Математические структуры и моделирование
2023. № 4 (68). С. 130–137

УДК 004.056.53
DOI 10.24147/2222-8772.2023.4.130-137

ФОРМИРОВАНИЕ ПРАКТИЧЕСКИХ НАВЫКОВ СТУДЕНТОВ ПРИ ИЗУЧЕНИИ ДИСЦИПЛИНЫ «АНАЛИЗ УЯЗВИМОСТЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ»

Д.Э. Вильховский
старший преподаватель, e-mail: vilkhovskiy@gmail.com

Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

Аннотация. Представлен обзор методики преподавания дисциплины «Анализ уязвимостей программного обеспечения», позволяющей не только обеспечить теоретическую подготовку будущих специалистов по защите информации, но и сформировать практические навыки обнаружения и анализа уязвимостей, а также внести вклад в формирование общепрофессиональной компетенции специалистов по компьютерной безопасности ОПК-2.

Ключевые слова: компьютерная безопасность, информационная безопасность, уязвимости программного обеспечения, обнаружение уязвимостей, bWAPP, Burp Suite.

Введение

Одной из общепрофессиональных компетенций выпускников специальности 10.05.01 «Компьютерная безопасность» является способность применять программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности (компетенция ОПК-2) [1].

В качестве формирующих данную компетенцию дисциплин может быть выбрана дисциплина «Анализ уязвимостей программного обеспечения», в рамках которой целесообразно не только обеспечивать теоретическую подготовку по номенклатуре, составу уязвимостей, но и проводить обучение по использованию различных отраслевых инструментов для выявления и устранения уязвимостей. Методика преподавания данной дисциплины должна быть основана на восхождении от простейшего к сложному, так как именно такой подход позволяет студентам сформировать устойчивые знания, не допуская возникновения хаоса.

Кроме того, при преподавании дисциплины необходимо применять практико-ориентированный подход. В отношении дисциплины «Анализ уязвимостей программного обеспечения» практикоориентированный подход предполагает получение студентами практических навыков работы с уязвимостями, т. е. не только знать в теории, какие типы уязвимостей и угроз существуют, но и научиться обнаруживать их, тем самым понимать возможную логику лиц, осуществляющих атаки. Кроме того, и что особенно важно, получение практических навыков работы по обна-

ружению уязвимостей способствует пониманию того, каким образом необходимо выстраивать безопасность программного обеспечения.

В качестве первичных инструментов, позволяющих студентам, обучающимся по специальности «Компьютерная безопасность», получить практическое представление об основных угрозах безопасности информации и уязвимостях программного обеспечения являются такие инструменты, как Burp Suite, а также специально созданное небезопасное веб-приложение bWAPP.

1. Изучение подмены запросов средствами Burp Suite

В настоящее время одной из самых распространенных и при этом самых простых атак является подмена запросов. В частности, это может быть подбор паролей для обхода защиты в виде аутентификации и вхождение в личный кабинет пользователя.

Отличным инструментом, позволяющим протестировать механизм осуществления подмены запросов, является платформа Burp Suite, позволяющая осуществлять тестирование на проникновение по различным направлениям, включая подмену запросов как уязвимости системы аутентификации к подбору паролей.

Перед тем как работать в программе, студентам рекомендуется обратиться к тьюториалу по использованию функционала программы (закладка Learn). Нажав на Start here, студент переходит на страницу, обучающую работе с программой, где подробно расписан общий функционал программы, включая модуль перехвата запросов и способы их модификации, а также различные инструменты.

1.1. Методология изучения подмены запросов средствами Burp Suite

С методической точки зрения следует отметить, что при изучении любой дисциплины степень усвоения материала студентом зависит от степени его вовлечённости и заинтересованности. В свою очередь, на вовлечённость и заинтересованность оказывает большое влияние практическая составляющая, а также соответствие предложенного к изучению инструментария актуальным проблемам современного мира. Причём даже не на профессиональном уровне (по сути, уровне каких-то пока ещё отдалённых информационных систем), а именно с точки зрения практической применимости в повседневной жизни – когда можно протестировать работу этого инструмента на том объекте, который интересен студенту в данный момент.

Таким образом, на первоначальном этапе освоения функционала Burp Suite являются его возможности в отношении подбора пароля, а следовательно, наиболее интересными для студентов здесь являются следующие инструменты:

- Proxy – модуль, позволяющий пользователю перехватывать запросы браузера, получая тем самым контроль над ними и проведением атак;
- Intruder – модуль, позволяющий перебирать параметры запроса и формировать атаки, после чего запускать их в автоматическом режиме.

Для получения доступа к запросам и, соответственно, возможности работы с подменами запросов нужно открыть вкладку Proxy и включить Перехватчик запро-

сов (режим Intercept is on). После студентам предлагается открыть браузер (нажимаем Open Browser) и ознакомиться с параметрами запросов, в том числе и с точки зрения того, с какими конкретно параметрами целесообразно работать далее в каждом конкретном запросе. А также базово ознакомиться с целевыми действиями, которые можно выполнить по каждому запросу:

- работать непосредственно в этом окне, отредактировав значения одного из / нескольких / всех параметров проведении атаки вручную, после чего переправлять запрос от браузера, нажав Forward;
- инициировать отказ браузера в отправлении запроса, нажав Drop;
- выполнить определённое целевое действие, нажав на Action – отправить запрос в Intruder, Repeater, Sequencer, Comparer, Decoder или Organizer.

Для изучения методов формирования автоматизированных атак студентам предлагается оправить один из запросов в Intruder (применится команда Send to в Intruder). При этом важно обратить внимание студентов, что для получения наилучшего эффекта следует выбирать такие запросы, в которых было бы достаточно большое количество параметров. Практика показывает, что именно изучение функционала инструмента Intruder вызывает у студентов максимальную вовлечённость.

При этом, предлагая к изучению функционала инструмента Intruder, также методически верным является учёт следующих аспектов.

1. Изучение каждого из четырех доступных режимов формирования атак необходимо производить последовательно, от простого к сложному (и самому интересному, открывающему множество возможностей):
    - Sniper – заданные подменяющие параметры (Payload) поочерёдно и последовательно подставляются только в один из выбранных для атаки параметров, пытаясь точечно пробить этот параметр;
    - Buttering ram – заданные подменяющие параметры (Payload) поочерёдно и последовательно подставляются во все выбранные для атаки параметры;
    - Pitchfork – набор подменяющих параметров (Payload) задаётся для каждого из выбранных для атаки параметров, после чего они применяются соответственно порядковому номеру атаки;
    - Cluster bomb – набор подменяющих параметров (Payload) может быть задан для каждого из выбранных для атаки параметров, после чего для каждого подменяемого параметра поочерёдно подставляются все подменяющие параметры, заданные для этого запроса в целом, т. е. подменяющие параметры, задаваемые не только для этого конкретного подменяемого параметра, но и для других параметров также.
2. По каждому из режимов необходимо обращать внимание студентов на количество создаваемых вариантов нагрузок и запросов (соответственно, Payload count и Request count), а также на ключевые особенности каждого из режимов.

Например, в качестве таких особенностей можно выделить следующие:

- По режиму Sniper. Всегда изменяется всегда только 1 параметр, а количество сформированных запросов определяется как количество подменяющих параметров (Payload), возведенное в степень количество подменяемых параметров;
- По режиму Buttering ram. Первый раз в данном режиме запрос отправляется с неизменёнными параметрами, а затем каждый из заданных подменяющих параметров подставляется во все выбранные для изменения параметры;
- По режиму Pitchfork. Для первой атаки для каждого из изменяемых параметров возьмёт первый из соответственно заданного набора подменяющих параметров, для второго – второй и так далее. Таким образом, количество атак обусловлено минимальным количеством подменяющих параметров среди всех подменяемых параметров. То есть если при выборе трёх параметров для атаки для первого параметра задать набор из четырёх подменяющих параметров, а для второго – набор из двух, а для третьего – набор из трёх подменяющих параметров, то количество сформированных атак будет равняться двум;
- По режиму Cluster bomb. Режим полного перебора, позволяет не вручную указывать подменяющие значения, а задавать их, используя один из предложенных типов нагрузки (Payload type).

  Одним из широко используемых задаваемых типов нагрузки является тип Brute forcer (режим полного автоматического перебора). Здесь в наборе подменяющих параметров (Caracter set) задаётся набор символов, из списка которых будет осуществляться перебор. В Min length и Max length, соответственно, задаётся минимальная и максимальная длина значения подменяющего параметра.

  Соответственно, количество сгенерированных подменяющих параметров (Счётчик нагрузок) и количество сформированных атак (Счётчик запросов) может быть огромен.

  Например, если для двух подменяемых параметров задать 4 значения вручную, а для третьего – выбрать тип Brute forcer, и в типе данных задать все цифры от 0 до 9 и все буквы латинского алфавита, указав минимальную и максимальную длину 4, то счётчики нагрузок и запросов будут, соответственно, равны 1 679 616 и 26 873 856. То есть будет в общей сложности проведено почти 27 миллионов атак.

  Если оставить значения, заданные вручную, только для одного из параметров, а для двух оставшихся задать Brute forcer с указанным выше набором значений для перебора, то количество запросов (подмен) составит уже более 1,5 миллиардов;
- По всем режимам. Работают со всеми типами данных; понять, была ли атака успешной, можно по коду статуса (Status code).

2. Ознакомление с инструментами обучения работе с уязвимостями, доступными на платформе GitHub

После изучения достаточно простого, но, как показывает практика, очень интересного студентам материала по подмене запросов следует начать углубляться в изучаемую дисциплину.

Для этого рекомендуется обратиться к инструментам обучения по работе с уязвимостями, доступными на платформе GitHub [2]. На платформе собран большой и всеобъемлющий перечень подобных инструментов в разделе Awesome Vulnerable Applications, посвящённом приложениям с уязвимостями.

В качестве знаний, необходимых для работы с данной платформой, можно выделить в первую очередь необходимость знания английского языка, так как вся информация, содержащаяся на платформе, представлена именно на английском языке. С одной стороны, обращение к англоязычным ресурсам позволит развить междисциплинарные навыки, в данном случае обуславливая необходимость глубокого изучения английского языка, владение которым является в наши дни практически необходимым навыком для инженеров-программистов и специалистов по защите информации. С другой стороны, возможность работы с материалом, представленным на платформе, доступна даже для тех студентов, уровень владения английским языком которых невысок – достаточно в браузере запустить команду «Перевести на русский язык». Конечно, в некоторой степени возможны определённые ограничения в связи с особенностями лексики или же не всегда корректной работы встроенного переводчика (алгоритмы которого, к слову, постоянно совершенствуются и уже сейчас находятся на достаточно высоком уровне, зачастую близком к человеческому переводу).

Итак, дадим краткую характеристику раздела Awesome Vulnerable Applications платформы GitHub. Во-первых, здесь собран большой набор различных уязвимостей, а также большой объем теоретической информации по уязвимостям, включая не только OWASP top 10 уязвимостей для веб-приложений, но и уязвимости виртуальных машин. Таким образом, студентам рекомендуется сперва изучить теоретические основы существующих уязвимостей.

Во-вторых, в разделе Awesome Vulnerable Applications собраны ссылки на различные онлайн-сервисы, позволяющие потренироваться в нахождении уязвимостей. Студентам рекомендуется изучить материалы, представленные в данном разделе, и поработать с полезными инструментами, позволяющими глубоко усвоить материал и прокачать навыки по информационной безопасности.

В качестве наиболее интересных в наших целях подразделов здесь можно выделить следующие:

- OWASP Top 10 – раздел, посвящённый безопасности веб-приложений, в котором содержится множество веб-приложений со встроенными уязвимостями и лабораторий для пентестов;
- Cloud Security – раздел, посвящённый облачной безопасности, в собранном перечне которого есть в том числе Kubernetes и AWS инфраструктуры со встроенными уязвимостями;

- Mobile Security – раздел, посвящённый безопасности мобильных приложений;
- Vulnerable VMs – раздел, посвящённый уязвимостям в виртуальных машинах;
- тематические разделы, посвящённые SQL-, XSS- и XXE-инъекциям, подделке запросов на стороне сервера и контрабанды запросов, а также проблемам неправильной конфигурации CORS.

В целом можно сказать, что раздел Awesome Vulnerable Applications с методической точки зрения выстроен достаточно хорошо: по каждому инструменту даётся краткая характеристика, на основании которой можно получить представление о том, какие задачи решает данный инструмент и какие навыки позволяет сформировать. Также наименование каждого инструмента выполнено в виде гиперссылки, ведущей на ветку, посвящённую исключительно данному инструменту. При этом в описании инструмента, содержащегося непосредственно в посвящённой ему ветке, достаточно подробно указывается, какие уязвимости содержит данный инструмент. Это позволяет студентам при минимальных временных затратах получить максимум информации о том, насколько данный инструмент интересен им для решения поставленных перед ними задач, например, в рамках самостоятельной работы, и, конечно же, исследовать различные небезопасные приложения и облачные инфраструктуры и др. То есть сформировать практические навыки поиска и анализа уязвимостей.

3. Формирование у студентов практических навыков обнаружения уязвимостей веб-приложений на примере небезопасного веб-приложения bWAAP

Формирование у студентов практических навыков обнаружения уязвимостей веб-приложений является ещё одной практикоориентированной составляющей предложенной методики преподавания дисциплины «Анализ уязвимостей программного обеспечения». С этой точки зрения наиболее полезным является раздел OWASP Top 10, посвящённый именно уязвимостям в веб-приложениях.

Среди небезопасных веб-приложений, представленных в данном подразделе, на наш взгляд, особенную ценность с точки зрения формирования у студентов практических навыков обнаружения уязвимостей в веб-приложениях представляет приложение bWAPP.

bWAPP является достаточно старым приложением (последний коммент на GitHub от декабря 21 года). Однако его ценность состоит в том, что с его помощью можно прицельно и максимально полно изучать отдельные уязвимости, в том числе и в их различных вариациях. С точки зрения методики обособление каждого типа уязвимостей и прицельная работа с какой-либо из них является особенно полезной, когда студент находится только в начале пути освоения основ информационной безопасности. По сути, это дидактическая единица, освоить которую необходимо прежде, чем попасть в реалии нескольких одновременно существующих дидактических единиц, или, что ещё более вероятно, реалии проведения тестов на проникновение,

реалии полной неопределённости, когда заранее неизвестно, какая уязвимость существует и каким образом она может быть отработана (тип атаки).

По работе с приложением bWAPP разработана очень подробная инструкция, её можно легко найти, вбив в строку поиска запросы типа «bWAPP tutorial» или же «bWAPP examples». В инструкции в содержании указаны все уязвимости, существующие в этом небезопасном приложении.

При этом в разделе, посвящённом отдельному типу уязвимостей, даётся пример её воспроизведения в уже известной нам программе Burp Suite, со скриншотами. Таким образом, студенты могут научиться воспроизводить предлагаемый способ атаки на данную уязвимость, т. е. осуществлять поиск уязвимости данного типа и её последующий анализ.

Что касается непосредственно работы с самим приложением bWAPP, в приложении есть выпадающий список, где можно выбрать уязвимость, навыки обнаружения и атаки на которую студент желает сформировать.

Отметим, что приложение содержит в общей сложности около 100 уязвимостей разного рода (наиболее распространённые уязвимости из OWASP Top 10), каждую из которых можно воспроизвести прицельно.

4. Заключение

Таким образом, предлагаемая методика преподавания дисциплины «Анализ уязвимостей программного обеспечения» представляет собой трёхступенчатую последовательность формирования у студентов практических навыков работы с уязвимостями.

1. Изучение подмены запросов средствами Burp Suite, позволяющее начать изучение уязвимостей с базовых вещей и сформировать у студентов общую вовлечённость в проблематику.

2. Ознакомление с инструментами обучения работе с уязвимостями, доступными на платформе GitHub, позволяющее получить достаточно полное представление о том, какие уязвимости существуют, особенности их жизнедеятельности в различных системах (веб- или мобильных приложениях, виртуальных машинах и облачных системах), а также сформировать вектор направления дальнейшей работы с уязвимостями в рамках как аудиторной, так и самостоятельной работы студентов.

3. Формирование у студентов практических навыков обнаружения уязвимостей веб-приложений на примере небезопасного веб-приложения bWAAP, позволяющее получить практические навыки обнаружения и анализа отдельных наиболее распространённых уязвимостей веб-приложений.

   В качестве дальнейшего вектора самостоятельной работы студентов, желающих углубить свои навыки обнаружения уязвимостей в веб-приложениях, можно выделить работу с приложением OWASP Juice Shop. Это ещё одно приложение, специально созданное со многими уязвимостями, относящееся,

в отличие от bWAAP, не к категории приложений, обучающих основам, а к категории приложений-челленджей.

Литература

1. Приказ от 26 ноября 2020 г. № 1459 «Об утверждении федерального государственного образовательного стандарта высшего образования – специалитет по специальности 10.05.01 Компьютерная безопасность». URL: `https://fgos.ru/fgos/fgos-10-05-01-kompyuternaya-bezopasnost-1459/` (дата обращения: 28.11.2023).
2. Раздел Awesome Vulnerable Applications на платформе GitHub. URL: `https://github.com/vavkamil/awesome-vulnerable-apps` (дата обращения: 28.11.2023).

DEVELOPING STUDENT PRACTICAL SKILLS BY THE SOFTWARE VULNERABILITY ANALYSIS COURSE

D.E. Vilkhovsky
Assistant Professor, e-mail: vilkhovskiy@gmail.com

Dostoevsky Omsk State University, Omsk, Russia

Abstract. The paper provides an overview of the methodology for teaching the discipline Software Vulnerability Analysis course methodology, which allows not only to provide future information security specialists with theory on the software vulnerability, but to develop their practical skills in detecting and analyzing these vulnerabilities, as well as contribute to their gaining general professional competence GPC-2.

Keywords: computer security, information security, software vulnerabilities, vulnerability detection, bWAPP, Burp Suite.

Дата поступления в редакцию: 28.11.2023