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

Legal Notice.

About the author:

1 WHY?

Target Audience

What exactly do you mean by 'information security'?

technologies *processes*
protect *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.

in
around

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

collection and handling of private data

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.*

Send detailed ASP error message to client

CERT® Advisory CA-2000-02 Malicious HTML Tags Embedded in Client Web Requests

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 **&lt;**
&gt;

`Server`
`HTMLEncode`

<script> **&lt;script&gt;**
see
☺

`Server.URLEncode`

buffer overflows

format string attacks

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

xmldsig

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

Using Distributed COM with Firewalls

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

Understanding the

Public-Key Infrastructure

Ten Risks of PKI

Cryptogram

appear
pseudo

SecureRandom

not

... ...
...