Smashing the Web for Fun and Profit

Beginner's Guide to Web Security

0xh0russ

Table of contents

01

What is HTTP?

An overview of the HTTP protocol and its roots.

02

HTTP Format

The skeleton of an HTTP packet.

03

BurpSuite

The #1 tool for web security testing.

04

Common Web Vulnerabilities

Two of the most common web security risks.

05

Demo

Live hacking on a live HackTheBox machine.

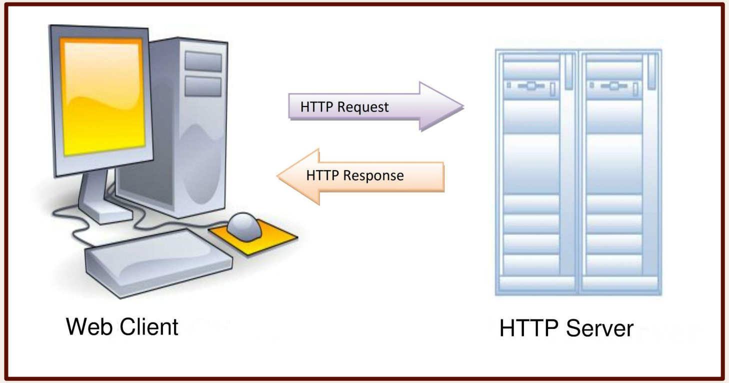
01

What is HTTP?

Roots and modern usage.

About HTTP

- Application Layer Protocol
- Consists Request/Response Pairs
- The standard protocol for client/server setups.
- The backbone of the modern internet.



HTTP Across Time

1989

Invention

HTTP was part of a proposal written by Tim-Berners Lee while working at CERN for the internet. It is a method of delivering HTML documents.

1994

Introduction of SSL

Netscape Communications introduces HTTP over SSL or HTTPS. This provides security and allows the web to be used for applications with higher security requirements such as e-commerce.

2023

HTTP Today

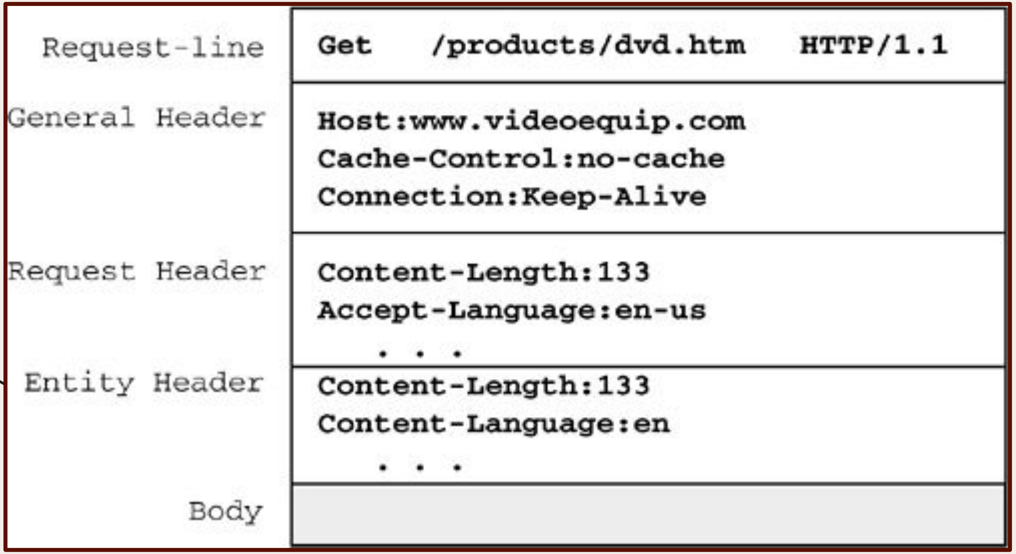
More versions of HTTP were released like HTTP2 and HTTP3 which offer a higher degree of efficiency. HTTP today is the protocol of choice for most applications where a client-server architecture is desired.

02

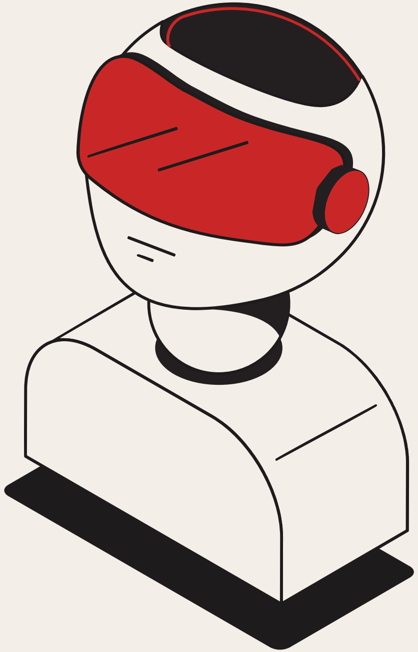
HTTP Format

The skeleton of an HTTP Message

HTTP Request



Request-line	Get /products/dvd.htm HTTP/1.1
General Header	Host:www.videoequip.com Cache-Control:no-cache Connection:Keep-Alive
Request Header	Content-Length:133 Accept-Language:en-us . . .
Entity Header	Content-Length:133 Content-Language:en . . .
Body	



HTTP Verbs

GET

- The `GET` method requests a representation of the specified resource. Requests using `GET` should only retrieve data.

POST

- The `POST` method submits an entity to the specified resource, often causing a change in state or side effects on the server.

HEAD

- The `HEAD` method asks for a response identical to a `GET` request, but without the response body.

OPTIONS

- Venus has a beautiful name and is the second planet from the Sun

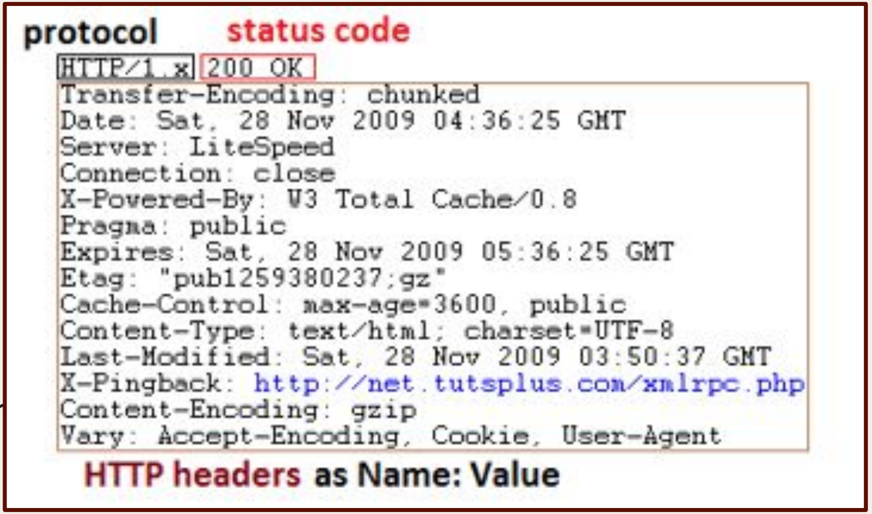
PUT

- The `PUT` method replaces all current representations of the target resource with the request payload.

PATCH

- The `PATCH` method applies partial modifications to a resource.

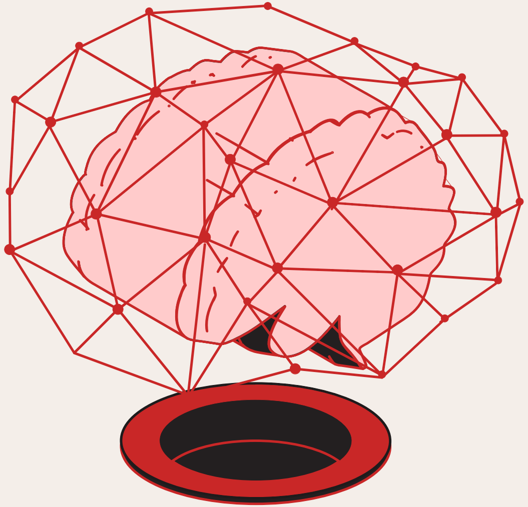
HTTP Response



protocol status code

```
HTTP/1.x 200 OK
Transfer-Encoding: chunked
Date: Sat, 28 Nov 2009 04:36:25 GMT
Server: LiteSpeed
Connection: close
X-Powered-By: W3 Total Cache/0.8
Pragma: public
Expires: Sat, 28 Nov 2009 05:36:25 GMT
Etag: "pub1259380237;gz"
Cache-Control: max-age=3600, public
Content-Type: text/html; charset=UTF-8
Last-Modified: Sat, 28 Nov 2009 03:50:37 GMT
X-Pingback: http://net.tutsplus.com/xmlrpc.php
Content-Encoding: gzip
Vary: Accept-Encoding, Cookie, User-Agent
```

HTTP headers as Name: Value



HTTP Response Status Codes

200 OK

- ○ The request succeeded. The result meaning of "success" depends on the HTTP method.

304 Not Modified

- ○ This is used for caching purposes. It tells the client that the response has not been modified, so the client can continue to use the same cached version of the response.

400 Bad Request

- ○ The server cannot or will not process the request due to something that is perceived to be a client error.

401 Unauthorized

- ○ Although the HTTP standard specifies "unauthorized", semantically this response means "unauthenticated".

404 Not Found

- ○ The server cannot find the requested resource. In the browser, this means the URL is not recognized. In an API, this can also mean that the endpoint is valid but the resource itself does not exist.

03

BurpSuite

Web Hacking Swiss-Army Knife

"I loved breaking into things. I loved being devious"

— Dafydd Stuttard

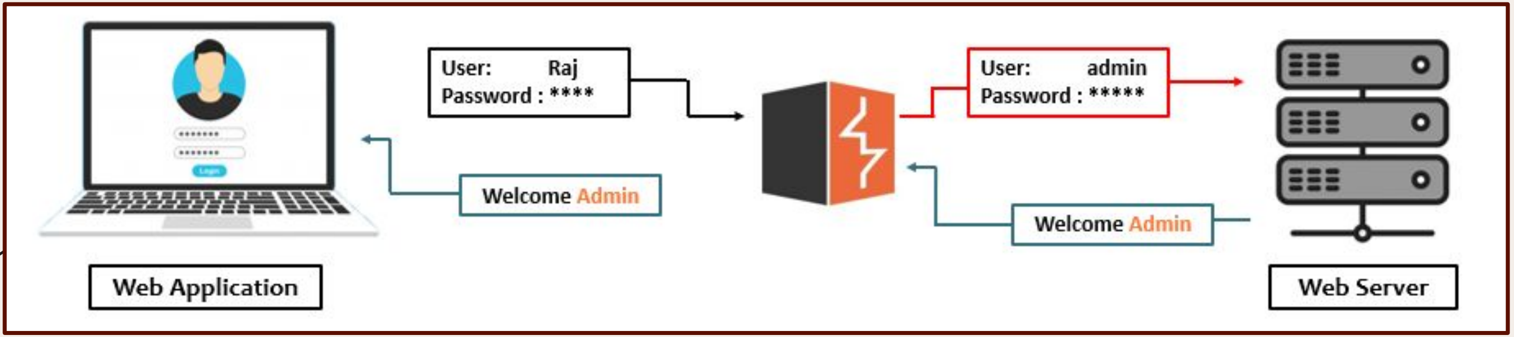
About BurpSuite

- Written in 2003 by Dafydd Stuttard.
- V1.0 had burping sound effects.
- The most widely used web security testing toolkit.

BURPSUITE

Burp Proxy

- Web proxy server between the web app and the web server.
- Allows interception, inspection, and modification of in-flight packets.



Burp Repeater

- Enables sending the same request to the server repeatedly.
- This is commonly used for finding input-based vulnerabilities
- Provides multiple tabs for to keep track of multiple requests at the same time.

04

Web Vulns

Finding cracks in the armor.

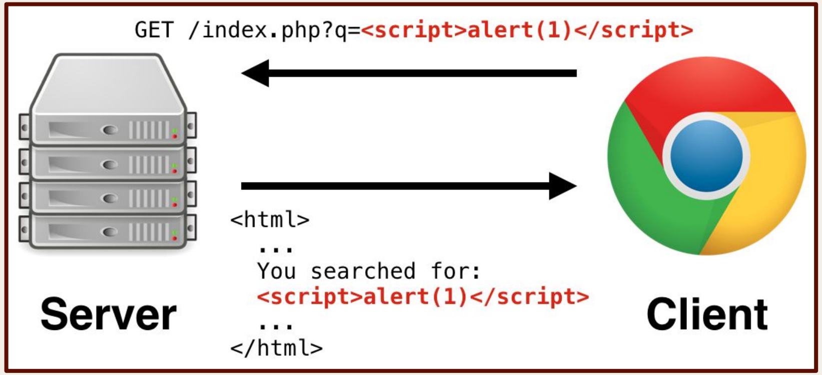
LFI - Local File Inclusion

- Injection vulnerability.
- When the application uses user-input as the path to a file.
- Leads to information disclosure.
- Can also lead to RCE and XSS.

Thank You!

XSS - Cross-Site Scripting

- Injection Vulnerability
- Attacker sends malicious client-side code to a different user.
- Usually accomplished using script tags.
- Works by modifying the HTML of the original page.



```
GET /index.php?q=<script>alert(1)</script>
```

```
<html>
  ...
  You searched for:
  <script>alert(1)</script>
  ...
</html>
```