Security despite of lazy developers – possible or not?

By Andrzej Kleśnicki
Laziness (also called indolence) is a disinclination to activity or exertion despite having the ability to do so.

By this definition – developers know how to create secure application – they just do not want to.

True or False?
Vulnerable application is not a failure of single developer but whole process of creating solution since first business requirement
The Software Assurance Maturity Model (SAMM) is an open framework to help organizations formulate and implement a strategy for software security that is tailored to the specific risks facing the organization. The resources provided by SAMM will aid in:
• No governance or requirements
• No security design
• Lack of security in QA
• Deployment – fast and cheep
• If we can not fight it - how to solve it?
• Secure the environment
• Implement secure configuration
• Learn your surroundings
• Check for known vulnerabilities

• How (examples only):
  – Nmap, OpenVAS, How To, Man pages, Friends ,
  – Qualys ;)
• Perform DAST / SAST

#1 Request
Payload:  q=x--%3E%3Cqss%3E
Request:  GET http://54.243.54.81:8080/bodgeit/search.jsp?q=x--%3E%3Cqss%3E

Click this link to try to reproduce the vulnerability using above payload. Note that clicking this link may not lead requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability.

#1 Response
&lt;a href="product.jsp?typeid=1">Widgets</a>&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;br/&gt;&lt;/td&gt;
</h3>
&lt;font size="-1"&gt;

&lt;b&gt;You searched for:&lt;/b&gt; z--&lt;qss&gt;&lt;br/&gt;&lt;br/&gt;
&lt;div&gt;&lt;b&gt;No Results Found&lt;/b&gt;&lt;/div&gt;
&lt;/font&gt;
&lt;/td&gt;
• Implement WAF

GET / HTTP/1.1
User-Agent: shellshock-scan
Accept: */*
Referer: () {::}; cat /etc/passwd

• How (examples only):
  – IronBee
  – Qualys
Monitor

- Look into logs and find suspicious behavior

- How (examples only)
  - By hand?
  - Splunk, Sawmill, Graylog2 etc.
  - Maybe Qualys? :D
• Scenario 1
  – We detect ShellShock attempt in HTTP request, knowing that host in vulnerable we block it, but also checking in logs to see backlog of 24h requests from same IP

• Scenario 2
  – We detect XSS possible vector using DAST, as result modifying WAF to protect it right away, tune up Log monitoring to find IOC

ETC...
• Andrzej Kleśnicki
  – @: aklesnicki@qualys.com
  – Security Expert
  – pl.linkedin.com/in/klesnicki/

• Qualys
  – Qualys.com
  – Cool company with cool services
  – OWASP supporter
  – OpenSource contributor
Security at Your Fingertips - FREE
Make sure your systems are secure and compliant.
Select a free tool below. There's nothing to download!

www.qualys.com/secure