УДК 004.056.5

РАЗРАБОТКА МЕТОДИКИ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПЛАТФОРМЫ «ПЛАТОНУС»

Таубай Нұрлан Медетұлы

Магистрант, «Факультет информационных технологий»,
специальность – «Системы информационной безопасности»,
«Евразийский Национальный Университет» им. Л. Н. Гумилева,
г. Астана, Казахстан

Научный руководитель: PhD, ст. преп. Жаркимбекова А. Т.

В данной статье рассматривается методика анализа угроз информационной безопасности образовательной платформы «Платонус», широко используемой во многих Казахстанских университетах. Представлены актуальные угрозы, методы их выявления и меры по снижению рисков. На основе анализа предложен набор мер по защите данных, охватывающий технические, организационные и административные аспекты. В качестве метода исследования использовано тестирование на проникновение с применением инструментов Burp Suite, Nmap, OWASP ZAP и OpenVAS. Особое внимание уделено конфиденциальности пользователей, целостности данных и доступности сервисов. Выводы исследования могут быть полезны для администраторов образовательных платформ, специалистов по информационной безопасности и разработчиков цифровых образовательных систем. Целью исследования является обнаружение угроз и разработка методики их устранения для более безопасного использования образовательной среды за счёт системного подхода к оценке уязвимостей.

Ключевые слова: информационная безопасность (ИБ), анализ угроз, тестирование на проникновение, Платонус, образовательная платформа (ОП), Burp suite.

Введение. В связи с переходом большинства университетов на образовательные платформы, такие как Платонус и LMS (Learning Management System), вопросы стабильности и безопасности становятся все более важными. Процесс тестирования помогает выявлять и устранять уязвимости до их эксплуатации, защищая данные студентов и интеллектуальную собственность. Повышая производительность и безопасность платформы, разработка системы пентестинга способствует развитию онлайн-образования. Кроме того,

результаты тестирования могут быть использованы для улучшения общей производительности и удобства платформы, выявляя области, требующие доработки. Это способствует улучшению пользовательского опыта и повышает уровень внедрения платформы среди студентов и преподавателей.

Материалы и методы исследования. В качестве метода оценки защищённости использовано тестирование на проникновение. Были применены инструменты Kali Linux, такие как Nmap, Burp Suite и Metasploit. Также проведён анализ уязвимостей OWASP. Этот метод исследования включает наблюдение и запись данных без вмешательства в естественные процессы или поведение, которые изучаются. Исследование может включать наблюдение за активностью платформы и сетевым трафиком с целью обнаружения потенциальных уязвимостей или проблем безопасности в контексте проектирования системы тестирования на проникновение для ОП Платонус. Наблюдательное исследование может предоставить ценную информацию о состоянии безопасности системы, не внося никаких предубеждений или мешающих факторов.

Согласно статистике за последние 10 лет, количество потенциально вредоносных атак на казахские домены выросло в несколько раз по сравнению с 2010 годом. Так, в 2018 году, 19 февраля, более 40 казахстанских сайтов подверглись хакерским атакам по официальным данным TSARKA, крупнейшего поставщика услуг по кибербезопасности в Центральной Азии, также с учетом данных, полученных от KZ-CERT за последующие 3 года, количество инцидентов на периметре казахстанского домена выросло с 83,7% до 120,1%. Как мы видим, рыночный спрос на передовые решения по тестированию и смягчению уязвимостей только растет. определение объема и целей тестирования, систем, которые будут тестироваться, и методов тестирования, которые будут применяться. Сбор информации помогает узнать больше о работе цели и возможных уязвимостях.

Сканирование: Следующий шаг — выяснить, как целевое приложение реагирует на различные попытки вторжения. Обычно это достигается с помощью:

Статический анализ: Изучение исходного кода программы для прогнозирования ее поведения при выполнении. Такие инструменты могут сканировать весь код за один проход.

Динамический анализ: Исследование кода работающего приложения. Этот вид сканирования более полезен, так как предоставляет реальную картину функционирования приложения в реальном времени.

Результаты исследования. В ходе тестирования были выявлены такие уязвимости, как DOM-based open redirection, устаревшие JavaScript-библиотеки и включенный автозаполнение паролей. Для каждой из них предложены конкретные меры по устранению, включая валидацию URL, обновление

библиотек и отключение автозаполнения форм. Эти меры позволят значительно повысить безопасность платформы.

Заключение. Таким образом, разработка системы тестирования на проникновение для ОП Платонус является шагом к обеспечению более высокого уровня безопасности для казахстанских образовательных платформ. Кроме того, Проект демонстрирует, что сочетание новейших технологий совместно с методами методологии и анализа затрат могут помочь в защите конфиденциальных информацией и укреплении доверия к образовательным цифровым решениям. В нашие времена угрозы в сфере интернета становятся все больше и больше, и подобные действия становятся актуальными.

Список использованной литературы

1. Иванов А.К., Петрова Б.М. Анализ цифровой грамотности преподавателей вузов Казахстана // Журнал информационной безопасности. – 2023. – №4. – С. 56–72.

2. Каримов А. Б. Анализ угроз информационной безопасности в системах дистанционного образования // Вестник КазНУ. Серия информатики. – 2023. – №2(45). – С. 89–104.

3. Назарбаев Университет. Годовой отчет по информационной безопасности за 2023 год. – Нур-Султан, 2020. – 64 с.

DEVELOPMENT OF A METHODOLOGY OF PENETRATION TESTING OF THE EDUCATIONAL PLATFORM "PLATONUS"

Taubay N.M.

Scientific Supervisor: Zharkimbekova A. T.

This article discusses the methodology for analyzing information security threats to the educational platform "Platonus", which is widely used in many Kazakhstani universities. Current threats, methods for identifying them, and risk mitigation measures are presented. Based on the analysis, a set of data protection measures is proposed, covering technical, organizational, and administrative aspects. Penetration testing using Burp Suite, Nmap, OWASP ZAP, and OpenVAS tools was used as a research method. Particular attention is paid to user privacy, data integrity, and service availability. The findings of the study may be useful for administrators of educational platforms, information security specialists, and developers of digital educational systems. The purpose of the study is to detect threats and develop a methodology for eliminating them for safer use of the educational environment through a systematic approach to vulnerability assessment.

Keywords: information security (IS), threat analysis, penetration testing, Platonus, educational platform (EP), Burp suite

«PLATONUS» БІЛІМ БЕРУ ПЛАТФОРМАСЫНЫҢ ЕНУ ТЕСТІЛЕУ ӘДІСТЕМЕСІН ӘЗІРЛЕУ

Таубай Н.М.

Ғылыми жетекші: Жаркимбекова А. Т.

Бұл мақалада көптеген қазақстандық жоғары оқу орындарында кеңінен қолданылатын «Platonus» білім беру платформасына ақпараттық қауіпсіздік қатерлерін талдау әдістемесі талқыланады. Ағымдағы қауіптер, оларды анықтау әдістері және тәуекелдерді азайту шаралары ұсынылған. Талдау негізінде техникалық, ұйымдастырушылық және әкімшілік аспектілерді қамтитын деректерді қорғау шараларының кешені ұсынылады. Қолданылған зерттеу әдісі Burp Suite, Nmap, OWASP ZAP және OpenVAS құралдары арқылы ену тесті болды. Пайдаланушының құпиялылығына, деректердің тұтастығына және қызметтің қолжетімділігіне ерекше назар аударылады. Зерттеу нәтижелері білім беру платформаларының әкімшілері, ақпараттық қауіпсіздік мамандары және цифрлық білім беру жүйесін әзірлеушілер үшін пайдалы болуы мүмкін. Зерттеудің мақсаты – осалдықты бағалаудың жүйелі тәсілі арқылы білім беру ортасын қауіпсіз пайдалану үшін қауіптерді анықтау және оларды жою әдістемесін әзірлеу.

Кілт сөздер: ақпараттық қауіпсіздік (АҚ), қауіпті талдау, ену тестілері, Platonus, білім беру платформасы (ББП), Burp Suite.

REFERENCES

1. Ivanov, A.K., & Petrova, B.M. (2023). Analysis of Digital Literacy Among University Faculty in Kazakhstan. *Journal of Information Security*, (4), 56–72.
2. Karimov, A.B. (2023). Analysis of Information Security Threats in Distance Learning Systems. *Bulletin of KazNU. Series of Informatics*, 2(45), 89–104.
3. Nazarbayev University. (2020). *Annual Report on Information Security for 2023*. Nur-Sultan, 64 p.