## Risk Assessment – Dread

# Omer Lev-Ron, Tal Hagag, Tal Nitzan and Daniel Shaal

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| High (3) | Medium (2) | Low (1) | Rating |  |
| The attacker can subvert the security system; get full trust authorization; run as administrator; upload content. | Leaking sensitive information | Leaking trivial information | Damage potential | D |
| The attack can be reproduced every time and does not require a timing window. | The attack can be reproduced, but only with a timing window and a particular race situation. | The attack is very difficult to reproduce, even with knowledge of the security hole. | Reproducibility | R |
| A novice programmer could make the attack in a short time. | A skilled programmer could make the attack, then repeat the steps. | The attack requires an extremely skilled person and in-depth knowledge every time to exploit. | Exploitability | E |
| All users, default configuration, key customers | Some users, non-default configuration | Very small percentage of users, obscure feature; affects anonymous users | Affected users | A |
| Published information explains the attack. The vulnerability is found in the most commonly used feature and is very noticeable. | The vulnerability is in a seldom-used part of the product, and only a few users should come across it. It would take some thinking to see malicious use. | The bug is obscure, and it is unlikely that users will work out damage potential. | Discoverability | D |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Threat | D | R | E | A | D | Total | Rating |
| Attacker obtains authentication credentials by monitoring the network. | 2 | 3 | 2 | 1 | 2 | 10 | High |
| SQL commands injected into application. | 3 | 3 | 3 | 3 | 2 | 14 | High |
| Attacker obtains user credentials by using email reset password (He has access to user email) | 2 | 1 | 1 | 1 | 3 | 8 | Medium |
| Attacker uses Web application vulnerability to get admin authorization | 3 | 2 | 2 | 3 | 2 | 12 | High |
| Attacker obtains authentication credentials by using brute-force attack | 2 | 1 | 3 | 2 | 3 | 11 | High |
| Attacker crashes the web server by using DDOS attack | 1 | 3 | 2 | 3 | 3 | 12 | High |
| Admin user publish sensitive data | 3 | 3 | 3 | 3 | 3 | 15 | High |
| Attacker preforms MITM attack over the communication between the web server and the DB to obtain superuser credentials | 3 | 1 | 1 | 3 | 2 | 10 | High |
| Attacker uploads a Webshell to the website and gains fully control over the web server | 3 | 1 | 1 | 3 | 2 | 12 | High |
| Attackers defaces the website main page | 1 | 2 | 2 | 2 | 2 | 9 | Medium |
| Website addon zero-day being used on an unknown vulnerability in any add-on to the server | 3 | 3 | 1 | 3 | 1 | 11 | High |
| Website addon one-day being used on a known vulnerability in any add-on to the server | 3 | 2 | 2 | 3 | 3 | 13 | High |
| Uploading Mock site in order to preform a phishing attack and steal credentials | 3 | 1 | 2 | 3 | 3 | 12 | High |