Plagiarism Checker X Originality Report

Plagiarism Quantity: 32% Duplicate

Date	Wednesday, February 12, 2020
Words	1970 Plagiarized Words / Total 6151 Words
Sources	More than 201 Sources Identified.
Remarks	Medium Plagiarism Detected - Your Document needs Selective Improvement.

A Study on Web Application Security Vulnerabilities Abstract The world is exceedingly dependent on the Internet, Web applications are one of the most prevalent platforms for information and services Exchange over Internet today. Nowadays, web security is greatest challenge in the corporate world. As almost all organizations has using the web application service to share or store sensitive information. So Web applications are inclined to security attacks and Number of security vulnerabilities in web application has grown with the tremendous growth of web application in last two decades. so web applications become a well known and important target for security attacks by attackers.

So it is very vital to secure a web application from attacks by unauthorized users. A lot of the issues that occur over a web application is basically due to the improper input provided by the client. This paper reviews about the vulnerability assessment and pentesting steps and types,area of web application security Vulnerabilities like sqlinjection,cross site scripting,file inclusion and broken authentication Introduction World Wide Web has advanced from a framework that delivers static pages to a stage that supports distributed and dynamic applications, known as web applications and become one of the foremost predominant technologies for delivering information and service over Web.

Web application advancements give a promising system of coordinating numerous useful segments over the web and therefore empower people and associations to cooperate each other utilizing application program interface along enormous topographical separations. Billions of people everywhere throughout the world use web application advancements to exchange data, perform money related exchanges, and have fun and communicate and to socialize themselves [3, 5, 6].

Sources found:

Click on the highlighted sentence to see sources.

Internet Pages

0% https://www.researchgate.net/publication
0% https://www.bing.com/aclk?ld=e3c9C7J0JPX
0% Empty
0% https://www.ijser.org/researchpaper/Web-
0% https://www.techdirt.com/articles/201705
0% https://www.quora.com/What-is-your-revie
0% https://ieeexplore.ieee.org/abstract/doc
0% https://en.wikipedia.org/wiki/Talk:OWASP
0% https://en.wikipedia.org/wiki/World_Wide
0% http://ssrg.site.uottawa.ca/docs/Surya-T
0% https://www.researchgate.net/publication
0% https://www.techrepublic.com/blog/10-thi
0% https://www.zdnet.com/article/these-are-
0% https://blog.gridinsoft.com/feed/
0% https://sites.cs.ucsb.edu/~chris/researc
1% https://www.chegg.com/homework-help/ques
0% https://www.upwork.com/hiring/developmen
0% http://www.bing.com/images/search?q=the+
0% https://searchsecurity.techtarget.com/ne
0% https://www.bing.com/aclk?ld=e3ixGTDHOGZ

Web application grew tremendously in the last few decades and it has brought great benefits to the people, however, these benefits are associated with some challenges and one of the most important challenges is that of security. Security in web application refers to the threat which occurs due to flaws in software design, coding, testing and implementation. Web application services are more prone to cyber attacks due to their public access.

And web applications are increasingly used to deliver security critical services so they become a valuable target for security attacks. Many web applications interact with back-end database systems, which may store sensitive information (e.g., financial, health), the compromise of web applications would result in breaching an enormous amount of information, leading to severe economical losses, ethical and legal consequences [7,8].

The Web platform is a complex ecosystem composed of large number of components and technologies, including HTTP protocol, web server and server-side application development technologies (e.g., CGI, PHP, ASP), web browser and client-side technologies (e.g., JavaScript, Flash). Web application built and hosted upon such a complex framework faces characteristic challenges postured by the highlights of those components and innovations and the irregularities among them.

For developers with insufficient security vulnerabilities knowledge or awareness results in a high rate of web applications sent on the Web is uncovered to security vulnerabilities. According to a report by the Internet Application Security Consortium, around 49% of the internet applications being looked into contain vulnerabilities of tall hazard level and more than 13% of the websites can be compromised totally naturally [1].

A later report [2] uncovers that over 80% of the websites on the Web have had at least one serious Vulnerability. Vulnerability refers to a weakness in systemﹾs security requirement, design, coding or operation that could accidently occur or intentionally violated and result in security failure. In last few years, number of reported web application security vulnerabilities has increased. Some commonly reported web application vulnerabilities include SQL injection, cross site scripting, command line injection, cross site request forgery and malicious file upload and execution [3, 4].

Introduction to web application The Web Application Security Consortium (WASC) [11] defines a web application as ﹾa software application, executed by a web server, which responds to dynamic web page requests over HTTP.ﹾ A web application is comprised of a collection of scripts, which reside on a web server and interact with databases or other sources of dynamic content. Using the infrastructure of the Internet, web applications allow service providers and clients to share and manipulate information in a platform-independent manner.

0% https://www.slideshare.net/jeremiahgross
0% https://www.slideshare.net/deepa4242/gui
0% https://www.darkreading.com/vulnerabilit
0% https://cheatsheetseries.owasp.org/cheat
0% https://github.com/rapid7/metasploit-fra
0% https://www.bing.com/aclk?ld=e3A5J9Hg5zr
0% https://samate.nist.gov/docs/webapp_scan
0% https://www.bing.com/aclk?ld=e3FFXOzTHrk
0% https://securitycafe.ro/2015/01/05/penet
1% https://samate.nist.gov/docs/wa_paper.pd
0% https://www.gkseries.com/computer-scienc
0% https://www.theserverside.com/feature/Ho
0% https://www.bing.com/aclk?ld=e3xIITjFuEp
0% https://pdfs.semanticscholar.org/5c56/cf
0% https://www.irjet.net/archives/V6/i5/IRJ
0% https://ctcarlsoncom.wordpress.com/
0% https://quizlet.com/88126894/ethical-hac
0% https://www.bing.com/aclk?ld=e3TxcueefB2
1% https://scialert.net/fulltext/?doi=jse.2
0% https://www.sans.org/reading-room/whitep
0% https://issuu.com/dragonjar/docs/owasp-t
0% https://www.owasp.org/images/1/10/Cambri
0% https://www.bing.com/aclk?ld=e34EyPJsYVf
0% https://www.ptsecurity.com/ww-en/analyti
0% https://docs.spring.io/spring-boot/docs/
0% https://www.icsc.com/uploads/t07-subpage
0% https://blog.thousandeyes.com/efficient-
0% https://dl.acm.org/citation.cfm?id=12513
0% http://downloads.hindawi.com/journals/je
0% http://scholar.google.com/citations?user

For a good introduction to web application from the penetration tester﹐s perspective, see [12]. The technologies used to build web applications include PHP, Active Server Pages (ASP), Perl, Common Gateway Interface (CGI), Java Server Pages (JSP), JavaScript, VBScript, hyper Text Markup Language(HTML) etc. Some of the broad categories of web application technologies are communication protocols, formats, server-side and client-side scripting languages, browser plug-ins, and web server API. A web application has a distributed n-tiered architecture.

Typically, there is a client (web browser), a web server, an application server (or several application servers), and a backend (database). Figure 1 presents a simplified view of a web application. There may be a firewall between web client and web server. / Figure 1. Web Application Environment Vulnerabilities in Web application Vulnerability is a weakness in application which can be design flaw or implementation bug that allows an attacker to cause harm to stakeholders of an application.

Formally, vulnerability is defined as ﹐The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved﹐ (Enisa, 2014) . Vulnerabilities are caused because of poor design, configuration mistakes, inappropriate and insecure coding techniques, complexity of software, unchecked user input, weak password management.

The impact of vulnerabilities is very harmful, if a hacker obtains the bank account details of an individual, he can misuse this information (like account number, account balance, loan amount, etc.) and can also alter the data to cause harm to the concerned individual. Vulnerability management in web applications is the cyclical practice of identifying, classifying, remediating and mitigating vulnerabilities. Today, thousands of vulnerabilities are present in web applications.

Vulnerability classification is done by different organizations like OWASP and Microsoft ,SANS etc based on their risk rating according to exploitability, prevalence, detect ability and impact. Classification according to OWASP, top 10 application security risks are given below: OWASP TOP 10 A1:2017-injection A2:2017-Broken Authentication A3:2017-Sensitive Data Exposure A4:2017-Xml External Entities(XXE) A5:2017-Broken Access control A6:2017-Security misconfiguration A7:2017-Cross-site Scripting A8:2017-Insecure Deserialization A9:2017-Using components with known Vulnerabilities A10:2017-Insufficient logging and Monitoring Table1.

OWASP (2017) Top Ten application security Risks In 2018, around 70 types of weaknesses in web applications are found. As always, Cross-Site Scripting (XSS) vulnerabilities are present in many web

0% https://www.researchgate.net/publication
0% http://www.webappsec.org/
0% https://www.bing.com/aclk?ld=e3E54Nk1Qzu
0% https://www.codeproject.com/articles/686
0% https://owasp.org/www-project-cheat-shee
0% https://onlinelibrary.wiley.com/doi/full
0% https://portswigger.net/web-security/csr
0% https://docs.djangoproject.com/en/3.0/re
0% https://owasp.org/www-project-top-ten/
0% https://markitzeroday.com/x-requested-wi
0% https://www.offensive-security.com/metas
0% https://unacademy.com/lesson/file-inclus
0% https://vulners.com/nessus/SMB_NT_MS17_A
0% https://www.quora.com/What-is-Remote-fil
0% https://ravibommali.blogspot.com/
0% https://www.acunetix.com/blog/articles/l
0% https://www.wordfence.com/learn/understa
0% https://portswigger.net/burp/samplerepor
0% https://www.bing.com/aclk?ld=e3S-_bOLNT4
0% https://quizlet.com/46811176/certified-e
0% https://github.com/mubix/tools/blob/mast
0% https://www.smashingmagazine.com/2011/01
0% https://insights.securecodewarrior.com/c
0% https://www.w3schools.com/PHP/php_includ
0% https://vnsys.wordpress.com/2011/12/23/s
0% https://owasp.org/www-community/attacks/
0% https://www.hackersmail.com/2013/
0% https://help.adobe.com/archive/en/after-
0% https://www.bing.com/aclk?ld=e3xoUyItMJM
0% https://www.imperva.com/learn/applicatio

applications. Four out of five web applications contained configuration errors such as default settings, standard passwords, error reporting, full path disclosure, and other information leaks that might have value for potential intruders [9].More applications are vulnerable to information exposure.

Access to configuration and debug information, source code, session identifiers, and other sensitive information is possible in 79 percent of web applications. This is concerning when compared to past years such as 2016 (60%) and 2017 (70%). / The types of application vulnerabilities based on severity are high, medium, low.fig 2 shows the percentage of web application affected based on severity levels of vulnerability / Figure 2.

Percentage of Web Application Affected yearly Sql injection and its type jk Xss and its types uuu Broken Authentication and Improper Session Management Hfg djk Conclusion Sk fjgvd,jmf References [1] WebApplicationSecurityStatistics,http://projects.webappsec.org/w/page/13246989/WebApplicationSecurityStatistics [2]White Hat Security, White Hat website security statistic report 2010. [3] Zhang, D., Liu, D., Csallner, C., Kung, D., & Lei, Y. (2014). A distributed framework for demand-driven software vulnerability detection. Journal of Systems and Software, 87, 60-73. [4] Huang, C. C., Lin, F. Y., Lin, F. Y.

S., & Sun, Y. S. (2013). A novel approach to evaluate software vulnerability prioritization. Journal of Systems and Software,86(11), 2822-2840. [5] Kaur, N., & Kaur, P. (2014). Input Validation Vulnerabilities in Web Applications. Journal of Software Engineering, 8(3), 116-126. [6] Austin, A., Holmgreen, C., & Williams, L. (2013). A comparison of the efficiency and effectiveness of vulnerability discovery techniques. Information and Software Technology, 55(7), 1279- 1288. [7] Shar, L. K., & Tan, H. B. K. (2012).

Automated removal of cross site scripting vulnerabilities in web applications. Information and Software Technology, 54(5), 467-478. [8] Avancini, A., & Ceccato, M. (2013). Comparison and integration of genetic algorithms and dynamic symbolic execution for security testing of cross-site scripting vulnerabilities. Information and Software Technology, 55(12), 2209-2222. [9] Web application Vulnerability Statistics(2018). https://www.ptsecurity.com/ww-en/analytics/web-application-vulnerabilities-statistics-2019/. [11] Web Application Security Consortium Glossary, http://www.webappsec.org/projects/glossary/ [12] Jody Melbourne and David Jorm, Penetration Testing for Web Applications, in SecurityFocus, 2003.

cross site request forgery(csrf): cross site request forgery is also known as csrf, one-click attack or session riding ,here the attacker will tries make the victim to perform actions specified by attacker when the user is authenticated , the impact of csrf will depend on the access rights that the victim has which includes change password of victims, creating the new user accounts, the attacker can also take full control of application data and functionality if victim is privileged user the cross site request forgery will be possible in the following cases

0% https://www.bing.com/aclk?ld=e3Ye46pe53s
0% https://resources.infosecinstitute.com/w
0% https://searchsecurity.techtarget.com/de
0% https://www.tojsat.net/journals/tojsat/a
0% https://www.industry-era.com/images/pdf/
0% https://www.researchgate.net/publication
0% https://www.360logica.com/blog/differenc
0% https://www.tutorialspoint.com/software_
0% https://www.us-cert.gov/bsi/articles/too
0% https://en.m.wikipedia.org/wiki/Software
0% https://www.guru99.com/user-acceptance-t
0% https://reqtest.com/testing-blog/grey-bo
0% https://www.mindtools.com/pages/article/
0% https://www.ncbi.nlm.nih.gov/books/NBK64
0% https://pentest-standard.readthedocs.io/
0% https://www.bing.com/aclk?ld=e31a84Pbjm9
0% https://www.bing.com/aclk?ld=e3r_6hLZIar
0% https://play.google.com/store/apps/detai
0% https://www.microsoft.com/en-in/download
0% https://www.skillset.com/questions/which
0% https://quizlet.com/386487919/ceh-toolss
0% https://en.wikipedia.org/wiki/Internal_s
0% https://csrc.nist.gov/CSRC/media/Publica
0% https://www.softwaretestinghelp.com/pene
0% https://www.schneier.com/blog/archives/2
0% https://www.bing.com/aclk?ld=e3leZFHDXmP
0% https://archive.org/stream/Power-Grid-Ha
0% https://www.nature.com/articles/d41586-0
0% https://cipher.com/blog/a-complete-guide
0% https://www.malwarebytes.com/malware/

if the application is using cookie based session handling, unpredictable request parameters should not be there and there should be a relevant action for a request to generate forged request for example password update page,new user creation pages etc.

A csrf attack works because session cookie, IP address, etc associated with the website will be automatically include in browsers request.so if user is authenticated the browser can not distinguish between the forged and legitimate request. csrf is serious vulnerability even though it is not included in owasp top 10. the best mitigation for csrf token is using the csrf token which has to be validated in every request and also implementing the same site cookie.

File Inclusion A file inclusion vulnerability is a web application vulnerability that will arise due to dynamic linking or execute the files or code from the webserver. On the file inclusion vulnerability, the application will build the path based on the user-supplied input and it can be controlled by user input .by taking this as advantage the attacker will tries to gives input or inject payloads that will leads to remote code execution, loading confidential files from server, deface the website etc.there are two types of files inclusion vulnerability 1.local file inclusion(LFI) Local file Inclusion is an attack targeting in web application that exist in the input fields(id field, text boxes, text fields, URL parameters, etc) that dynamically reference file and scripts from server storage and does not sanitize input fields properly, which allow an attacker to manipulate input and inject path traversal characters or to retrieve the files from the server.

The local file inclusion vulnerability will further lead to directory traversal, sensitive information disclosure, and code execution or even cross-site scripting(XSS). Local file inclusion will commonly arise in PHP web applications but can in all kinds of web applications.Based on the functionality of the application the LFI will lead to executing the input(file or command) by the language parser, download the requested file or display the content of file on the web page.

The remediation of lfi is the web application should accept only character and numbers for file names and should be blacklisted all the special characters,limit the access of files by the web application from specific directories only. 2. Remote Code Execution(RFI) Remote file inclusion is an attack targeting in the web application that exists in the input fields(id field, text boxes, text fields, URL parameters, etc) which dynamically reference external script and does not sanitize input fields properly.

using the remote file inclusion the attacker can include or load the file stored in a remote location. Almost all types of web applications support the file include but most commonly it will be found in a PHP web application because in PHP programming we will use file includes" extensive. By using the remote file inclusion the attacker can trick web application to load the malicious code stored in a remote location the malicious code

0% https://www.guru99.com/mis-types-informa
0% https://www.pbs.org/wgbh/pages/frontline
0% https://trailhead.salesforce.com/en/cont
0% https://www.ukstandards.org.uk/Published
0% https://www.velvetjobs.com/resume/techni
0% https://www.cisecurity.org/wp-content/up
0% https://www.sqreen.com/checklists/pentes
0% https://trusthackers.blogspot.com/2016/0
0% https://www.sitepoint.com/how-to-protect
0% http://ijarcsse.com/Before_August_2017/d
0% https://dzone.com/articles/what-is-the-s
0% https://www.phpdevelopers.com.au/news/da
0% https://www.ijresm.com/Vol_1_2018/Vol1_I
0% https://papers.ssrn.com/sol3/papers.cfm?
0% https://www.acunetix.com/blog/articles/i
0% https://appdividend.com/2019/07/18/sql-i
0% https://www.aaup.edu/sites/default/files
0% https://www.guru99.com/introduction-to-d
0% https://www.codecademy.com/articles/sql-
0% https://www.ptsecurity.com/ww-en/analyti
0% https://docs.oracle.com/cd/B10500_01/ser
0% https://portswigger.net/daily-swig/servi
0% https://support.office.com/en-us/article
0% https://it.slashdot.org/story/09/08/25/2
0% https://stackoverflow.com/questions/4212
0% https://aboutsqlserver.com/2014/12/02/si
0% https://searchdatabackup.techtarget.com/
0% http://onlinelibrary.wiley.com/doi/10.10
0% https://www.auctionsoftware.com/what-is-
0% https://www.dnsstuff.com/sql-injection

will include backdoors, web shells, code execution at OS level, etc.

By successfully exploiting the RFI the attacker can gain sensitive information from the server, take over the application or server, server hijacking, etc. The main causes for remote file inclusion are programming mistakes, misconfigurations of the respective programming language functionality. The best way to eliminate the RFI is to completely avoid the dynamically including the files based on user inputs or maintain the white list of filenames that can be included in user inputs.

Penetration Testing Methods Black box pen testing• Black box testing is carried out without the knowledge of evaluating infrastructure so pen tester will act as a real-world hacker in this case. The pen tester team will scan the entire infrastructure as an outsider to find vulnerabilities. Black-box penetration testing is based on a detailed review of currently running programs and systems. A black-box penetration tester should know both automated and manual penetration testing methodologies.

Generally, this is the best approach because it helps pen testing team to think out of the box and carry out testing in all levels according to their realistic knowledge and expertise and they will also use all the techniques and methodologies available to them for simulating the level of persistence, knowledge, and expertise that a real-world hacker can perform. White box pen testing• Pen testers will have full knowledge of the infrastructure and its internal design in white box pen testing and it is also known as clear box testing.

The penetration tester seeks to obtain as much input as they can to gain more knowledge and better understand the system so that they can further expand their penetration tests. The main challenge with white-box testing is to analyze the vast amount of data and extract data to identify possible vulnerability points, making it the most time-consuming method of penetration testing. In white-box testing, we can find logical errors, syntax error or typographical errors, design flaws, human errors, etc.

While performing the white box testing the pen testers will have full access to the system for performing audits on the high-risk area. Grey box pen testing• Grey box testing is also known as translucent testing, it is more efficient but time consuming because some times testers will test every single input path or field . in grey box testing the tester will have limited information of internal working of system and source code .the grey box testing will not be useful during the development phase because grey box testing is carried out based on end-user perspective that aims to test the front-end functionality and the internal workings of the system. grey box pen testing will have benefits of box whit and box pentesing.

grey box pentesting is very effective for web application testing, business domain testing and security assessment • Pre-Engagement Interactions or Scoping In this phase, the pen testing team will discuss in

0% https://medium.com/@hninja049/example-of
1% https://www.imperva.com/learn/applicatio
0% https://guide.offsecnewbie.com/5-sql
0% https://docs.oracle.com/en/cloud/saas/ta
0% https://www.tutorialspoint.com/python_pe
0% https://www.acunetix.com/blog/articles/c
0% https://en.wikipedia.org/wiki/SQL_inject
0% https://news.ycombinator.com/item?id=153
0% https://www.sootoday.com/around-ontario/
0% https://docs.oracle.com/cd/B28359_01/jav
0% https://quizlet.com/11456870/final-exam-
0% https://dzone.com/articles/sql-injection
0% https://dzone.com/articles/sqli-part-3-i
1% http://www.firewall.cx/general-topics-re
0% http://index-of.co.uk/Hacking-Coleccion/
0% https://www.tutorialcup.com/dbms/dynamic
0% https://pdfs.semanticscholar.org/624a/27
0% https://www.tutorialspoint.com/plsql/pls
0% https://www.reddit.com/r/2007scape/comme
0% https://community.powerbi.com/t5/Desktop
0% http://docshare.tips/taxation-in-india_5
0% https://www.mssqltips.com/sqlservertip/2
1% https://www.rapid7.com/fundamentals/sql-
0% https://www.microsoft.com/security/blog/
0% https://docs.oracle.com/en/database/orac
0% https://discussions.agilebits.com/discus
0% https://github.com/trimstray/Nginx-Admin
1% https://excess-xss.com/
0% https://owasp.org/www-community/Injectio
0% https://www.softwaretestinghelp.com/java

detail the scope of the assessment, objectives, legal implications, goals and organizational assets available in pre-engagement interactions or scoping phases. Penetration testers should collaborate with the organization to understand any threats, organizational culture, and best suited pen-testing technique for the organization, as well as all legal issues.

In this process, organizational assets will has to categorize based on assets in scope (assets on which pen testing has to perform) and assets out of scope (not included in pen testing) based on gathered information on all organizational assets Reconnaissance Reconnaissance or Open Source Intelligence gathering is one of the important step in penetration testing. A pen tester aims to gather as much as information and the potential targets for exploit required about client organization. Depending on the type of penetration test chosen, the penetration tester will have different degrees of organizational information collected during the first phase and may also find extra critical information on their own to locate hidden vulnerabilities and entry points in the system.

In generally pen testers will use the vast range Reconnaissance techniques which include searching in different search engines, Domain name searches or WHOIS lookups, social engineering, searching for tax records, internal Foot printing for email address, usernames and social networks accounts,tailgating,external Foot printing for port scanning ,reverse DNS,packet sniffing etc. THREAT MODELING & VULNERABILITY IDENTIFICATION The Reconnaissance will act as information gathering phase in the In the threat modeling and Vulnerability Identification and this phase will also be pre-attack phase .In

this phase pen testers will think like attackers and will scan the system as deep as they can and pen testers identifies different targets and also maps organizational attack vector based on threats, here targets will be business assets like employees data, customer data ,technical data and threats will be internal threats like management,employess,vendors,distributors etc and external threats like Ports, Network Protocols, Web Applications, Network Traffic, customers etc. The internal threats will be somewhat in the control of organization and external threats will be out of control.

In this phase the pen testers will use different automated tools and manual testing tools to scan all the organization in scope assets. After completion of this phase the information gained is different vulnerabilities in the servers, web application and all the in scope assets. EXPLOITATION The pen tester team will try different exploits contained in network, applications, and data with a list of all potential vulnerabilities and entry points gathered in Threat Modeling & Vulnerability Identification.

The main aim of the pen tester is to verify how far they can get into your system and find high-value targets without being avoid detected. The pen tester will exploit the system based on scope defined in the first

0% https://www.gspann.com/resources/blogs/h
0% https://quizlet.com/25055016/cissp-2013b
0% https://en.wikipedia.org/wiki/Talk:Cross
0% https://www.checkmarx.com/knowledge/know
0% https://en.wikipedia.org/wiki/XSS
0% https://secure.wphackedhelp.com/blog/wor
0% https://en.wikipedia.org/wiki/Scripting_
0% https://security-informatics.springerope
0% https://backstage.forgerock.com/docs/am/
0% https://www.c-sharpcorner.com/article/se
0% https://aniruddhsite.wordpress.com/2015/
0% https://mountainhomemarketing.com/cross-
2% https://www.ijedr.org/papers/IJEDR170302
0% https://quizlet.com/234125355/30-threats
0% https://docs.microsoft.com/en-us/deployo
0% https://academia.stackexchange.com/quest
0% https://www.sciencedirect.com/science/ar
0% https://www.researchgate.net/publication
0% https://www.computerweekly.com/tip/Cross
0% https://support.zendesk.com/hc/en-us/art
0% https://www.checkmarx.com/2017/10/09/3-w
0% https://en.m.wikipedia.org/wiki/Cross-si
0% https://pentest-tools.com/blog/xss-attac
0% http://abcd.lk/sliit/sliit%20books/CISSP
0% https://security.stackexchange.com/q/177
0% https://help.sharpspring.com/hc/en-us/ar
0% https://www.3ders.org/3d-software.html
1% https://www.dionach.com/blog/the-real-im
0% https://arxiv.org/pdf/2001.05668
0% https://www.universalclass.com/articles/

phase .the pen testers will use the standard exploits like Web Application Attacks, Network Attacks, Memory-based attacks, Wi-Fi attacks, Physical Attacks, Social engineering. In this phase the system has to exploit after developing the threat vector and attack plan based on vulnerabilities to gain access to system and sometimes the system can have the secure network which contains DMZ, firewall, honey pots, and honey well so that the pen tester should use different evacuation techniques to bypass these security devices.

0% http://www2.mitre.org/work/sepo/toolkits

POST-EXPLOITATION Upon completion of the exploitation process, the next aim is to record the methods used to gain access to valuable information of the organization. The pen tester should take all the evidences required to generate the report and after collecting the evidence the team should cleanup the system to revert the activities done during the exploitation phase. The clean up activities will include Removing any executables, scripts, and temporary files, Reconfiguring settings back to the original state prior to the test, Removing any user accounts created, removing any types of malware codes injected etc.

The clean-up process should ensure that all installed backdoors or root kits should be removed, and it should return the system configuration to its original, pre-engagement state. Any credentials changed has to restore, and any additional usernames created should be removed. Reporting This report is the best method to convey the findings of a pen test. This report will address managers and the technical team. From the manager's perspective, they will have information like different vulnerabilities available in the system and their Business impact on the system.

In the technical Team, they will have information like different vulnerabilities exist in the system with its remediation. The pen test report will begin with an executive summary outlining organizational business-related penetration test plan, defining outcomes by risk ranking. This section should be concise, and it could be the client's most important piece of decision-making and the business team can determine what to correct and what problems pose an appropriate level of risk.

The remaining part is technical detail, which will be descriptive, specific and generic or ambiguous statements will helps technical team to resolve security issues .

Resolution & Re-Testing In this phase, the technical team tries to resolve the issues and technical team will get some assistant from team to solve the issues and Once vulnerabilities have been remediated, the client has to retest their systems to ensure that fixes were successful and has to test whether new vulnerability was created as a result of remediation or not. And the pen test should also be conducted whenever there will be any modification in the system for finding new vulnerabilities. The attacker poisons dynamic SQL statements in the SQL Injection Attack to comment on some components of the declaration or to add a condition that will always be valid. The attacker uses the design faults to exploit SQL statements by implementing malicious

SQL code is poorly designed web applications.

Usually, SQL injection happens when input is taken from a user, such as their username, and in such fields, the user will provide a SQL statement instead of a name id that you will run on your database unknowingly. The attacker will execute malicious SQL statements in SQL Injection (SQLI) attack and attempts to control a database server behind a web application. And SQL Injection vulnerabilities can also be used to bypass security measures of application.

Vulnerability like SQLI can influence any website or web application using a SQL database such as MySQL, Oracle, SQL Server, or others. SQLI is a common attack vector that uses malicious SQL code for backend database manipulation to access confidential and sen0sitive information like customer information, personal data, trade secrets, intellectual property, and more.SQL Injection attack are one of the oldest, the most common and dangerous Vulnerability in the Web application.

An attacker must first discover vulnerable user inputs within the web page or web application to perform a SQL Injection attack and such user input is used as a target to pass an SQL query to a web page or web application for performing SQL Injection attack. SQL injection also termed SQLI. Input content can be created by the attacker. Such content is often referred to as a malicious payload and is the main component of the attack. After the attacker sends this content, the database executes malicious SQL commands.

The malicious queries can be inserted by the attacker via a web form or by attaching them directly to the end of the URL or HTTP headers. SQL is a query language for managing data stored in relational databases. And it can be used to access, edit, and delete data. Many websites and web applications manage all the data in SQL databases. You can also use SQL commands to execute operating system commands in some instances. An effective SQL Injection attack can, therefore, have very severe implications like [2].

Attackers can use SQL Injection to identify other user's credentials in the database. These users can then be impersonated by the attacker. The impersonated user can be an administrator with all the privileges of the database also [2]. SQL allows you to select and display information in the database. An SQL Injection vulnerability could give the attacker full access to all information on a database server. [2] SQL also allows you to change information and add new information to a database.

For instance, an attacker could use SQL Injection in a financial application to change balance, void transactions, or transfer cash to their account[2]. To delete documents from a database, you can use SQL, even to drop tables also. Even if database backups are made by the administrator, data deletion could influence the accessibility of the application until the database is restored. Backups may not also contain the latest information [2]. In some database servers, you can use the database server to access the working system.

This may be accidental or deliberate. In such a case, an attacker might use an initial vector of SQL Injection and then attack the internal network behind a firewall [2]. ---------- Types of SQL injection In-band SQLi The attacker utilizes the same communication channel to launch their assaults and collect outcomes.

The simplicity and effectiveness of In-band SQLI make it one of the most popular SQLi attack kinds. This technique has two sub-variations [3]: Error-based SQLi• The attacker executes activities that cause error messages to be generated by the database. The attacker may use the data supplied by the error messages to collect information about the database structure [3]. Union-based SQLi•This method uses the UNION SQL operator to fuse various select statements generated by the database to obtain a single HTTP response.

This result may include information that the attacker can leverage [3]. Inferential (Blind) SQLi The attacker sends payloads to the server and observes the server's response and behavior to know more about its database structure Because the data is not transferred from the website database to the attacker machine, this method is called blind SQLi, so the attacker can not see much information after an attack in in-band attack [3] Blind SQL injections depend on the server's response and behavior patterns, to perform these types of attacks typically consume time but can be just as damaging.

The following can be categorized as blind SQL injection: Boolean• that attacker sends a SQL query to the database prompting the application to return the result. The result depends on whether the request is true or false. Based on the result, the HTTP response data will change or remain unchanged. The attacker can then work out if a true or false outcome has been produced by the message. Time-based•the attacker will send a SQL request to the database, which will cause the database to wait (in seconds for a period) before it responds.

From the time the database takes to respond, the attacker can see if a request is true or false. An HTTP response will be produced immediately or after a waiting period based on the result. Thus, if the message they used returned true or false, the attacker can work out without depending on database information [3]. Out-of-band SQLi Only when certain features are enabled on the database server used by the web application the attacker can perform this type of attack.

This type of attack is used mainly as an alternative to the SQLi methods in-band and inferential. Out - of-band SQLi is conducted if the attacker is unable to use the same channel to start the attack and collect data, or if a server is too slow or unstable to perform such activities. These methods rely on the server's ability to generate DNS or HTTP requests for information transfer to an attacker [3]. ---------- Example: Username = request.post ['username'] password = request.post ['password'] // Statement vulnerable to SQL injection SQL = "SELECT userid FROM users

WHERE username='" + username + "' AND password='" + password + "'" // execute statements db.exec(SQL) The above example is vulnerable to SQL injection because the database server will interpret as a command whatever the user enters in the form.

For example, by setting the password field to ' or 1=1, an attacker could bypass this form. The following looks like a SQL statement. The following is what the SQL statement would look like. SELECT id FROM users WHERE username='foo' AND password='pass' OR 1=1 From the above statement, we can see that the user's input has changed the statement's functionality. Now, the value of the ID column is being returned if the submitted username is equal to foo, and the password is equal to pass, or if 1is equal to 1 (which will always be the case).

With this statement, only the username has to match the value in the database since the password condition can either match the value in the database or validate it if 1=1. With this trick, for any customer whose username is known, the intruder can bypass the authentication system of the website. An intruder may even comment on the remainder of the declaration to further regulate the SQL declaration. An intruder can, for instance, use the double-dash (--) notation to comment on the rest of the declaration: SELECT id FROM users WHERE username='username' --' AND password=bar' The highlighted portion of the above declaration, or after the double-dash, will be pointed out and thus not regarded during execution.

This will allow an attacker to bypass authentication once again ---------- How to Prevent against SQL Injection Attacks Do Not use dynamic SQL Quires Avoid placing user-provided input directly into SQL statements. Prefer prepared statements and parameterized queries[1], which are much safer. Stored procedures are also usually safer than dynamic SQL. Sanitize user-provided inputs Properly escape the characters and should Verify that the type of data submitted matches the type expected.

Don't leave sensitive data in plaintext: Encrypt private/confidential data stored in a database. This also provides a further level of protection if the attacker successfully enters into the system. Restrict the rights and privileges of the database by Reducing the user's capabilities to the bare minimum. This will restrict what an intruder or attacker can do if they succeed in gaining access.

Avoid displaying common database errors that help Attackers obtain information to execute additional attacks on the database so that we need to show custom error messages instead of standard error messages. Use a Web Application Firewall (WAF) for web applications that access databases This protects web-based applications. It can help to identify SQL injection attempts. It can also help prevent SQL injection attempts from reaching the application (and therefore the database) based on the configuration.

Xss Introduction Cross-site Scripting (XSS) is a client-side injection attack where, the attacker tries to execute

the malicious scripts in the victim's browser by injecting malicious payload in the legitimate web application. Every time the users accessing the web pages that are injected with the malicious script then the real attack will be happens. The web application becomes a means for delivering the malicious script to the user browser.

Usually, the attacker will target the web application with forums, message boards, and web pages that allow comments, search boxes, input fields will be targeted by attackers to perform cross-site scripting attacks. At first, the attacker tries to find web pages that are vulnerable to cross-site scripting and tries to inject the malicious payload in the vulnerable pages whenever the user tries to load that page then the malicious payload will be executed in victim browser and JavaScript will access the cookies and sends to attacker and by using these cookies the attacker can impersonate the victim by using session hijacking attack as shown in figure 1 Figure 1.

Demonstration of XSS attack By using the Cross-site Scripting the attacker may damage the website instead of targeting the user and the attacker can also use injected malicious scripts to change the content of the website and may even redirect to other web site or website with malicious contents Vulnerability is regarded to have less impact than SQL injection vulnerability. At first, the consequences of the ability to run JavaScript on a web page might not seem severe. Because most modern web browsers run java scripts in a very tightly controlled environment and have limited access to the user's OS and files.

But if JavaScript is used as part of malicious content, it can still be dangerous as Malicious JavaScript can also access to all objects that remaining web pages can access. Which includes access to the User cookies often used to store data related to the session? If an intruder succeeds in obtaining the session cookie of a user, they can impersonate that user and take action on behalf of the legitimate user and gain access to sensitive information of the user and JavaScript can use the XMLHttRequest object to send arbitrary HTTP requests to destinations. it can also use HTML5 APIs in modern browsers. For instance, gain access to specific files from the user's file system to the geo location, webcam, and microphone.

Most of these APIs require opt-in from the user, but the attacker may use social engineering to address that restriction. Types of XSS attacks As the main purpose of XSS attack is to execute malicious JavaScript in the victim's browser, and there are few fundamentally different ways of achieving that goal. ReflectedXSS: In reflected XSS, the malicious string is part of the victim's request to the website.It might seem harmless asit requires the victim himself to actually send a request containing a malicious string.

But attackers may trick the victims to send the malicious script without informing them. Whenthe attacker targets a specific individual or group theN attacker WILL send the malicious URL to the victim (using e-mail or instant messaging, or social networking link or link) and trick them into visiting link THEN AFTER vitctim visiting the link then attacker will steal confidential information stored in cookies. PersistentXSS: In persistent/stored XSS,the malicious string originates from the website's database.It

occurs when the data provided by the attacker is saved to the server, and then displaying on "normal" pages returned where proper HTML escaping which will dislayed to other users. Here, malicious code is inputted by attackersinto vulnerable web pages and is then stored on the web server for later use. The payload may be served back to other users browsing web pages and is executed in their context, at a later stage. Therefore, victims do not need to click on a malicious link to execute the payload (as in the case of Non-Persistent XSS); they just need to access the compromised web page, supplying user input from other web sessions that is not sanitized.

DOM-basedXSS: DOM XSS is a type ofcross site scripting attackwhich relies on inappropriate handling, in the HTML page, of the data from its associated DOM. Among the objects in the DOM, there are several which the attacker can manipulate in order to generate the XSS condition, and the most popular, from this perspective, arethedocument.url,document.locationanddocument.referrerobjects. XSSattacks have been around years now and lot of research in the field has been done by Industry and academic experts.In

literature, there are many methodologies, algorithms and techniques proposed in order to prevent XSS attacks. Analysis of XSSattacks reveal that they are caused due to improper coding of web applications and inability to filter or sanitize inputand encode the output. So, here known XSScountermeasures and mitigation techniques from various researchers are classified in phases of SDLC. Impact of Cross Site Scripting (XSS): The impact of XSS on web applications will be minimal if there is no confidential information and no dynamic content change based on user.

The impact will be critical on the web application that containing sensitive data, such as banking transactions, emails and health records, the impact will typically be significant. If the compromised user has admin privillages within the application, allowing the hacker to take full control of the insecure application and to compromise all users and their data. Session Hijacking The most popular XSS attack vectors are stealing the victim's session cookies to hijack the victim's accounts.

This enables attackers to impersonate victim account and access any sensitive data or features on behalf of victims. Stealing credentials The attacker will use HTML pages and JavaScript to steal customer credentials, instead of obtaining their cookies cloning the login page of the web application and then using XSS attacker steal credentials from the user. This situation is even more useful from an attacker's view, as they ultimately acquire plaintext credentials instead of expiring ephemeral session cookies.

Targeting Sensitive Data Another strong XSS attack vector is to use it to exfiltrate sensitive data (e.g. private identifiable data or cardholder data) or to conduct unauthorized activities. Key logger: Using JavaScript, all keystrokes entered by a user on a vulnerable site can be logged. For this purpose, Metasploit involves an off-the-shelf payload. There are also some commercial websites offering JavaScript software that records all

visitor motions, clicks, mobile gestures, or input forms that can be used for malicious reasons. Port scan: XSS is also an unexpected source for port scans to be initiated against a victim's internal network by accessing a vulnerable website.

Web site defacement: Changing the visual appearance of a website vulnerable to XSS is one of the easiest and yet most efficient ways for attackers to target companies or public organizations. Either this can take organizations to the spotlight for the improper reasons by using embarrassing pictures or hacktivism messages. Mitigations In order to minimize the risks associated with XSS, developers should encode all fields when displaying them in the browser. In addition, ensure that user input is filtered properly, particularly in the case of special characters.

A common source of XSS is outdated third party libraries integrated in the code, and as such, update these to the latest stable versions. As part of a defence in depth strategy, ensure that cookie properties (such as Http Only) and security headers, especially CSP, are set accordingly. On a higher level, ensure that security is properly integrated in all phases of the development process and that developers are aware of common web application vulnerabilities. Ultimately, regular penetration tests would help identify such flaws and improve the security stance of the web applications.