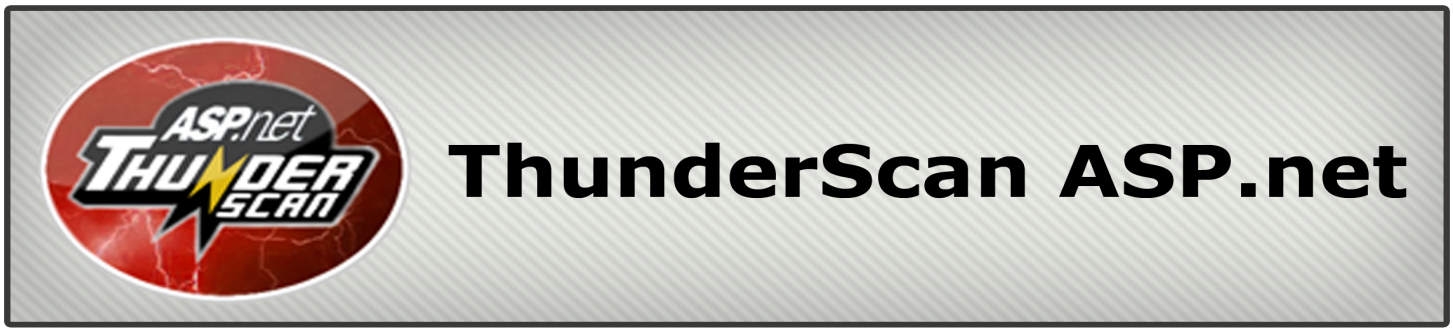
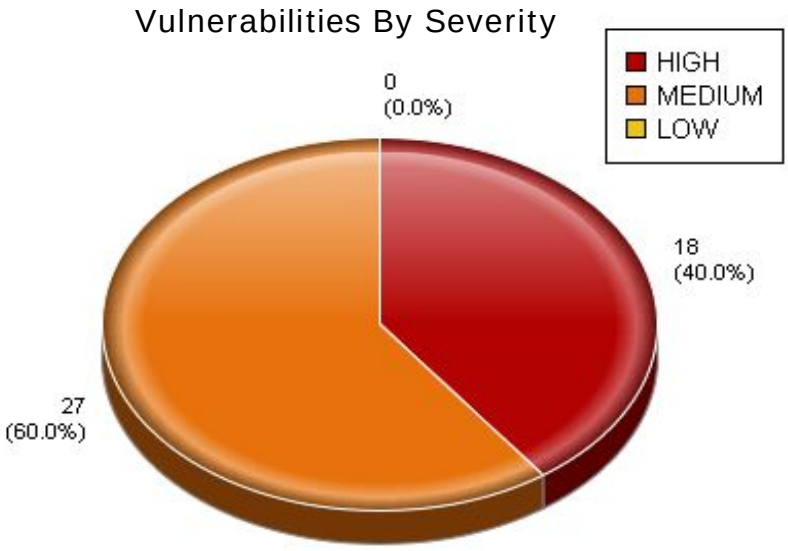


Web Application
Static Source Code Security Analysis
REPORT

www.defensecode.com

Scan Details

Project Name:	BugTracker.Net Security Audit	**Line per vuln:**	5491
Scanned Files:	190	**Filters:**	0
Code Lines:	247095	**Creation Date:**	11-15-2012
Vulnerabilities:	45	**Creation Time:**	19:22:19



Vulnerability group	Findings
SQL Injection	13
File Disclosure	5
Cross Site Scripting	9
HTTP Response Splitting	18

Project information	
Company	DefenseCode
Author	ThunderScan ASP.Net C#
E-mail	defensecode@defensecode.com
Brief Description	N/A

SQL Injection (13)

1. SQL Injection through SqlCommand()

Risk:	Code Line:	Vuln ID:
HIGH	57	6

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\dbutil.cs

Vulnerability:

57: SqlCommand(sql, conn)

Input variable:

row_id.Value

Stack (function/line/file):

1. SqlCommand() 56 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\dbutil.cs
0. execute_nonquery() 66 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\delete_customfield.aspx

User input flow:

0. row_id.Value
1. sql
2. sql

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

2. SQL Injection through SqlDataAdapter()

Risk:	Code Line:	Vuln ID:
HIGH	141	11

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\dbutil.cs

Vulnerability:

141: SqlDataAdapter da = new SqlDataAdapter(sql, conn)

Input variable:

row_id.Value

SQL Injection (13)

Stack (function/line/file):

2. SqlDataAdapter() 140 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\dbutil.cs
1. get_dataset() 174 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\dbutil.cs
0. get_datarow() 56 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\delete_report.aspx

User input flow:

0. row_id.Value
1. sql
2. sql
3. sql

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

3. SQL Injection through SqlDataAdapter()

Risk:	Code Line:	Vuln ID:
HIGH	141	3

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\dbutil.cs

Vulnerability:

141: SqlDataAdapter da = new SqlDataAdapter(sql, conn)

Input variable:

row_id.Value

Stack (function/line/file):

2. SqlDataAdapter() 140 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\dbutil.cs
1. get_dataset() 174 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\dbutil.cs
0. get_datarow() 40 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\delete_customfield.aspx

User input flow:

0. row_id.Value
1. sql
2. sql
3. sql

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

SQL Injection (13)

4. SQL Injection through SqlCommand()

Risk:	Code Line:	Vuln ID:
HIGH	57	7

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\dbutil.cs

Vulnerability:

57: SqlCommand(sql, conn)

Input variable:

row_id.Value

Stack (function/line/file):

1. SqlCommand() 56 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\dbutil.cs
0. execute_nonquery() 30 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\delete_org.aspx

User input flow:

0. row_id.Value
1. sql
2. sql

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

5. SQL Injection through SqlCommand()

Risk:	Code Line:	Vuln ID:
HIGH	57	9

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\dbutil.cs

Vulnerability:

57: SqlCommand(sql, conn)

Input variable:

SQL Injection (13)

row_id.Value

Stack (function/line/file):

1. SqlCommand() 56 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\dbutil.cs
0. execute_nonquery() 30 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\delete_project.aspx

User input flow:

0. row_id.Value
1. sql
2. sql

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

6. SQL Injection through SqlCommand()

Risk:	Code Line:	Vuln ID:
HIGH	57	12

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\dbutil.cs

Vulnerability:

57: SqlCommand(sql, conn)

Input variable:

row_id.Value

Stack (function/line/file):

1. SqlCommand() 56 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\dbutil.cs
0. execute_nonquery() 30 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\delete_status.aspx

User input flow:

0. row_id.Value
1. sql
2. sql

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

SQL Injection (13)

7. SQL Injection through SqlCommand()

Risk:	Code Line:	Vuln ID:
HIGH	57	2

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\dbutil.cs

Vulnerability:

57: SqlCommand(sql, conn)

Input variable:

row_id.Value

Stack (function/line/file):

1. SqlCommand() 56 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\dbutil.cs
0. execute_nonquery() 43 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\delete_comment.aspx

User input flow:

0. row_id.Value
1. sql
2. sql

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

8. SQL Injection through SqlCommand()

Risk:	Code Line:	Vuln ID:
HIGH	57	8

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\dbutil.cs

Vulnerability:

57: SqlCommand(sql, conn)

Input variable:

row_id.Value

SQL Injection (13)

Stack (function/line/file):

1. SqlCommand() 56 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\dbutil.cs
0. execute_nonquery() 30 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\delete_priority.aspx

User input flow:

0. row_id.Value
1. sql
2. sql

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

9. SQL Injection through SqlCommand()

Risk:	Code Line:	Vuln ID:
HIGH	57	1

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\dbutil.cs

Vulnerability:

57: SqlCommand(sql, conn)

Input variable:

row_id.Value

Stack (function/line/file):

1. SqlCommand() 56 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\dbutil.cs
0. execute_nonquery() 29 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\delete_category.aspx

User input flow:

0. row_id.Value
1. sql
2. sql

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

10. SQL Injection through SqlCommand()

SQL Injection (13)

Risk:	Code Line:	Vuln ID:
HIGH	57	4

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\dbutil.cs

Vulnerability:

57: SqlCommand(sql, conn)

Input variable:

row_id.Value

Stack (function/line/file):

1. SqlCommand() 56 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\dbutil.cs
0. execute_nonquery() 47 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\delete_customfield.aspx

User input flow:

0. row_id.Value
1. sql
2. sql

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

11. SQL Injection through SqlCommand()

Risk:	Code Line:	Vuln ID:
HIGH	57	13

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\dbutil.cs

Vulnerability:

57: SqlCommand(sql, conn)

Input variable:

row_id.Value

Stack (function/line/file):

SQL Injection (13)

1. SqlCommand() 56 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\dbutil.cs
0. execute_nonquery() 30 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\delete_udf.aspx

User input flow:

0. row_id.Value
1. sql
2. sql

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

12. SQL Injection through SqlCommand()

Risk:	Code Line:	Vuln ID:
HIGH	57	10

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\dbutil.cs

Vulnerability:

57: SqlCommand(sql, conn)

Input variable:

row_id.Value

Stack (function/line/file):

1. SqlCommand() 56 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\dbutil.cs
0. execute_nonquery() 43 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\delete_report.aspx

User input flow:

0. row_id.Value
1. sql
2. sql

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

13. SQL Injection through SqlCommand()

Risk:	Code Line:	Vuln ID:

SQL Injection (13)

HIGH	57	5

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\dbutil.cs

Vulnerability:

57: SqlCommand(sql, conn)

Input variable:

row_id.Value

Stack (function/line/file):

1. SqlCommand() 56 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\dbutil.cs
0. execute_nonquery() 57 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\delete_customfield.aspx

User input flow:

0. row_id.Value
1. sql
2. sql

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

File Disclosure (5)

1. File Disclosure through Response.WriteFile()

Risk:	Code Line:	Vuln ID:
HIGH	27	18

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\view_web_config.aspx

Vulnerability:

27: Response.WriteFile(path)

Input variable:

Request

Stack (function/line/file):

0. Response.WriteFile() 26 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\view_web_config.aspx

User input flow:

0. Request
1. path
2. path

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

2. File Disclosure through System.IO.File.OpenText()

Risk:	Code Line:	Vuln ID:
HIGH	84	16

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\edit_custom_html.aspx

Vulnerability:

84: System.IO.File.OpenText(path)

Input variable:

Request["which"]

Stack (function/line/file):

File Disclosure (5)

1. System.IO.File.OpenText() 83 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\edit_custom_html.aspx
0. load_file_into_control() 73 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\edit_custom_html.aspx

User input flow:

0. Request["which"]
1. which_file
2. file_name
3. file_name
4. path

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

3. File Disclosure through System.IO.File.OpenText()

Risk:	Code Line:	Vuln ID:
HIGH	84	17

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\edit_custom_html.aspx

Vulnerability:

84: System.IO.File.OpenText(path)

Input variable:

Request["which"]

Stack (function/line/file):

1. System.IO.File.OpenText() 83 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\edit_custom_html.aspx
0. load_file_into_control() 73 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\edit_custom_html.aspx

User input flow:

0. Request["which"]
1. which_file
2. file_name
3. file_name
4. path
5. path

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

File Disclosure (5)

4. File Disclosure through Response.WriteFile()

Risk:	Code Line:	Vuln ID:
HIGH	53	15

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\download_file.aspx

Vulnerability:

53: Response.WriteFile(path)

Input variable:

Request["filename"]

Stack (function/line/file):

0. Response.WriteFile() 52 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\download_file.aspx

User input flow:

0. Request["filename"]
1. filename
2. path
3. path

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

5. File Disclosure through Response.TransmitFile()

Risk:	Code Line:	Vuln ID:
HIGH	49	14

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\download_file.aspx

Vulnerability:

49: Response.TransmitFile(path)

Input variable:

File Disclosure (5)

Request["filename"]

Stack (function/line/file):

0. Response.TransmitFile() 48 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\download_file.aspx

User input flow:

0. Request["filename"]
1. filename
2. path

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

Cross Site Scripting (9)

1. Cross Site Scripting through Response.Write()

Risk:	Code Line:	Vuln ID:
MEDIUM	438	27

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\bug_list.cs

Vulnerability:

438: Response.Write(HttpContext.Current.Request["tags"])

Input variable:

Request["tags"]

Stack (function/line/file):

0. Response.Write() 437 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\bug_list.cs

User input flow:

0. Request["tags"]

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

2. Cross Site Scripting through Response.Write()

Risk:	Code Line:	Vuln ID:
MEDIUM	77	25

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\svn_blame.aspx

Vulnerability:

77: Response.Write(blame_text)

Input variable:

Request["path"]

Stack (function/line/file):

0. Response.Write() 76 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\svn_blame.aspx

Cross Site Scripting (9)

User input flow:

0. Request["path"]
1. path
2. blame_text

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

3. Cross Site Scripting through Response.Write()

Risk:	Code Line:	Vuln ID:
MEDIUM	92	21

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\git_diff.aspx

Vulnerability:

92: Response.Write(error)

Input variable:

Request["rev_1"]

Stack (function/line/file):

0. Response.Write() 91 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\git_diff.aspx

User input flow:

0. Request["rev_1"]
1. commit1
2. unified_diff_text
3. error

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

4. Cross Site Scripting through Response.WriteFile()

Risk:	Code Line:	Vuln ID:
MEDIUM	27	26

Cross Site Scripting (9)

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\view_web_config.aspx

Vulnerability:

27: Response.WriteFile(path)

Input variable:

Request

Stack (function/line/file):

0. Response.WriteFile() 26 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\view_web_config.aspx

User input flow:

0. Request
1. path

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

5. Cross Site Scripting through Response.WriteFile()

Risk:	Code Line:	Vuln ID:
MEDIUM	53	20

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\download_file.aspx

Vulnerability:

53: Response.WriteFile(path)

Input variable:

Request["filename"]

Stack (function/line/file):

0. Response.WriteFile() 52 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\download_file.aspx

User input flow:

0. Request["filename"]
1. filename
2. path

Cross Site Scripting (9)

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

6. Cross Site Scripting through Response.Write()

Risk:	Code Line:	Vuln ID:
MEDIUM	92	22

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\git_diff.aspx

Vulnerability:

92: Response.Write(error)

Input variable:

Request["rev_0"]

Stack (function/line/file):

0. Response.Write() 91 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\git_diff.aspx

User input flow:

0. Request["rev_0"]
1. commit0
2. unified_diff_text
3. error

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

7. Cross Site Scripting through Response.Write()

Risk:	Code Line:	Vuln ID:
MEDIUM	69	24

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\svn_blame.aspx

Vulnerability:

Cross Site Scripting (9)

69: Response.Write(raw_text)

Input variable:

Request["path"]

Stack (function/line/file):

0. Response.Write() 68 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\svn_blame.aspx

User input flow:

0. Request["path"]
1. path
2. raw_text

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

8. Cross Site Scripting through msg.InnerHtml()

Risk:	Code Line:	Vuln ID:
MEDIUM	88	19

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\default.aspx

Vulnerability:

88: msg.InnerHtml = "Error during windows authentication:
" + Request.QueryString["msg"];

Input variable:

Request.QueryString["msg"]

Stack (function/line/file):

0. msg.InnerHtml() 87 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\default.aspx

User input flow:

0. Request.QueryString["msg"]

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

Cross Site Scripting (9)

9. Cross Site Scripting through Response.Write()

Risk:	Code Line:	Vuln ID:
MEDIUM	63	23

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\hg_blame.aspx

Vulnerability:

```
63: Response.Write(revision + " -- " + HttpUtility.HtmlEncode(path))
```

Input variable:

Request["rev"]

Stack (function/line/file):

0. Response.Write() 62 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\hg_blame.aspx

User input flow:

0. Request["rev"]
1. revision

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

HTTP Response Splitting (18)

1. HTTP Response Splitting through Response.Redirect()

Risk:	Code Line:	Vuln ID:
MEDIUM	1186	35

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\util.cs

Vulnerability:

1186: Response.Redirect(url + "&url=" + Request.QueryString["url"] + "&qs=" + Request.QueryString["qs"])

Input variable:

Request.QueryString["qs"]

Stack (function/line/file):

0. Response.Redirect() 1185 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\util.cs

User input flow:

0. Request.QueryString["qs"]
1. url

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

2. HTTP Response Splitting through Response.Redirect()

Risk:	Code Line:	Vuln ID:
MEDIUM	1176	33

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\util.cs

Vulnerability:

1176: Response.Redirect(url + "?" + HttpUtility.UrlDecode(qs))

Input variable:

Request.QueryString["url"]

Stack (function/line/file):

HTTP Response Splitting (18)

0. Response.Redirect() 1175 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\util.cs

User input flow:

0. Request.QueryString["url"]
1. url

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

3. HTTP Response Splitting through Response.Redirect()

Risk:	Code Line:	Vuln ID:
MEDIUM	1176	32

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\util.cs

Vulnerability:

1176: Response.Redirect(url + "?" + HttpUtility.UrlDecode(qs))

Input variable:

Request.QueryString["qs"]

Stack (function/line/file):

0. Response.Redirect() 1175 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\util.cs

User input flow:

0. Request.QueryString["qs"]
1. qs

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

4. HTTP Response Splitting through Response.Redirect()

Risk:	Code Line:	Vuln ID:
MEDIUM	1190	42

File:

HTTP Response Splitting (18)

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\util.cs

Vulnerability:

1190: Response.Redirect(url + "?url=" + Request.QueryString["url"] + "&qs=" + Request.QueryString["qs"])

Input variable:

Request.QueryString["url"]

Stack (function/line/file):

0. Response.Redirect() 1189 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\util.cs

User input flow:

0. Request.QueryString["url"]
1. url

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

5. HTTP Response Splitting through Response.Redirect()

Risk:	Code Line:	Vuln ID:
MEDIUM	65	30

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\security.cs

Vulnerability:

65: Response.Redirect(target)

Input variable:

Request

Stack (function/line/file):

0. Response.Redirect() 64 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\security.cs

User input flow:

0. Request
1. original_querystring
2. target

HTTP Response Splitting (18)

Filter:

No mitigating factors. Input variable passed some security filters, but not for this vulnerability type.

6. HTTP Response Splitting through Response.Redirect()

Risk:	Code Line:	Vuln ID:
MEDIUM	1190	44

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\util.cs

Vulnerability:

1190: Response.Redirect(url + "?url=" + Request.QueryString["url"] + "&qs=" + Request.QueryString["qs"])

Input variable:

Request.QueryString["url"]

Stack (function/line/file):

0. Response.Redirect() 1189 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\util.cs

User input flow:

0. Request.QueryString["url"]

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

7. HTTP Response Splitting through Response.AddHeader()

Risk:	Code Line:	Vuln ID:
MEDIUM	44	29

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\download_file.aspx

Vulnerability:

44: Response.AddHeader ("content-disposition","attachment; filename=\"" + filename + "\"")

Input variable:

HTTP Response Splitting (18)

Request["filename"]

Stack (function/line/file):

0. Response.AddHeader() 43 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\download_file.aspx

User input flow:

0. Request["filename"]
1. filename

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

8. HTTP Response Splitting through Response.Redirect()

Risk:	Code Line:	Vuln ID:
MEDIUM	34	28

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\delete_subscriber.aspx

Vulnerability:

34: Response.Redirect("view_subscribers.aspx?id=" + Request["bg_id"])

Input variable:

Request["bg_id"]

Stack (function/line/file):

0. Response.Redirect() 33 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\delete_subscriber.aspx

User input flow:

0. Request["bg_id"]

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

9. HTTP Response Splitting through Response.Redirect()

Risk:	Code Line:	Vuln ID:
MEDIUM	1186	39

HTTP Response Splitting (18)

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\util.cs

Vulnerability:

1186: Response.Redirect(url + "&url=" + Request.QueryString["url"] + "&qs=" + Request.QueryString["qs"])

Input variable:

Request.QueryString["qs"]

Stack (function/line/file):

0. Response.Redirect() 1185 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\util.cs

User input flow:

0. Request.QueryString["qs"]
1. qs

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

10. HTTP Response Splitting through Response.Redirect()

Risk:	Code Line:	Vuln ID:
MEDIUM	1186	36

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\util.cs

Vulnerability:

1186: Response.Redirect(url + "&url=" + Request.QueryString["url"] + "&qs=" + Request.QueryString["qs"])

Input variable:

Request.QueryString["url"]

Stack (function/line/file):

0. Response.Redirect() 1185 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\util.cs

User input flow:

HTTP Response Splitting (18)

0. Request.QueryString["url"]
1. url

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

11. HTTP Response Splitting through Response.Redirect()

Risk:	Code Line:	Vuln ID:
MEDIUM	1190	40

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\util.cs

Vulnerability:

1190: Response.Redirect(url + "?url=" + Request.QueryString["url"] + "&qs=" + Request.QueryString["qs"])

Input variable:

Request.QueryString["qs"]

Stack (function/line/file):

0. Response.Redirect() 1189 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\util.cs

User input flow:

0. Request.QueryString["qs"]
1. qs
2. url

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

12. HTTP Response Splitting through Response.Redirect()

Risk:	Code Line:	Vuln ID:
MEDIUM	1190	41

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\util.cs

HTTP Response Splitting (18)

Vulnerability:

1190: Response.Redirect(url + "?url=" + Request.QueryString["url"] + "&qs=" + Request.QueryString["qs"])

Input variable:

Request.QueryString["qs"]

Stack (function/line/file):

0. Response.Redirect() 1189 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\util.cs

User input flow:

0. Request.QueryString["qs"]
1. url

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

13. HTTP Response Splitting through Response.Redirect()

Risk:	Code Line:	Vuln ID:
MEDIUM	1186	38

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\util.cs

Vulnerability:

1186: Response.Redirect(url + "&url=" + Request.QueryString["url"] + "&qs=" + Request.QueryString["qs"])

Input variable:

Request.QueryString["url"]

Stack (function/line/file):

0. Response.Redirect() 1185 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\util.cs

User input flow:

0. Request.QueryString["url"]

Filter:

HTTP Response Splitting (18)

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

14. HTTP Response Splitting through Response.Redirect()

Risk:	Code Line:	Vuln ID:
MEDIUM	1186	34

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\util.cs

Vulnerability:

1186: Response.Redirect(url + "&url=" + Request.QueryString["url"] + "&qs=" + Request.QueryString["qs"])

Input variable:

Request.QueryString["qs"]

Stack (function/line/file):

0. Response.Redirect() 1185 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\util.cs

User input flow:

0. Request.QueryString["qs"]
1. qs
2. url

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

15. HTTP Response Splitting through Response.Redirect()

Risk:	Code Line:	Vuln ID:
MEDIUM	1190	45

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\util.cs

Vulnerability:

1190: Response.Redirect(url + "?url=" + Request.QueryString["url"] + "&qs=" + Request.QueryString["qs"])

HTTP Response Splitting (18)

Input variable:

Request.QueryString["qs"]

Stack (function/line/file):

0. Response.Redirect() 1189 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\util.cs

User input flow:

0. Request.QueryString["qs"]
1. qs

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

16. HTTP Response Splitting through Response.Redirect()

Risk:	Code Line:	Vuln ID:
MEDIUM	1186	37

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\util.cs

Vulnerability:

1186: Response.Redirect(url + "&url=" + Request.QueryString["url"] + "&qs=" + Request.QueryString["qs"])

Input variable:

Request.QueryString["qs"]

Stack (function/line/file):

0. Response.Redirect() 1185 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\util.cs

User input flow:

0. Request.QueryString["qs"]

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

17. HTTP Response Splitting through Response.Redirect()

HTTP Response Splitting (18)

Risk:	Code Line:	Vuln ID:
MEDIUM	1190	43

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\util.cs

Vulnerability:

1190: Response.Redirect(url + "?url=" + Request.QueryString["url"] + "&qs=" + Request.QueryString["qs"])

Input variable:

Request.QueryString["qs"]

Stack (function/line/file):

0. Response.Redirect() 1189 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\util.cs

User input flow:

0. Request.QueryString["qs"]

Filter:

No mitigating factors, input variable did not pass through ASP.Net input validation functions.

18. HTTP Response Splitting through Response.Redirect()

Risk:	Code Line:	Vuln ID:
MEDIUM	151	31

File:

E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\security.cs

Vulnerability:

151: Response.Redirect(target)

Input variable:

Request

Stack (function/line/file):

0. Response.Redirect() 150 E:\ADVISORIES_SOURCE\btnet_3.5.4\www\App_Code\security.cs

User input flow:

HTTP Response Splitting (18)

0. Request
1. original_querystring
2. target

Filter:

No mitigating factors. Input variable passed some security filters, but not for this vulnerability type.