OWASP TBILISI

OWASP Top 10

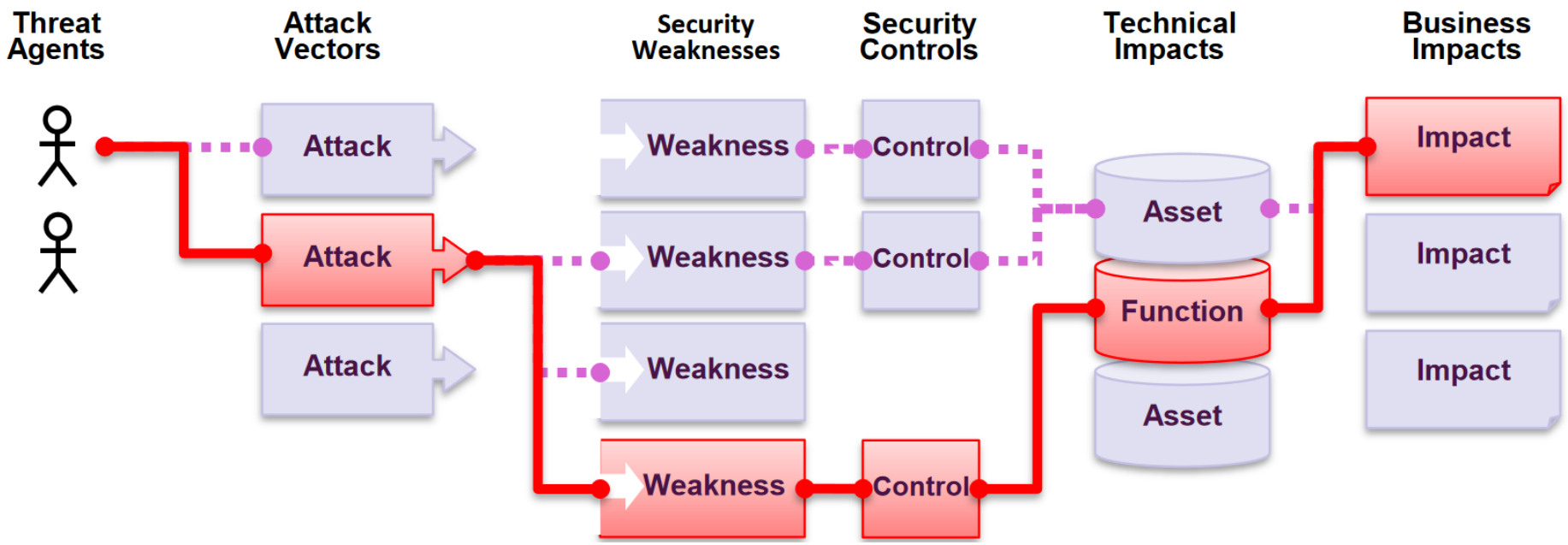
The Ten Most Critical Web Application Security Risks

 /index.php/Tbilisi

 /OWASP-Tbilisi-Chapter

 /OWASP.Tbilisi

Application Security Risks

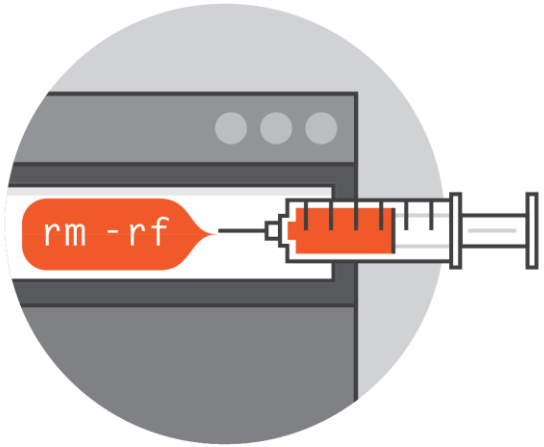


OWASP Top 10 - 2017

A1:2017 – Injection
A2:2017 – Broken Authentication
A3:2017 – Sensitive Data Exposure
A4:2017 – XML External Entities (XXE)
A5:2017 – Broken Access Control
A6:2017 – Security Misconfiguration
A7:2017 – Cross-Site Scripting (XSS)
A8:2017 – Insecure Deserialization
A9:2017 – Using Components with Known Vulnerabilities
A10:2017 – Insufficient Logging & Monitoring

OWASP TBILISI

A1:2017 - Injection



OS: https://website.com/status?productID=381**; ls**

SQL: String query = "SELECT * FROM accounts WHERE custID='" + **request.getParameter("id")** + "'";

XPath: FindUserXPath = "//Employee[UserName/text()='" + **Request("Username")** + "' And Password/text()='" + **Request("Password")** + "']";

admin**' or 1=1**

OWASP TBILISI

A2:2017 - Broken Authentication

SessionID in URL: https://website.com/login.jsp?**sessid=a1b2c3d4**

Default Username / Password: **Admin / Admin**

Weakly Hashed Password: **MD5("password")**

Ineffective Forgot-Password Processes: **“ What’s your Mother’s maiden name? ”**

No 2FA:

OWASP TBILISI

A3:2017 - Sensitive Data Exposure

Data Transmitted in Clear Text: **HTTP**, **SMTP**, **FTP**

Backups in Accessible Location: https://website.com/**backup.tar.gz**

Storing Unnecessary Data: **Credit card info**; **Plain text passwords**

OWASP TBILISI

A4:2017 - XML External Entities (XXE)

Extract Data:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [
   <!ELEMENT foo ANY >
   <!ENTITY xxe SYSTEM "file:///etc/passwd">
]>
<foo>&xxe;</foo>
```

Private Network: `<!ENTITY xxe SYSTEM "https://192.168.1.1/private">`

Denial-of-Service Attack: `<!ENTITY xxe SYSTEM "file:///dev/random">`

OWASP TBILISI

A5:2017 - Broken Access Control

Get Any User's Data: https://website.com/accountInfo?**id=1**

Access Admin's Account: https://website.com/profile?**id=1&admin=true**

Ineffective HTTP Methods: **POST**, **PUT**, **DELETE**

OWASP TBILISI

A6:2017 - Security Misconfiguration

Unnecessary Features are Enabled or Installed: Ports, Services, Pages

Default Accounts and Their Passwords Enabled and Unchanged.

Debugging is Enabled in Production Server.

Latest Security Features are Disabled or Not Updated.

OWASP TBILISI

A7:2017 - Cross-Site Scripting (XSS)

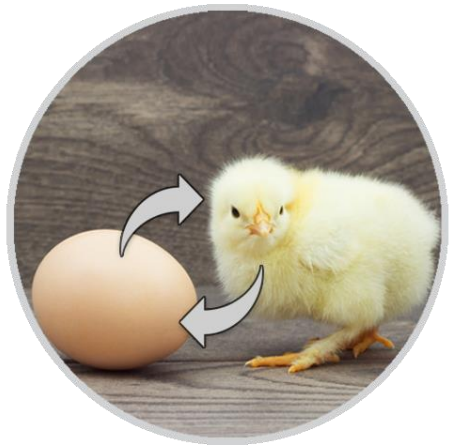
(String) page += "<input name='creditcard' type='text' value='" + **request.getParameter("CC")** + "'>";

Reflected:
Where the malicious string originates from the **victim's request**.

Persistent:
Where the malicious string originates from the **website's database**.

DOM-based:
Where the vulnerability is in the **client-side code**.

A8:2017 - Insecure Deserialization



Serialized Data in Cookie:

a:4:{i:0;i:132;i:1;s:5:"**Alice**";i:2;s:4:"**user**";i:3;s:32:"b6a8b3bea87fe0e0
5022f8f3c88bc960";}

Changed Serialized Data:

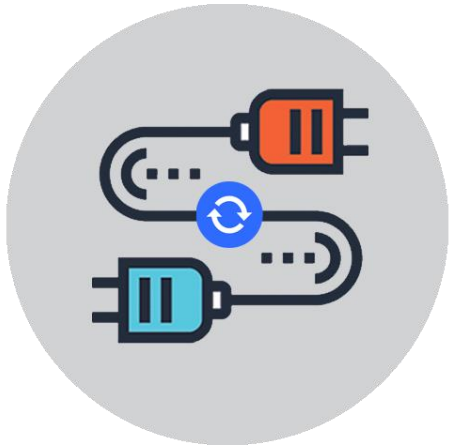
a:4:{i:0;i:132;i:1;s:5:"**Alice**";i:2;s:5:"**admin**";i:3;s:32:"b6a8b3bea87fe0
e05022f8f3c88bc960";}

Result:

```
array (
  0 => 132,
  1 => 'Alice',
  2 => 'admin',
  3 => 'b6a8b3bea87fe0e05022f8f3c88bc960',
)
```

OWASP TBILISI

A9:2017 - Using Components with Known Vulnerabilities



Remove Unused Dependencies, Unnecessary Features, Components, Files, and Documentation.

Stop Using Unmaintained and Outdated Version of the Components.

Only Obtain Components From Official Sources.

Continuously Monitor Sources Like CVE and NVD for Vulnerabilities in the Components.

OWASP TBILISI

A10:2017 - Insufficient Logging & Monitoring

Auditable Events, such as Logins, Failed Logins, and High-value Transactions are Not Logged.

Logs of Applications and APIs are Not Monitored for Suspicious Activity.

Logs are Only Stored Locally.

Penetration Testing and Scans Do Not Trigger Alerts.

Application is Unable to Detect, Escalate, or Alert for Active Attacks in Real Time or Near Real Time.

What's Next for :

- Developers
- Security Testers
- Organizations
- Application Managers

OWASP TBILISI

OWASP TBILISI

Questions ?

Thank you.

 /index.php/Tbilisi

 /OWASP-Tbilisi-Chapter

 /OWASP.Tbilisi