



ПРЕИМУЩЕСТВА ИСПОЛЬЗОВАНИЯ WAF ДЛЯ ЗАЩИТЫ ВЕБ-ПРИЛОЖЕНИЙ – ЧАСТЬ 2

Майкл Койфман (Michael Koefman), главный разработчик глобальных решений Netskope, США

Поговорим на примере о самой последней уязвимости Apache Struts и кратко опишем, какое внедрение стратегии безопасности поможет защититься от атак нулевого дня.

Начало статьи читайте в [части 1](#).

За последние несколько лет в Apache Struts обнаружился ряд уязвимостей. Компания F5 впервые [обезвредила их](#) в 2014 году. В марте 2017 года обнаружилась еще одна критическая уязвимость, связанная с удаленным исполнением кода. Специалист по безопасности компании F5 Гал Голдштейн [описал подробности закрытия уязвимости и меры, которые необходимо предпринять в системе ASM для снижения рисков безопасности](#). А седьмого июля был выпущен информационный бюллетень, описывающий следующую уязвимость, связанную с удаленным выполнением кода на веб-фреймворке Struts 2.

К счастью, правильно внедренная в ASM стратегия безопасности в большинстве случаев защищает от уязвимостей нулевого дня. О том, каким образом это происходит, написано в [статье](#) Гала Голдштейна. Выводам специалиста по безопасности F5 стоит доверять. Но вот в чем вопрос – каковы последствия реальной атаки на систему информационной безопасности компании?

Чтобы ответить на него, обратимся к логам ASM, в которые несколько недель назад внедрили стратегию безопасности для защиты целевого приложения.

Вот скриншот с журналом логов ASM, в котором были найдены записи, содержащие слово **struts** в URI:



ПРЕИМУЩЕСТВА ИСПОЛЬЗОВАНИЯ WAF ДЛЯ ЗАЩИТЫ ВЕБ-ПРИЛОЖЕНИЙ – ЧАСТЬ 2

The screenshot displays the F5 WAF interface. At the top right, a box indicates 'Total Entries: 141'. Below this, a summary bar shows 'Attack signature detected [11]' and 'HTTP protocol compliance failed [2]'. A red arrow points to a message: 'Latest Struts 0-day attack triggers 11 attack signatures in ASM!'. The main log entry is for a request to '/struts/index.do' from the United States, with a violation rating of 5. The 'Attack Types' list includes: Non-browser Client, Other Application Attacks, Predictable Resource Location, Server Side Code Injection, Command Execution, and HTTP Parser Attack. The 'Request' tab is selected, showing the following details:

```
Request actual size: 1258 bytes.
POST /Struts/index.do HTTP/1.1
Host: [redacted]:443
User-Agent: curl/7.47.0
Accept: */*
Content-Type: multipart/form-data; boundary=-----24857537117525
Connection: close
Content-Length: 1032
-----24857537117525
Content-Disposition: form-data; name="upload"; filename="%{(#nike='multipart/form-data').(#dm=@ognl.Ognl
```

Как видите, отчет был создан девятого июля, – всего через пару дней после объявления об уязвимости Struts. Число, выделенное в верхнем правом углу, показывает, что система сохранила записи о 141 выполненном запросе к целевому приложению (маленькому сайту без рекламы), которые были заблокированы как уязвимости Struts. Скриншот с последним вредоносным запросом показывает эффективность стратегии безопасности для защиты от последней уязвимости.

Во-первых, стратегия безопасности заблокировала запрос, потому что IP-адрес присутствует в заголовке хоста. Получается, что даже если стратегия безопасности не обнаружила характерные сигнатуры или методы сокрытия, позволяющие обнаружить эксплойт, запрос в любом случае будет заблокирован как неправомерный. Имеется также другое нарушение соответствия протоколу HTTP, которое выделено красным цветом, – это искажение формата заголовка типа контента.

Но это только на пользу. Во всем входном потоке запросов ASM нашел **11** различных характерных сигнатур. Почему система отреагировала на такое количество? Причина в том, что в ходу целый ряд способов использования данной уязвимости. Для остановки атаки нужно обнаружить только одну характерную сигнатуру. А их общее число показывает, насколько изощренными могут быть запросы эксплойтов, ведь они используют комбинацию методов и уязвимостей.



ПРЕИМУЩЕСТВА ИСПОЛЬЗОВАНИЯ WAF ДЛЯ ЗАЩИТЫ ВЕБ-ПРИЛОЖЕНИЙ – ЧАСТЬ 2

Однако поскольку наш материал называется «Преимущества использования WAF для защиты веб-приложений», то следует продемонстрировать и экономическую выгоду от его использования. В сентябре 2016 года [вышло много новостей](#) о студенте Райне Пикрене, который заработал 15 миллионов миль, участвуя в программе Bug bounty от авиакомпании United Airlines. Этот авиаперевозчик платит специалистам по безопасности, которые сообщают о различных уязвимостях, обнаруженных на публичных сайтах компании. Хотя информация об ошибках, обнаруженных в программе bug bounty, конфиденциальна, можно сделать вывод, что с большой долей вероятности Пикрен налетал **15 миллионов миль**.

United Airlines оценила уязвимость удаленного кода (тот же класс, что и уязвимость Struts 2, про которую мы только что говорили) как одну из самых дорогостоящих, соответствующих 1 миллиону миль. Поэтому можно сделать обоснованный вывод, что Пикрен обнаружил 15 проблем с удаленным кодом. Сколько это стоило компании United Airlines? Они оценивают каждую милю в \$0,02, поэтому ущерб можно оценить в **\$300 тысяч**. И, конечно же, Пикрен – не единственный энтузиаст, который собрал миллионы миль от компании United Airlines, – имеются и [другие](#). Программный продукт WAF определенно стоит дешевле.



Группа компаний БАКОТЕК – официальный дистрибьютор F5 Networks в Украине, Азербайджане, Республике Беларусь, Грузии, Армении и Молдове.
<https://bakotech.com>, f5@bakotech.com, +38 044 273 33 33.

F5 Networks, Inc.

401 Elliott Avenue West, Seattle, WA 98119
888-882-4447 f5.com

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com