php injection and html session injection

Submitted 2 days ago

Status

Not applicable

This submission was marked not applicable. It is not a rewardable submission at this time.

Reward

VRT version

1.9

Program

Binance

Closed on

2 Apr 2021

CrowdStream visibility

Choose to associate your details with this submission in CrowdStream when accepted.

Show username

Show reward

Please note: This program does not currently disclose submission activity in CrowdStream.

Appeals

You can resolve most issues through communication with the program owner.

If you are unable to resolve your issue, you can make an appeal.

Make an appeal

Disclosure policy

Please note: This program does **not allow** disclosure. You may not release information about vulnerabilities found in this program to the public.

Need Help?

Issues with a submission?
Please reach out to support@bugcrowd.com

Reference
`be32833b4de50132707bd5fd95a0965f6fd21d96fe4779e812b512e81159e20f`

Submitted
02 Apr 2021 16:11:51 EDT

Target Location
`binance.us`

Target category
Website Testing

VRT
Client-Side Injection

Bug URL
https://www.binance.us/en/home

Description
binance is suspectible to php injection and also session hijack through kali linux via metasploit using armitage gui

using php_utility_belt exploit as a prelimenary entry point and ideal to further enter the system is exposed from the client side of the website even where session information can be dumped

I am not sure if I have the know how to craft a custom payload after analyzing wireshark packet capture data to further decode the packets moving through the session to place a payload as an open hole in the system for further use of a reverse shell

I dont know further details about the actual host that binance.us uses to serve its html for the website to properly setup a reverse shell from windows cmd or linux cmd or vice versa.

I also sent binance.com an email in 2019 before they migrated to binance.us
https://drive.google.com/file/d/1u8UhJQu6PmC-sgLGkohe4hHUPMRTTy1w/view

---EMAIL--- 2019 July 21st

[Binance] 回复： major hole in http cgi modules, any kind of reward?

harley0027@gmail.com

Jul 19, 11:48 CST

there is a major hole in binance.com via the old style structure of the site's running http cgi modules, allowing for a reverse shell session with the possibility to wrap a reverse tcp shell for higher level escalation and subversive permissions deeper into binance's filesystem and other current running systems attached to the windows server host , hosting binance,

simple suggestion set up an IDS snort or suricata as an intermediary between the web server running on ports 80 and 443 and the incoming connections to port 80, 443

binance.com -> snort IDS <- incoming connections to 80,443

seperate snort's false positives for http / https, but allow regular http / https traffic,

the bug is apparent in httpd_mod_cgi (bash exec)

as you can see from my screen recording via pentesting

https://drive.google.com/file/d/1u8UhJQu6PmC-sgLGkohe4hHUPMRTTy1w/view

HTTP request
Empty

Extra info
Binance should consider setting up an IDS such as snort or suricata to protect the website further they offer command line solutions compared to gui only deployments

me personally I run pfsense + clamAV scanning for active viruses recently discovering some infected websites with XORED PUA virus which is also setup with snort on max-detect, legacy, and blocking

I have a working template of pfsense with some basic default protection but it is mostly gui and not just a snort IDS command line setup

https://drive.google.com/file/d/1cL7XMvpDy1qgqzoPSkRRZEF-ICNoXRD8/view?usp=sharing

the best bet would be to run snort or suricata as a command line solution (i've never used suricata but they are interchangable pretty much)

running an IDS can stop port scans and Emerging threats such as nginx and apache2 attempts as they are added to free based and paid based subscriber rulesets to protect a home or business user's IP from active threats that roam the internet unattended or directly target computers such as individual or small hacking groups

Files attached

- binance-php-session-injection1.png (75.7 KB)
- binance-php-session-injection2.png (56.5 KB)
- binance-php-session-injection.mp4 (5.16 MB)
- binance-php-session-injection.gif (16.4 MB)

Activity

c4pt000 created the submission
02 Apr 2021 16:11:52 EDT

c4pt000 sent a message
02 Apr 2021 17:43:51 EDT

Email 2019-July-20th

[Binance] 回复： major hole in http cgi modules, any kind of reward?
Inbox

Binance support@binance.zendesk.com
Jul 19, 2019, 12:03 AM
to me

- Please type your reply above this line -

Your request (1842652) has been updated. To add another comment, please reply to this email.

CS Hank (Binance)

Jul 19, 12:03 CST

Hi there,

We're following up to confirm that we have received your message.

Rest assured that we will review your case and reach back out to you as soon as possible.

In the meantime, please let us know if you have any additional concerns.

Your patience and continued support is greatly appreciated.

Kind regards,
Binance Support Team

harley0027@gmail.com

Jul 19, 11:48 CST

there is a major hole in binance.com via the old style structure of the site's running http cgi modules,
allowing for a reverse shell session with the possibility to wrap a reverse tcp shell for higher level escalation and subversive permissions deeper into binance's filesystem and other current running systems attached to the windows server host , hosting binance,

simple suggestion set up an IDS snort or suricata as an intermediary between the web server running on ports 80 and 443 and the incoming connections to port 80, 443

binance.com -> snort IDS <- incoming connections to 80,443

seperate snort's false positives for http / https, but allow regular http / https traffic,

the bug is apparent in httpd_mod_cgi (bash exec)

as you can see from my screen recording via pentesting

https://drive.google.com/file/d/1u8UhJQu6PmC-sgLGkohe4hHUPMRTTy1w/view

This email is a service from Binance. Delivered by Zendesk
[93O96X-MMYE]
Attachments area

Binance support@binance.zendesk.com
Jul 19, 2019, 12:08 AM
to me

- Please type your reply above this line -

Your request (1842652) has been updated. To add another comment, please reply to this email.

CS star (Binance)

Jul 19, 12:08 CST

Dear user,

Thanks for reaching out.

Thank you for your feedback and comments, we will send your comments and feedback to the technical department. If you have any other questions, please contact us, thank you for your cooperation.

Thank you for your understanding.

Best Regards,
Binance Support Team

CS Hank (Binance)

Jul 19, 12:03 CST

Hi there,

We're following up to confirm that we have received your message.

Rest assured that we will review your case and reach back out to you as soon as possible.

In the meantime, please let us know if you have any additional concerns.

Your patience and continued support is greatly appreciated.

Kind regards,
Binance Support Team

harley0027@gmail.com

Jul 19, 11:48 CST

there is a major hole in binance.com via the old style structure of the site's running http cgi modules,
allowing for a reverse shell session with the possibility to wrap a reverse tcp shell for higher level escalation and subversive permissions deeper into binance's filesystem and other current running systems attached to the windows server host , hosting binance,

simple suggestion set up an IDS snort or suricata as an intermediary between the web server running on ports 80 and 443 and the incoming connections to port 80, 443

binance.com -> snort IDS <- incoming connections to 80,443

seperate snort's false positives for http / https, but allow regular http / https traffic,

the bug is apparent in httpd_mod_cgi (bash exec)

as you can see from my screen recording via pentesting

https://drive.google.com/file/d/1u8UhJQu6PmC-sgLGkohe4hHUPMRTTy1w/view

Jul 20, 2019, 12:28 AM
to Binance

threw vulnerabilities in nginx modules

Sent from my iPhone

On Jul 19, 2019, at 12:08 AM, Binance support@binance.zendesk.com wrote:

- Please type your reply above this line -

Your request (1842652) has been updated. To add another comment, please reply to this email.

CS star (Binance)

Jul 19, 12:08 CST

Dear user,

Thanks for reaching out.

Thank you for your feedback and comments, we will send your comments and feedback to the technical department. If you have any other questions, please contact us, thank you for your cooperation.

Thank you for your understanding.

Best Regards,
Binance Support Team
CS Hank (Binance)

Jul 19, 12:03 CST

Hi there,

We're following up to confirm that we have received your message.

Rest assured that we will review your case and reach back out to you as soon as possible.

In the meantime, please let us know if you have any additional concerns.

Your patience and continued support is greatly appreciated.

Kind regards,
Binance Support Team

harley0027@gmail.com

Jul 19, 11:48 CST

there is a major hole in binance.com via the old style structure of the site's running http cgi modules,
allowing for a reverse shell session with the possibility to wrap a reverse tcp shell for higher level escalation and subversive permissions deeper into binance's filesystem and other current running systems attached to the windows server host , hosting binance,

simple suggestion set up an IDS snort or suricata as an intermediary between the web server running on ports 80 and 443 and the incoming connections to port 80, 443

binance.com -> snort IDS <- incoming connections to 80,443

seperate snort's false positives for http / https, but allow regular http / https traffic,

the bug is apparent in httpd_mod_cgi (bash exec)

as you can see from my screen recording via pentesting

https://drive.google.com/file/d/1u8UhJQu6PmC-sgLGkohe4hHUPMRTTy1w/view

This email is a service from Binance. Delivered by Zendesk
[93O96X-MMYE]

Jul 20, 2019, 12:30 AM
to Binance

https://github.com/c4pt000/bitcoin-lost-deep-key-private-key/blob/master/README.md

^ some of the stuff i work on

Sent from my iPhone

On Jul 19, 2019, at 12:08 AM, Binance support@binance.zendesk.com wrote:

- Please type your reply above this line -

Your request (1842652) has been updated. To add another comment, please reply to this email.

CS star (Binance)

Jul 19, 12:08 CST

Dear user,

Thanks for reaching out.

Thank you for your feedback and comments, we will send your comments and feedback to the technical department. If you have any other questions, please contact us, thank you for your cooperation.

Thank you for your understanding.

Best Regards,
Binance Support Team
CS Hank (Binance)

Jul 19, 12:03 CST

Hi there,

We're following up to confirm that we have received your message.

Rest assured that we will review your case and reach back out to you as soon as possible.

In the meantime, please let us know if you have any additional concerns.

Your patience and continued support is greatly appreciated.

Kind regards,
Binance Support Team

harley0027@gmail.com

Jul 19, 11:48 CST

there is a major hole in binance.com via the old style structure of the site's running http cgi modules,
allowing for a reverse shell session with the possibility to wrap a reverse tcp shell for higher level escalation and subversive permissions deeper into binance's filesystem and other current running systems attached to the windows server host , hosting binance,

simple suggestion set up an IDS snort or suricata as an intermediary between the web server running on ports 80 and 443 and the incoming connections to port 80, 443

binance.com -> snort IDS <- incoming connections to 80,443

seperate snort's false positives for http / https, but allow regular http / https traffic,

the bug is apparent in httpd_mod_cgi (bash exec)

as you can see from my screen recording via pentesting

https://drive.google.com/file/d/1u8UhJQu6PmC-sgLGkohe4hHUPMRTTy1w/view

This email is a service from Binance. Delivered by Zendesk
[93O96X-MMYE]

Binance support@binance.zendesk.com
Jul 21, 2019, 6:08 AM
to me

- Please type your reply above this line -

Your request (1842652) has been updated. To add another comment, please reply to this email.

CS Harper (Binance)

Jul 21, 18:08 CST

Dear user,

Thanks for your inquiry.

We would appreciate it if you would write an e-mail to "product@binance.com" and outlining your feature request. Please be as detailed as possible. If your proposal is adopted, you will see the updates on the Binance platform in the near future.

Thanks for your support and understanding.

Best Regards,
Binance support team

harley0027@gmail.com

Jul 20, 12:33 CST

https://github.com/c4pt000/bitcoin-lost-deep-key-private-key

Sent from my iPhone

harley0027@gmail.com

Jul 20, 12:30 CST

https://github.com/c4pt000/bitcoin-lost-deep-key-private-key/blob/master/README.md

^ some of the stuff i work on

Sent from my iPhone

harley0027@gmail.com

Jul 20, 12:28 CST

threw vulnerabilities in nginx modules

Sent from my iPhone

CS star (Binance)

Jul 19, 12:08 CST

Dear user,

Thanks for reaching out.

Thank you for your feedback and comments, we will send your comments and feedback to the technical department. If you have any other questions, please contact us, thank you for your cooperation.

Thank you for your understanding.

Best Regards,
Binance Support Team

CS Hank (Binance)

Jul 19, 12:03 CST

Hi there,

We're following up to confirm that we have received your message.

Rest assured that we will review your case and reach back out to you as soon as possible.

In the meantime, please let us know if you have any additional concerns.

Your patience and continued support is greatly appreciated.

Kind regards,
Binance Support Team

harley0027@gmail.com

Jul 19, 11:48 CST

there is a major hole in binance.com via the old style structure of the site's running http cgi modules,
allowing for a reverse shell session with the possibility to wrap a reverse tcp shell for higher level escalation and subversive permissions deeper into binance's filesystem and other current running systems attached to the windows server host , hosting binance,

simple suggestion set up an IDS snort or suricata as an intermediary between the web server running on ports 80 and 443 and the incoming connections to port 80, 443

binance.com -> snort IDS <- incoming connections to 80,443

seperate snort's false positives for http / https, but allow regular http / https traffic,

the bug is apparent in httpd_mod_cgi (bash exec)

as you can see from my screen recording via pentesting

https://drive.google.com/file/d/1u8UhJQu6PmC-sgLGkohe4hHUPMRTTy1w/view

Gmail - [Binance] 回复： major hole in http cgi modules, any kind of reward_.pdf (124 KB)

BNB_Security sent a message
02 Apr 2021 22:12:56 EDT

99.84.47.81 is a Amazon Cloudfront IP address, which is owned and controlled by Amazon.

BNB_Security changed the state to **Not applicable**
02 Apr 2021 22:12:59 EDT

Send a message

Write
Preview

To Everyone

Your message to everyone here…

Embed images by dragging & dropping, **selecting**, or pasting them.

Add attachments

You can attach multiple files (up to 20). Please keep individual upload size under 400MB.

You can embed attachments (.jpg/.gif/.png, smaller than 2MB) into the Markdown fields. You can copy the embed code using the 'Copy as Markdown' button.

Send message