TEKsystems
Own change

TEKsystems Global Services

Introduction to Security Testing

Presented by: **Santosh Patra**

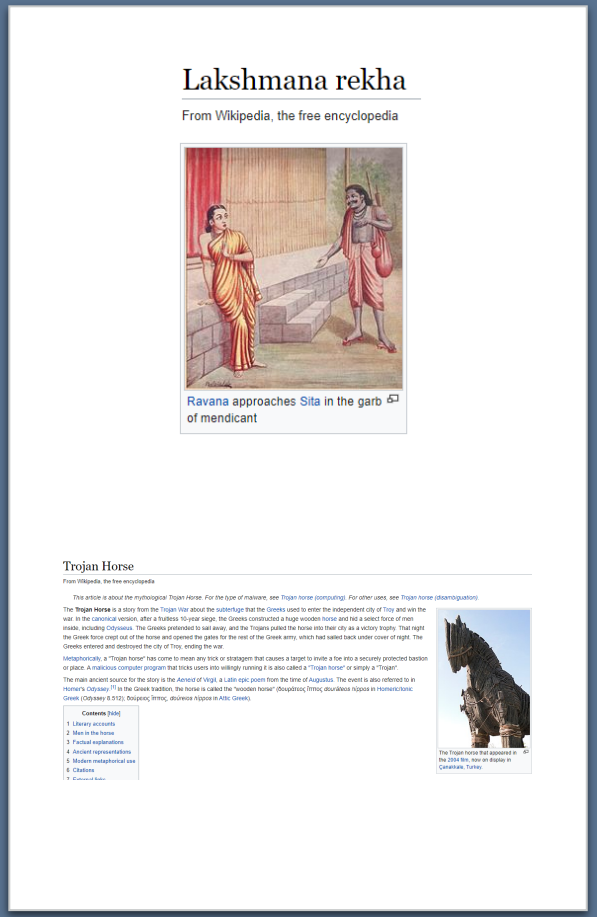
Date of Presentation:
August 17, 2020

TEKsystems | DIGITAL

Agenda

- WHAT IS SECURITY TESTING?
- HISTORY OF SECURITY
- WHY SECURITY TESTING IS IMPORTANT
- WHAT ARE TOOLS AND TECHNIQUES OF SECURITY TESTING.
- WHAT DOES A SECURITY TESTER DO?
- TEK SECURITY PROCESS
- HOW WE DELIVER
- QUESTIONS

What is **SECURITY**



Lakshmana rekha

From Wikipedia, the free encyclopedia

Ravana approaches Sita in the garb of mendicant

Trojan Horse

From Wikipedia, the free encyclopedia

This article is about the mythological Trojan Horse. For the type of malware, see Trojan horse (computing). For other uses, see Trojan horse (disambiguation).

The **Trojan Horse** is a story from the Trojan War about the subterfuge that the Greeks used to enter the independent city of Troy and win the war. In the canonical version, after a fruitless 10-year siege, the Greeks constructed a huge wooden horse and hid a select force of men inside, including Odysseus. The Greeks pretended to sail away, and the Trojans pulled the horse into their city as a victory trophy. That night the Greek force crept out of the horse and opened the gates for the rest of the Greek army, which had sailed back under cover of night. The Greeks entered and destroyed the city of Troy, ending the war.

Metaphorically, a "Trojan horse" has come to mean any trick or stratagem that causes a target to invite a foe into a securely protected bastion or place. A malicious computer program that tricks users into willingly running it is also called a "Trojan horse" or simply a "Trojan".

The main ancient source for the story is the *Aeneid* of Virgil, a Latin epic poem from the time of Augustus. The event is also referred to in Homer's *Odyssey*.[1] In the Greek tradition, the horse is called the "wooden horse" (δουράτειος ἵππος *douráteios híppos* in Homeric/Ionic Greek (*Odyssey* 8.512); δούρειος ἵππος, *doúreios híppos* in Attic Greek).

Contents [hide]

1 Literary accounts
2 Men in the horse
3 Factual explanations
4 Ancient representations
5 Modern metaphorical use
6 Citations

The Trojan horse that appeared in the 2004 film, now on display in Çanakkale, Turkey

History of security

- From Ramayana to Ancient Greeks, there are instances where security was breached by hackers.

- On the left the first pictures depicts the incident from Ramayana where Ravan hacks into Sita's home by luring her out of the Lakshman Rekha.
- The second picture is where the city of Troy was invaded using a Horse shaped figure in which fighters were hiding.

What is
SECURITY TESTING

Methodologies/ Approach / Techniques for Security Testing

In security testing, different methodologies are followed, and they are as follows:

- **Tiger Box**: This hacking is usually done on a laptop which has a collection of OSs and hacking tools. This testing helps penetration testers and security testers to conduct vulnerabilities assessment and attacks.
- **Black Box**: Tester is authorized to do testing on everything about the network topology and the technology.
- **Grey Box**: Partial information is given to the tester about the system, and it is a hybrid of white and black box models.

Security Testing Roles

- Hackers - Access computer system or network without authorization
- Crackers - Break into the systems to steal or destroy data
- Ethical Hacker - Performs most of the breaking activities but with permission from the owner
- Script Kiddies or packet monkeys - Inexperienced Hackers with programming language skill

OWASP top 10 2020

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access control
- Security misconfigurations
- Cross Site Scripting (XSS)
- Insecure Deserialization
- Using Components with known vulnerabilities

OWASP API security top 10 2020

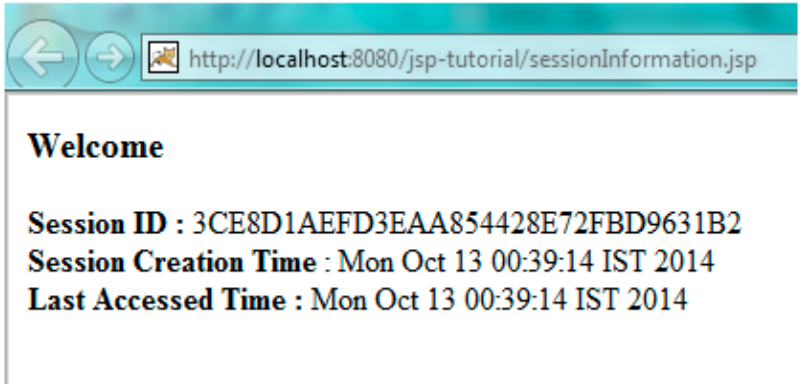
- Broken Object Level Authorization
- Broken User Authentication
- Excessive Data Exposure
- Lack of Resources & Rate Limiting
- Broken Function Level Authorization
- Mass Assignment
- Insufficient Logging & Monitoring

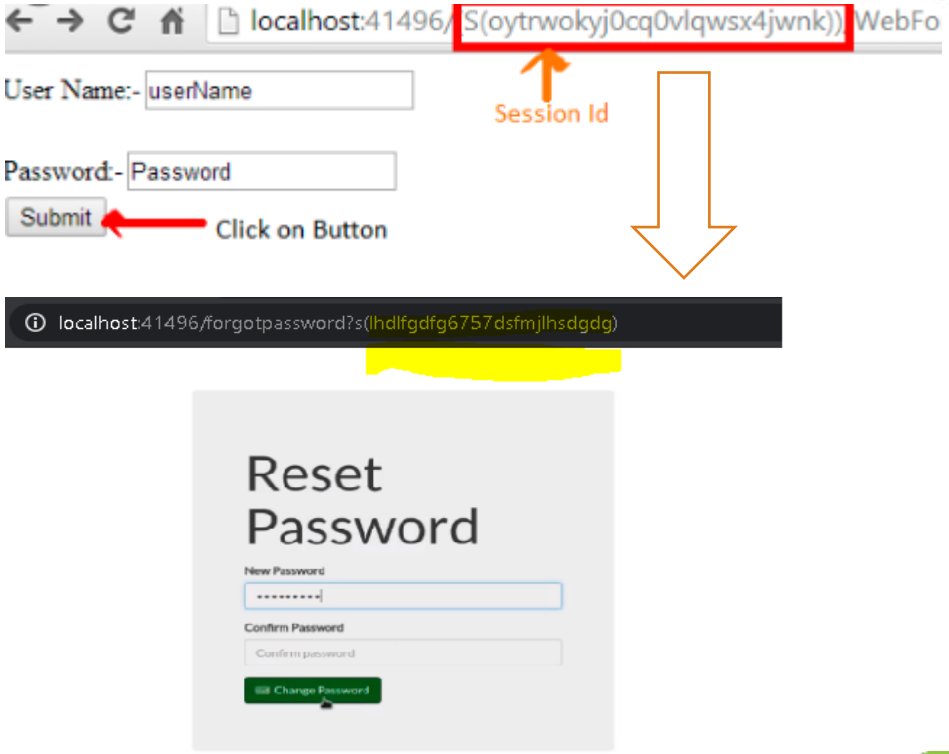
SQL Injection


```
SELECT *
FROM USERS
WHERE email= 'test@test.com'
AND pass = '' OR 1=1--' LIMIT 1
```

Broken Authentication

SESSION Hijacking





The Cisco study also found that 20% of breached organizations lost customers, with 40% of them losing more than 20% of their customer base. As many as 29 % lost revenue and 23% breached organizations lost business opportunities.

Security Testing Tools

1. **Knock Subdomain Scan**
   - Knock is an effective scanning tool to scan Transfer Zone discovery, subdomains, Wildcard testing with an internal or external wordlist. This tool can be very helpful in black box penetration test to find vulnerable subdomains.
   - URL: https://github.com/guelfoweb/knock
2. **Iron Wasp**
   - It is a GUI-based powerful scanning tool which can check over 25 kinds of web vulnerabilities. It can detect false positives and false negatives. It is built on Python and Ruby and generates HTML and RTF reports.
   - URL: https://ironwasp.org/
3. **HP Webinspect**
   - It is an automated dynamic application security testing (DAST) tool that mimics real-world hacking techniques and attacks and provides comprehensive dynamic analysis of complex web applications and services.
   - URL: http://www8.hp.com/in/en/software-solutions/webinspect-dynamic-analysis-dast/
4. **Google Nogotofail**
   - It is a network traffic security testing tool. It checks applications for known TLS/SSL vulnerabilities and misconfigurations. It scans SSL/TLS encrypted connections and checks whether they are vulnerable to man-in-the-middle (MiTM) attacks. It can be set up as a router,

Example Test Scenarios for Security Testing:

Sample Test scenarios to give you a glimpse of security test cases -

- A password should be in encrypted format
- Application or System should not allow invalid users
- Check cookies and session time for application
- For financial sites, the Browser back button should not work.

Security testing vs pen testing

Security testing mostly refers to a software functionality and it's behavior, how the program behaves in the presence of the attack when software launched into use, and if a leakage of information occurs, how it measures with major principles of security: confidentiality, integrity, authentication, including availability, authorization and non-repudiation. Security of network is provided via architecture where baseline is established for network traffic to detect anomalous behavior. Firewalls and intrusion detection systems along with proper training of users on cyber security threats is, collectively, security.

Penetration testing, or we call it pentest, refers to the POA - point of access, identification of weaknesses in the network (such as ports), firewalls, servers, routers, switches, internal and web applications, mobile devices. Pentest is usually automated process, able to identify vulnerabilities giving a gateway to be potentially exploited by hackers.

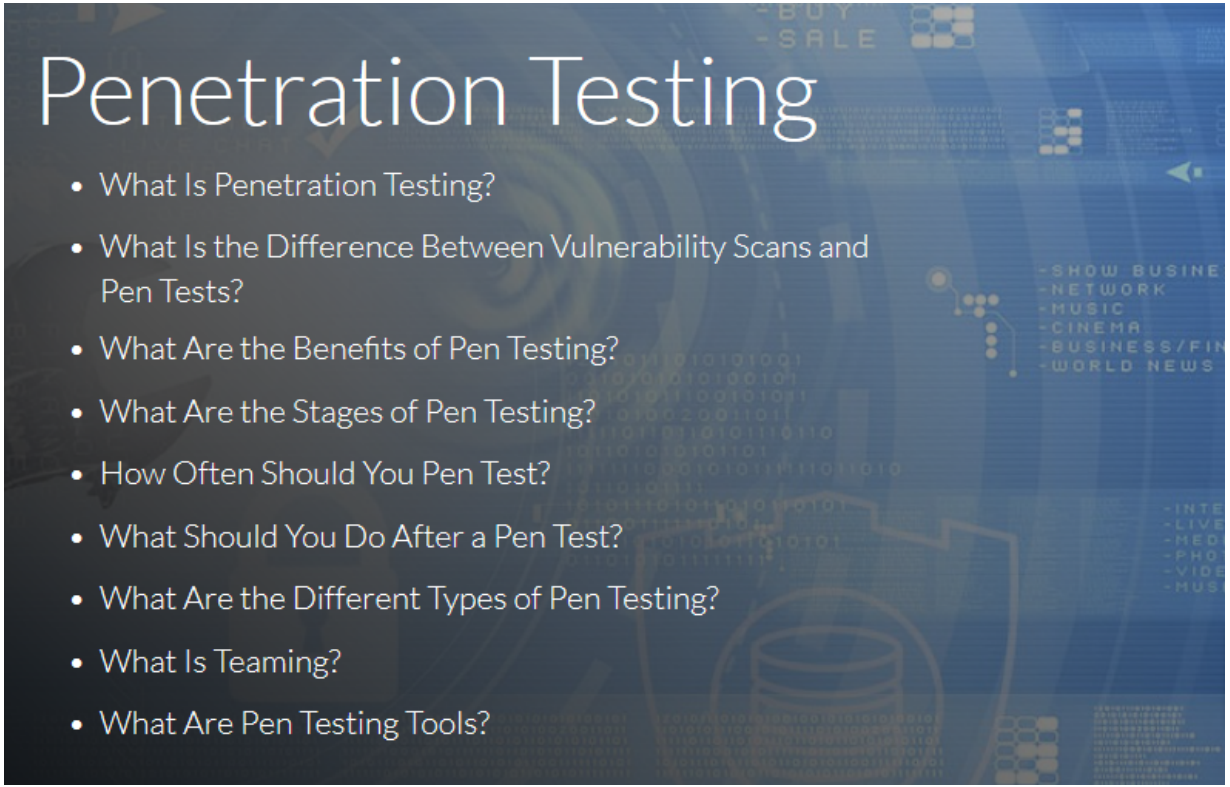


Image courtesy - https://www.coresecurity.com

What's next …
Explore some tools.
All the best.

TEKsystems
Own change

THANK YOU