**TEAM XX IR REPORT**

|  |  |
| --- | --- |
| **Affected Host** | Box Name |
| **Source IP Address** | 10.10.10.10 (attacker) |
| **Destination IP Address** | 172.25.21.11 (ecom) |
| **Port and Service** | TCP/80 – HTTP |
| **Initial Access Timestamp** | 10:12am CT |
| **Service Downtime** | around 10:15-10:27am CT |
| **Remediated Timestamp** | 10:24am CT |
| **Affected Account** | www-data |

## Summary

(Summary).

## Vulnerability

### Explanation

Explanation.

### Evidence

|  |
| --- |
| **> Evidence** |

## Initial Access

### Explanation

Explanation.

### Evidence

|  |
| --- |
| **> Evidence** |

## Impact

### Explanation

Explanation.

### Evidence

|  |
| --- |
| **> Evidence** |

## Eradication

### Explanation

Explanation.

### Evidence

|  |
| --- |
| **> Evidence** |

## Remediation

### Explanation

Explanation.

### Evidence

|  |
| --- |
| **> Evidence** |