Sri Lanka Institute of Information Technology

IE2062

Web Security

Bug Bounty Report III

Submitted by:

Student Registration Number	Student Name
IT21197550	Nihila Premakanthan

Date of Submission: 28.05.2023

Acknowledgement

I would like to express my special thanks to our mentor Ms. Chethana Liyanapathirana and Dr. Lakmal Rupansighe for their time and efforts she provided throughout the course, and for the Web Security lecture panel for guiding us through this semester and for helping us by giving examples, guidelines, and advice about the project. Your useful advice and suggestions were really helpful to me during the project's completion. In this aspect, I am eternally grateful to you.

Executive Summary

This report aims to provide an overview of the vulnerability identified in a particular domain. The bug bounty platform called Hackerone was used for this purpose.

This report uses different tools to gather information detect vulnerabilities and perform penetration testing. The tool name Netsparker and Owasp Zap was mainly used to identify the vulnerability. Further this report provides the vulnerability title, vulnerability description, Affected Components, Impact Assessment, Steps to reproduce the vulnerability, proof of concept and the proposed mitigation.

By including these comprehensive details for each vulnerability, the report provides a comprehensive overview of the security weaknesses present within the system and offers actionable insights for remediation and improvement.

Contents

Vulnerability Title

Breach Attack Detected

Severity Level

Vulnerability Description

It is challenging to identify security problems and efficiently respond to them when there is insufficient logging and monitoring. Without thorough records and adequate monitoring, firms risk missing attempts at unauthorized access, malicious activity, or warning signals of a security breach.

Affected Components

Different systems and infrastructure parts of a business may be impacted during a breach attack. Here are several elements that are frequently targeted:

- User Accounts: By exploiting weak passwords, carrying out credential stuffing attacks, or utilizing social engineering strategies, attackers frequently try to compromise user accounts. Compromised user accounts can provide hackers access to private information or let them behave maliciously on behalf of real users.
- Databases: Targeted databases frequently contain important data, such consumer information, financial records, or intellectual property. Unauthorized data extraction, modification, or deletion due to database breaches can cause considerable harm and result in data breaches.
- Apps and Web Servers: Breach attempts usually take advantage of holes in web servers, apps, or the frameworks that support them. Attackers may try to obtain access without authorization, insert malicious code, or take advantage of flaws like remote code execution, SQL injection, or cross-site scripting (XSS).
- Network Infrastructure: To gain unauthorized access, intercept network traffic, or launch additional assaults within the network, attackers may target network infrastructure elements like routers,

switches, or firewalls. A compromised network infrastructure might allow lateral movement within the organization's network or give unauthorized access to critical data.

- Operating Systems: Operating system flaws can give attackers a point of entry. Attackers are able to install malware, elevate privileges, get unauthorized access, and more by taking advantage of these vulnerabilities on infected systems.
- Endpoints and Devices: In a breach attack, a single endpoint—such as a workstation, a laptop, or a mobile device—is frequently compromised. Attackers can take control of these devices and obtain sensitive data by taking advantage of flaws, tricking users into installing malware, or using social engineering strategies.

Impact Assessment

Depending on the assault's nature, the target system or network, and the exact vulnerabilities exploited, the effect estimate of a breach attack might differ dramatically. However, the following common effects of a breach attack are listed:

- Data Exposure: One of the main issues with a breach attack is the disclosure of private or sensitive information. This can apply to any sensitive data that is kept or processed by the targeted system, including personally identifiable information (PII), financial information, intellectual property, and others. The effects might range from seriously harming an organization's finances and reputation to jeopardizing people's privacy.
- Financial Loss: Attacks on breaches may cause large financial losses. Costs for incident response, forensic investigations, legal fees, customer notifications, credit monitoring services for impacted persons, and potential fines or penalties may be incurred by organizations. In addition, breaches may result in a loss of customers' trust, business, and potential legal action.
- Reputational Damage: Breaches can harm an organization's reputation for a very long time. A breach's public exposure could reduce customer trust, turn off new customers, and damage the brand's reputation as a whole. Rebuilding reputation and trust can be a difficult and time-consuming task.
- Operational Disruption: Attacks that compromise security can stop a company's regular business activities, leading to system outages, service disruptions, and lost productivity. To address the

breach, repair systems, and tighten security measures, organizations may need to devote a sizable amount of resources, which would incur additional costs and perhaps cause delays in ongoing projects or services.

- Legal and Compliance Obligations: Following a breach, corporations may be required by law to notify relevant authorities, regulatory agencies, and affected parties. Additional legal repercussions as well as reputational damage may result from failure to adhere to these commitments.

Steps to Reproduce

To minimize the harm and stop further compromise, it is essential to act immediately and efficiently after a breach attack is discovered. The general procedures to follow while reacting to a breach attack are as follows:

- Determine and validate the breach: Examine the available information and indicators of compromise (IoCs) to confirm that a breach has in fact taken place. This could entail keeping an eye on network logs, going over system alarms, or running a forensic investigation.
- Assemble a team for crisis response: Form a multidisciplinary team of experts, including IT security experts, system administrators, attorneys, and key stakeholders. Coordination of the breach response efforts will fall under the purview of this team.
- Determine the breadth: Isolate the afflicted systems from the rest of the network after determining its scope. This process aids in containing the attack and stops malware from spreading or illegal access.
- Save evidence: Save any digital records that may have been compromised. System logs, network traffic information, and any other pertinent artifacts are included in this. This information will be crucial for comprehending the attack, evaluating its effects, and maybe taking legal action.
- Notify the proper parties: Notifying different parties can be required, depending on the violation's nature and the rules that apply. Law enforcement organizations, regulatory organizations, impacted clients or consumers, and any other pertinent stakeholders may fall under this category. To make sure that all legal obligations are being followed, legal advice should be engaged.

- Determine the size of the breach and the systems or data that were compromised when evaluating the effect. Analyze any possible harm or illegal access that may have taken place. This analysis will guide the formulation of a remediation plan and assist in prioritizing recovery activities.
- Remedy and contain: Create a strategy to address the breach and put the impacted systems back in a secure state. This can entail eradicating malware, fixing security holes, or reconstructing hacked systems. To stop similar assaults in the future, install more security safeguards and measures.
- Monitor and look into: Keep an eye out for any indications of further compromise or re-entry into the network and compromised systems. Conduct a thorough investigation to pinpoint the breach's underlying cause and comprehend the attack methods used. This knowledge will assist strengthen security procedures and stop upcoming hacks.

- Learn and get better: To evaluate the reaction efforts and pinpoint areas for improvement, do a post-incident evaluation. Adapt security guidelines, practices, and training courses in light of the breach's lessons learnt. Continually evaluate the organization's security posture and improve it.

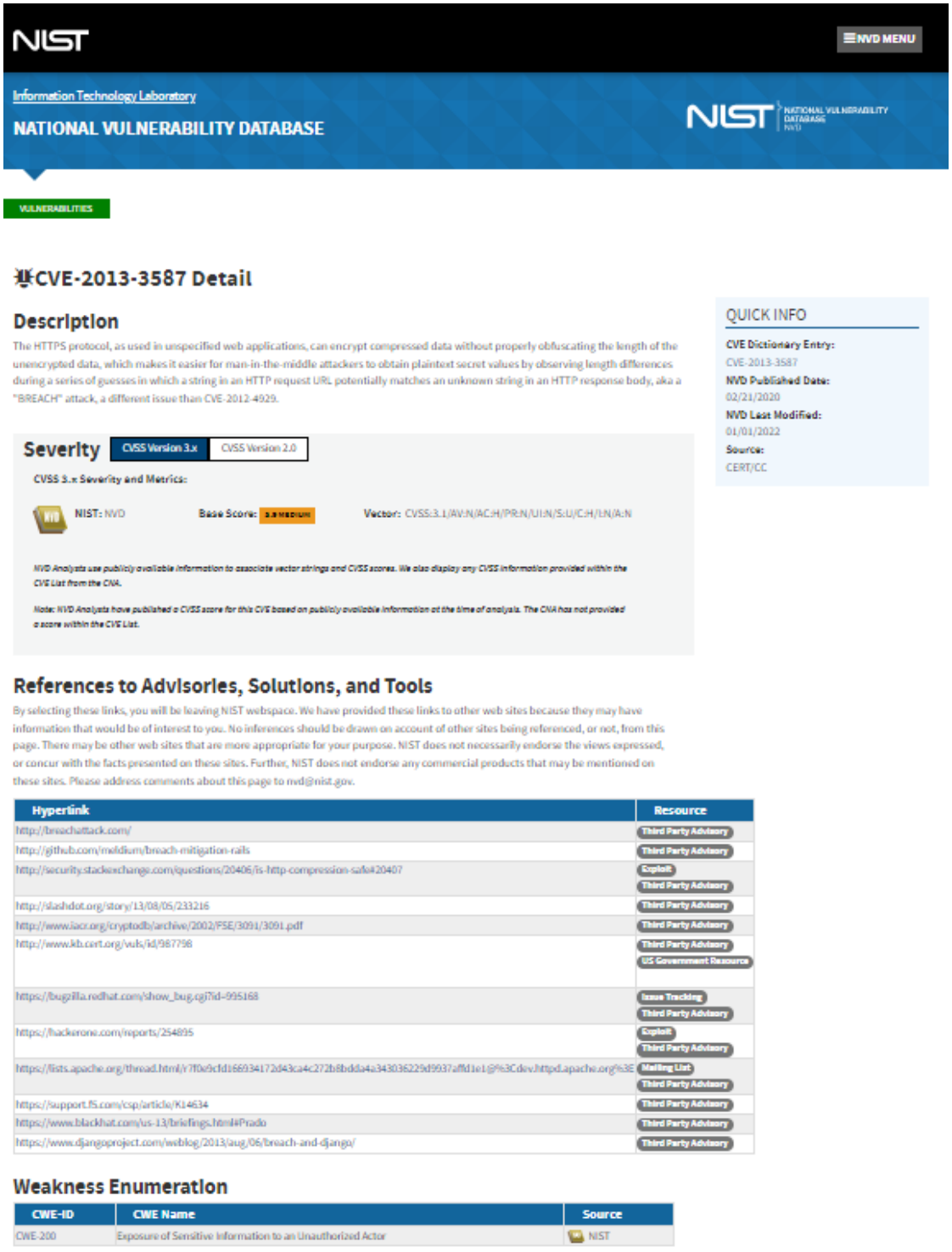
Proposed mitigation

Mitigating a breach attack entails acting quickly to reduce the harm done and stop further unauthorized access. To lessen a breach attack, take the following general precautions:

- Engage the incident response team to coordinate the mitigation activities by activating the team that was previously constituted. System administrators, IT security experts, and any other pertinent stakeholders ought to be on this team.
- Isolate the vulnerable systems from the network to stop the attacker from gaining more access or stealing data. By cutting off the afflicted systems, the attacker's capacity to move laterally is reduced, and their ability to inflict more damage is constrained.
- Change any compromised credentials, including passwords, access keys, and user accounts linked to the systems that were breached. To increase security, use multi-factor authentication and strong, one-time passwords.

- Patching vulnerabilities entails finding any holes or flaws that the attacker may have exploited. To address known vulnerabilities in your systems, keep up with vendor security patches and software updates.
- Remove malicious software and activity. Perform a thorough scan of the afflicted systems to find and eliminate any malware or malicious files. Utilize trustworthy antivirus and anti-malware tools to find and get rid of risks.
- Access controls should be reviewed and strengthened to make sure that only people with permission can access sensitive systems and data. Apply the concept of least privilege, which states that users should only be given the access they absolutely need to complete their duties.
- Put additional security measures in place. Implementing additional security measures will improve your organization's security stance. Network segmentation, firewalls, intrusion prevention systems (IPS), data loss prevention (DLP) tools, and security information and event management (SIEM) systems may all be included in this.
- Employers should be trained and made aware. Inform staff members about the breach situation and reiterate best security measures. Give instruction on spotting phishing emails, using secure passwords, and remaining alert to social engineering assaults.

External Reference



NIST

NVD MENU

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NIST NATIONAL VULNERABILITY DATABASE NVD

VULNERABILITIES

CVE-2013-3587 Detail

Description

The HTTPS protocol, as used in unspecified web applications, can encrypt compressed data without properly obfuscating the length of the unencrypted data, which makes it easier for man-in-the-middle attackers to obtain plaintext secret values by observing length differences during a series of guesses in which a string in an HTTP request URL potentially matches an unknown string in an HTTP response body, aka a "BREACH" attack, a different issue than CVE-2012-4929.

QUICK INFO

CVE Dictionary Entry:
CVE-2013-3587
NVD Published Date:
02/21/2020
NVD Last Modified:
01/01/2022
Source:
CERT/CC

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD Base Score: 5.9 MEDIUM Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
http://breachattack.com/	Third Party Advisory
http://github.com/meldium/breach-mitigation-rails	Third Party Advisory
http://security.stackexchange.com/questions/20406/is-http-compression-safe#20407	Exploit Third Party Advisory
http://slashdot.org/story/13/08/05/233216	Third Party Advisory
http://www.iacr.org/cryptodb/archive/2002/FSE/3091/3091.pdf	Third Party Advisory
http://www.kb.cert.org/vuls/id/987798	Third Party Advisory US Government Resource
https://bugzilla.redhat.com/show_bug.cgi?id=995168	Issue Tracking Third Party Advisory
https://hackerone.com/reports/254895	Exploit Third Party Advisory
https://lists.apache.org/thread.html/r7f0x9cfd166934172d43ca4c272b8bdda4a343036229d9937affd1e1@%3Cdev.httpd.apache.org%3E	Mailing List Third Party Advisory
https://support.f5.com/csp/article/K14634	Third Party Advisory
https://www.blackhat.com/us-13/briefings.html#Prado	Third Party Advisory
https://www.djangoproject.com/weblog/2013/aug/06/breach-and-django/	Third Party Advisory

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor	NIST