



Meeting Starts at 7:05PM

In the meantime, checkout <https://granitecity.io>

OWASP Sacramento

April 2023

Agenda

- 1) Food & Drinks
- 2) Intro to the chapter
- 3) Desired outcome from the community
- 4) Next Months' Teaser: Modern Phishing with Evilginx2



Being at Granite City means you're part of an engaging, inviting and supportive ecosystem. It means you're in the company of like-minded and exciting professionals. It means you've joined a place to grow your business and be supported in the process.

All memberships include:

- ✓ High-speed & secure wi-fi
- ✓ Access to printer/copier/scanner
- ✓ Invites to exclusive member-only social events and programs
- ✓ Use of our community kitchen
- ✓ Locally roasted craft coffee served hot and ready until 3pm

Private Office & what you'll get:

- ✓ 24/7 Access
- ✓ Digital Key Access
- ✓ 2 hours of free meeting room space per month (Town Hall or Gallery)

Coworking & what you'll get:

- ✓ **Part-Time Membership** – 4 days per month access
- ✓ **Weekdays** – 8:30am-5pm Monday – Friday access, digital key entry, 2 hours of free meeting space per month (Gallery)
- ✓ **Full Time** – 24/7 access, digital key access, 2 hours of free meeting space per month (Gallery)

History of the Sacramento Chapter



2023: Meetings lined up for April, May, June, July, August and September

Chapter Started - 2010?

Chapter with some attendance

Chapter died out and leaders were non-responsive - 2014?

We rebooted the chapter - 2019

We were doing okay... ish

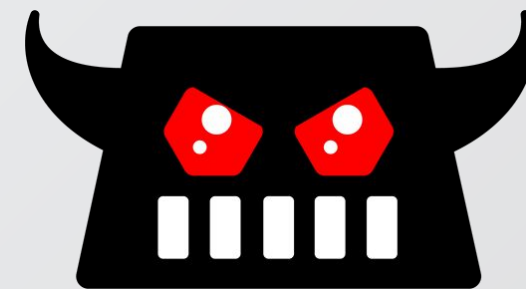
COVID - 2020

Now Let's do better this time

OWASP Sacramento Chapter

Let's discuss

- How can we make this chapter better?
- What are our members looking to get out of this group?



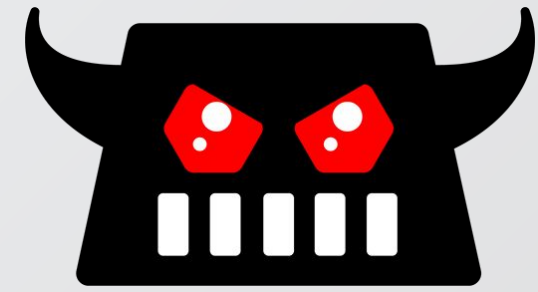
Modern Phishing with Evilginx2 (Preview)

evilginx2 is a man-in-the-middle attack framework used for phishing login credentials along with session cookies, which in turn allows to bypass 2-factor authentication protection.

- Custom version of nginx HTTP server to provide man-in-the-middle functionality to act as a proxy between a browser and phished website.
- Implements its own HTTP and DNS server.
- Utilizes LetsEncrypt for TLS certs.
- Does contain known signatures for Blue Teams.
- FIDO2 will protect you as it's domain specific.
- Operationalizing it takes creativity, speed, and contains many other small nuances (next month).

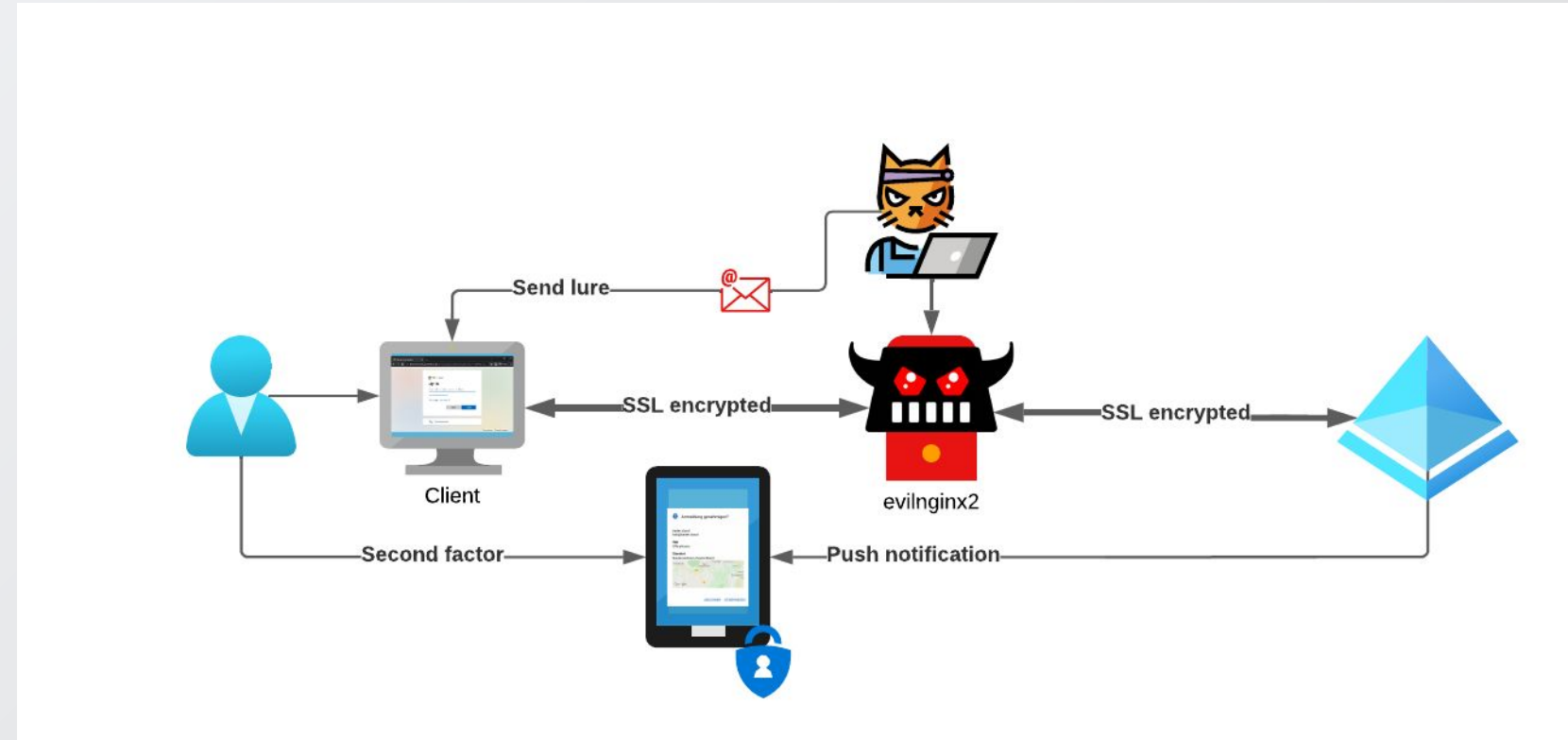
GitHub Project: <https://github.com/kgretzky/evilginx2>

Modern Phishing with Evilginx2 (Preview)



Lures can be....

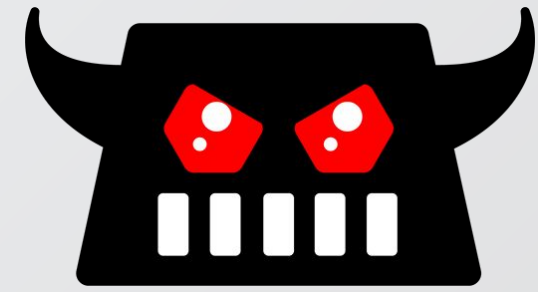
- Placed on creative TLDs.
- Emailed to victims directly.
- Presented via DNS Spoofing.
- QR codes, etc...



Modern Phishing with Evilginx2

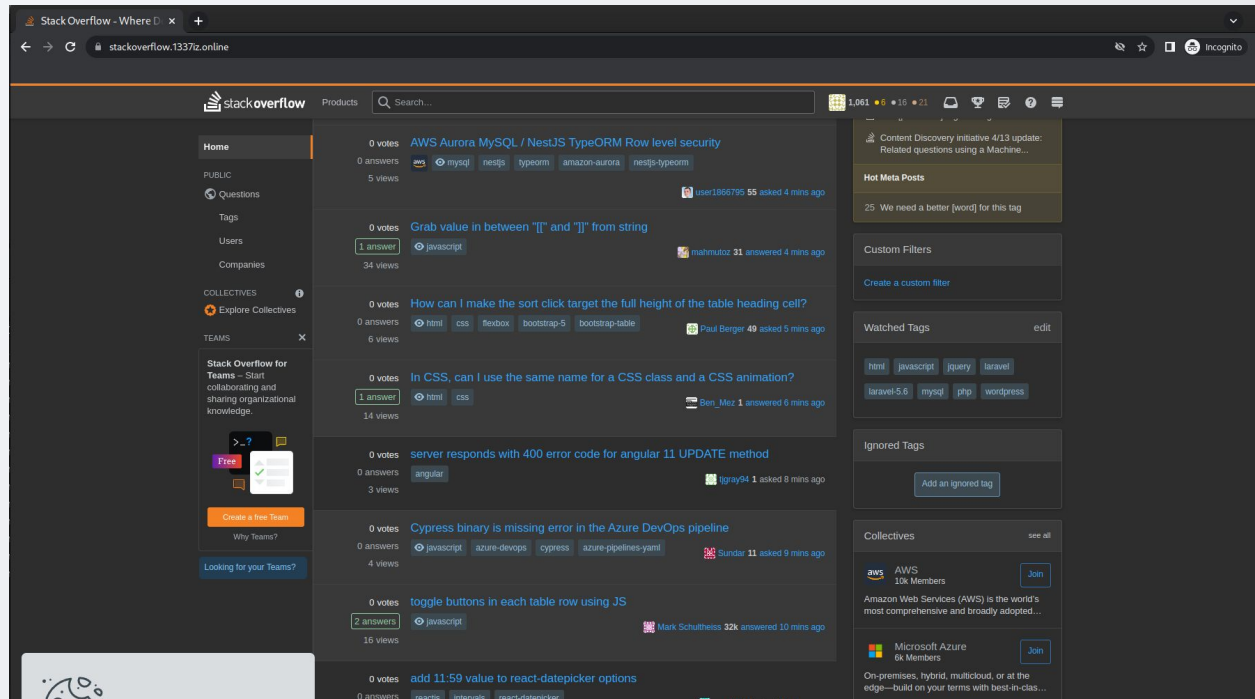
Demo (preview?)

Modern Phishing with Evilginx2 (Preview)



stackoverflow.coach	60 €	Select Domain
stackoverflow.codes	60 €	Select Domain
stackoverflow.coffee	30 €	Transfer domain

Next month we'll teach you how to phishlet ;)



```
lures get-url 7
https://stackoverflow.1337iz.online/thKvKDuY
21:46:57] [imp] [0] [stackoverflow] new visitor has arrived: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/111.0 (73.235.22.9)
21:46:57] [inf] [0] [stackoverflow] landing URL: https://stackoverflow.1337iz.online/thKvKDuY
21:48:11] [+++] [0] all authorization tokens intercepted!
21:48:18] [imp] [0] redirecting to URL: https://stackoverflow.com (1)
21:50:31] [war] [stackoverflow] unauthorized request: https://stackoverflow.1337iz.online/ (facebookexternalhit/1.1 (+http://www.facebook.com/externalhit_uatext.php)) [69.171.249.12]
21:50:45] [+++] [0] Password: [redacted]
21:50:45] [+++] [0] Username: [ryan.kozak@owasp.org]
21:50:45] [+++] [0] Username: [ryan.kozak@owasp.org]
21:50:45] [+++] [0] Password: [redacted]
21:50:46] [war] [stackoverflow] unauthorized request: https://stackoverflow.1337iz.online/?fbclid=IwAR2fSVW0vzn7yYoBPECZMQEj09PNrOHGgDnFw2qw8lyYvPCQ0GrTAyGAI (Mozilla/5.0 (iPhone; CPU iPhone OS 16_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) CriOS/110.0.5481.83 Mobile/15E14 Safari/604.1) [31.13.115.24]
[0] 0:./evilginx+ "scanner" 21:51:19-Apr-23
```

OWASP Community

Next Meeting: **May 17th** from 7PM-9PM (same location)

Call for Presentations: **June** and **July** (same location)

If you'd like to present (or know someone else who would) at the OWASP Sacramento Chapter's upcoming meetings, please email us your topic.

You don't need to be an expert!

Joubin: joubin.jabbari@owasp.org

Ryan: ryan.kozak@owasp.org