Назва Захист систем електронної комерції та мультисервісних систем
Шифр.
Тип. базова
Рік навчання. 2018-2019
Семестр. II
Кількість кредитів ЄКТС. 5
ПІБ лектора, науковий ступінь, посада. Погасій Сергій Сергійович, ст. викладач

Результати навчання.

Формування у студентів знань про основні типи атак на веб-додатки та веб-сервіси і методів, їх запобігання. Знання, отримані в результаті вивчення цієї дисципліни, дозволять студентам не допускати стандартних помилок в області безпеки при роботі з системам електронної комерції. освоєння принципів використання програмного забезпечення для тестування та виявлення вразливостей веб-додатків та веб-сервісів та створення систем захисту від виявлених вразливостей, запобігання шляхів несанкціонованого доступу (НСД) до даних в мультисервісних системах та системах електроної комерції; вживання заходів протидії проникненню шкідливого програмного забезпечення та відновлення працездатності мультисервісних систем після знешкодження загроз.

Обов'язкові попередні навчальні дисципліни
Основи побудови та захисту сучасних операцінйих систем
Організаційне забезпечення захисту інформації
Комплексні системи захисту інформації

Зміст.
Основи захисту веб-додатків та веб-сервісів. Атака на web-сервер.Атака «Міжсайтовий скриптинг». Безпека адрес.Термінологія, статистика атак на web-ресурси.

Рекомендовані джерела.
Основна

1. Damn Vulnerable Web Application (DVWA). http://www.dvwa.co.uk/
2. Damn Vulnerable Linux. https://distrowatch.com/dvl
3. OWASP WebGoat Project. https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project
4. Статистика уязвимостей веб-приложений (2013 г.) – Positive Technologies https://www.ptsecurity.com/ww-en/
5. Owasp Top 10: The Top 10 Most Critical Web Application Security Threats: Enhanced with Text Analytics and Content by Pagekicker Robot Phil 73 // Createspace. – 2014. – 54 p.
6. OWASP Testing Guide 4.0. https://www.owasp.org/images/1/19/OTGv4.pdf

7. How to Use Wireshark to Capture, Filter and Inspect Packets. https://www.howtogeek.com/104278/how-to-use-wireshark-to-capturefilter-and-inspect-packets/
8. Burp Suite Tutorial – Web Application Penetration Testing (Part 1). https://www.pentestgeek.com/web-applications/burp-suite-tutorial-1
9. Man-in-the-middle attack. https://www.owasp.org/index.php/Man-in-the-middle_attack
10.SQL Injection. https://www.owasp.org/index.php/SQL_Injection
11.Justine Clarke. SQL Injection Attacks and Defense. / Syngress Publishing, Inc., 2009. – 576 p.
12.А.Г. Тецкий. Исследование методов получения содержимого базы данных с помощью SQL-инъекций. – Открытые информационные и компьютерные интегрированные технологии: сб. науч. тр. – Х. : Нац. аэрокосм. ун-т «Харк. авиац. ин-т», 2014. – Вып. 66. – с. 188-191.
Додаткова
13.Sqlmap. http://sqlmap.org/
14.NT Web Technology Vulnerabilities. http://phrack.org/issues/54/8.html
15.Cross-site Scripting (XSS). https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
16.XSSer: Cross Site "Scripter". https://xsser.03c8.net /
17.Metasploit Framework User Guide. http://cs.uccs.edu/~cs591/metasploit/users_guide3_1.pdf
5.3 Інформаційні ресурси в Інтернеті
18.Penetration Testing Software | Metasploit. https://www.metasploit.com/
19.Unrestricted File Upload. https://www.owasp.org/index.php/Unrestricted_File_Upload
20.Nmap: the Network Mapper - Free Security Scanner. https://nmap.org/
21.Secunia Research Community https://secuniaresearch.flexerasoftware.com/community/research/
22.OSVDB | Everything is Vulnerable. https://blog.osvdb.org/
23.National Vulnerability Database. https://nvd.nist.gov/
24.Common Vulnerabilities and Exposures. https://cve.mitre.org/
25.Web Application Firewall. https://www.owasp.org/index.php/Web_Application_Firewall

Методи навчання.
Лекції, лабораторні, лекції проблемного.
Комунікативні методи навчання на лабораторних заняттях

Методи оцінювання
Поточний контроль (опитування)
Модульний контроль (контрольна робота)
Підсумковий контроль(залік)

Мова навчання Українська