

Ø=Þá VIYUH BDR — Category 2 Test Links

Web-Based Attacks · click each link to verify a detection. Email this PDF to yourself and click from Gmail to test the real delivery path.

Setup: extension v0.9.4+ reloaded · backend :4004 up · fixtures :4005 up. Most detections are a WARN interstitial or an in-page BANNER (precision-first).

Suspicious redirects (incl. chains)

[%¶ Realtime 302 !' paypal look-alike](#)

<http://localhost:4004/api/web-attacks/redir?url=http://paypa1.com/login>

Expect: WARN — suspicious redirect to a look-alike of paypal

[%¶ Realtime 4-hop chain !' microsof](#)

<http://localhost:4004/api/web-attacks/redir?url=http://microsof.com/verify&hops=3>

Expect: WARN — multi-hop redirect chain

[%¶ Open-redirect param !' paypa1](#)

<http://localhost:4005/web-attacks/redirects/go.html?forward=http://paypa1.com/login>

Expect: WARN — open-redirect (non-standard param)

[%¶ Meta-refresh chain \(local\)](#)

<http://localhost:4005/web-attacks/redirects/meta-to-lookalike.html>

Expect: WARN — auto-forward to a look-alike

[%¶ SquareX redirect range \(real chain\)](#)

<https://sqattckrange.com/rdrct/linkedin.html>

Expect: WARN — redirect chain (+ brand-impersonation on the clone)

Look-alike domains (typosquat / eTLD / unicode)

5 · etld-typosquat **WARN**

[%¶ paypal on .co](#)

<http://paypal.co/>

Expect: WARN — look-alike TLD

[%¶ microsoft on .help](#)

<http://microsoft.help/>

Expect: WARN — look-alike TLD

[%¶ apple on .support](#)

<http://apple.support/>

Expect: WARN — look-alike TLD

6 · unicode-domain **WARN**

[%¶ paypal with a Cyrillic 'a'](#)

<http://xn--pypal-4ve.com/>

Expect: WARN — unicode look-alike

Free-hosted brand pages

[%¶ paypal-login.weebly.com](#)

<http://paypal-login.weebly.com/>

Expect: WARN — brand on a free host

[%¶ microsof-verify.glitch.me](#)

<http://microsof-verify.glitch.me/>

Expect: WARN — look-alike on a free host

Content-based (open these fixtures)

11 · page-content **WARN**

[%¶ Account-suspended phishing login](#)

<http://localhost:4005/web-attacks/page-content/account-suspended.html>

Expect: WARN — login + lure text

12 · clickjacking **BANNER**

[%¶ Invisible overlay iframe](#)

<http://localhost:4005/web-attacks/clickjacking/clickjacking.html>

Expect: BANNER — clickjacking overlay

13 · magecart **BANNER**

[%¶ Fake checkout + skimmer script](#)

<http://localhost:4005/web-attacks/magecart/fake-checkout.html>

Expect: BANNER — untrusted skimmer

14 • drive-by **BLOCK**

[%T Dangerous .exe download](#)

<http://localhost:4005/web-attacks/redirects/driveby.html>

Expect: Download cancelled + notification

15 • malvertising **WARN**

[%T Fake virus-alert scam](#)

<http://localhost:4005/web-attacks/malvertising/fake-virus-alert.html>

Expect: WARN — scam page

Full test consoles

[%T Master console \(all 14 features\)](#)

<http://localhost:4005/web-attacks/category2-all.html>

Expect: 75 cases, PASS/FAIL tracker

[%T LIVE tests \(real hosts: social / Forms / geo / NRD\)](#)

<http://localhost:4005/web-attacks/live-tests.html>

Expect: step-by-step for the LIVE-only features

Note: localhost: links only work on the machine running BDR (fine for self-testing — email to yourself, click from Gmail). The look-alike + sqattckrange links are external; BDR warns BEFORE the page loads.*