5

Account takeover due to CSRF in "Account details" option on [redacted]

Share:

State	○ Resolved (Closed)
Disclosed	**January 11, 2019 6:32pm +0530**
Reported To	**U.S. Dept Of Defense**
Weakness	Cross-Site Request Forgery (CSRF)
Severity	Medium (4 ~ 6.9)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE · EXPORT

mik317 submitted a report to U.S. Dept Of Defense. Sep 15th (about 1 year ago)

Summary:

Hi DoD team,
similarly to the previous CSRF that I've reported, I've found another CSRF in the same domain, but on the `Account details` option.

Description:

The CSRF issue allows me to modify the datas of every victim that is targeted using the CSRF file, and leading to account takeover simply setting my email as email of the victim: logging out I can recover the password of the infected account using the attacker-email that has replaced the victim-email.

Step-by-step Reproduction Instructions

1. Login as victim and check your infos in the account details
2. Open the CSRF malicious file {F346689}
3. Recheck the infos: now the email is different (also the username) {F346690}

(In the video the `@` char is replaced with `%40` (url encoded version of the `@` char), but is due to a problem in the CSRF value, simply replacing `%40` to `@` in the `email` parameter, the `@` char appears).

For account takeover now:

1. Go in anonymous mode (now you're the attacker that hasn't access to the accounts)
2. The victim has opened the CSRF file, so your email is setted in the victim's account
3. Go on the login, and request the `Forgot password` option, inserting the email used for replace the one of the victim
4. You obtain a link for reset the password (I've not done a video, but if you can't reproduce the steps I can do one for these steps also :))

Suggested Mitigation/Remediation Actions

Use captchas and CSRF-tokens for be sure that the victim is changing the datas knowing that.

Impact

The [redacted]ShopCart has a POST CSRF issue also in the account details, that can lead to account takeover replacing the email of the victim with the email of the attacker, and requesting a new password using the `Forgot password` option.

BOT: U.S. Dept Of Defense posted a comment. Sep 15th (about 1 year ago)

Greetings from the Department of Defense (DoD),

Thank you for supporting the DoD Vulnerability Disclosure Program (VDP).

By submitting this report, you acknowledge understanding of, and agreement to, the DoD Vulnerability Disclosure Policy as detailed at @DeptofDefense.

The VDP Team will review your report to ensure compliance with the DoD Vulnerability Disclosure Policy. If your report is determined to be out-of-scope, it will be closed without action.

We will attempt to validate in-scope vulnerability reports and may request additional information from you if necessary. We will forward reports with validated vulnerabilities to DoD system owners for their action.

Our goal is to provide you with status updates not less than every two weeks until the reported vulnerability is resolved.

Regards,

The VDP Team

mik317 posted a comment. Sep 15th (about 1 year ago)

Complete video PoC: {F346717}
CSRF form file used for the PoC : {F346716}

ag3nt-z3 updated the severity to Medium. Sep 18th (about 1 year ago)

ag3nt-z3 changed the status to ○ **Triaged**. Sep 18th (about 1 year ago)

Greetings,

We have validated the vulnerability you reported and are preparing to forward this report to the affected DoD system owner for resolution.

Thank you for bringing this vulnerability to our attention!

We will endeavor to answer any questions the system owners may have regarding this report; however, there is a possibility we will need to contact you if they require more information to resolve the vulnerability.

You will receive another status update after we have confirmed your report has been resolved by the system owner. If you have any questions, please let me know.

Thanks again for supporting the DoD Vulnerability Disclosure Program.

Regards,

The VDP Team

ag3nt-z3 updated the severity from Medium to Medium. Sep 18th (about 1 year ago)

ag3nt-j1 closed the report and changed the status to ○ **Resolved**. Dec 17th (10 months ago)

Good news!

The vulnerability you reported has been resolved and this report is now closed. If you have any further questions or disagree that the report is resolved, please let us know.

Thank you for your time and effort to improve the security of the DoD information network.

Regards,

The VDP Team

mik317 requested to disclose this report. Dec 31st (9 months ago)

Can we disclose partially (only the title or just a simple description) ?

Regards, Mik

mik317 posted a comment. Jan 3rd (9 months ago)

Hi @ag3nt-j1 , @ag3nt-z3 and @ag3nt-s21
good new year and hope a better one :)
Can we disclose (partially) some of my reports?

Best, Mik

agent-1 posted a comment. Jan 5th (9 months ago)

Mik,
The following message is approved for public disclosure:

A cross-site request forgery (CSRF) vulnerability was found on a Department of Defense (DoD) website which could allow an unauthorized account takeover. mik317 was able to demonstrate this vulnerability by setting the email as that of the victim using the CSRF file. Thank you for the disclosure of this vulnerability, and helping us increase the security of our website!

Do you have a Twitter handle that we can tweet out a thanks to? @DC3VDP

mik317 posted a comment. Updated Jan 5th (9 months ago)

Hi @agent-1 ,
good new year and nice to meet you :)
The message is perfect, like this program.
No, I haven't any social, for me the best thank is see these reports resolved :) Perhaps, if you can send to me an email with the same text that you send on Twitter, I will really appreciate. (If possible, my email is kickmik.mr@hotmail.com)

Best, Mik

agent-1 posted a comment. Jan 5th (9 months ago)

Thanks Mik. It is nice to meet you as well. I gave you a shout-out anyway. https://twitter.com/DC3VDP/status/1081260229889835008

Keep up the great work!

DC3 VDP Team

deez_nops posted a comment. Jan 5th (9 months ago)

@mik317 Congrats on being our 1st researcher shoutout Tweet!! Keep bringing us those High and Critical vulns'!

mik317 posted a comment. Updated Jan 5th (9 months ago)

Thank you so much ;)

Best, Mik

mik317 posted a comment. Updated Jan 5th (9 months ago)

Can we also disclose partially on this platform (HackerOne) ?
Best, Mik

ag3nt-j1 posted a comment. Jan 5th (9 months ago)

Hey Mik, I'm going to be playing around with trying to redact and disclose the report. If you see it come in and out of disclosure don't panic, trying to figure out how this thing works.

mik317 posted a comment. Jan 5th (9 months ago)

Thank you so much,
excuse me if I waste your time with these stuffs, but probably is one the best I've found :)
If you have any doubt you can I'm here for help you (more or less I know how works)

Cheers, Mik

ag3nt-j1 posted a comment. Jan 5th (9 months ago)

All good Mik, we appreciate all the work and effort. I put in a request to H1 for a little more detail on what to expect when I publish this out as disclosed. Might be beginning of next week before I can publish this to you as I wait for a response.

mik317 posted a comment. Jan 5th (9 months ago)

Thank you so much :)

Regards, Mik

ag3nt-j1 agreed to disclose this report. Jan 11th (9 months ago)

This report has been disclosed. Jan 11th (9 months ago)

mik317 posted a comment. Jan 11th (9 months ago)

Thank you so much @ag3nt-j1 , @ag3nt-s21 , @ag3nt-z3 and @agent-1 .
Always the best :)
Hope you'll pass a good year ;)

Regards, Mik