OWASP TOP 10

Bhavin Raninga

This is a brief information about the OWASP Top 10 2021 along with their examples.

A01:2021 Broken Access control

This allows an attacker gain unauthorised access to restricted resources (Resources which are not open publically such as admin page, bank employees login, etc). By exploiting this vulnerability attacker can gave access to such systems or data.

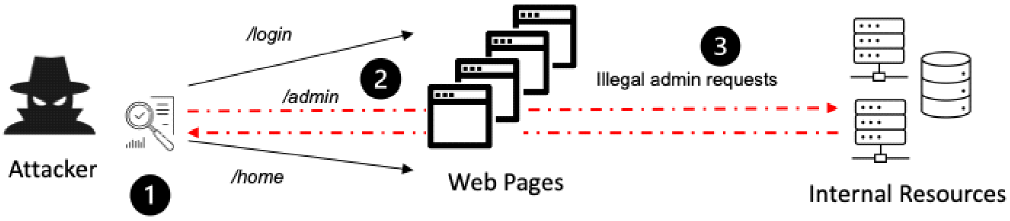


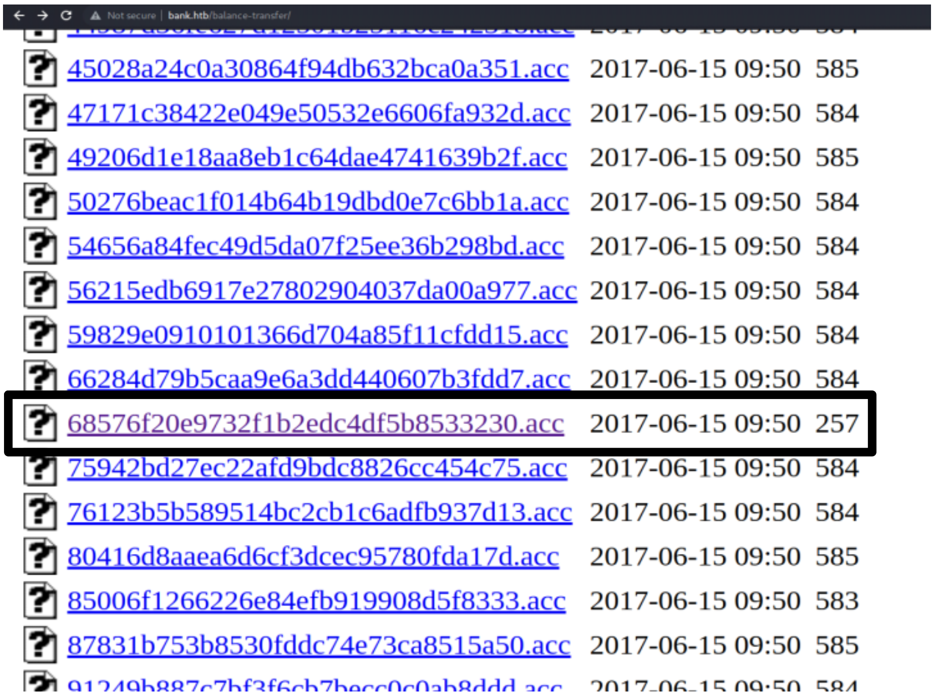
Fig. Broken access control

A02:2021 Cryptographic Failure

This means the attacker can gain access to confidential information such as passwords, card details, etc when not stored in secure format (i.e., either through encryption, hashing or various other encryption techniques).

For example if a user got a file directory (Domain.com/users) in the "users" all the users login data is stored and is a file was left unencrypted then attacker can access it.

In the below image you can see all the files with almost same size are encrypted but 1 file is not encrypted leading to cryptographic failure.



```
45028a24c0a30864f94db632bca0a351.acc  2017-06-15 09:50  585
47171c38422e049e50532e6606fa932d.acc  2017-06-15 09:50  584
49206d1e18aa8eb1c64dae4741639b2f.acc  2017-06-15 09:50  585
50276beac1f014b64b19dbd0e7c6bb1a.acc  2017-06-15 09:50  584
54656a84fec49d5da07f25ee36b298bd.acc  2017-06-15 09:50  584
56215edb6917e27802904037da00a977.acc  2017-06-15 09:50  584
59829e0910101366d704a85f11cfdd15.acc  2017-06-15 09:50  584
66284d79b5caa9e6a3dd440607b3fdd7.acc  2017-06-15 09:50  584
68576f20e9732f1b2edc4df5b8533230.acc  2017-06-15 09:50  257
75942bd27ec22afd9bdc8826cc454c75.acc  2017-06-15 09:50  584
76123b5b589514bc2cb1c6adfb937d13.acc  2017-06-15 09:50  584
80416d8aaea6d6cf3dcec95780fda17d.acc  2017-06-15 09:50  585
85006f1266226e84efb919908d5f8333.acc  2017-06-15 09:50  583
87831b753b8530fddc74e73ca8515a50.acc  2017-06-15 09:50  585
91249b887c7bf3f6cb7becc0c0ab8ddd.acc  2017-06-15 09:50  584
```

Fig. Cryptographic Failure

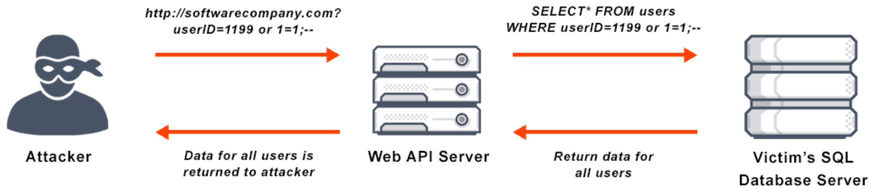
A03:2021 Injection

This flaw in very common in applications today. Here the user supplied input to passed directly to the server and server accepts and executes it as a command.

Here the user input is not sanitized and this help attacker to pass malicious command as an input to the application.

2 injection attacks are:

1. SQL injection
2. Command injection



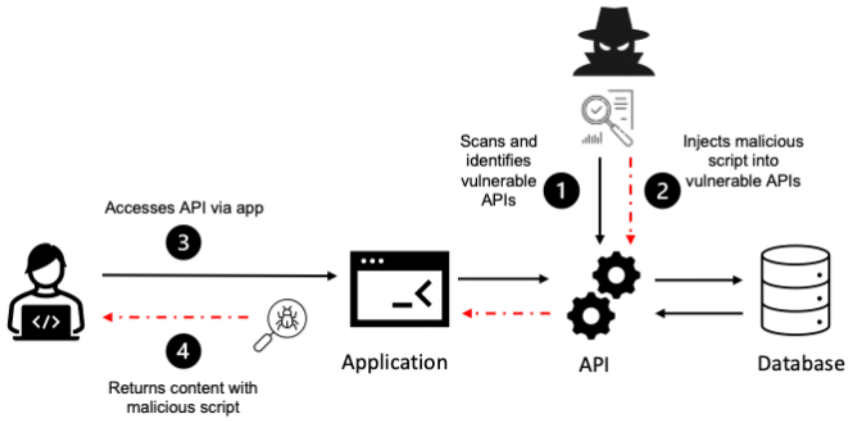
http://softwarecompany.com?userID=1199 or 1=1;--
SELECT* FROM users WHERE userID=1199 or 1=1;--
Attacker
Web API Server
Victim's SQL Database Server
Data for all users is returned to attacker
Return data for all users

Fig. Injection

A04:2021 Insecure Design

Insecure design means the lack of security controls implementation in the process of Software Development Life cycle (SDLC).

The application is designed and implemented in such a way that threats to the organizations data and system.



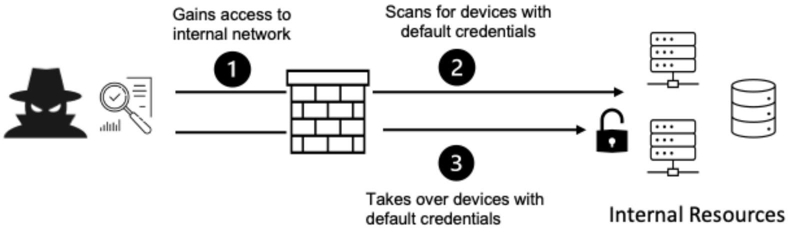
Scans and identifies vulnerable APIs
1
Injects malicious script into vulnerable APIs
2
Accesses API via app
3
4
Returns content with malicious script
Application
API
Database

Fig. Insecure Design

A05:2021 Security Misconfiguration

As the name suggests security misconfiguration is the security control which is implemented inaccurately or sometimes even left unsecure.

This could be anything from poor configuration, default settings, or improper endpoint security.



Gains access to internal network
1
Scans for devices with default credentials
2
3
Takes over devices with default credentials
Internal Resources

Fig. Security misconfiguration

A06:2021 Vulnerable and outdated components

The use of components or services which has been outdated or a publically know vulnerability exists and The outdated software are no longer supported by the developer is called vulnerable software and it has a publically available exploit which is very dangerous for the security of data.

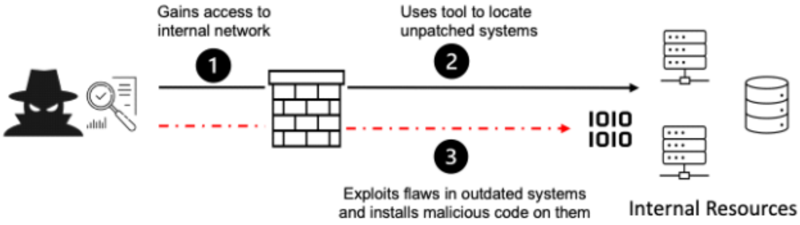

Gains access to internal network
1
Uses tool to locate unpatched systems
2
IOIO
IOIO
3
Exploits flaws in outdated systems and installs malicious code on them
Internal Resources

Fig. Vulnerable and outdated components

A07:2021 Identification and authorization failure

If an attacker is able to find flaws in an authentication mechanism, they would then successfully gain access to other users' accounts. This would allow the attacker to access sensitive data.
In this the identification and authorization mechanism of the system fails to identify whether the user is a legitimate user or an attacker.

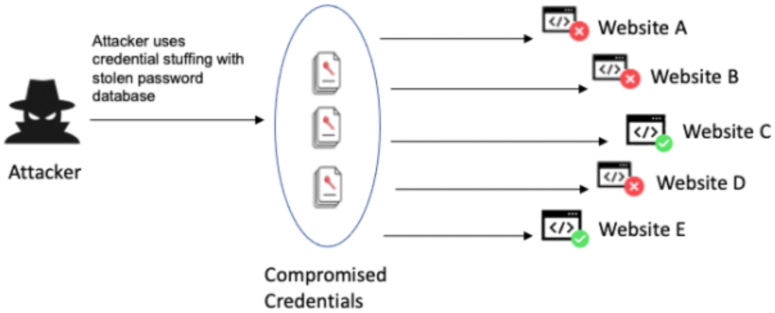


Fig. Identification and authorization failure

A08:2021 Software and data integrity failure

Software and data integrity failures frequently occur when the code implementation and the underlying infrastructure lack the ability to protect the code against all integrity violations.

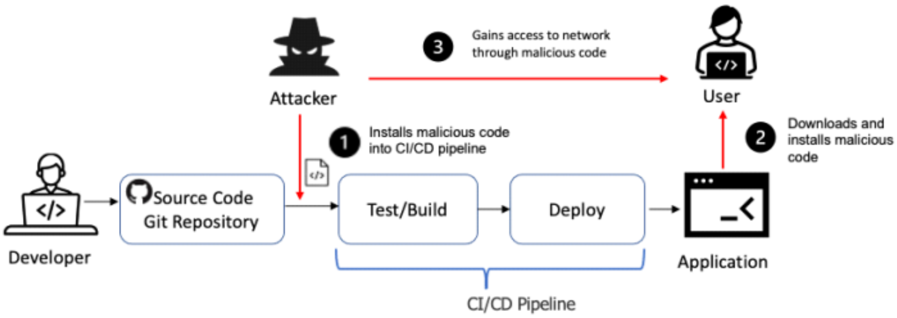

Attacker
3
Gains access to network through malicious code
User
1
Installs malicious code into CI/CD pipeline
2
Downloads and installs malicious code
Developer
Source Code
Git Repository
Test/Build
Deploy
Application
CI/CD Pipeline

Fig. Software and data integrity failure

A09:2021 Security logging and monitoring failure

This means your systems must log all the action performed whether it be from a known user or outsider so that it could be an early step to manage security risk as we can know about for example multiple login attempts could be identified and security measure could be taken. But the risk increases along with the security and monitoring failure.

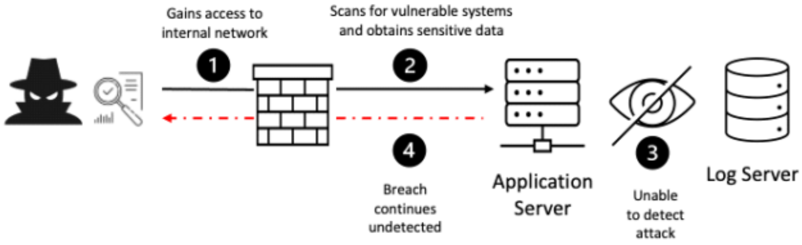

Gains access to internal network
1
Scans for vulnerable systems and obtains sensitive data
2
Application Server
3
Unable to detect attack
Log Server
4
Breach continues undetected

Fig. Security logging and monitoring failure

A10:2021 Server Side Request Forgery

In this attack the attacker can induce the server side application to make a request to an unintended user / location. This attack involves an attacker abusing server functionality and can modify or access the resources.

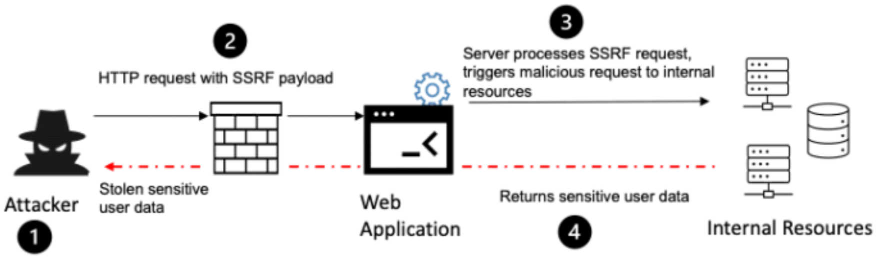

Attacker
1
2
HTTP request with SSRF payload
Stolen sensitive user data
Web Application
3
Server processes SSRF request, triggers malicious request to internal resources
Returns sensitive user data
4
Internal Resources

Fig. Server side Request Forgery