



9

attacker can book unlimited tickets in free at https://aaf.com/checkout/order-received/21237/?key=wc_order_5bbef48fa35b2

Share:      State Resolved (Closed)Disclosed **April 25, 2019 10:27am +0530**Reported To [Alliance of American Football](#)Asset
aaf.com
(Domain)

Weakness Business Logic Errors

Bounty \$500

Severity High (7 ~ 8.9)Participants   

Visibility Disclosed (Full)

[Collapse](#)

SUMMARY BY GUJJUBOY10X00



Hi Team,

After looking into ticket booking at <https://aaf.com/checkout/XXXXXX> request, i tried to change value of ticket in burp request, but there is proper validation, so it was not possible to buy ticket by changing amount of ticket.

after looking request carefully, i saw that user can buy 3-seats-3 only from UI level, what if i changed from 3-seats-3 to 10-seats-10, and change money amount from 23\$ to 0\$ and i was able to forward that request, success.

same way attacker can buy unlimited ticket in 0\$

my suggestion is to think out of box and dig each and every request completely without just doing normal known test cases.

Team is very cool and reply very quick and fixed this issue by changing complete architecture of this product.

TIMELINE

[gujjuboy10x00](#) submitted a report to [Alliance of American Football](#).

Oct 11th (7 months ago)

Dear Team,

Summary: [add summary of the vulnerability]After looking into <https://aaf.com/>

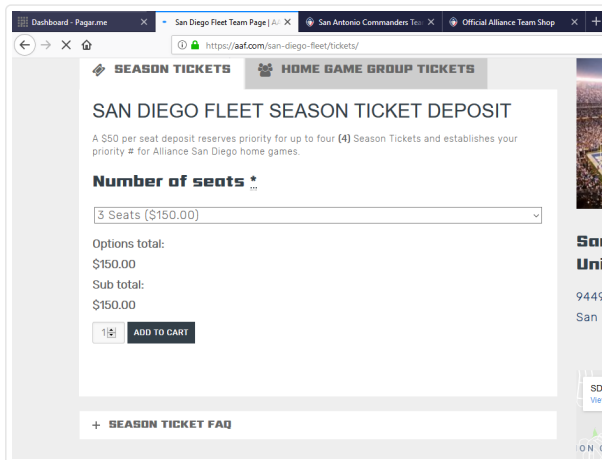
i get to know that there is way where i can book a ticket and can play around, but it asked for valid credit card and all stuff so, i tried to bypass and bought a ticket 23 with 0\$

Live PoC:

https://aaf.com/checkout/order-received/21237/?key=wc_order_5bbef48fa35b2 (check this one)**Description:** [add more details about this vulnerability]attacker can book unlimited tickets in free at https://aaf.com/checkout/order-received/21237/?key=wc_order_5bbef48fa35b2

Steps To Reproduce:

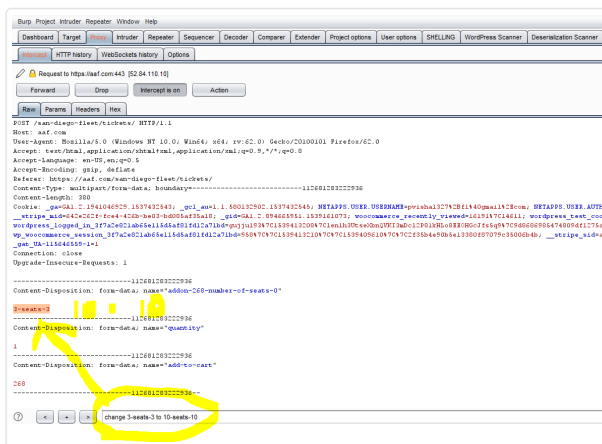
1. go to aaf.com and login with your account
2. click on ticket option and select San Antonio Commanders Season and click on that and select 3 or any ticket and intercept that request, and change from 3-seats-3 to 10-seats-10



snip:

Content-Disposition: form-data; name="addon-268-number-of-seats-0"

10-seats-10



1. click on add tickets and you can see your order is 0\$

and book any number of ticket at 0\$

Supporting Material/References:

Please find attachment

Thanks,

Vishal

Impact

attacker can book unlimited tickets in free at https://aaf.com/checkout/order-received/21237/?key=wc_order_5bbef48fa35b2

2 attachments:

F358788: [t12.PNG](#)

F358789: [t1.PNG](#)



ktistai HackerOne staff changed the status to Needs more info.

Oct 31st (6 months ago)

Hi @gujjuboy10x00 ,

While it does look as you describe it, this one may not be a security issue.

Is there any payment process in between? Have you actually paid \$0? Or is it just a booking?

Thank you,

@ktistai



gujjuboy10x00 changed the status to New.

Nov 1st (6 months ago)

yeah , its like i manipulate that and i need to pay only 0\$

but if you don't manipulate that then you need to pay actually 60\$ for that :) please check that



ktistai HackerOne staff changed the status to Needs more info.

Nov 1st (6 months ago)

@gujjuboy10x00 ,

Soo, in order for us to be able to validate this, we need to confirm that the system has allowed you to buy 10 tickets using 0\$ (or at least one ticket with 0\$)

The problem is that, and I've seen it quite a number of times, sometimes a hacker can manipulate the ordering process to make it look like it will cost 0\$, but then when the actual payment is done, the backend system is making some other checks that would either invalidate the request or re-calculate the whole amount.

At this very moment, you have manipulated the backend server to create an order for you that looks like it costs 0\$, and I agree fully so far. But for this to be an actual issue it has to go further than this and actually accept the payment.

Thanks,

@ktistai



gujjuboy10x00 changed the status to New.

Updated Nov 1st (6 months ago)

Here , is proof:

https://aaf.com/checkout/order-received/21237/?key=wc_order_5bbef48fa35b2

click on that , that is receipt for 23 tickets at 0\$, i got email for same also

if there is any additionally check , that server should not generate this ticket and send an email , so this looks actual bypass



ktistai HackerOne staff changed the status to Needs more info.

Nov 2nd (6 months ago)

Oook this is weird. I do not have the same options as you do to buy tickets. I get redirected to another website (<https://oss.ticketmaster.com/>) when I click on the Buy Now.

Can you please have a look and let me know what I am missing. I followed your steps exactly, but I don't get the same options. I have an European IP though, can that be the problem?

Thanks,

@ktistai

1 attachment:

F369745: [Screenshot_2018-11-02_at_09.22.22.png](#)



gujjuboy10x00 changed the status to New.

Nov 2nd (6 months ago)

ya @ktistai ,

can you please check with team , they looks did some changes , its complete changed flow (as its almost 22 days from i reported this vulnerability)

Thanks god that i have 100% Proof about this vulnerability , so you people know that this is actual vulnerability.

Thanks,

Vishal



ktistai HackerOne staff changed the status to Triaged.





Nov 19th (5 months ago)



Hi @gujjuboy10x00 ,





You were correct and indeed this was an issue. We will now triage it and will let you know once we have more information to share.



Thanks,

@ktistai

-  [ktistai](#) HackerOne staff updated the severity from Critical to Critical (9.3). Nov 19th (5 months ago)
-  [ktistai](#) HackerOne staff updated the severity from Critical (9.3) to High. Nov 19th (5 months ago)
-  [Alliance of American Football](#) rewarded [gujjuboy10x00](#) with a \$500 bounty. Nov 28th (5 months ago)
-  [gujjuboy10x00](#) posted a comment. Nov 28th (5 months ago)
Dear [@aaf](#) ,

i can see this looks , booking of unlimited ticket and can sold out with huge price as attacker (still high or critical can be more than 1500\$ -3000\$) , can you please check about rewards again?
-  [ccbrown_aaf](#) posted a comment. Nov 28th (5 months ago)
We found this to fall into the "high" severity range, which is documented on our program page as rewarding \$500-\$1500. We have people looking at all of the orders, so this issue would have been unlikely to actually result in free tickets being delivered. Thus the reward is on the lower end of the "high" severity range.
-  [gujjuboy10x00](#) posted a comment. Nov 28th (5 months ago)
Ok [@ccbrown_aaf](#) ,

Thanks for quick info , can i have bonus bounty for this amazing bug?
-  [ccbrown_aaf](#) changed the scope from *.aaf.com to aaf.com. Jan 26th (3 months ago)
-  [gujjuboy10x00](#) posted a comment. Jan 28th (3 months ago)
This is fixed now [@ccbrown_aaf](#)
-  [ccbrown_aaf](#) closed the report and changed the status to Resolved. Jan 29th (3 months ago)
-  [gujjuboy10x00](#) posted a comment. Jan 31st (3 months ago)
Dear [@ccbrown_aaf](#) ,

I wrote little info about this bug in sort , can we disclose it limited , if its in your policy?
Limited disclosure only :)
-  [gujjuboy10x00](#) requested to disclose this report. Mar 26th (about 1 month ago)
limited disclose please?
-  This report has been disclosed. Apr 25th (6 hrs ago)