Application Level DoS Attacks

Akash Venky Jan 24 · 3 min read

What is Application-Level DoS?

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it **inaccessible** to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.

What are types of DOS attacks?

> *· flooding services*
>
> *· Rate limiting*

> *· Distributed Denial of Service Attacks (DDoS) …*
>
> *· Unintended Denial of Service Attacks.*

Buffer overflow attacks, ICMP flood, SYN flood, volume based attacks, rate limiting based attacks — the most common **DoS attack.**

What is DDOS attack?

A DDoS attack occurs when multiple systems orchestrate a synchronized DoS attack to a single target. The essential difference between DOS and DDOS is that instead of being attacked from one location, the target is attacked from many locations at once.

What is Rate limit in an application?

A rate limiting algorithm is used to check if the user session (or IP-address) has to be limited based on the information in the session cache. In case a client made too many requests within a given timeframe, HTTP-Servers can respond with status code 429: Too Many Requests.

How we can Perform a DOS attack to a target application?

1. Long String Based DoS attacks

· Try to input long password when registering an account in the input field

· Try to input long text in Address, Name, Username, etc.

· Try to input malicious DOS payload or commands like **Sleep, Timeout** etc in the input field

2. Picture Name Parameter

· Upload a picture with large value in the name parameter.

· Upload a picture with the DoS payload inside it.

· Insert various payload in the meta-data of the pic and upload.

3. Pixel Flood Attack

· Try to upload a picture with large resolution image

Eg: The exploit is really simple. An image of 5kb, 260x260 pixels. In the image itself we have to exchange the 260x260 values with 0xfafa x 0xfafa (so 64250x64250 pixels).

If the application is vulnerable then it will be loading the ‘whole image’ into memory, it tries to allocate 4128062500 pixels into memory, flooding the memory and causing DoS.

This also happens with Windows Photo Viewer on my computer. When you download the same exploit.

4.Rate Limiting resulting in DOS attacks.

A rate limiting algorithm is used to check if the user session (or IP-address) has to be limited based on the information in the session cache. Some of the real time examples where rate limiting vulnerabilities can be found

i. Password reset — Capture the request in burp and use intruder and repeat the request for 1000 times and check limiting

ii. Comments in blogs — Capture the request in burp and use intruder and repeat the request for 1000 times and check limiting

iii. Email Bombing — capture the request in burp and use intruder and repeat the request for 1000 times and check limiting

iv. Account creation activation request- capture the request in burp and use intruder and repeat the request for 1000 times and check limiting.

v. And many more……..

5. Application-Level DoS via XMLRPC in wordpress sites.

```
Eg: POST /xmlrpc.php HTTP/1.1
Host: vulnerable-website.com
Accept: /
Accept-Language: en
Connection: close
Content-Length: 93
<methodCall>
<methodName>system.listMethods</methodName>
<params></params>
</methodCall>
```

2. Use the “pingback” methods to cause a DDOS attack against victim host

```
Eg: POST /xmlrpc.php HTTP/1.1
Host: vulnerable-website.com
Accept: /
Accept-Language: en
Connection: close
Content-Length: 93
<methodCall>
<methodName>pingback.ping</methodName>
```

```
<value><string>http://yourip:port</string></value>

</param><param>

<value>

<string>https://target.com></string>

</value>

</param></params>

</methodCall>
```

Best Mitigation methods in order to Prevent DOS/DDOS attacks

· Implement IDS/IPS to network in order to identify the occurring attacks

· Increase Network bandwidth

· Manage and block malicious traffic

· Implement captcha services, JS tests, Cookie challenges etc.

· Implement DOS/DDOS attacks preventing Tools or software's.

· Consult me Akash.venky091@gmail.com for more mitigations.

Any suggestions are most welcomed write a mail to Akash.venky091@gmail.com

or contact me @ https://www.linkedin.com/in/akash-h-c-4a4090a7/

Bug Bounty Dos Attack Vapt Hacking Pentesting

Get the Medium app

Download on the App Store

GET IT ON Google Play