

Forum:[Hack Forums](#)

Thread: [How To Exploit HTTP DELETE Method](#)

Nortrium - April 11, 2020, 12:25 pm

Good afternoon,

I was hoping the high intellects of HackForums could teach me how to exploit this vulnerability.
Thank you!

TELEGRAM: @M4MB4

??¢??? - April 13, 2020, 3:36 pm

(Apr 11, 2020 12:25 PM)Nortrium Wrote: [\[CITE\]](#) Good afternoon,

I was hoping the high intellects of HackForums could teach me how to exploit this vulnerability.
Thank you!

TELEGRAM: @M4MB4

HTTP DELETE Method is most commonly used with API Calls. For Example: You have a website where you have provided a feature of Delete User button.

When a user clicks on delete, a HTTP request like this is sent:

Code DELETE <https://examplewebsite/api/deleteuser/2345>
Here "2345" is the UserID.

Now in cases like IDOR (Insecure Object Reference) a different USER with UserID 4567 clicks on the "Delete account " button and then in the HTTP Request which follows he/she replaces his own ID "4567" with the victim's ID "2345". Thereby, he ends up deleting someone else's account on the website.

Another bug would be that no authentication is actually required you simply call the URL with DELETE method and change the ID and the respective accounts will start getting deleted from the server.

Some other cases would be
Delete File uploaded by another user

Delete Post/Comment of another User

Delete His saved profile

Delete items from a shopping cart

Delete any stored information in any other user's profile

Real Life bug example would be when a user was able to delete the tweet of any other user (was patched last year)

Shisho - April 13, 2020, 3:49 pm

(Apr 13, 2020 03:36 PM)??¢??? Wrote: [\[CITE\]](#) HTTP DELETE Method is most commonly used with API Calls. For Example: You have a website where you have provided a feature of Delete User button.

When a user clicks on delete, a HTTP request like this is sent:

Code DELETE <https://examplewebsite/api/deleteuser/2345>
Here "2345" is the UserID.

Now in cases like IDOR (Insecure Object Reference) a different USER with UserID 4567 clicks on the "Delete account " button and then in the HTTP Request which follows he/she replaces his own ID "4567" with the victim's ID "2345". Thereby, he ends up deleting someone else's account on the website.

Another bug would be that no authentication is actually required you simply call the URL with DELETE method and change the ID and the respective accounts will start getting deleted from the server.

Some other cases would be
Delete File uploaded by another user

Delete Post/Comment of another User

Delete His saved profile

Delete items from a shopping cart

Delete any stored information in any other user's profile

Real Life bug example would be when a user was able to delete the tweet of any other user (was patched last year)

Vouch for this.

DELETE is generally going to result in some kind of deletion of some kind of object like a file or a database record through processing of an unauthenticated request or some type of authentication bypass/XSRF.

Sometimes you get similar results with PUT.

??¢??? - April 13, 2020, 3:55 pm

(Apr 13, 2020 03:49 PM)Shisho Wrote: [\[CITE\]](#) Vouch for this.

DELETE is generally going to result in some kind of deletion of some kind of object like a file or a database record through processing of an unauthenticated request or some type of authentication

bypass/XSRF.

Sometimes you get similar results with PUT.
PUT or PATCH Method.