ISSN:0975-9646

Web Development and Cryptography

Prof.Pranit Gaikwad[1], BhavyaGoradia[2], Prashanti Bhatt[3]

Assistant professor,
Universal College of Engineering
Kaman, Vasai, India.

[2,3] B. E Computer Science
Universal College of Engineering
Kaman, Vasai, India.

Abstract-Web applications are one of the most ubiquitous platforms for information and service delivery in internet today. Web development from the day of introduction of "www" involved developing tools, languages, security processes to ensure that the web site is user friendly. Today languages and web developing tools have evolved and are known to everyone considering security aspects. Web Sites need to be interactive and secured and should follow security protocols to ensure the proper quality of services and end-user loyalty. All web services follow co-ordination protocols and enhance service execution to the customers. A part of web sitedevelopment includes multimedia development which plays an important role for User interfacing. Privacy, Security and better UI is what a consumer expects.As they are increasingly used for critical services, web applicationshave become a popular and valuable target for security attacks.

Some web developing technologies involve Mark-up languages and Stylesheets, Scripting and Extensive Mark-up formats and frameworks developing tools, Server site languages. Such Languages includes HTML, CSS, PHP, AJAX, JAVASCRIPT etc. All these together help a website look more attractive, responsive and easy to use.

Keywords- Web development, Co-ordination protocols, Consumer loyalty, Service execution, Multimedia Development, Security.

INTRODUCTION

Today, Web sites being developed for e-commerce, advertising purposes or social networks are developed using various web developing languages combined together and hence show a better interface. The ultimate goal of developing websites is to make data available to all users/consumers globally and provide access to it.

Web development languages are used for creating a better UI.A better UI increases the probability of a customer visiting the website.

Web development is a broad term and can be accessed in two ways namely internet and intranet.

For any website, there are some protocols followed and from developers' side it is necessary that they provide better QoS to consumers by maintaining their data security and accessibility. Some aspects of web development are:

1) *Quality of Services*
2) *Web Transactions*
3) *Web Security*
4) *User Interface*
5) *Service Execution*
6) *Multimedia Development*
7) *Web Co-ordination Protocols*
8) *Web Development Languages*
9) *Consumer Loyalty*
10) *Security Algorithms*

Websites now can be accessed using cell phones and even laptops and desktops.

Following are some factors for better outputs for websites:

Ease of finding data	76%
Beautiful Appearance	10%
Interactive Experience	9%
Other Aspects	5%

Some risk factors for web site include:
Authentication
Authorization and Access management
Session Management
knowledge and Input Validation
Cross website Scripting (XSS)
Command Injection Flaws
Buffer Overflows
Error Handling
Logging
Remote Administration
internet Application and Server Configuration

WEB DEVELOPING LANGUAGES

Following are Languages used for web development which also can be said to be web developing tools for both front end and back end purposes or for multimedia as well:

1) HTML
2) CSS
3) JAVASCRIPT
4) AJAX
5) PHP

HTML

HTML is a mark-up language use for front end purpose and basically used for static websites.HTML used along Cascaded Stylesheet and JavaScript forms a cornerstone for any web application or a website.

Elements of HTML are the building blocks for any HTML page along with its pre-defined tags. HTML can be used to interpret or compose text inform of written/audible/visual format.

Sample Code for HTML:

```
<!doctype html>
<html>
<head>…. </head>
<title>HTML</title>
<body>
.
.
.
.
.
</body>
</html>
```

All the texts described insde “<>” are the predefined tags.

VERSIONS OF HTML

HTML 1.0 (1989 - 1994)

The first version of hypertext mark-up language that supported inline pictures and text controls. HTML 1.0 was terribly restricted in terms of styling and presentation of content. In HTML 1.0, for instance, you'll not:

use tables or frames,
specify fonts,
change page background, or
use forms

HTML 2.0 (1995)

This specification supported a lot of browsers. HTML 2.0 was significantly improved to support: It conjointly supported:

forms with restricted set of type parts like text boxes, and possibility buttons
change of page background
use of tables

HTML 3.20 (1997)

This version enclosed support for making tables and enlarged choices for type parts. This version conjointly allowed websites to incorporate advanced mathematical equations.

Notes:

Because W3C delayed agreeing on subsequent version (after hypertext mark-up language two.0) of HTML, HTML 3.2 was created rather than hypertext mark-up language three.0.

Although hypertext mark-up language three.20 specifications enclosed support for CSS (cascaded vogue sheets), browser manufactures didn't support it fine in their browsers.

Browser manufactures enclosed support for frames even supposing hypertext mark-up language three.2 specifications didn't support this feature.

HTML 4.01 (1999)

This version supplementary support for vogue sheets and scripting ability for multimedia system parts. Itcentred on separating presentation styling info from the particular content by the utilization of fashion sheets. In HTML 4.0 with the utilization of fashion sheets, it's currently potential to vary the appearance/look of the web site by ever-changing simply the design sheet (s) itself.

XHTML

It is a wholly new branch of hypertext mark-up language, incorporating the rigours of XML, so code should be properly written if it's to figure once it reaches the reader’s browser. There weren’t several new or deprecated tags and attributes in XHTML, however some things modified with a read of inflated accessibility and practicality. It’s chiefly simply a replacement set of committal to writing rules.

HTML5

The path that XHTML two was taking began to look each boring and surreal, and it became pretty clear that a replacement approach was required. It was around now that a replacement specification was developed.HTML5 is intended for the online, each currently and within the future. this is often the specification that we are going to be operating with for subsequent decade a minimum of, therefore the method of its development is comparatively slow and regarded.

CSS

CSS is Cascaded Stylesheet, used for styling and is a stylesheet language for showing the representation of data. CSS enables separation of document data and document presentation. CSS elements can be linked with HTML page using three methods namely, a) inline, b) interior, c) exterior.

Sample Code for CSS:

```
body {
  background-color: lightblue;
}

h1 {
 color: white;
  text-align: center;
}

p {
  font-family: veranda;
  font-size: 20px;
}
```

This code is an external document linked with HTML using Href.

VERSIONS OF CSS

CSS 1

The first CSS specification to become a political candidate W3C Recommendation is CSS level one, printed on Dec seventeen, 1996. Among its capabilities square measure support for

Font properties like type and stress
Color of text, backgrounds, and alternative components
Text attributes like spacing between words, letters, and contours of text
Alignment of text, images, tables and alternative components
Margin, border, padding, and positioning for many components
Unique identification and generic classification of teams of attributes

CSS 2

CSS level a pair of specification was developed by the W3C and printed as a recommendation in could 1998. CSS a pair of includes variety of latest capabilities like absolute, relative, and stuck positioning of components and z-index, the construct of media varieties, support for aural vogue sheets (which were later replaced by the CSS three speech modules) and bidirectional text, and new font properties like shadows.

CSS 2.1

CSS 2.1 may be a sheet of paper language that permits authors and users to connect vogue to structured documents. By separating the presentation variety of documents from the content of documents, CSS a pair of simplifies internet authoring and web site maintenance. It supports media-specific vogue sheets in order that authors could tailor the presentation of their documents to visual browsers, aural devices, printers, braille devices, hand-held devices, etc. It conjointly supports content positioning, table layout, options for internationalisation and a few properties associated with interface. CSS 2.1 corrects a couple of errors in CSS2 (the most vital being a brand new definition of the height/width of fully positioned components, a lot of influence for HTML's "style" attribute and a brand new calculation of the 'clip' property)

CSS 2.2

CSS 2.2 is that the second revision of CSS level a pair of. CSS level a pair of supports media-specific vogue sheets in order that authors could tailor the presentation of their documents to visual browsers, aural devices, printers, braille devices, hand-held devices, etc. It conjointly supports content positioning, table layout, options for internationalisation and a few properties associated with interface.

CSS 3

CSS3 has been split into "modules". It contains the "old CSS specification" (which has been split into smaller pieces). additionally, new modules square measure other.
Some of the foremost necessary CSS3 modules are:
Selectors
Box Model
Backgrounds and Borders
Image Values and Replaced Content
Text Effects
2D/3D Transformations
Animations
Multiple Column Layout
User Interface
Advertisement

JAVASCRIPT

JAVASCRIPT is a scripting language used along with HTML to check conditions and verification purposes.

AJAX

AJAX is a web development language which enables client side to run their own applications and to create asynchronous web processes. Which is done using various web technologies.

PHP

PHP is Hypertext Pre-processor. It is a server scripting language used for dynamic websites.

QUALITY OF SERVICES

The major requirements for supporting QoS in Web services are as follows:

Availability: Availableness represents that the web site is obtainable or not in achievement and also the time it takes to load. A proper web site ought to be accessible all the time and its TTR i.e. Time to Repair ought to be as low as attainable.
Availability deals with quality a part of an internet site.
All the services of an internet site ought to be accessible all the time.

Accessibility: Accessibility, another quality a part of service wherever it deals with however simply and firmly the info is accessed. net service request. will be expressed in from wherever the info is definitely and with success accessible and extracted. There can be things once an internet service is obtainable however not accessible. High accessibility of net services will be achieved by building extremely ascendable systems. the flexibility to feature capability (and users) to a deployed system over time. quantifiably usually involves adding resources to the system however mustn't need changes to the preparation design.

Integrity: Integrity deals with the correctness of the info and. Is an additional quality side correct execution of net service transactions can give the correctness of interaction. A dealing refers to a sequence of activities to be treated as one unit of labor. All the activities have to be compelled to be completed to create the dealing winning. once a dealing doesn't complete, all the changes created ar rolled back.

Performance: Performance is that the quality side of net service, that is measured in terms of turnout and latency. Higher the turnout and lower the latency higher the web site performs.

Reliability: Responsibility is that the quality side of an internet service that deals with the potential of conjugation of an internet site. the amount of failures per month or year represents a live of responsibility of an internet service. In another sense, responsibility refers to the assured and ordered delivery for messages being sent and received by service requestors and repair suppliers.

Regulatory: restrictive is that the quality side of the net service in agreement with the principles, the law, compliance with standards, and also the established service level agreement. net services use lots of standards like SOAP, UDDI, and WSDL. Strict adherence to correct versions of standards (for example, SOAP version one.2) by service suppliers is important for correct invocation of net services by service requestors.

Security: Security could be a complicated topic that involves all levels of a deployed system. Developing security needs revolves around distinctive the safety threats and developing a method to combat them. This security analysis includes the subsequent steps:
1. distinctive crucial assets
2. distinctive threats to those assets
3. distinctive vulnerabilities that expose the threats that make risk to the organization
4. Developing a security arrange that mitigates the chance to the organization

WEB TRANSACTIONS AND SECURITY

For any online transactions, it is necessary to have security to avoid data loss or any other kind of integrity failure. A powerful transaction security server capable of providing secured two-factor authentication, SSL, and digital signature capabilities for any web service regardless of application platform is needed.

USER INTERFACE AND MULTIMEDIA

User Interface plays an important role for any web site. The more attractive it is the more the user feels to visit the website.
Multimedia in Web Page can be in the audio or visual form which can be collaborated with web pages, hence enabling users to use that media and entertain themselves.

WEB CO-ORDINATION PROTOCOLS

Web Coordination protocols play a vital role for any online page and embody cache communication protocols. a number of them like WCCP deals with traffic handling of net cache/proxy with sure protocol versions are:

1) WCCPv1

- Single router services a cluster system.
- Only supports hypertext transfer protocol communications protocol Port eighty
- Provides Generic Routing Encapsulation.
- Routers and cache engines communicate to every different via an impact channel supported UDP port 2048

2) WCCPv2

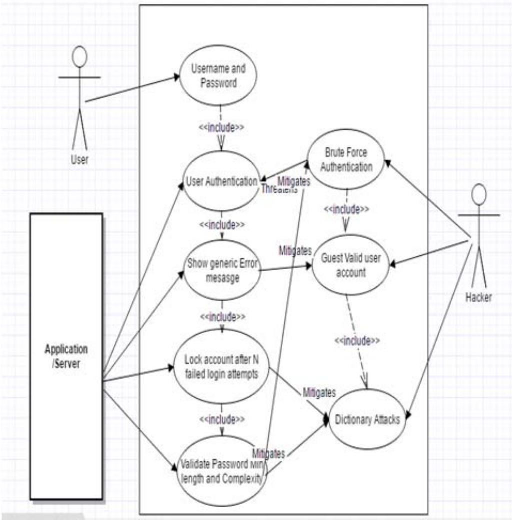
- Allows spend to thirty two Routers.
- Supports up to thirty two engines.
- Supports any information processing protocol as well as any communications protocol or UDP
- Supports up to 255 service teams (0-254)
- Adds MD5 shared secret security

WEB SECURITY AND ALGORITHMS

Web Security is a vital consider maintaining the integrity of websites and applications. It additionally helps avoiding knowledge loss and protocol of shopper loyalty, thus preventing group action failures. If websites aren't secured, they fail to make sure shopper security. thus there are some net security algorithms wont to guarantee security.
It will be explained in terms of vulnerability.
The 3 most identified vulnerabilities are:
1) SQL Injection
2) Cross website Request Forgery
3) Cross website Scripting

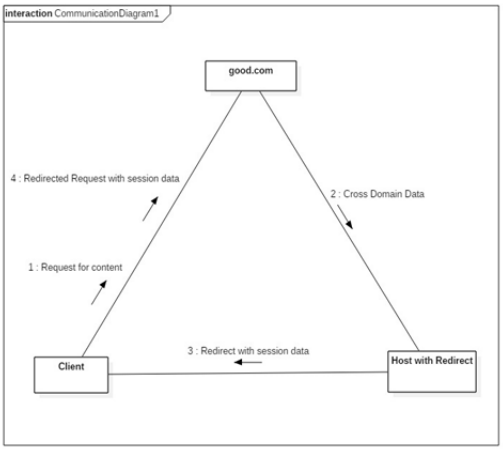
SQL INJECTION

a) Browser sends malicious input to server due to which malicious data is interpreted in the query.



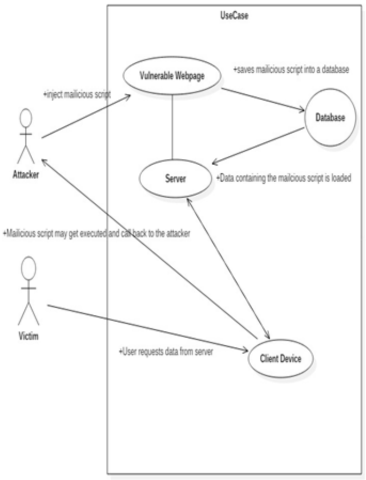
CROSS SITE REQUEST FORGERY

a) Bad website sends browser request to good website due to which credentials of innocent victims are affected.


interaction CommunicationDiagram1
good.com
4 : Redirected Request with session data
2 : Cross Domain Data
1 : Request for content
3 : Redirect with session data
Client
Host with Redirect

CROSS SITE SCRIPTING

a) Bad website sends innocent victim a script which on using steals information from original website.


UseCase
Vulnerable Webpage
+saves mailicious script into a database
+inject mailicious script
Database
Attacker
Server
+Data containing the mailcious script is loaded
+Mailicious script may get executed and call back to the attacker
Victim
+User requests data from server
Client Device

CRYPTOGRAPHIC ALGORITHMS FOR SAFEGAURDING DATA

HTTPS

Trivial transactions can be done using HTTP. However, for transactions where more sensitive data is to be handled HTTPS is used.

When a securedwebsite is visited, browser represents a padlock on the address bar. When receives an SSL certificate from web server. Along with this a public key is provided by the browser to encrypt messages that are sent to server.

PUBLIC OR PRIVATE KEY CRYPTOGRAPHY

There square measure ways that in wherever sensitive info is sent across associate insecure network mistreatment - isobilateral key or uneven keys.

In the symmetric key methodology, identical secret is wont to each encode and rewrite. Suppose if Desires to send a secret message to B. Then A will place the key message in an exceedingly box and place a padlock on it box together with his key (encryption). He then sends the box through regular mail to B. B encompasses a copy of the key that a second hand and once B receives the box he will open it together with his key and browse the message (decryption). the matter with this methodology is the way to provide B a replica of the key that a second hand.

In the uneven key methodology there square measure 2 keys - a public key and a non-public key. Within the on top of state of affairs A desires to send a secret message to B and he lets B understand that. thus B sends A associate open padlock. A then puts that padlock on the box containing the key message and sends the box by regular mail. once B receives it, he will open the padlock since solely he has the key. In different words, B sends his public key. A encrypts the message with this public key and sends it to B. B decrypts the message together with his personal key. the tactic works as a result of possessing the general public key doesn't let anyone rewrite the encrypted message therewith key. Itwill solely be decrypted with the personal key. the safety of this methodology lies in however safe Bwill keep his personal key.

There is another protocol that one will use - three-pass protocol - that doesn't involve causation keys across the network. associate analogy can even facilitate justify this methodology. If A desires to send a secret message to B he will send it in an exceedingly box together with his padlock. once B receives the box he sends it back to A with a padlock of his own. when receiving the box, A removes his padlock and returns the box to B. B will currently open the box as a result of it's solely his padlock on that.RSA algorithmic rule RSA standing for the surnames of Bokkos Rivest, Adi Shamir, and Dutch Leonard Adleman . It shows and works in an exceedingly unidirectional perform that is traightforward to work out however exhausting to invert. Consider associate example wherever we have a tendency to take product of 2 prime numbers however it's tough to separate its factors, explained below:

Choose 2 massive and Distinct Prime Numbers,
Let them be P and Q
Multiply them
N=P*Q
Compute integers but N however are co-prime with N,
N=(P-1) *(Q-1)
Choose associate number E specified,
1<E<N
Choose a price for D that satisfies

(D*E) %N=1
Public secret is (E, N)
Private secret is (D, N)
Encrypt M mistreatment public key C= machine
Decrypt C mistreatment personal key M=CD%N

Encryption mistreatment public keys is often computationally intensive. So, in observe the sender encrypts the message with a secret key that's every which way generated. the key secret is encrypted mistreatment the general public key of the recipient and sent with the encrypted message. The recipient decrypts the key key mistreatment his personal key and mistreatment that decrypts the remainder of the message. the subsequent lists all the steps within the process:

- The consumer and server bear a acknowledgement procedure.
- The shake begins once the consumer connects to a SSL enabled server requesting a secure association and presents a listing of secret writing algorithms and hash functions that it supports.
- From this list the server chooses the foremost secure secret writing algorithmic rule and hash perform that it additionally supports and lets the consumer realize its selection.
- In the on top of dealing, the server additionally sends it identification within the type of a digital certificate. The digital certificate contains the server's name, the trusty Certificate Authority, and therefore the server's public secret writing key.
- The consumer might contact the trusty Certificate Authority for verification.
- The consumer generates a random variety and encrypts it with the server's public key and sends it to the server. solely the server will rewrite this with its personal key.
- The random variety generated by the consumer is then employed in the secret writing and decoding method on each the consumer and server sides**.**

DIGITAL CERTIFICATE

Authenticates a person/organization on internet. It verifies that the public key belongs only to an individual. It is verified by digital certification authority and can be revoked if private key is compromised and there is a revoked certification list maintained.

It works on three algorithms:

a) Key Generation algorithm that randomly uses key pair
b) Signature Algorithm on input generates a signature.
c) Signature verifying algorithm that on input verifies key and signature decides to accept or reject.

CRYPTOGRAPHIC HASH FUNCTION

Takes an input of any length and returns an output of fixed size. String is in form of a digital signature.

CONCLUSION

Web development becomes easier using web technology languages which enable us to createmore interactive, less time consuming, highly effective and efficient and lower latency websites. For a website in the form of social media or e-commerce, its major purpose is to enable people around the globe to communicate and exchange data. In order to maintain stability, the website must be reliable, available, secured and easily accessible. A website with a better interface and friendly usage will attract more users then a website with less friendly UI. Any website which is accessed using a phone or a computer should not lose its dimensions and maintain as it was developed, it is the responsibility of a developer to take care of all aspects.

Security is a major factorfor any website and the developer should maintain a secured database that cannot be hacked so thatthe users feel safe to share their information over it. Be it SQL Injection, Forgery or Site Scripting, with the help of above mentioned algorithms websites can be kept secured.

REFERENCES:

[1] Survey on web services composition,SchahramDustdar* and Wolfgang Schreiner Distributed Systems Group, Vienna University of Technology, TU Wien E-mail: dustdar@infosys.tuwien.ac.at E-mail: *schreiner@infosys.tuwien.ac.at*

[2] Agarwal, S., Handschuh, S. and Staab, S. (2003) Fensel, D. et al. (Eds.): Surfing the Service Web, ISWC, LNCS 2870, Springer-Verlag Berlin Heidelberg, pp.211–226.

[3] Benatallah, B. et al. (2004a) Atluri, V. (Ed.): On Automating Web services Discovery, Received: December 15, 2002/Accepted: September 15, Published online: February 6, Springer-Verlag.

[4] Benatallah, B., Casati, F. and Toumani, F. (2004b) Web Service Conversation Modeling. A Cornerstone for E-business Automation, IEEE Internet Computing, January–February.

[5] Cabrera, F., Copeland, G., Cox, B., Freund, T., Klein, J., Storey, T. and Thatte, S. (2001) Specification: Web Services Transaction (WS-Transaction), http://www-106.ibm.com/ developerworks/webservices/library/ws-transpec/.

[6] A survey of multimedia and web development techniques and methodology usage, Lang, Michael; Barry, Chris, 2001. Barry, C., & Lang, M. (2001). A survey of multimedia and web development techniques and methodology usage. "IEEE Multimedia", 8(2), 52-60.

[7] Trust, Satisfaction, and Loyalty Formation in Electronic Commerce MaizatulAkmar Ismail and Nader SohrabiSafa University of Malaya, Faculty of Computer Science & Information Technology, Kua

[8] N. S. Safa and M. A. Ismail, "A customer loyalty formation model in electronic commerce," Economic Modelling, vol. 35, pp. 559- 564, 2013.

[9] M. G. Helander and H. M. Khalid, "Modeling the customer in electronic commerce,"Applied Ergonomics, vol. 31, no. 6, pp. 609-619, 2000.

[10] WhiteHat Security, “WhiteHat website security statistic report 2010.”

[11] S. Tang, H. Mai, and S. T. King, “Trust and protection in the illinois browser operating system,” in OSDI’10: Proceedings of the 9th USENIX conference on Operating systems design and implementation, 2010, pp. 1–8