WEBAPPLICATIE-SCAN

Kiezen op Afstand

Datum : 1 september 2006

INHOUDSOPGAVE

1 MANAGEMENTSAMENVATTING

In opdracht van het ICTU-programma 'Kiezen op Afstand' heeft GOVCERT.NL een scan uitgevoerd op de website www.internetstembureau.nl. Het doel van de scan is het verkrijgen van inzicht in het huidige ICT-beveiligingsniveau van de applicatie. Door middel van een technische scan is de functionele werking van de applicatie in de productieomgeving getest op bekende kwetsbaarheden. Alleen de technische werking van de applicatie is onderzocht, de architectuur van de achterliggende systemen is niet beoordeeld. Dit rapport beschrijft beknopt de resultaten van de uitgevoerde scan.

Dit rapport geeft geen uitputtend beeld van de beveiliging van de applicatie. De scan is slechts een momentopname. Conclusies zijn getrokken vanuit de bevindingen die zijn opgedaan in een onderzoek van twee dagen.

De resultaten en bevindingen uit de scan leiden tot de volgende conclusies:

+ Er zijn geen kritieke kwetsbaarheden gevonden in de website.

- Een kwaadwillende kan via Cross-Frame Scripting (XFS) trachten gegevens van een gebruiker te onderscheppen.

- Via verschillende parameters die de website gebruikt is het mogelijk om Cross-Site Scripting (XSS) uit te voeren.

GOVCERT.NL geeft de volgende aanbevelingen:

- Neem maatregelen om te voorkomen dat de verschillende pagina's van de website niet geopend kunnen worden in een frame.
- Zorg voor voldoende validatie van de invoer en parameters zodat Cross-Site-Scripting niet mogelijk is.

2 INLEIDING

Dit rapport beschrijft de bevindingen van scan die uitgevoerd is door GOVCERT.NL op de website www.internetstembureau.nl op 24 en 25 augustus 2006.

Dit hoofdstuk beschrijft dit rapport eerst de doelstelling en scope van deze scan. Tevens wordt ingegaan op de wijze waarop de scan is uitgevoerd. De resultaten en bevindingen van de scan vindt u terug in hoofdstuk 3. Hoofdstuk 4 beschrijft de conclusies en aanbevelingen die volgen uit de resultaten en bevindingen.

2.1 Doelstelling en scope

In opdracht van het ICTU-programma 'Kiezen op Afstand' heeft GOVCERT.NL op 24 en 25 augustus een scan uitgevoerd op de website www.internetstembureau.nl. Het doel van de scan is het verkrijgen van inzicht in het huidige ICT-beveiligingsniveau van deze webapplicatie. Hiertoe is er een technisch geautomatiseerd onderzoek uitgevoerd naar de eventuele kwetsbaarheden van de webapplicatie. Alleen de applicatie is onderzocht, de architectuur van de achterliggende systemen is niet beoordeeld.

Dit onderzoek is slechts een momentopname en is nadrukkelijk niet bedoeld om kant en klare oplossingen voor geconstateerde problemen te leveren. Wel zullen de aanbevelingen in dit rapport zo concreet mogelijk verwijzen naar oplossingen voor de geconstateerde kwetsbaarheden.

Het onderzoek is gelimiteerd door de beschikbare tijd. Van de gevonden kwetsbaarheden worden alleen de kwetsbaarheden die voor een aanvaller de meeste kans op uitbuiting geven, behandeld. Door de voortschrijdende technologische ontwikkelingen en wijzigingen op de webapplicatie is een constante alertheid ten aanzien van de beveiliging noodzakelijk.

Een test op de bestendigheid van de webapplicatie en de infrastructuur tegen Distributed Denial-of-Service (DDoS) aanvallen behoorde niet tot de scope en is tevens moeilijk te testen. Het is echter niet ondenkbaar dat kwaadwillenden tijdens een verkiezingsperiode zullen trachten om via een DDoS-aanval de website ontoegankelijk te maken. Maatregelen tegen DDoS-aanvallen kunt u terugvinden in het whitepaper "Bescherming tegen DDoS-aanvallen" van GOVCERT.NL. Dit document kunt u hier vinden: http://www.govcert.nl/render.html?it=50.

2.2 Beschrijving scanproces

Om tot de rapportage van kwetsbaarheden in software van de systemen binnen het netwerk te komen worden er 3 stappen doorlopen.

1. Verkenning van de webapplicatie;
2. Het uitvoeren van een geautomatiseerd kwetsbaarhedenonderzoek op de website en de webserver;
3. Het analyseren en rapporteren van de uitkomsten van het kwetsbaarhedenonderzoek.

Een kwaadwillende zal over het algemeen dezelfde stappen ondernemen om misbruik te maken van de systemen. De uitgevoerde technische scan bestond uit het automatisch onderzoeken van kwetsbaarheden die aanwezig zijn in de verschillende stappen van het stemproces. Op basis van de uitkomsten van het geautomatiseerde onderzoek is de webapplicatie handmatig onderzocht. Het handmatige onderzoek was erop gericht de kwetsbaarheden te verifiëren en te bepalen in hoeverre zij een bedreiging vormen voor de webapplicatie.

3 RESULTATEN EN BEVINDINGEN

In dit hoofdstuk komen de resultaten en bevindingen van de scan aan de orde.

3.1 Algemene bevindingen

De website www.internetstembureau.nl blijkt op basis van Round-Robin DNS (RR DNS) benaderbaar te zijn via twee IP-adressen (192.87.106.206 en 195.169.124.95). Beide IP-adressen vallen onder het beheer van SURFnet.

Een poortscan op deze IP-adressen leert ons dat de webservers alleen op basis van 80/tcp en 443/tcp via het internet te bereiken zijn. Dit is een gewenste en te verwachten situatie.

3.2 Resultaten

Uit de geautomatiseerde scan zijn twee aandachtspunten naar voren gekomen. Het betreft Cross-Frame Scripting (XFS) en Cross-Site Scripting (XSS). Geen van deze aandachtspunten vormt een direct risico voor wat betreft de integriteit, vertrouwelijkheid of beschikbaarheid van de webapplicatie. De komende paragrafen beschrijven deze aandachtspunten.

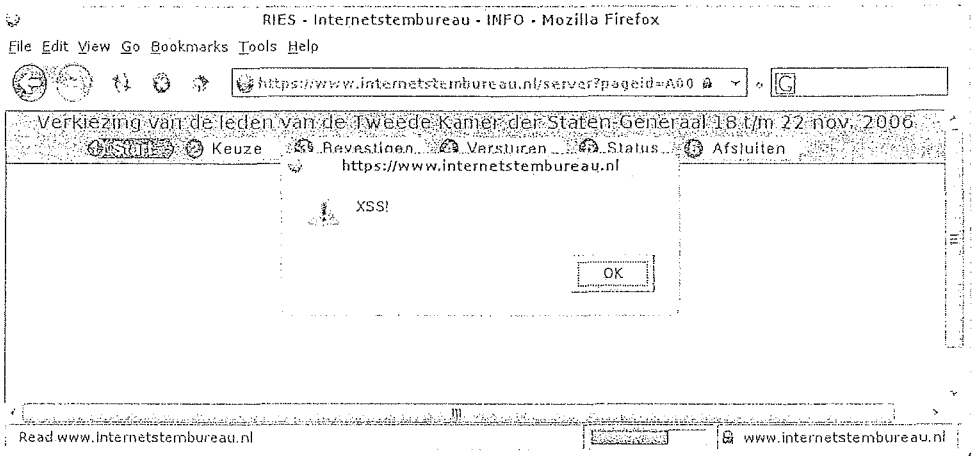
3.2.1 Cross-Frame Scripting (XFS)

De website is kwetsbaar voor Cross-Frame Scripting (XFS). XFS is een phishing-aanval waarbij een kwaadwillende een eigen webpagina opzet en daarin – in een apart frame – een legitieme pagina (in dit geval een pagina van www.internetstembureau.nl) verwerkt. Doordat de legitieme pagina onderdeel uitmaakt van de pagina van de kwaadwillende, kan de kwaadwillende de gegevens die de gebruiker invoert, onderscheppen.

3.2.2 Cross-Site Scripting (XSS)

Verschillende onderdelen van de website zijn gevoelig voor Cross-Site Scripting (XSS). XSS is een veel voorkomend probleem in webapplicaties. XSS houdt in dat een kwaadwillende kwaadaardige code injecteert in een link die verwijst naar een vertrouwde website. Hiertoe moet de kwaadwillende de beschikking hebben over een alom vertrouwde website die mogelijkheden biedt tot XSS. De website van Kiezen op Afstand is in dit geval een dergelijke vertrouwde website. Het is van belang bij het ontwikkelen van de website de invoer van de verschillende stappen uit het stemproces te valideren en zo de mogelijkheid tot misbruik te beperken. Figuur 4-1 toont een voorbeeld van de manier waarop XSS via de website van Kiezen op Afstand mogelijk is. In dit voorbeeld is een stukje Javascript geïnjec-

teerd in de sessiondata parameter van de URL. Het feit dat een pop-up scherm verschijnt, bewijst dat de website de invoer niet voldoende controleert.



Figuur 4-1: XSS

XSS is in ieder geval mogelijk via de parameters 'elid' en 'sessiondata'. Dit is zowel via een HTTP GET als via een HTTP POST het geval. Onderstaande URL illustreert een mogelijke manier om XSS via de website uit te voeren:

```
https://www.internetstembureau.nl/server?
   elid=null&sessiondata="><script>alert("XSS!")</script>
```

OPMERKING Het ontbreken van voldoende inputvalidatie kan ook leiden tot kwetsbaarheden als SQL injection die ernstiger van aard zijn. We hebben tijdens het uitvoeren van de scan echter geen dergelijke kwetsbaarheid kunnen ontdekken.

4 CONCLUSIES EN AANBEVELINGEN

GOVCERT.NL geeft de volgende conclusies en aanbevelingen. Deze conclusies zijn gebaseerd op de resultaten en bevindingen uit hoofdstuk 4.

4.1 Conclusies

De resultaten en bevindingen uit hoofdstuk 4 resulteren in de volgende conclusies:

\+ Er zijn geen kritieke kwetsbaarheden gevonden in de website.

\- Een kwaadwillende kan via Cross-Frame Scripting trachten gegevens van een gebruiker te onderscheppen. Hiertoe moet de kwaadwillende er wel in slagen om de gebruiker een bepaalde URL te laten openen.

\- Via verschillende parameters die de website gebruikt is het mogelijk om Cross-Site Scripting (XSS) uit te voeren. Om deze kwetsbaarheid te kunnen misbruiken moet een kwaadwillende er wel in slagen om de gebruiker een bepaalde URL te laten openen.

4.2 Aanbevelingen

GOVCERT.NL geeft de volgende aanbevelingen:

- Neem maatregelen zodat de verschillende pagina's van de website niet geopend kunnen worden in een frame. Dit kan men bereiken door elke webpagina van de website te laten starten met een script zoals hieronder weergegeven:

```
<SCRIPT LANGUAGE=JAVASCRIPT>
<!--
   if (top.frames.length!=0)
         top.location=self.document.location;
// -->
</SCRIPT>
```

- Zorg voor voldoende validatie van de invoer en parameters om Cross-Site Scripting te voorkomen. Goede validatie van invoer beperkt de mogelijkheden tot misbruik van de website.