# Quarterly Vulnerability Challenge // iDefense Labs

//  q4 2006: $10,000 vulnerability challenge
**Challenge Focus:** Instant Messaging Applications
**Time Period:** Q4, 2006
**Prize Amount:** $10,000
**Submission Deadline:** Before Midnight EST on December 31, 2006

**Challenge:**
iDefense Labs is pleased to announce the launch of the next installment in our quarterly vulnerability challenge. For the 4th quarter, we are going to focus on instant messaging (IM) based vulnerabilities.

For submissions received before midnight on 31 December 2006, iDefense Labs will pay $10,000 for each vulnerability submission resulting in the discovery of a remotely exploitable IM vulnerability that meets the following criteria:

- Technologies:
  - Microsoft MSN Messenger
  - ICQ
  - AOL Instant Messenger
  - Google Talk
  - Apple iChat
  - Yahoo! Messenger
- The vulnerability must be remotely exploitable, allowing arbitrary code execution on the targeted machine, in a default installation of one of the technologies listed above.
- The vulnerability must exist in the latest version of the affected

technology with all available patches/upgrades applied 'RC' (Release candidate), 'Beta', 'Technology Preview' and similar versions of the listed technologies are not included in this challenge.

- The vulnerability must be original and not previously disclosed either publicly or to the vendor by another party.
- The vulnerability cannot be caused by or require any additional third party software installed on the target system.
- The vulnerability must not require any additional social engineering or user interaction such as visiting a malicious web site, clicking a link, or accepting a dialog message.

In order to qualify, the submission must include a full working exploit, be sent during the current quarter and be received by midnight EST on December 31, 2006.

The $10,000 prizes will be paid out following confirmation with the affected vendor and will be paid in addition to any amount paid for the vulnerability when it is first accepted.

Only the initial submission for a given vulnerability will qualify for the reward and a maximum of three awards will be paid out. Should more than three submissions qualify, the first three submissions will receive the reward. VeriSign will be responsible for making the final determination of whether or not a submission qualifies for the award.

// q3 2006: $10,000 vulnerability challenge

**Challenge Focus:** Web Browsers

**Time Period:** Q3, 2006

**Prize Amount:** $10,000

**Submission Deadline:** Before Midnight EST on September 30, 2006

**Challenge:**

iDefense Labs is pleased to announce the launch of next installment in our

quarterly vulnerability challenge. For the third quarter of 2006, we'll focus on browser based vulnerabilities, a topic which has been receiving plenty of attention lately with a steady increase in client side vulnerabilities which lend themselves to phising and identity theft attacks. For submissions received before September 30, 2006, iDefense Labs will pay $10,000 for each vulnerability submission that results in the discovery of a remotely exploitable web browser vulnerability that meets the following criteria.

- Technologies:
    - Microsoft Internet Explorer 6.0
    - Mozilla Firefox 1.5 (or latest)
    - IBM DB Universal Database 8.2
    - Apple Safari 2.0
    - Opera 9
- The vulnerability must be remotely exploitable, allowing arbitrary code execution on the targeted machine, in a default installation of one of the technologies listed above
- The vulnerability must exist in the latest version of the affected technology with all available patches/upgrades applied
- 'RC' (Release candidate), 'Beta', 'Technology Preview' and similar versions of the listed technologies are not included in this challenge
- The vulnerability must be original and not previously disclosed either publicly or to the vendor by another party
- The vulnerability cannot be caused by or require any additional third party software installed on the target system
- The vulnerability must not require additional social engineering beyond browsing a malicious site

In order to qualify, the submission must be sent during the current quarter and be received by midnight EST on September 30, 2006. The $10,000 prizes will be paid out following confirmation with the affected vendor and will be paid in addition to any amount paid for the vulnerability when it is

first accepted.

Only the initial submission for a given vulnerability will qualify for the reward and a maximum of six awards will be paid out. Should more than six submissions qualify, the first six submissions will receive the reward. VeriSign will be responsible for making the final determination of whether or not a submission qualifies for the award.

// q2 2006: $10,000 vulnerability challenge

**Challenge Focus:** Databases

**Time Period:** Q2, 2006

**Prize Amount:** $10,000

**Submission Deadline:** Before Midnight EST on June 30, 2006

**Challenge:**

iDefense Labs will pay $10,000 for each vulnerability submission that results in the discovery of a remotely exploitable database vulnerability that meets the following criteria.

- Technologies:
    - Oracle Database 10G
    - Microsoft SQL Server 2005
    - IBM DB Universal Database 8.2
    - MySQL 5.0
    - PostgreSQL 8.1
- The vulnerability must be original and not previously disclosed either publicly or to the vendor by another party
- The vulnerability must be remotely exploitable in a default installation of one of the targeted technologies
- The vulnerability must exist in the latest version of the affected technology with all current patches/upgrades applied
- The vulnerability cannot be caused by or require third party software
- The vulnerability must result in root access on the target machine
- The vulnerability must not require the use of authentication

credentials
- The vulnerability must receive the vendor's maximum severity ranking when the advisory is published (if applicable)

In order to qualify, the submission must be sent during the current quarter and be received by midnight EST on June 30, 2006. The $10,000 prizes will be paid out following confirmation with the affected vendor and will be paid in addition to any amount paid for the vulnerability when it is first accepted.

Only the initial submission for a given vulnerability will qualify for the reward and a maximum of six awards will be paid out. Should more than six submissions qualify, the first six submissions will receive the reward.
//  q1 2006: $10,000 vulnerability challenge

**Challenge Focus:** Microsoft Technologies
**Time Period:** Q1, 2006
**Prize Amount:** $10,000
**Submission Deadline:** Before Midnight EST on March 31, 2006

**Challenge:**
iDefense Labs is pleased to announce the launch of our quarterly hacking challenge. Going forward, on a quarterly basis, we will select a new focus for the challenge and outline the rules for vulnerability discoveries that will qualify for the monetary rewards. For the current quarter, iDefense Labs will pay $10,000 for each vulnerability submission that results in the publication of a Microsoft Security Bulletin with a severity rating of critical. In order to qualify, the submission must be sent during the current quarter and be received by midnight EST on March 31, 2006. The $10,000 prizes will be paid out following the publication of the Microsoft Security Bulletin and will be paid in addition to any amount paid for the vulnerability when it is initially accepted. Only the initial submission for a given vulnerability will

qualify for the reward.

For more information on eligibility and conditions, visit the iDefense Labs VCP overview or read about other reward programs.