Agenda

- Short history of XSS
- XSS defined
- Defence
- Resources
- Q&A
Short history of XSS

- XSS is at least 15 years old (was born somewhere around 1996)
- Back then You could with use of Javascript create iframe, load another page inside it and script it anyway You like :) 
- SOP was introduced in Netscape Navigator 2.0 
- 2005 – Samy – first XSS worm, hit MySpace – it finally went offline, 1 000 000 infections in less than 24 hours
XSS defined

- „XSS flaw occurs when application includes user supplied data in a page sent to the browser without properly validating or escaping that content” – from OWASP TOP 10

- XSS can be
  - Stored
  - Reflected
  - Dom based <- no server side interaction

- Some (bad) statistics:
  - OWASP TOP 10 2010: A2
  - 2011 CVE/SANS Top 25 Most Dangerous Software Errors: 4
XSS defined

- What can happen?
  - Site defacement
  - Identity theft, data theft
  - Force user action
  - Redirect to hostile content
  - User tracking
  - ...

- More:
  - https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29
  - http://www.youtube.com/watch?v=_Z9RQSnf8-g
Defence

- Input Validation
  - Simple and straightforward
  - **Blacklist** approach
  - ASP.Net use request validation mechanism (when it is turn on)
  - when first time HttpRequest.Form collection getter is called, all form fields are validated
  - **CrossSiteScriptingValidation** class and IsDangerousString method

- More about request validation:
  - [http://alexsmolen.com/blog/?p=15](http://alexsmolen.com/blog/?p=15)
Defence

- **Output Encoding**
  - `HttpUtility` class
  - but when to use what?
  - MSDN doesn’t help much...

`HttpUtility.JavaScriptStringEncode` Method

**(String)**

*.NET Framework 4*

Encodes a string.

- ...but we have OWASP XSS Prevention Cheat Sheet!
Defence

- **AntiXSS:**
  - *Whitelist* approach (better)
  - Can be easily plugged as .Net encoder for http runtime
  - There is brand new version due to some recent vulnerability ;)

- **XSS Detect? OWASP ESAPI ??**

- **More:**
  - [https://www.owasp.org/index.php/XSS_%28Cross_Site_Scripting%29_Prevention_Cheat_Sheet](https://www.owasp.org/index.php/XSS_%28Cross_Site_Scripting%29_Prevention_Cheat_Sheet)
Q & A

mateusz.olejarka@owasp.org
Resources

Books:
- XSS Attacks, J.Grossman, R.Hansen and others
- Web application obfuscation, M.Heiderich
- The Tangled Web, M.Zalewski

Online:
- http://ha.ckers.org/xss.html
- http://code.google.com/p/browsersec/wiki/Main
Resources

Blogs:
- http://samy.pl
- http://jeremiahgrossman.blogspot.com/
- http://heideri.ch/
- http://www.thespanner.co.uk/
- http://threats.pl/bezpieczenstwo-aplikacji-internetowych
- http://blog.kotowicz.net/
Resources

Recent:

- [http://lcamtuf.coredump.cx/postxss/](http://lcamtuf.coredump.cx/postxss/)
- [http://idunno.org/archive/2012/01/10/vulnerability-in-antixss-library-could-allow-information-disclosure.aspx](http://idunno.org/archive/2012/01/10/vulnerability-in-antixss-library-could-allow-information-disclosure.aspx)