Owning Your Home Network: Router Security Revisited

Marcus Niemietz, Jörg Schwenk

{marcus.niemietz, joerg.schwenk} @rub.de

Ruhr University Bochum

hgi Horst Görtz Institute for IT-Security

RUB

Table of Contents

Introduction

- Routers: center of private home networks
- Web stores like Amazon offer them for <$20
  - No keys and no displays
  - Web interface
- Our paper:
  Web-based attacks against these interfaces
  - Change critical settings

Introduction

- Methodology
  - 10 most popular routers from Amazon
    - TP-Link, Netgear, Buffalo, ...
  - Default configuration evaluated
  - UI redressing, Cross-Site Scripting, SSL/TLS
  - Fingerprinting possibilities analyzed
  - Countermeasures analyzed

Web Attacker

- Sets up a website → lures the victim to this site
- Arbitrary JavaScript code may be executed
- May send requests and may use scripts

Generalization

- Conditions
  - Web interface
  - Connected pointing device (e.g., mouse)
- Routers, network switches, smart TV systems, and network attached storage devices
- Router: Widely used, complex, important functionalities

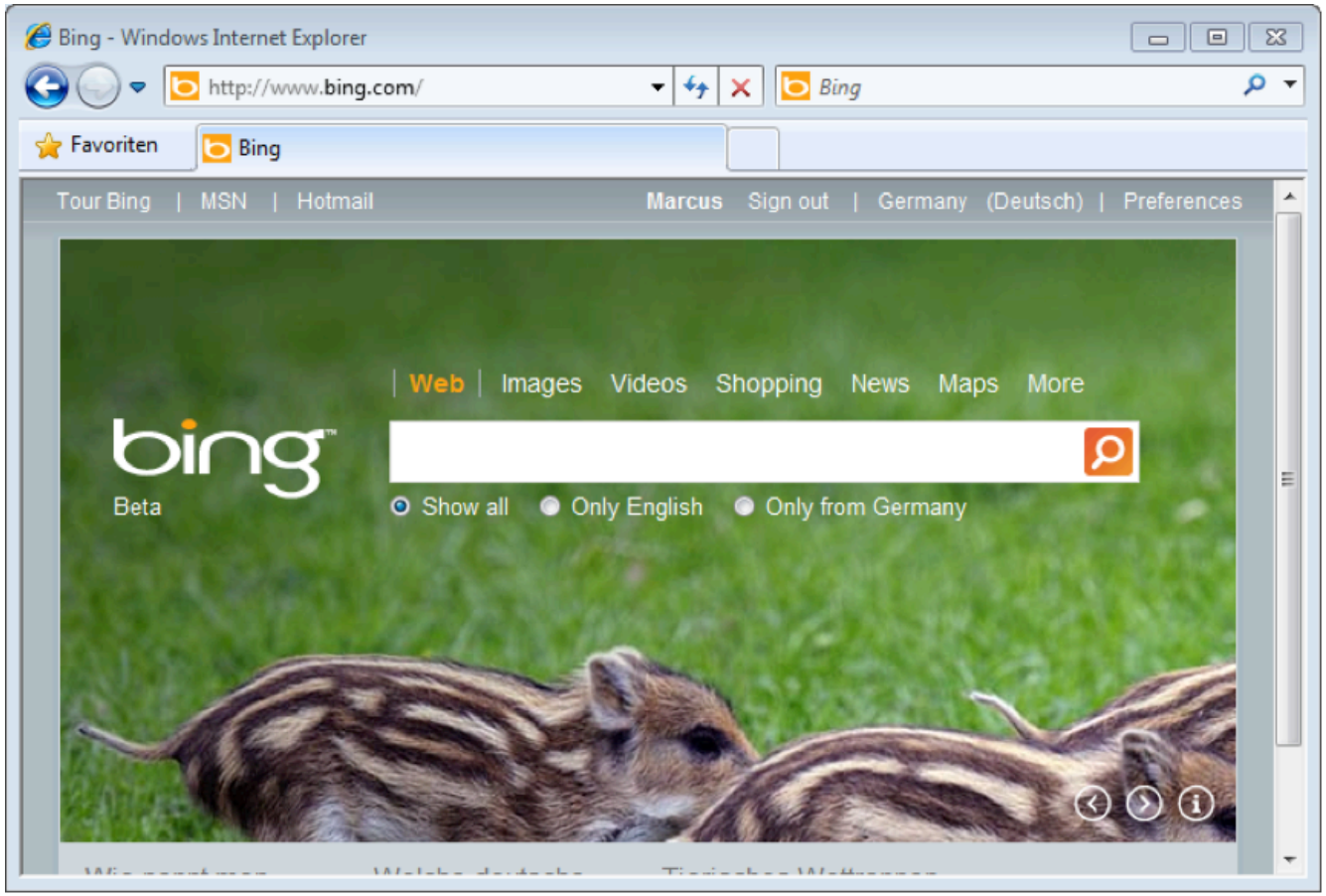
Default Configuration

Router	Method	Username	Password	URL
TP-Link WR841N	BA	admin	admin	http://192.168.0.1
Netgear N150	BA	admin	password	http://192.168.1.1
Huawei E5331	Web	admin	admin	http://192.168.1.1
D-Link DIR-615	Web	admin	(empty)	http://192.168.0.1
Linksys WRT54GL	BA	(empty)	admin	http://192.168.1.1
LogiLink WL0083	BA	admin	admin	http://192.168.2.1
Belkin F7D4301	Web	–	(empty)	http://192.168.2.1
Buffalo WCR-GN	BA	root	(empty)	http://192.168.11.1
Fritz!Box 2170	Web	–	–	http://192.168.178.1
Asus RT-N12	BA	admin	admin	http://192.168.1.1

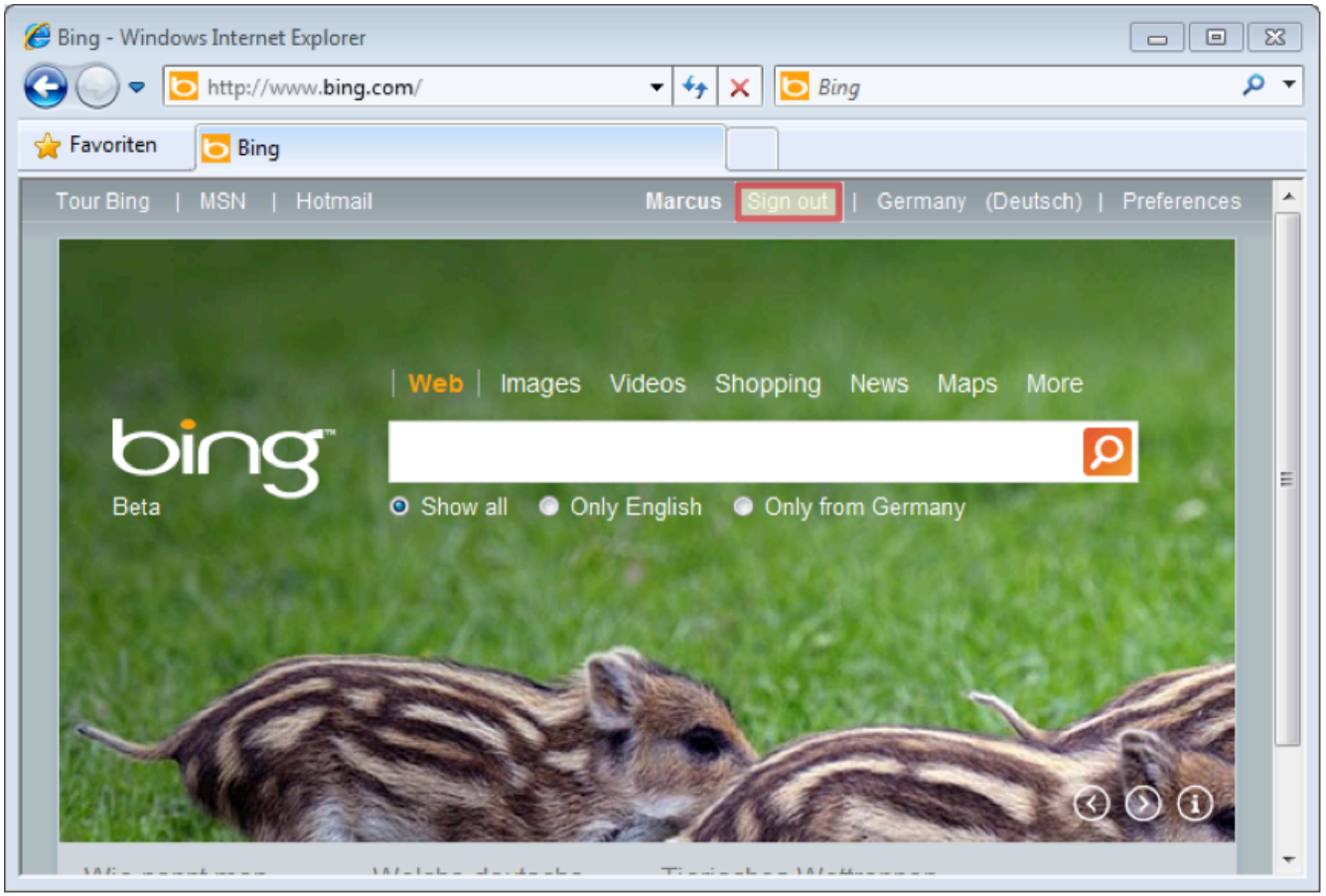
XSS, CSRF, UIR, and SSL/TLS

- XSS: Focus on reflected and stored XSS
  - Control the victim‘s browser
- CSRF
  - Manipulate DNS settings
  - Change default passwords (D-Link DIR-615)
- UIR: Classic Clickjacking & Tabjacking
- SSL/TLS

UI Redressing



UI Redressing

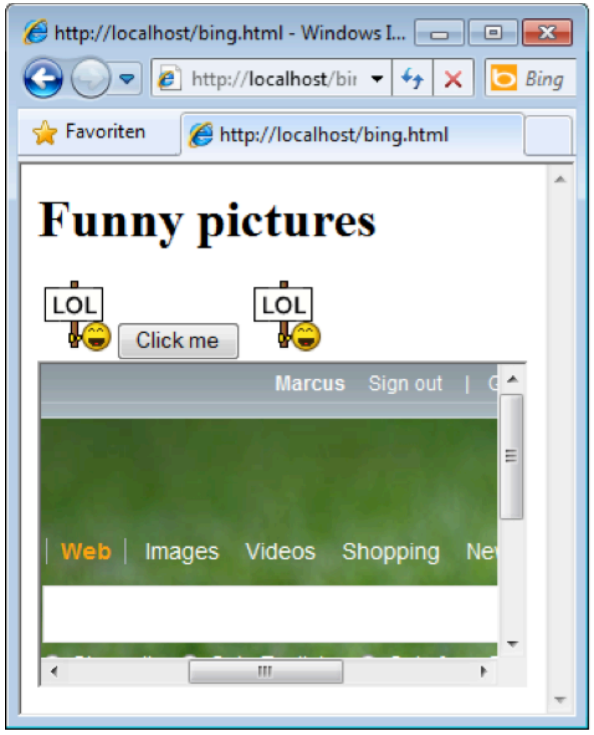


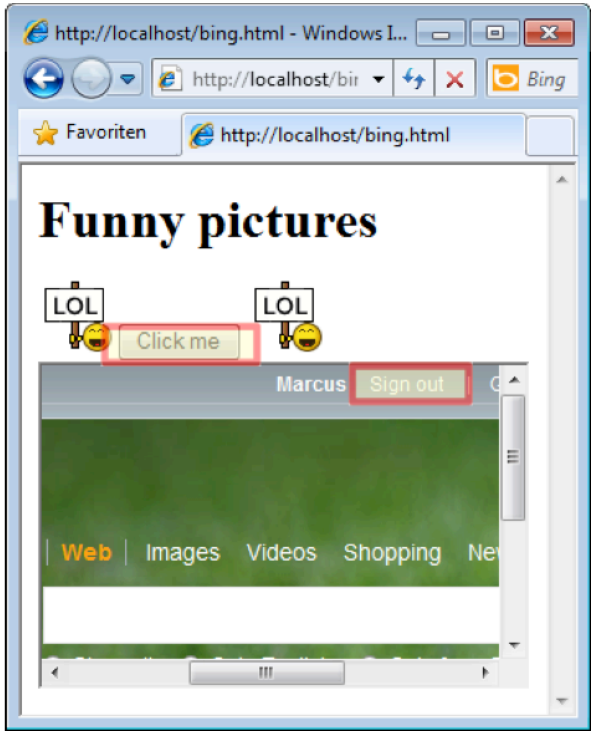
UI Redressing

hgi
Horst Görtz Institute
for IT-Security

RUB

UI Redressing

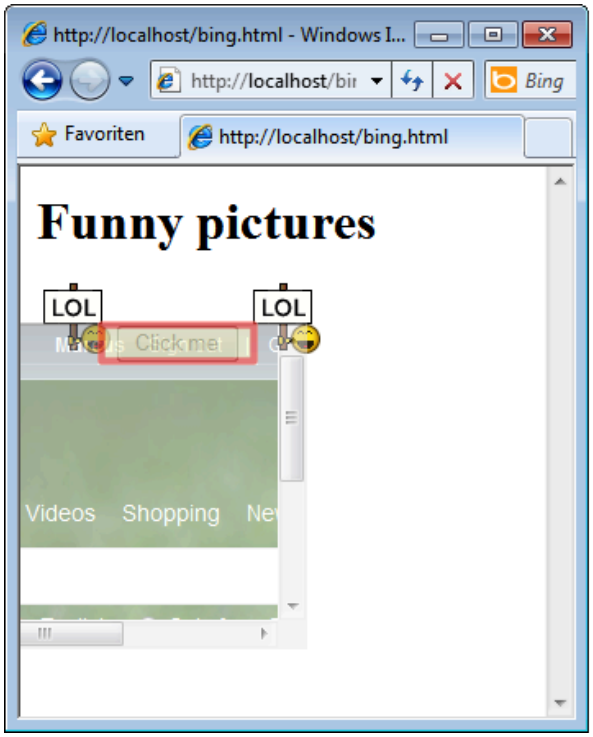


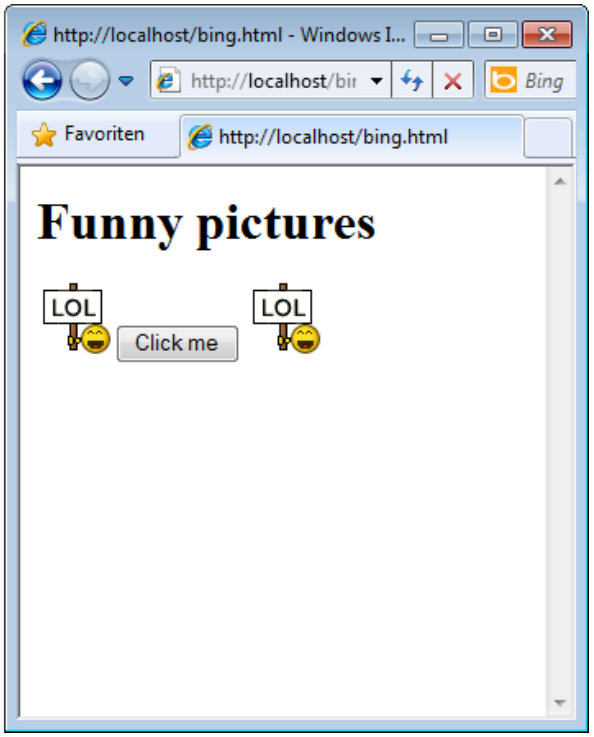


hgi
Horst Görtz Institute
for IT-Security

RUB

UI Redressing





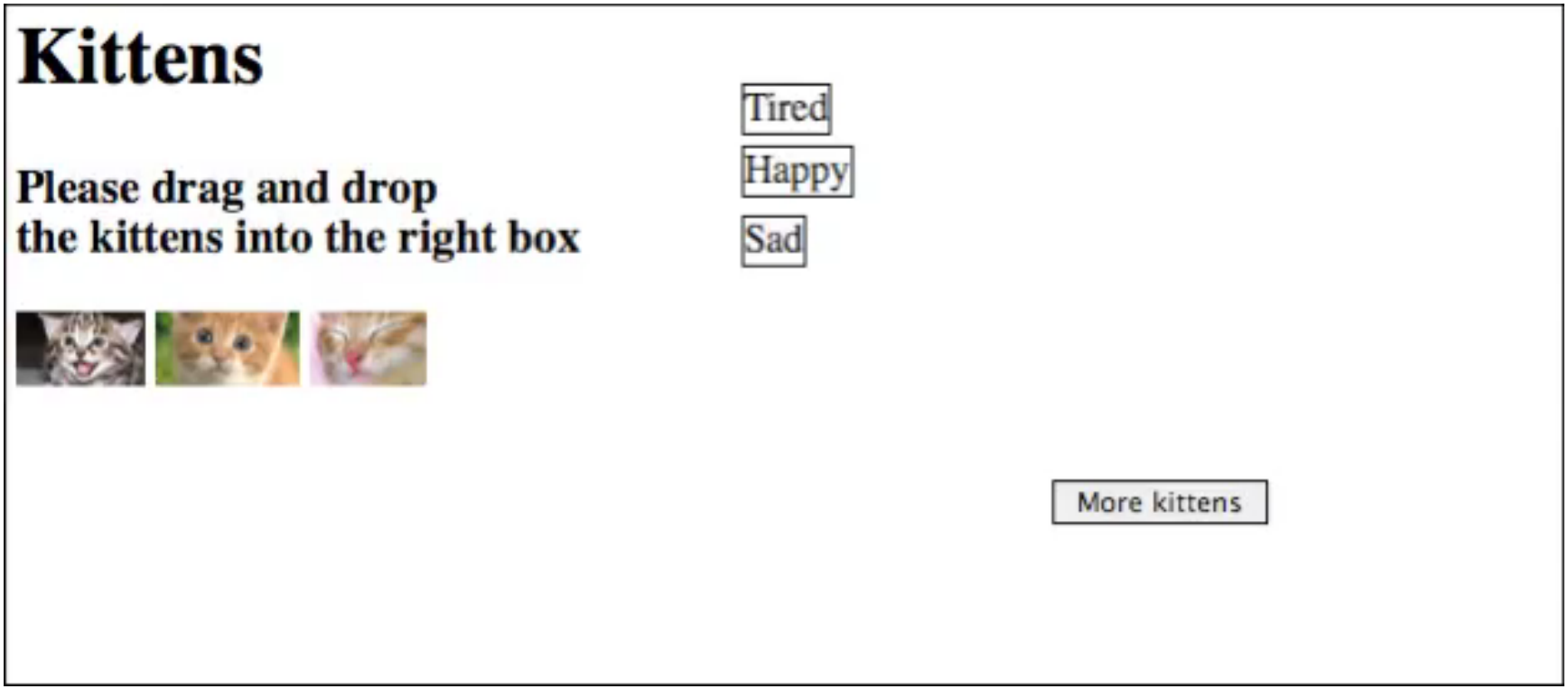
UI Redressing

```
<h1>Funny pictures</h1>
<img src="lol.gif">
<button>Click me</button>
<img src="lol.gif">
<iframe style="position:absolute; z-index:1;
   opacity:0.0; filter:alpha(opacity=0);
   left:-120px; top:95px;"
   width="300" height="200"
   src="http://www.bing.com">
</iframe>
```

Web Attacks

Router	Version	UIR	XSS	TLS
TP-Link WR841N	3.13.27	✓	S	–
Netgear N150	1.0.2.54	✓	S	–
Huawei E5331	21.344.11	✓	–	(✓)
D-Link DIR-615	8.03	✓	S	–
Linksys WRT54GL	4.30.16	✓	S	(✓)
LogiLink WL0083	3.33.13	✓	R	–
Belkin F7D4301	1.00.25	✓	S	–
Buffalo WCR-GN	1.04	✓	R	–
Fritz!Box 2170	51.04.57	✓	–	–
Asus RT-N12	3.0.0.4.260	✓	R	–

UIR – Fritz!Box 2170



UIR – Fritz!Box 2170

```
<style>div, button { position:absolute; z-
index:1; border:1px solid; pointer-
events:none }</style>...
<img src="kitten-1.png" draggable="true"
ondragstart="event.dataTransfer.setData('tex
t/plain','foobar')">...
<div style="top:35px; left:300px">Tired</
div>...
<button style="top:195px; left:425px">More
kittens</button>
<iframe src="http://192.168.178.1/cgi-bin/
webcm?getpage=...
```

hgi Horst Görtz Institute for IT-Security

RUB

Fingerprinting

- Get unique identifiers
  - HTTP Basic Authentication
    - WWW-Authenticate: Basic realm="VALUE"
  - Web Interface Authentication
    - HTTP ressources

Fingerprinting

Router	VALUE
TP-Link WR841N	TP-LINK Wireless N Router WR841N
Netgear N150	NETGEAR WNR1000v3
Linksys WRT54GL	WRT54GL
LogiLink WL0083	Portable Wireless AP/Router
Buffalo WCR-GN	AirStation: Enter ”root” for user name.
Asus RT-N12	RT-N12

Fingerprinting

- Huawei E5331
  - SIM, http://192.168.1.1/res/no card.png
- D-Link DIR-615
  - Logo, http://192.168.0.1/pictures/wlan/masthead.gif
- Fritz!Box 2170
  - Logo, http://192.168.178.1/html/de/images/fw header.gif
- Belkin F7D4301
  - Logo, http://192.168.2.1/images/head logo.gif

Countermeasures

- Randomization of the default login data

hgi Horst Görtz Institute for IT-Security

RUB

Countermeasures

- Minimize Information Leakage
  - "TP-Link WR841N" ➔ "Router Login XXX"
- SSL/TLS
- Input Validation
- X-Frame-Options
- Window name
  - `window.name="TOKEN"`
- Cookie flags: *httpOnly* and *secure*

Conclusions

- Representative overview of the security of current home router Web interfaces
- All 10 Web interfaces are vulnerable
- Well-known countermeasures like `X-Frame-Options` are not implemented

Thank you for your attention.
Questions?