Testing Web-based Systems cont …

Prof. Durga Prasad Mohapatra
Professor
Dept.of CSE, NIT Rourkela

Navigation Testing

- Navigation testing is performed on various possible paths in web applications
  - to ensure the functioning of correct sequence of navigations
- Design the test cases such that the following navigations are correctly executing :
  - Internal links & External links
  - Redirected links (the redirected links should be with proper messages displayed to the user)
  - Navigation for searching inside the web application

Navigation Testing cont…

- The errors must be checked for the followings:
  - The broken links (the links should not be broken due to any reason).
  - The proper redirected links with proper messages displayed
  - Ensuring whether all possible navigation paths active and relevant or not.
  - The navigations for the back and forward buttons, and their proper working

Configuration/Compatibility Testing

- Diversity in configuration for web applications makes the testing of these systems very difficult.
- There may be various types of :
  - Browsers supporting different operating systems
  - Variation in servers
  - Networks, etc.

Configuration/Compatibility Testing cont …

- Therefore, configuration testing becomes important so that there is compatibility between various available resources and application software.
- The tester must consider these configurations and compatibility issues
  - so that they can design the test cases incorporating all the configurations.

Configuration/Compatibility Testing cont …

Some important points for configuration testing:

- There are a number of different browsers and browser options.
  - The web application has to be designed to be compatible for majority of the browsers.

Configuration/Compatibility Testing cont …

- The graphics and other objects on a website have to be tested on multiple browsers.
  - If more than one browser will be supported, then the graphics have to be visually checked for differences in the physical appearance.
  - Some of the things to check are
    - ✓ centering of objects,
    - ✓ table layouts,
    - ✓ colours,
    - ✓ monitor resolution,
    - ✓ forms and
    - ✓ buttons

Configuration/Compatibility Testing cont …

- The code that executes from the browser also has to be tested.
  - There are different versions of HTML.
  - They are similar in some ways

    but they have different tags which may produce different features.

Configuration/Compatibility Testing cont …

- Some of the other codes, besides HTML, to be tested are
  - ✓ Java
  - ✓ JavaScript
  - ✓ ActiveX
  - ✓ VBScripts
  - ✓ Cgi-Bin Scripts
  - ✓ Database access
- Cgi-Bin Scripts have to be checked for end-to-end operations and is most essential for e-commerce sites.
- The same goes for database access.

Configuration/Compatibility Testing cont …

- All new technologies used in the web development like graphics designs, interface calls like different API's, may not be available in all the operating systems.
  - Test your web application on different operating systems:
    - ✓ Windows,
    - ✓ Unix,
    - ✓ MAC,
    - ✓ Linux,
    - ✓ Solaris with different OS flavors.

Security Testing

- The most challenging issue is to protect the web applications from
  - Hackers
  - Crackers
  - Spoofers
  - Virus launchers, etc.

Security Testing

cont …

- Through security testing we try to ensure:
  - Confidentiality
  - Integrity
  - Availability
  - Non Repudiation
- The web application must be able to nullify the external attacks

Security Test Plan

- Security testing is carried out for:
  - Security of the infrastructure hosting the web application
  - Vulnerabilities of the web application
- Firewall and port scans can be the solutions for security infrastructure
- For vulnerabilities, user authentication, restricted and encrypted use of cookies, data communication must be planned. Users should not be able to browse through the directories in the server.

Security Test Plan cont …

- Check the interfaces of the components, because most of the security bugs lie on the interfaces only.
- Prioritize the interfaces according to their level of vulnerability.
- High-priority interfaces are tested thoroughly by injecting mutated data to be accessed by that interface in order to check the security.

Security Test Plan cont …

- While performing security checking, do not modify
  - the configuration of the system or server,
  - services running on the server, and
  - existing user or customer data hosted by the application.

Various Threat types and their Corresponding Test Cases

- Unauthorized users/fake identity/password cracking
  - check for the confidentiality of the contents/data.
- Buffer overflows
  - Due to this malicious code can be executed
  - Check the buffer overflow module and the different ways of submitting a range of lengths to the application

Threats and their Test Cases cont..

- URL manipulation
  - Web application uses HTTP GET method to pass information between the client and server. The information is passed through parameters in the query string. An attacker may change some information in the query string passed from GET request so that he may get some information or corrupt the data. When somebody attempts to modify the data, it is known as fiddling of data.
  - Prevent fiddling in the HTTP GET query string for the change or corruption of the data.
  - Design test cases to check that an user is trying to modify the private information.

Threats and their Test Cases cont..

- SQL injection
  - Hackers can put some SQL statements through the web interface (inputs) to get vital information
  - Design test cases such that the special characters from the user inputs should be handled/escaped properly.

Threats and their Test Cases cont …

- Denial of service (DoS)

When a service does not respond, it is known as denial of service

  - There are several ways that can make an application fail:
    - Heavy load
    - Distorted data that may crash an application
    - Overloading of memory, etc.
  - Testers should design the test cases considering all the above factors.

Threats and their Test Cases cont …

- Cross-Site Scripting (XSS)
  - When a user inserts HTML/client side script in the user interface of a web application and this insertion is visible to other users, it is called cross-site scripting (XSS).
  - Using XSS, the attacker can use scripts like Java Scripts to steal user cookies and information stored in the cookies.
  - To avoid this, tester should check web application for XSS.

Performance Testing

- Performance testing helps the developer to identify the bottlenecks in the web application and can be rectified.
- The bottlenecks can be
  - code,
  - database,
  - network,
  - peripheral devices, etc.

Performance Parameters

- Resource Utilization
  - The percentage of time a resource(CPU, memory, I/O, Peripheral, Network) is busy.
- Throughput
  - The number of event responses that have been completed over a given interval of time.
- Response time
  - The time lapsed between a request and its reply.

Performance Parameters cont …

- Round-Trip Time
  - How long does the entire user-requested transaction take, including connection and processing time?
- Scalability
  - The ability of an application to handle additional workload, without adversary affecting performance, by adding resources such as processor, memory, and storage capacity.
- Database load
  - The number of times database is accessed by web application over a given interval of time.

Types of Performance Testing for web applications

- Load Testing
- Stress Testing

Load Testing

- This testing is performed to check that whether the system can sustain at times of peak load.
- The site should handle many simultaneous user requests, large input data from users, simultaneous connections to database, heavy load on specific pages, etc. When we test the system with these types of loads, this testing is called load testing.
- It focuses on determining or validating performance characteristics of the system when subjected to workloads & load volumes expected during production operations. It refers to how much maximum load can be put on the web application & it will still serve flawlessly (e.g. 10 concurrent users).

Types of load testing

- Capacity testing
  - Determines the maximum load the web service can handle before failing.
  - Reveals the web services' ultimate limit.
- Scalability testing
  - Determines how effectively the web service will expand to accommodate an increasing load.

Stress Testing

- Stress refers to stretching the system beyond its specification limits.
- Web stress testing is performed to break the site by giving stress and to know how the system reacts to the stress and how the system recovers from crashes.
- It focuses on determining or validating performance characteristics of the system when subjected to conditions beyond those expected during production operations.
- Tests the performance of the system under stressful conditions such as
  - memory overflow,
  - insufficient disk space,
  - server failure etc.

Stress Testing cont …

- These tests are designed to determine under what conditions an application will fail, and how gracefully it may recover from failure.
- Examples of graceful failure:
  - The system saves the state at the time of failure and does not crash suddenly
  - On restarting it, the system recovers from the last good state
  - The system shows meaningful error messages to the user, etc.

Summary

- Discussed the following types of testing for web-based systems:
  - Navigation Testing
  - Configuration/Compatibility Testing
  - Security Testing
  - Performance Testing

References

1. Naresh Chauhan, Software Testing: Principles and Practices, (Chapter – 15), Second Edition, Oxford University Press, 2018.

Thank You