phpBB Security

van

Paul Sohier (0806122)

CMI-Opleiding *Technische Informatica* – Hogeschool Rotterdam

23 mei 2011

Eerste docent *P.J. den Brok*
Tweede docent

Samenvatting

hpBB is een op het internet bekend geworden software voor het maken van een eigen forum. Het in 2000[7] begonnen project is op dit moment nog steeds actief, maar heeft veel probleme met security gehad. In de afgelopen jaren zijn er grote wijzigingen geweest binnen phpBB om te zorgen dat de security problemen die er zijn geweest voorkomen kunnen worden.

Inhoudsopgave

Inleiding

In dit verslag probeer ik te kijken wat de security problemen zijn van phpBB in het verleden en wat de oorzaak hiervan is. phpBB heeft een aantal jaren geleden intern een groot aantal wijzingen aangebracht in de manier van werken om security problemen te voorkomen. In de afgelopen 3 jaar zijn er binnen de phpBB core geen grote security problemen opgetreden[8].

Niet alleen het core product van phpBB heeft last van security problemen, ook MODifications[1] hadden security problemen. Ook bij deze MODs is geprobeerd om het aantal security problemen wat er was terug te brengen tot een minimaal aantal.

phpBB had sinds de problematische 2.0 branch een slechte naam op het gebied van security, maar sinds de 3.0 release staat phpBB bekend om zijn goede security en het snelle oplossen van problemen.

[1] MODifications (Ook wel MODs genoemd) zijn aanpassen aan de code van phpBB welke extra functionaliteit toevoegen aan het product

De historie van phpBB

Toen James Atkinson met phpBB begon in 2000 was het bedoeld als “concurent” van UBB, wat al bestaande forum software was. In eerste instantie was phpBB niet heel populair en werd er dus ook weinig aandacht gegegeven aan security. Toen in 2002 phpBB2 uitkwam was phpBB wel al een stuk populairder, maar was er nog steeds weinig gedaan aan security. Dit was helaas ook te zien in de jaren die erna kwamen, doordat ze vol zaten met security releases. Sinds 2.0.4 tot 2.0.23 (Verspreid over 6 jaar) losten alle versies een probleem op gerelateerd aan security. Niet alle problemen waren even groot, maar er waren hierop een aantal uitzonderingen.

Hieronder staat klein overzicht van de problemen welke phpBB heeft gehad in de afgelopen jaren, met de grootste problemen welke er de afgelopen jaren zijn geweest.

Op 14 november 2004 werd phpBB 2.0.11 uitgebracht[3] welke een drietal security problemen oplosten. Deze security problemen waren op 18 november 2004 al gemeld en een oplossing was publiekelijk gemaakt[2] om te zorgen dat zo snel mogelijk mensen zouden updaten. Helaas bleek later dit niet het geval[4]. Doordat het probleem wat gevonden was zo serieus was hadden hackers een worm ontwikkeld welke alle phpBB fora op internet afging en ging kijken of een forum vatbaar was voor het 2.0.11 probleem. Doordat veel fora niet geüpdated waren, kon deze worm een hoop fora hacken. De worm pasten dan alle bestanden welke schrijfbaar waren aan met een tekst dat de site “Defaced” was. Deze worm, genaamd de Never Ever No Sanity worm (Ook wel Santy worm genoemd), kwam “uit” op 20 december 2004[9], ruim een maand nadat phpBB een update had released voor de software en gebruikers hadden dus kunnen updaten binnen deze tijd. Om te zorgen dat de Worm minder goed werkten, besloot Google om gebruikers die zochten naar phpBB een foutmelding te geven[1].

phpBB reageerde met de 2.0.11 release goed door snel een patch uit te brengen voor het security probleem wat gevonden was. Het grootste probleem was echter dat gebruikers van de software de software hierna niet bijwerkten naar de nieuwste uitgebrachten release van phpBB. Om dit op te lossen besloot het development team om een aantal verbeteringen hierin aan te brengen zodat gebruikers sneller op de hoogte gesteld konden worden van nieuwe releases. Een goed voorbeeld hiervan was een versie checker in de software, welke controleerde op het forum zelf of de gebruiker de laatste versie had[5].

Het soort probleem wat optrad in phpBB 2.0.11 te voorkomen door gebruik te maken van vooraf gestelde methode om data te verwerken welke door de user is ingevoerd. In phpBB2 was er geen standaard manier om data te verwerken en leverde user input veel problemen op met diverse security issues tot gevolg. Ook in 2.0.13 was dit het geval. phpBB maakt gebruik van cookies om te controleren of een gebruiker ingelogd is of wanneer dit niet het geval is of een gebruiker automatische ingelogd mag worden. In de code voor dit automatische inloggen zat echter een fout waardoor als je het cookie aanpasten welke op je computer stond je automatische kon inloggen, als elke gebruiker. Een hacker kon dus op deze manier ook inloggen als een beheerder van het forum

en op deze manier alles aanpassen wat hij wou. De oplossing voor de probleem was ontzettend eenvoudig, php is standaard niet type strict waardoor een vergelijk zoals hieronder uitvoerd, het eindresultaat true is.

```
if (true == 1)
```

Dit betekend alleen wel, wanneer je wel een type stricte vergelijking wilt uitvoeren, je hierbij in je statements rekening mee moet houden. In het geval van de bug inphpBB 2.0.13 moest er een type strict statement uitgevoerd worden, maar dit werd niet gedaan. Dit soort problemen zijn in php een stuk lastiger te vinden zodra ze eenmaal aanwezig zijn. Ook hacker hebben er ruim 2 jaar over gedaan om dit probleem in de source code te vinden. phpBB heeft met de release van 2.0.13 snel gereageerd om het probleem op te lossen, phpBB 2.0.12 was 6 dagen eerder released, maar het probleem was toen nog niet bekend.

Naast de diverse problemen in phpBB zelf heeft de site van phpBB zelf ook diverse malen last gehad om zelf gehacked te worden. Door de intern gebruikte software niet up to date te houden is het diverse malen gebeurd dat de complete server van phpBB gehacked was en alle interne fora op torrent netwerken te vinden waren. Ook om dit in het vervolg te voorkomen zijn er intern een aantal verbeteringen doorgevoerd zodat dit niet meer gebeurd.

De verbeteringen

Om het imago te verbeteren van phpBB werd er besloten om in phpBB 2.2 (Welke later phpBB 3.0 werd[6]) de aandacht te leggen op security. In phpBB2 zijn een groot aantal maatregelen genomen om de security te verbeteren zonder inbreuk te doen op de werking van de software. De belangrijkste maatregel hierin was het strict regelen van de manier waarop phpBB geschreven is. Dit is vastgelegd in een document en alle code voor phpBB moet voldoen aan deze richtlijnen. Een belangrijk deel hierbij was dat user input, wat in veel gevallen zorgden voor security problemen, op een vast manier afgehandeld wordt.

Conclusies en aanbevelingen

Conclusies en aanbevelingen moeten verzameld worden in een apart en herkenbaar deel van het verslag. Hoewel in het hoofdverslag op diverse plaatsen conclusies getrokken kunnen worden, moeten de belangrijkste conclusies samengevoegd en samengevat worden.

Belangrijk is dat het verschil tussen objectief controleerbare conclusies en subjectieve aanbevelingen duidelijk wordt aangegeven. Ook is het aan te bevelen om de belangrijkste conclusies conform de opdrachtomschrijving te formuleren.

Bronnen

[1] Google stops spread of santy worm. http://www.zdnet.co.uk/news/security-management/2004/12/22/google-stops-spread-of-santy-worm-39181937/.

[2] howdark.com exploits - follow up. http://www.phpbb.com/community/viewtopic.php?f=14&t=240513.

[3] phpbb 2.0.11 released - critical update. http://www.phpbb.com/community/viewtopic.php?f=14&t=240636.

[4] phpbb 2.0.11 upgrade reminder. http://www.phpbb.com/community/viewtopic.php?f=14&t=244451.

[5] phpbb 2.0.12 released. http://www.phpbb.com/community/viewtopic.php?f=14&t=265423.

[6] phpbb 2.2 is no more ... meet olympus. http://www.phpbb.com/community/viewtopic.php?f=14&t=256072.

[7] phpbb history. http://www.phpbb.com/about/history/.

[8] phpbb security problemen. http://secunia.com/advisories/product/17998/?task=statistics.

[9] Santy worm makes unwelcome visit. http://news.bbc.co.uk/2/hi/technology/4117711.stm.

Evaluatie

In de evaluatie reflecteer je over je eigen afstudeerproces. Daarbij moet je vooral letten op de leereffecten. Welke competenties had je nodig? Welke competenties kwam je tekort en moest je zelf verwerven? Waren dit algemene of specifieke competenties? Voldeden de beroepscompetenties aan de standaard van het *HBO-I* (analyseren, adviseren, ontwerpen, realiseren en beheren)? Vielen de algemene competenties in de vijf categorieën van de *Dublin Descriptoren*[2] zoals het verkrijgen van kennis en inzicht, het toepassen van kennis en inzicht, het maken van onderbouwde keuzen (oordeelsvorming), het communiceren (schriftelijk en mondeling) en het verkrijgen van leervaardigheden?

[2]Dublin Descriptoren zijn eisen aan de competenties voor de bachelor en master studies aan universiteiten en hogescholen in Europa.

Bijlage A

Achtergrond materiaal

In de bijlagen komen alle gegevens die nodig zijn voor de onderbouwing, maar die de leesbaarheid van het hoofdverslag verlagen.