18CSE383T

Assignment -1
Topic: Vulnerability analysis and a case study on OTT platforms
Team:
RA1911030010005
RA1911030010019
RA1911030010027

(i) Need for Cyber Security:

The Relevance of Cybersecurity for OTT Platforms

The popularity of OTT platforms has skyrocketed due to the COVID-19 pandemic. As consumers retreated indoors to stay safe from the novel coronavirus, they turned to Netflix, Disney+, Hulu, and other streaming services.

The downside to this phenomenon is that streaming media services have now caught the attention of cybercriminals. For example, in March 2021, ZEE5 – one of India's leading OTT platforms – was embroiled in a data breach. The breach exposed the personal information of 9 million users, including their names, email addresses, and phone numbers.

What Makes OTT Platforms Vulnerable to Cyberattacks?

To begin with, users don't treat their OTT login credentials with the same gravity as their online banking details and other sensitive information. They often log into multiple devices and even use the same password to sign-up for different video streaming services.

Many users also share their login credentials with their friends, coworkers, and family members. That makes it easier for cybercriminals to hack into their accounts using various bots and brute force attacks. OTT platform users are also prone to fall prey to phishing attacks.

The Importance of Cybersecurity for OTT Service Providers

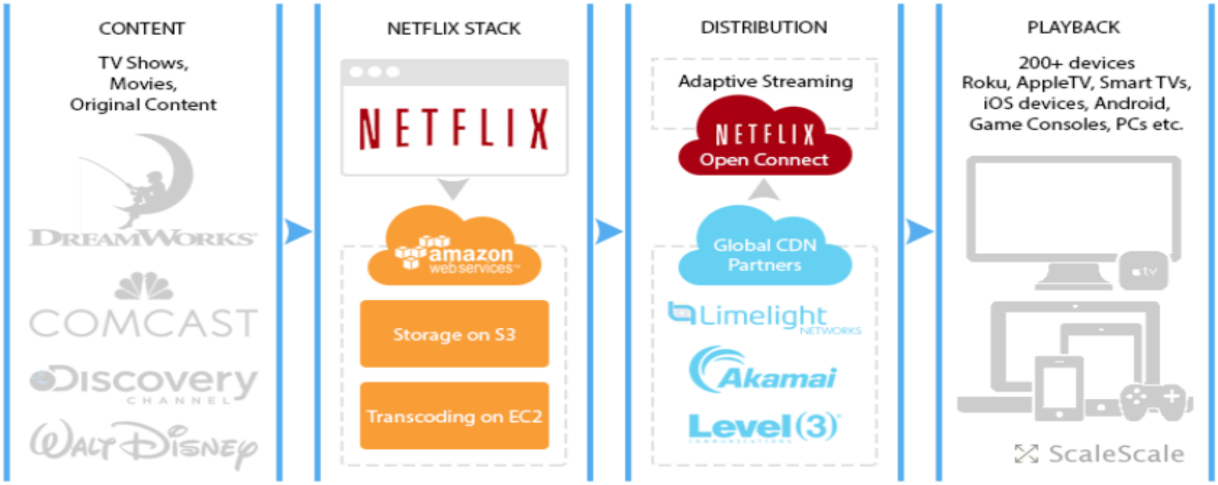
Any cyberattack that results in a data breach could expose sensitive information, including your customers' credit card numbers and bank details. Cybercriminals could also access and manipulate your app's source code to collect user data and sell it on the dark web.

Similarly, tampering of SO files and reverse-engineering attacks can result in further loss of revenue. Hackers could even leak premium content online or sell it at a discounted price. That's why it has become imperative for today's streaming service providers to implement suitable cybersecurity protocols to safeguard user data and revenue.

(ii) Maintain Information and databases:

- They're essentially made up of a combination of hard drives crammed together in a server.
- Most OTT services combine live and on-demand content, especially broadcaster OTT services that incorporate linear channels, live programming, and VOD libraries
- The company uses a content delivery network (CDN), a global network of storage servers that cache content close to where it will be viewed. That local caching reduces bandwidth costs and makes it easier to scale the service over a wide area.
- If a CDN is compromised or damaged by a DDoS attack, content that relies on that CDN can be taken out to deliver content. Having a CMP(Cloud Management Platform) for the surveillance reduces the risk; by making you follow all the security best practices and alarm you for any suspicious activity.
- Netflix has about a thousand of these spread across the globe. Each one collects content to then be transmitted to various devices.
- Live-only | CDN storage | Central storage | VOD-only | small VOD library | Large VOD library

- Databases: | Netflix Media Database (NMDB) | Netflix uses DynamoDB and Cassandra | Mysql



(iii) Prioritise risk and frame policies:

Risk management (prioritizing risks)

Risk	severity	Priority	Solution
1) authentication flaw	High	2	patch vulnerability
2)Lack of security measures	Medium	3	Mitigate risk
3)Internal Threat actors	Very High	1	Mitigate risk
4)Accessing premium content for free	High	2	Patch vulnerability
5)cache poisoning	High	2	Mitigate risk
6)Human error	Medium	3	Mitigate risk

7)Basic Technical glitches	Low	4	● Acceptable level risk ● Can be mitigated

Key-
Very High - extremely sure to occur
High - Likely to occur
Medium - An even chance to occur
Low - Not very likely to occur

(iv) Data to protect

1. User login credentials such as username and password
2. credit/debit/net banking details of a user such as account number, CVV, net banking ID and password
3. Classified company information such as employee info, customer information, acquisition plans etc..
4. Company's Business information such as financial plans , trade secrets etc..
5. Intellectual property which is basically anything that is under a NDA(non disclosure agreement) , which ranges from code , schematics to product specifications.

Security Policy

- Web application security assessments must be performed on the OTT web application to identify potential or realized weaknesses (e.g., insecure coding, inadvertent misconfiguration, weak authentication, insufficient error handling, sensitive information leakage) per the Vulnerability Management Policy.

- New or significant application releases are subject to the Software Development Life Cycle and Secure SDLC before the change control documentation or release into the live environment.
- unknown acquired web applications (i.e., commercial applications for which source code is not available) must be scanned when installed or upgraded.
- Shared accounts are prohibited, except where it is not technically possible to provision accounts individually.
- All Internet-facing OTT applications should deploy the ISO approved technical controls (e.g., Web Application Firewall (WAF) or Intrusion detection and prevention System (IDS and IPS)).
- To avoid insider threats frequent internal audits should be performed.
- Other security controls include: (but are not limited to the following:)

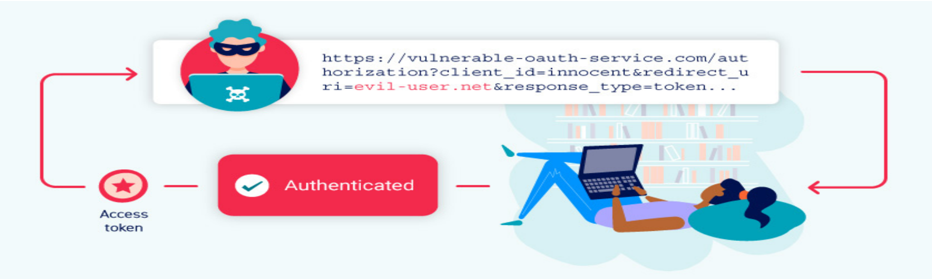
1. Access controls,
2. Configuration changes (you must submit non-agreed upon configuration changes to the ISO for review),
3. Authentication (multi-factor authentication must be used except where it is not technically possible),
4. Data protection (e.g., encryption, data masking),
5. Error handling and logging,
6. Input and output handling, and
7. Session management

- Policy Violation

Violation of any of the above mentioned policies may lead to suspension or Termination based on severity .

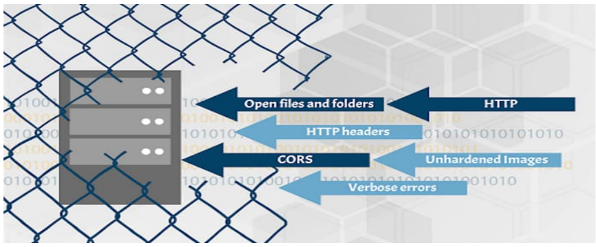
(v) List threats and vulnerabilities:

- Authentication and Authorization flaws


https://vulnerable-oauth-service.com/authorization?client_id=innocent&redirect_uri=evil-user.net&response_type=token...
Authenticated
Access token

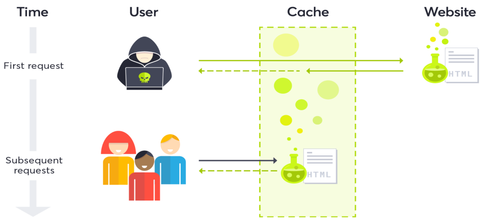
- Insufficient session expiration

- OWASP top 10 - 2017
- Security misconfiguration

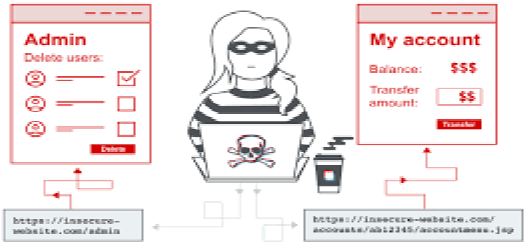


- Insecure design
- Failure of secure logging and monitoring

- Data Integrity failures
- Web Cache poisoning



- Rate limiting issues
- Access control issues


Admin
Delete users:
Delete
My account
Balance:
$$$
Transfer amount:
$$
Transfer
https://insecure-website.com/admin
https://insecure-website.com/accounts/abc12345/accountmess.jsp

- Cryptographic failures

And checking out and patching vulnerabilities listed in OWASP top 10 is a good practice.

(vi) Remedial actions and preventions:

---Remedial actions for the Company---

1. Ensure that user registration, especially self-registration on web applications, forces users to create a strong password. The riskier the data, the more complex the password should be.
2. Encourage users (and application architects) to use long passphrases instead of hard-to-remember mixes of upper, lower, numerical, special character, 8-character-long passwords.
3. Always change default credentials and disable unnecessary accounts *before* a system is deployed.
4. Employ secondary mechanisms for forgotten password retrieval to ensure that only the legitimate users can request a reset.

5. Always send passwords securely to prevent interception in transit. And be sure to avoid sending usernames and passwords in the same delivery.
6. Prevent methods for “workarounds.” For example, if there is no minimum password age, someone could indefinitely keep the same password even if it expires by simply changing it as many times as necessary…until the “remember previous password” threshold is exceeded, allowing it to be changed back to the original password by the user.
7. Consider implementing Single Sign On (SSO) with a known, high-reputation system or partner. SSO can significantly reduce end-users’ burden of managing, remembering, and changing multiple passwords. Remember, your end-users are often your weakest vulnerability. Making things easy for them reduces your risk and theirs.
8. Two-factor authentication, which introduces a second (or third) element to the authentication process, is highly effective at preventing unauthorized access as an attacker would need more than just a user’s password to impersonate them.

- **https://www.whitehatsec.com/glossary/content/insufficient-session-expiration**
- **https://www.manageengine.com/vulnerability-management/misconfiguration/**
- **https://www.vistainfosec.com/blog/what-is-insufficient-logging-monitoring-and-how-can-it-be-prevented/**
- **https://www.mastercontrol.com/gxp-lifeline/identifying-and-preventing-common-data-integrity-issues/**
- **https://portswigger.net/web-security/web-cache-poisoning**

---Prevention Measures for the Organization---

- **To prevent unauthorized access and to remain on the right side of data protection acts:**

1. OAuth Identification

2. End-to-end data encryption
3. Secure code
4. Multi-level authorization
5. 5.Compliance with regulatory standards

- A web application should invalidate a session after a predefined idle time has passed (a timeout) and provide users the means to invalidate their own sessions, (logout). These simple measures help to keep the lifespan of a session ID as short as possible. To protect against Insufficient Session Expiration attacks, the logout function should be prominently visible to the user, explicitly invalidate a user's session, and disallow reuse of the session token

- Prevent Security Misconfiguration

  The principle of least privilege: Everything off by default.

  - Disable administration interfaces.
  - Disable debugging.
  - Disable use of default accounts/passwords.
  - Configure server to prevent unauthorized access, directory listing, etc.
  - Consider running scans and doing audits periodically to help detect future misconfigurations or missing patches.

(vii) Sample reports from bug bounty platforms:

--Bypassing Hotstar OTP Verification--
https://medium.com/@amalthamban/how-i-bypassed-hotstar-otp-verification-a478e4951989

-- Insufficient session expiration in Hotstar--
Exploiting in real time

-- Bug reports

1. Hotstar
   https://www.openbugbounty.org/reports/159997/

2. Zee5
   https://www.openbugbounty.org/reports/753417/