Security Assessment for http://yehg.net

Summary

Site:	**http://yehg.net**
Methodology used:	**PortSwigger**
Number Of Tests:	**69**
Number Of Flaws:	**20**
Date: (mm/dd/yyyy)	**6-23-2008**
Penetration Tester:	**d0ubl3_h3lix**

Problems Identified

Flaw 1. **Hidden & default content** — Refer to Test 2

Flaw 2. **Data entry points** — Refer to Test 4

Flaw 3. **Account recovery function** — Refer to Test 9

Flaw 4. **Impersonation function** — Refer to Test 11

Flaw 5. **Fail-open conditions** — Refer to Test 14

Flaw 6. **Multi-stage mechanisms** — Refer to Test 15

Flaw 7. **Tokens predictability** — Refer to Test 17

Flaw 8. **Disclosure of tokens in logs** — Refer to Test 19

Flaw 9. **Session termination** — Refer to Test 21

Flaw 10. **SQL injection** — Refer to Test 29

Flaw 11. **HTTP header injection** — Refer to Test 32

Flaw 12. **Arbitrary redirection** — Refer to Test 33

Flaw 13. **SOAP injection** — Refer to Test 41

Flaw 14. **LDAP injection** — Refer to Test 42

Flaw 15. **Logic attack surface** — Refer to Test 44

Flaw 16. **Transmission of data via client** — Refer to Test 45

Flaw 17. **Dangerous HTTP methods** — Refer to Test 57

Flaw 18. **Sensitive data in URL parameters** — Refer to Test 66

Flaw 19. **Forms with autocomplete enabled** — Refer to Test 67

Flaw 20. **Information leakage** — Refer to Test 68

Results Detailed

† Recon and analysis †

Test 1. **Map visible content**

Vulnerable? **NO**

Test 2. **Discover hidden & default content**

Vulnerable? **YES**

Test 3. **Test for debug parameters**

Vulnerable? **NO**

Result/Note:

Result/Note may be

----

* Notes for this test.

* Fixes for this test.

* Findings for this test. - can contain attack/response strings

?admin=1

?str="><script>alert(0)//</script><!---

Test 4. **Identify data entry points**

Vulnerable? **YES**

Test 5. **Identify the technologies used**

Vulnerable? **NO**

Test 6. **Test password quality rules**

Vulnerable? **NO**

† Test handling of access » Authentication †

Test 7. **Test for username enumeration**

Vulnerable? **NO**

Test 8. **Test resilience to password guessing**

Vulnerable? **NO**

Test 9. **Test any account recovery function**

Vulnerable? **YES**

Test 10. **Test any `remember me` function**

Vulnerable? **NO**

Test 11. **Test any impersonation function**

Vulnerable? **YES**

Test 12. **Test username uniqueness**

Vulnerable? **NO**

Test 13. **Check for unsafe distribution of credentials**

Vulnerable? **NO**

Test 14. **Test for fail-open conditions**

Vulnerable? **YES**

Test 15. **Test any multi-stage mechanisms**

Vulnerable? **YES**

† Test handling of access » Session handling †

Test 16. **Test tokens for meaning**

Vulnerable? **NO**

Test 17. **Test tokens for predictability**

Vulnerable? **YES**

Test 18. **Check for insecure transmission of tokens**

Vulnerable? **NO**

Test 19. **Check for disclosure of tokens in logs**

Vulnerable? **YES**

Test 20. **Check mapping of tokens to sessions**

Vulnerable? **NO**

Test 21. **Check session termination**

Vulnerable? **YES**

Test 22. **Check for session fixation**

Vulnerable? **NO**

Test 23. **Check for cross-site request forgery**

Vulnerable? **NO**

Test 24. **Check cookie scope**

Vulnerable? **NO**

† Test handling of access » Access controls †

Test 25. **Understand the access control requirements**

Vulnerable? **NO**

Test 26. **Test effectiveness of controls, using multiple accounts if possible**

Vulnerable? **NO**

Test 27. **Test for insecure access control methods (request parameters, Referer header, etc)**

Vulnerable? **NO**

† Test handling of input †

Test 28. **Fuzz all request parameters**

Vulnerable? **NO**

Test 29. **Test for SQL injection**

Vulnerable? **YES**

Test 30. **Identify all reflected data**

Vulnerable? **NO**

Test 31. **Test for reflected XSS**

Vulnerable? **NO**

Test 32. **Test for HTTP header injection**

Vulnerable? **YES**

Test 33. **Test for arbitrary redirection**

Vulnerable? **YES**

Test 34. **Test for stored attacks**

Vulnerable? **NO**

Test 35. **Test for OS command injection**

Vulnerable? **NO**

Test 36. **Test for path traversal**

Vulnerable? **NO**

Test 37. **Test for script injection**

Vulnerable? **NO**

Test 38. **Test for file inclusion**

Vulnerable? **NO**

Test 39. **Test for SMTP injection**

Vulnerable? **NO**

Test 40. **Test for native software flaws (buffer overflow, integer bugs, format strings)**

Vulnerable? **NO**

Test 41. **Test for SOAP injection**

Vulnerable? **YES**

Test 42. **Test for LDAP injection**

Vulnerable? **YES**

Test 43. **Test for XPath injection**

Vulnerable? **NO**

† Test application logic †

Test 44. **Identify the logic attack surface**

Vulnerable? **YES**

Test 45. **Test transmission of data via the client**

Vulnerable? **YES**

Test 46. **Test for reliance on client-side input validation**

Vulnerable? **NO**

Test 47. **Test any thick-client components (Java, ActiveX, Flash)**

Vulnerable? **NO**

Test 48. **Test multi-stage processes for logic flaws**

Vulnerable? **NO**

Test 49. **Test handling of incomplete input**

Vulnerable? **NO**

Test 50. **Test trust boundaries**

Vulnerable? **NO**

Test 51. **Test transaction logic**

Vulnerable? **NO**

† Assess application hosting †

Test 52. **Test segregation in shared infrastructures**

Vulnerable? **NO**

Test 53. **Test segregation between ASP-hosted applications**

Vulnerable? **NO**

Test 54. **Test for web server vulnerabilities**

Vulnerable? **NO**

Test 55. **Default credentials**

Vulnerable? **NO**

Test 56. **Default content**

Vulnerable? **NO**

Test 57. **Dangerous HTTP methods**

Vulnerable? **YES**

Test 58. **Proxy functionality**

Vulnerable? **NO**

Test 59. **Virtual hosting mis-configuration**

Vulnerable? **NO**

Test 60. **Bugs in web server software**

Vulnerable? **NO**

† Miscellaneous tests †

Test 61. **Check for DOM-based attacks**

Vulnerable? **NO**

Test 62. **Check for frame injection**

Vulnerable? **NO**

Test 63. **Check for local privacy vulnerabilities**

Vulnerable? **NO**

Test 64. **Persistent cookies**

Vulnerable? **NO**

Test 65. **Caching**

Vulnerable? **NO**

Test 66. **Sensitive data in URL parameters**

Vulnerable? **YES**

Test 67. **Forms with autocomplete enabled**

Vulnerable? **YES**

Test 68. **Follow up any information leakage**

Vulnerable? **YES**

Test 69. **Check for weak SSL ciphers**

Vulnerable? **NO**

Generated by YEHG.Net Report Generator