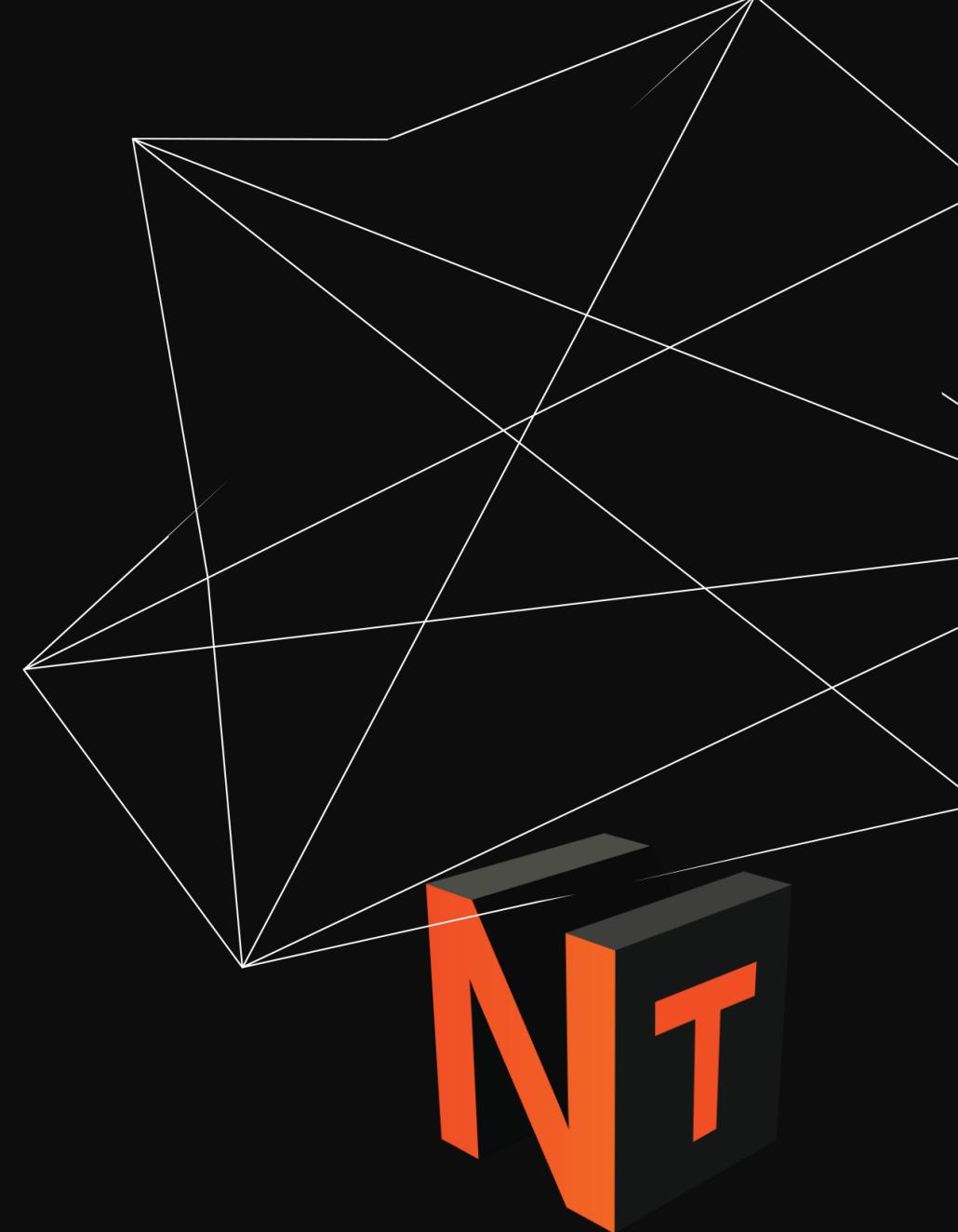


Ko se heker in razvijalec srečata na virtualni kavi

Milan Gabor
Gregor Spagnolo

#ntk18



Heker

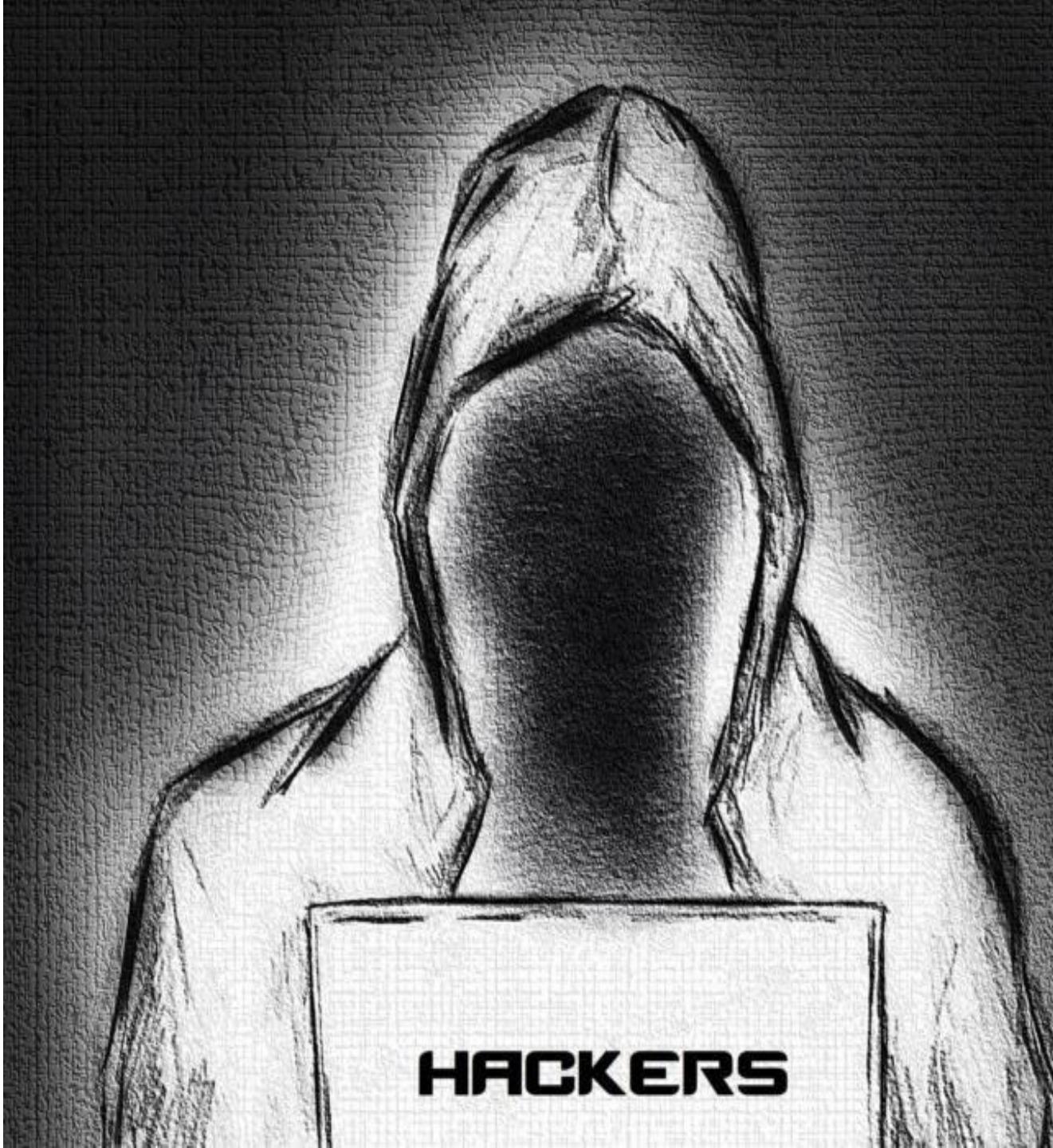
Ni razvijalec

Rad razbija stvari

Posebej rad ima nevešče razvijalce



#ntk18



Orodja

Kali Linux



#ntk18



Razvijalec

G33k

Latest&Gratest

Ni še bil na izobraževanju s tega področja



#ntk18



“THE FULL STACK DEVELOPER”

(no other developers required)

Orodja

Visual studio

Git

Docker

Linux



#ntk18

The screenshot shows the Microsoft Visual Studio interface with the title bar "CustomCompareValidator (Debug|Any CPU) - Microsoft Visual Studio (Administrator)". The main window displays the code for "CompareValidator.cs" located in the namespace "Wallace.Web.ControlsValidators". The code implements a custom validator for comparing two input controls. It includes properties for the control to compare and whether it's embedded in an Ajax panel, along with methods for validation and rendering.

```
1  using System;
2  using System.ComponentModel;
3  using System.Web.UI;
4  using System.Web.UI.WebControls;
5
6  [assembly: WebResource("Wallace.Web.ControlsValidators.Resources")]
7  namespace Wallace.Web.ControlsValidators
8  {
9      /// <summary>
10     /// Allows to compare input controls value without case-sensitive comparison
11     /// </summary>
12     [ToolboxData("<{0}>:CompareValidator runat=\"server\" />")]
13     [DefaultProperty("Name")]
14     public sealed class CompareValidator : BaseValidator
15     {
16         private static readonly string _scriptBlockKey = "CompareValidator_" + Guid.NewGuid();
17         private string _controlToValidateClientID;
18         private string _controlToCompareClientID;
19
20         /// <summary>
21         /// The control you want to compare with
22         /// </summary>
23         public string ControlToCompare
24         {
25             get;
26             set;
27         }
28
29         /// <summary>
30         /// Set this property to true when the control is in an Ajax panel
31         /// </summary>
32         public bool EmbeddedInAjaxPanel
33         {
34             get;
35             set;
36         }
37
38         protected void Page_Load(object sender, EventArgs e)
39         {
40             if (!IsPostBack)
41             {
42                 ControlToCompare = null;
43                 EmbeddedInAjaxPanel = false;
44             }
45         }
46
47         protected void ControlToCompare_Changed(object sender, EventArgs e)
48         {
49             ControlToCompare = ((Control)sender).ID;
50         }
51
52         protected void Page_PreRender(object sender, EventArgs e)
53         {
54             if (ControlToCompare != null)
55             {
56                 string controlID = ControlToCompare;
57                 if (controlID == null || controlID == string.Empty)
58                     return;
59
60                 string clientID = ClientIDForControl(controlID);
61                 if (clientID == null)
62                     return;
63
64                 string validateClientID = ClientIDForControl(_controlToValidateClientID);
65                 if (validateClientID == null)
66                     return;
67
68                 string compareClientID = ClientIDForControl(_controlToCompareClientID);
69                 if (compareClientID == null)
70                     return;
71
72                 string scriptBlock = string.Format("function {0}_OnCompare() {{ var validateValue = document.getElementById('{1}'); var compareValue = document.getElementById('{2}'); if (validateValue.value != compareValue.value) {{ validateValue.className = 'invalid'; compareValue.className = 'invalid'; }} else {{ validateValue.className = 'valid'; compareValue.className = 'valid'; }} }}", _scriptBlockKey, validateClientID, compareClientID);
73
74                 string script = string.Format("{{ id: '{0}', type: 'script', text: '{1}' }}", _scriptBlockKey, scriptBlock);
75
76                 ScriptManager.RegisterClientScriptBlock(this, this.GetType(), _scriptBlockKey, script, true);
77             }
78         }
79
80         protected void ControlToValidate_Changed(object sender, EventArgs e)
81         {
82             ControlToValidate = ((Control)sender).ID;
83         }
84
85         protected void Page_LoadComplete(object sender, EventArgs e)
86         {
87             if (ControlToValidate != null)
88             {
89                 string validateClientID = ClientIDForControl(ControlToValidate);
90                 if (validateClientID == null)
91                     return;
92
93                 string validateValue = string.Format("{{ id: '{0}', type: 'text', value: '{1}' }}", validateClientID, ControlToValidate);
94
95                 ScriptManager.RegisterClientScriptBlock(this, this.GetType(), validateClientID, validateValue, true);
96             }
97         }
98
99         protected void ControlToCompare_PreRender(object sender, EventArgs e)
100        {
101            ControlToCompare = null;
102        }
103    }
104}
```

Aplikacije

Velika množica pregledanih aplikacij

Veliko ponavljačih se napak

Niso odvisne od tehnologije

Copy paste

Roki



#ntk18



O aplikaciji

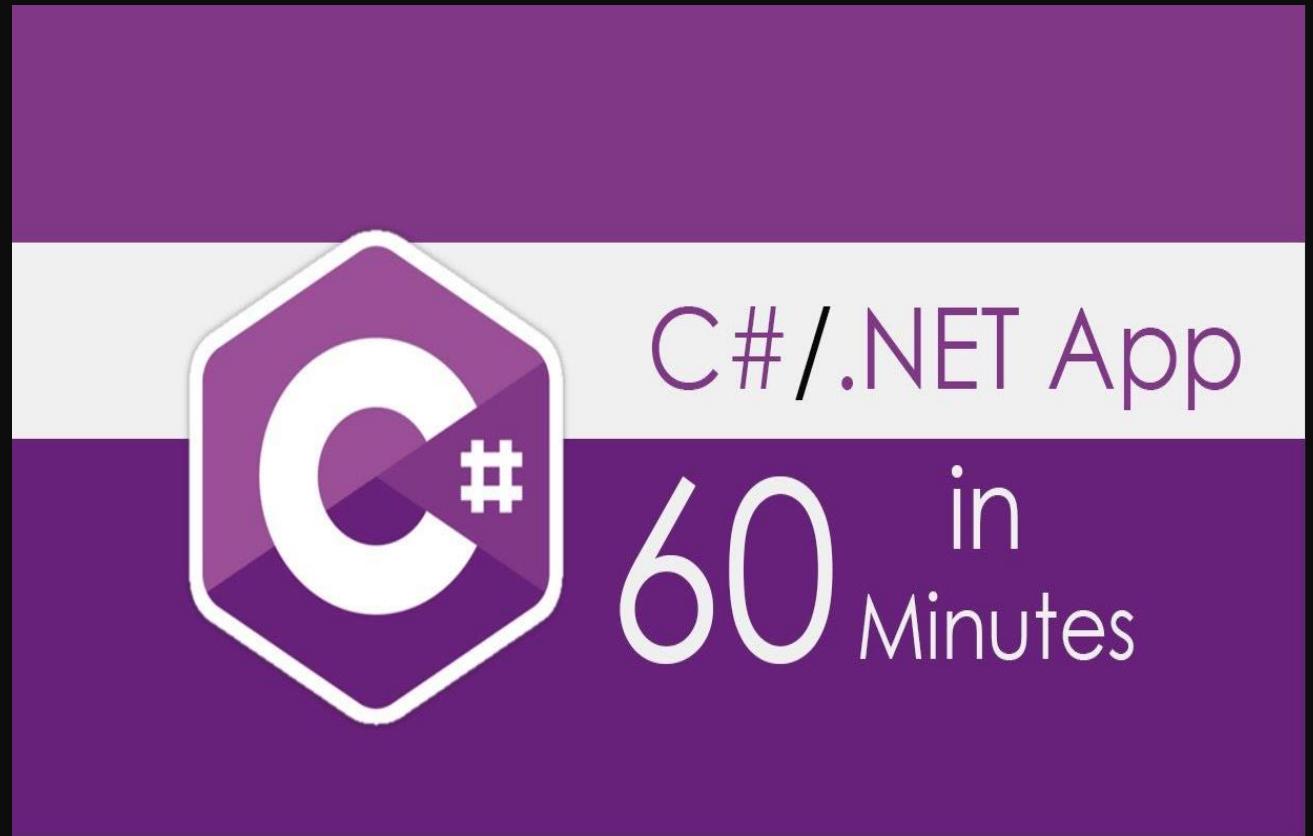
.Net Core

Jquery

API

Docker build

Git SC



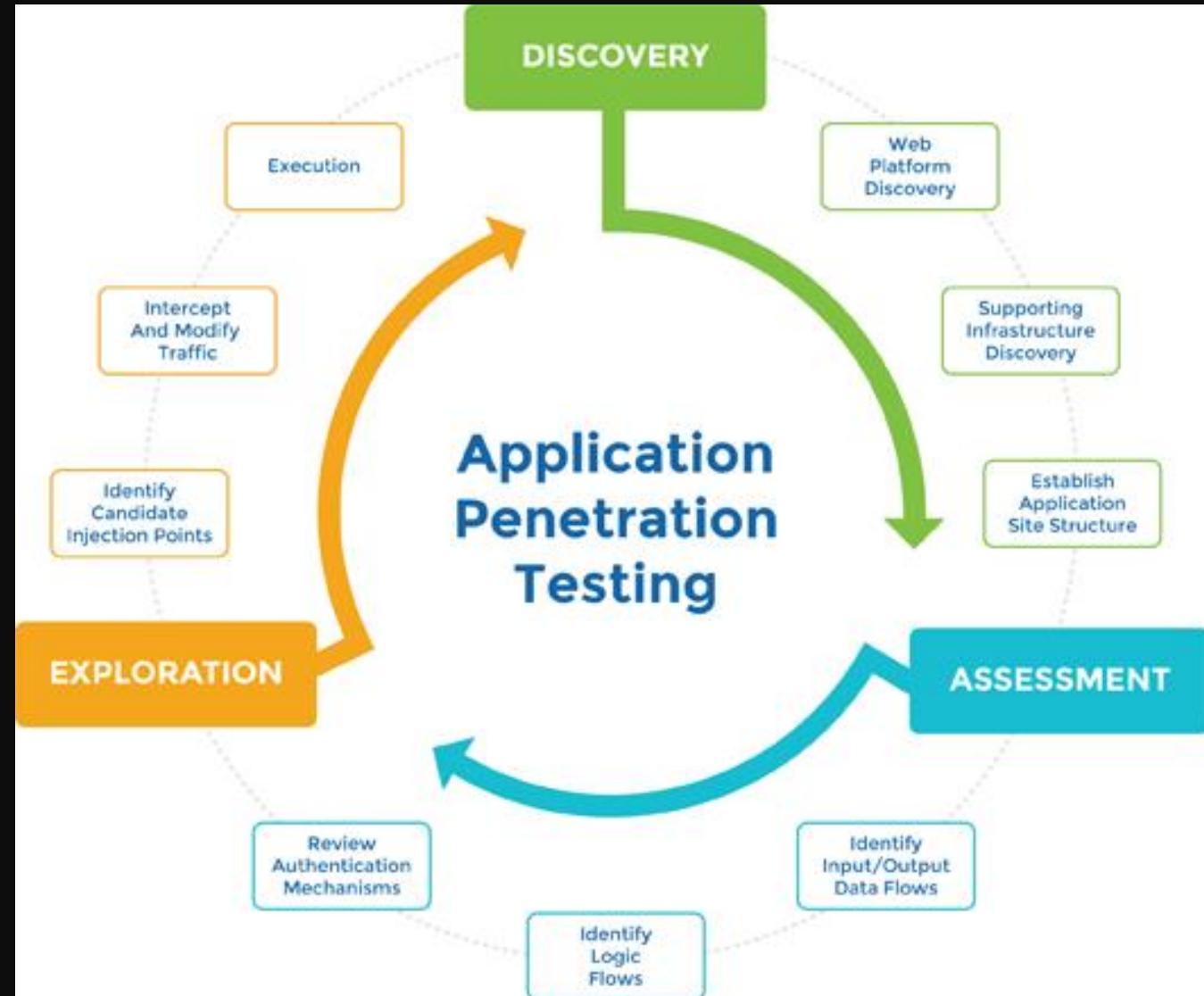
#ntk18



Virtual
Coffee
Date

Faze

1. OSINT
2. Avtomatska analiza
3. Analiza in identifikacija
4. Kraja podatkov, razmaličenje, ...
5. Izkoriščanje



OSINT

Google

Shodan

Drugi iskalniki



#ntk18

1

Aktivno skeniranje

Nikto

OWASP ZAP

Burp

Drugi namenski skenerji in proksiji



Aktivno izkoriščanje

OWASP TOP 10

OWASP Testing metodologija

Druge aktivnosti na podlagi izkušenj

Včasih nujne nore ideje



Najdene stvari

- git
- swagger
- auth controller logging passwords
- APITransaction -> brez autorizacije
- Logs (exposed)
- transaction create stored XSS
- transaction create senderId se lahko spreminja
- search sql injection



OWASP

- Open Web Application Security Project
 - Odprta skupnost
 - Neprofitna organizacija
- Glavni cilj
 - Varna programska oprema
- <https://www.owasp.org>



OWASP TOP 10

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)	X	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	X	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]



Primer: OWASP Security Shepherd

The screenshot shows a web-based security training application. On the left, a sidebar lists navigation options: Open and Close Modules, Open or Close by Category, View Feedback, View Progress, and User Management. Below these are tabs for Scoreboard, Field Training, Private, Corporal, Sergeant, Lieutenant, and Major. The Private tab is currently selected. The main content area displays a challenge titled "SQL Injection". It includes a detailed description of how parameters are concatenated into SQL queries, a note about escaping strings with apostrophes, and a search form where users can enter a user name. A sample SQL query is provided: `SELECT * FROM tb_users WHERE username = 'jim' OR 1=1;`. A "Get this user!" button is present. Below the search form, a "Search Results" section lists user data:

User Id	User Name	Comment
12345	user	Try Adding some SQL Code
12346	OR 1 = 1	Your Close, You need to escape the string with an apostrophe so that your code is interpreted
12543	Fred Mtenzi	A lecturer in DIT Kevin Street
14232	Mark Denihan	This guy wrote this application
61523	Cloud	Has a Big Sword
82642	qwldshs@ab	Lesson Completed. The result key is 3c17f6bf34080979e0cebda5672e989c07ceec9fa4ee7b7c17c9e3ce26bc63e0



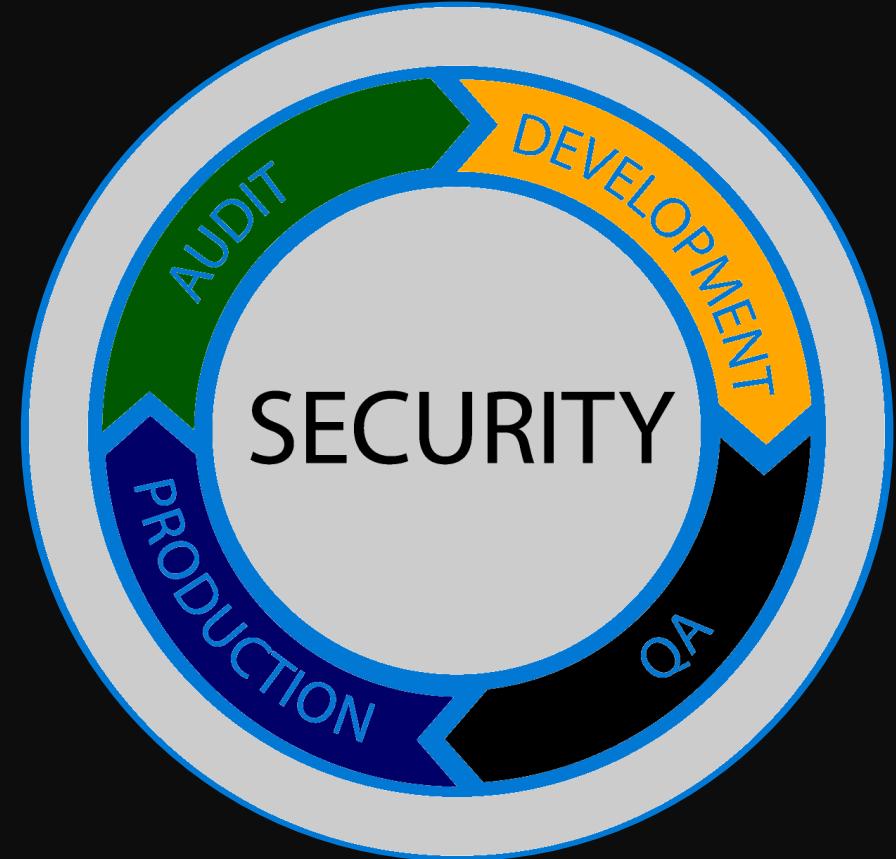
Priporočila za varnejše spletnne Aplikacije

- Sistem
 - Popravki
 - Ustrezne verzije
 - Nadzor
 - Odstranitev nepotrebnih aplikacij
- Aplikacije
 - Zadnja verzija?
 - Nepotrebni moduli?
 - Izveden pregled ali vsaj avtomatski sken?



Kako zaščiti aplikacije/sisteme

- Vgraditi varnost v cel življenjski cikel
 - Uporabiti varnostne principe v vseh fazah in aktivnostih
- Izobraževanje
 - Zavedanje se potencialnih napadov
 - Pošiljanje ljudi na različne izobraževanja (tudi NTK šteje)



Izobraževati

- **Razvijalce** – Najboljše prakse iz varnega razvoja SW
- **Testerje** – Metode za identifikacijo ranljivosti
- **Varnostne inženirje** – Proces varnega razvoja SW
- **Lastnike, menedžment** – Razumeti tveganja in zakaj je to sploh pomembno za varnost spletnih aplikacij

Ustrezna kombinacija

Sharing is caring

Skupaj za istim ciljem



#ntk18



{ THE SECURE } DEVELOPER

Varno programiranje

Seznanitev s tipičnimi napakami

Uporaba zadnjih tehnologij

Za noobs in seniors

Kombinacija napada in obrambe

Developer + Hacker



#ntk18



thank you

děkuji gracie fiik
gracie sobodi akpé tänan mèsi
dankie

merci choukrane aciuy
trugéré go chai dhanyavadagalu
murakoze

blagodaria dank grazie
chnorakaloutioun deh-ku-yih tzu
tanemirt tesekkur khob trugarez

tenki kasih xie
eskerrik arigató terima edirem

gracias paldies agat kié
dahn-kah faleminderit

gratias kyay hvala fyri
mehr-see ef-har-rih-stowe dhanyabaad
syeh-syeh hamnida shoe-krahn
köszönöm dahn-kee dankewol
agimus aabhar gràcies
salamat salamat
kiitos

takk shoo-kree-a
wel ago sag
shukran sukria vianka
mahalo kamsah Barak
danke cox toda asko
tin Allahu maith