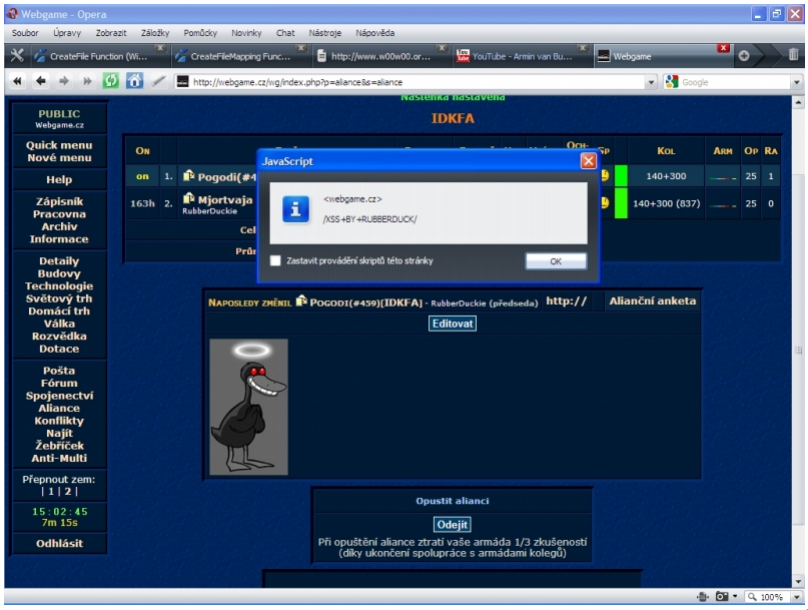
Webgame - Mám se bát o svůj účet?

Vložil/a RubberDuck [1], 23 Prosinec, 2009 - 02:43

Přesně nad touhle otázkou se jistě pozastavil každý, kdo Webgame, populární českou on-line webovou hru, alespoň na krátkou dobu okusil. A přemýslí správně.

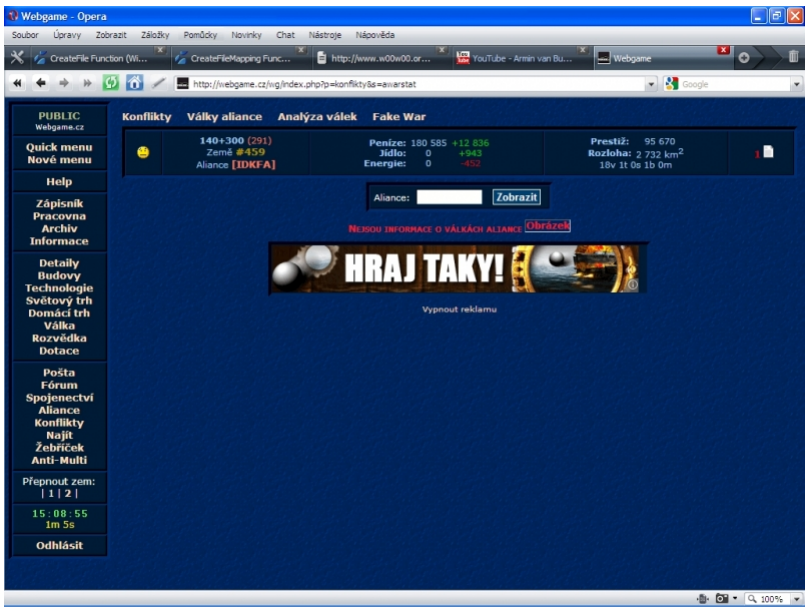
Vezmeme-li v úvahu, že Webgame vznikla jako diplomová práce (takové informace se ke mě dostaly - pokud je to jinak, uveďte v komentech veci na pravou míru) a to již před značnou dobou. Vzhledem k tomu, že na vývoji se stále pracuje a stále se tak zasahuje i do kódů samotné aplikace, je pravděpodobné, že se dřív nebo později do kódu "zanesou" chyby. Někdy z nedbalosti, někdy nahodile v závislosti na úpravách jiných částí kódu.

I mě tato myšlenka dostihla a nedala mi spát. Po nějaký čas jsem Webgame hrával a byl na výsost spokojený. Ale jak už to tak v pohádkách bývá, jal jsem se jednoho večera/noci provést aspoň rychlotest, který mě nemile překvapil, ale kecal bych, kdybych řekl, že jsem podobný výsledek nečekal. Zkrátka jsem objevil několik non-persistentních a jednu persitentní XSS. Začal jsem přemýšlet a rozvíjet teorie zneužití těchto zranitelností. V neposlední řadě jsem kontaktoval null.pointera, který na Webgame zastává funkci vedoucího vývojového týmu. Přes počáteční nedorozumění jsme nakonec došli ku společné myšlence, že by bylo zdrávo aspoň ty nejvíce bijící chyby opravit. Celková revize kódu by byla zbytečná, protože Webgame se přepisuje do nové, lepší a čistší formy. Ač mě null.pointer ubezpečoval, že chyby budou v dohledné době opraveny, nestalo se tak ani po !!TŘECH TÝDNECH!! (nic proti, null-pointere, ale tohle považuji za nezodpovědnost a přehlížení zájmů hráčů, protože náprava by nezabrala více, než pár minut a logování ti moc nepomůže, pokud vám někdo pokazí celý věk). Původně jsem chtěl se zveřejněním počkat až do okamžiku opravení děr. Ovšem to bych taky mohl čekat navždy.



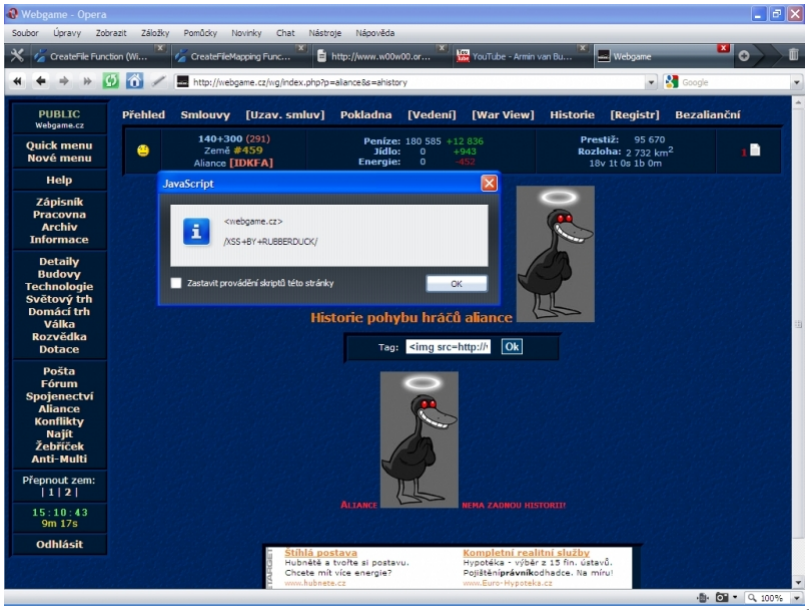
[2]

Persistent XSS v Nástěnce



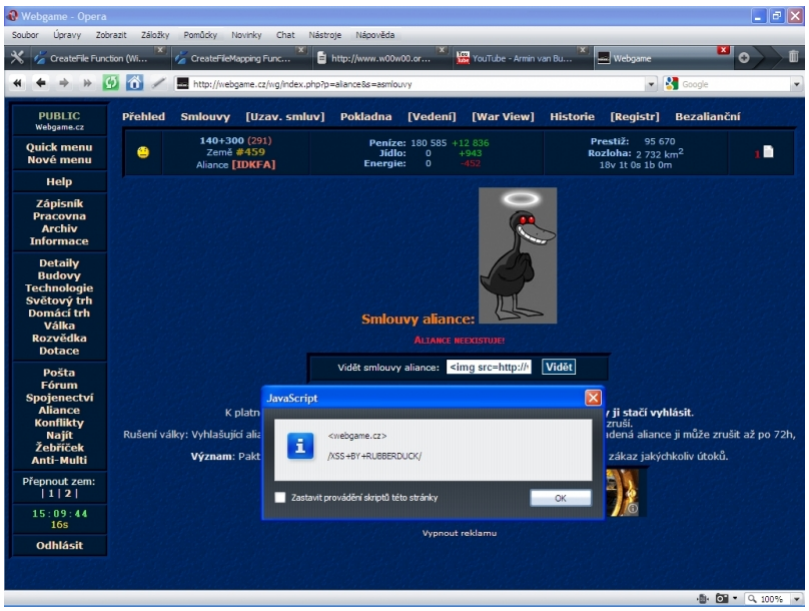
[3]

Nedokončená non-persistent XSS v WarStat



[4]

Non-persistent XSS



[5]

Non-persistent XSS

(Poznámka: Je tomu již nějaký ten pátek, kdy bylo na Webgame možné zneužít SQL Injection. Předpokládám, že chyb bude mnohem více - jen já jsem málo všímavý ;) Takže si klidně udělejme soutěž, kdo najde další chyby ;))

URL článku:
https://security-portal.cz/blog/webgame-m%C3%A1m-se-b%C3%A1t-o-sv%C5%AFj-%C3%BA%C4%8Det

Odkazy:
[1] https://security-portal.cz/users/rubberduck
[2] http://security-portal.cz/sites/default/files/aliance.jpg
[3] http://security-portal.cz/sites/default/files/awarstat.jpg
[4] http://security-portal.cz/sites/default/files/ahistory.jpg
[5] http://security-portal.cz/sites/default/files/asmlouvy.jpg