

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:

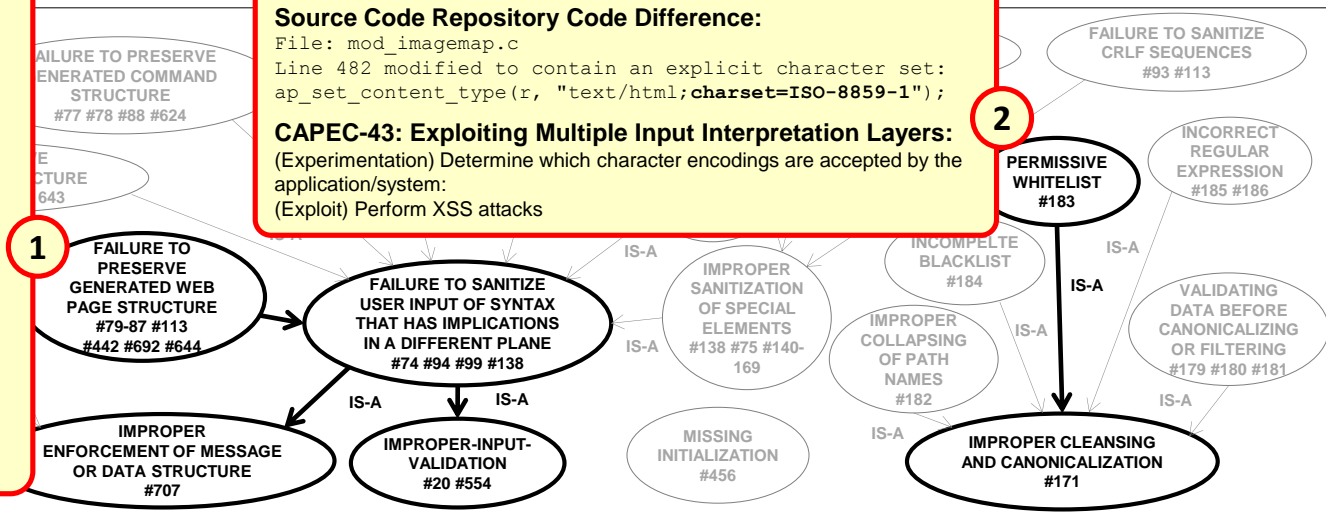
...ensure that a charset parameter is sent in the content-type ...

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

3

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

NVD CVE-2007-5000 : allows remote attackers to inject...

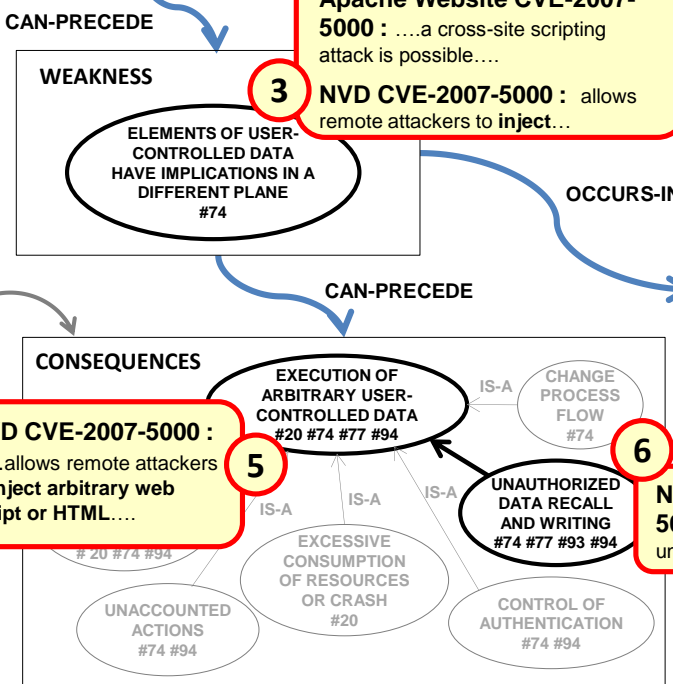
Source Code Repository developer fix documentation:

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)`

4

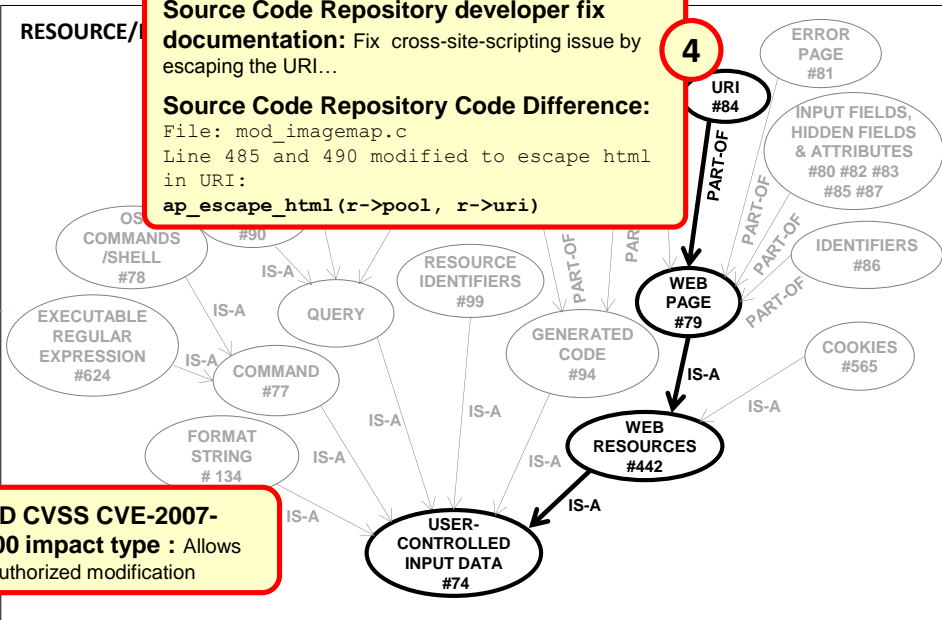


5

6

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

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



4

6