Advanced Security

Nsovo Baloyi
Penetration Tester, Investec Bank

C:\WINDOWS\system32>whoami

- Penetration Tester (Ethical Hacker) at Investec
- CEH, OSCP
- UP alumni
- nsovo.baloyi@protonmail.com
- Twitter: @baloyi23
- All opinions are my own, and may not reflect those of my past, present, or future employers

Disclaimer

Any information presented in these slides should be used for educational and research purposes only. I or the University of Pretoria are in no way responsible for any misuse of the information.

I do not promote hacking; I am only showing you ways hackers may compromise your systems, therefore allowing us to protect ourselves.

Hacking is illegal, and performing hack attempts without permission on computers that you do not own my result in you being prosecuted by the law.

Agenda

1. What is Cyber Security?
2. Common Web Application Flaws
3. Securing Web Applications

What is Cyber Security?

Cyber Security Defined

Sure. Cyber security is the practice of protecting systems, networks, and data from unauthorized access, use, disclosure, disruption, modification, or destruction. It is a broad term that encompasses a wide range of security measures, including:

- **Information security:** The protection of data from unauthorized access, use, disclosure, disruption, modification, or destruction.
- **Network security:** The protection of networks from unauthorized access, use, disclosure, disruption, modification, or destruction.
- **Application security:** The protection of applications from unauthorized access, use, disclosure, disruption, modification, or destruction.
- **Endpoint security:** The protection of end-user devices, such as laptops, smartphones, and tablets, from unauthorized access, use, disclosure, disruption, modification, or destruction.
- **Operational security:** The protection of the people, processes, and procedures that are used to manage and operate IT systems and data.

Cyber Security Defined

Cybersecurity refers to the practice of protecting computer systems, networks, and digital data from unauthorized access, damage, or theft. It involves the implementation of measures and safeguards to prevent and detect potential cyber threats, such as hacking, malware infections, data breaches, and other malicious activities.

The field of cybersecurity encompasses various technologies, processes, and practices designed to ensure the confidentiality, integrity, and availability of digital information. It involves both proactive and reactive measures to defend against cyber attacks and minimize the potential risks and vulnerabilities associated with computer systems and networks.

Some common areas of focus in cybersecurity include:

1. Network security: Securing computer networks from unauthorized access, monitoring network traffic, and implementing firewalls, intrusion detection systems, and virtual private networks (VPNs).
2. Application security: Protecting software applications from vulnerabilities and ensuring they are developed with secure coding practices.
3. Data security: Safeguarding sensitive data from unauthorized access or theft through encryption, access controls, and data backup and recovery processes.
4. Incident response: Developing strategies and plans to respond to and mitigate the impact of cyber incidents, including investigating and recovering from security breaches.
5. Vulnerability management: Identifying and addressing vulnerabilities in computer systems and networks through regular security assessments, penetration testing, and patch management.
6. Identity and access management: Managing user identities, authentication, and authorization to ensure only authorized individuals have access to resources and systems.
7. Security awareness and training: Educating users about best practices, security policies, and potential risks to improve overall security posture and reduce human-related security breaches.
8. Cloud security: Ensuring the security of data and applications stored and accessed in cloud computing environments.

Effective cybersecurity involves a combination of technical solutions, robust policies and procedures, and a well-trained workforce. It is an ongoing and evolving process due to the constantly changing nature of cyber threats and the advancement of technology.

Cyber Security Defined

“An approach or series of steps to prevent or manage the risk of damage to, unauthorized use of, exploitation of, and—if needed—to restore electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity, and availability of these systems.” - NIST

Careers in Cyber Security

Security Analyst
Incident Responder
Ethical Hacker/Penetration Tester
Security Engineer
Security Architect

Security Consultant
Forensic Analyst
Security Operations Center (SOC) Analyst
Malware Analyst
Threat Hunter

Common Web Application Flaws

Common Web Application Flaws

- Two general lists used
  - OWASP top 10
  - Mitre CWE Top 25
- The Open Web Application Security Project® (OWASP) is a nonprofit foundation that works to improve the security of software
  - Most recent published in 2021
  - Rely on data supplied by researchers and reward programs
- The CWE Top 25 is a compilation of the most widespread and critical weaknesses that could lead to severe software vulnerabilities.
  - The most recent CWE Top 25 was published in 2022
  - Uses a scoring system based on the NVD
- Bonus: PortSwigger Top 10 Hacking Techniques

OWASP Top 10

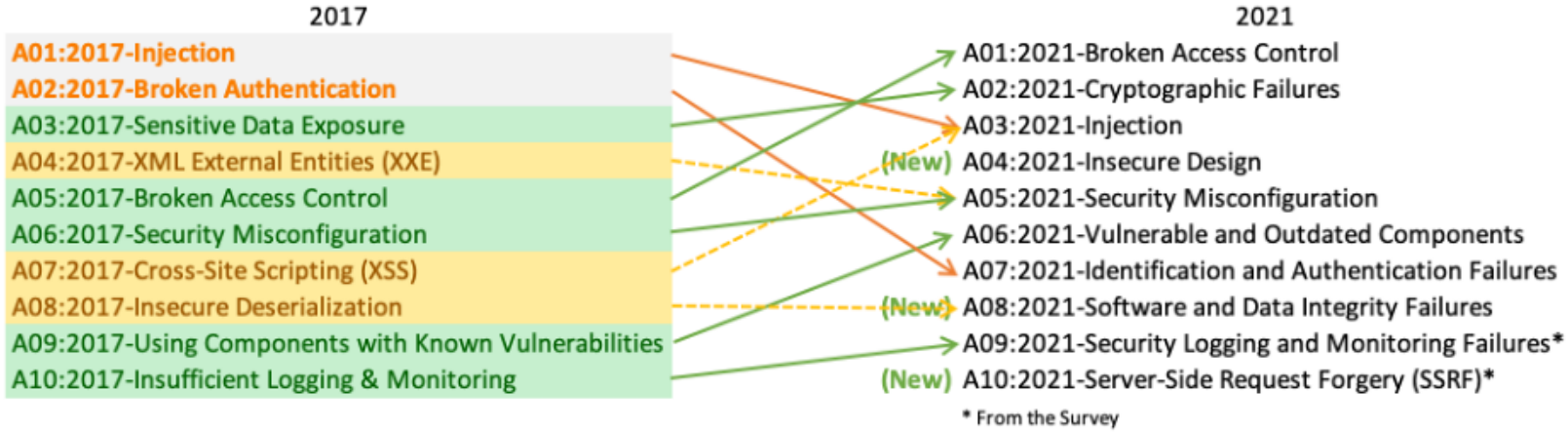


Image Source: [OWASP Top Ten | OWASP Found]

OWASP Top 10 2021

1. A1 - Broken Access Control
2. A2 - Cryptographic Failures
3. A3 - Injection
4. A4 - Insecure Design
5. A5 - Security Misconfiguration
6. A6 - Vulnerable and Outdated Components
7. A7 - Identification and Authentication Failures
8. A8 - Software and Data Integrity Failures
9. A9 - Security Logging and Monitoring Failures
10. A10 - Server-Side Request Forgery (SSRF)

Mitre CWE top 25 2022

1. CWE787 - Out-of-bounds Write
2. CWE79 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
3. CWE89 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
4. CWE20 - Improper Input Validation
5. CWE125 - Out-of-bounds Read
6. CWE78 - Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
7. CWE416 - Use After Free
8. CWE22 - Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
9. CWE352 - Cross-Site Request Forgery (CSRF)
10. CWE434 - Unrestricted Upload of File with Dangerous Type
11. CWE476 - NULL Pointer Dereference
12. CWE502 - Deserialization of Untrusted Data

Mitre CWE top 25 2022

13. CWE190 - Integer Overflow or Wraparound
14. CWE287 - Improper Authentication
15. CWE798 - Use of Hard-coded Credentials
16. CWE862 - Missing Authorization
17. CWE77 - Improper Neutralization of Special Elements used in a Command ('Command Injection')
18. CWE306 - Missing Authentication for Critical Function
19. CWE119 - Improper Restriction of Operations within the Bounds of a Memory Buffer
20. CWE276 - Incorrect Default Permissions
21. CWE918 - Server-Side Request Forgery (SSRF)
22. CWE326 - Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
23. CWE400 - Uncontrolled Resource Consumption
24. CWE611 - Improper Restriction of XML External Entity Reference
25. CWE94 - Uncontrolled Resource Consumption

Penetration Testing

- Penetration testing, also referred to as pentesting, is a simulated real world attack on a network, application, or system that identifies vulnerabilities and weaknesses.
- Penetration tests (pen tests) are part of an industry recognised approach to identifying and quantifying risk.
- Penetration Testers actively attempt to ‘exploit’ vulnerabilities in a company’s infrastructure, applications, people and processes.
- It is an ongoing cycle of research and attack against a target or boundary
- It can identify logic coding errors which most, if not all, DAST and SAST tools will miss
- Tries to show the impact of vulnerability on business

Penetration Testing cont.

Stages of a penetration test

1. Planning (scoping)
2. Reconnaissance (Information Gathering)
3. Scanning/Discovery
4. Vulnerability Analysis
5. Exploitation and Post exploitation
6. Analysis and reporting

Server-Side Request Forgery (SSRF)

- What is SSRF?
  - Server-Side Request Forgery (SSRF) is a web security vulnerability that allows an attacker to induce the server-side application to make requests to an unintended location.
- Potential Consequences
  - Unauthorized access, data exfiltration, lateral movement and network reconnaissance, command execution
- Potential Mitigations
  - Input validation and sanitization, enforce strict access controls, use safe network access policies

SSRF cont.

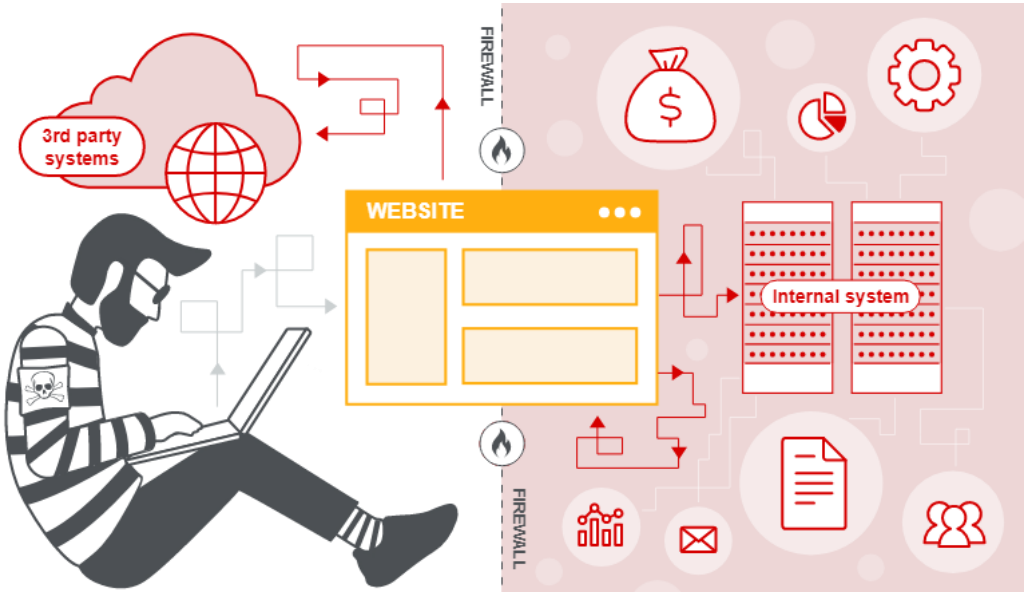


Image Source: https://portswigger.net/web-security/ssrf

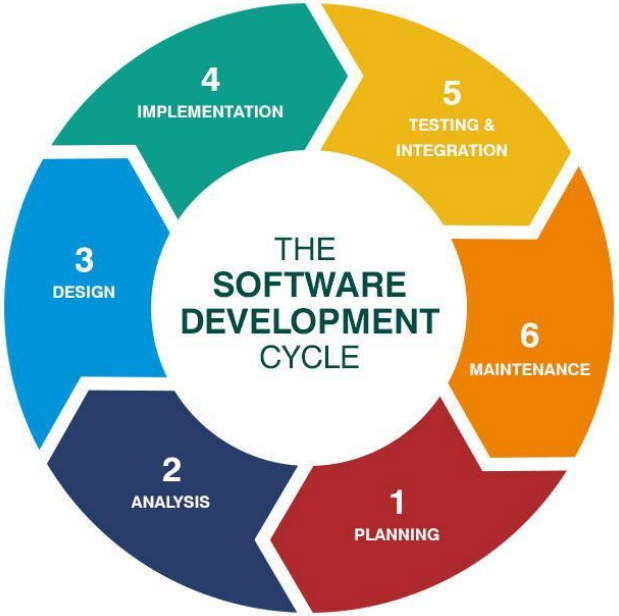
SSRF Demo

https://github.com/BenjiTrapp/ssrf-playground

Securing Web Applications

Practice Secure Coding

- Security is usually an afterthought
- We should incorporate security into the development life cycle
- Apply Security Best practices
  - Use CSPs and Secure Headers
  - Use WAFs
- Use DAST and SAST tools where possible
  - Netsparker, Veracode
  - Vulnerability scanning (Nessus, Qualys, OpenVAS)
  - Burp Suite, Zap Attack Proxy
  - WPScan, Joomscan, droopescan
  - Anchore, TwistLock, Synk, Wiz
- Manual Testing



Understanding Adversary Behavior

- MITRE ATT&CK®
  - Adversarial Tactics, Techniques, and Common Knowledge
  - Curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle
- Lockheed Martin Cyber Kill Chain®
  - Another well-known framework for understanding adversary behaviour in a cyber-attack

MITRE ATT&CK®

1. **Reconnaissance**: gathering information to plan future adversary operations, i.e., information about the target organization
2. **Resource Development**: establishing resources to support operations, i.e., setting up command and control infrastructure
3. **Initial Access:** trying to get into your network, i.e., spear phishing
4. **Execution:** trying the run malicious code, i.e., running a remote access tool
5. **Persistence:** trying to maintain their foothold, i.e., changing configurations
6. **Privilege Escalation:** trying to gain higher-level permissions, i.e., leveraging a vulnerability to elevate access
7. **Defense Evasion:** trying to avoid being detected, i.e., using trusted processes to hide malware

MITRE ATT&CK®

8. **Credential Access:** stealing accounts names and passwords, i.e., keylogging
9. **Discovery:** trying to figure out your environment, i.e., exploring what they can control
10. **Lateral Movement:** moving through your environment, i.e., using legitimate credentials to pivot through multiple systems
11. **Collection:** gathering data of interest to the adversary goal, i.e., accessing data in cloud storage
12. **Command and Control:** communicating with compromised systems to control them, i.e., mimicking normal web traffic to communicate with a victim network
13. **Exfiltration:** stealing data, i.e., transfer data to cloud account
14. **Impact:** manipulate, interrupt, or destroy systems and data, i.e., encrypting data with ransomware

MITRE ATT&CK®

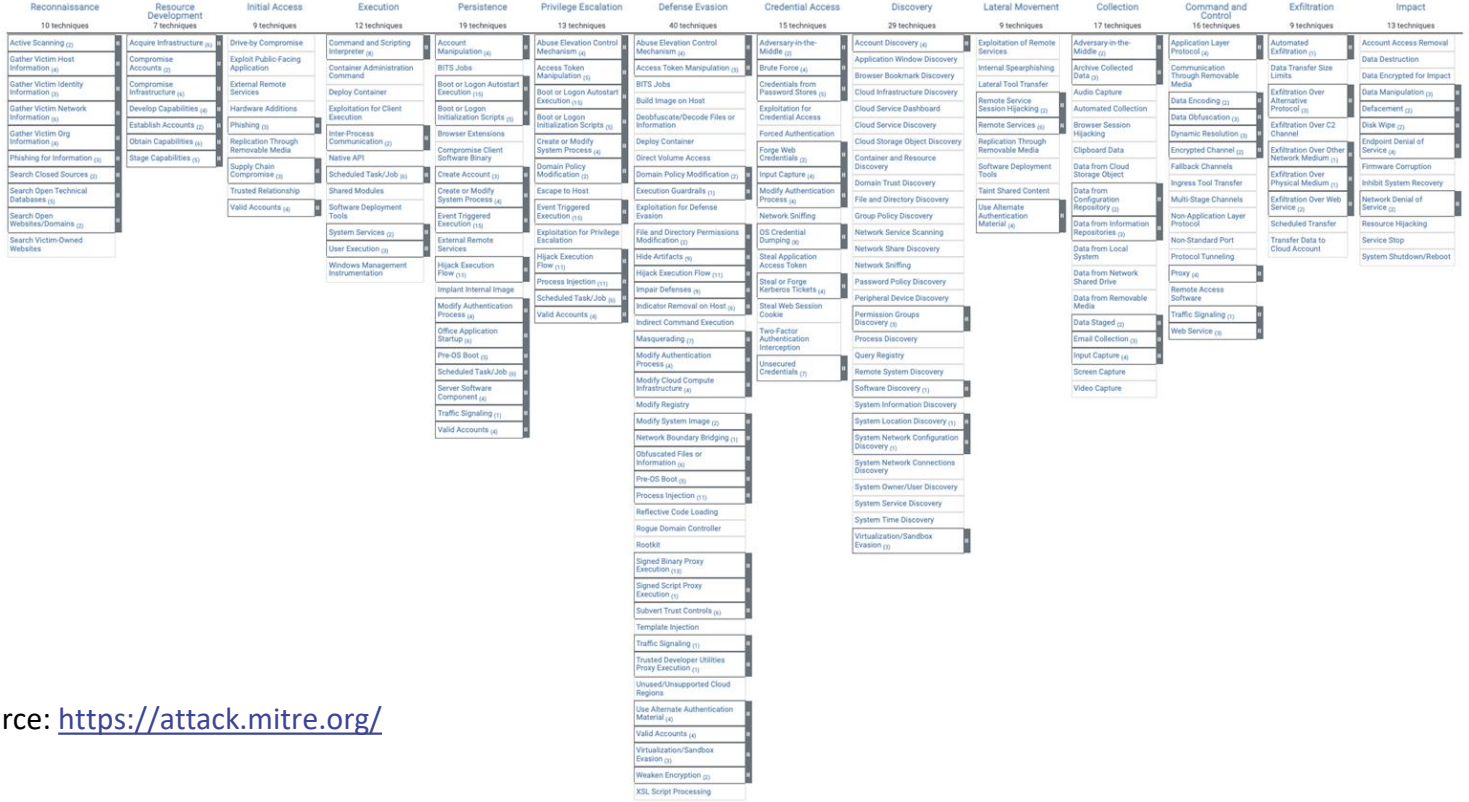
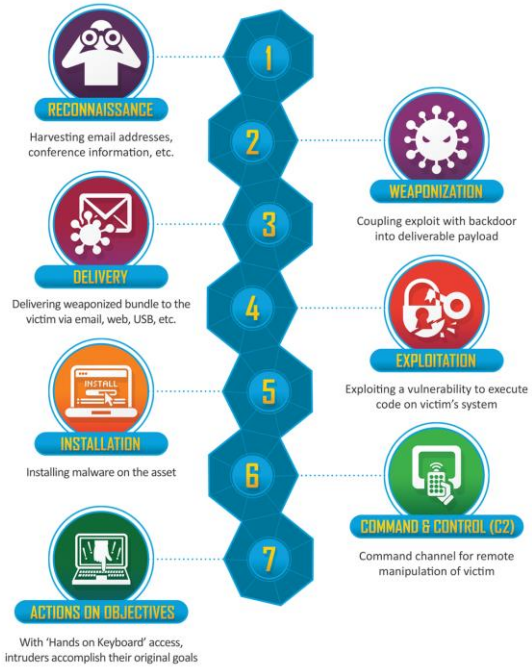


Image Source: https://attack.mitre.org/

Lockheed Martin Cyber Kill Chain®

1. **Reconnaissance** – Harvests email addresses, conference information, etc.
2. **Weaponization** – Couples exploit with backdoor into deliverable payload.
3. **Delivery** – Delivers weaponized bundle to the victim via email, web, USB, etc.
4. **Exploitation** – Exploits a vulnerability to execute code on a victim's system.
5. **Installation** – Installs malware on the asset.
6. Command & Control (C2) – Includes command channel for remote **manipulation**.
7. **Actions on Objectives** – Using 'Hands on Keyboards' access, intruders accomplish their original goals.

Image Source: Cyber Kill Chain



When Security goes wrong: The Capital One Data Breach Case Study

- In 2019 Capital One was breached
  - About 140,000 Social Security numbers of credit card customer stolen
  - About 80,000 linked bank account numbers of secured credit card customers stolen
- A misconfiguration in the WAF allowed the attacker to perform a SSRF attack
  - Attacker compromised AWS WAF role,
  - Attacker was able to use AWS WAF role to make requests to other S3 AWS buckets to pull information
- Proper logging helped catch the attacker

References

1. https://owasp.org/www-project-top-ten/
2. https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html
3. https://martinfowler.com/articles/web-security-basics.html
4. https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards
5. https://attack.mitre.org/
6. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
7. https://online.husson.edu/software-development-cycle/
8. https://owasp.org/www-project-secure-headers/
9. https://developers.google.com/web/fundamentals/security/csp
10. https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP

References

11. https://www.youtube.com/watch?v=DDtM9caQ97I
12. https://www.youtube.com/watch?v=p8CQcF_9280
13. https://www.capitalone.com/facts2019/
14. https://www.justice.gov/usao-wdwa/press-release/file/1188626/download

Questions?