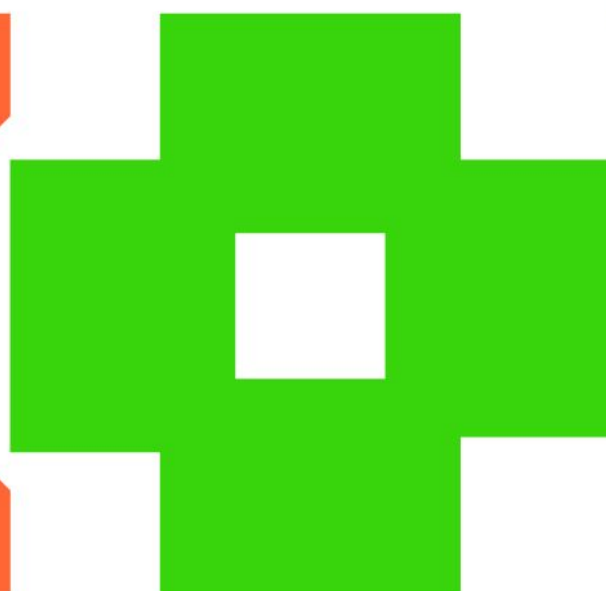
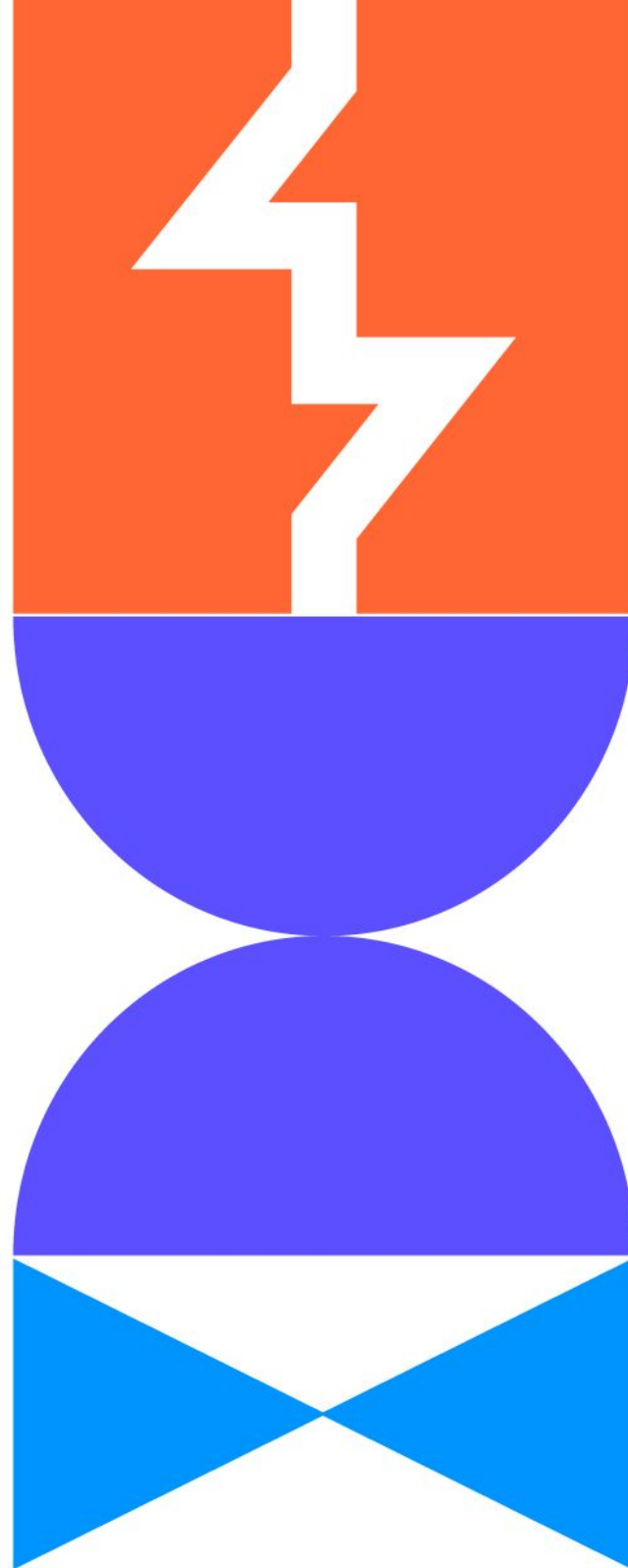


# Results

## Top 10 NEW Web Hacking Techniques 2024



# 10 Hijacking OAuth flows via Cookie Tossing

*Elliot Ward*

# 09 Wildcard Web Cache Deception in ChatGPT

*Harel Security Research*

# 08 OAuth Non-Happy Path to ATO

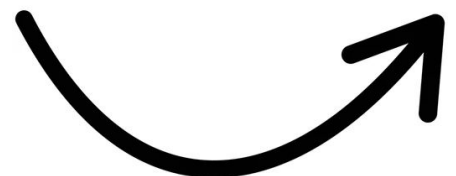
*Oxrz*

# 07 Arbitrary JavaScript execution in PDF.js

*Thomas Rinsma*

# 06 DoubleClickjacking: A New Era of UI Redressing

*Paulos Yibelo*





Mizu

# Exploring the DOMPurify Library

Mutation XSS by leveraging node flattening, stack of open elements, and namespace confusion to bypass DOMPurify.





*Orange Tsai*

# WorstFit: Hidden Transformers in Windows ANSI

Exploiting Windows Best-Fit character conversion for attacks like Path Traversal, Argument Injection, and RCE across various applications.





*Paolo Arnolfo (@sw33tLie), Guillermo Gregorio (@bsysop) and @\_medusa\_1\_*

# Unveiling TE.0 HTTP Request Smuggling

A novel HTTP Request Smuggling vector affecting Google Cloud-hosted websites.





*Paul Gerste*

# SQL Injection Isn't Dead

Protocol-level SQL injection attacks  
via database wire protocol smuggling.





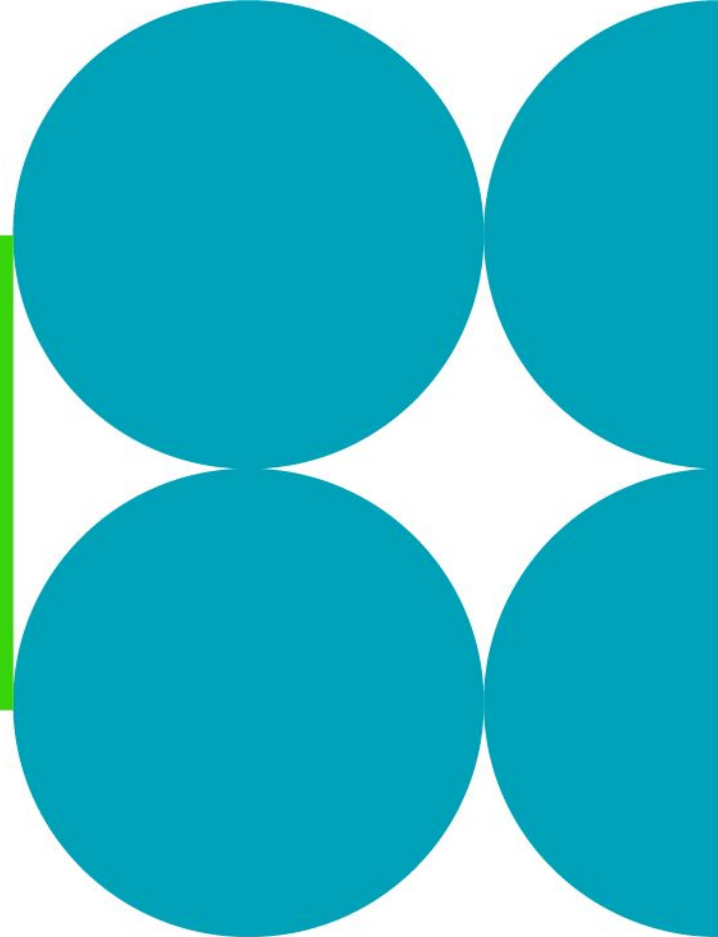
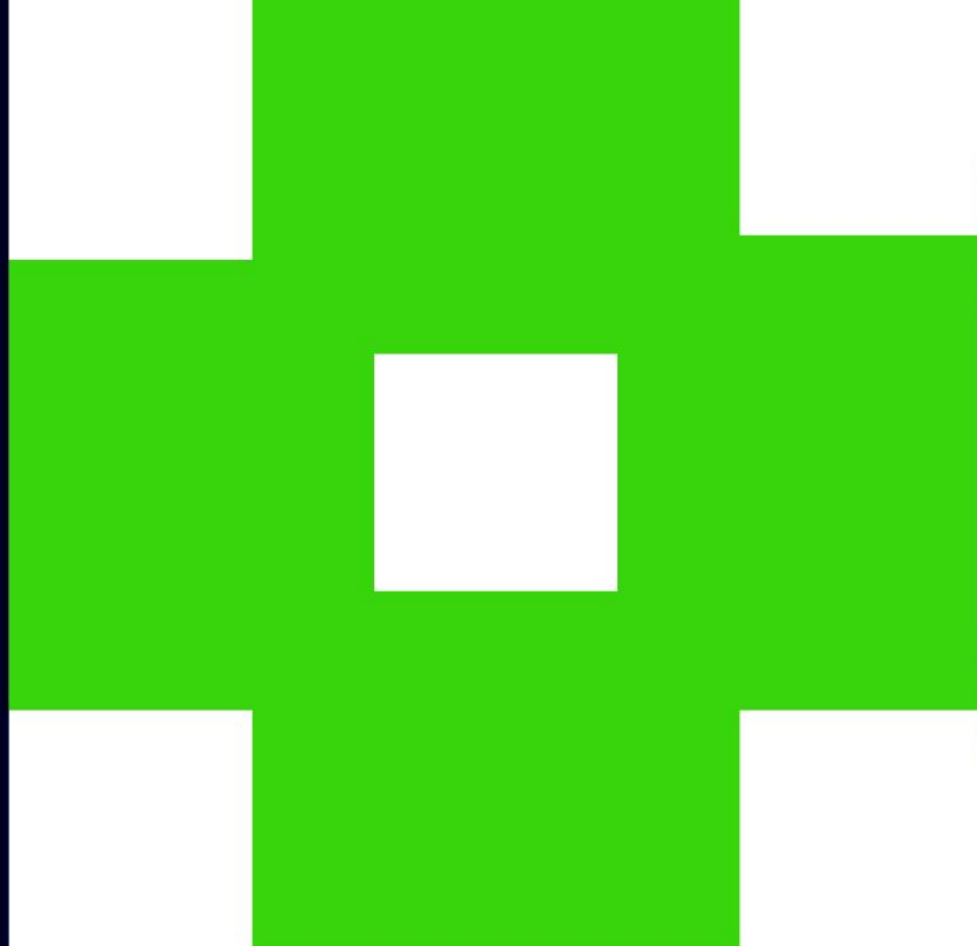
*Orange Tsai*

# Exploiting Hidden Semantic Ambiguity in Apache

Exploiting architectural flaws in Apache HTTP Server's module interactions to achieve insecure path access, predictable handler manipulation, and authentication bypass.



**2024**



**View the full list  
in the link  
below.**

