

BSIDESTLV 2026 · BUG BOUNTY VILLAGE

Redirected.

Open redirect in the real world - how to send a phishing email.

ABOUT ME



Avishai Gonen

A cyber security researcher. In my free time I do CTFs, bug bounty, and independent research. 30+ CVEs to my name, found as a vulnerability researcher at Pluto Security.



<https://avishaigonen123.github.io>



<https://www.linkedin.com/in/avishai-gonen-997148289>

AGENDA

- Open redirect, in 60 seconds
- JBL: finding → fix → bypass **DEMO**
- Haaretz: from open redirect to phishing **DEMO**
- Haaretz, round 2: the newly found one **DEMO**
- Haaretz, round 3: a bypass of their fix **LIVE DEMO**

OPEN REDIRECT

A redirect you control

A site takes its destination from user input and sends you there - without checking where.



WHY IT MATTERS

Everyone underrates it

- Triage calls it low severity
- But it sends phishing from a domain users trust
- For hunters: a fast, common, low-hanging find

OWASP Top 10 2013 · A10 · CWE-601

Open redirect

JBL

Haaretz

CASE 01



Open redirect

JBL

Haaretz

● DEMO

The report - YesWeHack

Open redirect

JBL

Haaretz

Bypass techniques

The @ trick

trusted.com@evil.com

Protocol-relative

//evil.com

Fragment

trusted.com#@evil.com

Subdomain

trusted.com.evil.com

Backslash

https://evil.com

Encoded slash

trusted.com%2f@evil.com

● DEMO

Breaking the fix

```
https://www.jbl.com@evil.com
```

Filter sees jbl.com. Browser goes to evil.com.

Open redirect

JBL

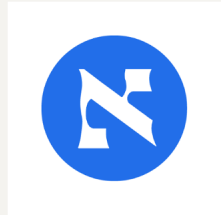
Haaretz

CASE 01 · RECAP

JBL, in short

- An open redirect in a recipe-link email
- Reported, fixed, then bypassed with the @ trick
- \$350 · CWE-601 · rated medium
- Lesson: sell the impact, verify the fix

CASE 02



TheMarker

Haaretz TheMarker

A phishing email that really came Haaretz.

Open redirect

JBL

Haaretz

● DEMO

Watch this.

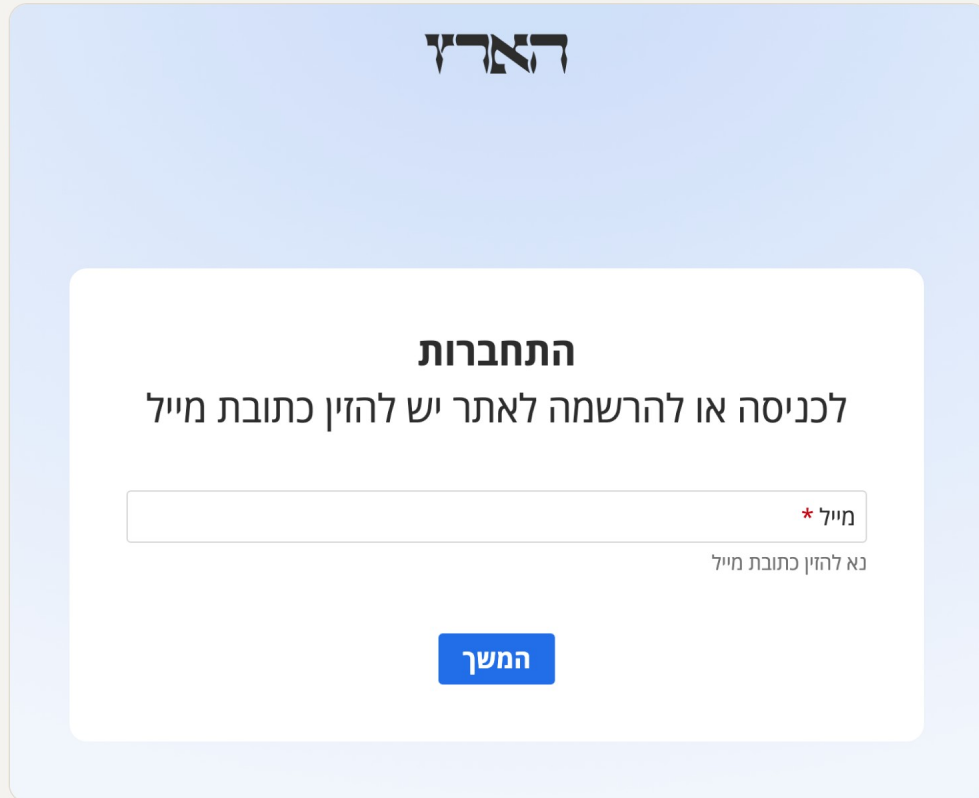
How I phished Ran Bar Zik.

Open redirect

JBL

Haaretz

Sign in - and it emails you



The screenshot shows the Haaretz login interface. At the top is the Haaretz logo. Below it, the heading "התחברות" (Login) is centered. Under the heading is the text "לכניסה או להרשמה לאתר יש להזין כתובת מייל" (To log in or register on the site, you must enter an email address). There is a text input field for the email address, with a red asterisk and the word "מייל" (Email) to its right. Below the input field is the text "נא להזין כתובת מייל" (Please enter email address). At the bottom of the form is a blue button labeled "המשך" (Continue).

The mail is really from Haaretz. The link inside is mine.

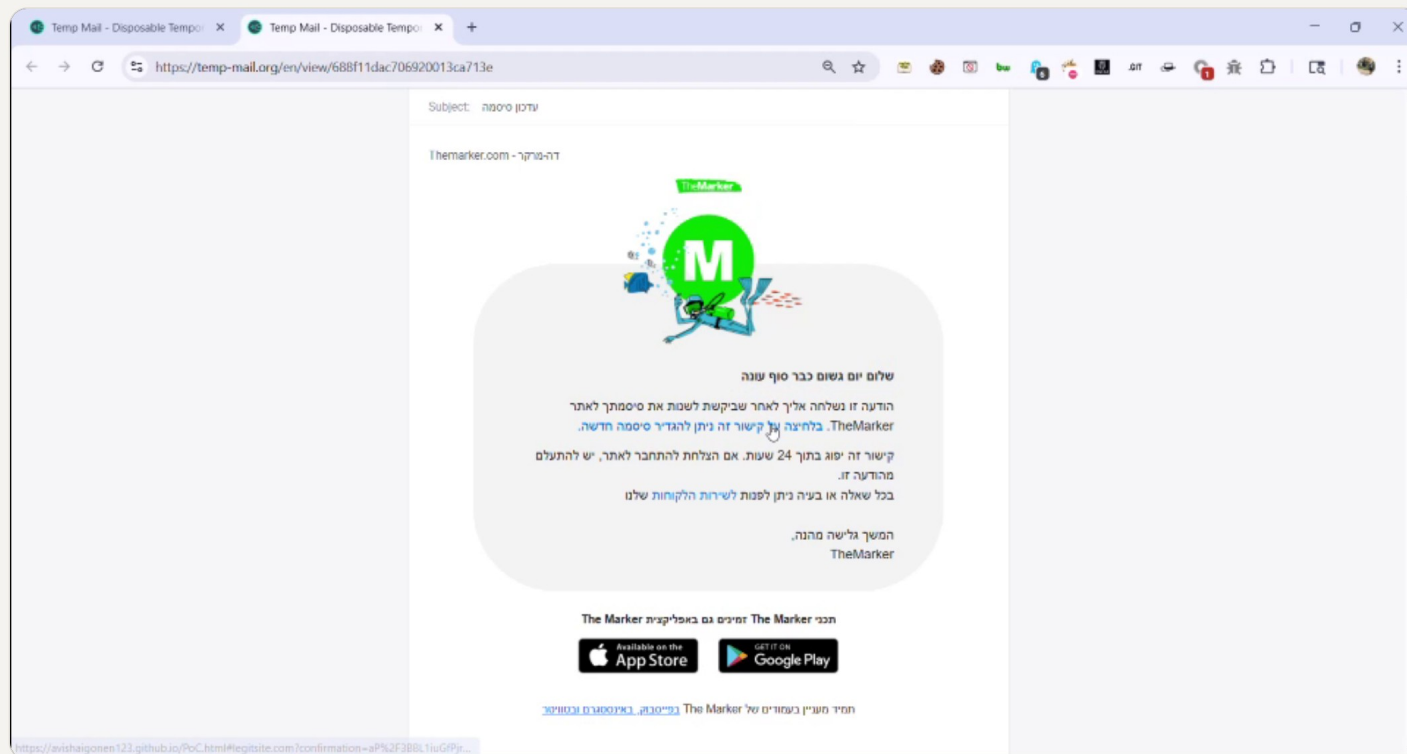
Open redirect

JBL

Haaretz

● DEMO

The redirect, start to finish



Open redirect

JBL

Haaretz

HAARETZ · V2

A year later, I found another.

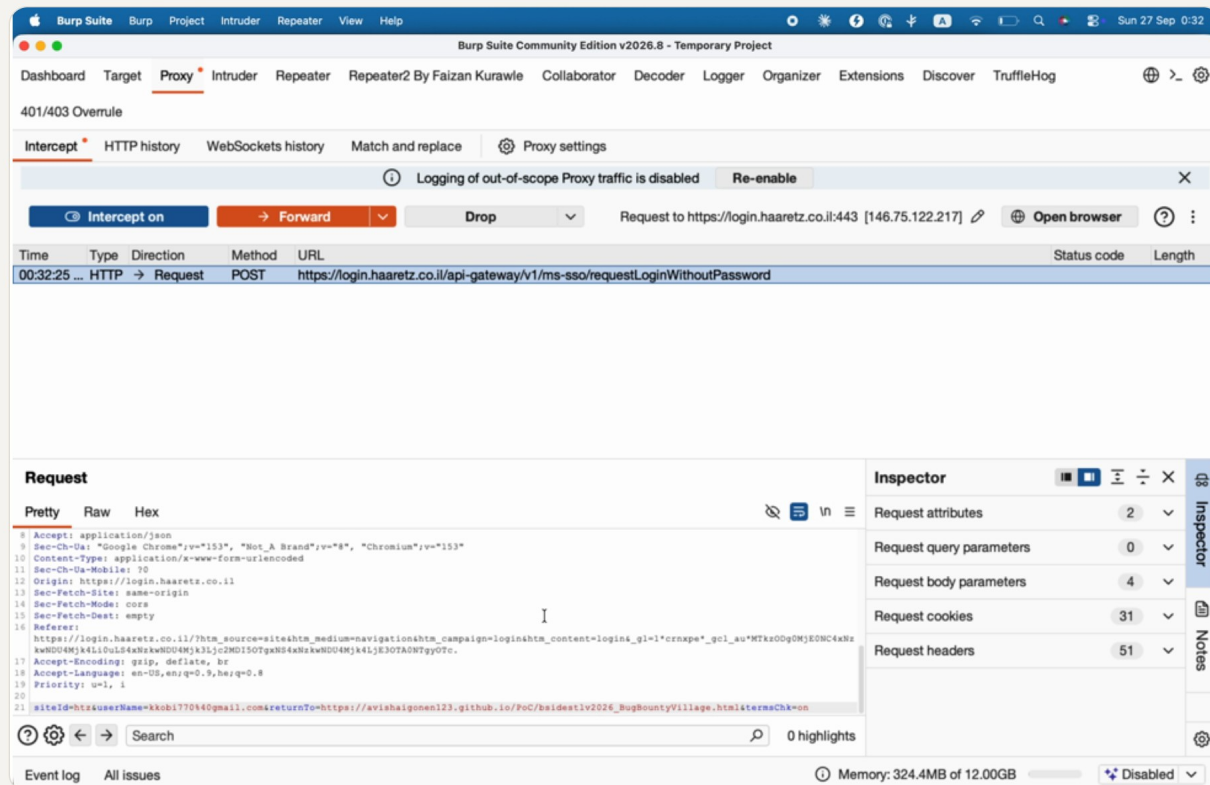
Open redirect

JBL

Haaretz

● DEMO

The **returnTo** redirect



returnTo = my page

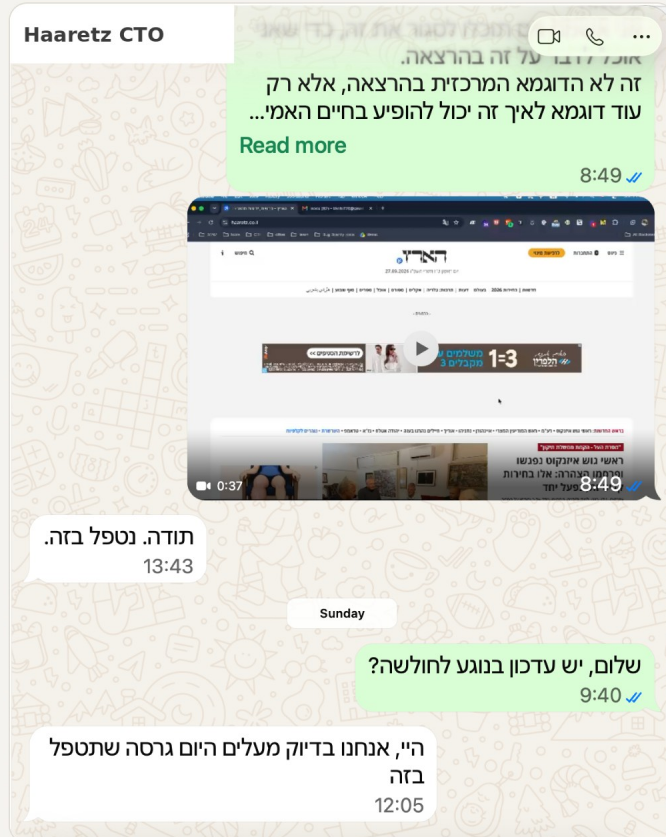
login email → confirmation → my page

Open redirect

JBL

Haaretz

I reported it. They fixed it.



The CTO confirmed the fix - in the thread.
Reported, acknowledged, shipped.

Open redirect

JBL

Haaretz

https://login.haaretz.co.il//avishaigonen123.github.io

11. Intruder attack of https://login.haaretz.co.il

Attack Save ?

Results Positions

Capture filter: Capturing all items Apply capture filter

View filter: Showing all items

Request ^	Payload	Status code	Response rece...	Error	Timeout	Length	Comment
0		200	179			1088	
1	https://avishaigonen123.github.io	200	105			1088	
2	//avishaigonen123.github.io	200	160			1088	
3	https://login.haaretz.co.il//avishaigonen12...	200	853			1185	
4	/avishaigonen123.github.io	200	175			1088	
5	https://avishaigonen123.github.io	200	96			1088	
6	https://login.haaretz.co.il@avishaigonen1...	200	102			1088	
7	https://login.haaretz.co.il.avishaigonen12...	200	156			1088	
8	https://avishaigonen123.github.io/login.ha...	200	158			1088	
9	https://avishaigonen123.github.io/login.h...	200	160			1088	
10	https://login.haaretz.co.il%5C@avishaigo...	200	159			1088	

Request

Pretty Raw Hex

```
15 Sec-Fetch-Dest: empty
16 Referer:
https://login.haaretz.co.il/?htm_source=site&htm_medium=navigation&htm_campaign=login&htm_con
tent=login&_gl=1*m6zc4h*_gcl_au*MTQ1NzQ2MjE0LjE3OTI3Mzg1OTIuLS4tLjE3OTI3Mzg1OTIuNTY0NjQ3ODk1L
jE3OTI3Mzg1OTIuMTc5Mjc5ODU5Mg..
17 Accept-Encoding: gzip, deflate, br
18 Accept-Language: en-US,en;q=0.9,he;q=0.8
19 Priority: u=1, i
20 Connection: keep-alive
21
22 siteId=htz&userName=kkobi770@gmail.com&returnTo=
https%3A%2F%2Flogin%2Ehaaretz%2Eco%2Eil%2F%2Favishaigonen123%2Egithub%2Eio&termsChk=on
```

Response

Pretty Raw Hex Render

```
22 Access-Control-Allow-Credentials: true
23 Content-Length: 174
24
25 {
  "success":true,
  "userMail":"kkobi770@gmail.com",
  "url":"/requestLoginWithoutPassword",
  "message":"email sent to kkobi770@gmail.com",
  "code":200,
  "status":"success",
  "params":null
}
```

Finished

Open redirect

JBL

Haaretz

Then one payload passed



Found while proving v2 was dead.
Reported again.

● LIVE DEMO • HANDS ON

Today? Blocked.

Reported again - live, even the // bypass now returns **400**.

Open redirect

JBL

Haaretz

WHAT WE SAW

- **JBL** - an open redirect that sends phishing from jbl.com (\$350, CWE-601).
- **JBL** - they "fixed" it; the @ trick walked right through.
- **Haaretz** - an open redirect that sends phishing from haaretz.com.
- **Haaretz, round 2** - another open redirect in the login, reported and fixed.
- **Haaretz, round 3** - their fix fell to a double-slash, found live and reported again.

Questions?



Slides & demos



Website



LinkedIn

Thank you.