

Міністерство освіти і науки України
Кам'янець-Подільський національний університет імені Івана Огієнка
Фізико-математичний факультет
Кафедра інформатики

Дипломна робота
магістра

з теми: **«Технології доступу до захищених об'єктів критичної
інфраструктури закладів вищої освіти»**

Виконав: студент 2 курсу KN1-M19 групи
спеціальності 122 Комп'ютерні науки
Королюк Володимир Володимирович

Керівник:

Слободянюк О. В., доцент кафедри
інформатики, кандидат технічних наук

Рецензент:

Кам'янець-Подільський – 2020 р.

ЗМІСТ

ВСТУП		4
Розділ 1 Розробка веб інтерфейсів		5
1.1. Огляд концепції API		5
1.2. Типи API		6
1.2.1 API за доступністю, тобто політика випуску.....		6
1.2.2 API за випадками використання		7
1.2.3 Специфікації/протоколи API.....		8
1.2.4 Порівняння архітектурних стилів API.....		11
Висновок до розділу.....		21
Розділ 2 Методи захисту від несанкційного доступу до ресурсів веб-застосунків		23
2.1. Вступ		23
2.2. OWASP.....		23
2.2.1. Injection		24
2.2.2. Broken Authentication.....		30
2.2.3. Sensitive Data Exposure		39
2.2.4. XML External Entities (XXE).....		41
2.2.5. Broken Access Control.....		47
2.2.6. Security Misconfiguration		51
2.2.7. Cross-Site Scripting XSS.....		54
2.2.8. Insecure Deserialization		60
2.2.9. Using Components with Known Vulnerabilities.....		63
2.2.10. Insufficient Logging & Monitoring.....		66

	3
Висновок до розділу.....	70
Розділ 3 Технології Cloud.....	72
3.1. Що таке хмарні обчислення?	72
3.2 Типи хмарних служб.....	73
3.3 Види хмарних обчислень	74
3.3.1 Що таке публічна хмара?	74
3.3.2 Що таке приватна хмара?	75
3.3.3 Що таке гібридна хмара?	75
3.4 Переваги хмарних обчислень	76
3.5 Недоліки хмари	77
3.4 Географія та хмарні обчислення	77
3.6 Безпека хмарних обчислень.....	79
Висновок до розділу.....	80
Розділ 4 Розробка API для доступу до захищених об'єктів критичної інфраструктури закладів вищої освіти.....	82
4.1. Огляд концепції двох-факторної автентифікації.....	82
4.2. Підготовка перед розробкою API.....	83
4.3. Реалізація API.....	84
4.4. Альтернативна реалізація API	90
Висновок до розділу.....	95
ВИСНОВКИ.....	98
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	99

ВСТУП

Актуальність дослідження. Більшість організацій обробляють безліч інформації, включаючи системну інформацію, комерційну таємницю, персональні дані.

І вся ця інформація зберігається в базах даних, що робить їх критичним об'єктом захисту.

Як би ми не захищали інформацію, до неї в будь-якому випадку потрібно мати доступ, але як це реалізувати? Як можна одночасно бути захищеним та мати змогу вільно користуватися інформацією, яка зберігається в базах даних?

Метою даної роботи є огляд технологій доступу до захищених об'єктів критичної інфраструктури закладів вищої освіти.

Об'єктом дослідження є технології доступу до захищених об'єктів критичної інфраструктури закладів вищої освіти

Предметом дослідження є розробка захищеної інфраструктури для закладів вищої освіти.

Відповідно до мети основним завданням роботи є:

- розглянути основні теоретичні відомості про концепцію розробки веб-додатку;
- дослідити популярні ризики захисту та методи захисту від несанкційного доступу до ресурсів веб-застосунків;
- дослідити важливість та ефективність хмарних технологій;
- провести розробку веб-додатку, який надає доступ до захищених об'єктів критичної інфраструктури закладів вищої освіти з використанням технології двох-етапної аутентифікації.

Методи дослідження: метод аналізу та синтезу, систематизація знань та метод наукового пізнання.

Структура роботи: робота складається із вступу, чотирьох розділів, висновків та списку використаних джерел.

ВИСНОВКИ

В ході проведеної роботи були дослідженні різні типи API, їх переваги та недоліки, розглянули технології розробки веб-інтерфейсів. Прийшли до висновку, що вибір архітектури API визначається: мовою програмування та середовищем розробки. Не потрібно списувати з рахунків ті технології, які вам не подобаються, прийде час та місце, вони стануть вам у нагоді. Всі технології розвиваються, те що було неактуальним вчора, сьогодні може зробити прорив в індустрії.

Детально описали десять самих популярних ризиків захисту веб-додатків. Визначили коли та при яких обставинах, ми стаємо вразливими. Розібралися як запобігти виникненню вразливостей. Розглянули на прикладах, як можна себе захистити від атак.

Зрозуміли на скільки перспективними та важливими можуть бути хмарні технології. Перерахували плюси та недоліки, які можуть виникнути при використанні хмари. Визначилися на скільки слабка безпека хмарних сервісів.

Розробили два варіанти реалізації двох-етапної аутентифікації за допомогою Google сервісів. Розглянули які бувають ще варіанти та способи реалізації двох-етапної аутентифікації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Clarke, S. "API Usability and the Cognitive Dimensions Framework", 2003. – 217p.
2. Ellis, B., Stylos, J. and Myers, B. The Factory Pattern in API Design: A Usability Evaluation. International Conference on Software Engineering, 2007
3. James Snell Programming Web Services with SOAP / James Snell, Doug Tidwell, PavelKulchenko. – Publisher: O'Reilly MediaReleased: December 2001Pages: 264
4. Jim Webber REST in PracticeHypermedia and Systems Architecture / Jim Webber, SavasParastatidis, Ian Robinson / Publisher: O'Reilly Media, September 2010. – 448p.
5. Mark MasseREST API Design RulebookDesigning Consistent RESTful Web Service Interfaces / Publisher: O'Reilly Media, October 2011. – 116p.
6. James McGovernJava Web Services Architecture / James McGovern, Sameer Tyagi, Michael Stevens, Sunil Mathew / Publisher: Elsevier, May 2003. – 832p.
7. Kevin MakiceTwitter API: Up and RunningLearn How to Build Applications with the Twitter API / Publisher: O'Reilly Media, March 2009. – 416p.
8. ГенриБекетJava SOAP дляпрофессионаловProfessional Java SOAP Programming. – Издательство: Лори, 2004. – 458с.
9. Брайан ТрэвисНазвание: XML и SOAP программирование для серверов. – М.: Русская Редакция, 2001. – 216с.
- 10.Ken Pugh Interface Oriented DesignWith Patterns. / Publisher: Pragmatic Bookshelf, July 2006. – 240p
- 11.Debbie StoneUser Interface Design and Evaluation / Debbie Stone, Debbie Stone, Caroline Jarrett, Mark Woodroffe, ShaileyMinocha. – Publisher: Elsevier / Morgan Kaufmann, April 2005. – 704p

12. Eric Elliott Programming JavaScript Applications Robust Web Architecture With Node, HTML5, and Modern JS Libraries. / Publisher: O'Reilly Media, February 2013. – 300p.
13. SOAP и REST [Электронный ресурс] / Л. Черняк. – 2003. – Режим доступа: <http://www.osp.ru/os/2003/09/183376/>
14. Правильно написание API сервиса [Электронный ресурс] – Режим доступа: <http://habrahabr.ru/qa/21031/>
15. Интеграция приложений в WWW [Электронный ресурс] – Режим доступа: <http://www.4stud.info/networking/web-services.html>
16. API [Электронный ресурс] – Режим доступа: <http://progschool.ru/products/webapi/>
17. Learn API testing [Электронный ресурс] – Режим доступа: 52 <http://www.guru99.com/api-testing.html>
18. A Web application as a REST API client [Электронный ресурс] – Режим доступа: <http://supervisord.org/api.html>
19. SOAP-vs-REST [Электронный ресурс] – Режим доступа: <http://www.alliancetek.com/Blog/post/2012/10/12/SOAP-vs-REST.aspx>
20. Webservices [Электронный ресурс] – Режим доступа: https://www.eeducation.psu.edu/geog583/files/geog583/keynote_chappell.pdf
21. Definision of SOAP and REST [Электронный ресурс] – Режим доступа: <http://spf13.com/post/soap-vs-rest>
22. Web Services, Part 1: SOAP vs. REST [Электронный ресурс] – Режим доступа: <http://www.ajaxonomy.com/2008/xml/web-services-part-1-soap-vs-rest>
23. Вікіпедія [Электронный ресурс] – Режим доступа: <https://ua.wikipedia.org/>
24. Using the API [Электронный ресурс] – Режим доступа: <https://developers.google.com/books/docs/v1/using>
25. REST API Development [Электронный ресурс] – Режим доступа: <https://developer.atlassian.com/display/DOCS/REST+API+Development>