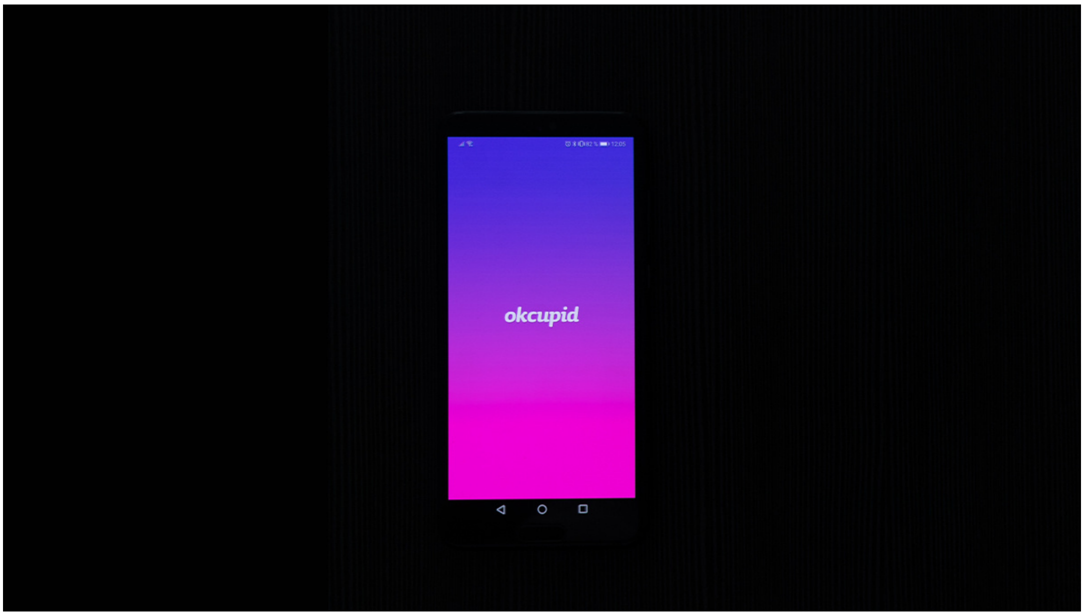
The Daily Swig
Cybersecurity news and views

Vulnerability in dating site OkCupid could be used to trick users into 'liking' or messaging other profiles

Adam Bannister 04 August 2021 at 14:13 UTC
Updated: 04 August 2021 at 14:28 UTC

Vulnerabilities CSRF Privacy

Miscreants could also potentially see dating profiles of logged-in victims



A security vulnerability in popular dating site OkCupid meant an attacker could dupe users into unknowingly 'liking' or sending messages to other profiles.

The flaw, which earned its finder an undisclosed bug bounty reward, has now been patched.

Contingent on tricking victims into clicking a malicious link, the feat was achieved by combining a cross-site request forgery (CSRF) bug with a "JSON type confusion" vulnerability, explained Yan Zhu, security engineer at privacy-focused browser Brave, in a blog post.

"Obviously you could abuse this in order to match with anyone you could trick into clicking a link, or you could spam the link to a bunch of people to increase your profile's rankings in whatever mysterious algorithm OkCupid uses to suggest people," continued Zhu.

Catch up on the latest security vulnerability news and analysis

"It also occurred to me that if I redirected my website to the CSRF link that automatically sent a message to me, I could see the OkCupid profiles of my website visitors who were logged into okcupid.com, which would make for an intense web analytics tool."

Cunning Casanova

The researcher studied OkCupid after "checking if websites were sending CSRF tokens alongside requests that require authentication, like sending messages to another user from your account".

She noticed that messages sent on the dating site were sent via `POST` requests that lacked protective CSRF tokens to https://www.okcupid.com/1/apitun/messages/send with a JSON-encoded body.

Zhu then created a webpage that, after some trial and error, successfully sent a cross-origin `POST` request to OkCupid's message-sending endpoint on the third attempt.

She tested the exploit against friends who had active OkCupid profiles, explaining that: "Lo and behold, my OkCupid test profile was serenaded by a series of messages that they didn't mean to send me."

Zhu joked: "I briefly felt very popular, which made it all worthwhile."

Latest Posts

Black Hat 2021: New tool si
web-wide vulnerability resea
'Even the most resource-constrain
researcher can now add web-scale
to their arsenal'

#BHUSA 2021
Zero-days, ransoms, supply chains

Authentication bypass vulne
found in multiple routers anc
modems
Devices using Arcadyan software

OkCupid, which was alerted to the flaw during April 2021, told the researcher that it had promptly fixed the flaw.

Interrogate your inputs

Zhu also investigated whether other sites’ authenticated endpoints similarly accepted `POST`s with `content-type: text/plain`, despite expecting JSON.

Of 215 endpoints associated with Alexa’s top 500 sites that sought requests containing `api` or `json`, 87 failed to return errors, with many apparently returning JSON responses.

“Granted most of these are probably not authenticated endpoints and some of them may need to accept non-JSON text, but this suggests to me that developers should be careful accepting `text/plain` inputs on endpoints that parse JSON,” concluded Zhu.

Regardless, however, she also noted that setting your browser’s `SameSite` cookie attribute to ‘Strict’ effectively prevents this, most other CSRF attacks.

The Daily Swig has contacted OkCupid for further comment. We will update the article if we receive a response.

YOU MIGHT ALSO LIKE Security researcher finds dangerous bug in Chromium, nabs $15,000 bounty

Vulnerabilities CSRF Privacy Browsers Bug Bounty Social Engineering Phishing Research Authentication API
Secure Development Hacking News Hacking Techniques Hacking Tools Social Media VDP

Adam Bannister

@Ad_Nauseum74

Related stories

Black Hat 2021: New tool simplifies web-wide vulnerability research

04 August 2021

#BHUSA 2021

Zero-days, ransoms, supply chains, oh my!

04 August 2021

Authentication bypass vulnerability found in multiple routers and modems

04 August 2021

Dating deception

OkCupid flaw could be used to t
users into messaging other profi

04 August 2021

Burp Suite

Web vulnerability scanner
Burp Suite Editions
Release Notes

Vulnerabilities

Cross-site scripting (XSS)
SQL injection
Cross-site request forgery
XML external entity injection
Directory traversal
Server-side request forgery

Customers

Organizations
Testers
Developers

Company

About
PortSwigger News
Careers
Contact
Legal
Privacy Notice

Insights

Web Security Academy
Blog
Research
The Daily Swig

PortSwigg

Follow us