Apache Website CVE-2007-5000 :
….a cross-site scripting attack is possible….

NVD CVE-2007-5000: a Cross-site scripting (XSS) vulnerability in the ….mod_imap module….

Source Code Repository developer fix documentation: Fix cross-site-scripting issue by escaping the URI…

Source Code Repository Code Difference:

```
File: mod_imagemap.c
Line 485 and 490 modified to
escape html in URI:
ap_escape_html(r->pool, r->uri)
```

CAPEC-63: Simple Script Injection:
(Experimentation) Use a list of XSS probe strings to inject script into resources accessed by the application
(Exploit) Develop malicious JavaScript that is injected through vectors identified during the Experiment Phase

Source Code Repository developer fix documentation:
….ensure that a charset parameter is sent in the content-type …

Source Code Repository Code Difference:

```
File: mod_imagemap.c
Line 482 modified to contain an explicit character set:
ap_set_content_type(r, "text/html;charset=ISO-8859-1");
```

CAPEC-43: Exploiting Multiple Input Interpretation Layers:
(Experimentation) Determine which character encodings are accepted by the application/system:
(Exploit) Perform XSS attacks

1

2

FAILURE TO PRESERVE GENERATED WEB PAGE STRUCTURE #79-87 #113 #442 #692 #644

FAILURE TO SANITIZE USER INPUT OF SYNTAX THAT HAS IMPLICATIONS IN A DIFFERENT PLANE #74 #94 #99 #138

IMPROPER ENFORCEMENT OF MESSAGE OR DATA STRUCTURE #707

IMPROPER-INPUT-VALIDATION #20 #554

IMPROPER CLEANSING AND CANONICALIZATION #171

PERMISSIVE WHITELIST #183

INCOMPLETE BLACKLIST #184

IMPROPER SANITIZATION OF SPECIAL ELEMENTS #138 #75 #140-169

IMPROPER COLLAPSING OF PATH NAMES #182

MISSING INITIALIZATION #456

FAILURE TO SANITIZE CRLF SEQUENCES #93 #113

INCORRECT REGULAR EXPRESSION #185 #186

VALIDATING DATA BEFORE CANONICALIZING OR FILTERING #179 #180 #181

IS-A

CAN-PRECEDE

WEAKNESS

ELEMENTS OF USER-CONTROLLED DATA HAVE IMPLICATIONS IN A DIFFERENT PLANE #74

3

Apache Website CVE-2007-5000 : ….a cross-site scripting attack is possible….

NVD CVE-2007-5000 : allows remote attackers to **inject**…

OCCURS-IN

RESOURCE/

4

Source Code Repository developer fix documentation: Fix cross-site-scripting issue by escaping the URI…

Source Code Repository Code Difference:

```
File: mod_imagemap.c
Line 485 and 490 modified to escape html
in URI:
ap_escape_html(r->pool, r->uri)
```

URI #84

WEB PAGE #79

WEB RESOURCES #442

USER-CONTROLLED INPUT DATA #74

ERROR PAGE #81

INPUT FIELDS, HIDDEN FIELDS & ATTRIBUTES #80 #82 #83 #85 #87

IDENTIFIERS #86

COOKIES #565

RESOURCE IDENTIFIERS #99

QUERY

COMMAND #77

GENERATED CODE #94

EXECUTABLE REGULAR EXPRESSION #624

FORMAT STRING # 134

OS COMMANDS /SHELL #78

PART-OF

IS-A

CAN-PRECEDE

CONSEQUENCES

EXECUTION OF ARBITRARY USER-CONTROLLED DATA #20 #74 #77 #94

CHANGE PROCESS FLOW #74

UNAUTHORIZED DATA RECALL AND WRITING #74 #77 #93 #94

EXCESSIVE CONSUMPTION OF RESOURCES OR CRASH #20

UNACCOUNTED ACTIONS #74 #94

CONTROL OF AUTHENTICATION #74 #94

5

NVD CVE-2007-5000 :
…..allows remote attackers to **inject arbitrary web script or HTML**….

6

NVD CVSS CVE-2007-5000 impact type : Allows unauthorized modification