



## AntiSamy.NET

keep on keepin' on  
fighting xss the .NET way



**OWASP**  
**EU Summit**  
**Portugal**

SETTING THE APPSEC  
AGENDA FOR '09  
3-7 November

---

Jerry Hoff (developer)  
Marcin Wielgoszewski (reviewer)  
Arshan Dabirsiaghi (project lead)

# Personnel File

---

- Marcin Wielgoszewski
- Technology Risk Consultant in NYC
- Perform web application security assessments and secure software development lifecycle consulting
- NYC OWASP Chapter Special Projects
- Involved in OWASP since March of 2007
- Prominent blogger and owner of [tssci-security.com](http://tssci-security.com)

# Samy is not my hero

---

- Samy made friends, lots of them
- Arshan got jealous. He had none
- If Arshan can't have friends, no one can
- Thus, AntiSamy was born

# Where did MySpace go wrong?

---

- They used a word blacklist
- Negative security models are error prone
- Back in August 2003, a site for indy bands was created that allowed...

## Recommendations:

- Many of us recommend “all output be entity-encoded,” rah rah rah!
- Perform strict input validation and don’t accept HTML, JavaScript, etc.



## Do we *really* need to accept HTML?

---



- MySpace and Facebook users want to customize profiles
- Community sites like eBay/Craigslist allow public listings
- CM solutions used by news sites, blogs, etc allow rich comment sharing

YES – we really do need it!

Let's stop talking about using Lynx like we enjoy it

# Introduction to AntiSamy

---

- API used to ensure user input is compliant with applications' acceptance rules
- Define policies and choose what to accept
- Safely allow rich HTML and CSS – say what???
- Display errors back to the user – hello information leakage?
- Not in line with current security practices

# Who's Using AntiSamy??

---

- 10 contributors from around the world
- 9 translated languages
- 1000's of downloads
- Worked with Microsoft to implement similar functionality in .NET framework

# Project Overview

---

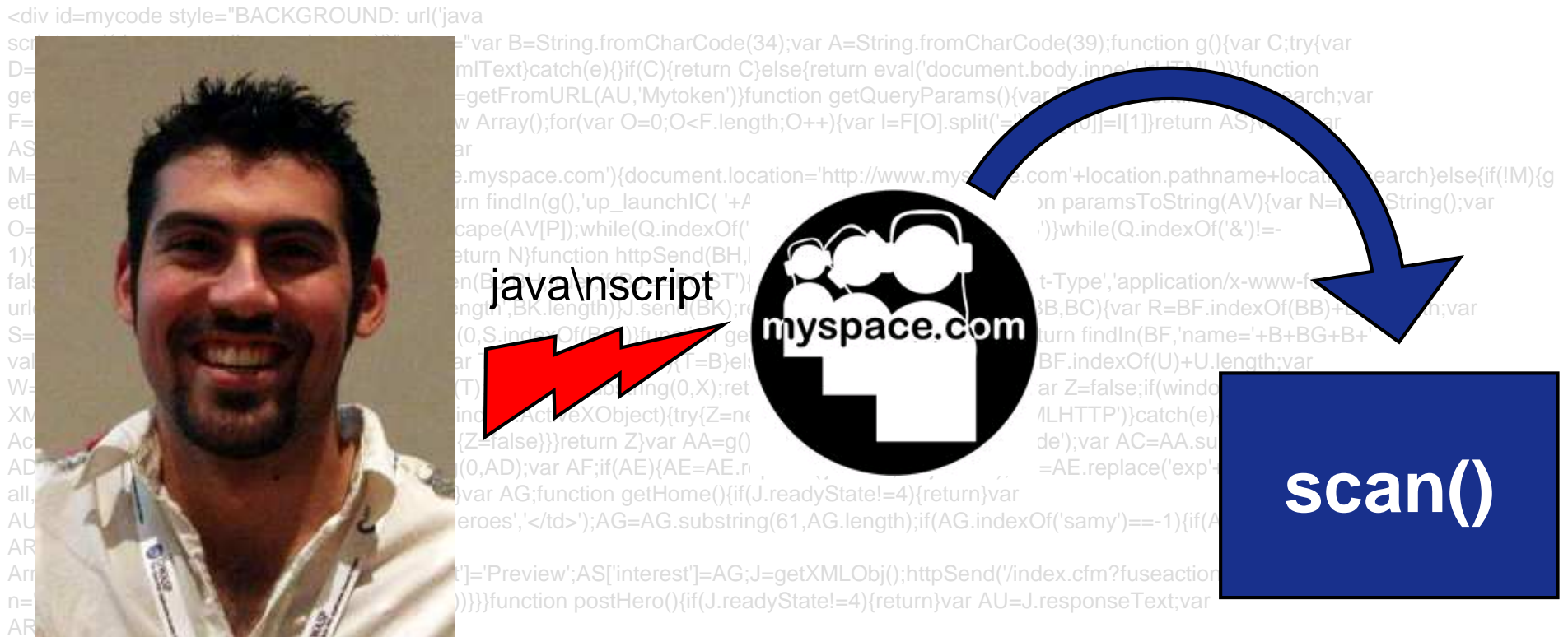
- AntiSamy was well received in San Jose at the OWASP/WASC conference
- Used by many folks, implemented in ESAPI
- ESAPI .NET began development, so naturally...
- .NET needed lovin' too
- Develop AntiSamy.NET
- ???



# How it Works™

```

<div id=mycode style="BACKGROUND: url('/java
sc
D=
ge
F=
AS
M=
etD
O=
1){
fa
ur
S=
va
W=
XM
Ac
AD
all
AU
AR
Arr
n=
AR
    "var B=String.fromCharCode(34);var A=String.fromCharCode(39);function g(){var C;try{var
    mlText}catch(e){if(C){return C}else{return eval('document.body.innerHTML')}function
    =getFromURL(AU,'Mytoken');function getQueryParams(){var search;var
    w Array();for(var O=0;O<F.length;O++){var l=F[O].split('=')[0];return AS;var
    ar
    e.myspace.com'}(document.location='http://www.myspace.com'+location.pathname+location.search}else{if(!M){g
    on paramsToString(AV){var N=String();var
    ')}while(Q.indexOf('&')!=-
    t-Type','application/x-www-f
    B,BC){var R=BF.indexOf(BB)+1;in;var
    urn findIn(BF,'name='+B+BG+B+
    BF.indexOf(U)+U.length;var
    ar Z=false;if(window
    /LHTTP')}catch(e)
    de');var AC=AA.sub
    =AE.replace('exp'
    heroes','<td>');AG=AG.substring(61,AG.length);if(AG.indexOf('samy')===-1){if(A
    t']='Preview';AS['interest']=AG;J=getXMLObj();httpSend('/index.cfm?fuseaction
    ))}}function postHero(){if(J.readyState!=4){return}var AU=J.responseText;var
    Array());AS['interestLabel']='heroes';AS['submit']='Submit';AS['interest']=AG;AS['hash']=getHiddenParameter(AU,'hash');httpSend('/index.cfm?fuseaction=profil
    e.processInterests&Mytoken='+AR,nothing,'POST',paramsToString(AS))}function main(){var AN=getClientFID();var
    RH='/index.cfm?fuseaction=user.viewProfile&friendID='+AN+'&Mytoken='+AR;getXMLObj();httpSend(RH,getHome,'GET');xmlhttp2
    '+L,proc
    Text;var
    friendID
    n='+AR,
    BJ=='PC
    mlhttp2.s
  
```



**DOMScanner**  
(magic happens)

**HTMLAgility**

**getCleanHTML**

**policy.xml**

# policy.xml

Define what you want to allow:

- Accepted tags
- Common attributes
- Global attributes

```
56 <common-attributes>
57
58   <attribute name="align" description="The 'align' attribute of an HTML element is
59     <literal-list>
60       <literal value="center"/>
61       <literal value="left"/>
62       <literal value="right"/>
63       <literal value="justify"/>
64       <literal value="char"/>
65     </literal-list>
66   </attribute>
67
68 </common-attributes>
69
70 <global-tag-attributes>
71   <attribute name="title"/>
72   <attribute name="lang"/>
73 </global-tag-attributes>
74
75
76 <tag-rules>
77
78   <tag name="img" action="validate">
79     <attribute name="src" onInvalid="removeTag">
80       <regexp-list>
81         <regexp name="onsiteURL"/>
82         <regexp name="offsiteURL"/>
83       </regexp-list>
84     </attribute>
85     <attribute name="name"/>
86     <attribute name="alt"/>
87     <attribute name="height"/>
88     <attribute name="width"/>
89     <attribute name="border"/>
90     <attribute name="align"/>
91   </tag>
92
93
94   <!-- Tags related to JavaScript -->
95
96   <tag name="script" action="remove"/>
97   <tag name="noscript" action="remove"/>
98
99   <!-- Frame & related tags -->
```

# Project Objectives

---

- Deliver functionally identical version of AntiSamy for .NET
- Deliver a release quality product by conclusion of *Summer of Code 2008*

# Status and Future Steps

---

Beta Quality (v0.7) Summer of Code 2008

- Current!

Release Quality (v1.0)

- Need to run Fortify SCA against codebase to quality check
- About 90% completed – still lacking CSS support
- Document usage of AntiSamy and various functionality

# Closing

---

Thanks to the following people for all of their hard work on AntiSamy:

- Jerry Hoff
- Jason Li
- Arshan Dabirsiaghi

Download AntiSamy from:

- <http://code.google.com/p/owaspantisamy/downloads/list>
- [http://www.owasp.org/index.php/Category:OWASP\\_AntiSamy\\_Project](http://www.owasp.org/index.php/Category:OWASP_AntiSamy_Project)