/(?P<var>\x24\w+)\s\*=\s\*(new Tidy|Tidy->new)\x28\s\*[\x22\x27]\x2a[\x22\x27]\s\*\x29.{1,256}(?P=var)->diagnose/ims"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:cve,2011-4153; classtype:attempted-dos; sid:23995; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ad.cgi access"; flow:to\_server,established; content:"/ad.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,2103; reference:cve,2001-0025; reference:nessus,11464; classtype:web-application-activity; sid:1709; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP SpamExcp.dll access"; flow:to\_server,established; content:"/SpamExcp.dll"; nocase; http\_uri; metadata:service http; reference:bugtraq,3327; reference:cve,2001-0958; reference:nessus,11747; classtype:web-application-activity; sid:2235; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP basilix mysql.class access"; flow:to\_server,established; content:"/class/mysql.class"; http\_uri; metadata:service http; reference:bugtraq,2198; reference:cve,2001-1044; reference:nessus,10601; classtype:web-application-activity; sid:1527; rev:14;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP OpenView Network Node Manager URI rping stack buffer overflow attempt"; flow:to\_server,established; content:"/OvCgi/webappmon.exe"; nocase; content:"act=rping"; distance:0; nocase; pcre:"/sel\x3d[^\x26\x0a]{73}/i"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,35267; reference:cve,2009-1420; classtype:attempted-user; sid:15726; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP TUTOS path disclosure attempt"; flow:to\_server,established; content:"/note\_overview.php"; http\_uri; content:"id="; metadata:service http; reference:bugtraq,10129; reference:url,www.securiteam.com/unixfocus/5FP0J15CKE.html; classtype:web-application-activity; sid:2588; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP webdist.cgi access"; flow:to\_server,established; content:"/webdist.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,374; reference:cve,1999-0039; reference:nessus,10299; classtype:web-application-activity; sid:1163; rev:17;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 383 (msg:"SERVER-WEBAPP HP Operations Agent stack buffer overflow attempt"; flow:to\_server,established; flowbits:isset,hp\_openview\_coda; content:"|00 00 00 96|"; depth:4; offset:18; byte\_jump:2,8,relative; byte\_jump:2,12,relative; byte\_test:2,>,1024,0,relative; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,54362; reference:cve,2012-2019; reference:url,h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03397769; classtype:attempted-admin; sid:24318; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP b2 cafelog gm-2-b2.php access"; flow:to\_server,established; content:"/gm-2-b2.php"; nocase; http\_uri; metadata:service http; reference:nessus,11667; classtype:web-application-activity; sid:2144; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ppdscgi.exe access"; flow:to\_server,established; content:"/ppdscgi.exe"; nocase; http\_uri; metadata:service http; reference:bugtraq,491; reference:nessus,10187; reference:url,online.securityfocus.com/archive/1/16878; classtype:attempted-recon; sid:889; rev:20;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Oracle ONE Web Server JSP source code disclosure attempt"; flow:to\_server,established; content:".jsp"; nocase; http\_uri; content:"|3A 3A 24|DATA"; distance:0; nocase; metadata:policy security-ips drop, service http; reference:cve,2009-2445; classtype:misc-attack; sid:16682; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Netscape Enterprise directory listing attempt"; flow:to\_server,established; content:"INDEX "; depth:6; metadata:service http; reference:bugtraq,2285; reference:cve,2001-0250; reference:nessus,10691; classtype:web-application-attack; sid:1048; rev:15;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Cisco Common Services Device Center XSS attempt"; flow:to\_server,established; content:"/cwhp/device.center.do"; fast\_pattern:only; http\_uri; pcre:"/device\.center\.do\?[^$\n]\*(DeviceID|objectID|dsOsName|device)=[^$\n]\*([\x3C\x3E\x22\x27]|script|src|location|document)/Ui"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:cve,2011-0962; classtype:web-application-attack; sid:21389; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Oracle 10g iSQLPlus login.unix connectID overflow attempt"; flow:to\_server,established; content:"/login.uix"; nocase; http\_uri; content:"connectID="; nocase; isdataat:255,relative; pcre:"/connectID=[^&\x3b\r\n]{255}/smi"; metadata:service http; reference:bugtraq,10871; reference:url,www.nextgenss.com/advisories/ora-isqlplus.txt; classtype:web-application-attack; sid:2704; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP phpBB mod tag board sql injection attempt"; flow:to\_server,established; content:"tag\_board.php"; fast\_pattern; nocase; http\_uri; content:"action=delete"; nocase; http\_uri; content:"id="; nocase; http\_uri; pcre:"/tag\_board\.php\x3F[^\r\n]\*action=delete[^\r\n]\*id=[^\r\n\x26]\*(select|insert|delete)/Usmi"; metadata:policy security-ips alert, service http; reference:bugtraq,32701; reference:cve,2008-6314; classtype:web-application-attack; sid:15425; rev:11;)

#alert tcp $HOME\_NET any -> $EXTERNAL\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP RealNetworks RealPlayer realtext long URI request attempt"; flow:to\_server,established; content:".rt"; fast\_pattern:only; http\_uri; pcre:"/\x2f[^\x2f]{188,}\x2ert/Ui"; metadata:service http; reference:bugtraq,14048; reference:cve,2005-1766; reference:nessus,18558; classtype:protocol-command-decode; sid:3822; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 9850 (msg:"SERVER-WEBAPP Novell GroupWise Internet Agent content-length integer overflow attempt"; flow:to\_server,established; content:"Content-Length: -1|0D 0A|"; fast\_pattern:only; metadata:policy security-ips drop, service http; reference:bugtraq,55551; reference:cve,2012-0271; classtype:attempted-admin; sid:24239; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP sojourn.cgi access"; flow:to\_server,established; content:"/sojourn.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,1052; reference:cve,2000-0180; reference:nessus,10349; classtype:web-application-activity; sid:1195; rev:20;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP viewtopic.php access"; flow:to\_server,established; content:"/viewtopic.php"; fast\_pattern; nocase; http\_uri; content:"days="; nocase; http\_uri; metadata:service http; reference:bugtraq,7979; reference:cve,2003-0486; reference:nessus,11767; classtype:web-application-attack; sid:2229; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP search.cgi access"; flow:to\_server,established; content:"/search.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,921; reference:cve,2000-0054; classtype:web-application-activity; sid:1599; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP gallery remote file include attempt"; flow:to\_server,established; content:"/setup/"; http\_uri; content:"GALLERY\_BASEDIR="; http\_uri; pcre:"/GALLERY\_BASEDIR=(https?|ftps?|php)/Ui"; metadata:service http; reference:bugtraq,8814; reference:nessus,11876; classtype:web-application-attack; sid:2306; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP count.cgi access"; flow:to\_server,established; content:"/count.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,128; reference:cve,1999-0021; reference:nessus,10049; classtype:web-application-activity; sid:1149; rev:22;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Novell ZENworks Configuration Management UploadServlet code execution attempt"; flow:to\_server,established; content:"/zenworks-fileupload/?"; nocase; pcre:"/(filename|type)=[^\x26]\*?\x2E\x2E/R"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,39914; reference:url,www.novell.com/support/viewContent.do?externalId=7005573; classtype:attempted-admin; sid:18793; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP classifieds.cgi access"; flow:to\_server,established; content:"/classifieds.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,2020; reference:cve,1999-0934; classtype:attempted-recon; sid:854; rev:17;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP sqlmap SQL injection scan attempt"; flow:to\_server,established; content:"User-Agent|3A| sqlmap"; fast\_pattern:only; http\_header; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:url,sqlmap.sourceforge.net; classtype:web-application-activity; sid:19779; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Nortel Contivity cgiproc access"; flow:to\_server,established; content:"/cgiproc"; http\_uri; metadata:service http; reference:bugtraq,938; reference:cve,2000-0063; reference:cve,2000-0064; reference:nessus,10160; classtype:web-application-activity; sid:1765; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP console.exe access"; flow:to\_server,established; content:"/cgi-bin/console.exe"; nocase; http\_uri; metadata:service http; reference:bugtraq,3375; reference:cve,2001-1252; classtype:attempted-recon; sid:1302; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP redirect.exe access"; flow:to\_server,established; content:"/redirect.exe"; nocase; http\_uri; metadata:service http; reference:bugtraq,1256; reference:cve,2000-0401; reference:nessus,11723; classtype:web-application-activity; sid:2239; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP perl.exe access"; flow:to\_server,established; content:"/perl.exe"; nocase; http\_uri; metadata:service http; reference:cve,1999-0509; reference:nessus,10173; reference:url,www.cert.org/advisories/CA-1996-11.html; classtype:attempted-recon; sid:832; rev:22;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP philboard.mdb access"; flow:to\_server,established; content:"/philboard.mdb"; http\_uri; metadata:service http; reference:nessus,11682; classtype:web-application-activity; sid:2135; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP jigsaw dos attempt"; flow:to\_server,established; content:"/servlet/con"; http\_uri; pcre:"/\x2Fcon\b/Ui"; metadata:service http; reference:bugtraq,5258; reference:cve,2002-1052; reference:nessus,11047; classtype:web-application-attack; sid:1831; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP System variable directory traversal attempt - %HOMEPATH%"; flow:to\_server,established; content:"%HOMEPATH%"; fast\_pattern:only; http\_uri; metadata:service http; classtype:attempted-recon; sid:21825; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ksh access"; flow:to\_server,established; content:"/ksh"; nocase; http\_uri; metadata:service http; reference:cve,1999-0509; reference:url,www.cert.org/advisories/CA-1996-11.html; classtype:attempted-recon; sid:865; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Lotus DelDoc attempt"; flow:to\_server,established; content:"?DeleteDocument"; nocase; http\_uri; metadata:service http; classtype:attempted-recon; sid:1116; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS 80 (msg:"SERVER-WEBAPP sphpblog password.txt access attempt"; flow:to\_server,established; content:"sphpblog"; http\_uri; content:"password.txt"; fast\_pattern; nocase; http\_uri; metadata:service http; reference:bugtraq,14667; reference:cve,2005-2733; classtype:attempted-user; sid:11664; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP convert.bas access"; flow:to\_server,established; content:"/scripts/convert.bas"; nocase; http\_uri; metadata:service http; reference:bugtraq,2025; reference:cve,1999-0175; classtype:attempted-recon; sid:1127; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP nph-exploitscanget.cgi access"; flow:to\_server,established; content:"/nph-exploitscanget.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,7910; reference:bugtraq,7911; reference:bugtraq,7913; reference:cve,2003-0434; reference:nessus,11740; classtype:web-application-activity; sid:2222; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP .history access"; flow:to\_server,established; content:"/.history"; http\_uri; metadata:service http; classtype:web-application-attack; sid:1433; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP phpbb quick-reply.php arbitrary command attempt"; flow:to\_server,established; content:"/quick-reply.php"; http\_uri; content:"phpbb\_root\_path="; metadata:service http; reference:bugtraq,6173; classtype:web-application-attack; sid:1967; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ustorekeeper.pl access"; flow:to\_server,established; content:"/ustorekeeper.pl"; nocase; http\_uri; metadata:service http; reference:cve,2001-0466; reference:nessus,10645; classtype:web-application-activity; sid:1483; rev:20;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP w3tvars.pm access"; flow:to\_server,established; content:"/w3tvars.pm"; nocase; http\_uri; metadata:service http; classtype:attempted-recon; sid:878; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Ipswitch WhatsUp Gold dos attempt"; flow:to\_server,established; content:"/prn"; nocase; http\_uri; pcre:"/\/prn\.(asp|cgi|html?)/Ui"; metadata:service http; reference:bugtraq,11110; reference:cve,2004-0799; reference:url,www.idefense.com/application/poi/display?id=142&type=vulnerabilities; reference:url,www.ipswitch.com/Support/WhatsUp/patch-upgrades.html; reference:url,www.secunia.com/advisories/12578/; classtype:attempted-dos; sid:3469; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP input2.bat access"; flow:to\_server,established; content:"/input2.bat"; http\_uri; metadata:service http; reference:bugtraq,762; reference:cve,1999-0947; reference:nessus,10016; classtype:web-application-activity; sid:1515; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 9090 (msg:"SERVER-WEBAPP Jive Software Openfire logviewer.jsp XSS attempt"; flow:to\_server,established; content:"/logviewer.jsp"; fast\_pattern:only; http\_uri; pcre:"/logviewer\.jsp\?.\*?=([^\x26]\*[\x22\x27\x3C\x3E\x28\x29\x3B]|script|src|location|document)/U"; metadata:policy security-ips drop, service http; reference:bugtraq,32935; reference:cve,2009-0496; classtype:web-application-attack; sid:20862; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 3443 (msg:"SERVER-WEBAPP HP Openview NNM cdpView.ovpl port 3443 Unix command execution attempt"; flow:to\_server,established; content:"/cdpView.ovpl"; nocase; http\_uri; content:"cdpnode="; nocase; http\_uri; pcre:"/cdpView\.ovpl[^\r\n]\*cdpnode=[^\r\n]\*%[\x2c\x24\x7c\x3b\x22\x26\x3c\x3f]/Usmi"; metadata:service http; reference:bugtraq,14662; reference:cve,2005-2773; classtype:web-application-attack; sid:8086; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cgiforum.pl attempt"; flow:to\_server,established; content:"/cgiforum.pl?thesection=../.."; nocase; http\_uri; metadata:service http; reference:bugtraq,1963; reference:cve,2000-1171; reference:nessus,10552; classtype:web-application-attack; sid:1573; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP printmail.cgi access"; flow:to\_server,established; content:"/printmail.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,3427; reference:bugtraq,4579; reference:cve,2001-1283; reference:nessus,11748; classtype:web-application-activity; sid:2217; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP testcgi access"; flow:to\_server,established; content:"/testcgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,7214; reference:nessus,11610; classtype:web-application-activity; sid:1645; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP phpinfo GET POST and COOKIE Parameters cross site scripting attempt"; flow:to\_server,established; content:"|3D|"; content:"script"; within:9; nocase; pcre:"/(\x5B|\x25\x35\x62)(\x5D|\x25\x35\x64)\x3D(\x3C|\x25\x33\x63)script/i"; metadata:service http; reference:cve,2007-1287; reference:url,php-security.org/MOPB/MOPB-08-2007.html; classtype:attempted-user; sid:21670; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP bslist.cgi access"; flow:to\_server,established; content:"/bslist.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,2160; reference:cve,2001-0100; classtype:web-application-activity; sid:1712; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Chunked-Encoding transfer attempt"; flow:to\_server,established; content:"Transfer-Encoding|3A|"; nocase; http\_header; content:"chunked"; nocase; http\_header; metadata:service http; reference:bugtraq,4474; reference:bugtraq,4485; reference:bugtraq,5033; reference:cve,2002-0071; reference:cve,2002-0079; reference:cve,2002-0392; reference:nessus,10932; classtype:web-application-attack; sid:1807; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 9090 (msg:"SERVER-WEBAPP Jive Software Openfire muc-room-edit-form.jsp XSS attempt"; flow:to\_server,established; content:"/muc-room-edit-form.jsp"; fast\_pattern:only; http\_uri; pcre:"/muc-room-edit-form\.jsp\?.\*?=([^\x26]\*[\x22\x27\x3C\x3E\x28\x29\x3B]|script|src|location|document)/U"; metadata:policy security-ips drop, service http; reference:bugtraq,32935; reference:cve,2009-0496; classtype:web-application-attack; sid:20868; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP imagemap.exe access"; flow:to\_server,established; content:"/imagemap.exe"; nocase; http\_uri; metadata:service http; reference:bugtraq,739; reference:cve,1999-0951; reference:nessus,10122; classtype:web-application-activity; sid:1700; rev:19;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 4080 (msg:"SERVER-WEBAPP iChat directory traversal attempt"; flow:to\_server,established; content:"/../../"; reference:cve,1999-0897; classtype:web-application-activity; sid:1604; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP alibaba.pl arbitrary command execution attempt"; flow:to\_server,established; content:"/alibaba.pl|7C|"; http\_uri; metadata:service http; reference:bugtraq,770; reference:cve,1999-0885; reference:nessus,10013; classtype:web-application-attack; sid:1507; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP fom.cgi access"; flow:to\_server,established; content:"/fom.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,4579; reference:cve,2002-0230; reference:nessus,11748; classtype:web-application-activity; sid:2208; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Twiki view rev command injection attempt"; flow:to\_server,established; content:"/view/"; nocase; http\_uri; content:"twiki"; distance:0; nocase; http\_uri; content:"|7C|"; distance:0; nocase; http\_uri; metadata:service http; reference:bugtraq,14834; reference:cve,2005-2877; classtype:attempted-admin; sid:4986; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP anform2 access"; flow:to\_server,established; content:"/AnForm2"; nocase; http\_uri; metadata:service http; reference:bugtraq,719; reference:cve,1999-0066; classtype:attempted-recon; sid:843; rev:20;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP vpasswd.cgi access"; flow:to\_server,established; content:"/vpasswd.cgi"; http\_uri; metadata:service http; reference:bugtraq,6038; reference:nessus,11165; classtype:web-application-activity; sid:1994; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cd.."; flow:to\_server,established; content:"cd.."; nocase; metadata:service http; classtype:attempted-recon; sid:1136; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP wwwboard.pl access"; flow:to\_server,established; content:"/wwwboard.pl"; nocase; http\_uri; metadata:service http; reference:bugtraq,1795; reference:bugtraq,649; reference:cve,1999-0930; reference:cve,1999-0954; classtype:attempted-recon; sid:1175; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP args.cmd access"; flow:to\_server,established; content:"/args.cmd"; nocase; http\_uri; metadata:service http; reference:cve,1999-1180; reference:nessus,11465; classtype:attempted-recon; sid:1452; rev:17;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP OpenView Network Node Manager cookie buffer overflow attempt"; flow:to\_server,established; content:"/OVCgi/ovlaunch.exe"; fast\_pattern:only; http\_uri; pcre:"/(OvJavaScript|OvTitleFrame|OvHelpWindow|OvMap|OvSession|OvJavaLocale|OvOSLocale|OvLogin|OvDebug|OvDeveloper|OvTreeControl|OvJavaScript|OvProduct|OvPort|OvLocale|OvWebSession)\s\*\x3D[^\x3B\x2C]{1024}/iC"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,42154; reference:cve,2010-2709; classtype:attempted-user; sid:18915; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Venom Board SQL injection attempt"; flow:to\_server,established; content:"venomboard|2F|forum"; fast\_pattern; nocase; http\_uri; content:"post.php3"; nocase; http\_uri; content:"parent="; nocase; http\_uri; pcre:"/\x2Fpost\.php3?[^\r\n]\*?parent=[^\r\n\x26]\*?union[^\r\n\x26]\*select/Ui"; metadata:service http; reference:bugtraq,16176; reference:cve,2006-0160; classtype:web-application-activity; sid:20624; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Blahz-DNS dostuff.php modify user attempt"; flow:to\_server,established; content:"/dostuff.php?action=modify\_user"; nocase; http\_uri; metadata:service http; reference:bugtraq,4618; reference:cve,2002-0599; classtype:web-application-attack; sid:1742; rev:15;)

alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP nessus 2.x 404 probe"; flow:to\_server,established; content:"/NessusTest"; nocase; http\_uri; metadata:policy balanced-ips drop, policy connectivity-ips drop, policy security-ips drop, service http; reference:nessus,10386; classtype:attempted-recon; sid:2585; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP jrun directory browse attempt"; flow:to\_server,established; content:"/?.jsp"; http\_uri; metadata:service http; reference:bugtraq,3592; classtype:web-application-attack; sid:1376; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ISAPISkeleton.dll access"; flow:to\_server,established; content:"/ISAPISkeleton.dll"; nocase; http\_uri; metadata:service http; reference:bugtraq,9516; classtype:web-application-activity; sid:2369; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Advanced Poll booth.php access"; flow:to\_server,established; content:"/booth.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,8890; reference:nessus,11487; classtype:web-application-activity; sid:2301; rev:14;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP Intelligent Management Center database credentials information disclosure attempt - 1"; flow:to\_server,established; content:"/imc/reportscript/sqlserver/deploypara.properties"; nocase; http\_uri; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,40298; reference:url,secunia.com/advisories/39891; classtype:attempted-user; sid:17157; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 8090 (msg:"SERVER-WEBAPP TrackerCam negative Content-Length attempt"; flow:to\_server,established; content:"Content-Length|3A|"; nocase; pcre:"/^Content-Length\x3a(\s\*|\s\*\r?\n\s+)-\d+/smi"; reference:bugtraq,12592; reference:cve,2005-0481; classtype:web-application-attack; sid:3548; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Netscape Enterprise Server directory view"; flow:to\_server,established; content:"?wp-cs-dump"; nocase; http\_uri; metadata:service http; reference:bugtraq,1063; reference:cve,2000-0236; reference:nessus,10352; classtype:attempted-recon; sid:1183; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Domino domcfg.nsf access"; flow:to\_server,established; content:"/domcfg.nsf"; nocase; http\_uri; metadata:service http; reference:nessus,10629; classtype:attempted-recon; sid:1151; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ax-admin.cgi access"; flow:to\_server,established; content:"/ax-admin.cgi"; http\_uri; metadata:service http; classtype:web-application-activity; sid:1204; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ibillpm.pl access"; flow:to\_server,established; content:"/ibillpm.pl"; nocase; http\_uri; metadata:service http; reference:bugtraq,3476; reference:cve,2001-0839; reference:nessus,11083; classtype:web-application-activity; sid:2669; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Oracle Secure Backup Administration Server authentication bypass attempt"; flow:to\_server,established; content:"login.php"; nocase; http\_uri; content:"attempt"; nocase; http\_uri; content:"uname="; nocase; http\_uri; pcre:"/uname\x3D[^\x26\x2D\s]\*?\x2D/iU"; metadata:policy security-ips drop, service http; reference:bugtraq,41596; reference:cve,2010-0904; classtype:attempted-admin; sid:17050; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP rpc-smb.pl access"; flow:to\_server,established; content:"/rpc-smb.pl"; http\_uri; metadata:service http; reference:cve,1999-1278; classtype:web-application-activity; sid:1932; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Cisco IOS HTTP configuration attempt"; flow:to\_server,established; content:"/level/"; http\_uri; pcre:"/\x2flevel\x2f\d+\x2f(exec|configure)/iU"; metadata:service http; reference:bugtraq,2936; reference:cve,2001-0537; reference:nessus,10700; classtype:web-application-attack; sid:1250; rev:19;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS 1220 (msg:"SERVER-WEBAPP streaming server parse\_xml.cgi access"; flow:to\_server,established; content:"/parse\_xml.cgi"; fast\_pattern:only; reference:bugtraq,6954; reference:bugtraq,6955; reference:bugtraq,6956; reference:bugtraq,6958; reference:cve,2003-0050; reference:cve,2003-0051; reference:cve,2003-0052; reference:cve,2003-0053; reference:cve,2003-0423; classtype:web-application-activity; sid:2086; rev:11;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP OpenView Network Node Manager cookie buffer overflow attempt"; flow:to\_server,established; content:"/OVCgi/ovlogin.exe"; fast\_pattern:only; http\_uri; pcre:"/(OvJavaScript|OvTitleFrame|OvHelpWindow|OvMap|OvSession|OvJavaLocale|OvOSLocale|OvLogin|OvDebug|OvDeveloper|OvTreeControl|OvJavaScript|OvProduct|OvPort|OvLocale|OvWebSession)\s\*\x3D[^\x3B\x2C]{1024}/iC"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,42154; reference:cve,2010-2709; classtype:attempted-user; sid:18917; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP TSEP remote file include in colorswitch.php tsep\_config[absPath]"; flow:to\_server,established; content:"tsep\_config[absPath]="; fast\_pattern:only; http\_uri; pcre:"/\x2F(colorswitch|copyright)\.php\?[^\r\n]\*?tsep\_config\x5BabsPath\x5D\x3D(https?|ftps?)\x3A\x2F/Ui"; metadata:service http; reference:bugtraq,19326; reference:cve,2006-3993; classtype:web-application-attack; sid:20731; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 2301 (msg:"SERVER-WEBAPP Compaq web-based management agent denial of service attempt"; flow:to\_server,established; content:"<!"; depth:75; content:">"; within:50; reference:bugtraq,8014; classtype:web-application-attack; sid:2394; rev:7;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 8080 (msg:"SERVER-WEBAPP Novell iManager eDirectory plugin schema buffer overflow attempt - GET request"; flow:to\_server,established; content:"GET"; nocase; http\_method; content:"/nps/servlet/"; nocase; http\_uri; content:"taskId=base.ExtendSchema"; nocase; http\_uri; pcre:"/(((DestFile|encryptPass)\x3D[^\x26]{50})|((BaseDN|SearchFilter)\x3D[^\x26]{128}))/Ui"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,37672; reference:cve,2009-4486; classtype:attempted-admin; sid:16429; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP WordPress XSS fs-admin.php injection attempt"; flow:established,to\_server; content:"page=forum-server/fs-admin/fs-admin.php"; fast\_pattern:only; http\_uri; pcre:"/[?&](groupid|usergroup\_id)=[^&]+?([\x22\x27\x3c\x3e\x28\x29]|script|onload|src)/Ui"; metadata:policy security-ips drop, service http; classtype:web-application-attack; sid:24561; rev:1;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Advanced Poll poll\_ssi.php access"; flow:to\_server,established; content:"/poll\_ssi.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,8890; reference:nessus,11487; classtype:web-application-activity; sid:2302; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP edittag.pl access"; flow:to\_server,established; content:"/edittag.pl"; nocase; http\_uri; metadata:service http; reference:bugtraq,6675; classtype:web-application-activity; sid:2400; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Mambo upload.php upload php file attempt"; flow:to\_server,established; content:"/upload.php"; http\_uri; content:"userfile\_name="; content:".php"; distance:1; metadata:service http; reference:bugtraq,6572; reference:cve,2003-1204; reference:nessus,16315; classtype:web-application-attack; sid:2075; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Oracle Java System Web Server 7.0 WebDAV format string exploit attempt - LOCK method"; flow:to\_server,established; content:"LOCK"; nocase; http\_method; content:"<?xml"; fast\_pattern; content:"encoding"; within:50; pcre:"/\<\?xml[^\>]+encoding\s\*\=\s\*(\'|\")[^\'\"\>\%]\*\%/"; metadata:service http; reference:bugtraq,37910; reference:cve,2010-0388; classtype:attempted-user; sid:16427; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP test.bat arbitrary command execution attempt"; flow:to\_server,established; content:"/test.bat|7C|"; http\_uri; metadata:service http; reference:bugtraq,762; reference:cve,1999-0947; reference:nessus,10016; classtype:web-application-attack; sid:1510; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP 4DWebstar ShellExample.cgi information disclosure"; flow:to\_server,established; content:"/ShellExample.cgi"; nocase; http\_uri; pcre:"/ShellExample\.cgi\?[^\n\r\&]\*\x2a/Ui"; metadata:service http; reference:bugtraq,10721; reference:url,www.atstake.com/research/advisories/2004/a071304-1.txt; classtype:attempted-recon; sid:4128; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP Data Protector FinishedCopy SQL Injection attempt"; flow:to\_server,established; content:"POST"; nocase; http\_method; content:"/dpnepolicyservice/DPNECentral.asmx"; nocase; http\_uri; content:"FinishedCopy"; nocase; http\_client\_body; content:"<type"; distance:0; nocase; http\_client\_body; content:"|3B|"; distance:0; http\_client\_body; content:"</type"; distance:0; nocase; http\_client\_body; metadata:service http; reference:cve,2011-3162; reference:url,h20565.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr\_na-c03058866&ac.admitted=1321285525395.876444892.492883150; reference:url,osvdb.org/show/osvdb/76707; classtype:attempted-user; sid:20628; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP handler access"; flow:to\_server,established; content:"/handler"; nocase; http\_uri; metadata:service http; reference:bugtraq,380; reference:cve,1999-0148; reference:nessus,10100; classtype:web-application-activity; sid:1141; rev:17;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP Data Protector Media Operations SignInName Parameter overflow attempt"; flow:to\_server,established; content:"/4daction/wHandleURLs/handleSignIn"; fast\_pattern:only; http\_uri; content:"SignInName="; nocase; http\_client\_body; isdataat:256,relative; content:!"&"; within:256; http\_client\_body; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,44381; classtype:attempted-admin; sid:19155; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET [80,8000] (msg:"SERVER-WEBAPP IceCast header buffer overflow attempt"; flow:to\_server,established; content:"HTTP/1."; nocase; isdataat:32,relative; pcre:"/HTTP\/1\.[01].\*?\n([^\r\n]+?\r?\n){32}/i"; reference:bugtraq,11271; reference:cve,2004-1561; reference:url,archives.neohapsis.com/archives/bugtraq/2004-09/0366.html; classtype:attempted-admin; sid:8701; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Lizard Cart CMS SQL injection in pages.php id attempt"; flow:to\_server,established; content:"pages.php"; fast\_pattern:only; http\_uri; content:"id"; nocase; pcre:"/id=[^\r\n\x26]\*?([\x22\x27]|%2[27])/i"; metadata:service http; reference:bugtraq,16140; reference:cve,2006-0087; classtype:web-application-attack; sid:20645; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP PHP truncated crypt function attempt"; flow:to\_server,established; content:"crypt("; fast\_pattern:only; http\_client\_body; content:"<?"; http\_client\_body; pcre:"/((?P<m1>\$\w+)\s\*=\s\*(?P<q1>[\x22\x27])\s\*[^(?P=q1)]+(\\x80|\x80).\*?crypt\(\s\*(?P=m1)|crypt\(\s\*(?P<q2>[\x22\x27])\s\*[^(?P=q1)]+(\\x80|\x80))/Psmi"; metadata:policy security-ips drop, service http; reference:cve,2012-2143; classtype:attempted-admin; sid:23896; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP wwwwais access"; flow:to\_server,established; content:"/wwwwais"; nocase; http\_uri; metadata:service http; reference:cve,2001-0223; reference:nessus,10597; classtype:attempted-recon; sid:1454; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Domino bookmark.nsf access"; flow:to\_server,established; content:"/bookmark.nsf"; nocase; http\_uri; metadata:service http; reference:nessus,10629; classtype:attempted-recon; sid:1584; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ttCMS header.php remote file include attempt"; flow:to\_server,established; content:"/admin/templates/header.php"; fast\_pattern; nocase; http\_uri; content:"admin\_root="; pcre:"/admin\_root=(https?|ftps?|php)/"; metadata:service http; reference:bugtraq,7542; reference:bugtraq,7543; reference:bugtraq,7625; reference:nessus,11636; classtype:web-application-attack; sid:2150; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Nortel Contivity cgiproc DOS attempt"; flow:to\_server,established; content:"/cgiproc?|24|"; http\_uri; metadata:service http; reference:bugtraq,938; reference:cve,2000-0063; reference:cve,2000-0064; reference:nessus,10160; classtype:web-application-attack; sid:1764; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP loadpage.cgi access"; flow:to\_server,established; content:"/loadpage.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,2109; reference:cve,2000-1092; reference:nessus,10065; classtype:web-application-activity; sid:1570; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 8004 (msg:"SERVER-WEBAPP Symantec Antivirus admin scan interface negative Content-Length attempt"; flow:to\_server,established; content:"Content-Length|3A| -1"; fast\_pattern:only; metadata:service http; reference:bugtraq,15001; reference:cve,2005-2758; classtype:attempted-admin; sid:4681; rev:8;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Oracle GlassFish Server authentication bypass attempt"; flow:to\_server,established; content:"GET"; nocase; http\_method; content:"/applications/upload"; http\_uri; pcre:"/^(Frame)?\.jsf/R"; content:!"JSESSIONID="; flowbits:set,glassfish\_unauth\_attempt; metadata:policy security-ips drop, service http; reference:bugtraq,47438; reference:cve,2011-0807; classtype:attempted-admin; sid:20159; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Oracle iSQL Plus cross site scripting attempt"; flow:to\_server,established; content:"/isqlplus"; nocase; http\_uri; content:"password="; nocase; http\_uri; pcre:"/password[\x3d\x3f][^\n\x26]\*\x3c[^\n\x26]+\x3e/Ui"; metadata:service http; reference:bugtraq,9484; reference:cve,2004-2115; classtype:web-application-attack; sid:11685; rev:8;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP test-cgi attempt"; flow:to\_server,established; content:"/test-cgi/\*?\*"; nocase; http\_uri; metadata:service http; reference:bugtraq,2003; reference:cve,1999-0070; reference:nessus,10282; classtype:web-application-attack; sid:1644; rev:19;)

alert tcp $EXTERNAL\_NET $FILE\_DATA\_PORTS -> $HOME\_NET any (msg:"SERVER-WEBAPP Invalid global flag attachment attempt"; flow:to\_client,established; file\_data; content:"<?php"; content:"ZipArchive"; content:"addGlob"; distance:0; pcre:"/\x24(?P<var1>\w\*)\s\*\x3d\s\*new\s\*ZipArchive\x28\x29.\*?\x24(?P=var1)\x2d\x3eaddGlob\x28[\x22\x27]?(?!GLOB\_BRACE|GLOB\_MARK|GLOB\_NOSORT|GLOB\_NOCHECK|GLOB\_NOESCAPE|GLOB\_ERR|GLOB\_ONLYDIR)/smi"; metadata:policy balanced-ips drop, policy security-ips drop, service http, service imap, service pop3; reference:bugtraq,49252; reference:cve,2011-1471; classtype:denial-of-service; sid:23937; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP /Carello/add.exe access"; flow:to\_server,established; content:"/Carello/add.exe"; nocase; http\_uri; metadata:service http; reference:bugtraq,1245; reference:cve,2000-0396; reference:nessus,11776; classtype:web-application-activity; sid:1943; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP JBoss JMX console access attempt"; flow:to\_server,established; content:"/jmx-console/"; fast\_pattern:only; http\_uri; metadata:service http; reference:cve,2007-1036; reference:url,docs.jboss.org/jbossas/6/Admin\_Console\_Guide/en-US/pdf/Admin\_Console\_Guide.pdf; classtype:attempted-recon; sid:21516; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cPanel resetpass access"; flow:to\_server,established; content:"/resetpass"; nocase; http\_uri; metadata:service http; reference:bugtraq,9848; reference:cve,2004-1769; classtype:web-application-activity; sid:2569; rev:8;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Phorum violation access"; flow:to\_server,established; content:"/violation.php3"; nocase; http\_uri; metadata:service http; reference:bugtraq,2272; classtype:attempted-recon; sid:1179; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Domino mab.nsf access"; flow:to\_server,established; content:"/mab.nsf"; nocase; http\_uri; metadata:service http; reference:bugtraq,4022; reference:nessus,10953; classtype:attempted-recon; sid:1575; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP shopping cart access"; flow:to\_server,established; content:"/quikstore.cfg"; nocase; http\_uri; metadata:service http; reference:bugtraq,1983; reference:bugtraq,2049; reference:cve,1999-0607; reference:cve,2000-1188; classtype:attempted-recon; sid:1164; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Subversion 1.0.2 dated-rev-report buffer overflow attempt"; flow:to\_server,established; content:"dated-rev-report"; nocase; content:"<D|3A|CREATIONDATE>"; nocase; isdataat:75,relative; pcre:"/^([^\x3C]{75}|[\s\x20-\x3B\x3D-\x7E]{0,74}[^\s\x20-\x7E])/R"; metadata:policy security-ips drop, service http; reference:bugtraq,10386; reference:cve,2004-0397; classtype:attempted-user; sid:15491; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Advanced Poll admin\_embed.php access"; flow:to\_server,established; content:"/admin\_embed.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,8890; reference:nessus,11487; classtype:web-application-activity; sid:2289; rev:14;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Wordpress timthumb.php theme remote file include attack attempt"; flow:to\_server,established; content:"timthumb.php|3F|"; nocase; http\_uri; content:"src=http"; distance:0; nocase; http\_uri; pcre:"/timthumb\x2ephp\x3f[^\r\n]\*src=http\x3a\x2f[^\x2e\x2f]+\x2e[^\x2e\x2f]+\x2e[^\x2e\x2f]+\x2e/Ui"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,47374; reference:url,code.google.com/p/timthumb/issues/detail?id=212; classtype:web-application-attack; sid:19653; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Modernbill remote file include in config.php DIR"; flow:to\_server,established; content:"config.php"; fast\_pattern:only; http\_uri; content:"DIR"; nocase; pcre:"/DIR=(https?|ftps?)/i"; metadata:service http; reference:bugtraq,19335; reference:cve,2006-4034; classtype:web-application-attack; sid:20651; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS 8000 (msg:"SERVER-WEBAPP Barracuda IMG.PL directory traversal attempt"; flow:to\_server,established; content:"/img.pl"; nocase; http\_uri; pcre:"/img\.pl\x3f[^\r\n]\*f=[^\x26\r\n\x2e]\*\x2e\x2e/Usmi"; metadata:service http; reference:bugtraq,14712; reference:cve,2005-2847; classtype:attempted-admin; sid:4988; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP encoded cross site scripting HTML Image tag attempt"; flow:to\_server,established; content:"ONERROR="; nocase; http\_uri; metadata:service http; reference:bugtraq,5847; reference:cve,2002-0840; classtype:web-application-attack; sid:10990; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP imageFolio.cgi access"; flow:to\_server,established; content:"/imageFolio.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,4579; reference:bugtraq,6265; reference:cve,2002-1334; reference:nessus,11748; classtype:web-application-activity; sid:2212; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP webspirs.cgi access"; flow:to\_server,established; content:"/webspirs.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,2362; reference:cve,2001-0211; reference:nessus,10616; classtype:attempted-recon; sid:901; rev:20;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP newsdesk.cgi access"; flow:to\_server,established; content:"/newsdesk.cgi"; fast\_pattern; nocase; http\_uri; content:"../"; distance:0; http\_uri; metadata:service http; reference:bugtraq,2172; reference:cve,2001-0232; reference:nessus,10586; classtype:attempted-recon; sid:1473; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP archie access"; flow:to\_server,established; content:"/archie"; nocase; http\_uri; metadata:service http; classtype:attempted-recon; sid:881; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS 80 (msg:"SERVER-WEBAPP sphpblog upload\_img\_cgi access attempt"; flow:to\_server,established; content:"sphpblog"; http\_uri; content:"upload\_img\_cgi.php"; fast\_pattern; nocase; http\_uri; metadata:service http; reference:bugtraq,14667; reference:cve,2005-2733; classtype:attempted-user; sid:11666; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP webplus directory traversal"; flow:to\_server,established; content:"/webplus?script"; fast\_pattern; nocase; http\_uri; content:"../"; metadata:service http; reference:bugtraq,1102; reference:cve,2000-0282; reference:nessus,10367; classtype:web-application-attack; sid:813; rev:20;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP IBM Net.Commerce orderdspc.d2w access"; flow:to\_server,established; content:"/ncommerce3/ExecMacro/orderdspc.d2w"; http\_uri; metadata:service http; reference:bugtraq,2350; reference:cve,2001-0319; reference:nessus,11020; classtype:web-application-activity; sid:1820; rev:14;)

#alert tcp $EXTERNAL\_NET $HTTP\_PORTS -> $HOME\_NET any (msg:"SERVER-WEBAPP Worldweaver DX Studio Player shell.execute command execution attempt"; flow:to\_client,established; file\_data; content:"0AC2706C-8623-46F8-9EDD-8F71A897FDAE"; fast\_pattern:only; flowbits:set,http.dxstudio.clsid; flowbits:noalert; metadata:service http; reference:bugtraq,35273; reference:cve,2009-2011; classtype:attempted-user; sid:20871; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP register.dll access"; flow:to\_server,established; content:"/register.dll"; nocase; http\_uri; metadata:service http; reference:bugtraq,3327; reference:cve,2001-0958; reference:nessus,11747; classtype:web-application-activity; sid:2231; rev:11;)

#alert tcp $EXTERNAL\_NET $FILE\_DATA\_PORTS -> $HOME\_NET any (msg:"SERVER-WEBAPP socket\_connect buffer overflow attempt"; flow:to\_client,established; file\_data; content:"str\_repeat(|22 5C|x90|22|, EVIL\_SPACE\_SIZE)"; content:"for ($i = 0, $j = EVIL\_SPACE\_SIZE - strlen($SHELLCODE) - 1"; distance:0; content:"socket\_create(AF\_UNIX, SOCK\_STREAM, 1)"; metadata:service http, service imap, service pop3; reference:bugtraq,49241; reference:cve,2011-1938; classtype:attempted-user; sid:24192; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP net attempt"; flow:to\_server,established; content:"net.exe"; nocase; metadata:service http; classtype:web-application-activity; sid:1067; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP awstats.pl command execution attempt"; flow:to\_server,established; content:"/awstats.pl?"; fast\_pattern; nocase; http\_uri; content:"update="; http\_uri; pcre:"/update=[^\r\n\x26]+/Ui"; content:"logfile="; nocase; http\_uri; pcre:"/awstats.pl?[^\r\n]\*logfile=\x7C/Ui"; metadata:service http; reference:bugtraq,12572; reference:nessus,16456; classtype:web-application-attack; sid:3464; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Nortel Contivity cgiproc DOS attempt"; flow:to\_server,established; content:"/cgiproc?Nocfile="; http\_uri; metadata:service http; reference:bugtraq,938; reference:cve,2000-0063; reference:cve,2000-0064; reference:nessus,10160; classtype:web-application-attack; sid:1763; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 80 (msg:"SERVER-WEBAPP chetcpasswd access"; flow:to\_server,established; content:"chetcpasswd.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,21102; reference:bugtraq,6472; reference:cve,2002-2220; reference:cve,2006-6679; classtype:web-application-activity; sid:10999; rev:12;)

#alert tcp $EXTERNAL\_NET $HTTP\_PORTS -> $HOME\_NET any (msg:"SERVER-WEBAPP cookiejacking attempt"; flow:to\_client,established; file\_data; content:"file|3A 5C 5C|127.0.0.1"; nocase; pcre:"/<\s\*[A-Z]+\s+[^>]\*file\x3A\x5C\x5C127\x2e0\x2e0\x2e1/smi"; metadata:service http; reference:url,www.soom.cz/index.php?name=articles/show&aid=550; classtype:attempted-recon; sid:19176; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP /\_admin access"; flow:to\_server,established; content:"/\_admin/"; nocase; http\_uri; metadata:service http; reference:bugtraq,9537; reference:nessus,12032; classtype:web-application-activity; sid:2393; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP enter\_bug.cgi access"; flow:to\_server,established; content:"/enter\_bug.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,3272; reference:cve,2002-0008; classtype:web-application-activity; sid:2055; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP gbook.cgi access"; flow:to\_server,established; content:"/gbook.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,1940; reference:cve,2000-1131; classtype:web-application-activity; sid:1716; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP \*%20.pl access"; flow:to\_server,established; content:" .pl"; nocase; http\_uri; pcre:"/\/[^\r\n]\*\x20.pl/Ui"; metadata:service http; reference:nessus,11007; reference:url,rtfm.vn.ua/inet/sec/cgi-bugs.htm; reference:url,www.securityfocus.com/archive/1/149482; classtype:web-application-attack; sid:1663; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP DNSTools authentication bypass attempt"; flow:to\_server,established; content:"/dnstools.php"; fast\_pattern; nocase; http\_uri; content:"user\_logged\_in=true"; metadata:service http; reference:bugtraq,4617; reference:cve,2002-0613; classtype:web-application-attack; sid:1740; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP htsearch arbitrary configuration file attempt"; flow:to\_server,established; content:"/htsearch?-c"; nocase; http\_uri; metadata:service http; reference:bugtraq,3410; reference:cve,2001-0834; classtype:web-application-attack; sid:1600; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP wais.pl access"; flow:to\_server,established; content:"/wais.pl"; nocase; http\_uri; metadata:service http; classtype:attempted-recon; sid:850; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 8028 (msg:"SERVER-WEBAPP novell edirectory imonitor overflow attempt"; flow:to\_server,established; content:"/nds"; nocase; http\_uri; isdataat:1000,relative; pcre:"/\x2fnds[^\r\n]{1000}/Usmi"; metadata:service http; reference:bugtraq,18026; reference:cve,2006-2496; classtype:attempted-admin; sid:6507; rev:8;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP Insight Diagnostics XSS attempt"; flow:to\_server,established; content:"/hpdiags/"; fast\_pattern:only; pcre:"/\x2fhpdiags\x2f(parameters|idstatusframe|survey|globals|custom)\.php\x3f.\*?(device|pid|cfg|category|tabpage|testmode)=[^\x26]\*?(script|onclick|onload|onmouseover|[\x22\x27\x3c\x3e\x28\x29])/i"; metadata:service http; reference:cve,2010-3003; classtype:web-application-attack; sid:21314; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP eshop.pl arbitrary command execution attempt"; flow:to\_server,established; content:"/eshop.pl?seite=|3B|"; nocase; http\_uri; metadata:service http; reference:bugtraq,3340; reference:cve,2001-1014; classtype:web-application-attack; sid:1565; rev:19;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP mailman cross site scripting attempt"; flow:to\_server,established; content:"/mailman/"; nocase; http\_uri; content:"?"; http\_uri; content:"info="; http\_uri; content:"<script"; nocase; http\_uri; metadata:service http; reference:bugtraq,5298; reference:cve,2002-0855; reference:nessus,14984; classtype:web-application-attack; sid:1839; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 8300 (msg:"SERVER-WEBAPP Novell Groupwise Messenger parameters invalid memory access attempt"; flow:to\_server,established; content:"tag=NM\_A\_PARM1"; fast\_pattern:only; content:"POST"; http\_method; content:"/login"; depth:6; nocase; http\_uri; content:"|0D 0A 0D 0A|"; content:"cmd=0"; distance:0; nocase; pcre:"/(^|[\x26\x3f])val\s\*?=\s\*?([\x26]|$)/mi"; metadata:policy security-ips drop, service http; reference:bugtraq,20316; reference:cve,2006-4511; classtype:attempted-admin; sid:16028; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP sojourn.cgi File attempt"; flow:to\_server,established; content:"/sojourn.cgi?cat="; fast\_pattern; nocase; http\_uri; content:"%00"; nocase; metadata:service http; reference:bugtraq,1052; reference:cve,2000-0180; reference:nessus,10349; classtype:web-application-attack; sid:1194; rev:19;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 383 (msg:"SERVER-WEBAPP HP Operations Agent stack buffer overflow attempt"; flow:to\_server,established; flowbits:isset,hp\_openview\_coda; content:"|00 00 00 82|"; depth:4; offset:18; byte\_jump:2,12,relative; byte\_jump:2,0,relative; byte\_test:2,>,1024,0,relative; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,54362; reference:cve,2012-2019; reference:url,h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03397769; classtype:attempted-admin; sid:24316; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Talentsoft Web+ exploit attempt"; flow:to\_server,established; content:"/webplus.cgi?Script=/webplus/webping/webping.wml"; nocase; http\_uri; metadata:service http; reference:bugtraq,1725; classtype:web-application-attack; sid:1097; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP webgais access"; flow:to\_server,established; content:"/webgais"; nocase; http\_uri; metadata:service http; reference:bugtraq,2058; reference:cve,1999-0176; reference:nessus,10300; classtype:attempted-recon; sid:838; rev:20;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP System variable directory traversal attempt - %COMMONPROGRAMFILES - x86%"; flow:to\_server,established; content:"%COMMONPROGRAMFILES|40|x86|41|%"; fast\_pattern:only; http\_uri; metadata:service http; classtype:attempted-recon; sid:21822; rev:3;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP OpenView CGI parameter buffer overflow attempt"; flow:to\_server,established; content:"POST"; nocase; http\_method; content:"/OvCgi/"; http\_uri; pcre:"/\/OvCgi\/(jovgraph|webappmon)\.exe/iU"; content:"-textfile+"; nocase; http\_client\_body; isdataat:201; content:!"+"; within:201; http\_client\_body; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:cve,2010-1551; reference:cve,2010-1552; reference:cve,2010-1553; reference:cve,2010-1554; reference:cve,2010-1555; reference:cve,2010-1960; reference:cve,2010-1961; reference:cve,2011-3167; classtype:attempted-user; sid:24693; rev:1;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cached\_feed.cgi moreover shopping cart directory traversal"; flow:to\_server,established; content:"/cached\_feed.cgi"; http\_uri; content:"../"; metadata:service http; reference:bugtraq,1762; reference:cve,2000-0906; classtype:web-application-attack; sid:1093; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP .htpasswd access"; flow:to\_server,established; content:".htpasswd"; nocase; metadata:service http; classtype:web-application-attack; sid:1071; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP logicworks.ini access"; flow:to\_server,established; content:"/logicworks.ini"; http\_uri; metadata:service http; reference:bugtraq,6996; reference:nessus,11639; classtype:web-application-activity; sid:2138; rev:8;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP VirusWall FtpSave access"; flow:to\_server,established; content:"/FtpSave.dll"; nocase; http\_uri; metadata:service http; reference:bugtraq,2808; reference:cve,2001-0432; reference:nessus,10733; classtype:attempted-recon; sid:1230; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 25 (msg:"SERVER-WEBAPP socket\_connect buffer overflow attempt"; flow:to\_server,established; file\_data; content:"str\_repeat(|22 5C|x90|22|, EVIL\_SPACE\_SIZE)"; content:"for ($i = 0, $j = EVIL\_SPACE\_SIZE - strlen($SHELLCODE) - 1"; distance:0; content:"socket\_create(AF\_UNIX, SOCK\_STREAM, 1)"; metadata:service smtp; reference:bugtraq,49241; reference:cve,2011-1938; classtype:attempted-user; sid:24193; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 8774 (msg:"SERVER-WEBAPP OpenStack Compute directory traversal attempt"; flow:to\_server,established; content:"<file"; content:"path="; within:25; content:"../"; within:5; metadata:policy security-ips drop, service http; reference:cve,2012-3360; reference:cve,2012-3361; classtype:attempted-admin; sid:24521; rev:1;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP OpenView Network Node Manager cookie buffer overflow attempt"; flow:to\_server,established; content:"/OVCgi/Main/Snmp.exe"; fast\_pattern:only; http\_uri; pcre:"/(OvJavaScript|OvTitleFrame|OvHelpWindow|OvMap|OvSession|OvJavaLocale|OvOSLocale|OvLogin|OvDebug|OvDeveloper|OvTreeControl|OvJavaScript|OvProduct|OvPort|OvLocale|OvWebSession)\s\*\x3D[^\x3B\x2C]{1024}/iC"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,42154; reference:cve,2010-2709; classtype:attempted-user; sid:18905; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP commerce.cgi access"; flow:to\_server,established; content:"/commerce.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,2361; reference:cve,2001-0210; reference:nessus,10612; classtype:attempted-recon; sid:898; rev:19;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP htgrep attempt"; flow:to\_server,established; content:"/htgrep"; http\_uri; content:"hdr=/"; metadata:service http; reference:cve,2000-0832; reference:nessus,10495; classtype:web-application-attack; sid:1615; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP globals.pl access"; flow:to\_server,established; content:"/globals.pl"; http\_uri; metadata:service http; reference:bugtraq,2671; reference:cve,2001-0330; classtype:web-application-activity; sid:2073; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP google proxystylesheet arbitrary command execution attempt"; flow:to\_server,established; content:"proxystylesheet"; http\_uri; content:"/search"; http\_uri; pcre:"/proxystylesheet=[-a-z0-9\_\.]\*[^-a-z0-9\_\.&\s]/sUmi"; metadata:service http; reference:bugtraq,15509; reference:cve,2005-3757; reference:url,metasploit.com/research/vulns/google\_proxystylesheet/; classtype:web-application-attack; sid:11223; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Advanced Poll admin\_help.php access"; flow:to\_server,established; content:"/admin\_help.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,8890; reference:nessus,11487; classtype:web-application-activity; sid:2290; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ?PageServices access"; flow:to\_server,established; content:"?PageServices"; nocase; http\_uri; metadata:service http; reference:bugtraq,1063; reference:bugtraq,7621; reference:cve,1999-0269; classtype:attempted-recon; sid:1123; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Fortinet FortiOS appliedTags field cross site scripting attempt"; flow:to\_server,established; content:"/firewall/policy"; fast\_pattern:only; http\_uri; content:"&tagList="; http\_client\_body; pcre:"/[?&]tagList=[^&]+?([\x3E\x3C\x28\x29]|%3E|%3C|%28|%29)([\x22\x27]|%22|%27)/Pi"; metadata:policy security-ips drop, service http; reference:bugtraq,51708; classtype:web-application-attack; sid:24289; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Domino log.nsf access"; flow:to\_server,established; content:"/log.nsf"; nocase; http\_uri; metadata:service http; reference:nessus,10629; classtype:attempted-recon; sid:1153; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ezboard.cgi access"; flow:to\_server,established; content:"/ezboard.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,4068; reference:bugtraq,4579; reference:cve,2002-0263; reference:nessus,11748; classtype:web-application-activity; sid:2205; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Symantec IM Manager LoggedInUsers.lgx definition file multiple SQL injections attempt"; flow:to\_server,established; content:"/IMManager/rdPage.aspx?"; fast\_pattern:only; http\_uri; pcre:"/\x2FIMManager\x2FrdPage\x2Easpx\x3F.\*?(loginTimeStamp|dbo|dateDiffParam|whereClause)\x3D[^\x26]\*?(\x3B|\x23|\x2D{2})/sU"; metadata:policy security-ips drop, service http; reference:bugtraq,44299; reference:cve,2010-0112; classtype:web-application-attack; sid:18956; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 8090 (msg:"SERVER-WEBAPP TrackerCam ComGetLogFile.php3 directory traversal attempt"; flow:to\_server,established; content:"/ComGetLogFile.php3"; nocase; pcre:"/fn=\x2e\x2e(\x2f|\x5c)/Rmsi"; reference:bugtraq,12592; reference:cve,2005-0481; reference:nessus,17160; classtype:web-application-attack; sid:3544; rev:8;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Web Shopper shopper.cgi access"; flow:to\_server,established; content:"/shopper.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,1776; reference:cve,2000-0922; classtype:attempted-recon; sid:1469; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Oracle Java Process Manager access"; flow:to\_server,established; content:"/oprocmgr-status"; http\_uri; metadata:service http; reference:nessus,10851; classtype:web-application-activity; sid:1874; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP inTouch SQL injection in index.php user attempt"; flow:to\_server,established; content:"index.php"; fast\_pattern:only; http\_uri; content:"user"; nocase; http\_header; pcre:"/user=[^\r\n\x26]\*?([\x22\x27]|%2[27])/Hi"; metadata:service http; reference:bugtraq,16110; reference:cve,2006-0088; classtype:web-application-attack; sid:24112; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP yabb directory traversal attempt"; flow:to\_server,established; content:"/YaBB"; fast\_pattern; nocase; http\_uri; content:"../"; metadata:service http; reference:bugtraq,1668; reference:cve,2000-0853; reference:nessus,10512; classtype:attempted-recon; sid:806; rev:22;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP SiteScope APISiteScopeImpl information disclosure attempt"; flow:to\_server,established; content:"POST"; http\_method; content:"/APISiteScopeImpl"; http\_uri; content:"impl:getFileInternal"; fast\_pattern:only; http\_client\_body; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,55269; reference:cve,2012-3259; reference:url,osvdb.org/85120; classtype:web-application-activity; sid:24292; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP wayboard attempt"; flow:to\_server,established; content:"/way-board/way-board.cgi"; http\_uri; content:"db="; content:"../.."; nocase; metadata:service http; reference:bugtraq,2370; reference:cve,2001-0214; reference:nessus,10610; classtype:web-application-attack; sid:1397; rev:14;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 4150 (msg:"SERVER-WEBAPP Oracle GoldenGate Veridata Server soap request overflow attempt"; flow:to\_server,established; content:"<soapenv:"; nocase; content:"<ns1:"; distance:0; nocase; isdataat:256,relative; content:!">"; within:256; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,45868; reference:cve,2010-4416; classtype:attempted-admin; sid:19168; rev:3;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP OpenView Network Node Manager ovwebsnmpsrv.exe OVwSelection buffer overflow attempt - POST"; flow:to\_server,established; content:"|2F|OvCgi|2F|jovgraph.exe"; nocase; http\_uri; content:"OVwSelection"; nocase; http\_client\_body; pcre:"/(arg=[^\x26]\*?OVwSelection[^\x26]\*?\x26.\*?sel=[^\s\x26]{1023}|sel=[^\x26]{1023,}\x26.\*?arg=[^\s\x26]\*?OVwSelection)/sP"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,37343; reference:cve,2009-4181; classtype:attempted-user; sid:16713; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Poll-it access"; flow:to\_server,established; content:"/pollit/Poll\_It\_SSI\_v2.0.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,1431; reference:cve,2000-0590; reference:nessus,10459; classtype:web-application-activity; sid:1106; rev:21;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP mod\_gzip\_status access"; flow:to\_server,established; content:"/mod\_gzip\_status"; http\_uri; metadata:service http; reference:nessus,11685; classtype:web-application-activity; sid:2156; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 3443 (msg:"SERVER-WEBAPP HP Openview NNM freeIPaddrs.ovpl port 3443 Unix command execution attempt"; flow:to\_server,established; content:"/freeIPaddrs.ovpl"; nocase; http\_uri; content:"netid="; nocase; http\_uri; pcre:"/freeIPaddrs\.ovpl[^\r\n]\*netid=[^\r\n]\*%[\x2c\x24\x7c\x3b\x22\x26\x3c\x3f]/Usmi"; metadata:service http; reference:bugtraq,14662; reference:cve,2005-2773; classtype:web-application-attack; sid:8087; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Devellion CubeCart multiple parameter XSS vulnerability"; flow:to\_server,established; content:"gateway/WorldPay/return.php?"; http\_uri; pcre:"/(amount|cartId|email|transId|transStatus)=[^&]\*[\x22\x27\x3c\x3e]/R"; metadata:service http; reference:url,www.acunetix.com/blog/web-security-zone/articles/sql-injection-xss-cubecart-4-3-3/; classtype:web-application-attack; sid:21270; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP csPassword.cgi access"; flow:to\_server,established; content:"/csPassword.cgi"; http\_uri; metadata:service http; reference:bugtraq,4885; reference:bugtraq,4886; reference:bugtraq,4887; reference:bugtraq,4889; reference:cve,2002-0917; reference:cve,2002-0918; classtype:web-application-activity; sid:1787; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP tst.bat access"; flow:to\_server,established; content:"/tst.bat"; http\_uri; metadata:service http; reference:bugtraq,770; reference:cve,1999-0885; reference:nessus,10014; classtype:web-application-activity; sid:1650; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP /\*.shtml access"; flow:to\_server,established; content:"/\*.shtml"; http\_uri; metadata:service http; reference:bugtraq,1517; reference:cve,2000-0683; reference:nessus,11604; classtype:web-application-activity; sid:2139; rev:11;)

#alert tcp $EXTERNAL\_NET $HTTP\_PORTS -> $HOME\_NET any (msg:"SERVER-WEBAPP Apple OSX software update command execution attempt"; flow:to\_client,established; file\_data; content:"installer-gui-script"; fast\_pattern:only; content:"allow-external-scripts"; nocase; pcre:"/^\s\*\x3d\s\*([\x22\x27])\s\*yes\s\*\1/Ri"; content:"system.run"; nocase; metadata:service http; reference:cve,2007-5863; reference:url,osvdb.org/40722; classtype:attempted-admin; sid:21051; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP VirusWall FtpSaveCSP access"; flow:to\_server,established; content:"/FtpSaveCSP.dll"; nocase; http\_uri; metadata:service http; reference:bugtraq,2808; reference:cve,2001-0432; reference:nessus,10733; classtype:attempted-recon; sid:1234; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP pagelog.cgi directory traversal attempt"; flow:to\_server,established; content:"/pagelog.cgi"; nocase; http\_uri; content:"name=../"; fast\_pattern:only; metadata:service http; reference:bugtraq,1864; reference:cve,2000-0940; reference:nessus,10591; classtype:web-application-activity; sid:1657; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP echo.bat arbitrary command execution attempt"; flow:to\_server,established; content:"/echo.bat"; http\_uri; content:"&"; metadata:service http; reference:bugtraq,1002; reference:cve,2000-0213; reference:nessus,10246; classtype:web-application-attack; sid:1705; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP DB4Web access"; flow:to\_server,established; content:"/DB4Web/"; http\_uri; metadata:service http; reference:nessus,11180; classtype:web-application-activity; sid:2060; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP wordpress cat parameter arbitrary file execution attempt"; flow:to\_server,established; content:"/wordpress/"; fast\_pattern; nocase; http\_uri; content:"cat="; nocase; content:"../"; distance:0; pcre:"/\x2Fwordpress\x2F\x3F[^\r\n]\*cat\s\*=\s\*[^\r\n\x26]\*\x2F\x2E\x2E/smi"; metadata:policy security-ips drop, service http; reference:bugtraq,28845; reference:cve,2008-4769; classtype:web-application-attack; sid:15432; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP environ.pl access"; flow:to\_server,established; content:"/environ.pl"; nocase; http\_uri; metadata:service http; classtype:web-application-activity; sid:1651; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cacti graph\_image SQL injection attempt"; flow:to\_server,established; content:"graph\_image.php"; nocase; http\_uri; pcre:"/rra\_id=(?!(\d+|all|)([\x26\s]|$))/smi"; metadata:service http; reference:bugtraq,14128; reference:bugtraq,14129; reference:cve,2005-2148; classtype:web-application-attack; sid:8713; rev:7;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 38292 (msg:"SERVER-WEBAPP Symantec Alert Management System pin number buffer overflow attempt"; flow:to\_server,established; content:"|FF FF FF FF|"; depth:4; content:"PAGE"; depth:4; offset:30; nocase; content:"PinNumber|00|"; distance:0; byte\_test:2,>,256,0,relative,little; metadata:policy balanced-ips drop, policy security-ips drop; reference:cve,2010-0110; reference:url,www.symantec.com/business/security\_response/securityupdates/detail.jsp?fid=security\_advisory&pvid=security\_advisory&year=2011&suid=20110126\_00; classtype:attempted-user; sid:18460; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP PHP-CGI command injection attempt"; flow:to\_server,established; content:"-s"; http\_uri; content:!"="; http\_raw\_uri; pcre:"/\x3F\s\*?-s/Ui"; metadata:service http; reference:cve,2012-1823; reference:cve,2012-2311; classtype:attempted-admin; sid:22097; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP SecureSite authentication bypass attempt"; flow:to\_server,established; content:"secure\_site, ok"; nocase; metadata:service http; reference:bugtraq,4621; classtype:web-application-attack; sid:1744; rev:8;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP day5datanotifier.cgi access"; flow:to\_server,established; content:"/day5datanotifier.cgi"; nocase; http\_uri; metadata:service http; reference:cve,1999-1232; classtype:attempted-recon; sid:864; rev:17;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 808 (msg:"SERVER-WEBAPP Youngzsoft CCProxy CONNECT Request buffer overflow attempt"; flow:to\_server,established; content:"CONNECT "; nocase; isdataat:1024,relative; pcre:"/^CONNECT\s[^\s]{1024}/i"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,31416; reference:cve,2008-6415; classtype:attempted-user; sid:15190; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP /~root access"; flow:to\_server,established; content:"/~root"; nocase; http\_uri; metadata:service http; classtype:attempted-recon; sid:1145; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP edit\_image.php access"; flow:to\_server,established; content:"/edit\_image.php"; http\_uri; metadata:service http; reference:bugtraq,3288; reference:cve,2001-1020; reference:nessus,11104; classtype:web-application-activity; sid:1999; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP MachineInfo access"; flow:to\_server,established; content:"/MachineInfo"; nocase; http\_uri; metadata:service http; reference:cve,1999-1067; classtype:web-application-activity; sid:1722; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cgiforum.pl access"; flow:to\_server,established; content:"/cgiforum.pl"; nocase; http\_uri; metadata:service http; reference:bugtraq,1963; reference:cve,2000-1171; reference:nessus,10552; classtype:web-application-activity; sid:1466; rev:18;)

#alert tcp $HOME\_NET $HTTP\_PORTS -> $EXTERNAL\_NET any (msg:"SERVER-WEBAPP Oracle GlassFish Server successful authentication bypass attempt"; flow:to\_client,established; flowbits:isset,glassfish\_unauth\_attempt; flowbits:unset,glassfish\_unauth\_attempt; content:"200"; http\_stat\_code; file\_data; content:"Deploy"; fast\_pattern:only; content:"Applications"; pcre:"/<title>Deploy\s\*(Enterprise)?\s\*Applications/si"; metadata:policy security-ips drop, service http; reference:bugtraq,47438; reference:cve,2011-0807; classtype:attempted-admin; sid:20160; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP HyperSeek hsx.cgi access"; flow:to\_server,established; content:"/hsx.cgi"; http\_uri; metadata:service http; reference:bugtraq,2314; reference:cve,2001-0253; reference:nessus,10602; classtype:web-application-activity; sid:1607; rev:13;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP PHP-CGI remote file include attempt"; flow:to\_server,established; content:"auto\_prepend\_file"; http\_uri; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:cve,2012-1823; reference:cve,2012-2311; classtype:attempted-admin; sid:22063; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP smssend.php access"; flow:to\_server,established; content:"/smssend.php"; http\_uri; metadata:service http; reference:bugtraq,3982; reference:cve,2002-0220; classtype:web-application-activity; sid:1407; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET [8093,8094] (msg:"SERVER-WEBAPP SyBase MBusiness xml closing tag overflow attempt"; flow:to\_server,established; content:"POST"; depth:4; nocase; content:"<SOAP-ENV"; nocase; content:"<|2F|password"; distance:0; nocase; isdataat:768,relative; content:!"|3E|"; within:768; metadata:policy security-ips drop; reference:bugtraq,47775; classtype:attempted-user; sid:20764; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP VsSetCookie.exe access"; flow:to\_server,established; content:"/VsSetCookie.exe"; nocase; http\_uri; metadata:service http; reference:bugtraq,3784; reference:cve,2002-0236; reference:nessus,11731; classtype:web-application-activity; sid:2244; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP bb-hostscv.sh access"; flow:to\_server,established; content:"/bb-hostsvc.sh"; nocase; http\_uri; metadata:service http; reference:bugtraq,1455; reference:cve,2000-0638; reference:nessus,10460; classtype:web-application-activity; sid:1533; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Muscat Empower cgi access"; flow:to\_server,established; content:"/empower?DB"; nocase; http\_uri; metadata:service http; reference:bugtraq,2374; reference:cve,2001-0224; reference:nessus,10609; classtype:web-application-activity; sid:1221; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP b2 arbitrary command execution attempt"; flow:to\_server,established; content:"/b2/b2-include/"; http\_uri; content:"b2inc"; content:"http|3A|//"; metadata:service http; reference:bugtraq,4673; reference:cve,2002-0734; reference:cve,2002-1466; reference:nessus,11667; classtype:web-application-attack; sid:1757; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Home Free search.cgi directory traversal attempt"; flow:to\_server,established; content:"/search.cgi"; http\_uri; content:"letter=../"; fast\_pattern:only; metadata:service http; reference:bugtraq,921; reference:cve,2000-0054; reference:nessus,10101; classtype:web-application-attack; sid:1598; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Phorum /support/common.php access"; flow:to\_server,established; content:"/support/common.php"; http\_uri; metadata:service http; reference:bugtraq,1997; reference:bugtraq,9361; classtype:web-application-attack; sid:1491; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP WebChat english.php file include"; flow:to\_server,established; content:"/defines.php"; nocase; http\_uri; content:"WEBCHATPATH="; nocase; content:"english.php"; fast\_pattern:only; metadata:service http; reference:bugtraq,7000; classtype:web-application-attack; sid:2357; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP apache ?M=D directory list attempt"; flow:to\_server,established; content:"/?M=D"; http\_uri; metadata:service http; reference:bugtraq,3009; reference:cve,2001-0731; reference:nessus,10704; classtype:web-application-activity; sid:1519; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cvsview2.cgi access"; flow:to\_server,established; content:"/cvsview2.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,4579; reference:bugtraq,5517; reference:cve,2003-0153; reference:nessus,11748; classtype:web-application-activity; sid:2197; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP directory.php arbitrary command attempt"; flow:to\_server,established; content:"/directory.php"; http\_uri; content:"dir="; content:"|3B|"; metadata:service http; reference:bugtraq,4278; reference:cve,2002-0434; reference:nessus,11017; classtype:misc-attack; sid:1815; rev:11;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP OpenView Network Node Manager cookie buffer overflow attempt"; flow:to\_server,established; content:"/OVCgi/getnnmdata.exe"; fast\_pattern:only; http\_uri; pcre:"/(OvJavaScript|OvTitleFrame|OvHelpWindow|OvMap|OvSession|OvJavaLocale|OvOSLocale|OvLogin|OvDebug|OvDeveloper|OvTreeControl|OvJavaScript|OvProduct|OvPort|OvLocale|OvWebSession)\s\*\x3D[^\x3B\x2C]{1024}/iC"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,42154; reference:cve,2010-2709; classtype:attempted-user; sid:18907; rev:3;)

#alert udp $HOME\_NET any -> $EXTERNAL\_NET 500 (msg:"SERVER-WEBAPP Openswan/Strongswan Pluto IKE daemon ISAKMP DPD malformed packet DOS attempt"; flow:to\_server; content:"|8D 29|"; depth:2; offset:38; isdataat:!41; reference:bugtraq,34296; reference:cve,2009-0790; classtype:attempted-dos; sid:21334; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP p-news.php access"; flow:to\_server,established; content:"/p-news.php"; http\_uri; metadata:service http; reference:nessus,11669; classtype:web-application-activity; sid:2140; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP EXIF header parsing integer overflow attempt big endian"; flow:to\_server,established; content:"Exif|00 00 4D 4D 00 2A 00 00 00 08|"; http\_client\_body; content:"|90 03 00 02|"; distance:0; http\_client\_body; byte\_test:4,>,2048,0,relative; metadata:policy security-ips drop, service http; reference:cve,2011-4566; reference:url,osvdb.org/77446; classtype:web-application-attack; sid:22950; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP store.cgi product directory traversal attempt"; flow:to\_server,established; content:"/store.cgi"; nocase; http\_uri; content:"product="; content:"../.."; fast\_pattern:only; metadata:service http; reference:bugtraq,2385; reference:cve,2001-0305; classtype:web-application-attack; sid:1306; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP lastlines.cgi access"; flow:to\_server,established; content:"/lastlines.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,3754; reference:bugtraq,3755; reference:cve,2001-1205; reference:cve,2001-1206; classtype:attempted-recon; sid:1392; rev:20;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP unify eWave ServletExec upload"; flow:to\_server,established; content:"/servlet/com.unify.servletexec.UploadServlet"; nocase; http\_uri; metadata:service http; reference:bugtraq,1868; reference:bugtraq,1876; reference:cve,2000-1024; reference:cve,2000-1025; reference:nessus,10570; classtype:web-application-attack; sid:1080; rev:21;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP news.php file include"; flow:to\_server,established; content:"/news.php"; fast\_pattern; nocase; http\_uri; content:"template="; nocase; metadata:service http; reference:bugtraq,6674; classtype:web-application-attack; sid:2361; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP 3Com 3CRADSL72 ADSL 11g Wireless Router app\_sta.stm access attempt"; flow:to\_server,established; content:"/app\_sta.stm"; nocase; http\_uri; metadata:service http; reference:bugtraq,11408; classtype:web-application-activity; sid:3086; rev:7;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP OpenView Network Node Manager ovwebsnmpsrv.exe displayWidth buffer overflow attempt - POST"; flow:to\_server,established; content:"|2F|OvCgi|2F|jovgraph.exe"; nocase; http\_uri; content:"displayWidth"; nocase; http\_client\_body; pcre:"/(displayWidth[\x2b\x20]\d[^\x2b\s\n]{128})/siP"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,45762; reference:cve,2011-0262; classtype:attempted-user; sid:18759; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP dfire.cgi access"; flow:to\_server,established; content:"/dfire.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,564; reference:cve,1999-0913; classtype:web-application-activity; sid:1219; rev:21;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP swsrv.cgi access"; flow:to\_server,established; content:"/swsrv.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,7510; reference:cve,2003-0217; reference:nessus,11608; classtype:web-application-activity; sid:2128; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP mod-plsql administration access"; flow:to\_server,established; content:"/admin\_/"; http\_uri; metadata:service http; reference:bugtraq,3726; reference:bugtraq,3727; reference:cve,2001-1216; reference:cve,2001-1217; reference:nessus,10849; classtype:web-application-activity; sid:1385; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP web-map.cgi access"; flow:to\_server,established; content:"/web-map.cgi"; http\_uri; metadata:service http; classtype:web-application-activity; sid:1211; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cgimail access"; flow:to\_server,established; content:"/cgimail"; nocase; http\_uri; metadata:service http; reference:bugtraq,1623; reference:cve,2000-0726; reference:nessus,11721; classtype:web-application-activity; sid:1542; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP faxsurvey access"; flow:to\_server,established; content:"/faxsurvey"; nocase; http\_uri; metadata:service http; reference:bugtraq,2056; reference:cve,1999-0262; reference:nessus,10067; classtype:web-application-activity; sid:857; rev:20;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP System variable in URI attempt - %PATHEXT%"; flow:to\_server,established; content:"%PATHEXT%"; fast\_pattern:only; http\_uri; metadata:service http; classtype:attempted-recon; sid:21842; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP wguest.exe access"; flow:to\_server,established; content:"/wguest.exe"; nocase; http\_uri; metadata:service http; reference:bugtraq,2024; reference:cve,1999-0287; reference:cve,1999-0467; classtype:attempted-recon; sid:852; rev:20;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET [8008,8028] (msg:"SERVER-WEBAPP Novell eDirectory management console Accept-Language buffer overflow attempt"; flow:to\_server,established; content:"/nds"; fast\_pattern; nocase; http\_uri; content:"Accept-Language"; distance:0; nocase; content:"|3A|"; distance:0; isdataat:19,relative; pcre:"/^\s\*Accept-Language\s\*\x3a\s\*([^\r\n]\*?\x2c){20}/mi"; metadata:policy security-ips drop; reference:bugtraq,31553; reference:cve,2008-5094; reference:url,download.novell.com/Download?buildid=Cf15mVyA3GI~; classtype:attempted-admin; sid:15446; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP gozila.cgi access"; flow:to\_server,established; content:"/gozila.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,6086; reference:cve,2002-1236; reference:nessus,11773; classtype:web-application-activity; sid:2225; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ttCMS header.php access"; flow:to\_server,established; content:"/admin/templates/header.php"; http\_uri; metadata:service http; reference:bugtraq,7542; reference:bugtraq,7543; reference:bugtraq,7625; reference:nessus,11636; classtype:web-application-activity; sid:2151; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP view-source directory traversal"; flow:to\_server,established; content:"/view-source"; fast\_pattern; nocase; http\_uri; content:"../"; nocase; metadata:service http; reference:bugtraq,2251; reference:bugtraq,8883; reference:cve,1999-0174; classtype:web-application-attack; sid:848; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP RBS ISP /newuser directory traversal attempt"; flow:to\_server,established; content:"/newuser?Image=../.."; http\_uri; metadata:service http; reference:bugtraq,1704; reference:cve,2000-1036; reference:nessus,10521; classtype:web-application-attack; sid:1492; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP L3retriever HTTP Probe"; flow:to\_server,established; content:"User-Agent|3A| Java1.2.1|0D 0A|"; http\_header; metadata:service http; classtype:web-application-activity; sid:1100; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP talkback.cgi directory traversal attempt"; flow:to\_server,established; content:"/talkbalk.cgi"; nocase; http\_uri; content:"article=../../"; fast\_pattern:only; metadata:service http; reference:bugtraq,2547; reference:cve,2001-0420; classtype:web-application-attack; sid:1719; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP upload.cgi access"; flow:to\_server,established; content:"/upload.cgi"; nocase; http\_uri; metadata:service http; reference:nessus,10290; classtype:attempted-recon; sid:1481; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ROXEN directory list attempt"; flow:to\_server,established; content:"/%00"; http\_uri; metadata:service http; reference:bugtraq,1510; reference:cve,2000-0671; reference:nessus,10479; classtype:attempted-recon; sid:1109; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Lotus Notes .exe script source download attempt"; flow:to\_server,established; content:".exe"; http\_uri; content:".exe"; content:"."; within:1; metadata:service http; reference:bugtraq,6841; classtype:web-application-attack; sid:2067; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP autohtml.php access"; flow:to\_server,established; content:"/autohtml.php"; http\_uri; metadata:service http; reference:nessus,11630; classtype:web-application-activity; sid:2154; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP IBM Lotus Domino webadmin.nsf directory traversal attempt"; flow:to\_server,established; content:"/webadmin.nsf"; fast\_pattern:only; http\_uri; pcre:"/|2E 2E|(%5C|%2F)|2E 2E|(%5C|%2F)|2E 2E|(%5C|%2F)/Pmi"; metadata:policy security-ips drop, service http; reference:bugtraq,9900; classtype:web-application-attack; sid:23480; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP NetObserve authentication bypass attempt"; flow:to\_server,established; content:"login=0"; nocase; content:"login=0"; nocase; http\_cookie; metadata:service http; reference:bugtraq,9319; classtype:web-application-attack; sid:2441; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP rolis guestbook access"; flow:to\_server,established; content:"/insert.inc.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,9057; classtype:web-application-activity; sid:2285; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP CSMailto.cgi access"; flow:to\_server,established; content:"/CSMailto.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,4579; reference:bugtraq,6265; reference:cve,2002-0749; reference:nessus,11748; classtype:web-application-activity; sid:2194; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP zml.cgi access"; flow:to\_server,established; content:"/zml.cgi"; http\_uri; metadata:service http; reference:bugtraq,3759; reference:cve,2001-1209; reference:nessus,10830; classtype:web-application-activity; sid:1396; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP Openview NNM freeIPaddrs.ovpl Unix command execution attempt"; flow:to\_server,established; content:"/freeIPaddrs.ovpl"; nocase; http\_uri; content:"netid="; nocase; http\_uri; pcre:"/freeIPaddrs\.ovpl[^\r\n]\*netid=[^\r\n]\*[\x2c\x24\x7c\x3b\x22\x26\x3c\x3f]/Usmi"; metadata:policy security-ips drop, service http; reference:bugtraq,14662; reference:cve,2005-2773; classtype:web-application-attack; sid:8090; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP user\_update\_passwd.pl access"; flow:to\_server,established; content:"/user\_update\_passwd.pl"; nocase; http\_uri; metadata:service http; reference:bugtraq,1486; reference:cve,2000-0627; classtype:attempted-recon; sid:1458; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Domino events4.nsf access"; flow:to\_server,established; content:"/events4.nsf"; nocase; http\_uri; metadata:service http; reference:nessus,10629; classtype:attempted-recon; sid:1580; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP TextPortal admin.php default password 12345 attempt"; flow:to\_server,established; content:"/admin.php"; http\_uri; content:"op=admin\_enter"; content:"password=12345"; fast\_pattern:only; metadata:service http; reference:bugtraq,7673; reference:nessus,11660; classtype:web-application-activity; sid:2146; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP System variable directory traversal attempt - %USERPROFILE%"; flow:to\_server,established; content:"%USERPROFILE%"; fast\_pattern:only; http\_uri; metadata:service http; classtype:attempted-recon; sid:21835; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP newsscript.pl admin attempt"; flow:to\_server,established; content:"/newsscript.pl"; nocase; http\_uri; content:"mode=admin"; nocase; metadata:service http; reference:bugtraq,12761; reference:cve,2005-0735; reference:nessus,17309; classtype:web-application-attack; sid:3676; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Blahz-DNS dostuff.php access"; flow:to\_server,established; content:"/dostuff.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,4618; reference:cve,2002-0599; classtype:web-application-activity; sid:1743; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP htsearch arbitrary file read attempt"; flow:to\_server,established; content:"/htsearch?exclude=`"; nocase; http\_uri; metadata:service http; reference:bugtraq,1026; reference:cve,2000-0208; reference:nessus,10105; classtype:web-application-attack; sid:1601; rev:19;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP VLC player web interface format string attack"; flow:to\_server,established; content:"Connection|3A|"; nocase; http\_header; content:"%"; distance:0; http\_header; pcre:"/^Connection\x3A[^\r\n]+%/smiH"; metadata:service http; reference:bugtraq,27015; reference:cve,2007-6681; classtype:attempted-admin; sid:18743; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP directorypro.cgi attempt"; flow:to\_server,established; content:"/directorypro.cgi"; http\_uri; content:"show="; content:"../.."; distance:1; nocase; metadata:service http; reference:bugtraq,2793; reference:cve,2001-0780; reference:nessus,10679; classtype:web-application-attack; sid:1574; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Domino webadmin.nsf access"; flow:to\_server,established; content:"/webadmin.nsf"; nocase; http\_uri; metadata:service http; reference:bugtraq,9900; reference:bugtraq,9901; reference:nessus,10629; classtype:attempted-recon; sid:1579; rev:13;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP OpenView NNM ovlogin.exe CGI Host parameter buffer overflow attempt"; flow:to\_server,established; content:"/OvCgi/snmpviewer|2E|exe"; fast\_pattern:only; http\_uri; content:"Host|3A|"; nocase; isdataat:121,relative; pcre:"/Host\x3A\s\*[^\x0D\x0A]{121}/iH"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:cve,2009-4180; reference:url,h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01950877; classtype:attempted-user; sid:20177; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP dnewsweb.cgi access"; flow:to\_server,established; content:"/dnewsweb.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,1172; reference:bugtraq,4579; reference:cve,2000-0423; reference:nessus,11748; classtype:web-application-activity; sid:2200; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET [1128,50013] (msg:"SERVER-WEBAPP SAP NetWeaver SOAP interface command injection attempt"; flow:to\_server,established; content:"<sapsess|3A|Session"; fast\_pattern; nocase; content:"<SOAP-ENV|3A|Body>"; distance:0; nocase; content:"<mKey>Database/Name</mKey>"; distance:0; nocase; content:"<mValue"; distance:0; nocase; pcre:"/^>[^<]+?[\r\n]+?\x21/R"; reference:url,securitytracker.com/id?1027406; classtype:attempted-admin; sid:24091; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP pgpmail.pl access"; flow:to\_server,established; content:"/pgpmail.pl"; http\_uri; metadata:service http; reference:bugtraq,3605; reference:cve,2001-0937; reference:nessus,11070; classtype:web-application-activity; sid:2670; rev:8;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Symantec IM Manager TOC\_simple cross site scripting attempt"; flow:to\_server,established; content:"/IMManager/Admin/IMAdminTOC\_simple.asp"; nocase; http\_uri; pcre:"/(menuitem=|nav=)[^\x26\s]\*[\x3e\x3d\x29\x3b]/Ui"; metadata:service http; reference:bugtraq,49739; reference:cve,2011-0552; reference:url,osvdb.org/75981; classtype:attempted-user; sid:21067; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP dcboard.cgi invalid user addition attempt"; flow:to\_server,established; content:"/dcboard.cgi"; http\_uri; content:"command=register"; content:"%7cadmin"; metadata:service http; reference:bugtraq,2728; reference:cve,2001-0527; reference:nessus,10583; classtype:web-application-attack; sid:817; rev:18;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Cisco Secure Access Control Server UCP Application CSuserCGI.exe buffer overflow attempt"; flow:to\_server,established; content:"/CSuserCGI.exe?Logout"; nocase; http\_uri; pcre:"/\x2FCSuserCGI\x2Eexe\x3FLogout.[^\s]{96}/Ui"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,28222; reference:cve,2008-0532; reference:url,www.cisco.com/warp/public/707/cisco-sa-20080312-ucp.shtml; classtype:attempted-admin; sid:13656; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 8888 (msg:"SERVER-WEBAPP answerbook2 arbitrary command execution attempt"; flow:to\_server,established; content:"/ab2/"; content:"|3B|"; distance:1; reference:bugtraq,1556; reference:cve,2000-0697; classtype:web-application-attack; sid:1947; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP PHPLIB remote command attempt"; flow:to\_server,established; content:"\_PHPLIB[libdir]"; fast\_pattern:only; metadata:service http; reference:bugtraq,3079; reference:cve,2001-1370; reference:nessus,14910; classtype:attempted-user; sid:1254; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP document.d2w access"; flow:to\_server,established; content:"/document.d2w"; http\_uri; metadata:service http; reference:bugtraq,2017; reference:cve,2000-1110; classtype:web-application-activity; sid:1642; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Domino catalog.nsf access"; flow:to\_server,established; content:"/catalog.nsf"; nocase; http\_uri; metadata:service http; reference:nessus,10629; classtype:attempted-recon; sid:1150; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Content-Length request offset smuggling attempt"; flow:to\_server,established,no\_stream; content:"Content-Length|3A|"; http\_raw\_header; byte\_jump:10,0,string,relative,post\_offset 4; pcre:"/^(GET|POST|TRACE|DESCRIBE|DELETE)/R"; metadata:service http; reference:bugtraq,14106; reference:cve,2005-2088; classtype:misc-attack; sid:16218; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP technote print.cgi directory traversal attempt"; flow:to\_server,established; content:"/technote/print.cgi"; fast\_pattern; nocase; http\_uri; content:"board="; nocase; content:"../../"; content:"%00"; metadata:service http; reference:bugtraq,2156; reference:cve,2001-0075; reference:nessus,10584; classtype:web-application-attack; sid:1052; rev:19;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 9090 (msg:"SERVER-WEBAPP Jive Software Openfire log.jsp XSS attempt"; flow:to\_server,established; content:"/log.jsp"; fast\_pattern:only; http\_uri; pcre:"/log\.jsp\?.\*?=([^\x26]\*[\x22\x27\x3C\x3E\x28\x29\x3B]|script|src|location|document)/U"; metadata:policy security-ips drop, service http; reference:bugtraq,32935; reference:cve,2009-0496; classtype:web-application-attack; sid:20863; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Symantec IM Manager IMAdminScheduleReport.asp SQL injection attempt"; flow:to\_server,established; content:"/IMManager/admin/IMAdminScheduleReport.asp"; fast\_pattern; nocase; http\_uri; content:"&email="; distance:0; nocase; pcre:"/&email=[^\x26]\*(%3b|\x3b)/i"; metadata:policy security-ips drop, service http; reference:bugtraq,44299; reference:cve,2010-0112; classtype:web-application-attack; sid:19142; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS 7779 (msg:"SERVER-WEBAPP Oracle iSQL Plus cross site scripting attempt"; flow:to\_server,established; content:"/isqlplus"; nocase; http\_uri; content:"username="; nocase; http\_uri; pcre:"/username[\x3d\x3f][^\n\x26]\*\x3c[^\n\x26]+\x3e/Ui"; metadata:service http; reference:bugtraq,9484; reference:cve,2004-2115; classtype:web-application-attack; sid:12059; rev:8;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP input2.bat arbitrary command execution attempt"; flow:to\_server,established; content:"/input2.bat|7C|"; http\_uri; metadata:service http; reference:bugtraq,762; reference:cve,1999-0947; reference:nessus,10016; classtype:web-application-attack; sid:1514; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP TOP10.dll access"; flow:to\_server,established; content:"/TOP10.dll"; nocase; http\_uri; metadata:service http; reference:bugtraq,3327; reference:cve,2001-0958; reference:nessus,11747; classtype:web-application-activity; sid:2234; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cs.exe access"; flow:to\_server,established; content:"/cgi-bin/cs.exe"; nocase; http\_uri; metadata:service http; reference:bugtraq,3375; reference:cve,2001-1252; classtype:attempted-recon; sid:1303; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP man.sh access"; flow:to\_server,established; content:"/man.sh"; nocase; http\_uri; metadata:service http; reference:bugtraq,2276; reference:cve,1999-1179; classtype:attempted-recon; sid:859; rev:19;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 9080 (msg:"SERVER-WEBAPP IBM Rational Quality Manager and Test Lab Manager policy bypass attempt"; flow:to\_server,established; content:"/manager"; nocase; http\_uri; content:"Authorization|3A 20|Basic|20|QURNSU46QURNSU4="; fast\_pattern:only; http\_header; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,44172; reference:cve,2010-4094; classtype:default-login-attempt; sid:19110; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP BBoard access"; flow:to\_server,established; content:"/servlet/sunexamples.BBoardServlet"; http\_uri; metadata:service http; reference:bugtraq,1459; reference:cve,2000-0629; reference:nessus,10507; classtype:web-application-activity; sid:1528; rev:14;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP OpenView Network Node Manager nnmRptConfig.exe multiple parameters buffer overflow attempt"; flow:to\_server,established; content:"nnmRptConfig.exe"; fast\_pattern:only; http\_uri; pcre:"/(data\_select1|nameParams|schdParams|text1|schd\_select1)=[^\x26]{512}/iP"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,45762; reference:cve,2011-0265; reference:cve,2011-0266; reference:cve,2011-0267; reference:cve,2011-0268; reference:cve,2011-0269; reference:url,osvdb.org/show/osvdb/70473; classtype:attempted-user; sid:18764; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 389 (msg:"SERVER-WEBAPP CommuniGate Systems CommuniGate Pro LDAP Server buffer overflow attempt"; flow:to\_server,established; content:"|80|"; content:"|FF FF FF FF|"; within:8; distance:1; pcre:"/\x80(\x84|\x85\x00|\x86\x00\x00|\x87\x00\x00\x00)\xFF\xFF\xFF\xFF/smi"; metadata:policy security-ips drop, service ldap; reference:bugtraq,16407; reference:cve,2006-0468; reference:url,www.gleg.net/cg\_advisory.txt; classtype:attempted-user; sid:17450; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP php.cgi access"; flow:to\_server,established; content:"/php.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,2250; reference:bugtraq,712; reference:cve,1999-0058; reference:cve,1999-0238; reference:nessus,10178; classtype:attempted-recon; sid:824; rev:25;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Ecommerce import.txt access"; flow:to\_server,established; content:"/orders/import.txt"; nocase; http\_uri; metadata:service http; classtype:attempted-recon; sid:1148; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Netscape PublishingXpert access"; flow:to\_server,established; content:"/PSUser/PSCOErrPage.htm"; nocase; http\_uri; metadata:service http; reference:cve,2000-1196; reference:nessus,10364; classtype:web-application-activity; sid:1157; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP listrec.pl access"; flow:to\_server,established; content:"/listrec.pl"; nocase; http\_uri; metadata:service http; reference:bugtraq,3328; reference:cve,2001-0997; reference:nessus,10769; classtype:attempted-recon; sid:1470; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP chip.ini access"; flow:to\_server,established; content:"/chip.ini"; http\_uri; metadata:service http; reference:bugtraq,2755; reference:bugtraq,2775; reference:cve,2001-0749; reference:cve,2001-0771; classtype:web-application-activity; sid:2069; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Netscape dir index wp"; flow:to\_server,established; content:"?wp-"; nocase; http\_uri; metadata:service http; reference:bugtraq,1063; reference:cve,2000-0236; reference:nessus,10352; classtype:attempted-recon; sid:1160; rev:19;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP dumpenv.pl access"; flow:to\_server,established; content:"/dumpenv.pl"; nocase; http\_uri; metadata:service http; reference:cve,1999-1178; reference:nessus,10060; classtype:attempted-recon; sid:869; rev:18;)

#alert tcp $EXTERNAL\_NET $HTTP\_PORTS -> $HOME\_NET any (msg:"SERVER-WEBAPP Citrix Program Neighborhood Agent Buffer Overflow attempt"; flow:to\_client,established; file\_data; content:"|3C|AppData|3E|"; nocase; content:"|3C|InName|3E|"; pcre:"/InName\x3E[^\x3C]{100}/i"; metadata:policy security-ips drop, service http; reference:bugtraq,13373; reference:cve,2004-1078; classtype:attempted-user; sid:17423; rev:8;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 8022 (msg:"SERVER-WEBAPP Ipswitch WhatsUp Small Business directory traversal attempt"; flow:to\_server,established; content:"|2E 2E 2F 2E 2E 2F 2E 2E 2F|"; depth:100; pcre:"/^(GET|POST)\h+[^\n]\*?\x2E\x2E\x2F\x2E\x2E\x2F\x2E\x2E\x2F[^\n]\*?HTTP/i"; metadata:policy security-ips drop, service http; reference:bugtraq,15291; reference:cve,2005-1939; classtype:attempted-user; sid:17279; rev:7;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 383 (msg:"SERVER-WEBAPP HP Operations Agent stack buffer overflow attempt"; flow:to\_server,established; flowbits:isset,hp\_openview\_coda; content:"|00 00 00 8C|"; depth:4; offset:18; byte\_jump:2,8,relative; byte\_jump:2,12,relative; byte\_test:2,>,1024,0,relative; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,54362; reference:cve,2012-2019; reference:url,h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03397769; classtype:attempted-admin; sid:24317; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Netscape Enterprise Server directory view"; flow:to\_server,established; content:"?wp-usr-prop"; nocase; http\_uri; metadata:service http; reference:bugtraq,1063; reference:cve,2000-0236; classtype:web-application-attack; sid:1198; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP shoutbox.php directory traversal attempt"; flow:to\_server,established; content:"/shoutbox.php"; http\_uri; content:"conf="; content:"../"; distance:0; metadata:service http; reference:nessus,11668; classtype:web-application-attack; sid:2141; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Macromedia SiteSpring cross site scripting attempt"; flow:to\_server,established; content:"/error/500error.jsp"; nocase; http\_uri; content:"et="; http\_uri; content:"<script"; nocase; http\_uri; metadata:service http; reference:bugtraq,5249; reference:cve,2002-1027; classtype:web-application-attack; sid:1835; rev:12;)

alert tcp $EXTERNAL\_NET $HTTP\_PORTS -> $HOME\_NET any (msg:"SERVER-WEBAPP IBM Lotus Expeditor cai URI handler command execution attempt"; flow:to\_client,established; file\_data; content:"cai|3A|"; nocase; content:"-launcher"; distance:0; nocase; pcre:"/cai\x3a[^\x3e]\*?(\x22|\x2522)[^\x3e\x22]\*?-launcher/smi"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:cve,2008-1965; reference:url,www-01.ibm.com/support/docview.wss?uid=swg21303813; classtype:attempted-user; sid:17376; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP way-board.cgi access"; flow:to\_server,established; content:"/way-board.cgi"; nocase; http\_uri; metadata:service http; reference:nessus,10610; classtype:web-application-activity; sid:1850; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP mailman directory traversal attempt"; flow:to\_server,established; content:"/mailman/"; http\_uri; content:".../"; http\_uri; metadata:service http; reference:cve,2005-0202; classtype:web-application-attack; sid:3131; rev:8;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP MsmMask.exe attempt"; flow:to\_server,established; content:"/MsmMask.exe"; http\_uri; content:"mask="; metadata:service http; reference:nessus,11163; classtype:web-application-attack; sid:2058; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET [8004,8005] (msg:"SERVER-WEBAPP Symantec Scan Engine authentication bypass attempt"; flow:to\_server,established; content:"<key mod=|22|784607708866"; content:"pub=|22|75429754206"; metadata:policy security-ips drop; reference:bugtraq,17637; reference:cve,2006-0230; classtype:attempted-recon; sid:16056; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cachemgr.cgi access"; flow:to\_server,established; content:"/cachemgr.cgi"; http\_uri; metadata:service http; reference:bugtraq,2059; reference:cve,1999-0710; reference:nessus,10034; classtype:web-application-activity; sid:1206; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP pals-cgi arbitrary file access attempt"; flow:to\_server,established; content:"/pals-cgi"; fast\_pattern; nocase; http\_uri; content:"documentName="; metadata:service http; reference:bugtraq,2372; reference:cve,2001-0217; reference:nessus,10611; classtype:web-application-attack; sid:1222; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Youngzsoft CMailServer CMailCOM Buffer Overflow attempt"; flow:established,to\_server; content:"POST"; http\_method; content:"/mail/mvmail.asp"; nocase; http\_uri; content:"indexOfMail="; nocase; isdataat:4104,relative; metadata:policy security-ips drop, service http; reference:bugtraq,30098; reference:cve,2008-6922; classtype:attempted-user; sid:21762; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP NPH-maillist access"; flow:to\_server,established; content:"/nph-maillist.pl"; nocase; http\_uri; metadata:service http; reference:bugtraq,2563; reference:cve,2001-0400; reference:nessus,10164; classtype:attempted-recon; sid:1451; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP FormHandler.cgi external site redirection attempt"; flow:to\_server,established; content:"/FormHandler.cgi"; fast\_pattern; nocase; http\_uri; content:"redirect=http"; metadata:service http; reference:bugtraq,798; reference:bugtraq,799; reference:cve,1999-1050; reference:nessus,10075; classtype:web-application-attack; sid:1593; rev:19;)

#alert tcp $EXTERNAL\_NET $FILE\_DATA\_PORTS -> $HOME\_NET any (msg:"SERVER-WEBAPP PHP 5.3.3 mt\_rand integer overflow attempt"; flow:to\_client,established; file\_data; content:"mt\_getrandmax("; fast\_pattern:only; content:"<?"; pcre:"/(define\(\s\*(?P<q1>[\x22\x27])\s\*(?P<m1>\w+)(?P=q1)\s\*,\s\*mt\_getrandmax\(\)\s\*\+\d+\s\*\)\x3b.\*?mt\_rand\(\s\*0\s\*,\s\*(?P=m1)\s\*\)|(?P<m2>\$\w+)\s\*=\s\*mt\_getrandmax\(\)\s\*\+\s\*\d+\s\*\x3b.\*?mt\_rand\(\s\*0\s\*,\s\*(?P=m2)\s\*\)|mt\_rand\(\s\*0\s\*,\s\*mt\_getrandmax\(\)\s\*\+\s\*\d+\s\*\)\x3b)/smi"; metadata:service http, service imap, service pop3; reference:cve,2011-0755; classtype:misc-activity; sid:24060; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP System variable directory traversal attempt - %LOCALAPPDATA%"; flow:to\_server,established; content:"%LOCALAPPDATA%"; fast\_pattern:only; http\_uri; metadata:service http; classtype:attempted-recon; sid:21826; rev:3;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 17000 (msg:"SERVER-WEBAPP Oracle TimesTen In-Memory Database evtdump CGI module format string exploit attempt"; flow:to\_server,established; content:"GET "; depth:4; nocase; content:"evtdump?"; distance:0; nocase; pcre:"/evtdump\x3f.\*?\x2525[^\x20]\*?\x20HTTP/i"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,33177; reference:cve,2008-5440; classtype:attempted-admin; sid:15264; rev:2;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP SiteScope DownloadFilesHandler directory traversal attempt"; flow:to\_server,established; content:"REMOTE\_HANDLER\_KEY=DownloadFilesHandler"; fast\_pattern:only; http\_uri; content:"DownloadFilesHandler.file.name="; http\_uri; content:".."; within:3; http\_uri; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,55273; reference:cve,2012-3264; classtype:web-application-activity; sid:24447; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP CSGuestbook setup attempt"; flow:to\_server,established; content:"csGuestbook.cgi"; http\_uri; content:"command=savesetup&setup="; http\_uri; metadata:service http; reference:bugtraq,4448; reference:cve,2002-1750; classtype:web-application-activity; sid:12255; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 2301 (msg:"SERVER-WEBAPP Compaq Insight directory traversal"; flow:to\_server,established; content:"../"; reference:bugtraq,282; reference:cve,1999-0771; classtype:web-application-attack; sid:1199; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP math\_sum.mscgi access"; flow:to\_server,established; content:"/math\_sum.mscgi"; http\_uri; metadata:service http; reference:bugtraq,10831; reference:nessus,14182; classtype:web-application-activity; sid:3468; rev:7;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP Power Manager formExportDataLogs directory traversal attempt"; flow:to\_server, established; content:"|2F|goform|2F|formExportDataLogs"; nocase; http\_uri; pcre:"/fileName\x3d[^\x26]\*(\x2e\x2e\x5c|\x2e\x2e\x2f)/Ri"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,37866; reference:cve,2009-4000; classtype:web-application-attack; sid:18802; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP view\_source access"; flow:to\_server,established; content:"/view\_source"; nocase; http\_uri; metadata:service http; reference:bugtraq,2251; reference:cve,1999-0174; reference:nessus,10294; classtype:attempted-recon; sid:1482; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP bash access"; flow:to\_server,established; content:"/bash"; nocase; http\_uri; metadata:service http; reference:cve,1999-0509; reference:url,www.cert.org/advisories/CA-1996-11.html; classtype:web-application-activity; sid:885; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP server-status access"; flow:to\_server,established; content:"/server-status"; http\_uri; metadata:service http; reference:url,httpd.apache.org/docs/mod/mod\_info.html; classtype:web-application-activity; sid:1521; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP telnet attempt"; flow:to\_server,established; content:"telnet.exe"; nocase; metadata:service http; classtype:web-application-activity; sid:1066; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP bb-hostscv.sh attempt"; flow:to\_server,established; content:"/bb-hostsvc.sh?HOSTSVC?../.."; nocase; http\_uri; metadata:service http; reference:bugtraq,1455; reference:cve,2000-0638; reference:nessus,10460; classtype:web-application-attack; sid:1532; rev:17;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Novell ZENworks Asset Management default admin credentials function call attempt"; flow:to\_server,established; content:"/rtrlet/rtr"; fast\_pattern:only; http\_uri; content:"username=ivanhoe"; nocase; http\_uri; content:"password=scott"; nocase; http\_uri; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:cve,2012-4933; reference:url,www.kb.cert.org/vuls/id/332412; classtype:attempted-admin; sid:24436; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP readmail.cgi access"; flow:to\_server,established; content:"/readmail.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,3427; reference:bugtraq,4579; reference:cve,2001-1283; reference:nessus,11748; classtype:web-application-activity; sid:2216; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Trend Micro OfficeScan attempt"; flow:to\_server,established; content:"/officescan/cgi/jdkRqNotify.exe?"; nocase; http\_uri; content:"domain="; nocase; http\_uri; content:"event="; nocase; http\_uri; metadata:service http; reference:bugtraq,1057; classtype:attempted-recon; sid:1381; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP openview network node manager ovlogin.exe buffer overflow - userid parameter"; flow:to\_server,established; content:"/ovlogin.exe"; nocase; http\_uri; content:"userid="; nocase; http\_client\_body; pcre:"/userid=[^\x26\r\n]{128}/Psmi"; metadata:policy security-ips drop, service http; reference:bugtraq,37330; reference:cve,2009-4176; reference:url,h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01950877; classtype:attempted-admin; sid:18480; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP .wwwacl access"; flow:to\_server,established; content:".wwwacl"; nocase; http\_uri; metadata:service http; classtype:attempted-recon; sid:1130; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Vmist Downstat remote file include in admin.php art"; flow:to\_server,established; content:"downstat"; nocase; http\_uri; content:"admin.php"; nocase; http\_uri; content:"art="; nocase; http\_uri; pcre:"/\x2Fadmin\.php\x3F[^\r\n]\*?art\x3Dhttp\x3A\x2F/Ui"; metadata:service http; reference:bugtraq,20007; reference:cve,2006-4827; classtype:web-application-activity; sid:20816; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP CISCO VoIP DOS ATTEMPT"; flow:to\_server,established; content:"/StreamingStatistics"; http\_uri; metadata:service http; reference:bugtraq,4794; reference:cve,2002-0882; reference:nessus,11013; classtype:misc-attack; sid:1814; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Novell Teaming ajaxUploadImageFile remote code execution attempt"; flow:to\_server,established; content:"|2F|ssf|2F|a|2F|do"; nocase; http\_uri; content:"operation=upload\_image\_file"; nocase; http\_uri; content:"action=\_\_ajax\_request"; nocase; http\_uri; content:"Content-Disposition"; nocase; http\_client\_body; content:"filename"; http\_client\_body; pcre:"/Content-Disposition[^\r\n]+?filename\s\*\x3D[^\r\n]\*?\x2F(\x2E{2}\x5C|\x5C\x2E{2})/iP"; metadata:policy security-ips drop, service http; reference:bugtraq,41795; reference:cve,2010-2773; classtype:attempted-admin; sid:18902; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Comet WebFileManager remote file include in CheckUpload.php Language"; flow:to\_server,established; content:"CheckUpload.php"; fast\_pattern:only; http\_uri; pcre:"/Language=(https?|ftps?)/i"; metadata:service http; reference:bugtraq,19433; reference:cve,2006-4077; classtype:web-application-attack; sid:20663; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP alya.cgi access"; flow:to\_server,established; content:"/alya.cgi"; http\_uri; metadata:service http; reference:nessus,11118; classtype:web-application-activity; sid:1995; rev:8;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP OpenView Network Node Manager OpenView5 CGI buffer overflow attempt"; flow:to\_server,established; content:"/OvCgi/OpenView5.exe"; fast\_pattern:only; http\_uri; pcre:"/(Context|Action)\x3D[^\x26\x3b]{1024}/i"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,33147; reference:cve,2008-0067; classtype:attempted-user; sid:18579; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP calendar-admin.pl access"; flow:to\_server,established; content:"/calendar-admin.pl"; nocase; http\_uri; metadata:service http; reference:bugtraq,1215; reference:cve,2000-0432; reference:nessus,10506; classtype:web-application-activity; sid:1701; rev:16;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Cisco Common Services Help servlet XSS attempt"; flow:to\_server,established; content:"com.cisco.nm.help.ServerHelpEngine"; fast\_pattern:only; http\_uri; pcre:"/com\.cisco\.nm\.help\.ServerHelpEngine\?[^$\n]\*tag=[^$\n]\*([\x3C\x3E\x22\x27]|script|src|location|document)/OUi"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:cve,2011-0961; classtype:web-application-attack; sid:21385; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP /cgi-bin/jj access"; flow:to\_server,established; content:"/cgi-bin/jj"; nocase; http\_uri; metadata:service http; reference:bugtraq,2002; reference:cve,1999-0260; reference:nessus,10131; classtype:web-application-activity; sid:1174; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP rksh access"; flow:to\_server,established; content:"/rksh"; nocase; http\_uri; metadata:service http; reference:cve,1999-0509; reference:url,www.cert.org/advisories/CA-1996-11.html; classtype:attempted-recon; sid:877; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP alibaba.pl access"; flow:to\_server,established; content:"/alibaba.pl"; http\_uri; metadata:service http; reference:bugtraq,770; reference:cve,1999-0885; reference:nessus,10013; classtype:web-application-activity; sid:1508; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP alienform.cgi access"; flow:to\_server,established; content:"/alienform.cgi"; http\_uri; metadata:service http; reference:bugtraq,4983; reference:cve,2002-0934; reference:nessus,11027; classtype:web-application-activity; sid:1824; rev:13;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP OpenView Network Node Manager cookie buffer overflow attempt"; flow:to\_server,established; content:"/OVCgi/ovalarm.exe"; fast\_pattern:only; http\_uri; pcre:"/(OvJavaScript|OvTitleFrame|OvHelpWindow|OvMap|OvSession|OvJavaLocale|OvOSLocale|OvLogin|OvDebug|OvDeveloper|OvTreeControl|OvJavaScript|OvProduct|OvPort|OvLocale|OvWebSession)\s\*\x3D[^\x3B\x2C]{1024}/iC"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,42154; reference:cve,2010-2709; classtype:attempted-user; sid:18914; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 1000 (msg:"SERVER-WEBAPP ALT-N WebAdmin user param overflow attempt"; flow:to\_server,established; content:"POST"; content:"/WebAdmin.dll?"; nocase; content:"View=Logon"; distance:0; nocase; pcre:"/WebAdmin\x2Edll\x3F[^\r\n]\*?View=Logon.\*?\r\n\r\n[^\r\n\x26]\*User=[^\r\n\x26]{100}/smi"; reference:bugtraq,8024; classtype:attempted-admin; sid:6511; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Venom Board SQL injection attempt "; flow:to\_server,established; content:"venomboard|2F|forum"; fast\_pattern; nocase; http\_uri; content:"post.php3"; nocase; http\_uri; content:"topic\_id="; nocase; http\_uri; pcre:"/\x2Fpost\.php3?[^\r\n]\*?topic\_id=[^\r\n\x26]\*?union[^\r\n\x26]\*select/Ui"; metadata:service http; reference:bugtraq,16176; reference:cve,2006-0160; classtype:web-application-activity; sid:20623; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP /home/ftp access"; flow:to\_server,established; content:"/home/ftp"; nocase; http\_uri; metadata:service http; reference:nessus,11032; classtype:web-application-activity; sid:1670; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP calendar\_admin.pl access"; flow:to\_server,established; content:"/calendar\_admin.pl"; http\_uri; metadata:service http; reference:bugtraq,1215; reference:cve,2000-0432; reference:nessus,10506; classtype:web-application-activity; sid:1537; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP bb-hist.sh access"; flow:to\_server,established; content:"/bb-hist.sh"; nocase; http\_uri; metadata:service http; reference:bugtraq,142; reference:cve,1999-1462; reference:nessus,10025; classtype:attempted-recon; sid:894; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP geoBlog SQL injection in viewcat.php cat parameter attempt"; flow:to\_server,established; content:"viewcat.php"; fast\_pattern:only; http\_uri; pcre:"/cat=[^\r\n\x26]\*([\x22\x27]|%2[27])/i"; metadata:service http; reference:bugtraq,16249; reference:cve,2006-0249; classtype:web-application-activity; sid:20629; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 8090 (msg:"SERVER-WEBAPP TrackerCam overly long php parameter overflow attempt"; flow:to\_server,established; content:"php"; nocase; isdataat:255,relative; pcre:"/php.\*\x3f[^\n]{256}/smi"; reference:bugtraq,12592; reference:cve,2005-0481; classtype:web-application-attack; sid:3547; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP getdoc.cgi access"; flow:to\_server,established; content:"/getdoc.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,4579; reference:cve,2000-0288; reference:nessus,11748; classtype:web-application-activity; sid:2209; rev:17;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP OpenView NNM nnmRptConfig.exe CGI Host parameter buffer overflow attempt"; flow:to\_server,established; content:"/OvCgi/nnmRptConfig|2E|exe"; fast\_pattern:only; nocase; http\_uri; content:"Action|3D|Create"; nocase; http\_client\_body; content:"Template|3D|"; isdataat:1000,relative; pcre:"/Template\x3D[^\x0D\x0A]{1000}/Pi"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:cve,2009-3848; reference:url,h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01950877; classtype:attempted-user; sid:20240; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 81 (msg:"SERVER-WEBAPP McAfee ePO file upload attempt"; flow:to\_server,established; content:"/spipe/repl\_file"; nocase; content:"Command=BEGIN"; nocase; reference:bugtraq,10200; reference:cve,2004-0038; classtype:attempted-admin; sid:2562; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP raSMP User-Agent XSS injection attempt"; flow:established, to\_server; content:"onload"; fast\_pattern:only; http\_header; content:"index.php"; nocase; http\_uri; content:"User-Agent|3A|"; nocase; http\_header; pcre:"/^User-Agent\x3A[^\r\n]\*?onload=/imH"; metadata:service http; reference:bugtraq,16138; reference:cve,2006-0084; classtype:attempted-admin; sid:18467; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Free File Hosting remote file include in forgot\_pass.php ad\_body\_temp"; flow:to\_server,established; content:"forgot\_pass.php"; fast\_pattern:only; http\_uri; content:"ad\_body\_temp"; nocase; pcre:"/ad\_body\_temp=(https?|ftps?)/i"; metadata:service http; reference:bugtraq,20781; reference:cve,2006-5762; classtype:web-application-attack; sid:20657; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP webdist.cgi arbitrary command attempt"; flow:to\_server,established; content:"/webdist.cgi"; nocase; http\_uri; content:"distloc=|3B|"; fast\_pattern:only; metadata:service http; reference:bugtraq,374; reference:cve,1999-0039; reference:nessus,10299; classtype:web-application-attack; sid:1865; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET [7100,7101] (msg:"SERVER-WEBAPP Novell GroupWise agents HTTP request remote code execution attempt"; flow:to\_server,established; content:"Host|3A|"; nocase; isdataat:500,relative; content:!"|0A|"; within:500; reference:bugtraq,44732; reference:cve,2010-4714; classtype:attempted-admin; sid:18960; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP content-disposition memchr overflow"; flow:to\_server,established; content:"Content-Disposition|3A|"; nocase; http\_header; content:"name=|22 CC CC CC CC CC|"; fast\_pattern:only; metadata:service http; reference:bugtraq,4183; reference:cve,2002-0081; reference:nessus,10867; classtype:web-application-attack; sid:1423; rev:23;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET any (msg:"SERVER-WEBAPP Trend Micro OfficeScan CGI password decryption buffer overflow attempt"; flow:to\_server,established; content:"/cgiablogon.exe"; fast\_pattern:only; content:"CRYPT"; nocase; isdataat:512,relative; pcre:"/pwd=(\!|\%21)CRYPT(\!|\%21)[A-Z0-9]{512}/i"; metadata:policy balanced-ips drop, policy security-ips drop; reference:bugtraq,28020; reference:cve,2008-1365; reference:url,secunia.com/advisories/29124; classtype:web-application-attack; sid:13591; rev:5;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 8081 (msg:"SERVER-WEBAPP Trend Micro OfficeScan CGI password decryption buffer overflow attempt"; flow:to\_server,established; content:"/cgiablogon.exe"; fast\_pattern:only; content:"CRYPT"; nocase; isdataat:512,relative; pcre:"/pwd=(\!|\%21)CRYPT(\!|\%21)[^\r\n&]{513}/i"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,28020; reference:cve,2008-1365; reference:url,secunia.com/advisories/29124; classtype:web-application-attack; sid:17605; rev:4;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Trend Micro OfficeScan Console authentication buffer overflow attempt"; flow:to\_server,established; content:"/officescan/console"; fast\_pattern; http\_uri; content:"session="; http\_cookie; pcre:"/session=[^\s\x3b&]{520}/iC"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,24641; reference:bugtraq,24935; reference:cve,2007-3454; reference:cve,2007-3455; classtype:attempted-admin; sid:17295; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP squirrel mail spell-check arbitrary command attempt"; flow:to\_server,established; content:"/squirrelspell/modules/check\_me.mod.php"; fast\_pattern; nocase; http\_uri; content:"SQSPELL\_APP["; nocase; metadata:service http; reference:bugtraq,3952; classtype:web-application-attack; sid:1736; rev:15;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP Intelligent Management Center database credentials information disclosure attempt - 2"; flow:to\_server,established; content:"/rpt/reportscript/sqlserver/deploypara.properties"; nocase; http\_uri; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,40298; reference:url,secunia.com/advisories/39891; classtype:attempted-user; sid:17158; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP axs.cgi access"; flow:to\_server,established; content:"/axs.cgi"; http\_uri; metadata:service http; classtype:web-application-activity; sid:1205; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP uselang code injection"; flow:to\_server,established; content:"/wiki"; nocase; http\_uri; content:"?uselang="; fast\_pattern; nocase; http\_uri; pcre:"/\x2fwiki[^\n]\*\x3fuselang=[^\n\x26\x3f]\*[a-zA-Z\x2d]/Usmi"; metadata:policy security-ips drop, service http; reference:bugtraq,15703; reference:cve,2005-4031; classtype:web-application-attack; sid:16079; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP PhpGedView PGV config\_gedcom.php base directory manipulation attempt"; flow:to\_server,established; content:"/config\_gedcom.php"; nocase; http\_uri; content:"PGV\_BASE\_DIRECTORY"; fast\_pattern:only; metadata:service http; reference:bugtraq,9368; reference:cve,2004-0030; classtype:web-application-attack; sid:2368; rev:11;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 8080 (msg:"SERVER-WEBAPP Novell iManager eDirectory plugin schema buffer overflow attempt - POST request"; flow:to\_server,established; content:"POST"; nocase; http\_method; content:"/nps/servlet/"; nocase; http\_uri; content:"taskId=base.ExtendSchema"; nocase; http\_uri; pcre:"/(((DestFile|encryptPass)\x3D[^\x26]{50})|((BaseDN|SearchFilter)\x3D[^\x26]{128}))/Pi"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,37672; reference:cve,2009-4486; classtype:attempted-admin; sid:16430; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 25 (msg:"SERVER-WEBAPP 5.3.3 mt\_rand integer overflow attempt"; flow:to\_server,established; file\_data; content:"mt\_getrandmax("; fast\_pattern:only; content:"<?"; pcre:"/(define\(\s\*(?P<q1>[\x22\x27])\s\*(?P<m1>\w+)(?P=q1)\s\*,\s\*mt\_getrandmax\(\)\s\*\+\d+\s\*\)\x3b.\*?mt\_rand\(\s\*0\s\*,\s\*(?P=m1)\s\*\)|(?P<m2>\$\w+)\s\*=\s\*mt\_getrandmax\(\)\s\*\+\s\*\d+\s\*\x3b.\*?mt\_rand\(\s\*0\s\*,\s\*(?P=m2)\s\*\)|mt\_rand\(\s\*0\s\*,\s\*mt\_getrandmax\(\)\s\*\+\s\*\d+\s\*\)\x3b)/smi"; metadata:service smtp; reference:cve,2011-0755; classtype:misc-activity; sid:24059; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP osCommerce categories.php Arbitrary File Upload And Code Execution"; flow:to\_server,established; content:"/admin/categories.php/login.php?cPath=&action=new\_product\_preview"; fast\_pattern:only; metadata:service http; reference:bugtraq,44995; classtype:web-application-attack; sid:18678; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP phpMyAdmin db\_details\_importdocsql.php access"; flow:to\_server,established; content:"db\_details\_importdocsql.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,7962; reference:bugtraq,7965; reference:nessus,11761; classtype:web-application-attack; sid:2228; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP post32.exe arbitrary command attempt"; flow:to\_server,established; content:"/post32.exe|7C|"; http\_uri; metadata:service http; reference:bugtraq,1485; classtype:web-application-attack; sid:2070; rev:8;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP newsPHP Language file include attempt"; flow:to\_server,established; content:"/nphpd.php"; fast\_pattern; nocase; http\_uri; content:"LangFile"; nocase; metadata:service http; reference:bugtraq,8488; classtype:web-application-activity; sid:2365; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP sendmessage.cgi access"; flow:to\_server,established; content:"/sendmessage.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,3673; reference:cve,2001-1100; classtype:attempted-recon; sid:1308; rev:18;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP OpenView NNM getnnmdata.exe CGI ICount parameter buffer overflow attempt"; flow:to\_server,established; content:"/OvCgi/getnnmdata|2E|exe"; fast\_pattern:only; http\_uri; content:"ICount|3D|"; nocase; isdataat:300,relative; pcre:"/ICount\x3D\x2D[^\x26\x3F\x3B\x0D\x0A\s]{300}/i"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:cve,2010-1554; classtype:attempted-user; sid:19137; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ministats admin access"; flow:to\_server,established; content:"/ministats/admin.cgi"; nocase; http\_uri; metadata:service http; classtype:web-application-activity; sid:1215; rev:16;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP OpenView Network Node Manager cookie buffer overflow attempt"; flow:to\_server,established; content:"/OVCgi/printsession.exe"; fast\_pattern:only; http\_uri; pcre:"/(OvJavaScript|OvTitleFrame|OvHelpWindow|OvMap|OvSession|OvJavaLocale|OvOSLocale|OvLogin|OvDebug|OvDeveloper|OvTreeControl|OvJavaScript|OvProduct|OvPort|OvLocale|OvWebSession)\s\*\x3D[^\x3B\x2C]{1024}/iC"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,42154; reference:cve,2010-2709; classtype:attempted-user; sid:18922; rev:3;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Joomla Remote File Include upload attempt"; flow:to\_server,established; content:"POST"; http\_method; content:"/images/psg.php"; http\_uri; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:url,stopmalvertising.com/security/95.211.20.103-local-file-inclusion-attack.html; reference:url,www.mmleoni.net/sql-iniection-lfi-protection-plugin-for-joomla; classtype:attempted-user; sid:23827; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP AnnoncesV remote file include in annonce.php page"; flow:to\_server,established; content:"annonce.php"; fast\_pattern:only; http\_uri; pcre:"/\x2Fannonce\.php?[^\r\n]\*?page=(https?|ftps?)/Ui"; metadata:service http; reference:bugtraq,19854; reference:cve,2006-4622; classtype:web-application-activity; sid:20632; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP nc.exe attempt"; flow:to\_server,established; content:"nc.exe"; nocase; metadata:service http; classtype:web-application-activity; sid:1062; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP PHP function CRLF injection attempt"; flow:to\_server,established; content:".php"; http\_uri; content:"|0A|"; http\_uri; metadata:service http; reference:bugtraq,52630; reference:bugtraq,5681; reference:cve,2002-1783; classtype:web-application-attack; sid:12360; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP CISCO PIX Firewall Manager directory traversal attempt"; flow:to\_server,established; content:"/pixfir~1/how\_to\_login.html"; http\_uri; metadata:service http; reference:bugtraq,691; reference:cve,1999-0158; reference:nessus,10819; classtype:misc-attack; sid:1858; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP rsh access"; flow:to\_server,established; content:"/rsh"; nocase; http\_uri; metadata:service http; reference:cve,1999-0509; reference:url,www.cert.org/advisories/CA-1996-11.html; classtype:attempted-recon; sid:868; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP wrap access"; flow:to\_server,established; content:"/wrap"; http\_uri; metadata:service http; reference:bugtraq,373; reference:cve,1999-0149; reference:nessus,10317; classtype:attempted-recon; sid:853; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP WebLogic ConsoleHelp view source attempt"; flow:to\_server,established; content:"/ConsoleHelp/"; nocase; http\_uri; content:".jsp"; nocase; http\_uri; metadata:service http; reference:bugtraq,1518; reference:cve,2000-0682; reference:nessus,11724; classtype:web-application-attack; sid:2238; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP sdbsearch.cgi access"; flow:to\_server,established; content:"/sdbsearch.cgi"; http\_uri; metadata:service http; reference:bugtraq,1658; reference:cve,2000-0868; reference:nessus,10503; classtype:web-application-activity; sid:1878; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP dcboard.cgi access"; flow:to\_server,established; content:"/dcboard.cgi"; http\_uri; metadata:service http; reference:bugtraq,2728; reference:cve,2001-0527; reference:nessus,10583; classtype:attempted-recon; sid:1410; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP .bash\_history access"; flow:to\_server,established; content:"/.bash\_history"; http\_uri; metadata:service http; reference:bugtraq,337; reference:cve,1999-0408; classtype:web-application-attack; sid:1434; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP SAP NetWeaver cross site scripting attempt"; flow:established,to\_server; content:"/RequestParts.htm"; fast\_pattern:only; http\_uri; pcre:"/[?&]sap-ffield=[^&]+?([\x22\x27\x3c\x3e\x28\x29]|script|onload|src)/Ui"; metadata:policy security-ips drop, service http; reference:url,service.sap.com/sap/support/notes/1422273; classtype:web-application-attack; sid:23260; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP csSearch.cgi arbitrary command execution attempt"; flow:to\_server,established; content:"/csSearch.cgi"; http\_uri; content:"setup="; content:"`"; content:"`"; distance:1; metadata:service http; reference:bugtraq,4368; reference:cve,2002-0495; reference:nessus,10924; classtype:web-application-attack; sid:1547; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP webfind.exe access"; flow:to\_server,established; content:"/webfind.exe"; nocase; http\_uri; metadata:service http; reference:bugtraq,1487; reference:cve,2000-0622; reference:nessus,10475; classtype:web-application-activity; sid:1849; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Free Download Manager Remote Control Server HTTP Auth Header buffer overflow attempt"; flow:to\_server,established; content:"Authorization|3A 20|Basic"; nocase; isdataat:256,relative; content:!"|0D 0A|"; within:256; metadata:service http; reference:bugtraq,33554; reference:cve,2009-0183; classtype:attempted-user; sid:17536; rev:8;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP DELETE attempt"; flow:to\_server,established; content:"DELETE "; depth:7; nocase; metadata:service http; reference:nessus,10498; classtype:web-application-activity; sid:1603; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 8080 (msg:"SERVER-WEBAPP Delegate whois overflow attempt"; flow:to\_server,established; content:"whois|3A|//"; nocase; reference:cve,2000-0165; reference:nessus,10054; classtype:web-application-activity; sid:1558; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP LWGate access"; flow:to\_server,established; content:"/LWGate"; nocase; http\_uri; metadata:service http; reference:url,www.netspace.org/~dwb/lwgate/lwgate-history.html; reference:url,www.wiretrip.net/rfp/p/doc.asp/i2/d6.htm; classtype:attempted-recon; sid:880; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Oracle iSQLPlus sid overflow attempt"; flow:to\_server,established; content:"/isqlplus"; nocase; http\_uri; pcre:"/sid=[^&\x3b\r\n]{255}/si"; metadata:service http; reference:bugtraq,10871; reference:url,www.nextgenss.com/advisories/ora-isqlplus.txt; classtype:web-application-attack; sid:2701; rev:9;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP OpenView Performance Insight Server backdoor account code execution attempt"; flow:to\_server,established; content:"/services"; nocase; http\_uri; content:"aGNoOTA4djp6NnQwaiQraQ=="; fast\_pattern:only; http\_header; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,46079; reference:cve,2011-0276; classtype:attempted-admin; sid:18560; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP strings overflow"; flow:to\_server,established; content:"|BA|I|FE FF FF F7 D2 B9 BF FF FF FF F7 D1|"; metadata:service http; reference:bugtraq,802; classtype:web-application-attack; sid:1085; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP F5 Networks FirePass my.activation.php3 state parameter sql injection attempt"; flow:established,to\_server; content:"/my.activation.php3"; fast\_pattern:only; http\_uri; content:"state="; nocase; http\_uri; pcre:"/[?&]state=[^&]\*?[\x22\x27]/Ui"; metadata:policy security-ips drop, service http; reference:cve,2012-1777; reference:url,support.f5.com/kb/en-us/solutions/public/13000/400/sol13463.html; classtype:attempted-admin; sid:24517; rev:1;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP apache chunked encoding memory corruption exploit attempt"; flow:to\_server,established; content:"|C0|PR|89 E1|PQRP|B8 3B 00 00 00 CD 80|"; metadata:service http; reference:bugtraq,5033; reference:cve,2002-0392; classtype:web-application-activity; sid:1808; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP DNSTools administrator authentication bypass attempt"; flow:to\_server,established; content:"/dnstools.php"; nocase; http\_uri; content:"user\_logged\_in=true"; nocase; content:"user\_dnstools\_administrator=true"; fast\_pattern:only; metadata:service http; reference:bugtraq,4617; reference:cve,2002-0613; classtype:web-application-attack; sid:1739; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 901 (msg:"SERVER-WEBAPP Samba SWAT HTTP Authentication overflow attempt"; flow:to\_server,established; content:"Authorization|3A 20|Basic|20 3D|"; http\_header; metadata:policy security-ips drop, service http; reference:bugtraq,10780; reference:cve,2004-0600; classtype:attempted-user; sid:18751; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP process\_bug.cgi access"; flow:to\_server,established; content:"/process\_bug.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,3272; reference:cve,2002-0008; classtype:web-application-activity; sid:2053; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HTTP response splitting attempt"; flow:to\_server,established; content:"Content-Length: 0|0D 0A|"; nocase; http\_uri; metadata:service http; classtype:attempted-user; sid:21465; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP System variable in URI attempt - %COMPUTERNAME%"; flow:to\_server,established; content:"%COMPUTERNAME%"; fast\_pattern:only; http\_uri; metadata:service http; classtype:attempted-recon; sid:21839; rev:3;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 383 (msg:"SERVER-WEBAPP HP Operations Agent stack buffer overflow attempt"; flow:to\_server,established; flowbits:isset,hp\_openview\_coda; content:"|FF FF 00 00 00 01 00 00 00 34 00 00 00 03 00 44 44 44 42 42|"; fast\_pattern:only; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,54362; reference:cve,2012-2019; reference:url,h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03397769; classtype:attempted-admin; sid:24320; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Advanced Poll admin\_preview.php access"; flow:to\_server,established; content:"/admin\_preview.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,8890; reference:nessus,11487; classtype:web-application-activity; sid:2294; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP finger access"; flow:to\_server,established; content:"/finger"; nocase; http\_uri; metadata:service http; reference:cve,1999-0612; reference:nessus,10071; classtype:attempted-recon; sid:839; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP directory.php access"; flow:to\_server,established; content:"/directory.php"; http\_uri; metadata:service http; reference:bugtraq,4278; reference:cve,2002-0434; classtype:misc-attack; sid:1816; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS 80 (msg:"SERVER-WEBAPP sphpblog arbitrary file delete attempt"; flow:to\_server,established; content:"sphpblog"; http\_uri; content:"comment\_delete\_cgi.php"; fast\_pattern; nocase; http\_uri; pcre:"/comment=[^\x26\s]\*[\x2f\x5c]/sUmi"; metadata:service http; reference:bugtraq,14667; reference:cve,2005-2733; classtype:attempted-user; sid:11667; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 3128 (msg:"SERVER-WEBAPP Squid authentication headers handling denial of service attempt"; flow:to\_server,established; flowbits:isset,ntlm\_authentication; content:"Proxy-Authorization: "; content:!"NTLM"; within:4; metadata:policy security-ips drop, service http; reference:bugtraq,14977; reference:cve,2005-2917; classtype:attempted-dos; sid:17371; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP cross-site scripting attempt via form data attempt"; flow:to\_server,established; content:"%3Cscript"; nocase; http\_client\_body; metadata:policy security-ips drop, service http; classtype:attempted-user; sid:19645; rev:4;)

#alert tcp $EXTERNAL\_NET $HTTP\_PORTS -> $HOME\_NET any (msg:"SERVER-WEBAPP Worldweaver DX Studio Player shell.execute command execution attempt"; flow:to\_client,established; flowbits:isset,http.dxstudio.clsid; content:"Content-Type|3A| application/octet-stream"; fast\_pattern; nocase; http\_header; file\_data; content:"header.xml"; depth:10; offset:30; nocase; metadata:service http; reference:bugtraq,35273; reference:cve,2009-2011; classtype:attempted-user; sid:20872; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Domino agentrunner.nsf access"; flow:to\_server,established; content:"/agentrunner.nsf"; nocase; http\_uri; metadata:service http; reference:nessus,10629; classtype:attempted-recon; sid:1585; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP PHPNuke Forum viewtopic SQL insertion attempt"; flow:to\_server,established; content:"/modules.php"; nocase; http\_uri; content:"name=Forums"; content:"file=viewtopic"; fast\_pattern:only; pcre:"/forum=.\*'/"; metadata:service http; reference:bugtraq,7193; classtype:web-application-attack; sid:2654; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP args.bat access"; flow:to\_server,established; content:"/args.bat"; nocase; http\_uri; metadata:service http; reference:cve,1999-1180; reference:nessus,11465; classtype:attempted-recon; sid:844; rev:19;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP SoftCart.exe CGI buffer overflow attempt"; flow:to\_server,established; content:"/SoftCart.exe"; nocase; http\_uri; pcre:"/\/SoftCart\.exe\?[^\s]{100}/smi"; metadata:service http; reference:bugtraq,10926; reference:cve,2004-2221; classtype:web-application-attack; sid:3638; rev:19;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP System variable directory traversal attempt - %COMSPEC%"; flow:to\_server,established; content:"%COMSPEC%"; fast\_pattern:only; http\_uri; metadata:service http; classtype:attempted-recon; sid:21823; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP environ.cgi access"; flow:to\_server,established; content:"/environ.cgi"; nocase; http\_uri; metadata:service http; classtype:attempted-recon; sid:856; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP mkplog.exe access"; flow:to\_server,established; content:"/mkplog.exe"; nocase; http\_uri; metadata:service http; classtype:web-application-activity; sid:1664; rev:11;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP SiteScope UploadFilesHandler directory traversal attempt"; flow:to\_server,established; content:"REMOTE\_HANDLER\_KEY=UploadFilesHandler"; fast\_pattern:only; http\_uri; content:"UploadFilesHandler.file.name="; http\_uri; content:".."; within:3; http\_uri; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,55273; reference:cve,2012-3264; classtype:web-application-activity; sid:24448; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP /ecscripts/ecware.exe access"; flow:to\_server,established; content:"/ecscripts/ecware.exe"; nocase; http\_uri; metadata:service http; reference:bugtraq,6066; classtype:web-application-activity; sid:1944; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Arbitrary file location upload attempt"; flow:to\_server,established; content:"POST"; http\_method; content:".php"; http\_uri; content:"Content-Type: multipart/form-data"; http\_header; content:"filename="; fast\_pattern:only; http\_client\_body; pcre:"/filename=(\x22|\x27)\.\.\x2f/smi"; metadata:service http; reference:bugtraq,11190; reference:cve,2004-0959; classtype:web-application-activity; sid:23613; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP carbo.dll access"; flow:to\_server,established; content:"/carbo.dll"; http\_uri; content:"icatcommand="; nocase; metadata:policy security-ips drop, service http; reference:bugtraq,2126; reference:cve,1999-1069; classtype:attempted-recon; sid:1001; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP System variable directory traversal attempt - %PROGRAMFILES - X86%"; flow:to\_server,established; content:"%PROGRAMFILES|40|X86|41|%"; fast\_pattern:only; http\_uri; metadata:service http; classtype:attempted-recon; sid:21828; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Setup.php access"; flow:to\_server,established; content:"/Setup.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,9057; reference:cve,2009-1151; classtype:web-application-activity; sid:2281; rev:13;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Novell ZENworks Asset Management default admin credentials function call attempt"; flow:to\_server,established; content:"/rtrlet/rtr"; fast\_pattern:only; http\_uri; content:"username=ivanhoe"; nocase; http\_client\_body; content:"password=scott"; nocase; http\_client\_body; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:cve,2012-4933; reference:url,www.kb.cert.org/vuls/id/332412; classtype:attempted-admin; sid:24435; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP oracle web arbitrary command execution attempt"; flow:to\_server,established; content:"/ows-bin/"; nocase; http\_uri; content:"?&"; http\_uri; metadata:service http; reference:bugtraq,1053; reference:cve,2000-0169; reference:nessus,10348; classtype:web-application-attack; sid:1193; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP SmartWin CyberOffice Shopping Cart access"; flow:to\_server,established; content:"\_private/shopping\_cart.mdb"; http\_uri; metadata:service http; reference:bugtraq,1734; reference:cve,2000-0925; classtype:web-application-attack; sid:1098; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP statsconfig.pl access"; flow:to\_server,established; content:"/statsconfig.pl"; nocase; http\_uri; metadata:service http; reference:bugtraq,2211; reference:cve,2001-0113; classtype:web-application-activity; sid:1718; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Webtrends HTTP probe"; flow:to\_server,established; content:"User-Agent|3A| Webtrends Security Analyzer|0D 0A|"; http\_header; metadata:service http; classtype:web-application-activity; sid:1101; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Novell Groupwise gwweb.exe access"; flow:to\_server,established; content:"/GWWEB.EXE"; nocase; metadata:service http; reference:bugtraq,879; reference:cve,1999-1005; reference:cve,1999-1006; reference:nessus,10877; classtype:attempted-recon; sid:1165; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP philboard\_admin.asp access"; flow:to\_server,established; content:"/philboard\_admin.asp"; http\_uri; metadata:service http; reference:bugtraq,7739; reference:nessus,11675; classtype:web-application-activity; sid:2137; rev:8;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP OpenView CGI parameter buffer overflow attempt"; flow:to\_server,established; content:"GET"; nocase; http\_method; content:"+textFile-"; fast\_pattern:only; nocase; http\_uri; content:"/OvCgi/"; http\_uri; pcre:"/\/OvCgi\/(jovgraph|webappmon)\.exe.\*?-textFile+[^+]{201}/iU"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:cve,2010-1551; reference:cve,2010-1552; reference:cve,2010-1553; reference:cve,2010-1554; reference:cve,2010-1555; reference:cve,2010-1960; reference:cve,2010-1961; reference:cve,2011-3167; classtype:attempted-user; sid:16674; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP php.exe access"; flow:to\_server,established; content:"/php.exe"; nocase; http\_uri; metadata:service http; reference:url,www.securitytracker.com/alerts/2002/Jan/1003104.html; classtype:web-application-activity; sid:1773; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP VirusWall catinfo access"; flow:to\_server,established; content:"/catinfo"; nocase; http\_uri; metadata:service http; reference:bugtraq,2579; reference:bugtraq,2808; reference:cve,2001-0432; reference:nessus,10650; classtype:attempted-recon; sid:1231; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP psunami.cgi access"; flow:to\_server,established; content:"/psunami.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,6607; reference:nessus,11750; classtype:web-application-activity; sid:2224; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS 3000 (msg:"SERVER-WEBAPP MDaemon form2raw.cgi overflow attempt"; flow:to\_server,established; content:"/form2raw.cgi"; fast\_pattern:only; pcre:"/\Wfrom=[^\x3b&\n]{100}/si"; reference:bugtraq,9317; reference:cve,2003-1200; reference:url,secunia.com/advisories/10512/; classtype:web-application-attack; sid:2433; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP oracle web application server access"; flow:to\_server,established; content:"/ows-bin/"; nocase; http\_uri; metadata:service http; reference:bugtraq,1053; reference:cve,2000-0169; reference:nessus,10348; classtype:web-application-activity; sid:1880; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP EXIF header parsing integer overflow attempt little endian"; flow:to\_server,established; content:"Exif|00 00 49 49 2A 00 08 00 00 00|"; http\_client\_body; content:"|03 90 02 00|"; distance:0; http\_client\_body; byte\_test:4,>,2048,0,relative,little; metadata:policy security-ips drop, service http; reference:cve,2011-4566; reference:url,osvdb.org/77446; classtype:web-application-attack; sid:22951; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP WebDAV search access"; flow:to\_server,established; content:"SEARCH "; depth:8; nocase; metadata:service http; reference:bugtraq,1756; reference:cve,2000-0951; classtype:web-application-activity; sid:1070; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Remote Execution Backdoor Attempt Against Horde"; flow:to\_server,established; content:"/services/javascript.php"; fast\_pattern:only; http\_uri; content:"href="; http\_cookie; content:"file=open\_calendar.js"; http\_client\_body; metadata:policy security-ips drop, service http; reference:cve,2012-0209; reference:url,dev.horde.org/h/jonah/stories/view.php?channel\_id=1&id=155; reference:url,eromang.zataz.com/2012/02/15/cve-2012-0209-horde-backdoor-analysis/; reference:url,pastebin.com/U3ADiWrP; classtype:web-application-attack; sid:21375; rev:5;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET [8008,8010,8028,8030] (msg:"SERVER-WEBAPP Novell eDirectory HTTP request content-length heap buffer overflow attempt"; flow:to\_server,established; content:"POST /SOAP"; depth:10; nocase; pcre:"/^Content-Length\s\*\x3A\s\*[1-9][0-9]{8}/mi"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:cve,2008-4478; classtype:attempted-user; sid:16194; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP System variable directory traversal attempt - %PUBLIC%"; flow:to\_server,established; content:"%PUBLIC%"; fast\_pattern:only; http\_uri; metadata:service http; classtype:attempted-recon; sid:21837; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 8000 (msg:"SERVER-WEBAPP nstelemetry.adp access"; flow:to\_server,established; content:"/nstelemetry.adp"; reference:nessus,10753; classtype:web-application-activity; sid:1518; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP .htgroup access"; flow:to\_server,established; content:".htgroup"; nocase; http\_uri; metadata:service http; classtype:web-application-activity; sid:1374; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Advanced Poll popup.php access"; flow:to\_server,established; content:"/popup.php"; fast\_pattern; nocase; http\_uri; content:"include\_path="; nocase; http\_uri; metadata:service http; reference:bugtraq,8890; reference:nessus,11487; classtype:web-application-activity; sid:2303; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP search.vts access"; flow:to\_server,established; content:"/search.vts"; http\_uri; metadata:service http; reference:bugtraq,162; classtype:attempted-recon; sid:1202; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP PhpGedView PGV base directory manipulation"; flow:to\_server,established; content:"\_conf.php"; nocase; http\_uri; content:"PGV\_BASE\_DIRECTORY"; fast\_pattern:only; metadata:service http; reference:bugtraq,9368; classtype:web-application-attack; sid:2926; rev:8;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP test-cgi access"; flow:to\_server,established; content:"/test-cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,2003; reference:cve,1999-0070; reference:nessus,10282; classtype:attempted-recon; sid:835; rev:20;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP HP OpenView Manager DOS"; flow:to\_server,established; content:"/OvCgi/OpenView5.exe?Context=Snmp&Action=Snmp&Host=&Oid="; nocase; http\_uri; metadata:service http; reference:bugtraq,2845; reference:cve,2001-0552; classtype:misc-activity; sid:1258; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP phpbb quick-reply.php access"; flow:to\_server,established; content:"/quick-reply.php"; http\_uri; metadata:service http; reference:bugtraq,6173; classtype:web-application-activity; sid:1968; rev:8;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP CVSTrac filediff function access"; flow:to\_server,established; content:"filediff"; fast\_pattern; nocase; http\_uri; content:"f="; nocase; metadata:service http; reference:bugtraq,10878; reference:cve,2004-1456; reference:nessus,14238; reference:url,www.kb.cert.org/vuls/id/770816; classtype:web-application-activity; sid:8084; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Annex Terminal DOS attempt"; flow:to\_server,established; content:"/ping?query="; http\_uri; metadata:service http; reference:cve,1999-1070; reference:nessus,10017; classtype:attempted-dos; sid:1181; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP edit\_action.cgi access"; flow:to\_server,established; content:"/edit\_action.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,3698; reference:bugtraq,4579; reference:cve,2001-1196; reference:nessus,11748; classtype:web-application-activity; sid:2202; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP redirect access"; flow:to\_server,established; content:"/redirect"; nocase; http\_uri; metadata:service http; reference:bugtraq,1179; reference:cve,2000-0382; classtype:attempted-recon; sid:895; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP LongTail Video JW Player XSS attempt link param"; flow:to\_server,established; content:"/player.swf?"; fast\_pattern; http\_uri; content:"link="; distance:0; http\_uri; content:"javascript:"; distance:0; http\_uri; metadata:policy security-ips drop, service http; reference:bugtraq,54101; reference:cve,2012-3351; classtype:web-application-attack; sid:23984; rev:2;)

alert tcp $HOME\_NET any -> $EXTERNAL\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Symantec Web Gateway PHP remote code injection attempt"; flow:established,to\_server; content:"/spywall/blocked\_file.php"; fast\_pattern:only; http\_uri; content:"<?"; http\_client\_body; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,53443; reference:cve,2012-0299; reference:url,osvdb.org/53443; reference:url,www.symantec.com/security\_response/securityupdates/detail.jsp?fid=security\_advisory&pvid=security\_advisory&year=2012&suid=20120517\_00; classtype:attempted-admin; sid:24518; rev:1;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP icat access"; flow:to\_server,established; content:"/icat"; http\_uri; metadata:service http; reference:cve,1999-1069; classtype:web-application-activity; sid:1606; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Symantec Sygate Policy Manager SQL injection"; flow:to\_server,established; content:"/servlet/Sygate.Servlet.login"; nocase; http\_uri; pcre:"/[^\x26\x20\x0a]\*insert[^\x26\x20\x0a]\*Login[^\x26\x20\x0a]\*Admin/smi"; metadata:service http; reference:bugtraq,16452; reference:cve,2006-0522; classtype:attempted-admin; sid:11616; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cart.cgi access"; flow:to\_server,established; content:"/cart.cgi"; http\_uri; metadata:service http; reference:bugtraq,1115; reference:cve,2000-0252; reference:nessus,10368; classtype:web-application-activity; sid:1933; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP eshop.pl access"; flow:to\_server,established; content:"/eshop.pl"; nocase; http\_uri; metadata:service http; reference:bugtraq,3340; reference:cve,2001-1014; classtype:web-application-activity; sid:1566; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ICQ webserver DOS"; flow:to\_server,established; content:".html/......"; nocase; http\_uri; metadata:service http; reference:cve,1999-0474; reference:url,www.securiteam.com/exploits/2ZUQ1QAQOG.html; classtype:attempted-dos; sid:1115; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Java floating point number denial of service - via URI"; flow:to\_server,established; content:"2.2250738585072012e-308"; nocase; http\_uri; metadata:policy security-ips drop, service http; reference:cve,2010-4476; reference:url,www.oracle.com/technetwork/topics/security/alert-cve-2010-4476-305811.html; classtype:attempted-dos; sid:18470; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Advanced Poll admin\_password.php access"; flow:to\_server,established; content:"/admin\_password.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,8890; reference:nessus,11487; classtype:web-application-activity; sid:2293; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP JBoss admin-console access"; flow:to\_server,established; content:"/admin-console/"; nocase; http\_uri; metadata:service http; reference:url,docs.jboss.org/jbossas/6/Admin\_Console\_Guide/en-US/pdf/Admin\_Console\_Guide.pdf; classtype:attempted-recon; sid:21517; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Phorum /support/common.php attempt"; flow:to\_server,established; content:"/support/common.php"; http\_uri; content:"ForumLang=../"; metadata:service http; reference:bugtraq,1997; classtype:web-application-attack; sid:1490; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cvslog.cgi access"; flow:to\_server,established; content:"/cvslog.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,4579; reference:bugtraq,5517; reference:cve,2003-0153; reference:nessus,11748; classtype:web-application-activity; sid:2198; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP readmsg.php access"; flow:to\_server,established; content:"/readmsg.php"; http\_uri; metadata:service http; reference:cve,2001-1408; reference:nessus,11073; classtype:web-application-activity; sid:2000; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP AltaVista Intranet Search directory traversal attempt"; flow:to\_server,established; content:"/query?mss=.."; http\_uri; metadata:service http; reference:bugtraq,896; reference:cve,2000-0039; reference:nessus,10015; classtype:web-application-attack; sid:1509; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP db2www access"; flow:to\_server,established; content:"/db2www"; http\_uri; metadata:service http; reference:cve,2000-0677; classtype:web-application-activity; sid:1643; rev:12;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP OpenView Network Node Manager ovwebsnmpsrv.exe displayWidth buffer overflow attempt - GET"; flow:to\_server,established; content:"|2F|OvCgi|2F|jovgraph.exe"; nocase; http\_uri; content:"displayWidth"; distance:0; nocase; http\_uri; pcre:"/(displayWidth[\x2b\x20]\d[^\x2b\s\n]{128})/siU"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,45762; reference:cve,2011-0262; classtype:attempted-user; sid:18760; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP echo.bat access"; flow:to\_server,established; content:"/echo.bat"; http\_uri; metadata:service http; reference:bugtraq,1002; reference:cve,2000-0213; reference:nessus,10246; classtype:web-application-activity; sid:1706; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cat%20 access"; flow:to\_server,established; content:"cat "; nocase; http\_uri; metadata:service http; reference:bugtraq,374; reference:cve,1999-0039; classtype:attempted-recon; sid:1147; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP WEB-INF access"; flow:to\_server,established; content:"/WEB-INF"; nocase; http\_uri; metadata:service http; reference:bugtraq,1830; reference:bugtraq,5119; reference:cve,2000-1050; reference:cve,2001-0179; reference:nessus,11037; classtype:web-application-activity; sid:1826; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP anaconda directory transversal attempt"; flow:to\_server,established; content:"/apexec.pl"; http\_uri; content:"template=../"; fast\_pattern:only; metadata:service http; reference:bugtraq,2338; reference:bugtraq,2388; reference:cve,2000-0975; reference:cve,2001-0308; reference:nessus,10536; classtype:web-application-attack; sid:820; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP AT-generated.cgi access"; flow:to\_server,established; content:"/AT-generated.cgi"; nocase; http\_uri; metadata:service http; reference:cve,1999-1072; classtype:attempted-recon; sid:1453; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP post-query access"; flow:to\_server,established; content:"/post-query"; nocase; http\_uri; metadata:service http; reference:bugtraq,6752; reference:cve,2001-0291; classtype:attempted-recon; sid:866; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP myPHPNuke partner.php access"; flow:to\_server,established; content:"/partner.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,6544; classtype:web-application-activity; sid:2347; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP admin.php file upload attempt"; flow:to\_server,established; content:"/admin.php"; fast\_pattern; nocase; http\_uri; content:"file\_name="; metadata:service http; reference:bugtraq,3361; reference:cve,2001-1032; classtype:attempted-admin; sid:1300; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ServletManager access"; flow:to\_server,established; content:"/servlet/ServletManager"; nocase; http\_uri; metadata:service http; reference:bugtraq,3697; reference:cve,2001-1195; reference:nessus,12122; classtype:web-application-activity; sid:2447; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cgforum.cgi access"; flow:to\_server,established; content:"/cgforum.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,1951; reference:cve,2000-1132; classtype:web-application-activity; sid:1713; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Demarc SQL injection attempt"; flow:to\_server,established; content:"/dm/demarc"; http\_uri; content:"s\_key="; content:"'"; distance:0; content:"'"; distance:1; content:"'"; distance:0; metadata:service http; reference:bugtraq,4520; reference:cve,2002-0539; classtype:web-application-activity; sid:2063; rev:12;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP PHP-CGI command injection attempt"; flow:to\_server,established; content:".php?"; http\_uri; content:"-s"; nocase; http\_uri; content:!"="; http\_raw\_uri; pcre:"/\x2ephp\x3f\s\*-s/Ui"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:cve,2012-1823; reference:cve,2012-2311; classtype:attempted-admin; sid:22064; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 3057 (msg:"SERVER-WEBAPP Borland StarTeam Multicast Service buffer overflow attempt"; flow:to\_server,established; content:"GET AAAAAAAAAAAAAAAAAAAAA"; depth:25; reference:bugtraq,28602; reference:cve,2008-0311; classtype:attempted-admin; sid:16283; rev:3;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 383 (msg:"SERVER-WEBAPP HP Operations Agent stack buffer overflow attempt"; flow:to\_server,established; flowbits:isset,hp\_openview\_coda; content:"|00 00 00 34|"; depth:4; offset:18; byte\_jump:2,16,relative; byte\_jump:2,0,relative; byte\_test:2,>,1024,0,relative; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,54362; reference:cve,2012-2019; reference:url,h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03397769; classtype:attempted-admin; sid:23959; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP get32.exe access"; flow:to\_server,established; content:"/get32.exe"; nocase; http\_uri; metadata:service http; reference:bugtraq,1485; reference:bugtraq,770; reference:cve,1999-0885; reference:nessus,10011; classtype:attempted-recon; sid:1180; rev:22;)

alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Symantec Web Gateway blocked.php blind sql injection attempt"; flow:to\_server,established; content:"GET"; http\_method; content:"/spywall/blocked.php"; nocase; http\_uri; content:"id="; distance:0; nocase; http\_uri; pcre:"/[\x3f\x26]id=[^$&]\*?\D/isU"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,54424; reference:cve,2012-2574; reference:url,osvdb.org/show/osvdb/84118; classtype:attempted-user; sid:23934; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP phf arbitrary command execution attempt"; flow:to\_server,established; content:"/phf"; fast\_pattern; nocase; http\_uri; content:"QALIAS"; nocase; content:"%0a"; nocase; metadata:service http; reference:bugtraq,629; reference:cve,1999-0067; classtype:web-application-attack; sid:1762; rev:20;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Symantec IM Manager administrator interface SQL injection attempt"; flow:to\_server,established; content:"/IMManager/Admin/IMAdminLDAPConfig.asp"; fast\_pattern; http\_uri; content:"action=edit"; nocase; http\_uri; pcre:"/(IMManager\_LdapUpdate\_ServerName|IMManager\_LdapUpdate\_UserDN|IMManager\_LdapUpdate\_Port|IMManager\_LdapUpdate\_Secure\_Port|IMManager\_LdapUpdate\_UserQuery|IMManager\_LdapUpdate\_GroupQuery|hdn\_IMManager\_LdapUpdate\_ObjectClasses)=[^\x26]\*?([\x27\x22]|%(22|27))/i"; metadata:service http; reference:bugtraq,49738; reference:cve,2011-0553; reference:url,secunia.com/advisories/43157; classtype:web-application-attack; sid:20832; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 8888 (msg:"SERVER-WEBAPP SiteScope Service access"; flow:to\_server,established; content:"/SiteScope/cgi/go.exe/SiteScope"; reference:nessus,10778; classtype:web-application-activity; sid:1499; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Gravity GTD objectname parameter injection attempt"; flow:to\_server,established; content:"/library/setup/rpc.php"; fast\_pattern:only; http\_uri; pcre:"/objectname=[^\x26]\*?(\x2e\x2e\x2f|[^a-z0-9])/iU"; metadata:service http; reference:cve,2008-5962; classtype:attempted-admin; sid:21594; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP responder.cgi access"; flow:to\_server,established; content:"/responder.cgi"; http\_uri; metadata:service http; reference:bugtraq,3155; classtype:web-application-activity; sid:1208; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ndcgi.exe access"; flow:to\_server,established; content:"/ndcgi.exe"; nocase; http\_uri; metadata:service http; reference:bugtraq,3583; reference:cve,2001-0922; reference:nessus,11730; classtype:web-application-activity; sid:2243; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 8080 (msg:"SERVER-WEBAPP Linksys router default password login attempt"; flow:to\_server,established; content:"Authorization|3A|"; nocase; http\_header; pcre:"/^Authorization\x3a(\s\*|\s\*\r?\n\s+)Basic\s+OmFkbWlu/smiH"; metadata:service http; reference:nessus,10999; classtype:default-login-attempt; sid:1860; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP oracle portal demo access"; flow:to\_server,established; content:"/pls/portal/PORTAL\_DEMO"; nocase; http\_uri; metadata:service http; reference:nessus,11918; classtype:web-application-activity; sid:2276; rev:7;)

#alert tcp $EXTERNAL\_NET $HTTP\_PORTS -> $HOME\_NET any (msg:"SERVER-WEBAPP Trend Micro atxconsole format string server response attempt"; flow:to\_client,established; file\_data; content:"-99 Cannot+find+"; content:"%25n"; distance:0; metadata:service http; reference:bugtraq,20284; reference:cve,2006-5157; classtype:attempted-user; sid:8444; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP auktion.cgi access"; flow:to\_server,established; content:"/auktion.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,2367; reference:cve,2001-0212; reference:nessus,10638; classtype:web-application-activity; sid:1465; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 8080 (msg:"SERVER-WEBAPP story.pl access"; flow:to\_server,established; content:"/story.pl"; http\_uri; metadata:service http; reference:bugtraq,3028; reference:cve,2001-0804; reference:nessus,10817; classtype:default-login-attempt; sid:1869; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP adminlogin access"; flow:to\_server,established; content:"/adminlogin"; nocase; http\_uri; metadata:service http; reference:bugtraq,1164; reference:bugtraq,1175; reference:nessus,11748; classtype:attempted-recon; sid:1218; rev:15;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 383 (msg:"SERVER-WEBAPP HP Operations Agent stack buffer overflow attempt"; flow:to\_server,established; flowbits:isset,hp\_openview\_coda; content:"|00 00 00 AC|"; depth:4; offset:18; byte\_jump:2,16,relative; byte\_jump:2,0,relative; byte\_test:2,>,1024,0,relative; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,54362; reference:cve,2012-2019; reference:url,h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03397769; classtype:attempted-admin; sid:23961; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ftp.pl attempt"; flow:to\_server,established; content:"/ftp.pl?dir=../.."; nocase; http\_uri; metadata:service http; reference:bugtraq,1471; reference:cve,2000-0674; reference:nessus,10467; classtype:web-application-attack; sid:1612; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ikonboard.cgi access"; flow:to\_server,established; content:"/ikonboard.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,7361; reference:nessus,11605; classtype:web-application-activity; sid:2127; rev:11;)

#alert tcp $EXTERNAL\_NET $HTTP\_PORTS -> $HOME\_NET any (msg:"SERVER-WEBAPP Citrix Program Neighborhood Agent Arbitrary Shortcut Creation attempt"; flow:to\_client,established; file\_data; content:"|3C|AppData|3E|"; nocase; content:"|3C|AppInStartmenu|20|value|3D 22|True|22|"; distance:0; nocase; metadata:policy security-ips drop, service http; reference:bugtraq,13379; reference:cve,2004-1077; classtype:attempted-user; sid:17420; rev:8;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Mambo uploadimage.php upload php file attempt"; flow:to\_server,established; content:"/uploadimage.php"; http\_uri; content:"userfile\_name="; content:".php"; distance:1; metadata:service http; reference:bugtraq,6572; reference:cve,2003-1204; reference:nessus,16315; classtype:web-application-attack; sid:2074; rev:9;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP phpMyAdmin session\_to\_unset session variable injection attempt"; flow:to\_server,established; content:"session\_to\_unset="; fast\_pattern:only; http\_uri; content:"\_SESSION["; nocase; http\_uri; pcre:"/session\_to\_unset=($|[\x26\x3B])/Ui"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:cve,2011-2505; reference:cve,2011-2506; reference:url,www.phpmyadmin.net/home\_page/security/PMASA-2011-5.php; reference:url,www.phpmyadmin.net/home\_page/security/PMASA-2011-6.php; classtype:attempted-user; sid:19553; rev:3;)

#alert tcp $EXTERNAL\_NET $HTTP\_PORTS -> $HOME\_NET any (msg:"SERVER-WEBAPP cookiejacking attempt"; flow:to\_client,established; file\_data; content:"file|3A 2F 2F 2F|"; nocase; pcre:"/<\s\*[A-Z]+\s+[^>]\*file\x3A\x2F\x2F\x2F/smi"; metadata:service http; reference:url,www.swisscyberstorm.com/speakers/valotta-slides; classtype:attempted-recon; sid:19177; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cal\_make.pl access"; flow:to\_server,established; content:"/cal\_make.pl"; nocase; http\_uri; metadata:service http; reference:bugtraq,2663; reference:cve,2001-0463; reference:nessus,10664; classtype:web-application-activity; sid:1474; rev:19;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP test.php access"; flow:to\_server,established; content:"/test.php"; nocase; http\_uri; metadata:service http; reference:nessus,11617; classtype:web-application-activity; sid:2152; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP WhatsUpGold instancename overflow attempt"; flow:to\_server,established; content:"/\_maincfgret.cgi"; fast\_pattern; nocase; http\_uri; content:"instancename="; nocase; http\_uri; isdataat:513,relative; pcre:"/instancename=[^&\x3b\r\n]{513}/Usmi"; metadata:service http; reference:bugtraq,11043; reference:cve,2004-0798; classtype:web-application-attack; sid:2663; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cvsweb.cgi access"; flow:to\_server,established; content:"/cvsweb.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,1469; reference:cve,2000-0670; reference:nessus,10465; classtype:attempted-recon; sid:823; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP mlog.phtml access"; flow:to\_server,established; content:"/mlog.phtml"; nocase; http\_uri; metadata:service http; reference:bugtraq,713; reference:cve,1999-0068; reference:cve,1999-0346; classtype:attempted-recon; sid:1119; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP /CVS/Entries access"; flow:to\_server,established; content:"/CVS/Entries"; http\_uri; metadata:service http; reference:nessus,10922; reference:nessus,11032; classtype:web-application-activity; sid:1551; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ws\_mail.cgi access"; flow:to\_server,established; content:"/ws\_mail.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,2861; reference:bugtraq,4579; reference:cve,2001-1343; reference:nessus,11748; classtype:web-application-activity; sid:2221; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP store.cgi access"; flow:to\_server,established; content:"/store.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,2385; reference:cve,2001-0305; reference:nessus,10639; classtype:web-application-activity; sid:1307; rev:19;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cgicso access"; flow:to\_server,established; content:"/cgicso"; http\_uri; metadata:service http; reference:bugtraq,6141; reference:cve,2002-1652; reference:nessus,10779; reference:nessus,10780; classtype:web-application-activity; sid:1875; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 5555 (msg:"SERVER-WEBAPP HP OpenView Storage Data Protector buffer overflow attempt"; flow:to\_server,established; content:"|FF FE 32 00 00 00|"; depth:6; offset:4; pcre:"/\x20\x00([^\x00].|.[^\x00]){255}/Osmi"; metadata:policy security-ips drop; reference:bugtraq,48486; reference:cve,2011-1865; classtype:attempted-admin; sid:20134; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP System variable in URI attempt - %PROMPT%"; flow:to\_server,established; content:"%PROMPT%"; fast\_pattern:only; http\_uri; metadata:service http; classtype:attempted-recon; sid:21843; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cacti graph\_image SQL injection attempt"; flow:to\_server,established; content:"graph.php"; nocase; http\_uri; pcre:"/rra\_id=(?!(\d+|all|)([\x26\s]|$))/smi"; metadata:service http; reference:bugtraq,14128; reference:bugtraq,14129; reference:cve,2005-2148; classtype:web-application-attack; sid:8715; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Axis Storpoint CD attempt"; flow:to\_server,established; content:"/cd/../config/html/cnf\_gi.htm"; metadata:service http; reference:bugtraq,1025; reference:cve,2000-0191; reference:nessus,10023; classtype:web-application-attack; sid:1524; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP myphpPagetool pt\_config.inc file include"; flow:to\_server,established; content:"/doc/admin"; nocase; http\_uri; content:"ptinclude="; nocase; content:"pt\_config.inc"; fast\_pattern:only; metadata:service http; reference:bugtraq,6744; classtype:web-application-attack; sid:2360; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET [8030,8028,8008,8010] (msg:"SERVER-WEBAPP Novell eDirectory SOAP Accept Charset header overflow attempt"; flow:to\_server,established; content:"/SOAP"; fast\_pattern; nocase; http\_uri; content:"Accept-Charset|3A|"; nocase; pcre:"/^Accept\x2dCharset\x3a\s\*?([^\x3b\x3d\x2c]{1,36}\s\*?[\x2d\x3b\x3d\x2c]\s\*?)\*[^\x2d\x3b\x2c\x3d\n]{37}/smi"; reference:cve,2008-4479; classtype:attempted-user; sid:14990; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Symantec IM Manager LoggedInUsers.lgx definition file multiple SQL injections attempt"; flow:to\_server,established; content:"/IMManager/rdpageimlogic.aspx?"; fast\_pattern:only; http\_uri; pcre:"/\x2FIMManager\x2Frdpageimlogic\x2Easpx\x3F.\*?(loginTimeStamp|dbo|dateDiffParam|whereClause)\x3D[^\x26]\*?(\x3B|\x23|\x2D{2})/sU"; metadata:policy security-ips drop, service http; reference:bugtraq,44299; reference:cve,2010-0112; classtype:web-application-attack; sid:18955; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP BadBlue ext.dll buffer overflow attempt"; flow:to\_server,established; content:"ext.dll"; http\_uri; content:"mfcisapicommand="; nocase; isdataat:250,relative; pcre:"/mfcisapicommand=[^&\r\n\x3b]{250}/smi"; metadata:service http; reference:bugtraq,12673; reference:cve,2005-0595; classtype:attempted-admin; sid:3816; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 8300 (msg:"SERVER-WEBAPP Novell Groupwise Messenger parameter memory corruption attempt"; flow:to\_server,established; content:"type=9"; fast\_pattern:only; content:"POST /createsearch HTTP/1.0"; depth:27; content:"|0D 0A 0D 0A|"; within:4; content:"cmd=0"; distance:0; nocase; content:"val=0"; nocase; metadata:policy security-ips drop, service http; reference:url,aluigi.altervista.org/adv/nmma\_3-adv.txt; classtype:attempted-admin; sid:23384; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Sabdrimer remote file include in advanced1.php pluginpath[0]"; flow:to\_server,established; content:"pluginpath[0]="; fast\_pattern:only; http\_uri; pcre:"/\x2Fadvanced1\.php\?[^\r\n]\*?pluginpath\x5B0\x5D=(https?|ftps?)/Ui"; metadata:policy security-ips drop, service http; reference:bugtraq,18907; reference:cve,2006-3520; classtype:web-application-attack; sid:20732; rev:6;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP OpenView Network Node Manager ovet\_demandpoll.exe format string execution attempt"; flow:to\_server,established; content:"POST"; nocase; http\_method; content:"/OvCgi/webappmon.exe"; fast\_pattern; nocase; http\_uri; content:"sel="; http\_client\_body; pcre:"/^[^\x26]\*?\x25/R"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,40065; reference:cve,2010-1550; classtype:attempted-admin; sid:18795; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP webspeed access"; flow:to\_server,established; content:"/wsisa.dll/WService="; fast\_pattern; nocase; http\_uri; content:"WSMadmin"; nocase; metadata:service http; reference:bugtraq,969; reference:cve,2000-0127; reference:nessus,10304; classtype:attempted-user; sid:805; rev:20;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP InteractiveQuery.jsp access"; flow:to\_server,established; content:"/InteractiveQuery.jsp"; nocase; http\_uri; metadata:service http; reference:bugtraq,8938; reference:cve,2003-0624; classtype:web-application-activity; sid:2395; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 25 (msg:"SERVER-WEBAPP Netop Remote Control dws file buffer overflow attempt"; flow:to\_server,established; flowbits:isset,file.dws; file\_data; pcre:"/[^\x0d\x0a]{520}/smi"; metadata:service smtp; reference:bugtraq,47631; reference:url,osvdb.org/72291; classtype:attempted-user; sid:24707; rev:1;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP Openview NNM cdpView.ovpl Unix command execution attempt"; flow:to\_server,established; content:"/cdpView.ovpl"; nocase; http\_uri; content:"cdpnode="; nocase; http\_uri; pcre:"/cdpView\.ovpl[^\r\n]\*cdpnode=[^\r\n]\*[\x2c\x24\x7c\x3b\x22\x26\x3c\x3f]/Usmi"; metadata:service http; reference:bugtraq,14662; reference:cve,2005-2773; classtype:web-application-attack; sid:8089; rev:12;)

#alert tcp $EXTERNAL\_NET $FILE\_DATA\_PORTS -> $HOME\_NET any (msg:"SERVER-WEBAPP socket\_connect buffer overflow attempt"; flow:to\_client,established; file\_data; content:"$padd = str\_repeat(|22|A|22|, 196)"; content:"$evil = $padd.$payload"; distance:0; fast\_pattern; content:"socket\_create(AF\_UNIX, SOCK\_STREAM, 1)"; metadata:service http, service imap, service pop3; reference:bugtraq,49241; reference:cve,2011-1938; classtype:attempted-user; sid:24194; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP apache source.asp file access"; flow:to\_server,established; content:"/site/eg/source.asp"; nocase; http\_uri; metadata:service http; reference:bugtraq,1457; reference:cve,2000-0628; reference:nessus,10480; classtype:attempted-recon; sid:1110; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Domino domlog.nsf access"; flow:to\_server,established; content:"/domlog.nsf"; nocase; http\_uri; metadata:service http; reference:nessus,10629; classtype:attempted-recon; sid:1152; rev:13;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP OpenView Network Node Manager cookie buffer overflow attempt"; flow:to\_server,established; content:"/OVCgi/jovw.exe"; fast\_pattern:only; http\_uri; pcre:"/(OvJavaScript|OvTitleFrame|OvHelpWindow|OvMap|OvSession|OvJavaLocale|OvOSLocale|OvLogin|OvDebug|OvDeveloper|OvTreeControl|OvJavaScript|OvProduct|OvPort|OvLocale|OvWebSession)\s\*\x3D[^\x3B\x2C]{1024}/iC"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,42154; reference:cve,2010-2709; classtype:attempted-user; sid:18908; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP download.cgi access"; flow:to\_server,established; content:"/download.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,4579; reference:cve,1999-1377; reference:nessus,11748; classtype:web-application-activity; sid:2201; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Venom Board SQL injection attempt"; flow:to\_server,established; content:"venomboard|2F|forum"; fast\_pattern; nocase; http\_uri; content:"post.php3"; nocase; http\_uri; content:"root="; nocase; http\_uri; pcre:"/\x2Fpost\.php3?[^\r\n]\*?root=[^\r\n\x26]\*?union[^\r\n\x26]\*select/Ui"; metadata:service http; reference:bugtraq,16176; reference:cve,2006-0160; classtype:web-application-activity; sid:20625; rev:4;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP OpenView Network Node Manager cookie buffer overflow attempt"; flow:to\_server,established; content:"/OVCgi/ovsessioninfo.exe"; fast\_pattern:only; http\_uri; pcre:"/(OvJavaScript|OvTitleFrame|OvHelpWindow|OvMap|OvSession|OvJavaLocale|OvOSLocale|OvLogin|OvDebug|OvDeveloper|OvTreeControl|OvJavaScript|OvProduct|OvPort|OvLocale|OvWebSession)\s\*\x3D[^\x3B\x2C]{1024}/iC"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,42154; reference:cve,2010-2709; classtype:attempted-user; sid:18918; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Netscape admin passwd"; flow:to\_server,established; content:"/admin-serv/config/admpw"; nocase; http\_uri; metadata:service http; reference:bugtraq,1579; reference:nessus,10468; classtype:web-application-attack; sid:1103; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Cisco IOS HTTP service HTML injection attempt"; flow:to\_server,established; content:"href|3D 22 2E 2F 2E 2E 2F 2E 2F 2F 2E 2E 2F 2E 2E 2F 2E 2E 2F 2E 2E 2F 2E 2E 2F 2F|"; fast\_pattern:only; metadata:service http; reference:bugtraq,15602; reference:cve,2005-3921; classtype:attempted-dos; sid:17287; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP System variable directory traversal attempt - %USERNAME%"; flow:to\_server,established; content:"%USERNAME%"; fast\_pattern:only; http\_uri; metadata:service http; classtype:attempted-recon; sid:21834; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP guestserver.cgi access"; flow:to\_server,established; content:"/guestserver.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,4579; reference:cve,2001-0180; reference:nessus,11748; classtype:web-application-activity; sid:2211; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP GrapAgenda remote file include in index.php page"; flow:to\_server,established; content:"index.php"; fast\_pattern:only; http\_uri; content:"page"; nocase; pcre:"/page=(https?|ftps?)/i"; metadata:service http; reference:bugtraq,19857; reference:cve,2006-4610; classtype:web-application-attack; sid:20654; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP PHPBB viewforum.php access"; flow:to\_server,established; content:"/viewforum.php"; nocase; http\_uri; content:"topic\_id="; nocase; http\_uri; metadata:service http; reference:bugtraq,9865; reference:bugtraq,9866; reference:nessus,12093; classtype:web-application-activity; sid:2566; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Advanced Poll admin\_templates.php access"; flow:to\_server,established; content:"/admin\_templates.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,8890; reference:nessus,11487; classtype:web-application-activity; sid:2298; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP OpenView Network Node Manager nnmRptConfig.exe Template format string code execution attempt"; flow:to\_server,established; content:"/OvCgi/nnmRptConfig.exe"; nocase; http\_uri; content:"Action=Create"; nocase; pcre:"/Template\x3D[^\x26]\*?\x25\d\*n/i"; metadata:policy security-ips drop, service http; reference:bugtraq,45762; reference:cve,2011-0270; classtype:attempted-user; sid:18930; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Vmist Downstat remote file include in modes.php art"; flow:to\_server,established; content:"downstat"; nocase; http\_uri; content:"modes.php"; nocase; http\_uri; content:"art="; nocase; http\_uri; pcre:"/\x2Fmodes\.php\x3F[^\r\n]\*?art\x3Dhttp\x3A\x2F/Ui"; metadata:service http; reference:bugtraq,20007; reference:cve,2006-4827; classtype:web-application-activity; sid:20817; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP pagelog.cgi access"; flow:to\_server,established; content:"/pagelog.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,1864; reference:cve,2000-0940; reference:nessus,10591; classtype:web-application-activity; sid:1658; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP AuthChangeUrl access"; flow:to\_server,established; content:"\_AuthChangeUrl?"; nocase; http\_uri; metadata:service http; reference:bugtraq,2110; reference:cve,1999-0407; classtype:attempted-recon; sid:1126; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP agora.cgi attempt"; flow:to\_server,established; content:"/store/agora.cgi?cart\_id=<SCRIPT>"; nocase; http\_uri; metadata:service http; reference:bugtraq,3702; reference:bugtraq,3976; reference:cve,2001-1199; reference:cve,2002-0215; reference:nessus,10836; classtype:web-application-attack; sid:1534; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Boite de News remote file include in inc.php url\_index"; flow:to\_server,established; content:"url\_index="; fast\_pattern:only; http\_uri; pcre:"/\x2F(inc2?|index)\.php?[^\r\n]\*?url\_index=(https?|ftps?)/Ui"; metadata:service http; reference:bugtraq,19440; reference:cve,2006-4123; classtype:web-application-activity; sid:20633; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP friends.php access"; flow:to\_server,established; content:"/friends.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,9088; classtype:web-application-activity; sid:2286; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cacti graph\_image SQL injection attempt"; flow:to\_server,established; content:"graph\_image.php"; nocase; http\_uri; pcre:"/local\_graph\_id=(?!(\d+|)([\x26\s]|$))/smi"; metadata:service http; reference:bugtraq,14128; reference:bugtraq,14129; reference:cve,2005-2148; classtype:web-application-attack; sid:8714; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 7510 (msg:"SERVER-WEBAPP HP OpenView Network Node Manager server name exploit attempt"; flow:to\_server,established; content:"/topology/pathView"; http\_uri; content:"|02 65 6E 74 00 00 73 71 00 7E 00 00 00 00 00 02|"; fast\_pattern:only; metadata:policy security-ips drop, service http; reference:bugtraq,45762; reference:cve,2011-0263; reference:url,h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02670501; classtype:attempted-admin; sid:18993; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP OpenView Network Node Manager webappmon.exe host header buffer overflow attempt"; flow:to\_server, established; content:"webappmon.exe"; nocase; http\_uri; content:"Host|3A|"; nocase; http\_header; content:!"|0A|"; within:120; http\_header; metadata:policy security-ips drop, service http; reference:bugtraq,37341; reference:cve,2009-4177; reference:url,h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01950877; classtype:attempted-admin; sid:20013; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP faqmanager.cgi arbitrary file access attempt"; flow:to\_server,established; content:"/faqmanager.cgi?toc="; http\_uri; content:"|00|"; nocase; http\_uri; metadata:service http; reference:bugtraq,3810; reference:nessus,10837; classtype:web-application-attack; sid:1590; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP campas attempt"; flow:to\_server,established; content:"/campas?|0A|"; nocase; http\_uri; metadata:service http; reference:bugtraq,1975; reference:cve,1999-0146; reference:nessus,10035; classtype:web-application-attack; sid:1652; rev:20;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP day5datacopier.cgi access"; flow:to\_server,established; content:"/day5datacopier.cgi"; nocase; http\_uri; metadata:service http; reference:cve,1999-1232; classtype:attempted-recon; sid:863; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Messagerie supp\_membre.php access"; flow:to\_server,established; content:"/supp\_membre.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,4635; classtype:web-application-activity; sid:1745; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Photopost PHP Pro showphoto.php access"; flow:to\_server,established; content:"/showphoto.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,9557; classtype:web-application-activity; sid:2372; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP mylog.phtml access"; flow:to\_server,established; content:"/mylog.phtml"; nocase; http\_uri; metadata:service http; reference:bugtraq,713; reference:cve,1999-0068; reference:cve,1999-0346; classtype:attempted-recon; sid:1120; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP admin.pl access"; flow:to\_server,established; content:"/admin.pl"; nocase; http\_uri; metadata:service http; reference:bugtraq,3839; reference:cve,2002-1748; reference:url,online.securityfocus.com/archive/1/249355; classtype:attempted-recon; sid:879; rev:18;)

#alert tcp $EXTERNAL\_NET $HTTP\_PORTS -> $HOME\_NET any (msg:"SERVER-WEBAPP Apple iChat url format string exploit attempt"; flow:to\_client,established; file\_data; content:"href="; content:"aim:GoChat"; fast\_pattern:only; pcre:"/aim\x3AGoChat[^\n]\*?\x25(\d+\x24)?(\d+)?[nxXcsd]/i"; metadata:service http; reference:bugtraq,22146; reference:cve,2007-0021; classtype:attempted-user; sid:23407; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP guestbook.cgi access"; flow:to\_server,established; content:"/guestbook.cgi"; nocase; http\_uri; metadata:service http; reference:cve,1999-0237; reference:nessus,10098; classtype:web-application-activity; sid:1597; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP view\_broadcast.cgi access"; flow:to\_server,established; content:"/view\_broadcast.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,8257; reference:cve,2003-0422; classtype:web-application-activity; sid:2387; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP horde help module arbitrary command execution attempt"; flow:to\_server,established; content:"/services/help/"; http\_uri; pcre:"/[\?\x20\x3b\x26]module=[a-zA-Z0-9]\*[\x3b\x21\x7c\x3c\x3e\x60\x5c\x2f]/Ui"; metadata:policy security-ips drop, service http; reference:bugtraq,17292; reference:cve,2006-1491; classtype:web-application-attack; sid:6403; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP rwwwshell.pl access"; flow:to\_server,established; content:"/rwwwshell.pl"; nocase; http\_uri; metadata:service http; reference:url,www.itsecurity.com/papers/p37.htm; classtype:attempted-recon; sid:834; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cross site scripting HTML Image tag set to javascript attempt"; flow:to\_server,established; content:"img src=javascript"; nocase; http\_uri; metadata:service http; reference:bugtraq,4858; reference:cve,2002-0902; classtype:web-application-attack; sid:1667; rev:13;)

#alert tcp $HOME\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP iPlanet Webserver command injection attempt"; flow:to\_server,established; content:"https-admserv/bin/perl/importInfo"; fast\_pattern:only; pcre:"/https-admserv\x2fbin\x2fperl\x2fimportInfo\x3F.\*?dir=[^\x26]\*?[\x7c]/iU"; metadata:service http; reference:bugtraq,6202; reference:cve,2002-1315; classtype:web-application-attack; sid:21358; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP forum\_details.php access"; flow:to\_server,established; content:"forum\_details.php"; http\_uri; metadata:service http; reference:bugtraq,7933; reference:nessus,11760; classtype:web-application-attack; sid:2227; rev:8;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP search.dll access"; flow:to\_server,established; content:"/search.dll"; http\_uri; metadata:service http; reference:bugtraq,1684; reference:cve,2000-0835; reference:nessus,10514; classtype:web-application-activity; sid:1767; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cgiWebupdate.exe access"; flow:to\_server,established; content:"/cgiWebupdate.exe"; nocase; http\_uri; metadata:service http; reference:bugtraq,3216; reference:cve,2001-1150; reference:nessus,11722; classtype:web-application-activity; sid:2237; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP CISCO VoIP Portinformation access"; flow:to\_server,established; content:"/PortInformation"; http\_uri; metadata:service http; reference:bugtraq,4798; reference:cve,2002-0882; classtype:web-application-activity; sid:3467; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Phorum code access"; flow:to\_server,established; content:"/code.php3"; nocase; http\_uri; metadata:service http; classtype:attempted-recon; sid:1197; rev:17;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 7510 (msg:"SERVER-WEBAPP HP OpenView Network Node Manager HTTP handling buffer overflow attempt"; flow:to\_server,established; content:"/topology/home"; fast\_pattern:only; http\_uri; urilen:>184; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,28569; reference:cve,2008-1697; classtype:attempted-admin; sid:13715; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP piranha passwd.php3 access"; flow:to\_server,established; content:"/passwd.php3"; http\_uri; metadata:service http; reference:bugtraq,1149; reference:cve,2000-0322; classtype:attempted-recon; sid:1161; rev:16;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP IBM System Storage DS storage manager profiler XSS attempt"; flow:established,to\_server; content:"/SoftwareRegistration.do"; fast\_pattern:only; http\_uri; pcre:"/SoftwareRegistration\.do.\*?updateRegn=[^\x26\r\n]+(script|onclick|onload|onmouseover|html|[\x22\x27\x3c\x3e\x28\x29])/Ui"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,54112; reference:cve,2012-2172; reference:url,www.exploit-db.com/exploits/19321/; classtype:web-application-attack; sid:23466; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP PHP-Wiki cross site scripting attempt"; flow:to\_server,established; content:"/modules.php?"; http\_uri; content:"name=Wiki"; fast\_pattern; nocase; http\_uri; content:"<script"; nocase; http\_uri; metadata:service http; reference:bugtraq,5254; reference:cve,2002-1070; classtype:web-application-attack; sid:1834; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP shoutbox.php access"; flow:to\_server,established; content:"/shoutbox.php"; fast\_pattern; nocase; http\_uri; content:"conf="; nocase; http\_uri; metadata:service http; reference:nessus,11668; classtype:web-application-activity; sid:2142; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP /~ftp access"; flow:to\_server,established; content:"/~ftp"; nocase; http\_uri; metadata:service http; classtype:attempted-recon; sid:1662; rev:11;)

#alert tcp $EXTERNAL\_NET $HTTP\_PORTS -> $HOME\_NET any (msg:"SERVER-WEBAPP Oracle Java Runtime CMM readMabCurveData buffer overflow attempt"; flow:to\_client, established; file\_data; content:"curv|00 00 00 00|"; byte\_test:4,>,0x1015,0,relative; metadata:policy security-ips drop, service http; reference:bugtraq,39069; reference:cve,2010-0838; classtype:attempted-user; sid:18803; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP apache directory disclosure attempt"; flow:to\_server,established; content:"////////"; fast\_pattern:only; content:"////////"; http\_raw\_uri; metadata:service http; reference:bugtraq,2503; reference:cve,2001-0925; classtype:attempted-dos; sid:1156; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP htgrep access"; flow:to\_server,established; content:"/htgrep"; http\_uri; metadata:service http; reference:cve,2000-0832; reference:nessus,10495; classtype:web-application-activity; sid:1207; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP bb-replog.sh access"; flow:to\_server,established; content:"/bb-replog.sh"; nocase; http\_uri; metadata:service http; reference:bugtraq,142; reference:cve,1999-1462; classtype:attempted-recon; sid:1462; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS 443 (msg:"SERVER-WEBAPP SSLv2 Client\_Hello with pad Challenge Length overflow attempt"; flow:to\_server,established; ssl\_version:sslv2; ssl\_state:client\_hello; content:"|01 00 02|"; depth:3; offset:2; byte\_test:2,>,32,9; metadata:service ssl; classtype:attempted-admin; sid:2657; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP sendform.cgi access"; flow:to\_server,established; content:"/sendform.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,5286; reference:cve,2002-0710; reference:url,www.scn.org/help/sendform.txt; classtype:attempted-recon; sid:890; rev:20;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP visadmin.exe access"; flow:to\_server,established; content:"/visadmin.exe"; nocase; http\_uri; metadata:service http; reference:bugtraq,1808; reference:cve,1999-0970; reference:nessus,10295; classtype:attempted-recon; sid:867; rev:20;)

#alert tcp $EXTERNAL\_NET $FILE\_DATA\_PORTS -> $HOME\_NET any (msg:"SERVER-WEBAPP PHP use-after-free in substr\_replace attempt"; flow:to\_client,established; file\_data; content:"substr\_replace("; fast\_pattern:only; content:"<?"; pcre:"/substr\_replace\((\s\*\$\w+\s\*,\s\*){3,}.\*?\)\x3b/smi"; metadata:service http, service imap, service pop3; reference:cve,2011-1148; classtype:misc-activity; sid:23791; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP active.log access"; flow:to\_server,established; content:"/active.log"; nocase; http\_uri; metadata:service http; reference:bugtraq,1497; reference:cve,2000-0642; reference:nessus,10470; classtype:web-application-activity; sid:1851; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Netscape Enterprise Server directory view"; flow:to\_server,established; content:"?wp-ver-diff"; nocase; http\_uri; metadata:service http; reference:bugtraq,1063; reference:cve,2000-0236; classtype:attempted-recon; sid:1186; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET [8030,8028,8008,8010] (msg:"SERVER-WEBAPP Novell eDirectory SOAP Accept Language header overflow attempt"; flow:to\_server,established; content:"/SOAP"; fast\_pattern; nocase; http\_uri; content:"Accept-Language|3A|"; nocase; pcre:"/^Accept\x2dLanguage\x3a\s\*(\w{1,36}\s\*(\x2e|\x2d|\x3b|\x3d|\x2c)\s\*)\*[^\x2d\x3b\x2c\x3d\n]{37}/smi"; metadata:policy security-ips drop, service http; reference:cve,2008-4479; classtype:attempted-user; sid:14989; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP webdriver access"; flow:to\_server,established; content:"/webdriver"; nocase; http\_uri; metadata:service http; reference:bugtraq,2166; reference:nessus,10592; classtype:attempted-recon; sid:808; rev:19;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP AT-admin.cgi access"; flow:to\_server,established; content:"/AT-admin.cgi"; nocase; http\_uri; metadata:service http; reference:cve,1999-1072; classtype:attempted-recon; sid:845; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP WinProxy overly long host header buffer overflow attempt"; flow:to\_server,established; content:"Host|3A|"; nocase; http\_header; isdataat:100,relative; pcre:"/^Host\x3A\s+[A-Z\d\x5F\x2E\x2E]\*\x3A[^\r\n]{100}/smiH"; metadata:service http; reference:bugtraq,16147; reference:cve,2005-4085; reference:url,www.bluecoat.com/support/knowledge/advisory\_host\_header\_stack\_overflow.html; classtype:attempted-admin; sid:5997; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP handler attempt"; flow:to\_server,established; content:"/handler"; http\_uri; content:"|7C|"; nocase; http\_uri; metadata:service http; reference:bugtraq,380; reference:cve,1999-0148; reference:nessus,10100; classtype:web-application-attack; sid:1613; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP agora.cgi access"; flow:to\_server,established; content:"/store/agora.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,3702; reference:bugtraq,3976; reference:cve,2001-1199; reference:cve,2002-0215; reference:nessus,10836; classtype:web-application-activity; sid:1406; rev:21;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP adcycle access"; flow:to\_server,established; content:"/adcycle"; nocase; http\_uri; metadata:service http; reference:bugtraq,3741; reference:cve,2001-1226; classtype:web-application-activity; sid:1721; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP System variable directory traversal attempt - %PROGRAMFILES%"; flow:to\_server,established; content:"%PROGRAMFILES%"; fast\_pattern:only; http\_uri; metadata:service http; classtype:attempted-recon; sid:21827; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP /~nobody access"; flow:to\_server,established; content:"/~nobody"; http\_uri; metadata:service http; reference:nessus,10484; classtype:web-application-attack; sid:1489; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Oracle reports CGI access"; flow:to\_server,established; content:"/rwcgi60"; http\_uri; content:"setauth="; metadata:service http; reference:bugtraq,4848; reference:cve,2002-0947; classtype:web-application-activity; sid:1805; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Oracle iSQLPlus username overflow attempt"; flow:to\_server,established; content:"/isqlplus"; nocase; http\_uri; pcre:"/username=[^&\x3b\r\n]{255}/si"; metadata:service http; reference:bugtraq,10871; reference:url,www.nextgenss.com/advisories/ora-isqlplus.txt; classtype:web-application-attack; sid:2702; rev:9;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP Intelligent Management Center database credentials information disclosure attempt - 3"; flow:to\_server,established; content:"/imc/reportscript/oracle/deploypara.properties"; nocase; http\_uri; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,40298; reference:url,secunia.com/advisories/39891; classtype:attempted-user; sid:17159; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ttawebtop.cgi access"; flow:to\_server,established; content:"/ttawebtop.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,2890; reference:cve,2001-0805; reference:nessus,10696; classtype:attempted-recon; sid:1480; rev:19;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP SalesLogix Eviewer access"; flow:to\_server,established; content:"/slxweb.dll"; nocase; http\_uri; metadata:service http; reference:bugtraq,1078; reference:bugtraq,1089; reference:cve,2000-0278; reference:cve,2000-0289; classtype:web-application-activity; sid:1588; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP openview network node manager ovlogin.exe buffer overflow - password parameter"; flow:to\_server,established; content:"/ovlogin.exe"; nocase; http\_uri; content:"password="; nocase; http\_client\_body; pcre:"/password=[^\x26\r\n]{128}/Psmi"; metadata:policy security-ips drop, service http; reference:bugtraq,37330; reference:cve,2009-4176; reference:url,h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01950877; classtype:attempted-admin; sid:18481; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP OpenView NNM ovwebsnmpsrv.exe command line argument buffer overflow attempt"; flow:to\_server,established; content:"/OvCgi/jovgraph.exe"; nocase; http\_uri; content:"arg="; distance:0; nocase; isdataat:1024,relative; content:!"|0D|"; within:1024; metadata:service http; reference:bugtraq,40873; reference:bugtraq,45762; reference:cve,2010-1964; reference:cve,2011-0261; classtype:attempted-user; sid:18998; rev:4;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 5555 (msg:"SERVER-WEBAPP HP OpenView Storage Data Protector directory traversal attempt"; flow:to\_server,established; content:"|2E 00 5C 00 2E 00 2E 00 5C 00|"; content:"|32 00 00 00|"; depth:4; offset:6; content:"1|00|7|00 00 00|"; distance:0; metadata:policy balanced-ips drop, policy security-ips drop; reference:cve,2011-1736; classtype:attempted-recon; sid:20531; rev:2;)

#alert tcp $EXTERNAL\_NET 70 -> $HOME\_NET any (msg:"SERVER-WEBAPP Squid Gopher protocol handling buffer overflow attempt"; flow:to\_client,established; content:"|30 41 73 09 30 2F 61 61 61 61 61 61 61 61 61 61 61 61 61 61|"; fast\_pattern:only; metadata:policy security-ips drop; reference:bugtraq,12276; reference:cve,2005-0094; classtype:attempted-dos; sid:17432; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS any (msg:"SERVER-WEBAPP IBM WebSphere j\_security\_check overflow attempt"; flow:to\_server,established; content:"POST"; content:"/admin/j\_security\_check"; nocase; isdataat:256,relative; pcre:"/j\_(username|password)=[^\n&]{256,}/smi"; metadata:service http; reference:bugtraq,13853; reference:cve,2005-1872; classtype:attempted-admin; sid:3693; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Oracle Java Web Server Webdav Stack Buffer Overflow attempt"; flow:to\_server,established; content:"OPTIONS"; depth:7; nocase; isdataat:200,relative; pcre:"/^OPTIONS\s+[^\s]{200}/smi"; metadata:policy security-ips drop, service http; reference:bugtraq,37874; reference:cve,2010-0361; classtype:attempted-admin; sid:18611; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP architext\_query.pl access"; flow:to\_server,established; content:"/ews/architext\_query.pl"; nocase; http\_uri; metadata:service http; reference:bugtraq,2248; reference:cve,1999-0279; reference:nessus,10064; reference:url,www2.fedcirc.gov/alerts/advisories/1998/txt/fedcirc.98.03.txt; classtype:attempted-recon; sid:1173; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP parse\_xml.cgi access"; flow:to\_server,established; content:"/parse\_xml.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,6954; reference:bugtraq,6955; reference:bugtraq,6956; reference:bugtraq,6958; reference:cve,2003-0050; reference:cve,2003-0051; reference:cve,2003-0052; reference:cve,2003-0053; reference:cve,2003-0423; classtype:web-application-activity; sid:2085; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS 8000:8001 (msg:"SERVER-WEBAPP Apple Quicktime User-Agent buffer overflow attempt"; flow:to\_server,established; content:"User-Agent|3A|"; nocase; isdataat:244,relative; pcre:"/^User-Agent\x3a[^\n]{244,255}/smi"; reference:bugtraq,9735; reference:cve,2004-0169; classtype:web-application-attack; sid:2442; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS 554 (msg:"SERVER-WEBAPP RealNetworks RealSystem Server DESCRIBE buffer overflow attempt"; flow:to\_server,established; content:"DESCRIBE"; nocase; content:"../"; distance:1; pcre:"/^DESCRIBE\s[^\n]{300}/smi"; reference:bugtraq,8476; reference:cve,2003-0725; reference:nessus,11642; reference:url,www.service.real.com/help/faq/security/rootexploit091103.html; classtype:web-application-attack; sid:2411; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP .htaccess access"; flow:to\_server,established; content:".htaccess"; nocase; http\_uri; metadata:service http; classtype:attempted-recon; sid:1129; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP LANDesk Thinkmanagement Suite ServerSetup Directory Transversal attempt"; flow:to\_server,established; content:"POST"; http\_method; content:"/landesk/managementsuite/core/core.anonymous/ServerSetup.asmx"; fast\_pattern:only; http\_uri; content:"<RunAMTCommand"; nocase; http\_client\_body; content:"-PutUpdateFileCore"; distance:0; nocase; http\_client\_body; metadata:service http; reference:bugtraq,52023; reference:cve,2012-1195; classtype:attempted-user; sid:23258; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP user\_update\_admin.pl access"; flow:to\_server,established; content:"/user\_update\_admin.pl"; nocase; http\_uri; metadata:service http; reference:bugtraq,1486; reference:cve,2000-0627; classtype:attempted-recon; sid:1457; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Oracle iSQL Plus cross site scripting attempt"; flow:to\_server,established; content:"/isqlplus"; nocase; http\_uri; content:"username="; nocase; http\_uri; pcre:"/username[\x3d\x3f][^\n\x26]\*\x3c[^\n\x26]+\x3e/Ui"; metadata:service http; reference:bugtraq,9484; reference:cve,2004-2115; classtype:web-application-attack; sid:11194; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP .FBCIndex access"; flow:to\_server,established; content:"/.FBCIndex"; http\_uri; metadata:service http; reference:url,www.securiteam.com/securitynews/5LP0O005FS.html; classtype:web-application-activity; sid:1770; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Macromedia JRun 4 mod\_jrun buffer overflow attempt"; flow:to\_server,established; content:".jsp"; http\_uri; content:"HOST"; nocase; isdataat:1000,relative; pcre:"/^HOST\s\*\x3a\s\*[^\x0a]{1000}/mi"; metadata:policy security-ips drop, service http; reference:bugtraq,11245; reference:cve,2004-0646; classtype:attempted-user; sid:15978; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP setpasswd.cgi access"; flow:to\_server,established; content:"/setpasswd.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,2212; reference:bugtraq,4579; reference:cve,2001-0133; reference:nessus,11748; classtype:web-application-activity; sid:2219; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP System variable in URI attempt - %USERDOMAIN%"; flow:to\_server,established; content:"%USERDOMAIN%"; fast\_pattern:only; http\_uri; metadata:service http; classtype:attempted-recon; sid:21844; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP phpBook mail command execution attempt"; flow:established, to\_server; content:"/lwc/index.php"; nocase; http\_uri; pcre:"/index\.php\?.\*mail=[^\r\n\x26]\*\x3C\x3F/smiU"; metadata:policy security-ips drop, service http; reference:bugtraq,16106; reference:cve,2006-0075; classtype:attempted-admin; sid:18334; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP dcforum.cgi access"; flow:to\_server,established; content:"/dcforum.cgi"; http\_uri; metadata:service http; reference:bugtraq,2728; reference:cve,2001-0527; reference:nessus,10583; classtype:attempted-recon; sid:818; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP upload.pl access"; flow:to\_server,established; content:"/upload.pl"; nocase; http\_uri; metadata:service http; classtype:attempted-recon; sid:891; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP global.inc access"; flow:to\_server,established; content:"/global.inc"; nocase; http\_uri; metadata:service http; reference:bugtraq,4612; reference:cve,2002-0614; classtype:web-application-attack; sid:1738; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP GestArtremote file include in aide.php3 aide"; flow:to\_server,established; content:"aide.php3"; fast\_pattern:only; http\_uri; content:"aide"; nocase; pcre:"/aide=(https?|ftps?)/i"; metadata:service http; reference:bugtraq,22825; reference:cve,2006-5612; classtype:web-application-attack; sid:20656; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP PhpGedView PGV functions.php base directory manipulation attempt"; flow:to\_server,established; content:"/functions.php"; nocase; http\_uri; content:"PGV\_BASE\_DIRECTORY"; fast\_pattern:only; metadata:service http; reference:bugtraq,9368; reference:cve,2004-0030; classtype:web-application-attack; sid:2367; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 8090 (msg:"SERVER-WEBAPP TrackerCam User-Agent buffer overflow attempt"; flow:to\_server,established; content:"User-Agent|3A|"; nocase; isdataat:215,relative; pcre:"/^User-Agent\x3a[^\n]{216}/smi"; reference:bugtraq,12592; reference:cve,2005-0481; classtype:web-application-attack; sid:3546; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP SWEditServlet directory traversal attempt"; flow:to\_server,established; content:"/SWEditServlet"; http\_uri; content:"template=../../../"; metadata:service http; reference:bugtraq,2868; reference:cve,2001-0555; classtype:attempted-user; sid:1241; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Symantec IM Manager Systemdashboard cross site scripting attempt"; flow:to\_server,established; content:"/IMManager/Admin/IMAdminSystemDashboard.asp"; nocase; http\_uri; content:"refreshRateSetting="; distance:0; nocase; http\_uri; pcre:"/refreshRateSetting=[^\x26\s]\*[\x3e\x3d\x26]/Ui"; metadata:service http; reference:bugtraq,49739; reference:cve,2011-0552; reference:url,osvdb.org/75981; classtype:attempted-user; sid:21066; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP dcforum.cgi directory traversal attempt"; flow:to\_server,established; content:"/dcforum.cgi"; http\_uri; content:"forum=../.."; metadata:service http; reference:bugtraq,2611; reference:cve,2001-0436; reference:cve,2001-0437; reference:nessus,10583; classtype:web-application-attack; sid:1571; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP IBM WebSphere Expect header cross-site scripting"; flow:to\_server,established; content:"Expect|3A|"; nocase; http\_header; content:"<script>"; nocase; http\_header; pcre:"/^Expect\x3A[^\r\n]+<script>/smiH"; metadata:policy security-ips drop, service http; reference:bugtraq,26457; reference:cve,2007-5944; classtype:web-application-attack; sid:18742; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP BitKeeper arbitrary command attempt"; flow:to\_server,established; content:"/diffs/"; http\_uri; content:"'"; content:"|3B|"; distance:0; content:"'"; distance:1; metadata:service http; reference:bugtraq,6588; classtype:web-application-attack; sid:2068; rev:8;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP txt2html.cgi access"; flow:to\_server,established; content:"/txt2html.cgi"; nocase; http\_uri; metadata:service http; classtype:web-application-activity; sid:1304; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ezman.cgi access"; flow:to\_server,established; content:"/ezman.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,4068; reference:bugtraq,4579; reference:cve,2002-0263; reference:nessus,11748; classtype:web-application-activity; sid:2206; rev:16;)

#alert tcp $EXTERNAL\_NET $FILE\_DATA\_PORTS -> $HOME\_NET any (msg:"SERVER-WEBAPP ocPortal cms cross site request forgery attempt"; flow:to\_client,established; file\_data; content:"ocPortal/adminzone/index.php?page=admin\_ocf\_join&type=step2|22|"; fast\_pattern:8,20; nocase; pcre:"/<form[^>]\*?action\s\*=\s\*[\x22\x27][^\x22\x27]+ocPortal\/adminzone\/index\.php\?page=admin\_ocf\_join&type=step2[\x22\x27][^>]\*?>/ims"; metadata:policy security-ips drop, service http, service imap, service pop3; reference:url,yehg.net/lab/pr0js/advisories/%5Bocportal\_8x%5D\_csrf; classtype:attempted-admin; sid:23988; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP VirusWall FtpSaveCVP access"; flow:to\_server,established; content:"/FtpSaveCVP.dll"; nocase; http\_uri; metadata:service http; reference:bugtraq,2808; reference:cve,2001-0432; reference:nessus,10733; classtype:attempted-recon; sid:1235; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP Openview NNM connectedNodes.ovpl Unix command execution attempt"; flow:to\_server,established; content:"/connectedNodes.ovpl"; nocase; http\_uri; content:"node="; nocase; http\_uri; pcre:"/connectedNodes.\ovpl[^\r\n]\*node=[^\r\n]\*[\x2c\x24\x7c\x3b\x22\x26\x3c\x3f]/Usmi"; metadata:service http; reference:bugtraq,14662; reference:cve,2005-2773; classtype:web-application-attack; sid:8088; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 9090 (msg:"SERVER-WEBAPP Jive Software Openfire group-summary.jsp XSS attempt"; flow:to\_server,established; content:"/group-summary.jsp"; fast\_pattern:only; http\_uri; pcre:"/group-summary\.jsp\?.\*?=([^\x26]\*[\x22\x27\x3C\x3E\x28\x29\x3B]|script|src|location|document)/U"; metadata:policy security-ips drop, service http; reference:bugtraq,32935; reference:cve,2009-0496; classtype:web-application-attack; sid:20864; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 457 (msg:"SERVER-WEBAPP Netscape Unixware overflow"; flow:to\_server,established; content:"|EB|\_|9A FF FF FF FF 07 FF C3|^1|C0 89|F|9D|"; reference:bugtraq,908; reference:cve,1999-0744; classtype:attempted-recon; sid:1132; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP TankLogger SQL injection in showInfo.php livestock\_id attempt"; flow:to\_server,established; content:"showInfo.php"; fast\_pattern:only; http\_uri; content:"livestock\_id"; nocase; pcre:"/livestock\_id=[^\r\n\x26]\*?([\x22\x27]|%2[27])/i"; metadata:service http; reference:bugtraq,16228; reference:cve,2006-0209; classtype:web-application-attack; sid:20642; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP IBM Lotus Domino Web Server Accept-Language header buffer overflow attempt"; flow:to\_server,established; content:"Accept-Language|3A|"; nocase; isdataat:110,relative; pcre:"/^Accept-Language\x3A[^\n]{110}/smi"; content:".nsf?"; nocase; http\_uri; metadata:service http; reference:bugtraq,29310; reference:cve,2008-2240; classtype:attempted-admin; sid:13819; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Amaya templates sendtemp.pl access"; flow:to\_server,established; content:"/sendtemp.pl"; nocase; http\_uri; metadata:service http; reference:bugtraq,2504; reference:cve,2001-0272; classtype:web-application-activity; sid:1702; rev:15;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP OpenView Network Node Manager cookie buffer overflow attempt"; flow:to\_server,established; content:"/OVCgi/OpenView.exe"; fast\_pattern:only; http\_uri; pcre:"/(OvJavaScript|OvTitleFrame|OvHelpWindow|OvMap|OvSession|OvJavaLocale|OvOSLocale|OvLogin|OvDebug|OvDeveloper|OvTreeControl|OvJavaScript|OvProduct|OvPort|OvLocale|OvWebSession)\s\*\x3D[^\x3B\x2C]{1024}/iC"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,42154; reference:cve,2010-2709; classtype:attempted-user; sid:18913; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Novell ZENworks patch management SQL injection attempt"; flow:to\_server, established; content:"/packages/default.asp?"; nocase; http\_uri; pcre:"/sort\x3d[^\s]\*\x3b+/Ui"; metadata:policy security-ips drop, service http; reference:bugtraq,15220; reference:cve,2005-3315; classtype:web-application-attack; sid:17449; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP calendar access"; flow:to\_server,established; content:"/calendar"; nocase; http\_uri; metadata:service http; classtype:attempted-recon; sid:882; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP intranet access"; flow:to\_server,established; content:"/intranet/"; nocase; http\_uri; metadata:service http; reference:nessus,11626; classtype:attempted-recon; sid:1214; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 9090 (msg:"SERVER-WEBAPP Oracle JavaServer default password login attempt"; flow:to\_server,established; content:"/servlet/admin"; content:"ae9f86d6beaa3f9ecb9a5b7e072a4138"; reference:nessus,10995; classtype:default-login-attempt; sid:1859; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP enter\_bug.cgi arbitrary command attempt"; flow:to\_server,established; content:"/enter\_bug.cgi"; fast\_pattern; nocase; http\_uri; content:"who="; content:"|3B|"; distance:0; metadata:service http; reference:bugtraq,3272; reference:cve,2002-0008; classtype:web-application-attack; sid:2054; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP DCShop access"; flow:to\_server,established; content:"/dcshop"; nocase; http\_uri; metadata:service http; reference:bugtraq,2889; reference:cve,2001-0821; classtype:web-application-activity; sid:1555; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP WhatsUpGold configuration access"; flow:to\_server,established; content:"/\_maincfgret.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,11043; reference:bugtraq,11109; reference:cve,2004-0798; classtype:web-application-activity; sid:11817; rev:12;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP OpenView Network Node Manager cookie buffer overflow attempt"; flow:to\_server,established; content:"/OVCgi/snmpviewer.exe"; fast\_pattern:only; http\_uri; pcre:"/(OvJavaScript|OvTitleFrame|OvHelpWindow|OvMap|OvSession|OvJavaLocale|OvOSLocale|OvLogin|OvDebug|OvDeveloper|OvTreeControl|OvJavaScript|OvProduct|OvPort|OvLocale|OvWebSession)\s\*\x3D[^\x3B\x2C]{1024}/iC"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,42154; reference:cve,2010-2709; classtype:attempted-user; sid:18923; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP mailnews.cgi access"; flow:to\_server,established; content:"/mailnews.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,2391; reference:cve,2001-0271; reference:nessus,10641; classtype:attempted-recon; sid:1471; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP phpBB privmsg.php access"; flow:to\_server,established; content:"/privmsg.php"; http\_uri; metadata:service http; reference:bugtraq,6634; classtype:web-application-activity; sid:2078; rev:8;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP zsh access"; flow:to\_server,established; content:"/zsh"; nocase; http\_uri; metadata:service http; reference:cve,1999-0509; reference:url,www.cert.org/advisories/CA-1996-11.html; classtype:attempted-recon; sid:1309; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP raSMP User-Agent XSS injection attempt"; flow:established, to\_server; content:"<script"; fast\_pattern:only; http\_header; content:"index.php"; nocase; http\_uri; content:"User-Agent|3A|"; nocase; http\_header; pcre:"/^User-Agent\x3A[^\r\n]\*?<script/imH"; metadata:service http; reference:bugtraq,16138; reference:cve,2006-0084; classtype:attempted-admin; sid:18466; rev:4;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Axis Storpoint CD access"; flow:to\_server,established; content:"/config/html/cnf\_gi.htm"; http\_uri; metadata:service http; reference:bugtraq,1025; reference:cve,2000-0191; reference:nessus,10023; classtype:web-application-activity; sid:1525; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Content-Length buffer overflow attempt"; flow:to\_server,established; content:"Content-Length|3A|"; nocase; http\_header; isdataat:100,relative; pcre:"/^Content-Length\x3A\s\*[^\r\n]{100}/smiH"; metadata:service http; reference:cve,2007-1260; reference:url,djeyl.net/w.php; classtype:attempted-admin; sid:10195; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP util.pl access"; flow:to\_server,established; content:"/util.pl"; nocase; http\_uri; metadata:service http; reference:bugtraq,9748; classtype:web-application-activity; sid:2407; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP NetGear router default password login attempt admin/password"; flow:to\_server,established; content:"Authorization|3A|"; nocase; http\_header; content:"YWRtaW46cGFzc3dvcmQ"; nocase; http\_header; pcre:"/^Authorization\x3a(\s\*|\s\*\r?\n\s+)Basic\s+YWRtaW46cGFzc3dvcmQ/smiH"; metadata:service http; reference:nessus,11737; classtype:default-login-attempt; sid:2230; rev:15;)

#alert tcp $EXTERNAL\_NET $FILE\_DATA\_PORTS -> $HOME\_NET any (msg:"SERVER-WEBAPP PHP truncated crypt function attempt"; flow:to\_client,established; file\_data; content:"crypt("; fast\_pattern:only; content:"<?"; pcre:"/((?P<m1>\$\w+)\s\*=\s\*(?P<q1>[\x22\x27])\s\*[^(?P=q1)]+(\\x80|\x80).\*?crypt\(\s\*(?P=m1)|crypt\(\s\*(?P<q2>[\x22\x27])\s\*[^(?P=q1)]+(\\x80|\x80))/smi"; metadata:policy security-ips drop, service http, service imap, service pop3; reference:cve,2012-2143; classtype:attempted-admin; sid:23895; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP server-info access"; flow:to\_server,established; content:"/server-info"; http\_uri; metadata:service http; reference:url,httpd.apache.org/docs/mod/mod\_info.html; classtype:web-application-activity; sid:1520; rev:12;)

alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP phpMyAdmin server\_sync.php backdoor access attempt"; flow:to\_server,established; content:"/phpMyAdmin/server\_sync.php"; fast\_pattern:only; http\_uri; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:url,phpmyadmin.net/home\_page/security/PMASA-2012-5.php; classtype:web-application-attack; sid:24256; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Tandberg VCS local file disclosure attempt"; flow:to\_server,established; content:"helppage.php"; fast\_pattern; nocase; http\_uri; content:"page="; nocase; http\_uri; content:".."; http\_uri; metadata:policy security-ips drop, service http; reference:cve,2009-4511; reference:url,secunia.com/advisories/39275/; classtype:web-application-attack; sid:16678; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP book.cgi arbitrary command execution attempt"; flow:to\_server,established; content:"/book.cgi"; fast\_pattern; nocase; http\_uri; content:"current=|7C|"; nocase; metadata:service http; reference:bugtraq,3178; reference:cve,2001-1114; reference:nessus,10721; classtype:web-application-attack; sid:1879; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP DCP-Portal remote file include lib script attempt"; flow:to\_server,established; content:"/library/lib.php"; fast\_pattern; nocase; http\_uri; content:"root="; http\_uri; metadata:service http; reference:bugtraq,6525; classtype:web-application-attack; sid:2342; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP maillist.pl access"; flow:to\_server,established; content:"/maillist.pl"; nocase; http\_uri; metadata:service http; classtype:attempted-recon; sid:828; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP cgiwrap access"; flow:to\_server,established; content:"/cgiwrap"; nocase; http\_uri; metadata:service http; reference:bugtraq,1238; reference:bugtraq,3084; reference:bugtraq,777; reference:cve,1999-1530; reference:cve,2000-0431; reference:cve,2001-0987; reference:nessus,10041; classtype:web-application-activity; sid:1543; rev:22;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP login.htm attempt"; flow:to\_server,established; content:"/login.htm?password="; nocase; http\_uri; metadata:service http; reference:bugtraq,665; reference:cve,1999-1533; classtype:web-application-activity; sid:1563; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP simplestguest.cgi access"; flow:to\_server,established; content:"/simplestguest.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,2106; reference:cve,2001-0022; classtype:web-application-activity; sid:1717; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP webcart-lite access"; flow:to\_server,established; content:"/webcart-lite/"; nocase; http\_uri; metadata:service http; reference:cve,1999-0610; reference:nessus,10298; classtype:web-application-activity; sid:1848; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP strings overflow"; flow:to\_server,established; content:"?STRENGUR"; nocase; http\_uri; metadata:service http; reference:bugtraq,1786; reference:cve,2000-0967; classtype:web-application-attack; sid:1086; rev:23;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP viralator.cgi access"; flow:to\_server,established; content:"/viralator.cgi"; http\_uri; metadata:service http; reference:bugtraq,3495; reference:cve,2001-0849; reference:nessus,11107; classtype:web-application-activity; sid:1996; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP PeopleSoft PeopleBooks psdoccgi access"; flow:to\_server,established; content:"/psdoccgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,9037; reference:bugtraq,9038; reference:cve,2003-0626; reference:cve,2003-0627; classtype:web-application-activity; sid:2277; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP IdeaBox cord.php file include"; flow:to\_server,established; content:"/index.php"; nocase; http\_uri; content:"ideaDir="; fast\_pattern:only; content:"cord.php"; nocase; metadata:service http; reference:bugtraq,7488; classtype:web-application-activity; sid:2353; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP System variable directory traversal attempt - %TEMP%"; flow:to\_server,established; content:"%TEMP%"; fast\_pattern:only; http\_uri; metadata:service http; classtype:attempted-recon; sid:21831; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP SIX webboard generate.cgi access"; flow:to\_server,established; content:"/generate.cgi"; http\_uri; metadata:service http; reference:bugtraq,3175; reference:cve,2001-1115; reference:nessus,10725; classtype:web-application-activity; sid:1495; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Advanced Poll admin\_templates\_misc.php access"; flow:to\_server,established; content:"/admin\_templates\_misc.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,8890; reference:nessus,11487; classtype:web-application-activity; sid:2297; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP System variable directory traversal attempt - %PSModulePath%"; flow:to\_server,established; content:"%PSModulePath%"; fast\_pattern:only; http\_uri; metadata:service http; classtype:attempted-recon; sid:21838; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Netscape Servers suite DOS"; flow:to\_server,established; content:"/dsgw/bin/search?context="; nocase; http\_uri; metadata:service http; reference:bugtraq,1868; reference:cve,2000-1025; classtype:web-application-attack; sid:1081; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Cyboards options\_form.php access"; flow:to\_server,established; content:"/options\_form.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,6597; classtype:web-application-activity; sid:2364; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP WoW Roster remote file include with hslist.php and conf.php"; flow:to\_server,established; content:"subdir="; fast\_pattern:only; http\_uri; pcre:"/\x2F(conf|hslist)\.php\?[^\r\n]\*?subdir=(https?|ftps?)/Ui"; metadata:service http; reference:cve,2006-3997; reference:cve,2006-3998; classtype:web-application-attack; sid:20728; rev:4;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Adobe RoboHelp rx SQL injection attempt"; flow:to\_server,established; content:"Top\_Unanswered\_Customer\_Questions.asp"; nocase; http\_uri; pcre:"/\x26r\d\x3d[^\x26\s]\*\x27/smi"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:cve,2008-2991; classtype:web-application-attack; sid:13929; rev:5;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Typo3 translations.php file include"; flow:to\_server,established; content:"/translations.php"; fast\_pattern; nocase; http\_uri; content:"ONLY="; nocase; metadata:service http; reference:bugtraq,6984; classtype:web-application-attack; sid:2358; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP JBoss JMXInvokerServlet access attempt"; flow:to\_server,established; content:"/invoker/JMXInvokerServlet"; fast\_pattern:only; http\_uri; metadata:service http; reference:cve,2007-1036; reference:url,docs.jboss.org/jbossas/6/Admin\_Console\_Guide/en-US/pdf/Admin\_Console\_Guide.pdf; classtype:attempted-admin; sid:24343; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP overflow.cgi access"; flow:to\_server,established; content:"/overflow.cgi"; http\_uri; metadata:service http; reference:bugtraq,6326; reference:cve,2002-1361; reference:nessus,11190; reference:url,www.cert.org/advisories/CA-2002-35.html; classtype:web-application-activity; sid:2052; rev:11;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP MyNewsGroups remote file include in layersmenu.inc.php myng\_root"; flow:to\_server,established; content:"layersmenu.inc.php"; fast\_pattern:only; http\_uri; content:"myng\_root"; nocase; pcre:"/myng\_root=(https?|ftps?)/i"; metadata:service http; reference:bugtraq,19258; reference:cve,2006-3966; classtype:web-application-attack; sid:20650; rev:6;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP JCE Joomla module vulnerable directory traversal or malicious file upload attempt"; flow:to\_server,established; content:"option=com\_jce"; fast\_pattern:only; http\_uri; content:"json"; nocase; http\_client\_body; pcre:"/json\s\*=\s\*\x7b.\*?\x22fn\x22\s\*\x3a\s\*\x22(getItems|folderRename|file(Delete|Copy))\x22\s\*\x2c\s\*\x22args\x22\s\*\x3a\x5b?[^\x7d]\*?\x22[^\x22]\*?(\.\.|0day)[^\x22]\*?\x22.\*?\x7d/imsP"; metadata:policy balanced-ips drop, policy security-ips drop, service http; classtype:attempted-user; sid:21926; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Lotus Notes .pl script source download attempt"; flow:to\_server,established; content:".pl"; http\_uri; content:".pl"; content:"."; within:1; metadata:service http; reference:bugtraq,6841; classtype:web-application-attack; sid:2066; rev:10;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 1812 (msg:"SERVER-WEBAPP VirusWall catinfo access"; flow:to\_server,established; content:"/catinfo"; nocase; reference:bugtraq,2579; reference:bugtraq,2808; reference:cve,2001-0432; reference:nessus,10650; classtype:attempted-recon; sid:1232; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP zml.cgi attempt"; flow:to\_server,established; content:"/zml.cgi"; http\_uri; content:"file=../"; metadata:service http; reference:bugtraq,3759; reference:cve,2001-1209; reference:nessus,10830; classtype:web-application-activity; sid:1395; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP IBM Lotus Domino cross site scripting attempt"; flow:established,to\_server; content:"/CitiPayPro.nsf"; fast\_pattern:only; http\_uri; pcre:"/[?&]Src=[^&]+?([\x22\x27\x3c\x3e\x28\x29]|script|onload|src)/Ui"; metadata:policy security-ips drop, service http; reference:bugtraq,14845; reference:cve,2005-3015; classtype:web-application-attack; sid:23434; rev:2;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP webhits.exe access"; flow:to\_server,established; content:"/scripts/samples/search/webhits.exe"; nocase; http\_uri; metadata:service http; reference:bugtraq,950; reference:cve,2000-0097; classtype:web-application-activity; sid:1073; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Domino ntsync4.nsf access"; flow:to\_server,established; content:"/ntsync4.nsf"; nocase; http\_uri; metadata:service http; reference:nessus,10629; classtype:attempted-recon; sid:1581; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP BLNews objects.inc.php4 remote file include attempt"; flow:to\_server,established; content:"/objects.inc.php4"; http\_uri; content:"Server[path]="; pcre:"/Server\x5bpath\x5d=(https?|ftps?|php)/"; metadata:service http; reference:bugtraq,7677; reference:cve,2003-0394; reference:nessus,11647; classtype:web-application-attack; sid:2147; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP guestbook.pl access"; flow:to\_server,established; content:"/guestbook.pl"; nocase; http\_uri; metadata:service http; reference:bugtraq,776; reference:cve,1999-0237; reference:cve,1999-1053; reference:nessus,10099; classtype:attempted-recon; sid:1140; rev:18;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP a1stats access"; flow:to\_server,established; content:"/a1stats/"; http\_uri; metadata:service http; reference:bugtraq,2705; reference:cve,2001-0561; reference:nessus,10669; classtype:web-application-activity; sid:1731; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP ExAir access"; flow:to\_server,established; content:"/exair/search/"; nocase; http\_uri; metadata:service http; reference:bugtraq,193; reference:cve,1999-0449; reference:nessus,10002; reference:nessus,10003; reference:nessus,10004; classtype:web-application-activity; sid:1500; rev:17;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Bit 5 Blog SQL injection in processlogin.php username via"; flow:to\_server,established; content:"processlogin.php"; fast\_pattern:only; http\_uri; content:"username"; nocase; pcre:"/username=[^\r\n\x26]\*?([\x22\x27]|%2[27])/i"; metadata:service http; reference:bugtraq,16244; reference:cve,2006-0320; classtype:web-application-attack; sid:20648; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP FormHandler.cgi access"; flow:to\_server,established; content:"/FormHandler.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,798; reference:bugtraq,799; reference:cve,1999-1050; reference:nessus,10075; classtype:web-application-activity; sid:1594; rev:20;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP csSearch.cgi access"; flow:to\_server,established; content:"/csSearch.cgi"; http\_uri; metadata:service http; reference:bugtraq,4368; reference:cve,2002-0495; reference:nessus,10924; classtype:web-application-activity; sid:1548; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP AlienForm af.cgi directory traversal attempt"; flow:to\_server,established; content:"/af.cgi"; http\_uri; content:".|7C|./.|7C|."; metadata:service http; reference:bugtraq,4983; reference:cve,2002-0934; reference:nessus,11027; classtype:web-application-attack; sid:1823; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS 7779 (msg:"SERVER-WEBAPP Oracle iSQL Plus cross site scripting attempt"; flow:to\_server,established; content:"/isqlplus"; nocase; http\_uri; content:"action="; nocase; http\_uri; pcre:"/action[\x3d\x3f][^\n\x26]\*\x3c[^\n\x26]+\x3e/Ui"; metadata:service http; reference:bugtraq,9484; reference:cve,2004-2115; classtype:web-application-attack; sid:12060; rev:8;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP spin\_client.cgi access"; flow:to\_server,established; content:"/spin\_client.cgi"; http\_uri; metadata:service http; reference:nessus,10393; classtype:web-application-activity; sid:1496; rev:13;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP GlobalFunctions.php access"; flow:to\_server,established; content:"/GlobalFunctions.php"; nocase; http\_uri; metadata:service http; reference:bugtraq,9057; classtype:web-application-activity; sid:2282; rev:12;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP Adobe JRun directory traversal attempt"; flow:to\_server,established; content:"/logviewer.jsp"; fast\_pattern; http\_uri; content:"logfile="; nocase; http\_uri; content:"../../../../"; http\_uri; metadata:policy security-ips drop, service http; reference:cve,2009-1873; reference:cve,2009-1874; reference:url,adobe.com/support/security/bulletins/apsb09-12.html; classtype:attempted-recon; sid:23403; rev:2;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP OpenView NNM snmp.exe CGI Host parameter buffer overflow attempt"; flow:to\_server,established; content:"/OvCgi/Main/Snmp|2E|exe"; fast\_pattern:only; http\_uri; content:"Oid|3D|"; nocase; http\_client\_body; isdataat:1000,relative; pcre:"/Oid\x3D[^\x0D\x0A]{1000}/Pi"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:cve,2009-3849; reference:url,h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01950877; classtype:attempted-user; sid:20241; rev:3;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Oracle Secure Backup Administration Server authentication bypass attempt via POST"; flow:to\_server,established; content:"login.php"; nocase; http\_uri; content:"attempt"; nocase; http\_client\_body; content:"uname="; nocase; http\_client\_body; pcre:"/uname\x3D[^\x26\x2D\s]\*?\x2D/iP"; metadata:policy security-ips drop, service http; reference:bugtraq,41596; reference:cve,2010-0904; classtype:attempted-admin; sid:17049; rev:6;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP input.bat access"; flow:to\_server,established; content:"/input.bat"; http\_uri; metadata:service http; reference:bugtraq,762; reference:cve,1999-0947; reference:nessus,10016; classtype:web-application-activity; sid:1513; rev:15;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET 8300 (msg:"SERVER-WEBAPP Novell GroupWise Messenger Accept-Language header buffer overflow attempt"; flow:to\_server,established; content:"Accept-Language"; nocase; isdataat:17,relative; pcre:"/^Accept-Language\x3A[^\r\n]{17}/smi"; metadata:service http; reference:bugtraq,17503; reference:cve,2006-0992; classtype:attempted-admin; sid:6414; rev:8;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP VMware SpringSource Spring Framework class.classloader remote code execution attempt"; flow:to\_server,established; content:"class|2E|classLoader"; fast\_pattern:only; http\_client\_body; metadata:service http; reference:bugtraq,40954; reference:cve,2010-1622; classtype:attempted-admin; sid:18959; rev:5;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP HP Openview Network Node Manager OvAcceptLang overflow attempt"; flow:to\_server,established; content:"/OVCgi/Toolbar.exe"; fast\_pattern:only; http\_uri; pcre:"/OvAcceptLang\s\*\x3d\s\*[^\x3b\n]{300}/ismC"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:bugtraq,34134; reference:cve,2009-0921; classtype:attempted-user; sid:16555; rev:7;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP ADNForum SQL injection in index.php fid attempt"; flow:to\_server,established; content:"index.php"; nocase; http\_uri; content:"fid="; fast\_pattern:only; pcre:"/fid=[^\r\n\x26]\*?([\x22\x27]|%2[27])/i"; metadata:service http; reference:bugtraq,16157; reference:cve,2006-0123; classtype:web-application-attack; sid:20649; rev:8;)

#alert tcp $HTTP\_SERVERS any -> $EXTERNAL\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP PHPLIB remote command attempt"; flow:to\_server,established; content:"/db\_mysql.inc"; http\_uri; metadata:service http; reference:bugtraq,3079; reference:cve,2001-1370; classtype:attempted-user; sid:1255; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP alchemy http server PRN arbitrary command execution attempt"; flow:to\_server,established; content:"/PRN/../../"; http\_uri; metadata:service http; reference:bugtraq,3599; reference:cve,2001-0871; reference:nessus,10818; classtype:web-application-activity; sid:1505; rev:14;)

#alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg:"SERVER-WEBAPP nsManager.cgi access"; flow:to\_server,established; content:"/nsManager.cgi"; nocase; http\_uri; metadata:service http; reference:bugtraq,1710; reference:bugtraq,4579; reference:cve,2000-1023; reference:nessus,11748; classtype:web-application-activity; sid:2215; rev:16;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Oracle BEA WebLogic overlong JESSIONID buffer overflow attempt"; flow:to\_server,established; content:"JSESSIONID="; isdataat:300,relative; pcre:"/JSESSIONID=[^\s\x26\x3a\x22\x27\x3b]{300}/smi"; metadata:service http; reference:cve,2008-5457; classtype:misc-attack; sid:15477; rev:9;)

#alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"SERVER-WEBAPP Ipswitch WhatsUp Gold DOS Device HTTP request denial of service attempt"; flow:to\_server,established; content:"prn"; http\_uri; pcre:"/^(GET|POST)\s+[^\x0a]\*?\x2fprn\x2e(htm|html|asp|cgi)/i"; metadata:policy security-ips drop, service http; reference:bugtraq,11110; reference:cve,2004-0799; classtype:attempted-dos; sid:15982; rev:5;)