The Dark Side of Computing

What Can Go Wrong?

Part I

June 28, 2002: NEW YORK (Reuters) - Software bugs are not just annoying or inconvenient. They are expensive. According to a study by the U.S. Department of Commerce's National Institute of Standards and Technology (NIST), the bugs and glitches cost the U.S. economy about $59,500,000,000 ($59.5 billion) a year.

The impact of software errors is enormous because virtually every business in the United States now depends on software for the development, production, distribution, and after-sales support of products and services," NIST Director Arden Bement said in a statement on Friday.

Software users contribute about half the problem, while developers and vendors are to blame for the rest, the study said. The study also found that better testing could expose the bugs and remove bugs at the early development stage could reduce about $22.2 billion of the cost.

"Currently, over half of all errors are not found until 'downstream' in the development process or during post-sale software use," the study said.

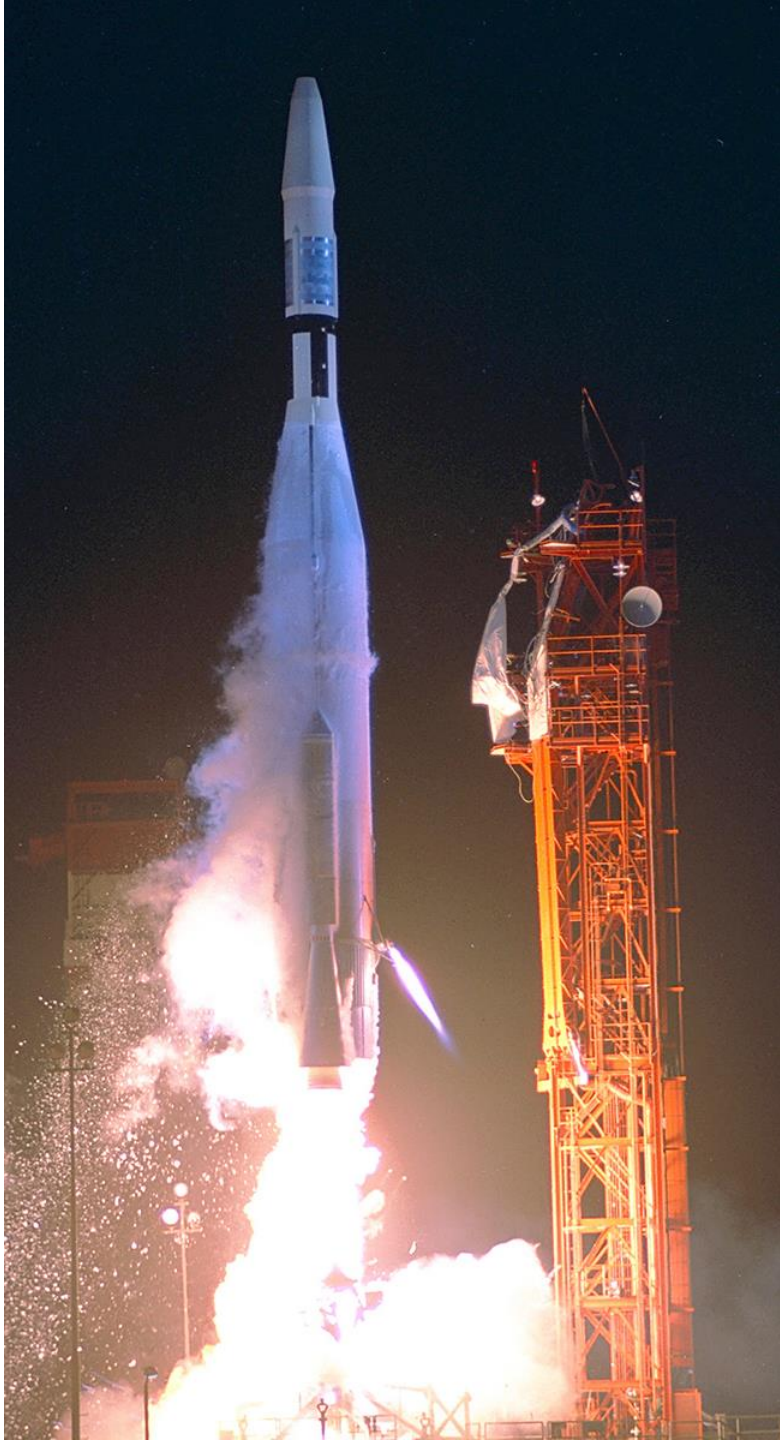
Update

The Cost of Poor Software Quality in the US (2022 Report) The Consortium for Information & Software Quality (CISQ) published its latest report on what poor software quality really costs. It is estimated that software quality issues may have cost the U.S. economy $2.41 **trillion** in 2022.

Some historical examples

Mariner I
Atlas-Agena rocket.

- Date: July 22, 1962
- Cost: $18.5 million
- Error: Used raw value instead of average
  - R instead of $\overline{R}$ (R Bar)
- Result: Rocket blown up by range safety officer



Nimbus 7 Ozone Satellites - 1978

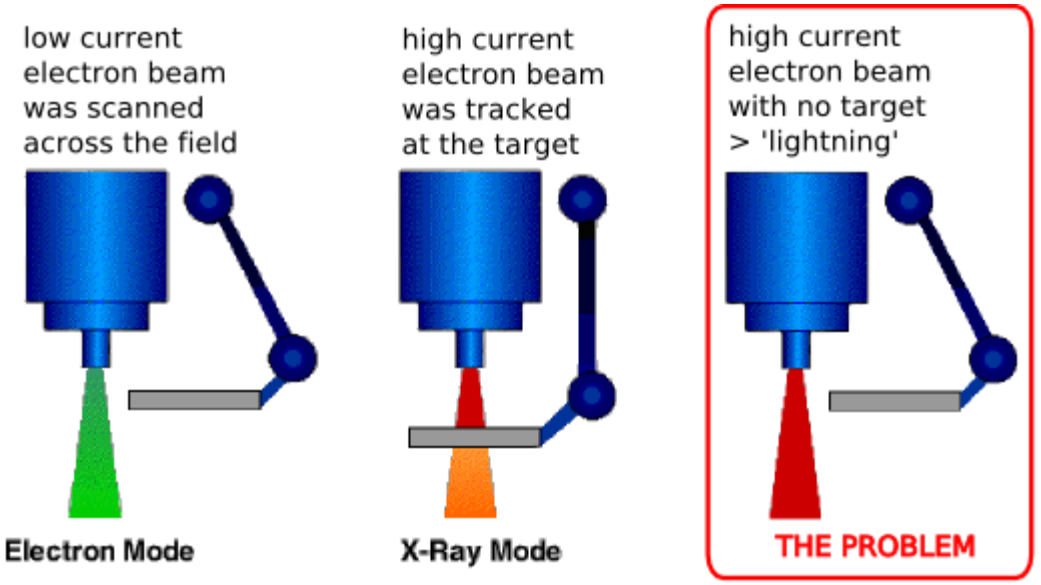
- Satellites designed to measure thickness of Ozone Layer
- Satellites correctly measure Ozone Layer thickness
- Ground data processing program ignored values that were very low assuming them to be in error.
- Cost: 7 year delay in knowing of problem
- Result: Holes in Ozone layers were not discovered until 1986.

Bank of New York

- Date: November 20, 1985
- Program: Bank of New York Program to track government securities transactions.
- Cost: $5 million
- Error: Latest transaction continuously overwriting last transaction Lost $32 BILLION. With effort had that down to only $23.6 BILLION by end of the day. $5 million was interest to cover missing funds for 2 days!!!
- Result: Bank lost confidence of investors.
- Comment: Disruption of econometric models.

Therac-25

- Date: June 1985 - January 1987
- Program: Therac 25. Computer controlled radiation therapy machine.
- Machine had two modes: Electrons, X-rays.



tray including the target, a flattening filter, the collimator jaws and an ion chamber was moved OUT for "electron" mode, and IN for "photon" mode.

Therac-25

- First model to rely strictly on computer control instead of mechanical interlocks. Reused software.
- Software bug caused machine to run at power setting 100 times too high. Cost: 6 patients died horribly painful deaths
- Result: Patients physically felt pain from beam. Rapidly developed radiation sickness and died agonizing deaths over the course of several months.

Patriot Missile Failure -- 1991

- Patriot ant-missile battery was installed in Dhahran, Saudi Arabia to protect American assets
- Internal clock on computer controlling missile batteries was drifting.
- Israelis has warned of this problem and told US to reboot the system every so often.
- This was not done.
- During a Scud missile attack Patriot control computer could not find incoming missiles because it was looking in the wrong place.
- Result: 28 American servicemen killed

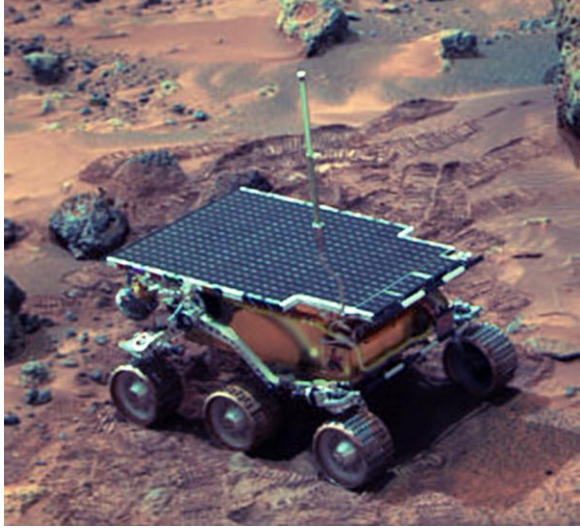
AT&T Switching

- Date: June and early July of 1991
- Program: Telephone switching software by DSC Communication
- Cost: Unknown (but a bunch)
- Error: After 13 weeks of successful testing changed 3 lines out of several million.
- Result: A series of outages affected telephone users in Los Angeles, San Francisco, Washington, D.C., Virginia, W. Virginia, Baltimore, and Greensboro, N.C.
- Comment: They knew what that change did, and they were confident that it did nothing else.(2) And presumably, the customer wanted it now.

Ariane 5 - 1996

- Launch site: French Guinea
- $500 million satellite
- Software bug in software written for Ariane 4
- Software tried to store a 64 bit value into a 16 bit location resulting in underflow (negative).
- Rocket destroyed 36.7 seconds after launch

Mars Pathfinder 1997



- Error: System periodically reset itself, cause unknown
- Solution: JPL engineers had fortuitously left the RTOS debugger/interpreter enabled in the software when it was installed. This allowed them to test and debug the mission software in situ. The fault was isolated, and a short C program was written and uploaded to the spacecraft. This program, when interpreted, fixed the problem
- Result: No more resets occurred

Mars Pathfinder

- Software designers had sacrificed "correct" software behavior for the sake of expediency and to meet mission deadlines (sound familiar?)
- Diagnosing the problem without direct access to the running system would have proved impossible
- Leaving the debugger installed and enabled saved the project

- Note: JPL engineers later confessed that a few unexplained resets had occurred during initial testing. The resets were not reproducible or explainable, and did not occur in what were considered to be "mission critical" parts of the software. They were eventually dismissed as the result of "hardware glitches".

Mars Polar Lander

- Date: December, 1999
- Cost: $185 million
- Error: Signaling problem in the landing legs caused by *one line* of missing computer code
- Deployment of landing legs caused vibration which was interpreted as touchdown which turned off descent engine.
- Result: Lander lost, presumed crash-landed

Mars Climate Orbiter - 1999

- Supposed to act as relay for polar lander.
- NASA uses the metric system
  - Their contracts require the contractor to convert all units to metric
- Orbiter entered atmosphere and burned up.

Mars Climate Orbiter - 1999

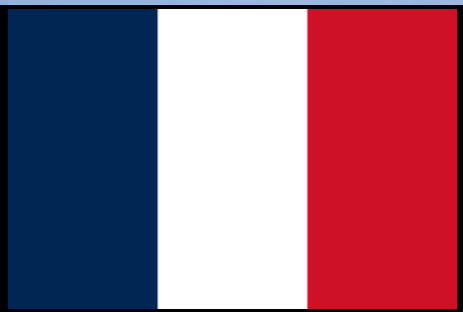
- An investigation indicated that the failure resulted from a navigational error due to commands from Earth being sent in English units (in this case, pound-seconds) without being converted into the metric standard (Newton-seconds).

I Love You -- 2000

- Clicking on the attachment sent the virus to everyone in your Outlook address book
- Would erase random files on your computer
- Cost $23 billion to clean up the mess

Airbus 380






Airbus 380 -- 2004

- Can hold over 800 passengers!
- Multination effort involving 4 countries
- Big and complex plane.
  - 100,000 different wires,
  - Totaling 330 miles in length
  - 1,150 separate functions.
- Each country used different software
- When they went to mate up the two halves of the planes the cables were wrong and had to be replaced.
- Delayed project by a year
- Cost unknown but a lot!

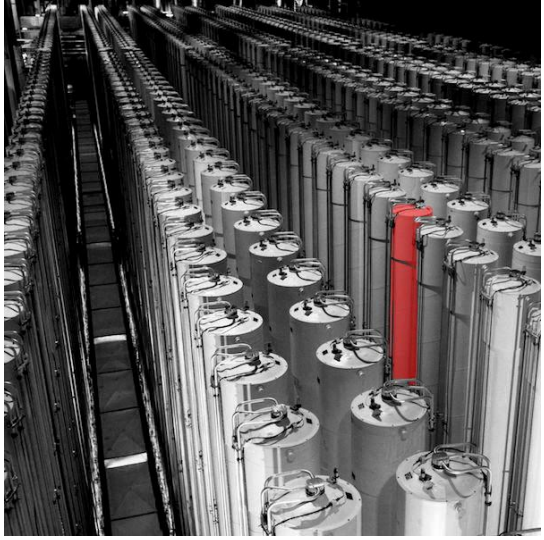
Knight Capital
2012

- Stock market opened
- Knight Capital computer began to buy large blocks of stock worth $7billion for 45 minutes.
- When they were stopped Knight had to sell all the mistakenly purchased stock now at low prices.
- $440 Million loss is 45 minutes.
- Problem cause: New software uploaded to 7 out of eight servers
- Knight was purchased by a rival a few months later.

Wannacry -- 2017

- A virus spread ransomware to computer demanding payment of $300-$500 to allow users to access their data.
- Worldwide cost to fix estimated at $4 billion.
- Experts claim it was done by North Korea

Stuxnet -- 2022



- A virus on a USB stick loaded itself onto a Windows computer in Iran.
- Once in the network the virus searched for Siemens Step7 controllers used to control centrifuges used to refine uranium for atomic weapons
- The virus caused about 1000 of these centrifuges to operate in such a way that they destroyed themselves.
- No one has claimed responsibility

Boeing 737 MAX 2019

- Design rushed into production
- Wanted larger engines for fuel economy
- Had to move engines forward
- Made planes want to dive
- Introduced software system to correct
- System not well understood by some pilots and blamed for two crashes
- Two year grounding $20-80 billion lost

Part II

Just how do they hack into my computer?

/ MAGAZINE
FEATURES 19.02

How a Remote Town in Romania Has Become Cybercrime Central

By Yudhijit Bhattacharjee ✉ January 31, 2011 | 12:00 pm | Wired February 2011

The sudden appearance of luxury car dealerships among the grass fields marks the entrance into Râmnicu Vâlcea.
Photo: Nick Waplington

Stack Smashing

- How hard is it to program a computer?

- Suppose there were no computers?

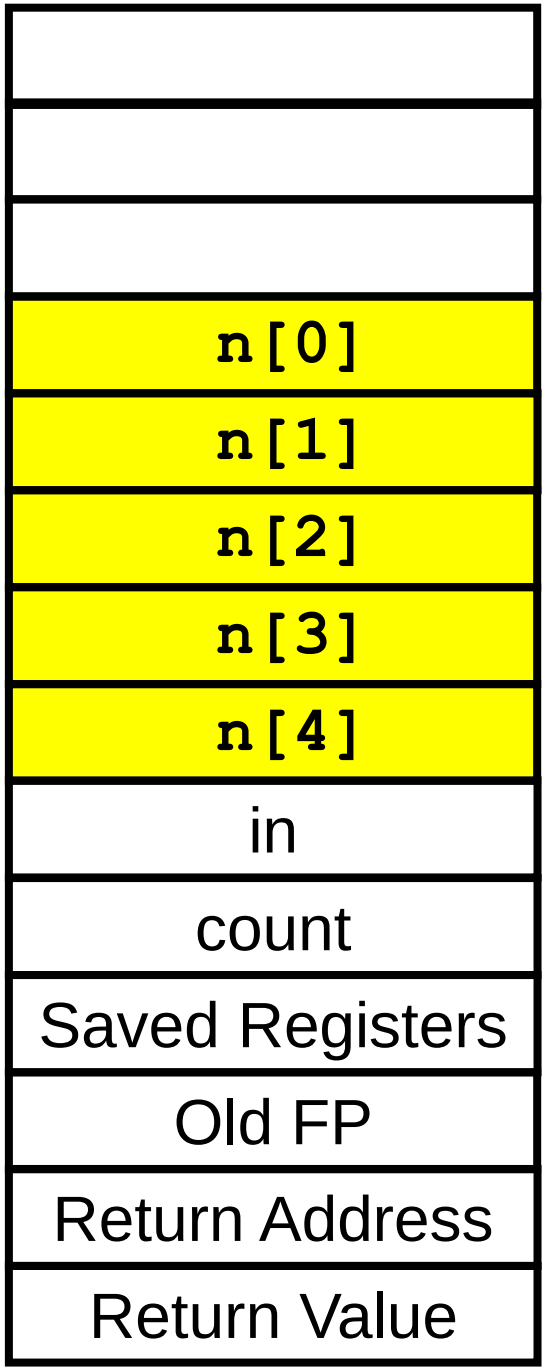
Computer Programs

- Broken up into pieces called modules or functions or subroutines, etc.
- Where do they store their data?
- The stack!

Imagine a Desk

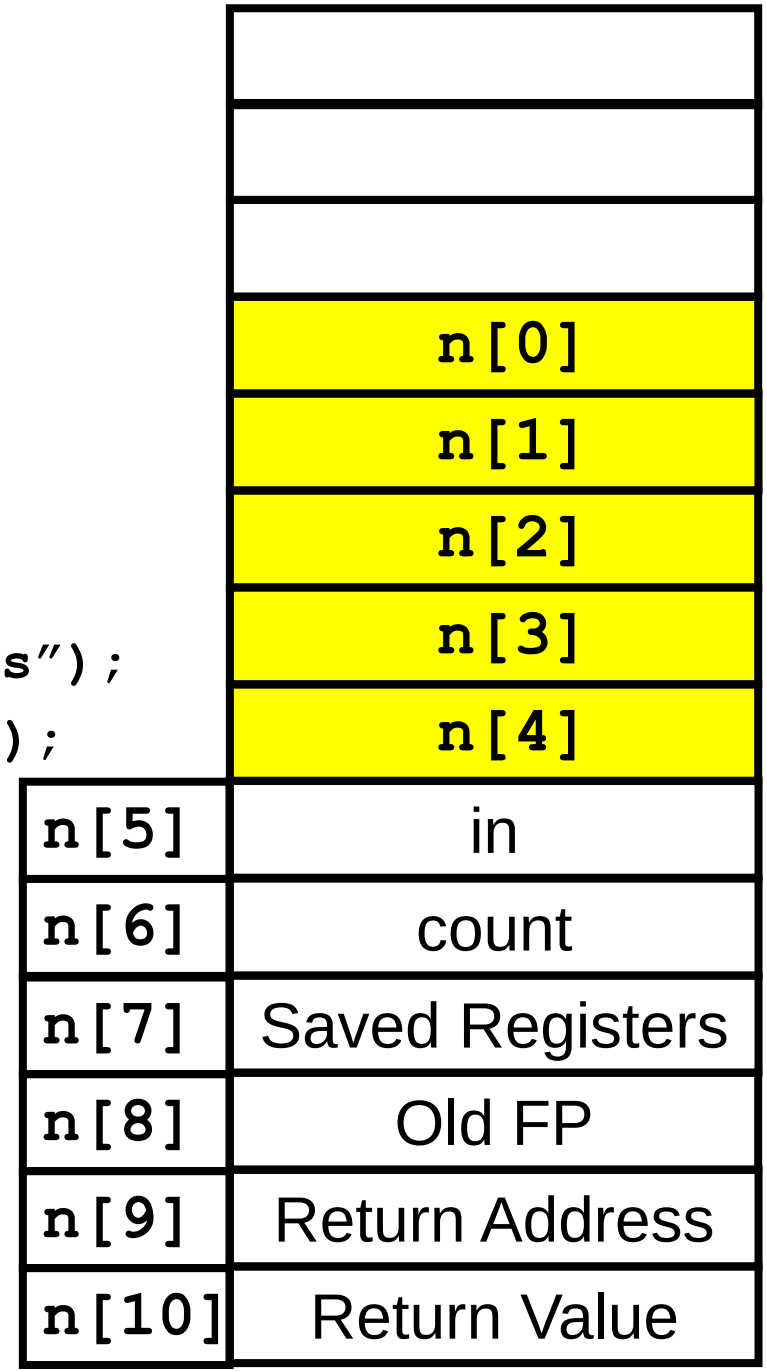
```
W = smash();

int smash()
{
  int count = 0;
  int in;
  int n[5];
  do {
   printf("Enter max of 5 vals");
   printf("Enter -99 to quit");
   scanf("%d", &in);
   if(in != -99)
       n[count] = in;
   count++; }
  while(count != -99);
  // do stuff
}
```



```
W = smash();

int smash()
{
  int count = 0;
  int in;
  int n[5];
  do {
   printf("Enter max of 5 vals");
   printf("Enter -99 to quit");
   scanf("%d", &in);
   if(in != -99)
       n[count] = in;
   count++; }
  while(count != -99);
  // do stuff
```



In some cases

- A nefarious user may be possible to take control of your program (worst case)
- Or perhaps just cause your program to crash

Doesn't Like You

SERVER

CRASH

Sends out virus!

- Attached to email
- Says:

Press this button to infect your computer with a virus

When it comes to phishing attacks, the Verizon team found that 23% of users open phishing emails and 11% take the extra PEBKAC step of actually clicking on the attachment. Even a small phishing campaign of 10 emails has a 90% chance of hooking at least one victim. IT folks have a tiny window to react to phishing attacks as the average time between email being sent and the first person clicking on the link is a mere one minute and 22 seconds.

PEBKAC: Problem Exists Between Keyboard and Chair

When it comes to phishing attacks, the Verizon team found that 23% of users open phishing emails and 11% take the extra PEBKAC step of actually clicking on the attachment. Even a small phishing campaign of 10 emails has a 90% chance of hooking at least one victim. IT folks have a tiny window to react to phishing attacks as the average time between email being sent and the first person clicking on the link is a mere one minute and 22 seconds.

campus and community

GTPD warns students of IRS spoofing scam

By Lance Wallace | AUGUST 12, 2016 • ATLANTA, GA

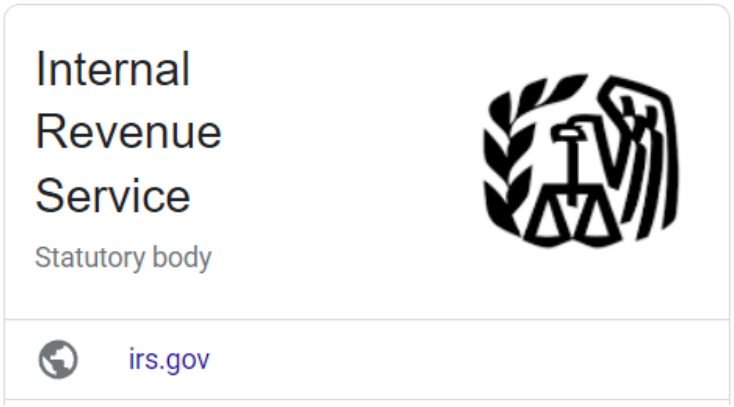
Since tax season, a scam has gone around the country in which callers attempt to persuade students to put money on gift cards and make other forms of payment to meet a previously unknown "federal student tax."

According to the Federal Bureau of Investigation (FBI) multiple universities have been targeted. Some examples of the varied tactics seen this year are:

- Demanding immediate tax payment for taxes owed on an iTunes gift card.
- Soliciting W-2 information from payroll and human resources professionals (**IR-2016-34**)
- "Verifying" tax return information over the phone (**IR-2016-40**)
- Pretending to be from the tax preparation industry (**IR-2016-28**)

Sends out virus!

- Attached to email
- Says:



Press this button to avoid audit

Now

- The kid who doesn’t like you has thousands of computers infected with a virus.
- What does the virus do?
- Every day it goes to a website and asks if there are any orders

www.yournamehere.com

Then he picks a target

ONLINE PIZZA SALES = $0.00

Uber Supposedly Paid Hackers $100,000 to Keep Quiet About a 2016 Data Breach

By Catalin Cimpanu

November 21, 2017 07:16 PM 2

One careless strcat . . . Yours ?

Remember – **Only you can**

PREVENT BUFFER OVERFLOWS !

SQL Injection

- Database – a structured set of data held in a computer, especially one that is accessible in various ways.

- SQL – Structured Query Language (pronounced Sequel)

Sample Database "Item"

ItemNumber	ItemName	ItemDescription	ItemQuantity
406	Sweater	Navy Cardigan	14
387	Shirt	Plaid short sleeve	23
112	Pants	Men's slacks	11
148	Scarf	Paisley	9
292	Shoe	Mary Jane	3
866	Belt	Cowhide	16

Sample Query

```
SELECT ItemName, ItemDescription, ItemQuantity
FROM Item
WHERE ItemNumber = 112
```

```
sql_query= "
SELECT ItemName, ItemDescription, ItemQuantity
FROM Item
WHERE ItemNumber = " & Request.QueryString("ItemID")
```

Sample Query

```
SELECT ItemName, ItemDescription, ItemQuantity
FROM Item
WHERE ItemNumber = 112
```

```
sql_query= "
SELECT ItemName, ItemDescription, ItemQuantity
FROM Item
WHERE ItemNumber = " & Request.QueryString("ItemID")
```

But…

- What if the user types in something like this?

```
112 OR 1=1
```

We get

```
SELECT ItemName, ItemDescription, ItemQuantity
FROM Item
WHERE ItemNumber = 112 OR 1=1
```

Even Worse…

- What if the user types in something like this?

```
112; DROP TABLE ITEM
```

We get

```
SELECT ItemName, ItemDescription, ItemQuantity
FROM Item
WHERE ItemNumber = 112; DROP TABLE ITEM
```

Which deletes all the data!!!


E
'OR 1=1;--

So to stop this

- You search for:

```
OR 1=1
```

- And delete it! So

```
999 OR 1=1
```

- Becomes

```
999
```

So now…

- The bad guy enters

```
999 OOR 1=1R 1=1
999 OOR 1=1R 1=1
```

- Your software removes the OR 1=1

```
999 OOR 1=1R 1=1

999 OR 1=1
```

NEVER TRUST USERS!!!

Questions?