



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



## L-Sec Application Security Seminar 2008 Conclusion

**Ir. Erwin Geirnaert, CISSP, CISA**  
Partner & Co-founder ZION SECURITY

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

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

```
<end if>
```



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



For a good conclusion

We need to define:

**Application Security Maturity**

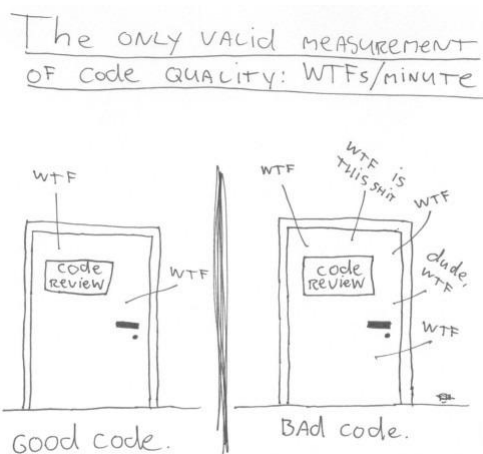
[www.zionsecurity.com](http://www.zionsecurity.com)

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

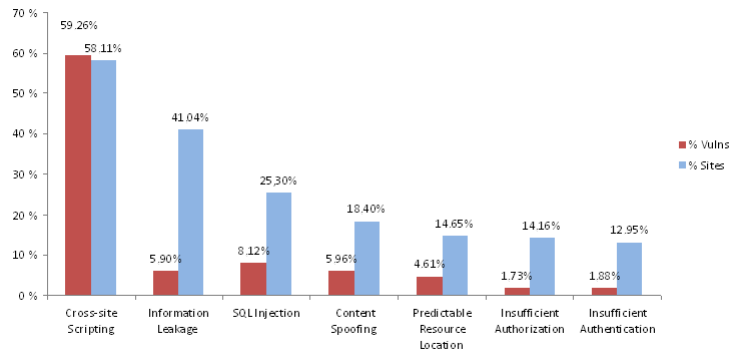
```
<end if>
```

1. The WTF factor
2. The hacking incidents
3. The technological improvements
4. The application security products
5. The reality

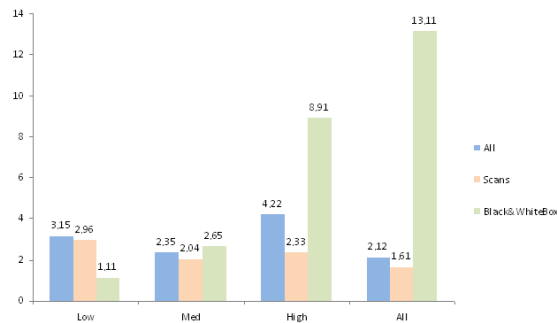
- # of vulnerabilities in the web application
- # of security controls in the web application
- # of hours spent on reviewing code or security testing the site
- Implementation of a Secure SDLC?



(c) 2008 Focus Shift/OSNews/Thom Holwerda - <http://www.osnews.com/comics>



## WASC Web Application Security Statistics 2007



## Number of vulnerabilities per site

- Disclaimer: this is based on personal experience and input from other people
- # of vulnerabilities in web applications  
     No idea
- # of security controls in web applications  
     1: authentication
- # of hours spent on reviewing code or security testing site  
     0
- Implementation of a Secure SDLC
  - SDLC? WTF?

Conclusion: still some work to do here

- If you don't get mentioned in the press, you aren't hacked so you are secure
  - Web Hacking Incident Database helps to show the trends in hacking not in securing
- Most people don't care about these incidents:
  - “We don't live in the US”-mentality
- Chicken or the egg problem

- People only think about security when there is a problem



- People only react when they are hacked
- Problem is that hacks will go under the radar
- Vulnerabilities will be exploited without impacting the users
  - No defacements
  - Already ongoing with JavaScript injections and web server bots

Conclusion: it's just the beginning of the malicious Internet

- The development frameworks like Struts, ASP.NET, Spring, ... are helping to improve software security
- Web servers are more secure
  - Apache 2.0
  - IIS 6 & IIS 7
- HTTPS is used more then before
  - Hopefully like it should

- But:
  - Too many legacy web sites use PHP, ASP, ...
  - Unpatched Content Management Systems
  - Cheap hosting
- Developers are unaware of the security features in development frameworks
- Developers aren't interested in security

Conclusion: more awareness and training

- Too much marketing
- No integration with other products like IAM
- Technology is there, also the price
- We need more implementations of
  - Code review tools
  - Web application firewalls
  - Honeypots/honeynets

Conclusion: waiting for some more consolidation

- We are now at a tipping point where anti-virus vendors were 10 years ago with the I Love You virus. Now almost everyone has an anti-virus
- We all know that anti-virus is not working against the latest threats
- We need to professionalise our work, our knowledge and support organizations like OWASP
- The fun has just begun

- The reality is scary
  - Too many sites have huge holes
  - No protection on an infrastructure or application layer against automated attacks
  - Browser security is terrible
  - Users are just humans
  - Passwords are terrible
  - Web 2.0, Ajax & JavaScript will introduce viruses, worms and spyware

E-mail: [erwin.geirnaert@zionsecurity.com](mailto:erwin.geirnaert@zionsecurity.com)

GSM: +32478289466

Tel: +3223350494

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

LinkedIn: [www.linkedin.com/in/erwingeirnaert](http://www.linkedin.com/in/erwingeirnaert)

Blog: [erwingeirnaert.blogspot.com](http://erwingeirnaert.blogspot.com)