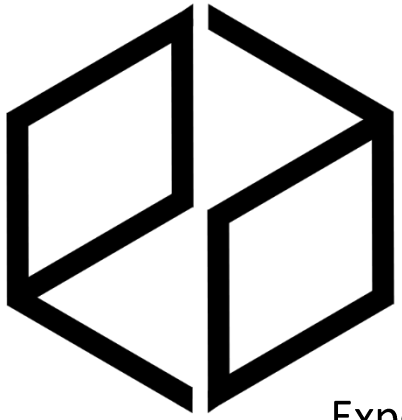
www.pandoralabs.net

PANDORA
SECURITY LABS

Expert advice. Experience advantage.
Proactive Security Solutions Through Cutting-Edge Research.

OWASP TOP 10: #6 Sensitive Data Exposure

By @isaacsabas



PANDORA
SECURITY LABS

Expert advice. Experience advantage.
Proactive Security Solutions Through Cutting-Edge Research.

www.pandoralabs.net

We are a Security-as-a-Service company

Providing businesses with on-demand IT security controls for them to meet their 24x7 security strategies & requirements.

We Make IT Secure

OWASP

Open Web Application Security Project


A1: Injection
A2: Broken Authentication and Session Management
A3: Cross-Site Scripting (XSS)
A4: Insecure Direct Object References
A5: Security Misconfiguration
A6: Sensitive Data Exposure
A7: Missing Function Level Access Controls
A8: Cross Site Request Forgery (CSRF)
A9: Using Components with Known Vulnerabilities
A10: Unvalidated Redirects and Forwards

OWASP #6

Sensitive Data Exposure

OWASP Top 10 Vulnerabilities

Weakness in a web application that compromises the safety of sensitive information such as credit card numbers and PII.

Sensitive Data Exposure

What is it?

What are Sensitive Data?

- Banking information
  - Credit cards
  - Account numbers
  - Login details
- PII
  - Birthday
  - Mother’s maiden name
  - Address
  - Government IDs

How is this vulnerability exploited?

1. Through communication
2. Unencrypted data storage

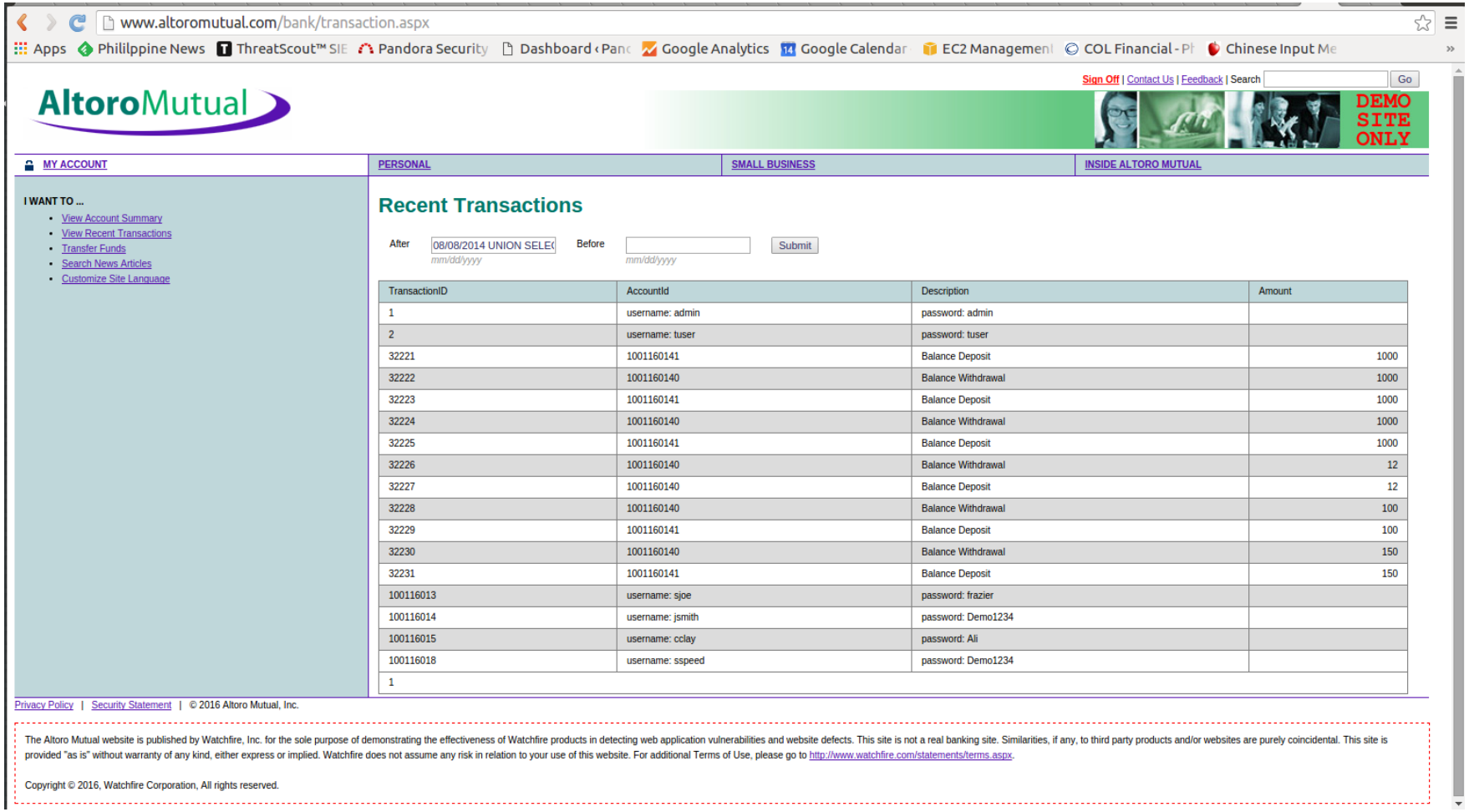
What are the Risks When Exploited?

- Potential financial loss
- Identify theft
- Decreased trust in vendor

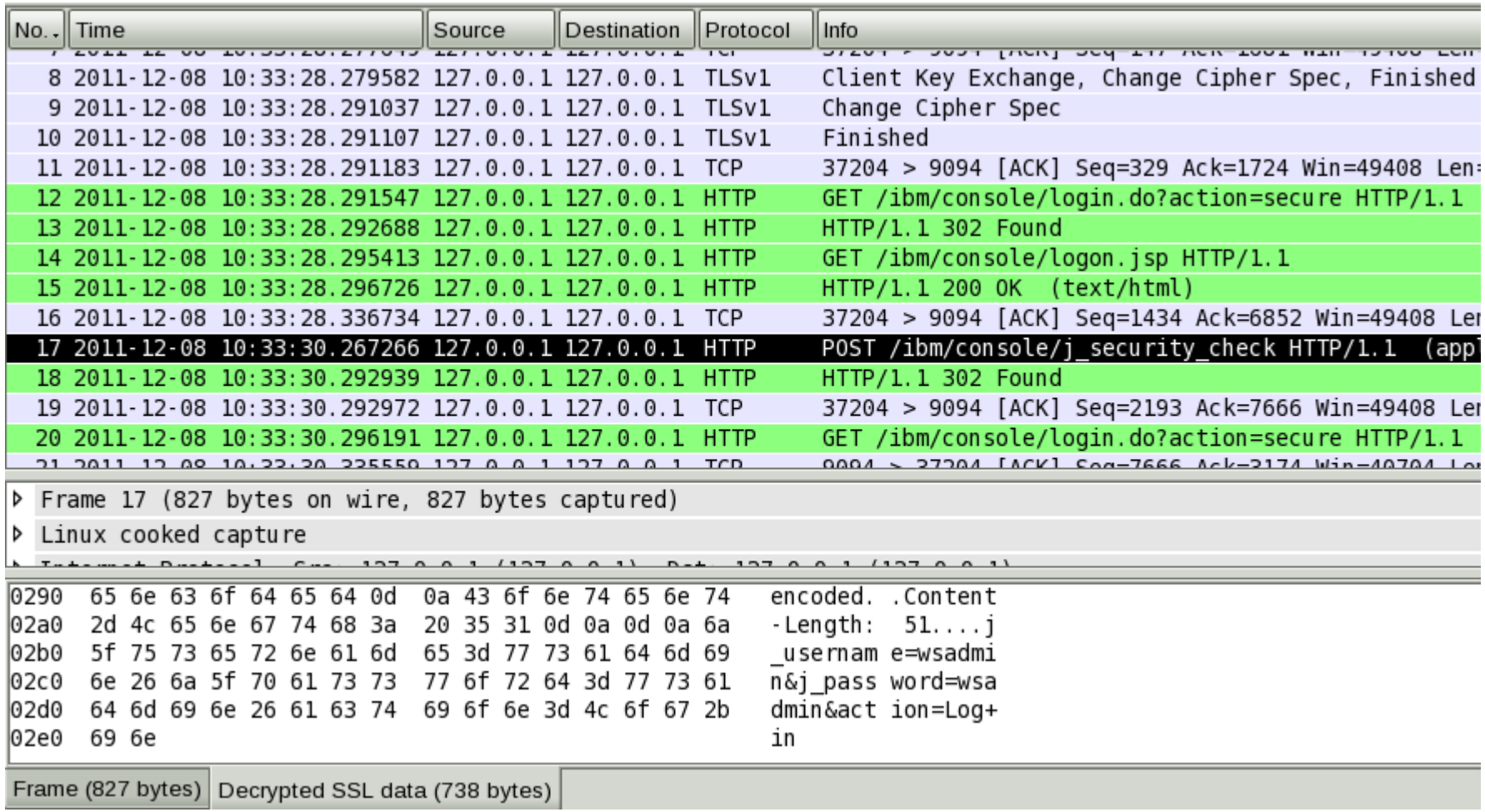
How do I Prevent Such Vulnerability?

- Encrypt data during transport and at rest
- Minimize data surface area
- Use the latest encryption algorithms
- Disable autocomplete on forms that collect data
- Disable caching on forms that collect data

Samples


www.altoromutual.com/bank/transaction.aspx
Apps
Philippine News
ThreatScout™ SIE
Pandora Security
Dashboard ‹ Panc
Google Analytics
Google Calendar
EC2 Management
COL Financial - Pl
Chinese Input Me
AltoroMutual
Sign Off | Contact Us | Feedback | Search
Go
DEMO SITE ONLY
MY ACCOUNT
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
I WANT TO ...
View Account Summary
View Recent Transactions
Transfer Funds
Search News Articles
Customize Site Language
Recent Transactions
After
08/08/2014 UNION SELE(
mm/dd/yyyy
Before
mm/dd/yyyy
Submit
TransactionID
AccountId
Description
Amount
1
username: admin
password: admin
2
username: tuser
password: tuser
32221
1001160141
Balance Deposit
1000
32222
1001160140
Balance Withdrawal
1000
32223
1001160141
Balance Deposit
1000
32224
1001160140
Balance Withdrawal
1000
32225
1001160141
Balance Deposit
1000
32226
1001160140
Balance Withdrawal
12
32227
1001160140
Balance Deposit
12
32228
1001160140
Balance Withdrawal
100
32229
1001160141
Balance Deposit
100
32230
1001160140
Balance Withdrawal
150
32231
1001160141
Balance Deposit
150
100116013
username: sjoe
password: frazier
100116014
username: jsmith
password: Demo1234
100116015
username: cclay
password: Ali
100116018
username: sspeed
password: Demo1234
1
Privacy Policy | Security Statement | © 2016 Altoro Mutual, Inc.
The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. Watchfire does not assume any risk in relation to your use of this website. For additional Terms of Use, please go to http://www.watchfire.com/statements/terms.aspx.
Copyright © 2016, Watchfire Corporation, All rights reserved.

Samples



No.	Time	Source	Destination	Protocol	Info
8	2011-12-08 10:33:28.279582	127.0.0.1	127.0.0.1	TLSv1	Client Key Exchange, Change Cipher Spec, Finished
9	2011-12-08 10:33:28.291037	127.0.0.1	127.0.0.1	TLSv1	Change Cipher Spec
10	2011-12-08 10:33:28.291107	127.0.0.1	127.0.0.1	TLSv1	Finished
11	2011-12-08 10:33:28.291183	127.0.0.1	127.0.0.1	TCP	37204 > 9094 [ACK] Seq=329 Ack=1724 Win=49408 Len=
12	2011-12-08 10:33:28.291547	127.0.0.1	127.0.0.1	HTTP	GET /ibm/console/login.do?action=secure HTTP/1.1
13	2011-12-08 10:33:28.292688	127.0.0.1	127.0.0.1	HTTP	HTTP/1.1 302 Found
14	2011-12-08 10:33:28.295413	127.0.0.1	127.0.0.1	HTTP	GET /ibm/console/logon.jsp HTTP/1.1
15	2011-12-08 10:33:28.296726	127.0.0.1	127.0.0.1	HTTP	HTTP/1.1 200 OK (text/html)
16	2011-12-08 10:33:28.336734	127.0.0.1	127.0.0.1	TCP	37204 > 9094 [ACK] Seq=1434 Ack=6852 Win=49408 Len
17	2011-12-08 10:33:30.267266	127.0.0.1	127.0.0.1	HTTP	POST /ibm/console/j_security_check HTTP/1.1 (appl
18	2011-12-08 10:33:30.292939	127.0.0.1	127.0.0.1	HTTP	HTTP/1.1 302 Found
19	2011-12-08 10:33:30.292972	127.0.0.1	127.0.0.1	TCP	37204 > 9094 [ACK] Seq=2193 Ack=7666 Win=49408 Len
20	2011-12-08 10:33:30.296191	127.0.0.1	127.0.0.1	HTTP	GET /ibm/console/login.do?action=secure HTTP/1.1

```
▷ Frame 17 (827 bytes on wire, 827 bytes captured)
▷ Linux cooked capture
```

```
0290  65 6e 63 6f 64 65 64 0d  0a 43 6f 6e 74 65 6e 74   encoded. .Content
02a0  2d 4c 65 6e 67 74 68 3a  20 35 31 0d 0a 0d 0a 6a   -Length:  51....j
02b0  5f 75 73 65 72 6e 61 6d  65 3d 77 73 61 64 6d 69   _usernam e=wsadmi
02c0  6e 26 6a 5f 70 61 73 73  77 6f 72 64 3d 77 73 61   n&j_pass word=wsa
02d0  64 6d 69 6e 26 61 63 74  69 6f 6e 3d 4c 6f 67 2b   dmin&act ion=Log+
02e0  69 6e                                             in
```

Frame (827 bytes) | Decrypted SSL data (738 bytes)

TIME FOR

Q&A

OWASP Top 10 – Sensitive Data Exposure

Go download WebGoat

https://github.com/WebGoat/WebGoat-Legacy

TRY IT YOURSELF

Some homework for you to learn a bit more.

WebGoat Installation How-To

1. Download Java VM, JDK 1.7
2. Download WebGoat: https://webgoat.atlassian.net/builds/browse/WEB-WGM/latestSuccessful/artifact/shared/WebGoat-Embedded-Tomcat/WebGoat-6.0.1-war-exec.jar
3. Run the .jar file:
    1. java -jar WebGoat-6.0-exec-war.jar
4. Then navigate in your browser to: (http://localhost:8080/WebGoat)
5. Login using guest account
6. Go to Insecure Storage & Insecure Communication and complete the exercises

OWASP #6

Sensitive Data Exposure

OWASP Top 10 Vulnerabilities

www.pandoralabs.net

PANDORA
SECURITY LABS

Expert advice. Experience advantage.
Proactive Security Solutions Through Cutting-Edge Research.

OWASP TOP 10: #6 Sensitive Data Exposure

By @isaacsabas