Доклад

Email-инъекции

Смирнов-Мальцев Егор Дмитриевич

Содержание

Список иллюстраций

1 Введение

Цель работы

Изучить основные виды атак, использующих email-инъекции, а также способы защиты от них.

Задачи

- Описать уязвимости email протоколов
- Привести примеры атак, использующих эти уязвимости
- Пеечислить способы защиты от подобных атак

Актуальность

Электронная почта — одна из самых популярных форм обмена информацией между пользователями. однако, она может быть уязвима для инъекций, отправленных через пользовательский ввод. В распоряжении атакующего оказывается цепочка из компонентов различных реализаций. Такая функциональность — просторное поле для анализа и проведения не одного, но сразу нескольких видов инъекций.

Ход времени, конечно, неизбежно приводит к сокращению числа уязвимостей и случаев использования электронной почты в качестве хранилища. Тем не менее никто никуда не вымер: формы в веб-приложениях крупных компаний всё так же возвращают отладочные SMTP логи, в веб-приложениях компаний поменьше – отправляют ответы самописными средствами, а уязвимости и вовсе имеют обыкновение появляться вновь.

Поэтому рассматриваемая тема остаётся полезной для ознакомления и любопытной для изучения.

2 Основы работы почты

2.1 Протоколы

Работа почты осуществляется с помощью специальных почтовых протоколов.

Существует некоторое количество почтовых протоколов, из которых принято использовать:

- POP, Post Office Protocol
- IMAP, Internet Message Access Protocol
- SMTP, Simple Mail Transfer Protocol

Протокол SMTP используется для отправки сообщений. Протоколы IMAP и POP используются для получения сообщений.

- Функциональность веб-приложения для отправки сообщений потенциально использует пользовательский ввод для взаимодействия с SMTP сервером;
- Функциональность веб-приложения для чтения сообщений потенциально использует пользовательский ввод для взаимодействия с IMAP сервером;

2.2 Почтовые компоненты

Почтовый клиент:

MUA — Mail User Agent; Компонент, с которым взаимодействует пользователь для осуществления работы с почтой

Почтовый сервер:

- MTA — Mail Transfer Agent; Компонент, пересылающий почту между почтовыми серверами
- MDA — Mail Delivery Agent; Компонент, доставляющий почту пользователю

2.3 Конструкция письма

Письма, посылаемые с помощью почтового протокола SMTP, должны состоять из нескольких частей: конверта + самого письма.

Конверт — информационная обёртка над письмом, запрашиваемая SMTP протоколом:

```
MAIL FROM: Отправитель
RCPT TO: Получатель
DATA: Начать письмо
```

Письмо — передаваемое сообщение. Включает в себя:
Заголовки:

- Content-Type: Тип содержимого
- From: Отправитель
- To: Получатель
- Subject: Тема
- Date: Дата и время
- Cc, Bcc, …

Тело письма — непосредственно содержимое сообщения.

2.4 Специальные конструкции

Для корректной работы протоколов используются следующие специальные конструкции:

- Возврат каретки (Carriage Return): = %0D = 0x13
- Перевод строки (Line feed): = %0A = 0x10
- Пробел (Space): = %20 = 0x32

<SP>: Отделяет команду от аргументов <CRLF>: Закрывает команду; Разделяет строки письма <CRLF>.: Закрывает письмо

3 Потенциальные уязвимости

3.1 CRLF инъекции

Почтовые клиенты, которым передаётся в недостаточной мере обработанный пользовательский ввод, могут оказаться уязвимы к CRLF инъекциям – внедрению вышеописанных специальных конструкций для влияния на поведение почтовых протоколов.

В случаях, когда подконтрольные пользователю данные впоследствии оказываются частью исполняемой клиентом команды, атакующим могут быть внедрены специальная конструкция , закрывающая текущую команду, а также специальная конструкция ., закрывающая письмо, для вывода полезной нагрузки за пределы предоставленной для заполнения секции письма.

Эксплуатация CRLF инъекции приведёт к возможности исполнения атакующим команд, определённых для используемого почтового протокола, что в свою очередь, в зависимости от целей атакующего, может привести к следующим последствиям: * Возможность взаимодействия с локальными почтовыми серверами * Утечка конфиденциальной информации * Обход накладываемых на пользователя ограничений (обход капчи, рейт лимитов, ...). Как следствие, злоупотребление выделенными ресурсами, DoS * Фишинг + рассылка вредоносного ПО * Спам

3.2 Arbitrary Command Flag Injection

Почтовые сервера, которым передаётся в недостаточной мере обработанный пользовательский ввод, могут оказаться уязвимы к инъекциям во флаги команды – внедрению дополнительных опций в исполняемую на целевой машине команду, которая отвечает за запуск почтового компонента.

В случаях, когда подконтрольные пользователю данные впоследствии оказываются среди аргументов исполняемой на целевой машине команды, атакующим могут быть внедрены дополнительные опции для влияния на поведение запускаемого компонента.

Последствия эксплуатации инъекции во флаги команды зависят от конкретного компонента, но нередко заключаются в возможности осуществления атакующим записи в файлы на целевой машине (Arbitrary File Write) и в вытекающей из этого возможности удалённого исполнения кода (Remote Code Execution) через внедрение атакующим веб-шелла.

4 Способы защиты от email инъекций

4.1 Защита от CRLF-инъекций

Предотвращение CRLF-инъекций требует строгого контроля над тем, что может быть введено в систему. Использование функций кодирования специальных символов, проверка и очистка пользовательского ввода – ключевые методы защиты. Разработчики должны быть осведомлены о том, как данные обрабатываются и передаются в их приложениях, чтобы предотвратить возможность таких атак.

Перенесите весь сервис, требующий входящих соединений (http, SMTP), на отдельную машину и оставьте ее в открытой сети. Удалите с этой машины все программы и информацию, не относящуюся к ее назначению. Все остальные машины спрячьте за файрволом с полным отключением входящего трафика. [1]

5 Выводы

В результате работы были рассмотрены основные уязвимости email протоколов для SQL инъекций.

Список литературы

1. Медведовский И. Д. П.В.В. Семьянов П. В. Атака через интернет. 1-е изд. СПб.: Мир и семья-95, 1997.