



Dealing with problems at source

```
Dim filePath
Dim Index
Dim username
Dim password
Dim a

username = request.form("username")
password = request.form("password")

filePath = Server.MapPath("users.mdb")

Set oConn = Server.CreateObject("ADODB.Connection")
Set oRs = Server.CreateObject("ADODB.Recordset")

oConn.Open "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" & filePath
oRs.Open "SELECT * FROM users Where (username='" & username & "' & password='" & password & "')"

%>

<% if oRs.RecordCount <= 0 then
Response.Redirect("/badlogin.asp?logfile=errorlog&logmsg=badlogin")
else %>

<html>
<head>
<title>Acme Inc. secure portal.</title>
</head>
<body bgcolor="#BF42D6">

<table width="100%" height="155">
<tr>
<td align="right" valign="top">
<td align="left" valign="middle"><font face="arial" size=4 color="#ffffff">
</tr>
</table>

<tr color="#ffffff">
<td align="center" colspan="2">
<table border="1" width="100%">
<tr>
<td align="center" colspan="2">
</td>
</tr>
</table>
</td>
</tr>
</table>
</body>
</html>
```

The highlighted line of code above could allow an attacker complete control over this web application





Source code: the very foundation of application security

No matter how well a penetration test or technical audit is performed, a source code review of a bespoke application gives the ultimate “hands on view” of a system and its weaknesses.

Available to all

Until recently, source code reviews have been an expensive commodity, for which only the largest financial and government organisations have been able to budget. Thus, despite the massive benefits, many have been unable to bear the cost of bought-in expertise in order to view an application at the lowest possible level.

Sec-Tec has changed this forever. As a direct response to the growing number of e-government websites containing highly confidential personal data, Sec-Tec have developed a simple, cost-effective source code review process, designed to highlight the security issues within applications throughout the development cycle. This process saves valuable rewrite costs, whilst helping to ensure projects meet their deadlines.

Sec-Tec's source code auditing solution

Our source code review consists of four stages:

1 Project brief

Sec-Tec will work with the client to define the scope of the project and confirm which areas of the application will actually require auditing.

2 Initial automated review

Whether working on-site, or within our testing facility, Sec-Tec will review the source code using a range of automated review tools. These tools will highlight any basic security pitfalls such as insufficient bounds checking or lack of input validation.

3 Manual source code review

With the automated findings gathered, Sec-Tec's consultants will then begin to review the source code, looking for more advanced security problems such as invalid application logic and a lack of entropy within random string-generation routines. **Such high-level problems can only be found by manual inspection of key areas of the code.**

4 Report writing/correction

Following on from internal quality assurance procedures, Sec-tec will draft a comprehensive report detailing all the findings, with a strong emphasis on corrective actions. If required, Sec-Tec can also correct most vulnerabilities within the source itself, and present to the development team a list of these findings, the corrections made and why the issues existed in the first place. This also has the advantage of providing education for any future application development.

Sec-Tec's source code auditing service thus provides the earliest and most thorough vulnerability identification service available, consequently reducing the likelihood of incurring the massive costs of later corrective actions. Whatever the application or purpose, source code reviews are a vital tool in the IT security armoury.

FAQs

Why is there a need for a source code review?

Whilst some services, such as Penetration Testing, provide an external viewpoint of an application's security, a source code review offers a far deeper inspection of a web application, and can investigate vulnerabilities that, for example, may only be internally exploited by malicious staff.

What languages can be source code-reviewed?

Almost any language can be reviewed, with Sec-Tec specialising in the following:

- ASP – VisualBasic
- NET/ASP.NET – C#/VB.NET
- ActiveX
- CGI – PERL/C/C++/Shell Script
- PHP
- X86 Assembler
- Java

How long will a source code audit take?

The time varies dramatically according to the size of the project and the languages and technologies in use. Many projects, however, can be fully audited within five working days.

Should penetration testing be replaced by a source code review?

Generally, no. A source code review will look at the application in great detail, but cannot take into consideration other factors such as the build and configuration of the infrastructure surrounding the application.

Is source code auditing expensive?

Independent research has shown that the cost of fixing an issue before a project is in a production environment is typically **seven times cheaper** than afterwards with reactive penetration testing.

```
Dim filePath
Dim index
Dim username
Dim password
Dim s

username = request.form("username")
password = request.form("password")

filePath = Server.MapPath("data\index.mdb")
Set oConn = Server.CreateObject("ADODB.Connection")
Set oRs = Server.CreateObject("ADODB.Recordset")
oConn.Open "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" & filePath
oRs.Open "SELECT * FROM users Where (username='" & username & "' AND password='" & password & "')"

%>
-% if oRs.RecordCount <= 0 then
Response.Redirect("/badlogin.asp?logfile=errorlog&logmeeg=badlogin.asp")
else %>
<html>
<head>
<title>Acme Inc. secure portal.</title>
</head>
<body bgcolor="#BF42D6">
<table width="100%" height="155">
<tr>
<td align="right" valign="top">
<td align="left" valign="middle"><font face="arial" size="4" color="#ffffff">
</td>
</tr>
</table>
</body>
</html>
```



www.sec-tec.co.uk



Tel: +44 (0) 20 8317 7962
Fax: +44 (0) 20 8317 8051
Email: info@sec-tec.co.uk
Web: www.sec-tec.co.uk

