МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет «Одеська юридична академія»

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ В УМОВАХ ВІЙНИ ТА ГЛОБАЛЬНИХ ВИКЛИКІВ XXI СТОЛІТТЯ: СИНЕРГІЯ НАУКОВИХ, ОСВІТНІХ ТА ТЕХНОЛОГІЧНИХ РІШЕНЬ

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

19 травня 2023 року

У двох томах

Том 1

Видавництво
«Юридика»
2023

УДК 005.332.2(4):316.42(477)"364""20"(062.552)
Є24

Рекомендовано до друку Вченою радою
Національного університету «Одеська юридична академія»
(протокол № 3 від 16.06.2023 р.)

За загальною редакцією **С. В. Ківалова.**

Відповідальний за випуск **М. Р. Аракелян.**
Матеріали видано в авторській редакції.

Є24 **Європейські** орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень : у 2 т. : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 19 травня 2023 р.) / за загальною редакцією С. В. Ківалова. – Одеса : Видавництво «Юридика», 2023. – Т. 1. – 790 с.

ISBN 978-617-8263-39-3

Матеріали Міжнародної науково-практичної конференції «Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень». У першому томі збірника містяться наукові напрацювання вчених, практиків, військовослужбовців у теоретичній та емпіричній площині в умовах повномасштабного військового вторгнення у сферах філософських основ, загальної теорії та історичних досліджень держави і права, актуальних проблем світових соціально-політичних процесів, соціології та психології. Висвітлено питання загроз національній безпеці в їхньому конституційному вимірі, у рамках міжнародного та європейського права, трудового права та права соціального забезпечення, земельного, аграрного та екологічного права, пов'язані з функціонуванням економіки та підприємництва в умовах європейського вибору України. Розглянуто проблеми інформатизації та цифровізації суспільства, захисту інформації та кібербезпеки в умовах військового вторгнення, питання методики викладання іноземних мов, теорії та практики перекладу, проблеми лінгвістики та журналістики.

Збірник розраховано на наукових та науково-педагогічних працівників, здобувачів вищої освіти, практичних працівників у сферах юридичної, економічної, соціологічної, політологічної, психологічної, філологічної наук, журналістики та кібербезпеки тощо.

УДК 005.332.2(4):316.42(477)"364""20"(062.552)

ISBN 978-617-8263-37-9 (у 2 т.)
ISBN 978-617-8263-39-3 (т. 1)

СЕКЦІЯ 13
КІБЕРБЕЗПЕКА ОСОБИ, СУСПІЛЬСТВА ТА ДЕРЖАВИ ЯК ФУНДАМЕНТАЛЬНИЙ ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ ОБОРОНОЗДАТНОСТІ УКРАЇНИ

СЛАТВІНСЬКА ВАЛЕРІЯ МИКОЛАЇВНА

Національний університет «Одеська юридична академія», асистент кафедри кібербезпеки

ДРИГА АРТЕМ ВАДИМОВИЧ

Національний університет «Одеська юридична академія», здобувач вищої освіти

ОРГАНІЗАЦІЯ ЗМАГАНЬ ПО ТИПУ CAPTURE THE FLAG З НАПРЯМКУ WEB В НУ «ОЮА»

Capture the flag, або CTF – популярний тип змагань з кібербезпеки, що включає в себе різні завдання, що призначені для перевірки навичок учасників у різних сферах, таких як:

- Криптографія (Cryptography);
- Веб-безпека (Web);
- Зворотна розробка (Reverse Engineering);
- Комп'ютерна криміналістика (Forensics);
- Експлуатація бінарних вразливостей (Binary Exploitation);
- Різне (Miscellaneous).

CTF зазвичай складаються з серії завдань, які вимагають від учасників виявлення вразливостей, їх використання, вирішення складних задач та виявлення прихованих прапорців (часто представлених у вигляді певних рядків тексту або файлів) протягом певного часу. Ці завдання призначені для моделювання реальних сценаріїв і надання практичного досвіду в різних аспектах кібербезпеки.

Факультет кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія» вирішив розробити свої змагання по типу CTF, які отримали назву «Hack & Slash». Нижче будуть представлені завдання, які були створені для напряму Web.

Перше завдання було на знаходження вразливості неправильної конфігурації веб-додатку, а саме експлуатації не вимкненого режиму відлагодження застосунку (debug mode) [1]. Учасником потрібно було перейти в будь-яку неіснуючу директорію всередині сайту, що призводило до виведення помилки 404 Page not found з детальною інформацією про всі каталоги сайту. Серед них була сторінка з назвою flag, де і був прапор.

На другому завданні був представлений сайт з вразливістю sql-ін'єкції [2]. Учасникам потрібно було ввести шкідливий sql код (наприклад' or'1'='1';--) у форму авторизації. Це призводило до успішної авторизації та переходу на сторінку з прапором.

Для третього завдання було розроблено сайт з уразливістю SSTI (Server Side Template Injection) [3]. Для знаходження прапора потрібно було в url сайту прописати параметр ?name={{config}}. Після цього виводилася конфігураційна інформація сайту, зокрема секретний ключ (Secret Key). У ньому і містився ключ у вигляді двійкового коду, який ще й був закодований за допомогою base64.

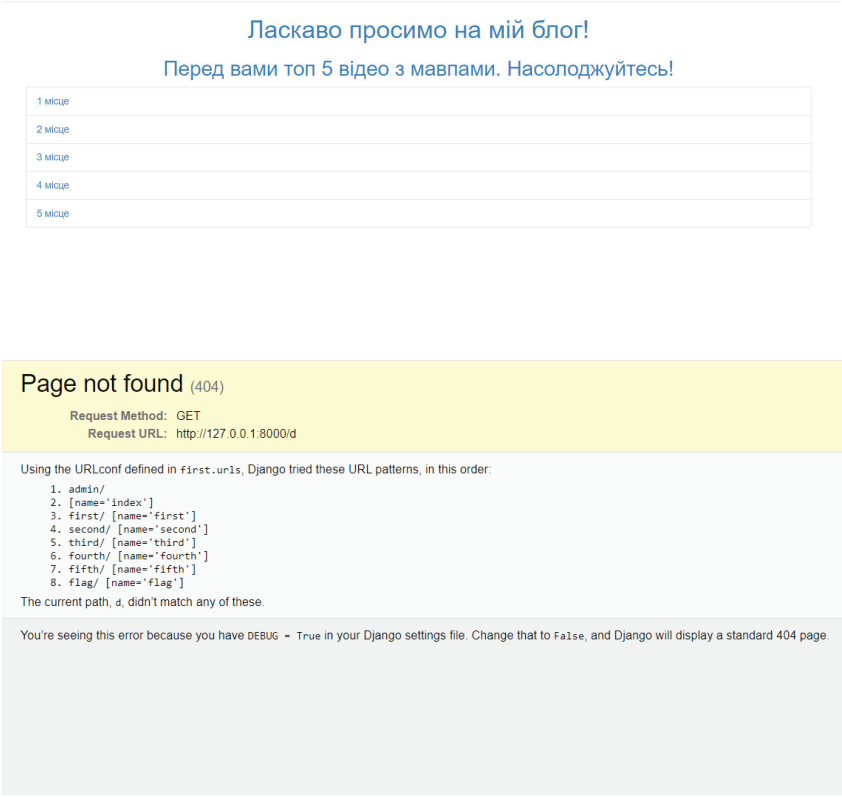

Рис. 1-3: Перше завдання

Привіт! Швидше заходь і отримай від мене подарунок

Твоє ім'я

Твій пароль

Зайти

Так тримати козаче! Ось і подарунок: FCIT{s1fg-gh6d-kjnx-h8ty}
Це ще шрекінчилося... це ніколи не шрекінчиться.

Рис. 4-5: Друге завдання

Лабораторна робота № 1
З веб технологій
Узумакі Наруто

Лабораторна робота № 1
З веб технологій
<Config {'ENV': 'production', 'DEBUG': False, 'TESTING': False, 'PROPAGATE_EXCEPTIONS': None, 'SECRET_KEY': 'MDEwMDAxMTAgMDEwMDAwMTEgMDEwMDEwMDEgMDEwMTAxMDAgMDExMTEwMTEgMDExM 'PERMANENT_SESSION_LIFETIME': datetime.timedelta(days=31), 'USE_X_SENDFILE': False, 'SERVER_NAME': None, 'APPLICATION_ROOT': '/', 'SESSION_COOKIE_NAME': 'session', 'SESSION_COOKIE_DOMAIN': False, 'SESSION_COOKIE_PATH': None, 'SESSION_COOKIE_HTTPONLY': True, 'SESSION_COOKIE_SECURE': False, 'SESSION_COOKIE_SAMESITE': None, 'SESSION_REFRESH_EACH_REQUEST': True, 'MAX_CONTENT_LENGTH': None, 'SEND_FILE_MAX_AGE_DEFAULT': None, 'TRAP_BAD_REQUEST_ERRORS': None, 'TRAP_HTTP_EXCEPTIONS': False, 'EXPLAIN_TEMPLATE_LOADING': False, 'PREFERRED_URL_SCHEME': 'http', 'JSON_AS_ASCII': None, 'JSON_SORT_KEYS': None, 'JSONIFY_PRETTYPRINT_REGULAR': None, 'JSONIFY_MIMETYPE': None, 'TEMPLATES_AUTO_RELOAD': None, 'MAX_COOKIE_SIZE': 4093}>

Рис. 6-7: Друге завдання

Розробка цих завдань не тільки дала змогу заглибитися в методику експлуатації вразливостей веб-додатків, а й дала уявлення про засоби програмного захисту від них.

Список використаних джерел:

1. Security Misconfiguration: Impact, Examples, and Prevention. URL: https://brightsec.com/blog/security-misconfiguration/
2. SQL Injection – W3Schools. URL: https://www.w3schools.com/sql/sql_injection.asp
3. SSTI (Server Side Template Injection) – HackTricks. URL: https://book.hacktricks.xyz/pentesting-web/ssti-server-side-template-injection

Ключові слова: CTF, Веб-безпека, SQL-ін'єкція, змагання, кібербезпека.
Key words: CTF, Web security, SQL injection, competitions, cybersecurity.