

1.

a) Ca să analizați/testați securitatea aplicației, ajuta să gândiți ca un atacator.

ADEVARAT

b) Pentru că sunt foarte multe, din punct de vedere al logicii/design-ului aplicației, nu încercați să acoperiți toate cazurile posibile pentru a preveni un comportament neașteptat. **FALS**

c) Întotdeauna validați câmpurile de input, atât ca format (tip de date, protejare împotriva SQL injection, etc.) dar și ca valori (dimensiuni, valori minime/maxime, verificări între diferite câmpuri de input; ex. data de început a unei activități anterioară datei de final, prețurile să aibă valori pozitive, etc.) **ADEVARAT**

d) Aveți în vedere vulnerabilități de tip buffer overflow. **ADEVARAT**

e) În general nu e o practică bună să stocați log-uri, pentru că ocupă spațiu și cresc timpul de așteptare al utilizatorului. **FALS**

f) Oferiți cât mai multe detalii posibile utilizatorilor când eșuează autentificarea prin username și parolă sau când implementați mecanisme de recuperare a parolei pentru a facilita accesul acestora (spre exemplu menționați „Adresa de e-mail nu corespunde unui cont activ” la încercarea de a recupera parola prin e-mail). **FALS**

g) Dacă folosiți baze de date, în mod normal la ștergerea unei înregistrări folosiți DELETE, pentru a nu mai păstra nicio urmă a acestora (afirmația nu face referire la ștergerea permanentă a unor date personale, conform GDPR [1]). **FALS**

h) Nu rețineți parole în clar. **ADEVARAT**

i) Hardcodeați parole în cod. **FALS**

2. -> trebuie sa fie validata adresa de email (sa fie o adresa valida)

-> adresa de email trebuie sa fie unica (sa nu existe deja un alt utilizator inregistrat cu aceeași adresa de email)

```
manager.UserValidator = new UserValidator<ApplicationUser>(manager)
{
    AllowOnlyAlphanumericUserNames = false,
    RequireUniqueEmail = true
};
```

-> sa aiba o parola puternica (sa contina majuscule, cifre si caractere speciale)

```
// Configure validation logic for passwords
manager.PasswordValidator = new PasswordValidator
{
    RequiredLength = 6,
    RequireNonLetterOrDigit = true,
    RequireDigit = true,
    RequireLowercase = true,
    RequireUppercase = true,
};
```

```
//
// POST: /Account/Register
[HttpPost]
[AllowAnonymous]
[ValidateAntiForgeryToken]
0 references
public async Task<ActionResult> Register(RegisterViewModel model)
{
    if (ModelState.IsValid)
    {
        var user = new ApplicationUser { UserName = model.Email, Email = model.Email };
        var result = await UserManager.CreateAsync(user, model.Password);
        if (result.Succeeded)
        {
            await SignInManager.SignInAsync(user, isPersistent:false, rememberBrowser:false);

            // For more information on how to enable account confirmation and password reset please visit https://go.microsoft.com/fwlink/?LinkID=320771
            // Send an email with this link
            // string code = await UserManager.GenerateEmailConfirmationTokenAsync(user.Id);
            // var callbackUrl = Url.Action("ConfirmEmail", "Account", new { userId = user.Id, code = code }, protocol: Request.Url.Scheme);
            // await UserManager.SendEmailAsync(user.Id, "Confirm your account", "Please confirm your account by clicking <a href=\"" + callbackUrl + "\">here</a>");

            return RedirectToAction("Index", "Home");
        }
        AddErrors(result);
    }

    // If we got this far, something failed, redisplay form
    return View(model);
}
```

Register.

Create a new account.

Email

Password

Confirm password

3. -> se verifica faptul ca exista contul

```
//
// GET: /Account/Login
[AllowAnonymous]
0 references
public ActionResult Login(string returnUrl)
{
    ViewBag.ReturnUrl = returnUrl;
    return View();
}

//
// POST: /Account/Login
[HttpPost]
[AllowAnonymous]
[ValidateAntiForgeryToken]
0 references
public async Task<ActionResult> Login(LoginViewModel model, string returnUrl)
{
    if (!ModelState.IsValid)
    {
        return View(model);
    }

    // This doesn't count login failures towards account lockout
    // To enable password failures to trigger account lockout, change to shouldLockout: true
    var result = await SignInManager.PasswordSignInAsync(model.Email, model.Password, model.RememberMe, shouldLockout: false);
    switch (result)
    {
        case SignInStatus.Success:
            return RedirectToLocal(returnUrl);
        case SignInStatus.LockedOut:
            return View("Lockout");
        case SignInStatus.RequiresVerification:
            return RedirectToAction("SendCode", new { ReturnUrl = returnUrl, RememberMe = model.RememberMe });
        case SignInStatus.Failure:
        default:
            ModelState.AddModelError("", "Invalid login attempt.");
            return View(model);
    }
}
```

-> user si parola sa fie corecte

-> mesajele de eroare sa nu fie prea detaliate

Log in.

Use a local account to log in.

Email

admin@gmail.com

Password

.....

☐ Remember me?

Log in

[Register as a new user](#)

4.

-> Daca utilizatorul baga o parola gresita, dar parola respectiva apartine altui utilizator, aplicatia afiseaza carui utilizator ii apartine parola. Trebuie sa ii se spuna utilizatorului doar faptul ca parola pe care a introdus-o nu este cea valida.

-> Rolurile sa nu fie vizibile si editabile decat pentru administrator. Daca acestea sunt editabile de catre toti utilizatorii, un anumit user ar putea sa isi modifice rolul pentru a primi permisiuni in plus.


-> Daca atacatorul a ajuns sa aiba acces la baza de date, isi poate modifica rolul si astfel si permisiunile din aplicatie.


-> Daca atacatorul are acces la baza de date acesta poate modifica parole, roluri si alte date cu caracter personal ale utilizatorilor.



-> Daca aplicatia divulga prea multe informatii, atacatorul ar putea afla daca un anumit utilizator are cont sau nu in aplicatie (daca atunci cand introduci un email, iti spune daca acesta a mai fost folosit sau nu).


5.


Id	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
1,372	1/11/22, 7:03:02 PM	1/11/22, 7:03:02 PM	POST	https://localhost:44367/Account/Register	200	OK	8 ms	462 bytes	3,870 bytes
1,373	1/11/22, 7:03:02 PM	1/11/22, 7:03:02 PM	POST	https://localhost:44367/Account/Register	200	OK	7 ms	462 bytes	3,870 bytes
1,375	1/11/22, 7:03:02 PM	1/11/22, 7:03:02 PM	GET	https://localhost:44367/Account/Login	200	OK	7 ms	625 bytes	4,918 bytes
1,377	1/11/22, 7:03:02 PM	1/11/22, 7:03:02 PM	POST	https://localhost:44367/Account/Register	200	OK	8 ms	462 bytes	3,956 bytes
1,378	1/11/22, 7:03:02 PM	1/11/22, 7:03:02 PM	POST	https://localhost:44367/Account/Login	500	Internal Server Error	6 ms	422 bytes	9,859 bytes
1,379	1/11/22, 7:03:02 PM	1/11/22, 7:03:02 PM	POST	https://localhost:44367/Account/Register	200	OK	7 ms	462 bytes	3,870 bytes
1,380	1/11/22, 7:03:02 PM	1/11/22, 7:03:02 PM	GET	https://localhost:44367/Account/Login	200	OK	6 ms	625 bytes	4,918 bytes
1,383	1/11/22, 7:03:02 PM	1/11/22, 7:03:02 PM	POST	https://localhost:44367/Account/Login	500	Internal Server Error	8 ms	422 bytes	9,859 bytes
1,384	1/11/22, 7:03:02 PM	1/11/22, 7:03:02 PM	POST	https://localhost:44367/Account/Register	200	OK	9 ms	462 bytes	3,956 bytes
1,385	1/11/22, 7:03:02 PM	1/11/22, 7:03:02 PM	POST	https://localhost:44367/Account/Register	200	OK	6 ms	462 bytes	3,870 bytes
1,387	1/11/22, 7:03:02 PM	1/11/22, 7:03:02 PM	GET	https://localhost:44367/Account/Login	200	OK	7 ms	625 bytes	4,918 bytes
1,389	1/11/22, 7:03:02 PM	1/11/22, 7:03:02 PM	POST	https://localhost:44367/Account/Register	200	OK	8 ms	462 bytes	3,956 bytes
1,390	1/11/22, 7:03:02 PM	1/11/22, 7:03:02 PM	POST	https://localhost:44367/Account/Login	500	Internal Server Error	7 ms	422 bytes	9,859 bytes
1,391	1/11/22, 7:03:02 PM	1/11/22, 7:03:02 PM	POST	https://localhost:44367/Account/Register	200	OK	7 ms	462 bytes	3,870 bytes
1,393	1/11/22, 7:03:02 PM	1/11/22, 7:03:02 PM	POST	https://localhost:44367/Account/Register	200	OK	6 ms	462 bytes	3,956 bytes
1,394	1/11/22, 7:03:02 PM	1/11/22, 7:03:02 PM	GET	https://localhost:44367/Account/Login	200	OK	7 ms	625 bytes	4,918 bytes
1,396	1/11/22, 7:03:02 PM	1/11/22, 7:03:02 PM	POST	https://localhost:44367/Account/Register	200	OK	8 ms	462 bytes	3,870 bytes
1,398	1/11/22, 7:03:02 PM	1/11/22, 7:03:02 PM	POST	https://localhost:44367/Account/Login	500	Internal Server Error	7 ms	422 bytes	9,859 bytes
1,399	1/11/22, 7:03:02 PM	1/11/22, 7:03:02 PM	POST	https://localhost:44367/Account/Register	200	OK	7 ms	462 bytes	3,956 bytes
1,400	1/11/22, 7:03:02 PM	1/11/22, 7:03:02 PM	POST	https://localhost:44367/Account/Register	200	OK	5 ms	462 bytes	3,870 bytes
1,402	1/11/22, 7:03:02 PM	1/11/22, 7:03:02 PM	POST	https://localhost:44367/Account/Register	200	OK	8 ms	462 bytes	3,956 bytes
1,403	1/11/22, 7:03:02 PM	1/11/22, 7:03:02 PM	GET	https://localhost:44367/Account/Login	200	OK	8 ms	625 bytes	4,918 bytes
1,405	1/11/22, 7:03:02 PM	1/11/22, 7:03:02 PM	POST	https://localhost:44367/Account/Register	200	OK	7 ms	462 bytes	3,870 bytes
1,406	1/11/22, 7:03:02 PM	1/11/22, 7:03:02 PM	POST	https://localhost:44367/Account/Login	500	Internal Server Error	7 ms	422 bytes	9,859 bytes
1,408	1/11/22, 7:03:02 PM	1/11/22, 7:03:02 PM	POST	https://localhost:44367/Account/Register	200	OK	6 ms	462 bytes	3,956 bytes
1,409	1/11/22, 7:03:02 PM	1/11/22, 7:03:02 PM	GET	https://localhost:44367/Account/Login	200	OK	10 ms	625 bytes	4,918 bytes
1,411	1/11/22, 7:03:02 PM	1/11/22, 7:03:02 PM	POST	https://localhost:44367/Account/Register	200	OK	11 ms	462 bytes	3,870 bytes


 History





 Search



 Alerts 













 Output

 Spider

 Active Scan

  Alerts (12)

- >  Missing Anti-clickjacking Header (4)
- >  Vulnerable JS Library
- >  Application Error Disclosure
- >  Cookie Without Secure Flag (2)
- >  Cookie without SameSite Attribute (2)
- >  Incomplete or No Cache-control Header Set (7)
- >  Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (17)
- >  Timestamp Disclosure - Unix (8)
- >  X-AspNet-Version Response Header (15)
- >  X-Content-Type-Options Header Missing (14)
- >  Information Disclosure - Suspicious Comments (29)
- >  Loosely Scoped Cookie (2)