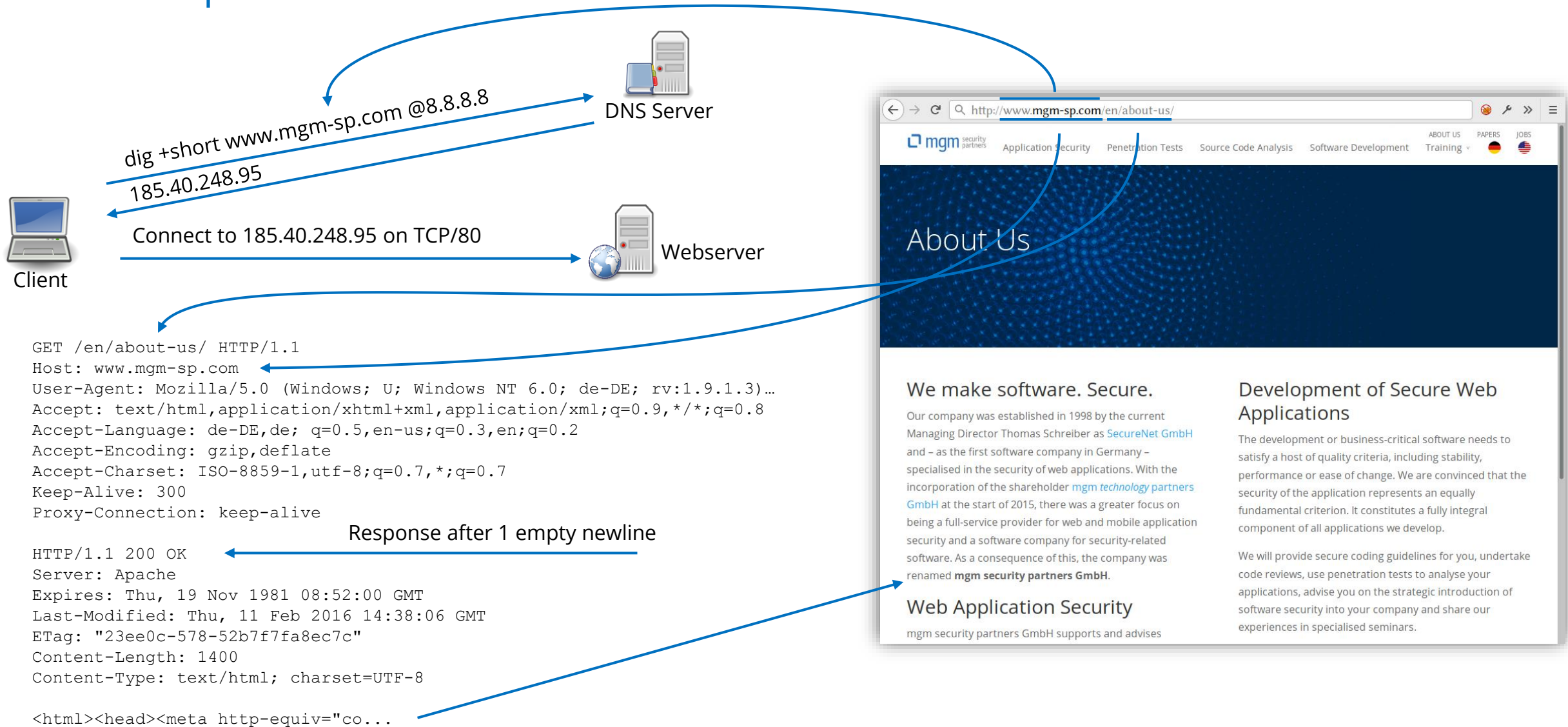


Basics & Tools

HTTP Request

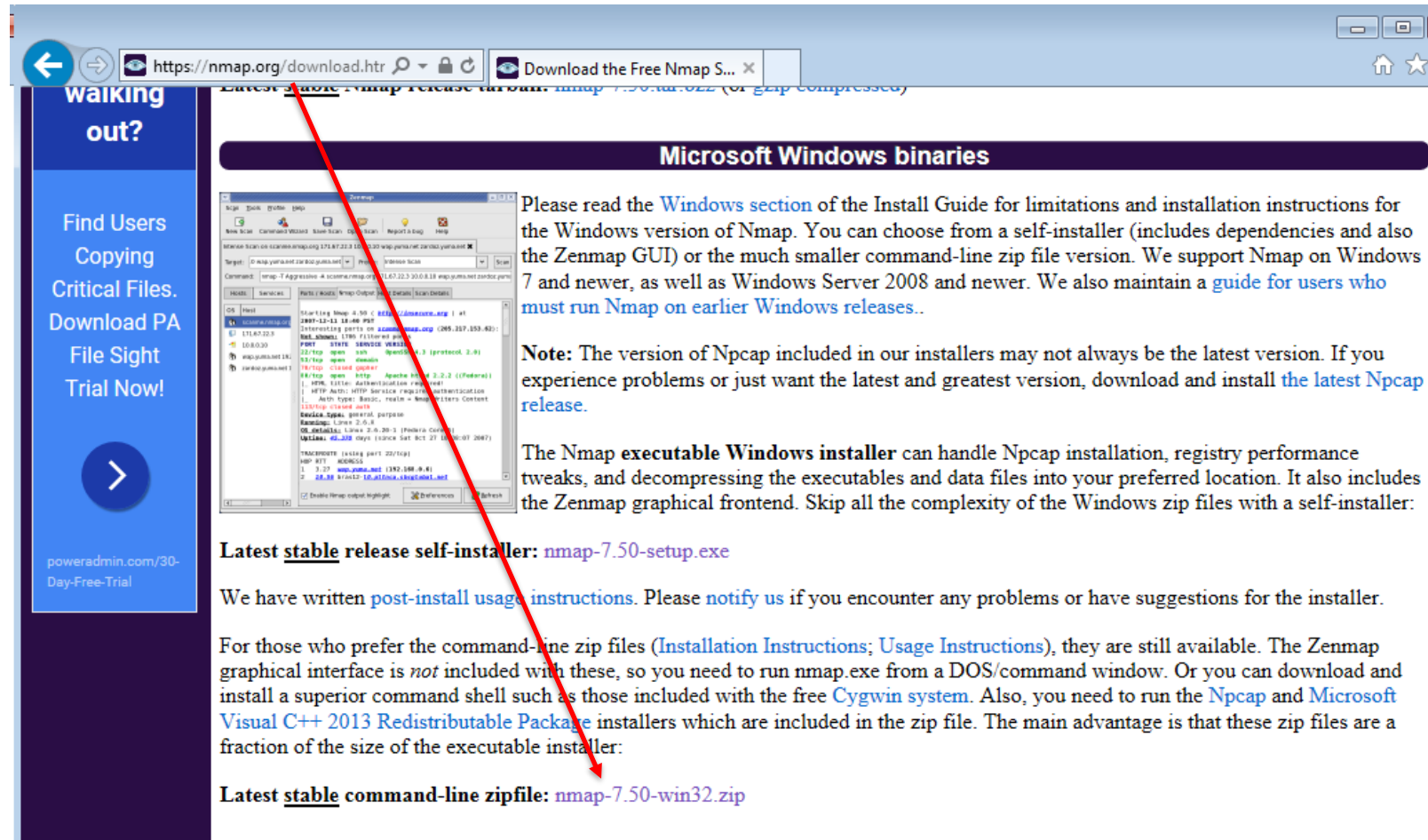


Exercise: Do you speak HTTP?

nmap / ncat

Download

- Download the nmap command-line zipfile:



The screenshot shows the Nmap website's download page. A red arrow points from the 'Latest stable release self-installer' link in the text to the 'nmap-7.50-win32.exe' link in the 'Microsoft Windows binaries' section. The page includes a sidebar with a 'Find Users Copying Critical Files. Download PA File Sight Trial Now!' button, a main content area with a 'Microsoft Windows binaries' header, and a footer with the MGM logo.

Microsoft Windows binaries

Please read the [Windows section](#) of the Install Guide for limitations and installation instructions for the Windows version of Nmap. You can choose from a self-installer (includes dependencies and also the Zenmap GUI) or the much smaller command-line zip file version. We support Nmap on Windows 7 and newer, as well as Windows Server 2008 and newer. We also maintain a [guide for users who must run Nmap on earlier Windows releases](#).

Note: The version of Npcap included in our installers may not always be the latest version. If you experience problems or just want the latest and greatest version, download and install [the latest Npcap release](#).

The Nmap **executable Windows installer** can handle Npcap installation, registry performance tweaks, and decompressing the executables and data files into your preferred location. It also includes the Zenmap graphical frontend. Skip all the complexity of the Windows zip files with a self-installer:

Latest stable release self-installer: [nmap-7.50-setup.exe](#)

We have written [post-install usage instructions](#). Please [notify us](#) if you encounter any problems or have suggestions for the installer.

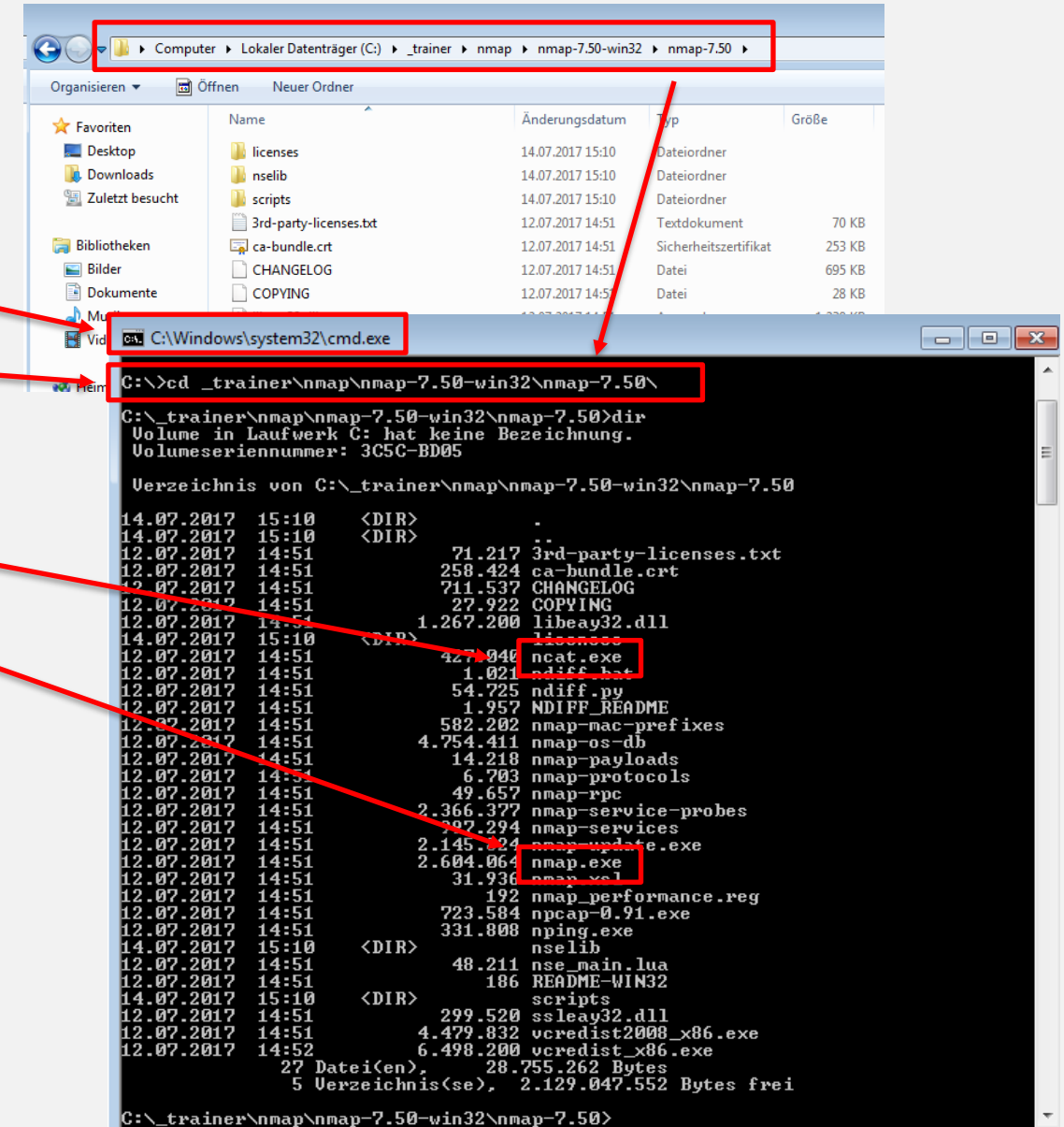
For those who prefer the command-line zip files ([Installation Instructions](#); [Usage Instructions](#)), they are still available. The Zenmap graphical interface is *not* included with these, so you need to run nmap.exe from a DOS/command window. Or you can download and install a superior command shell such as those included with the free [Cygwin system](#). Also, you need to run the [Npcap](#) and [Microsoft Visual C++ 2013 Redistributable Package](#) installers which are included in the zip file. The main advantage is that these zip files are a fraction of the size of the executable installer:

Latest stable command-line zipfile: [nmap-7.50-win32.zip](#)

nmap

Usage

1. Open a command shell (cmd)
2. navigate into the nmap directory
3. execute the binaries directly



Exercise: We are browser!

- Preparation
 - Open a terminal
- Exercise
 - Retrieve a website with the terminal (e.g. `http://www.mgm-sp.com/`)
 1. What is the ip address?
 - (possible tools: `host`, `nslookup`, `dig`)
 2. Open a TCP/80 connection to the ip address of `mgm-sp.com`
 - tools: `ncat`, `nc`, `telnet`
 3. Call the page / with the HTTP 1.1 protocol

```
GET / HTTP/1.1
Host: www.mgm-sp.com
<Return>
```

Solution: We are browser!

```
ben@liszt:~> host -t A mail.mgm-sp-lab.com
mail.mgm-sp-lab.com has address 172.23.42.22
ben@liszt:~> nc 172.23.42.22 80
GET / HTTP/1.1
Host: mail.mgm-sp-lab.com

HTTP/1.1 200 OK
Date: Mon, 12 Sep 2016 09:37:44 GMT
Server: Apache/2.2.22 (Debian)
Set-Cookie: _session_id=9fe1997791e4d84564e8c2f0a3c4af2d; path=/
Content-Length: 1047
Vary: Accept-Encoding
Content-Type: text/html; charset=utf-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN"
"http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en">
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
  <meta http-equiv="Content-Style-Type" content="text/css" />
  <title>Dvmail</title>
  <link rel="shortcut icon" href="/favicon.ico" type="image/vnd.microsof
t.icon">
  <link rel='stylesheet' type='text/css' href='dvmail.css' media='screen, proje
ction, tv, handheld' />
</head>
<body>
<div id='head'>Your friendly Webmailer</div>
```

Response Header

Response Body

Exercise: The browser is broken...

- Exercise:

- Vary the calls you made, e.g.:

GET /nonexistent HTTP/1.1	-- non existent resource
GET /xampp HTP/a.b	-- syntax error
ijde903qrnj09 oljfe90	-- whatever
GET / HTTP/1.0	-- protocol version 1.0
...	

Exercise: We are server!

- Open a TCP listener on port 8080
 - `ncat -lvp 8080`
- Verify that the listener is listening globally (0.0.0.0)
 - `netstat -tulpn`
- Connect to the netcat-server of another student and chat with them
 - `ncat 172.23.42.144 8080`
Hello? Anyone there?

Exercise: We are HTTP server!

- Open a TCP listener on port 8080
 - `ncat -klvp 8080`
- Use the browser to connect to your server
 - `http://localhost:8080/`
 - What does the browser send?
- Answer to the browser in correct HTTP
 - `HTTP/1.1 200 OK`
`Content-Type: text/plain`

`Hello browser!<Ctrl+d>`
 - Does the browser talk any more?

Solution: We are HTTP server!

```
ben@liszt:~> ncat -klvp 8080
Ncat: Version 7.01 ( https://nmap.org/ncat )
Ncat: Listening on :::8080
Ncat: Listening on 0.0.0.0:8080
Ncat: Connection from ::1.
Ncat: Connection from ::1:53357.
Ncat: Connection from ::1.
Ncat: Connection from ::1:53358.
GET / HTTP/1.1
Host: localhost:8080
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, sdch
Accept-Language: de,en-US;q=0.8,en;q=0.6

HTTP/1.1 200 OK
Content-Type: text/plain

Hallo Browser!
```



HTTP Methods

... and its intended meaning

Method	Intentional description	Req. has body?	Resp. has body?	Read only?	Idem-potent?	Cache-able?	Allowed in forms?
GET	Request some data (read).	no	yes	yes	yes	yes	yes
HEAD	GET without the body in response (only headers).	no	no	yes	yes	yes	no
POST	Sends data to the server (create).	yes	yes	no	no	may ¹	yes
PUT	Sends data to the server (update/replace).	yes	no	no	yes	no	no
DELETE	Deletes a resource (delete).	may	may	no	yes	no	no
CONNECT	Establishes a tunnel to a server.	no	yes	no	no	no	no
OPTIONS	Requests permitted communication options for a given URL or server.	no	yes	yes	yes	no	no
TRACE	Performs a message loop-back test to the target resource (debugging mechanism)	no	no	yes	yes	no	no
PATCH	Set of instructions on how to modify a resource (update/modify). (<i>PUT is rather complete resource</i>)	yes	yes	no	no	no	no

Wireshark

Tools - Wireshark

Sniffing the Network (1)

www.wireshark.org

The image displays the Wireshark network traffic analysis tool. The main window shows a capture of traffic on the 'Globetrotter 3G+ IRP WWAN ZCS Driver'. A filter is applied: `http.request and ip.addr == 10.161.84.82`. The packet list shows several HTTP GET requests to `/bank/login.aspx` from 10.161.84.82 to 65.61.137.117. The selected packet (No. 8009) is an HTTP POST request. The packet details pane shows the structure of the POST request, including headers like `Accept`, `User-Agent`, `Host`, `Cookie`, `Connection`, `x-forwarded-for`, and `Pragma`. The packet bytes pane shows the raw data in hexadecimal and ASCII.

Wireshark: Capture Interfaces

Description	IP	Packets	Packets/s	Stop
Globetrotter 3G+ IRP WWAN ZCS Driver	10.161.84.82	67	0	Start Options Details
Intel(R) 82567LM Gigabit Network Connection	10.30.18.5	0	0	Start Options Details
Microsoft	192.168.182.24	0	0	Start Options Details
Microsoft	0.0.0.0	0	0	Start Options Details
TAP-Win32 Adapter V9	172.16.18.9	0	0	Start Options Details
VMware Virtual Ethernet Adapter	192.168.0.1	0	0	Start Options Details
VMware Virtual Ethernet Adapter	192.168.109.1	0	0	Start Options Details

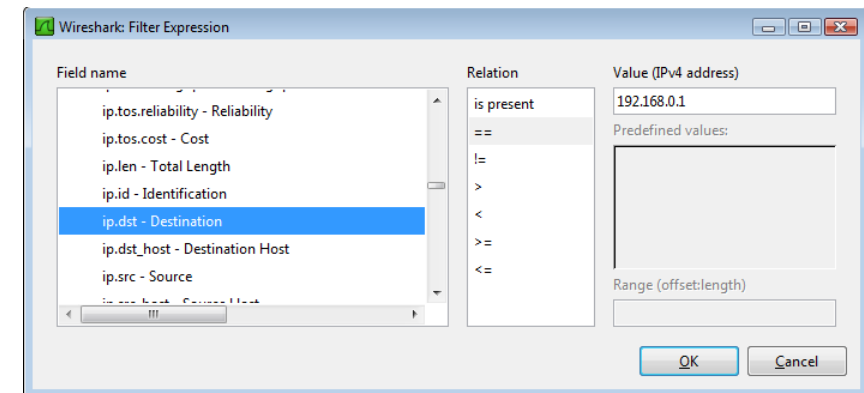
Tools - Wireshark

Sniffing the Network (2)

HTTP

http.notification - Notification (TRUE if HTTP notification)
http.response - Response (TRUE if HTTP response)
http.request - Request (TRUE if HTTP request)
http.authbasic - Credentials
http.request.method - Request Method (HTTP Request Method)
http.request.uri - Request URI (HTTP Request-URI)
http.request.version - Request Version (HTTP Request HTTP-Version)
http.response.code - Response Code (HTTP Response Code)
http.authorization - Authorization (HTTP Authorization header)
http.proxy_authenticate - Proxy-Authenticate (HTTP Proxy-Authenticate header)
http.proxy_authorization - Proxy-Authorization (HTTP Proxy-Authorization header)
http.proxy_connect_host - Proxy-Connect-Hostname (HTTP Proxy Connect Hostname)
http.proxy_connect_port - Proxy-Connect-Port (HTTP Proxy Connect Port)
http.www_authenticate - WWW-Authenticate (HTTP WWW-Authenticate header)
http.content_type - Content-Type (HTTP Content-Type header)
http.content_length - Content-Length (HTTP Content-Length header)
http.content_encoding - Content-Encoding (HTTP Content-Encoding header)
http.transfer_encoding - Transfer-Encoding (HTTP Transfer-Encoding header)
http.user_agent - User-Agent (HTTP User-Agent header)
http.host - Host (HTTP Host)
http.connection - Connection (HTTP Connection)
http.cookie - Cookie (HTTP Cookie)
http.cookie

http.accept - Accept (HTTP Accept)
http.referer - Referer (HTTP Referer)
http.accept_language - Accept-Language (HTTP Accept Language)
http.accept_encoding - Accept-Encoding (HTTP Accept Encoding)
http.date - Date (HTTP Date)
http.cache_control - Cache-Control (HTTP Cache Control)
http.server - Server (HTTP Server)
http.location - Location (HTTP Location)
http.set_cookie - Set-Cookie (HTTP Set Cookie)
http.last_modified - Last-Modified (HTTP Last Modified)
http.x_forwarded_for - X-Forwarded-For (HTTP X-Forwarded-For)



Tools - Wireshark

Sniffing the Network (3)

The screenshot shows the Wireshark network protocol analyzer interface. The title bar indicates the capture source is 'Globetrotter 3G+ IRP WWAN ZCS Driver: Capturing - Wireshark'. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, and Help. The toolbar contains various icons for file operations, capture control, and analysis. The filter bar shows 'Filter: tcp.stream eq 140' with buttons for 'Expression...', 'Clear', and 'Apply'. The packet list pane displays a table of captured packets. Packet 5887 is selected, and a context menu is open over it, with 'Follow TCP Stream' highlighted. The packet details pane shows the structure of packet 5887: Ethernet II, Internet Protocol, and Transmission Control Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Info
5665	531.374347	198.78.211.126	10.161.84.82	TCP	[TCP Keep-Alive] http > 64550 [ACK] Seq=108
5666	531.374382	10.161.84.82	198.78.211.126	TCP	[TCP Keep-Alive ACK] 64550 > http [ACK] Seq
5667	531.385194	198.78.211.126	10.161.84.82	HTTP	HTTP/1.1 200 OK (GIF89a)
5701	531.583256	10.161.84.82	198.78.211.126	TCP	64550 > http [ACK] Seq=1849 Ack=12033 win=1
5887	533.502694	10.161.84.82	198.78.211.126	HTTP	GET /search-css/sear
5909	533.643322	198.78.211.126	10.161.84.82	TCP	htt
5910	533.644320	198.78.211.126	10.161.84.82	TCP	[TC
5911	533.644347	10.161.84.82	198.78.211.126	TCP	[TC
5913	533.675355	198.78.211.126	10.161.84.82	TCP	[TC
5914	533.695329	198.78.211.126	10.161.84.82	TCP	[TC
5915	533.695391	10.161.84.82	198.78.211.126	TCP	645
5920	533.866345	198.78.211.126	10.161.84.82	TCP	[TC
5921	533.886339	198.78.211.126	10.161.84.82	TCP	[TC
5922	533.886397	10.161.84.82	198.78.211.126	TCP	645
5923	533.905339	198.78.211.126	10.161.84.82	TCP	[TC
5928	534.036357	198.78.211.126	10.161.84.82	TCP	[TC

Frame 5887 (505 bytes on wire, 505 bytes captured)
Ethernet II, Src: 00:f1:d0:00:f1:d0 (00:f1:d0:00:f1:d0), Dst: 00:
Internet Protocol, Src: 10.161.84.82 (10.161.84.82), Dst: 198.78.
Transmission Control Protocol, Src Port: 64550 (64550), Dst Port:
Source port: 64550 (64550)
Destination port: http (80)
tcp.stream index: 140

0000 00 ca fe c0 ff ee 00 f1 d0 00 f1 d0 08 00 45 00
0010 01 eb 69 b0 40 00 80 06 96 9c 0a a1 54 52 c6 4e ..i.@... ..TR.N
0020 d3 7e fc 26 00 50 16 1b a4 ec 3d 30 88 83 50 18 ..&.P.. ..0..P.
0030 0f 09 49 8a 00 00 47 45 54 20 2f 69 6d 61 67 65 ..I...GE T /image
0040 73 2f 47 2f 30 31 2f 6e 61 76 32 2f 67 61 6d 6d s/G/01/n av2/gamm
0050 61 2f 72 65 61 72 62 68 2d 62 72 72 2f 72 65 61 2/62arch css/602

Globetrotter 3G+ IRP WWAN ZCS Driver: <li... Packets: 11274 Displayed: 51 Marked: 0

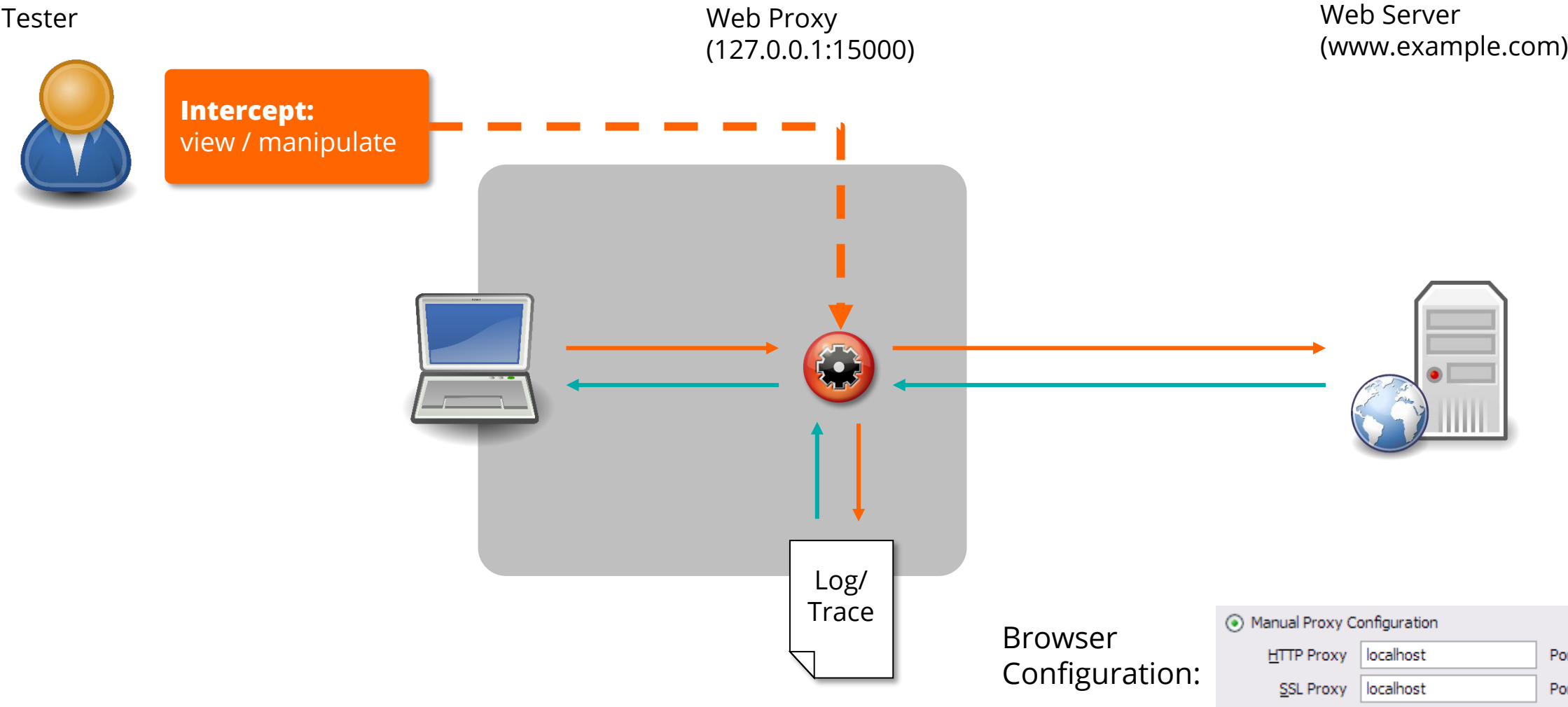
HTTP Proxy

The swiss knife of Web Application Security



Tools

Using a Web Proxy



Tools

Using a Web Proxy

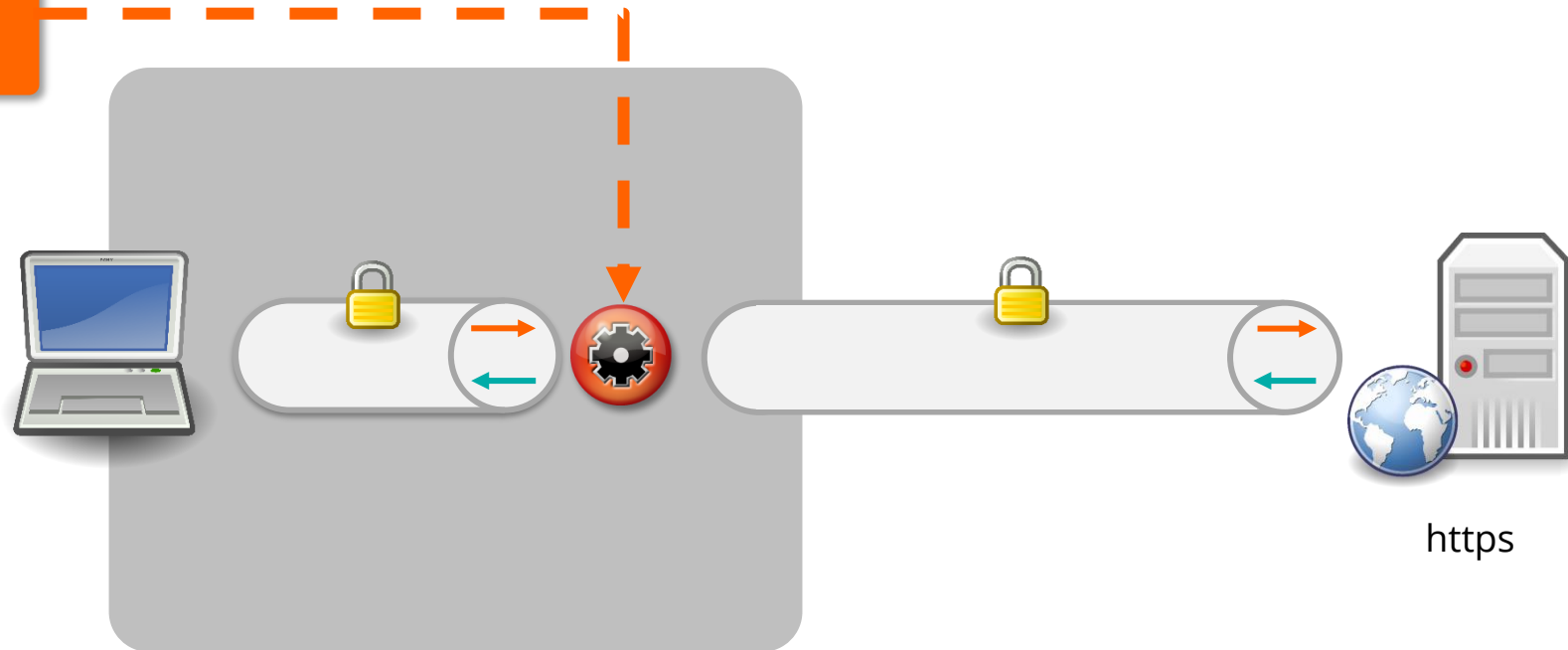
Tester



Intercept:

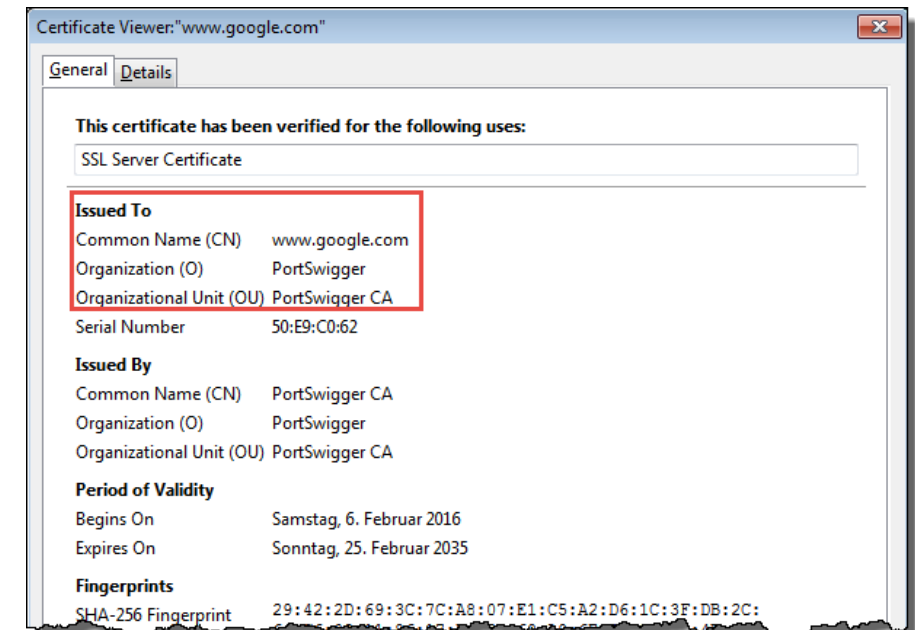
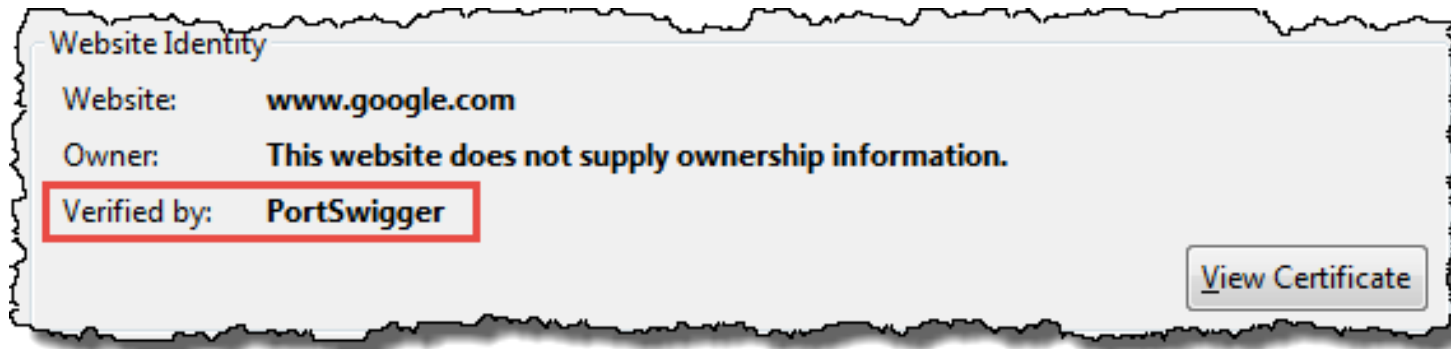
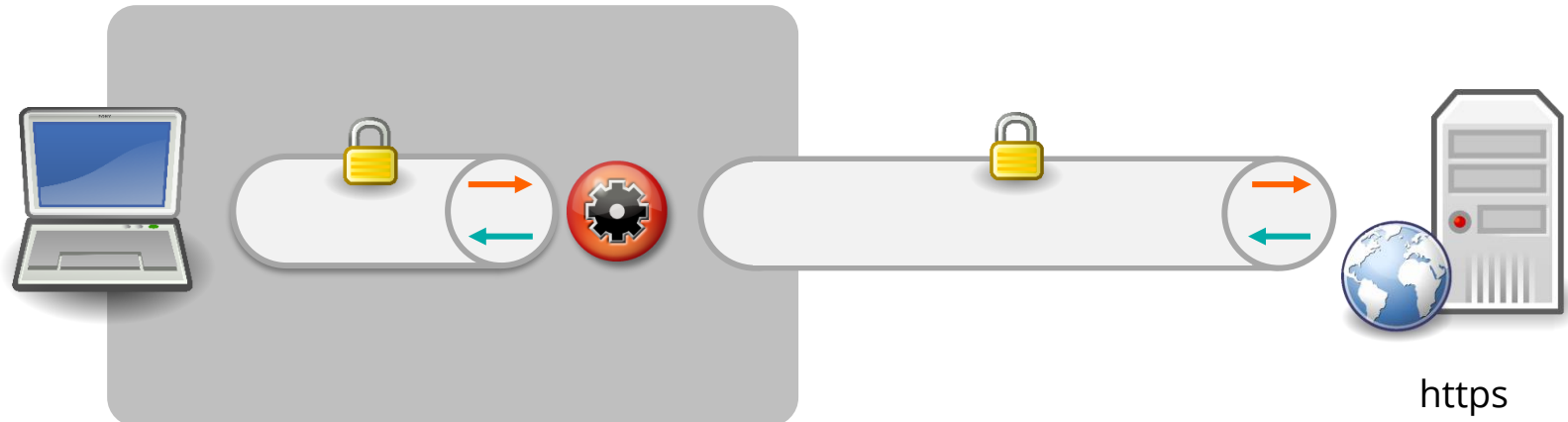
Web Proxy
(127.0.0.1:15000)

Web Server
(www.example.com)



Tools

Using a Web Proxy



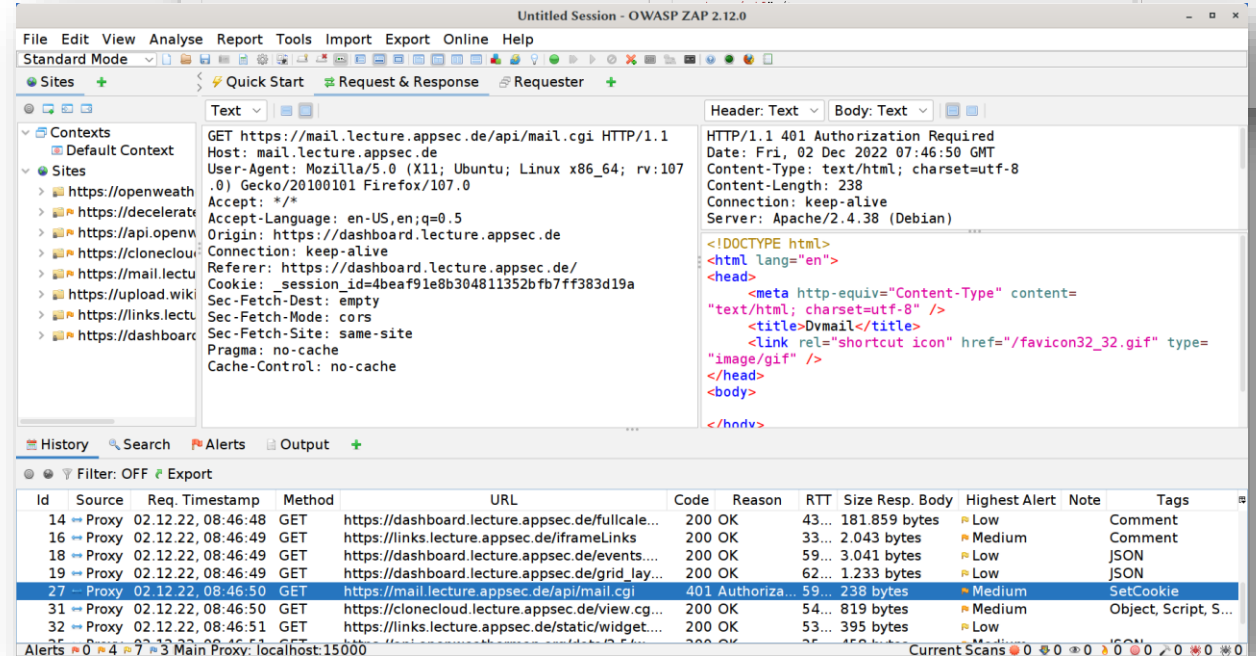
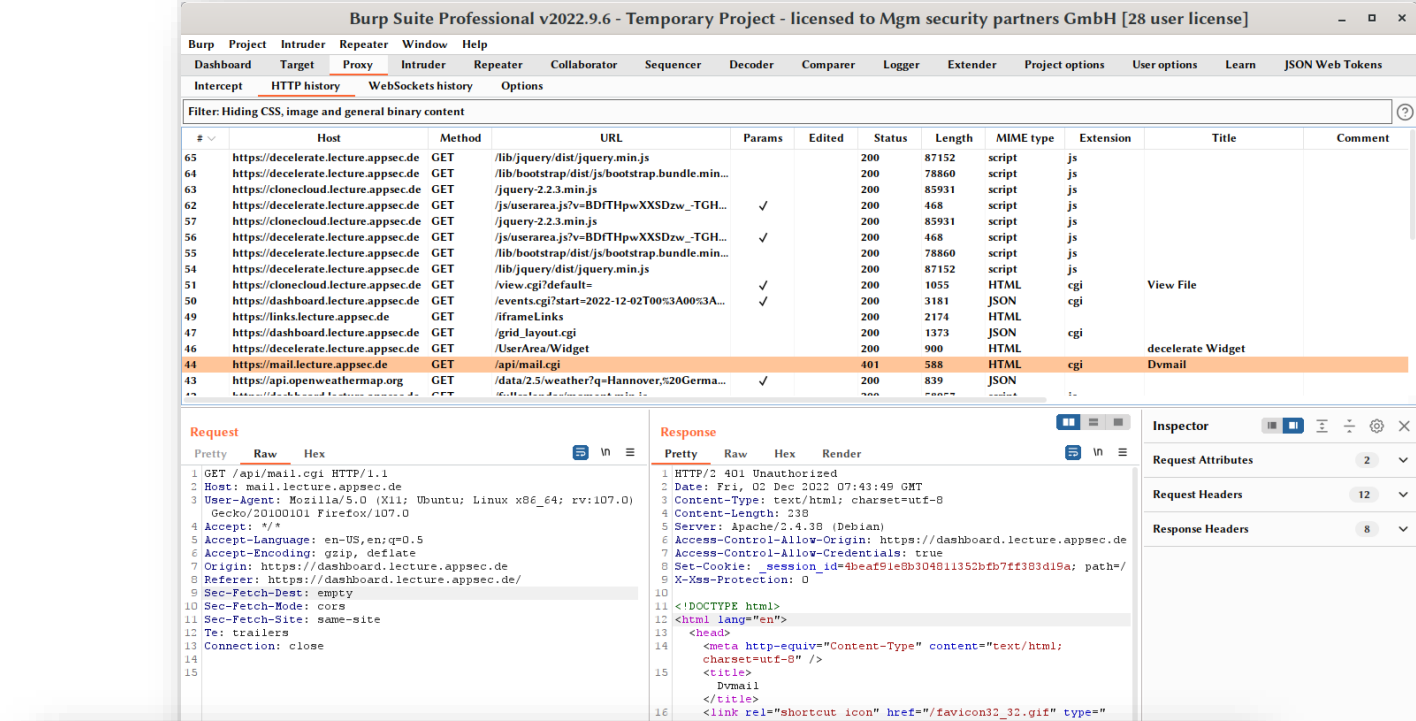
HTTP-Proxy Tools

Commercial Penetration-test-centric

- Portswigger BurpSuite
 - <https://portswigger.net>

OpenSource developer-centric

- OWASP ZAP Proxy
 - <https://www.zaproxy.org>



Firefox (Exercise)

Useful Firefox Add-ons



FoxyProxy Standard

Proxy switching made simple!



HackBar

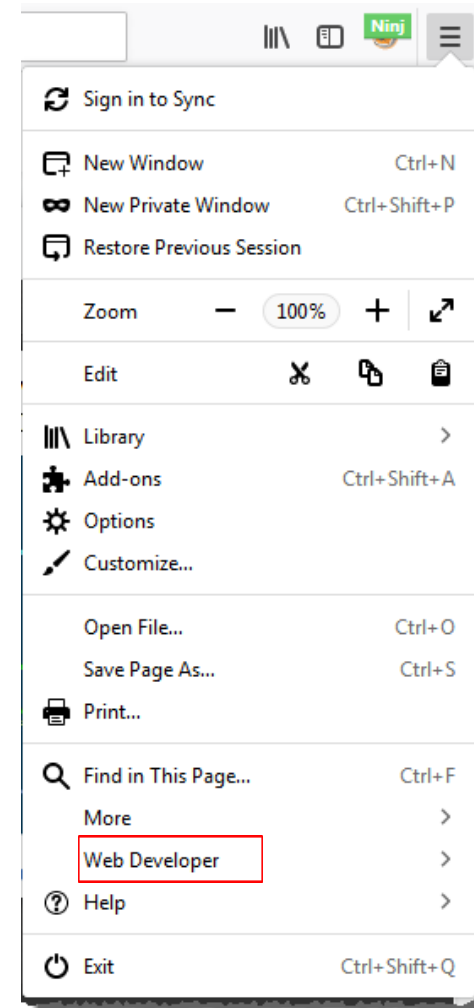
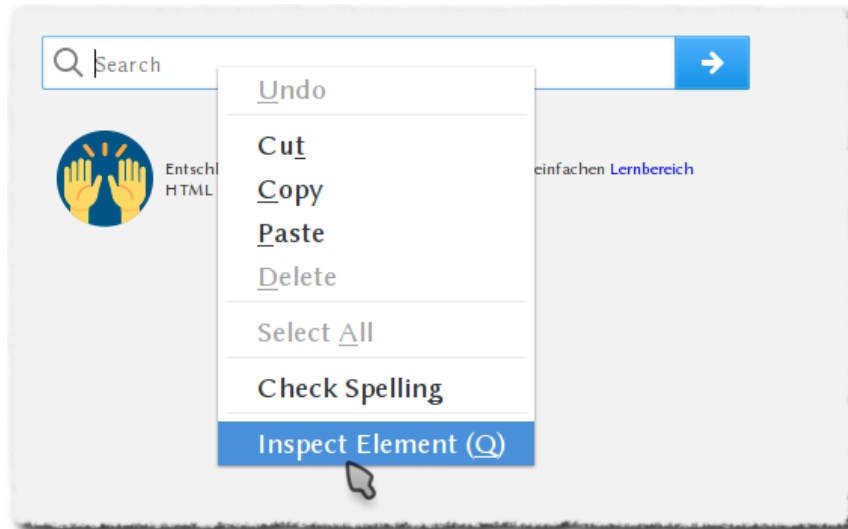
A HackBar for new firefox (Firefox Quantum).



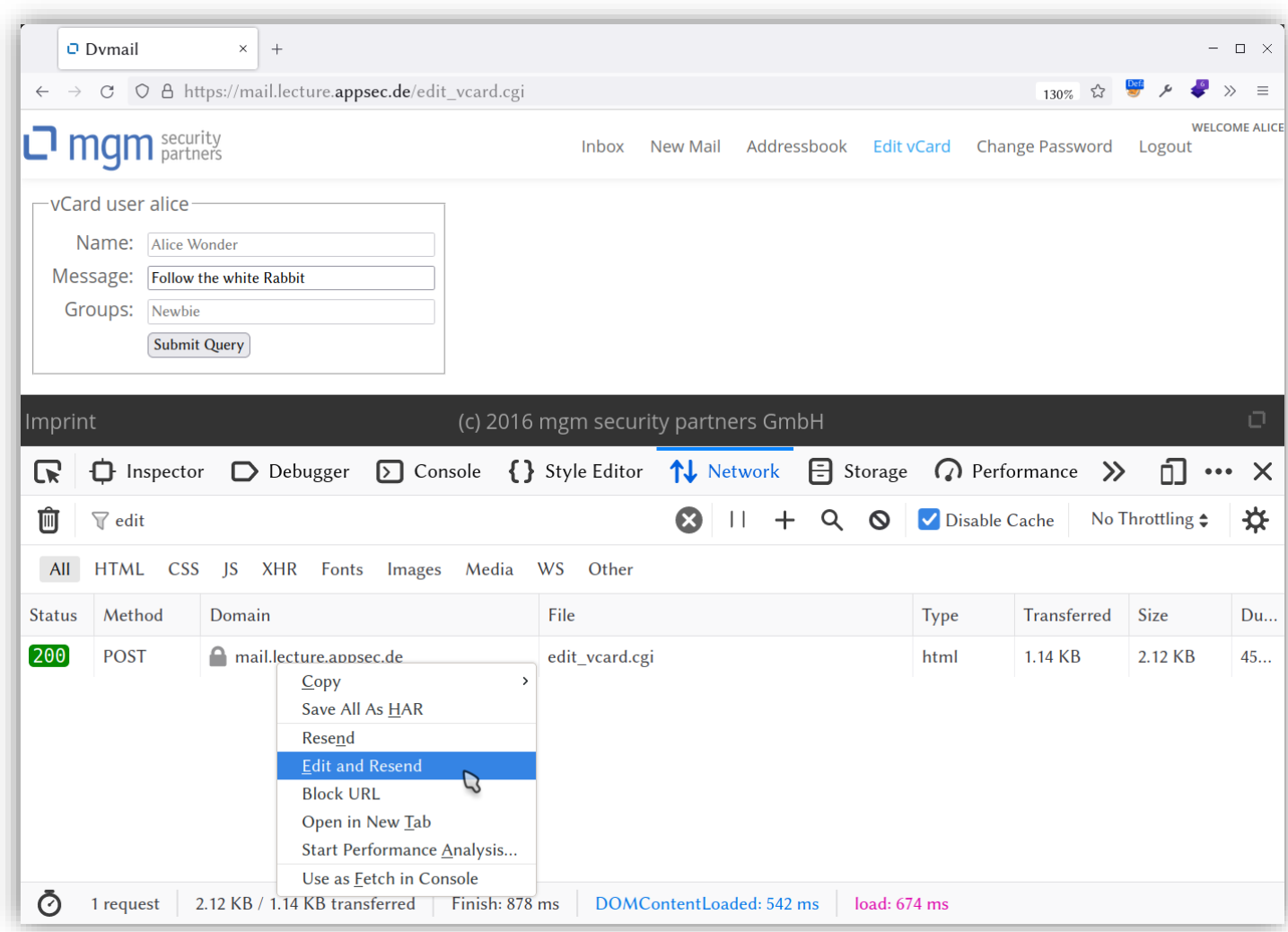
**disable
NOSCRIPT!**

Firefox build-in: Web developer tools

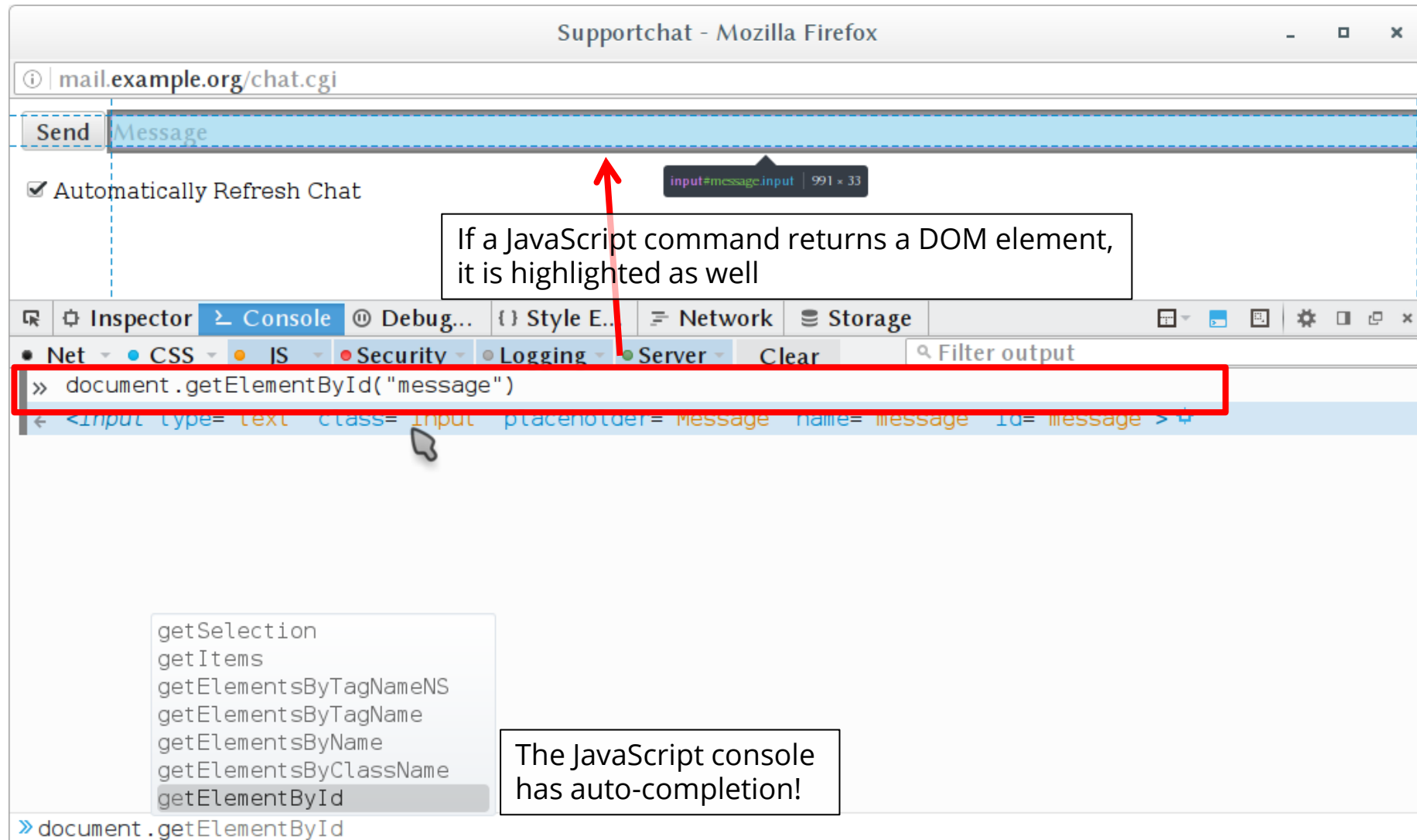
- Open with F12 or via the menu:
- alternative:
show an element directly in the inspector



Firefox build-in: Edit and Resend

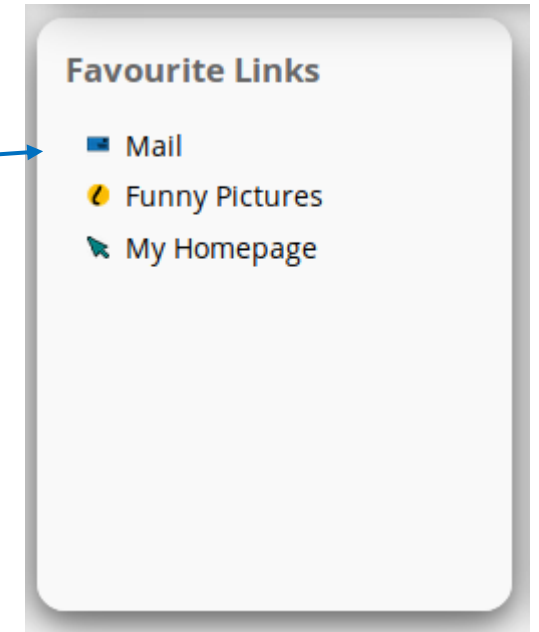


JavaScript console



Exercise: JavaScript console

- Preparation
 - Start Firefox
 - Open the developer tools
 - Open the „console tab“
- Exercise
 1. Navigate to the Mail app (linked from the Dashboard)
 2. Open the Chat (link in the upper right when not logged in)
 3. Write a message into the message field using JavaScript
 4. Submit the form using JavaScript
- The following functions could be of use for this exercise:
 - `document.getElementById()`
 - `<dom-input-element>.value = "foo"`
 - `<dom-form-element>.submit()`




Exercise: Parameter Tampering

- Exercise

1. Browse to the mail app
2. Register an account and log in
3. Change your name

Favourite Links

- ✉ Mail
- 📺 Funny Pictures
- 🖱 My Homepage



vCard user alice

Name:

Message:

Groups:

The name can not be changed!

Parameter Tampering → your everyday advice

Parameter Tampering

→ Privilege Escalation

The screenshot shows a web browser window displaying the 'Edit Profile' page of a user named Benjamin Kellermann. The page is titled 'Edit Profile | Name and Address' and contains a form with fields for Contact Information. The 'Prefix' dropdown menu is open, showing options: '>', 'Capt.', 'Col.', 'Dr.', 'FR.', 'Gen.', 'H.', 'Lt.', 'Lt Col.', 'Mr.' (selected), 'Ms.', and 'Rev.'. The browser's developer tools are open, showing the HTML structure of the page. The selected option 'Mr.' is highlighted in the dropdown menu. The HTML structure shows a table with a row for the Prefix field, which is a dropdown menu with the selected option 'Mr.'.

```
<tr>
  <td class="isg_formLabel" style="width:30%;">></td>
  <td class="isg_formData" colspan="1" style="width:70%;">
    <span id="ddlPrefix" disabled="disabled">
      <select id="ddlddlPrefix" class="isg_input" name="ddlddlPrefix" disabled="disabled">
        <option value=" "></option>
        <option value="Capt">Capt.</option>
        <option value="Col">Col.</option>
        <option value="Dr">Dr.</option>
        <option value="FR.">Father</option>
        <option value="Gen">Gen.</option>
        <option value="H">Hon.</option>
        <option value="Lt">Lt.</option>
        <option value="Lt Col">Lt. Col.</option>
        <option value="Mr" selected="selected">Mr.</option>
        <option value="Ms">Ms.</option>
        <option value="Rev">Rev.</option>
      </select>
    </span>
  </td>
</tr>
```

GET vs. POST

GET versus POST

Means to limit attack surface:
accept forms only by POST

The screenshot shows a web browser at `https://funny-pics.lab.appsec.de`. The page has a header with "seminarhaha" and "yet another funny imgur". Below the header is a form with a text input containing `https://media.makeameme.org/created/brace-yourself-csrf.jpg` and an "Add" button. The Network tab is open, showing a list of requests. The first request is a POST to `funny-pics.lab.appsec.de /` with a status of 200. The request payload is `pic_url=https%3A%2F%2Fmedia.makeameme.org%2Fcreated%2Fbrace-yourself-csrf.jpg`.

Status	Method	Domain	File	Type	Transfe...	Size	Du
200	POST	funny-pics.lab.appsec...	/	html	803 B	2.27 KB	6...
200	GET	funny-pics.lab.appsec...	funny_pics.css	css	1.06 KB	1.99 KB	3...
200	GET	media.makeameme....	brace-yourself-csrf.jpg	jpeg	149.67 ...	149.63 KB	2...

6 requests | 1.21 MB / 1.20 MB transferred | Finish: 1.10 s | DOMContentLoaded: 619 ms | load: 1.03 s

Filter Request Parameters

Form data

`pic_url: "https://media.makeameme.org/created/brace-yourself-csrf.jpg"`

Request payload

1 `pic_url=https%3A%2F%2Fmedia.makeameme.org%2Fcreated%2Fbrace-yourself-csrf.jpg`

POST / HTTP/1.1

Host: funny-pics.lecture.appsec.de

Content-Type: application/x-www-form-urlencoded

Content-Length: 77

`pic_url=https%3A%2F%2Fmedia.makeameme.org%2Fcreated%2Fbrace-yourself-csrf.jpg`

POST request may be transformed by a client
to a GET request with same variable-names

1. add separator

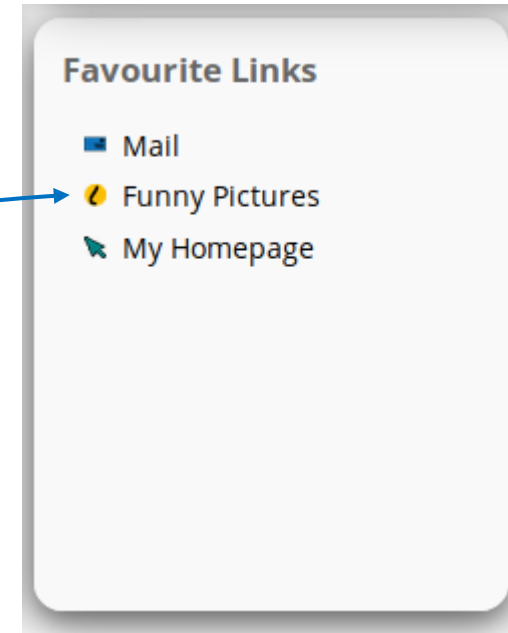
2. copy variables

`https://funny-pics.lecture.appsec.de/?pic_url=https%3A%2F%2Fmedia.makeameme.org%2Fcreated%2Fbrace-yourself-csrf.jpg`

Exercise

Exercise: GET vs. POST

- Preparation
 - Start Firefox
 - Open the Web developer tools
 - Open the network tab
- Exercise
 - Browse to the Funny Pictures Webapplication
 - Submit a url to a picture in the form and follow the submission in the network tab
 - What is the request method (GET, POST, ...)?
 - How many parameters are used?
 - What are the names and values?



- Submit the request once again
 - Change the parameters (lets play a bit...)!



Exercise: GET vs. POST

- What happens if you change the POST to a GET?
- Can you insert an image-inserting-image?