Stored XSS in BigBlueButton

Pentests.nl has discovered a vulnerability in BigBlueButton (version 2.4.7 and prior) which could be exploited to perform stored Cross-Site Scripting (XSS) attacks by sending private messages to users.

About BigBlueButton

BigBlueButton is an open source web conferencing system designed for online meetings and online learning. BigBlueButton is a tool used by instructors and teachers, which helps them access to Learning Management Systems, engagement tools and analytics.

Overview

The XSS vulnerability can be triggered by joining a room with a XSS payload as username and send a private message to a user.

Impact

A successful exploit allows attackers to inject malicious JavaScript code. Doing this could lead to multiple exploitation scenarios using XSS in BigBlueButton, including adding an administrator account.

CVSS score: *7.2 High*
CVSS string: *3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N*

Remediation

Update BigBlueButton to version 2.48 or 2.5.

Disclosure timeline

24-03-2022 – Bug discovered, initial report to BigBlueButton team
01-04-2022 – A reminder sent
03-04-2022 – Vulnerability acknowledgement by BigBlueButton
09-06-2022 – Private patch was released and pentests.nl verified the patch
09-06-2022 – Public patch was released for versions 2.4 and 2.5 from BigBlueButton
22-06-2022 – Full disclosure

References

https://github.com/bigbluebutton/bigbluebutton/releases/tag/v2.4.8
https://github.com/bigbluebutton/bigbluebutton/releases/tag/v2.5.0
https://github.com/bigbluebutton/bigbluebutton/security/advisories/GHSA-hwv2-5pf5-hr87

Hoe kunnen wij u helpen?

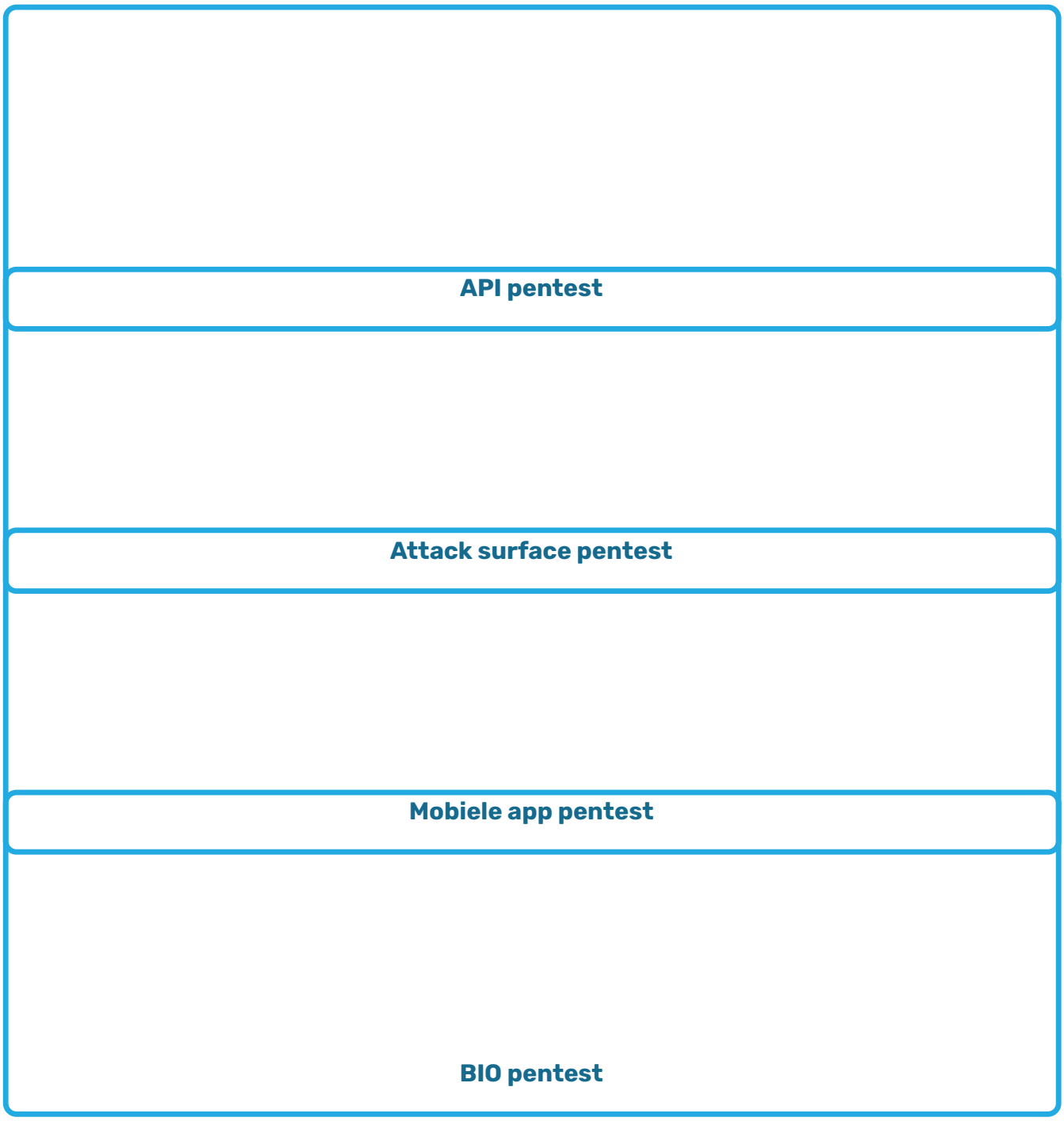
CONTACT

Waarom pentests.nl?

Webapplicatie pentest

Bedrijfsnetwerk pentest

DigiD pentest



Responder: toegang krijgen tot een netwerk

Een van de allereerste stappen die we ondernemen tijdens een bedrijfsnetwerk pentest is het aanzetten van de tool Responder. Dit is een tool die luistert en antwoordt op broadcast verkeer binnen

Content Security Policy (CSP): Maak je website veiliger

In deze blogpost lees je het hoe en waarom van de Content Security Policy (CSP). Met deze HTTP security header kan je de webbrowser van gebruikers fijnmazige instructies geven die bescherming bieden tegen hackaanvallen.

het subnet, met als doel het verkrijgen van NTLM hashes van gebruikers.

Win een phishing simulatie

Pentests.nl bestaat vandaag precies 100 dagen en wie jarig is trakteert. Daarom geven we drie gratis phishing simulaties weg! Laat een bericht achter via LinkedIn of onze contactpagina, dan ontvangt u van ons een lotnummer. Volgende week dinsdag zullen we de winnende lotnummers bekendmaken.

Pentests

+31 85 050 8055

contact@pentests.nl

KVK: 85690449

BTW: NL863708377B01

Pentest

- Webapplicaties
- Bedrijfsnetwerk
- DigiD Pentest
- BIO Pentest
- Ransomware Pentest

Overig

- Pentest Uitvoeren
- Pentest Begrippen
- Pentest Blog
- Penetratietest
- Pentest Bedrijven

Publicaties

- Responder: toegang krijgen tot een netwerk
- Content Security Policy (CSP): Maak je website veiliger
- Win een phishing simulatie

Pentests is onderdeel van Hackify BV en helpt organisaties weerbaar te worden tegen cyberaanvallen.