Web Application Penetration Testing

whoami

Bogomolov Egor

Links

Comment

Telegram: @empty_jack

Telegram Channel: @YAH_Channel

E-mail: empty.jack@yandex.ru

Corp: e.bogomolov@hackeru.com

Certificates

Offensive Security Certified Professional (OSCP)

Work experience

Positive Technologies | InfoSec.ru | Bi.Zone | Wallarm | HackerU

Now

Independent Security Expert

ТЕМЫ КУРСА

1. Введение.
2. Обзор веб-технологий
3. Структура веб-приложений
4. Первоначальный анализ, сбор информации
5. Уязвимости серверной части веб-приложений
6. Тестирование механизмов аутентификации и менеджмента сессий
7. Логические уязвимости
8. Безопасность протокола HTTP
9. Безопасность клиентской части веб-приложений
10. Вопросы на собеседовании

HACKERU

ТЕМЫ ЗАНЯТИЯ

- Обзор тестирования веб-приложений
- Что есть полезного для изучающих пентест веба
- HTTP
- Кодировки в вебе
- HTTPS vs HTTP
- HTML, Javascript, CSS.

HACKERU

Обзор тестирования веб-приложений

HACKERU

Проект

- Пресейл - определение объема работы и уточнение деталей
- Договор
- Авторизационное письмо - перед началом работы клиент подтверждает что разрешает такой-то компании его пенетрировать, с таких то IP-адресов, в такие то даты и т.д. и т.п.
- Непосредственный анализ защищенности
- Формирование рекомендаций и написание отчета.

Тестирование

Тестирование веб-приложений может быть как отдельным проектом, так и входить в более крупный проект (например, в проект по внешнему тестированию на проникновение)

Подходы к анализу

- Черный ящик - специалисту не известно ничего о системе
- Серый ящик - клиент предоставляет ограниченный доступ, например, с правами обычного пользователя
- Белый ящик - клиент предоставляет полный доступ к приложению, в том числе к исходным кодам

HACKERU

Что есть полезного для изучающих пентест веба

HACKERU

OWASP - Open Web Application Security Project

- [Testing Guide]
- [Cheat sheets]
- [Developer Guide]
- [OWASP Top 10]

HACKERU

Portswigger Web Security Academy

https://portswigger.net/web-security

Тут есть как текстовые материалы, так и лаборатории, в которых можно упражняться

HackerU

Площадки для тренировок

- Capture the Flag (CTF) - соревнования хакеров
  - https://ctftime.org/ - агрегатор

Основные категории:

- web
- crypto
- reverse
- binary (он же pwn, он же exploit)
- forensics
- osint

HackerU

Площадки для тренировок

- ever CTF
  - https://www.root-me.org/
  - https://w3challs.com/
- Vulnerable Applications
  - bWAPP
  - Damn Vulnerable Web Application
  - etc

HACKERU

Bug Bounty

Поиск уязвимостей за вознаграждение

- https://www.hackerone.com
- https://bugcrowd.com

HACKERU

Площадки для тренировок

Статья 272 УК РФ. Неправомерный доступ к компьютерной информации

Программное обеспечение

- **Burp Suite**
- **Сервис хранения заметок**

Репозитории на github

- https://github.com/danielmiessler/SecLists - словари для всех случаев жизни
- https://github.com/swisskyrepo/PayloadsAllTheThings - информация по эксплуатации различных уязвимостей
- https://github.com/tennc/webshell - коллекция веб-шеллов

HACKERU

HTTP

HACKERU

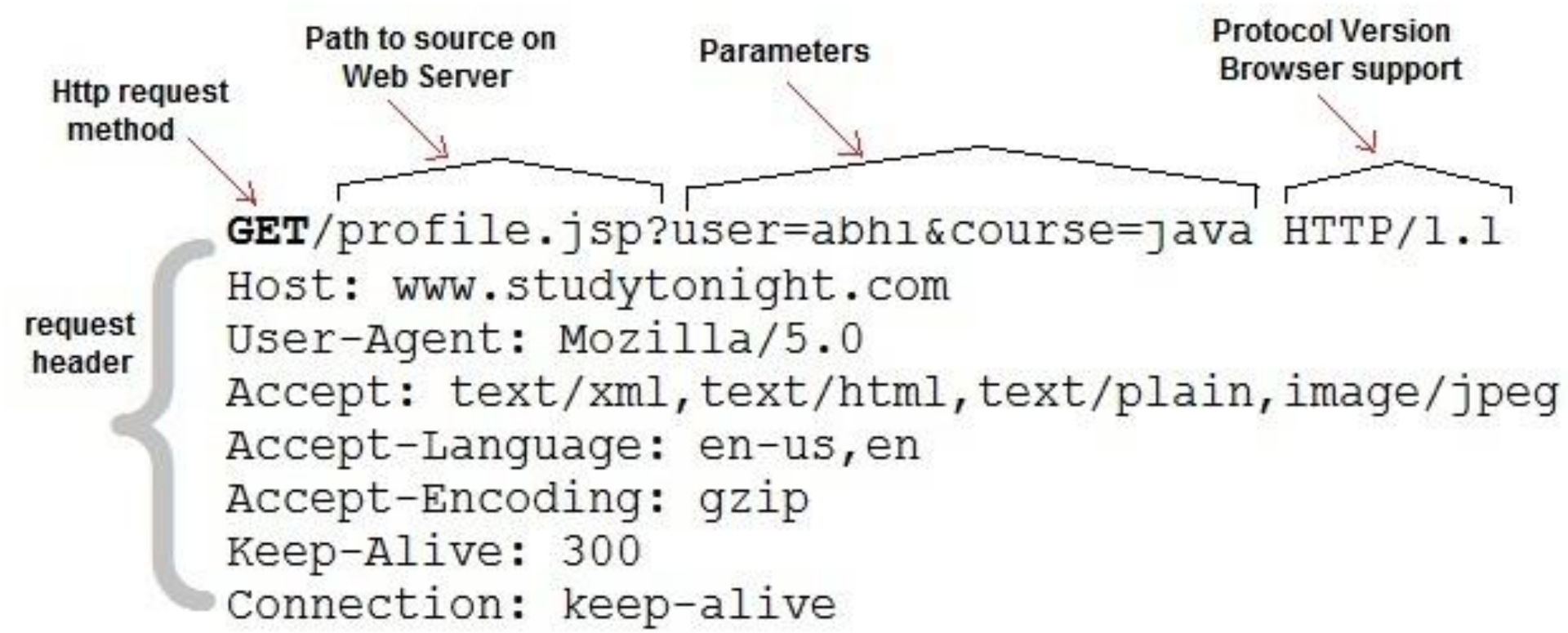
HTTP

HyperText Transfer Protocol

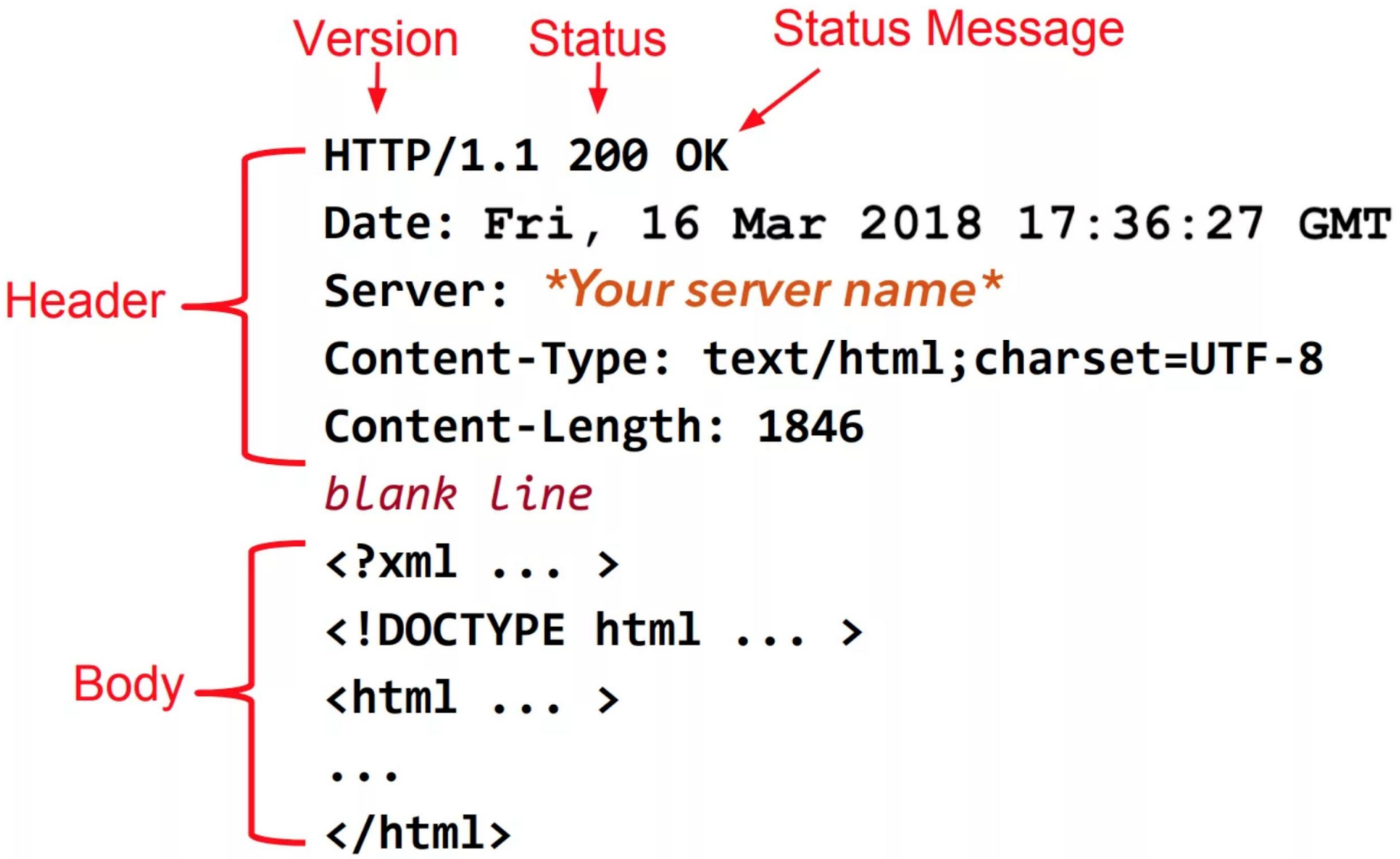
- Протокол 7 уровня ISO OSI.
- Работает поверх TCP.
- Клиент-серверный протокол
- Сейчас используются две версии: HTTP/1.1 и HTTP/2

HackerU

HTTP request



HTTP response



HACKERU

Методы HTTP (HTTP verbs)

Метод – операция, выполняемая над ресурсом.

Виды методов:

- **GET – получает содержимое узла (Read)**
- **POST – передаёт пользовательские данные (Write).**
- **PUT – загружает содержимое на сервер, чаще обновляет существующее (Update)**
- **DELETE – удаляет указанный ресурс (Delete)**
- **HEAD – аналогичен GET, но возвращает только заголовки**
- **OPTIONS – определение параметров сервера (почти не используется).**
- **и другие (TRACE, PATCH, CONNECT).**

HACKERU

Коды состояния ответов HTTP

Код состояния:

- 1xx – информационной (102 Processing);
- 2xx – успех (200 OK);
- 3xx – перенаправление (301 Moved Permanently);
- 4xx – ошибка клиента (400 Bad Request);
- 5xx – ошибка сервера (500 Internal Server Error)

HACKERU

URL - Uniform Resource Locator

Структура: schema://host:port/path?parameter=value#anchor

Схема: http, https, ftp и другие;
Узел: доменное имя или IP-адрес;
Порт: порт ресурса (80 – порт по умолчанию для HTTP);
Путь: путь к ресурсу;
Параметр: отправляемые на сервер переменные имеют вид – parameter0=value0&parameter1=value1;
Якорь: идентификатор элемента HTML внутри документа для перемещения браузера на него;

HTTP - текстовый протокол

Демонстрация запроса через nc

HACKERU

Демонстрация и настройка среды

Burp
FoxyProxy
Инструменты разработчика браузера

HACKERU

HTML

HackerU

HTML - HyperText Markup Language

Язык разметки гипертекста.

Является XML-образным языком.

(демонстрация)
<body>
<title>
<hX>
<a>
<form>
<input>

HACKERU

Javascript и CSS

Javascript - язык программирования, который позволяет работать с отображаемыми в браузере элементами. Позволяет создавать динамические веб-интерфейсы

CSS - Cascading Style Sheets - язык описания внешнего вида документа. Декларирует как браузер должен отображать тот или иной элемент HTML.

HACKERU

Кодировки в вебе

HEX - кодирует каждый символ в два символа из набора `0123456789abcedf'. Шестнадцатиричная кодировка `admin/test` -> `61646d696e2f74657374`

URL - кодирует некоторые символы в HEX, добавляя перед ними символ %
`admin/test` -> `admin%2ftest`

Base64 - кодирует 3 байта в 4 символа из набора [a-z A-Z 0-9] а также / и +. В конце может быть несколько символов = для выравнивания.
`admin/test` -> `YWRtaW4vdGVzdA==`

HACKERU

Кодировки в вебе

Демонстрация кодировок

CyberChef: https://gchq.github.io/CyberChef/

Burp

Автоматическая URL-кодировка параметров

HACKERU

Кодировки в вебе

Практика.

Раскодируйте:

1) 4865782d656e636f64696e67272068657265
2) %48%34%43%6b%33%52%59%30%55
3) %22hack%65r%22%20%69%73%20%68er%65%3f
4) SSBMaUszIFAzbIQzc3Q=

HACKERU

HTTP vs HTTPS

HTTPS - это тот же HTTP, который работает поверх SSL/TLS.

Данные передаваемые по HTTPS криптографически защищены от перехвата в канале (просмотра и модификации).

Важные данные не должны передаваться по HTTP без шифрования.

HACKERU

Content-Type

Content-Type - заголовок HTTP. Определяет тип передаваемого содержимого. В зависимости от него веб-приложение и браузер будут обрабатывать тело HTTP по разному

Для указания формата использует MIME типы.

Content-Type

Браузер как правило использует в запросах:

text/plain
application/x-www-form-urlencoded
multipart/form-data

<демонстрация различия>

Content-Type

Веб-приложение использует в ответах:

text/html
text/javascript
text/css
application/json
text/xml
и многие другие.

Практика

Задачи на Root-me:

- HTML source
- HTTP - User-agent
- HTTP - Headers
- HTTP - Improper redirect
- HTTP - Verb tampering
- HTTP - Open redirect

HACKERU

Тест для самопроверки

В LMS

HACKERU

Дополнительные задания

Оставшиеся задания на root-me

HACKERU

Спасибо за внимание!

Богомолов Егор
telegram: @empty_jack

HackerU