Windesheim

Verslag security

Offroad Compass Portugal

Versie 1.0
December 2016

Projectgroep GFY01-3

Inhoudsopgave

Inleiding

Dit document betreft een beknopte analyse van potentiële dreigingen die zich voor kunnen doen inzake de veiligheid van de website. Daarna volgt een analyse van de ingebouwde veiligheidsniveaus en hoe de reeds geïdentificeerde dreigingen het hoofd worden geboden. Ten slotte volgt een advies over resterende kwetsbaarheden en hoe deze eventueel later opgepakt kunnen worden.

Dreigingen worden omschreven vanuit het oogpunt van Beschikbaarheid, Integriteit en Vertrouwelijkheid, beter bekend als de BIV-classificatie. Deze begrippen worden later toegelicht.

Naast de BIV-principes spelen nog 3 termen een belangrijke rol: identificatie, authenticatie en autorisatie. Wie ben je, ben je het echt en wat mag je dan?

Risicoanalyse

In deze risicoanalyse kijken we eerst naar de kwetsbaarheden en of de dreigingen die de website met zich mee kan brengen. De website verleent een dienst (men kan er een vakantie boeken) en dat zorgt ervoor dat de data die via deze website loopt gevoelige informatie kan bevatten. Denk aan reisgegevens, klantgegevens, maar ook bijvoorbeeld de agenda van het bedrijf.

Het is van groot belang dat deze informatie alleen toegankelijk is voor de mensen die deze informatie nodig hebben. Daarnaast is het ook erg belangrijk dat de beschikbare informatie nauwkeurig is en geen fouten bevat.

Uiteraard is het ook van belang dat deze informatie überhaupt beschikbaar is. Dit is echter sterk afhankelijk van de host naar voorkeur van de opdrachtgever, en is niet iets waar wij als projectgroep maatregelen voor kunnen nemen. Mede hierdoor wordt er in deze analyse voornamelijk aandacht besteed aan de potentiële gevaren omtrent Integriteit en Vertrouwelijkheid.

Voordat we verder gaan is het belangrijk om eerst een aantal sleutelbegrippen te benoemen en toe te lichten wat wij hieronder verstaan. Deze begrippen zijn: Beschikbaarheid, Integriteit en Vertrouwelijkheid. Dit zijn de zogenoemde BIV-principes:

- **Beschikbaarheid** is de mate waarin informatie beschikbaar is voor de gebruiker en het informatiesysteem in bedrijf is op het moment dat de organisatie deze nodig heeft.
- **Integriteit** is de mate waarin de informatie actueel en zonder fouten is. Kenmerken van integriteit zijn de juistheid en de volledigheid van de informatie.
- **Vertrouwelijkheid** is de mate waarin de toegang tot informatie beperkt is tot een gedefinieerde groep die daar rechten toe heeft. Hieronder vallen ook maatregelen die de privacy beschermen.

Voor we gaan kijken naar specifieke dreigingen is het belangrijk om in ieder geval een goede basis vast te stellen: denk aan continue up to date software, niet gebruikte functies binnen een website verwijderen en simpelweg geen standaard gebruikersnaam en een goed wachtwoord gebruiken. Zonder deze stappen kun je tegenover specifieke dreigingen allerlei maatregelen zetten maar is de kans op hacking alsnog aanwezig.
Voor een aantal dreigingen is het belangrijk specifieke maatregelen te nemen, dit verminderd de kans, en zorgt ervoor dat de beschikbaarheid, integriteit of de vertrouwelijkheid van de website geen gevaar loopt.

In het volgende schema worden deze dreigingen benoemd, met een Hoge, Lage, of Middelmatige schade/kans en het beveiligingsaspect dat risico loopt. De ingebouwde maatregelen binnen de website zorgen ervoor dat het restrisico laag ligt, mits uiteraard de bovengenoemde basis in orde is. Ook wordt de aard van de maatregel aangegeven de kolom ‘type’. Wij maken onderscheid tussen reductieve, preventieve, detectieve, repressieve en correctieve maatregelen:

- **Red**uctief(RD): reduceren (verminderen) bedreigingen;
- **P**reventief(P): voorkomen incidenten;
- **D**etectief(D): detecteren (opmerken) incidenten;
- **Rep**ressief(RP): gevolgen van incident beperken;
- **C**orrectief(C): schade corrigeren (herstellen)

Dreiging	BIV	Schade	Kans	Maatregel	Type	Restrisico
SQL-injectie	I	H	H	Prepared statements gebruiken	P	L
Malafide invoer formulieren	I	M	H	Invoer filteren	P	M***
Onjuiste invoer formulieren	I	L	M	Invoer controleren en eventuele foutmeldingen geven	P	L
Man in the middle-attack	V	H	L	HTTPS	RD	L
Toegang tot bestanden waarvan dat niet de bedoeling is	V	L	M	Mensen doorsturen naar een 403-pagina	D	L
(D)DoS-aanval	B	H	L	Speciale software installeren op webserver	P	H
Fout bij aanpassen pagina-inhoud	I	L	M	Gebruikershandelingen vastleggen	RP	L
Storing	B	H	M	2e locatie server/backup	RP	L

Beschrijving ingebouwd veiligheidsniveau

In dit hoofdstuk wordt beschreven welke oplossingen wij geïmplementeerd hebben rond de geïdentificeerde beveiligingsrisico's, omschreven in de risicoanalyse. De oplossingen worden benoemd per risico waarop ze gericht zijn, en zijn ingedeeld op Beschikbaarheid, Integriteit en Vertrouwelijkheid.

Ook wordt gekeken naar hoe autorisatie, authenticatie en identificatie zijn geregeld. Hieronder wordt kort toegelicht hoe dit geregeld is en welke oplossingen hierop van toepassing zijn.

Identificatie, authenticatie en autorisatie

De website maakt onderscheid tussen drie soorten gebruikers. Ten eerste is er uiteraard de bezoeker. Dit type gebruiker kan alleen de openbare delen van de website bekijken en hoeft zich niet te identificeren.
Ten tweede is er de klant. De klant heeft een gebruikersnaam en een wachtwoord gebaseerd op het weeknummer en het jaar. Na succesvolle authenticatie, krijgt de klant autorisatie om zijn reisgegevens in te zien.
Ten derde is er de beheerder. De beheerder heeft ook een gebruikersnaam en heeft een zelfgekozen wachtwoord. Na succesvolle authenticatie, krijgt de beheerder volledige toegang tot alle delen van de website, waaronder het beheerpaneel.

Om onderscheid te kunnen maken tussen de verschillende soorten gebruikers, wordt er gebruik gemaakt van privilege niveaus. Als een klant bijvoorbeeld probeert in te loggen als beheerder, dan zal hij/zij een foutmelding krijgen.

Waarborging Beschikbaarheid

Storing

Dit is iets waar wij als programmeurs weinig aan kunnen doen. De voornaamste maatregelen die hiertegen genomen kunnen worden zoude door de klant zelf moeten worden genomen. Van belang is dat onze klant kiest voor een betrouwbare host voor de website, die zelf voldoende maatregelen genomen heeft om

Uitwijklocatie

(D)DoS-aanval

Hier hebben wij geen maatregelen tegen genomen. Het implementeren van een systeem te kosten > baten

Waarborging Integriteit

Fout bij aanpassen pagina-inhoud

Het systeem houdt bij wie het meest recent de pagina-inhoud heeft aangepast. Bij het updaten van een pagina, wordt de gebruikersnaam vastgelegd van degene die de pagina heeft aangepast.

```
$stmt = $pdo->prepare("UPDATE content
                       SET title=?, bodytext=?, updated_by=?
                       WHERE pagina=?
                       AND lang=?");
```

Malafide invoer formulieren

Onjuiste invoer formulieren

Bij het invullen van formulieren wordt gecontroleerd of de invoer correct is. Er wordt bijvoorbeeld gecontroleerd of er daadwerkelijk een e-mailadres wordt ingevuld waar dat verwacht wordt.

```
//checkt of de ingevulde email, naam, achternaam en onderwerp
//voldoen aan de eisen gesteld in $email_exp (komen de variabelen overeen?)
$email_exp = '/^[A-Za-z0-9._%-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,4}$/';

if(!preg_match($email_exp,$email_from)) {
     $error_message .= 'The Email Address you entered does not appear to be valid.<br />';
}
```

Waarborging Vertrouwelijkheid

Inloggen op het beheerpaneel

Bij het inloggen op het beheerpaneel wordt om een gebruikersnaam en wachtwoord gevraagd. Deze staan in onze mysql database opgeslagen, en wachtwoorden zijn versleuteld middels het bcrypt algoritme. Hiervoor hebben we gebruik gemaakt van de PHP-functie password_hash. Het ingevoerde wachtwoord wordt met de PHP-functie password_verify vergeleken met het gehashte wachtwoord uit de database, indien deze juist is krijgt de gebruiker toegang tot het systeem.

In dit voorbeeld nemen we 123456 als wachtwoord, het gehashte wachtwoord ziet er als volgt uit:

echo password_hash("123456", PASSWORD_DEFAULT)."\n";
$2y$10$CBKttgwd0hAWyrvVZ6OHtOCY.BNY.6HM20HOLym1YOwb4deAYDaqq

SQL-injectie

Om aanvallen middels SQL-injectie te voorkomen maken we gebruik van prepared statements. Hiermee wordt voorkomen de database door kwaadwillenden aangepast, gekopieerd of verwijderd wordt.

```php
$stmt = $pdo->prepare("INSERT INTO nieuwsbericht (lang,title,bodytext,posted) VALUES (?,?,?,?)");
$stmt->execute(array($lang, $titel, $bodytext,$date));
$userRow = $stmt->fetch(PDO::FETCH_ASSOC);
$res = $stmt->rowCount();
if ($res > 0) {
    //feedback aan gebruiker geven
    print("Het bericht " . $titel . " is toegevoegd.");
    print("<script>window.onload = popup;</script>");
```

Man in the middle-attack

Het is de bedoeling om gebruik te maken van HTTPS. Hierdoor kunnen verstuurde gegevens bij het plaatsen van een boeking, of bij het stellen van een vraag middels het contactformulier lastig afgevangen worden door kwaadwillenden.

Toegang tot bestanden waarvan dat niet de bedoeling is

Het is niet de bedoeling dat gebruikers toegang hebben tot bepaalde bestanden. Deze bestanden zijn belangrijk voor het functioneren van de website, maar hebben voor de gebruiker geen toegevoegde waarde.
Als een gebruiker een link invoert waar hij niet mag komen, dan wordt hij doorverwezen naar de 403-pagina. Dit voorkomt dat kwaadwillenden onnodig informatie kunnen krijgen over de structuur en innerlijke werking van de website. Tevens zorgt dit voor een consistent functionerende website, wat de gebruikerservaring ten goede komt.

```php
<?php
if(!defined('toegang')) {
   header("Location: 404.php");
   exit();
}
```

```php
<?php define("toegang", true); ?>
```

Advies over vervolgstappen

<veiligheidsrisico’s die wij niet hebben kunnen wegnemen>
Dreiging (D)DoS