

# CIS3165 – WEB SECURITY

BY PELIN

# GENERAL SECURITY PRINCIPLES

THESE PRINCIPLES  
ARE THE  
FOUNDATION FOR  
DIFFERENT  
SECURITY ISSUES

ARE THE  
FUNDAMENTALS  
OF ALL SECURITY

THEY PROVIDE  
GUIDANCE

# 1. LEAST PRIVILEGES

---

"every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job" – Jerome Saltser

## **Benefits:**

Code stability

- Controlled data access
- Easier to test actions and interactions

System security

Vulnerabilities are limited and localized



## 2. SIMPLE IS MORE SECURE

---

Complexity invites bugs

Use clearly named functions and variables

Write code comments

Break up long sections of code into smaller functions

Don't repeat yourself

Legacy code is a security concern

Built-in functions are often better than your own versions

Disable or remove unused features when possible



# 3. NEVER TRUST USERS

---

Well-meaning users can cause problems

Be paranoid

Don't even trust admin users completely

Can become unhappy employees or ex-employees

May not take security seriously

Can have identity stolen



# NEVER TRUST USERS

---

Use caution with contractors

- Both insider and outsider status
- Often not fully vetted
- Often transient

Make it easier to revoke their access privileges

- Even offline
- Phone
- Email
- printing

## 4. EXPECT THE UNEXPECTED

Security is not reactive

Prevent the crime before it happens

What are all the things a user could try on this page?

Consider “edge cases”

Get creative

# SEARCH BOX EXAMPLE

Length: too little or too much

Content type: high-ASCII, multi-byte

Content: \ " ' ( ) { } < > ` & ? % \$ \* + \_ :

Formats: safe for use in all formats

Structure and inputs: can they be modified



# 5. DEFENSE IN DEPTH

---

## Layered defenses

Originally a military term

- Slowing the advance of an attacker
- Attacks lose momentum

## Redundant security

There are three main areas that you want to focus on through defense in depth:

People: Awareness,

Technology: technical controls( hardware, software, network)

Operations: Administrative controls  
(Policy, procedures)



# 6. SECURITY THROUGH OBSCURITY

---

- More information benefits hackers
- Limit exposed information
- Limit feedback
- Obscurity does not mean misdirection



## 7. BLACKLISTING AND WHITELISTING

### **Black list:**

“No access” list

Reference list for What is forbidden

Blacklist= [div, span, image, input, form,.....]

### **White list:**

Opposite of blacklisting

Reference list of what is permitted

Opposites, but no equal

Whitelist=[p, br, strong, em]

## 8. MAP EXPOSURE POINTS AND DATA PASSAGEWAYS

### **Incoming exposure points:**

- URLs
- Forms
- Cookies/sessions
- Database reads
- Your public API

### **Outgoing exposure points:**

- Html
- JavaScript./JSON/XML/RSS
- Cookies/sessions
- Database writes
- Third-party APIs

### **Mapping data passageways**

What paths does data take?

Understand site topography

Awareness + protection= security

Helps “expect the unexpected”



THANK YOU