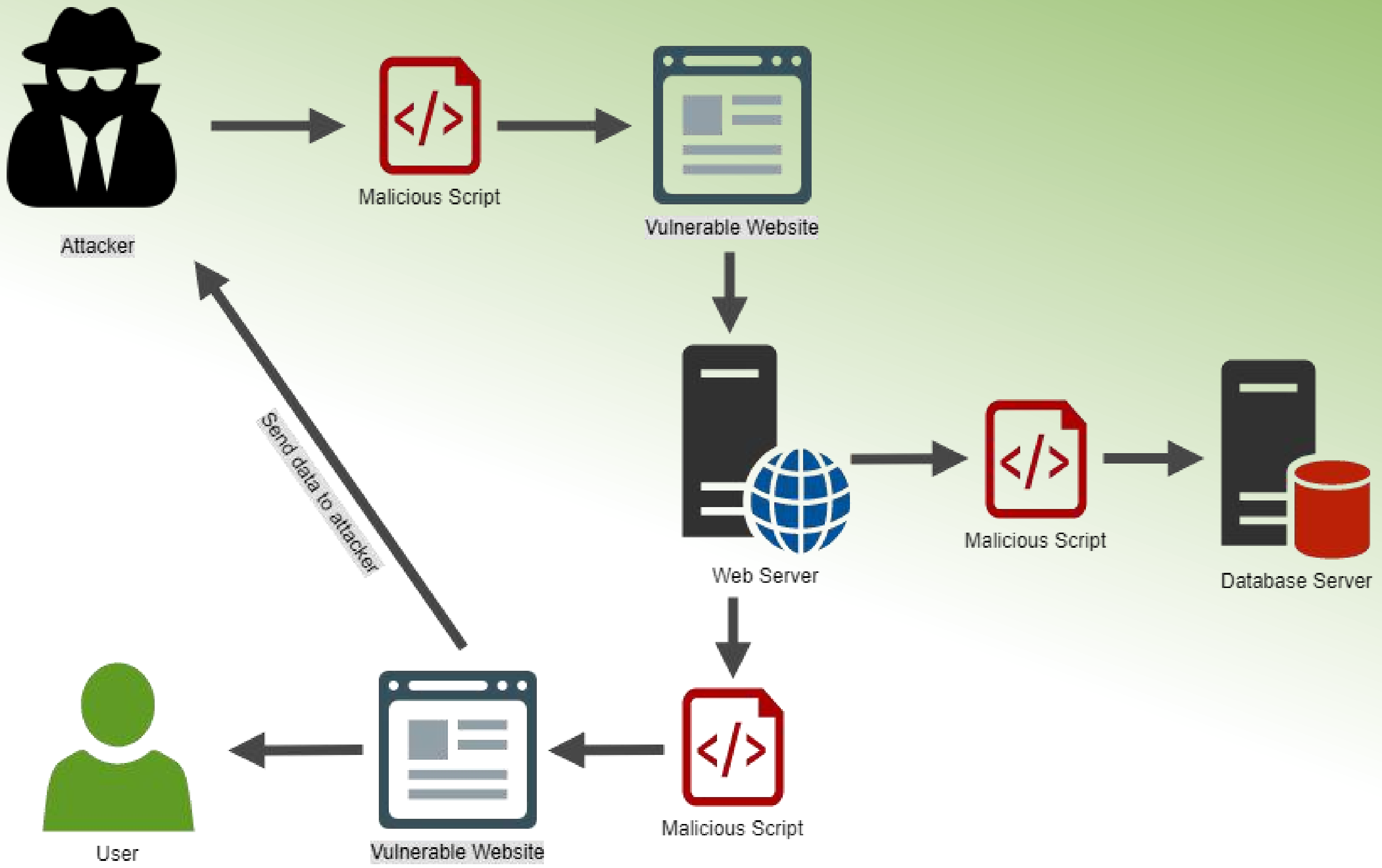
Ethics in IT

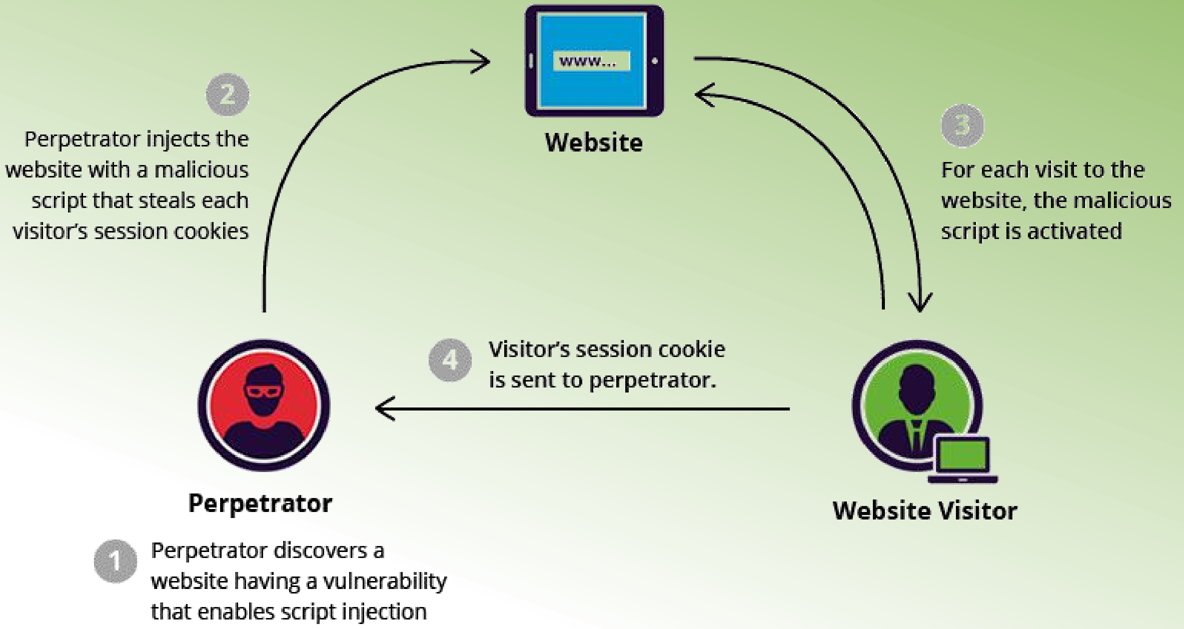
Class X
lab 4

Cross-Site Scripting



XSS Attack

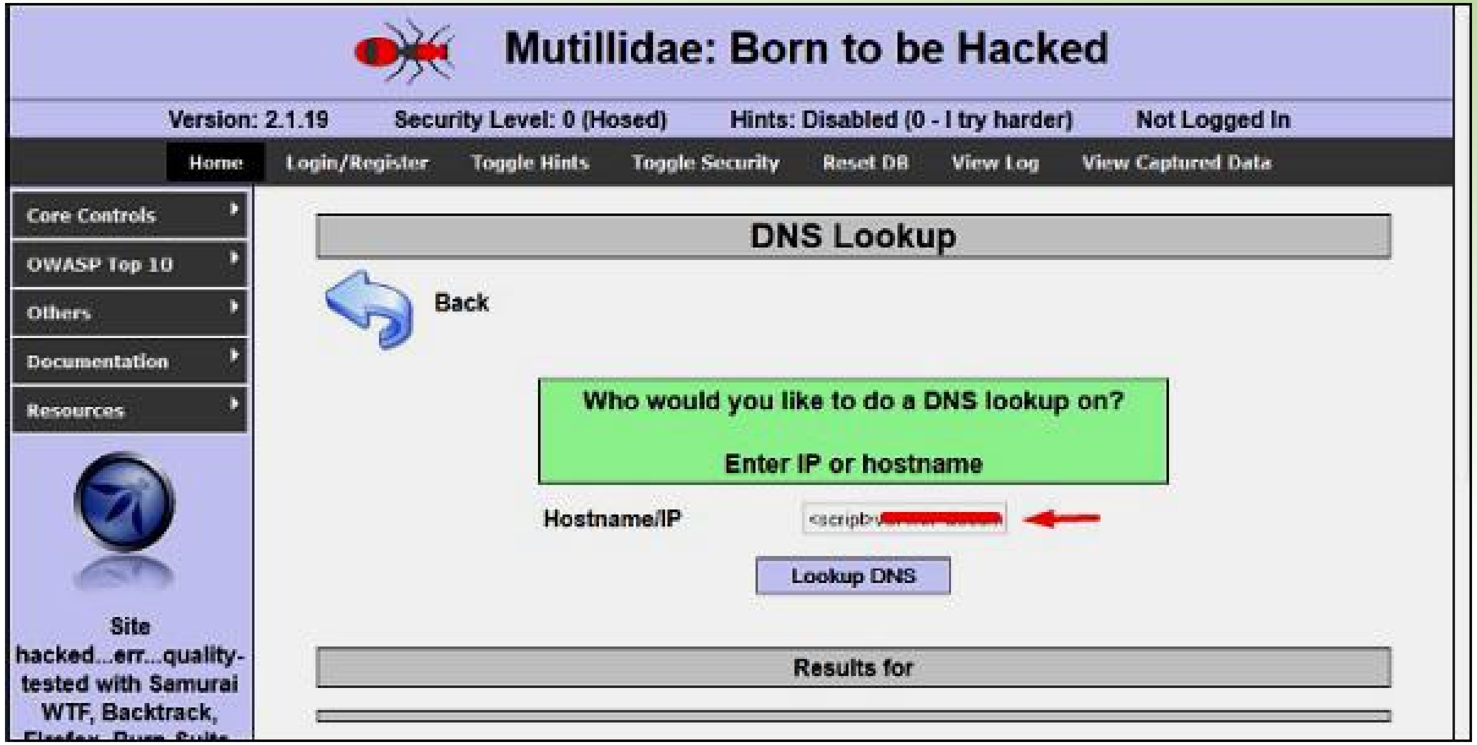
XSS enables attackers to inject client-side scripts into web pages viewed by other users


www...
Website
2
Perpetrator injects the website with a malicious script that steals each visitor's session cookies
3
For each visit to the website, the malicious script is activated
4
Visitor's session cookie is sent to perpetrator.
Perpetrator
Website Visitor
1
Perpetrator discovers a website having a vulnerability that enables script injection

UNITED TRUST

bdeducation
Bangladesh Digital Education Research Limited
সময়ের পাঠশালা

XSS Example



Mutillidae: Born to be Hacked

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

DNS Lookup

Who would you like to do a DNS lookup on?

Enter IP or hostname

Hostname/IP <script>[redacted]

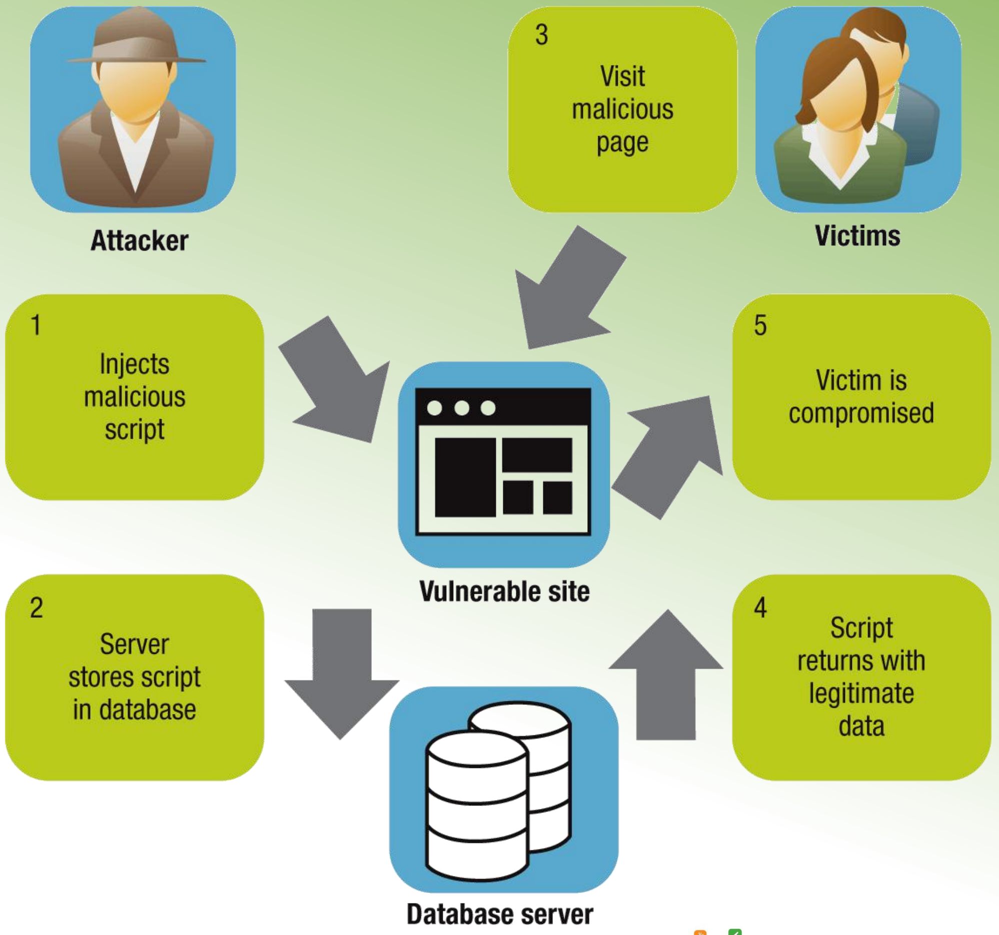
Results for

Site hacked...err...quality-tested with Samurai WTF, Backtrack,

```
<script>
   alert(‘I am Vulnerable’)
</script>
```

Types of XSS Attacks

1. Persistent XSS
2. Reflected XSS
3. DOM-based XSS



UNITED TRUST

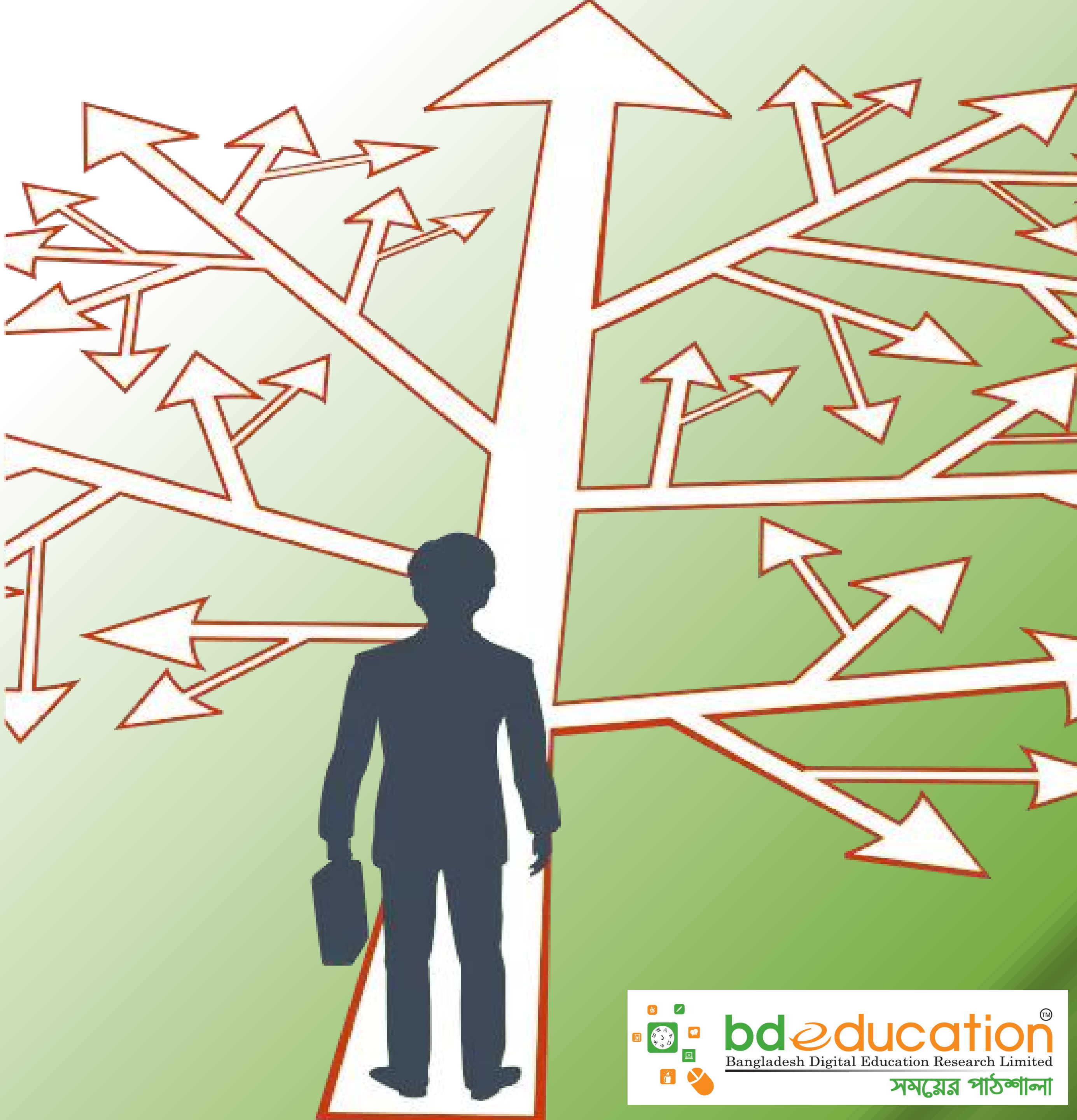
bdeducation
Bangladesh Digital Education Research Limited
সময়ের পাঠশালা

SQL Injection

SQL injection is a set of SQL commands that are placed in a URL string or in data structures in order to retrieve a response

SQL Injection Tools

SQLMAP
SQL NInja
JSQL Injection



UNITED
TRUST

bdeducation™
Bangladesh Digital Education Research Limited
সময়ের পাঠশালা