

Best Practices for Secure Web Development

Revision 3.0

Revision Date

Revision History

Acknowledgments

Secure Programming for Linux and Unix HOWTO

The World Wide Web Security FAQ

Contents

1	WHY?	1
1.1	Frequently Asked Questions.....	2
2	FUNDAMENTALS	4
2.1	Security as part of the business picture	4
2.2	Security as part of the requirements gathering.....	4
2.3	Security as part of the architecture.....	4
2.4	Watch what you use.....	5
2.5	Never trust incoming data. Never.....	5
2.6	When possible, help the user	6
2.7	Code reviews are your friends.....	6
2.8	Privacy & law	6
2.9	Stay up-to-date!.....	7
2.10	Document, document, document!.....	7
3	TECH DETAILS	8
3.1	Don't be anonymous when you won't end up so.....	8
3.2	Do not use more power than you actually need.....	8
3.3	Don't use GET to send sensitive data!	9
3.4	Never trust incoming data – details	10
3.5	Don't rely on the client to keep important data	10
3.6	Don't store sensitive stuff in the *SP page itself.....	11
3.7	Beware of extensions.....	11
3.8	Keep an eye on HTML Comments left in production code	12
3.9	Error messages	12
3.10	Cross-site scripting	12
3.11	Check the wizard-generated or sample code.....	16
3.12	Language & technology specifics	16
3.13	Middleware security	19
3.14	Declarative vs programmatic.....	20
3.15	Distributed systems and firewalls	21
	PKI is not a silver bullet.....	23
3.17	Snake oil	23
3.18	When randomness matters.....	23
3.19	Use the logs. Create useful logs.	24
3.20	SSL	24
3.21	Other pointers	25

Legal Notice.

About the author:

1 WHY?

Target Audience

What exactly do you mean by 'information security'?

protect

technologies

*processes
enable*

- *authentication*
- *authorization*
- *privacy*
- *accountability & non-repudiation*

- *integrity*
- *detection & monitoring*
- *legal aspects*

I thought the firewall would take care of this. Or file permissions. Or SSL.

around

in

I'm an experienced web developer and don't think I need this.

secure

Can't someone do this after I finish my dev work?

Note

2 FUNDAMENTALS

managing risk

assets

risks

- *assets*
- *use cases*
- *the users, their roles and rights*
- *legal and business issues*

-

-

-

reported

of private data

collection and handling

Crypto Law Survey

3 TECH DETAILS

...



-

-

**relying on
hidden form fields to maintain sensitive data between requests**

**Form Tampering Vulnerabilities in Several
Web-Based Shopping Cart Applications**

source

::\$DATA

Translate: f

.

.inc

- *physical paths*

c:\inetpub\wwwroot\common.asp

- *platform architecture.*

client

Send detailed ASP error message to

not

```
<html>
<%
    if request.form ("yourname") <>" then
        Response.Write("Hello " + request.form ("yourname"))
    else
%>
    <form method="POST">
        <input type="text" name= yourname>
        <input type="submit" value="submit">
    </form>
<%
    end if
%>
</html>
```

```
<script language='javascript' >alert ('gotcha!');</script>
```

the visitor will get the script as if it were part of the legitimate site and

the script will get executed on the browser.

cannot be identified by the browser

within an HTML tag

```
<a href=" [event]='bad script here' "> click me </a>
```

```
<% Response.Write("<BODY BGCOLOR=\"\" +  
Request.Cookies("UserColor") + "\">"); %>
```

```
Cookie: %22+onload%3D%27window%2Elocation%3D  
%22http%3A%2F%2Fwww%2Eevilsite%2Ecom%22%3B%27
```

```
<body BGCOLOR="" onload=  
'window.location="http://www.evilsite.com";' ">
```

What to do?

displayed

>

<

Server

HTMLEncode

<script>

<script>

see



Server.URLEncode

buffer overflows

attacks

format string

relying

correctly.

Java Authentication and Authorization

Service

Java Security

Inside Java 2 Platform Security

Security Code Guidelines

Secure

Programming for Linux and Unix HOWTO

`-Djava.security.debug`

`java -Djava.security.debug=help`

World Wide Web Security FAQ

whisker

CGI/Perl Taint Mode FAQ"

Secure Programming for Linux and Unix HOWTO

Secure UNIX Programming FAQ

Writing Safe Setuid Programs _____

How to find security holes _____

How to Write Secure Code _____

xmlsig

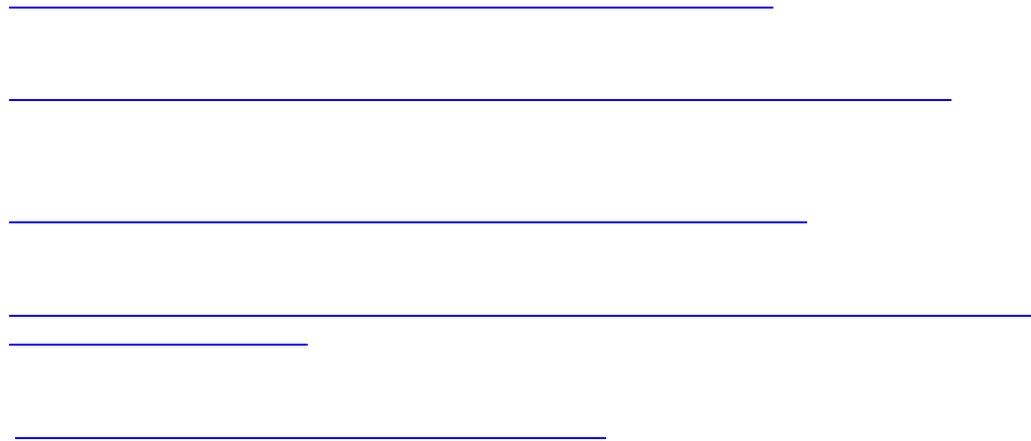
authentication authorization impersonation delegation of credentials

the

Programming Windows Security

Designing Enterprise Applications with J2EE

Building Java Enterprise Systems with J2EE



Declarative

Programmatic

IsCallerInRole

and

COM Internet Services DCOM over HTTP)

RMI ,Servlets and Object Serialization FAQ

Joint Firewall Revised Submission

CORBA Firewalls

SOAPMethodName

text/xml text/xml-SOAP

M-POST

Simple Object Access Protocol (SOAP) and Firewalls

Public-Key Infrastructure

Understanding the

Ten Risks of PKI

Cryptogram

pseudo *appear*

SecureRandom

not

...

...

...
