Global
SYMPOSIUM ON RACING
& GAMING 2013

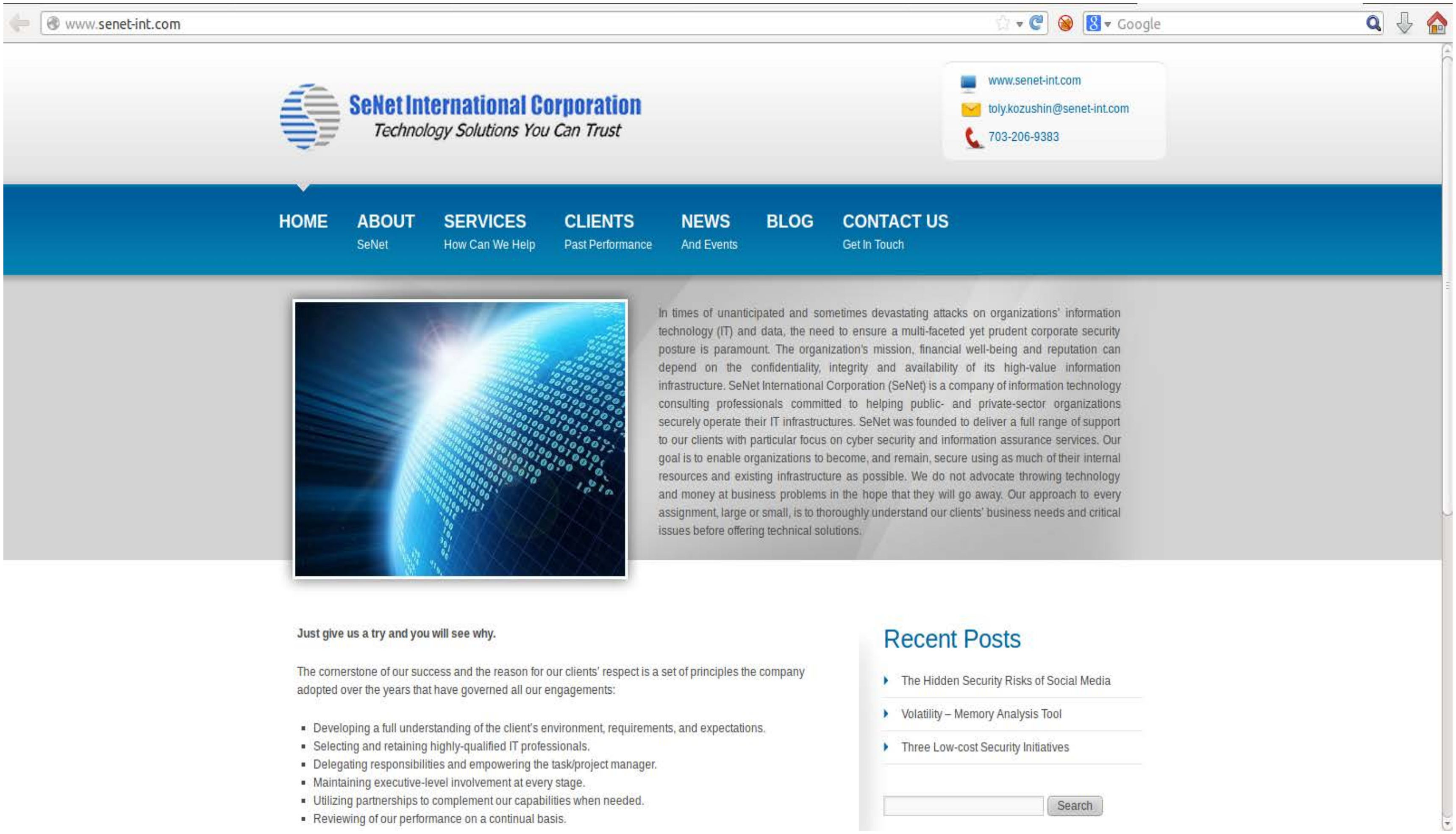
Security Trifecta – Overview of Vulnerabilities in the Racing Industry

Gus Fritschie

December 11, 2013

SeNet International Gaming Labs
"Don't Gamble with Security"

Who We Are – SeNet International



SeNet International Corporation

Technology Solutions You Can Trust

www.senet-int.com
toly.kozushin@senet-int.com
703-206-9383

In times of unanticipated and sometimes devastating attacks on organizations' information technology (IT) and data, the need to ensure a multi-faceted yet prudent corporate security posture is paramount. The organization's mission, financial well-being and reputation can depend on the confidentiality, integrity and availability of its high-value information infrastructure. SeNet International Corporation (SeNet) is a company of information technology consulting professionals committed to helping public- and private-sector organizations securely operate their IT infrastructures. SeNet was founded to deliver a full range of support to our clients with particular focus on cyber security and information assurance services. Our goal is to enable organizations to become, and remain, secure using as much of their internal resources and existing infrastructure as possible. We do not advocate throwing technology and money at business problems in the hope that they will go away. Our approach to every assignment, large or small, is to thoroughly understand our clients' business needs and critical issues before offering technical solutions.

Just give us a try and you will see why.

The cornerstone of our success and the reason for our clients' respect is a set of principles the company adopted over the years that have governed all our engagements:

- Developing a full understanding of the client's environment, requirements, and expectations.
- Selecting and retaining highly-qualified IT professionals.
- Delegating responsibilities and empowering the task/project manager.
- Maintaining executive-level involvement at every stage.
- Utilizing partnerships to complement our capabilities when needed.
- Reviewing of our performance on a continual basis.

Recent Posts

- The Hidden Security Risks of Social Media
- Volatility – Memory Analysis Tool
- Three Low-cost Security Initiatives

Who We Are – Gus Fritschie

- CTO of SeNet International
- Subject Matter Expert in Gaming and iGaming security
- Presented at multiple conferences, including Defcon on iGaming issues
- Written multiple articles on gaming security for both print and online publications
- Most importantly I want sites and organizations to be safe and secure because I am also a player
- Follow on Twitter @gfritschie

Why This Talk?

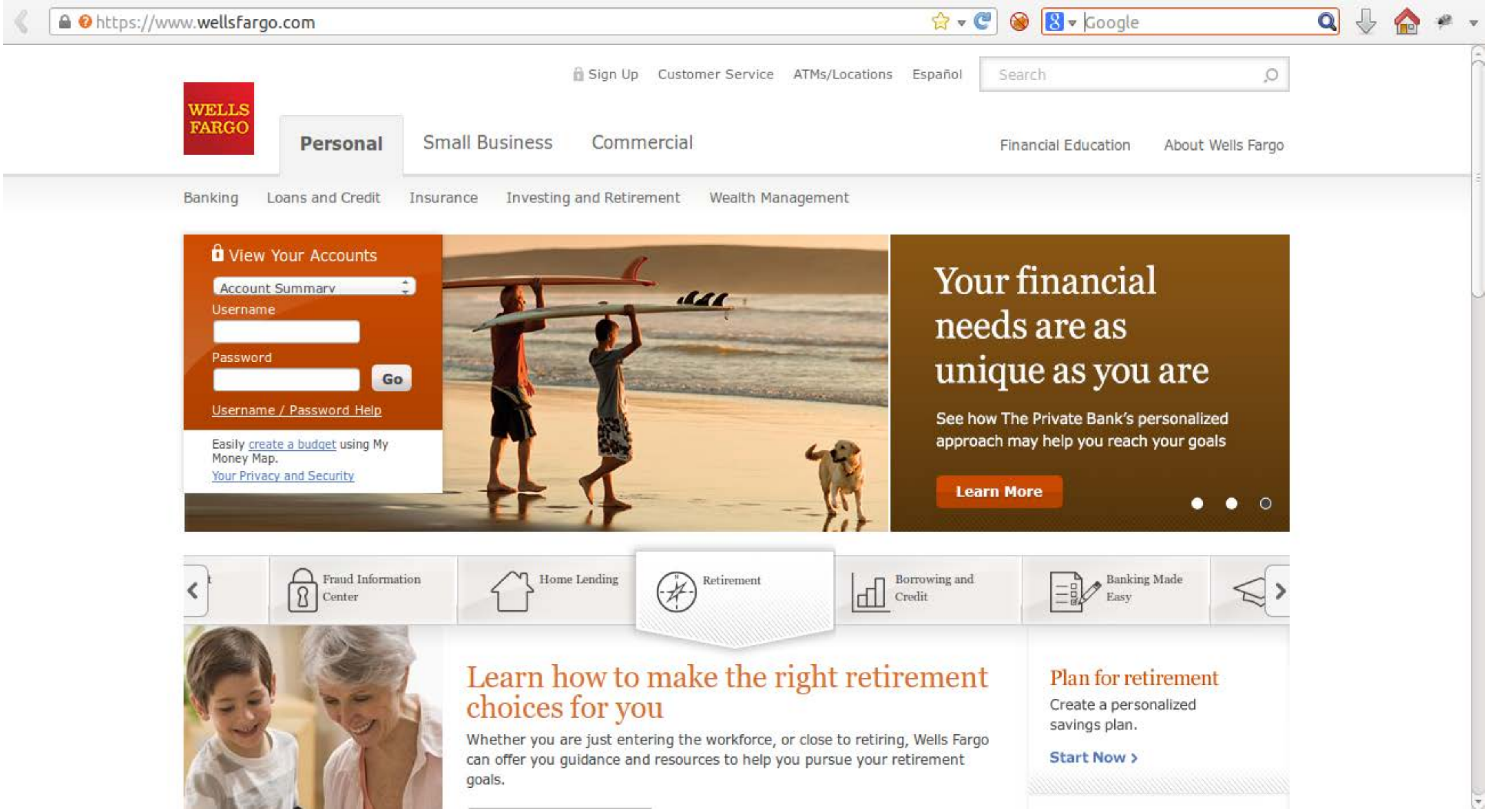
- The future of gaming, if not the Internet is tied closely to it. Even those components that may not be specifically tied to iGaming (i.e. OTB) still require a certain level of security.

- While the racing industry has had a head start (thanks to UIEGA) it only leads by a couple of lengths, and when it comes to security it is neck-to-neck.

- We need to learn from past mistakes in other sectors in order to avoid them in the future.

- Often security is seen as a cost and something we don’t think about until there is a problem (similar to flooded basement). However, this trend needs to change and we need to become more proactive compared to reactive.

How is Online Racing Security Different From This?



Easily create a budget using My Money Map.

Your financial needs are as unique as you are

See how The Private Bank's personalized approach may help you reach your goals

Learn how to make the right retirement choices for you

Whether you are just entering the workforce, or close to retiring, Wells Fargo can offer you guidance and resources to help you pursue your retirement goals.

Plan for retirement

Create a personalized savings plan.

Security is Security

- There is no difference!

- Racing and iGaming face the same problems and need the same level of protection as other verticals.

- Areas that need to be taken into account include:
  - Application Security
  - Network Security
  - System Security
  - Database
  - Mobile
  - Physical
  - And more………

Security is all About Managing Risk

- You will never be 100% secure, the key is to understand the risks you face and with that information make informed business decisions.

- In order to be 100% secure you would need to do this…….

Are Compliance Standards the Answer?

Compliance Does Not Equal Security

Compliance != Secure

- But it is a starting point and better than nothing.
- Need to approach it from more than a paperwork exercise.
- The problem is most of the compliance standards (current gaming included) are not strict enough and leave organizations with a false sense of security.

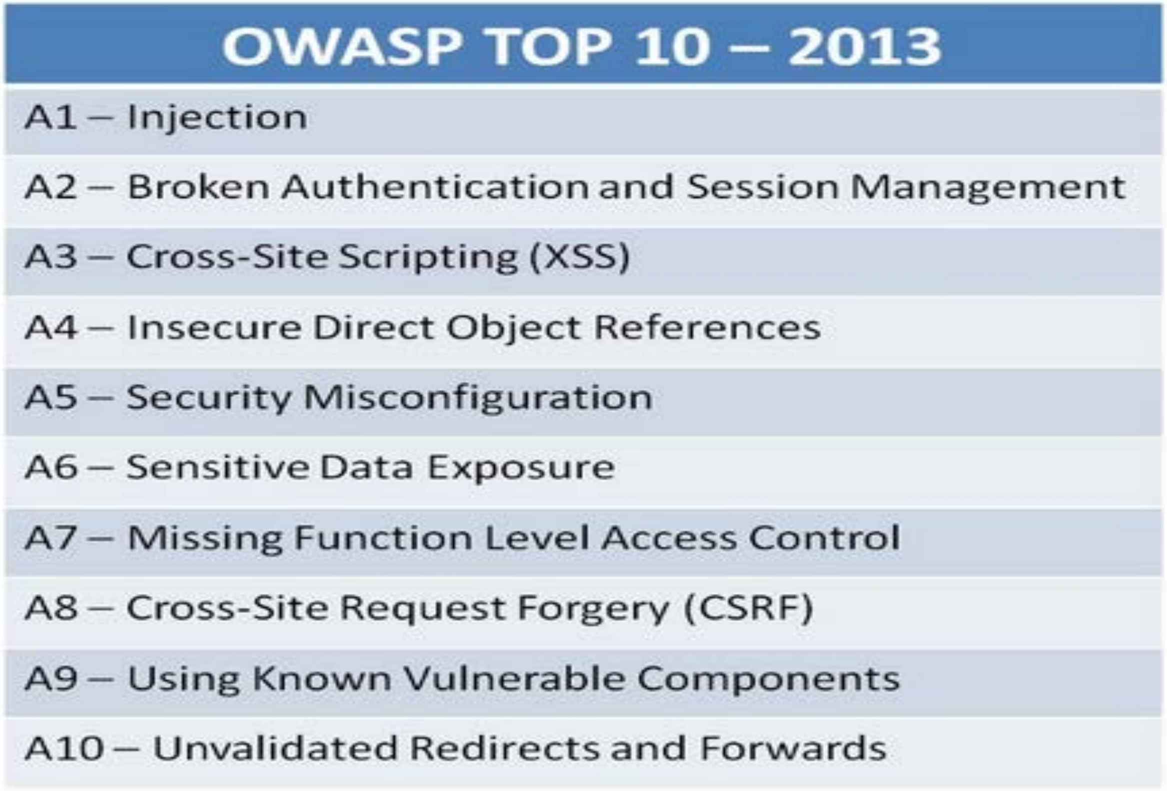
What is the Solution?

- The answer is a comprehensive, enterprise solution across all facets. Too long of an answer for this brief presentation.

- In my opinion two ways organizations are most likely to get compromised.
  1. Attacks via the application (both web and mobile)
  2. Social engineering attacks

- Let's look closer at the first method……

Types of Application Attacks



OWASP TOP 10 – 2013
A1 – Injection
A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References
A5 – Security Misconfiguration
A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control
A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards

Security Needs to be Baked into the SDLC

Important!

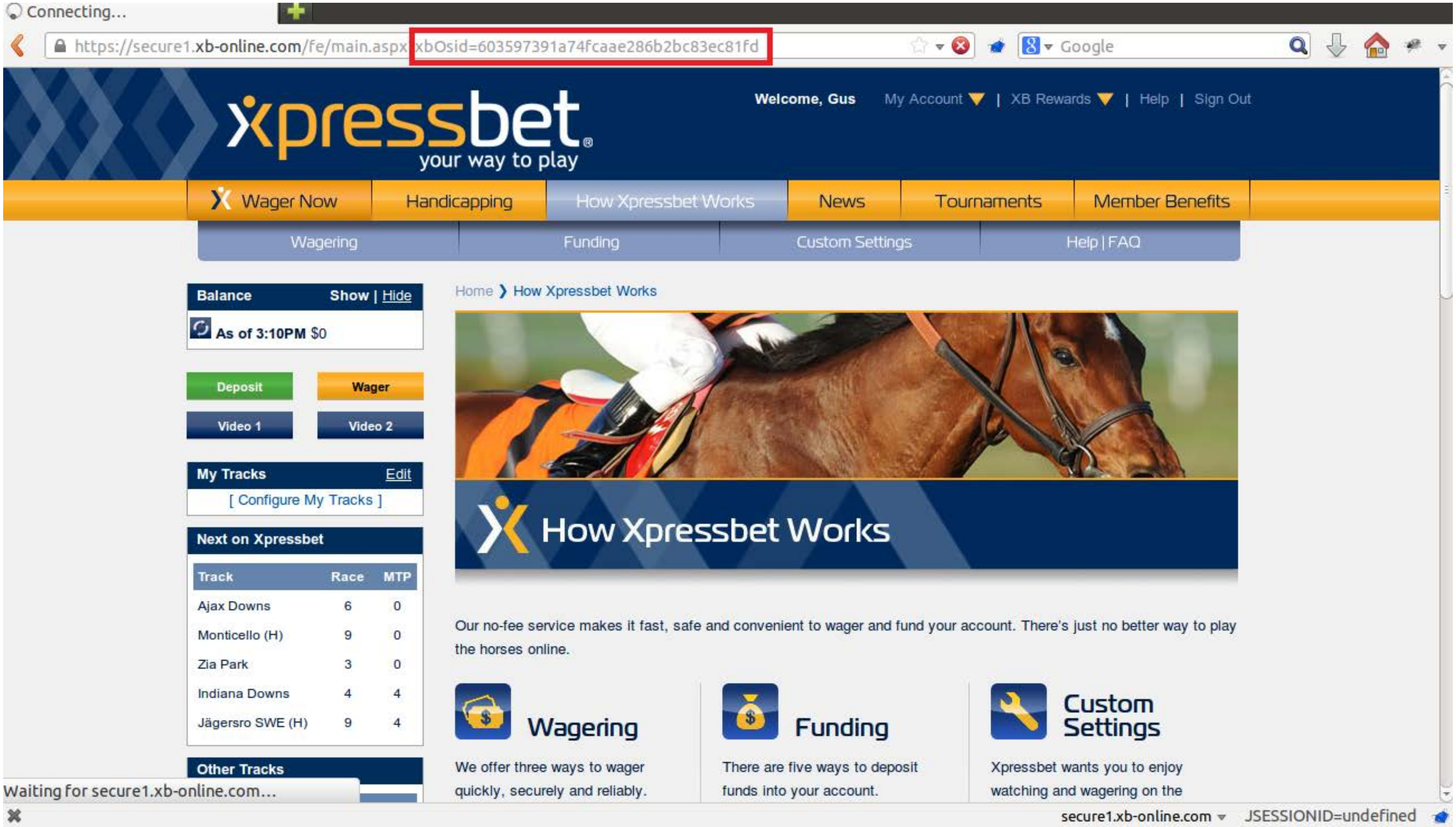
- Risk-based approach vs. compliance-only focus.
- Security integration to system development is critical to front-end design

- Examples:
- Audit logging design
- possibly include redundancy, retention, and reliability (unintentional 3 r's there);
- Session design
- possibly include concurrency control, lock, identification, replay
- Access, authentication, and authorization (intentional 3 a's there)
- Error handling design
- Unit test automation by check-in gates
- Code coverage
- Design for functional testing
- Information input restriction
- RBAC
- Partitioning
- Information validation
- Rules engine/input validation, app firewall

Examples

I DONT ALWAYS LISTEN ABOUT SECURITY
BUT WHEN I DO I LIKE TO SEE EXAMPLES

Session Token in URL



https://secure1.xb-online.com/fe/main.aspx xbOsid=603597391a74fcaae286b2bc83ec81fd

Balance Show | Hide

As of 3:10PM $0

My Tracks

Next on Xpressbet

Track	Race	MTP
Ajax Downs	6	0
Monticello (H)	9	0
Zia Park	3	0
Indiana Downs	4	4
Jägersro SWE (H)	9	4

Our no-fee service makes it fast, safe and convenient to wager and fund your account. There's just no better way to play the horses online.

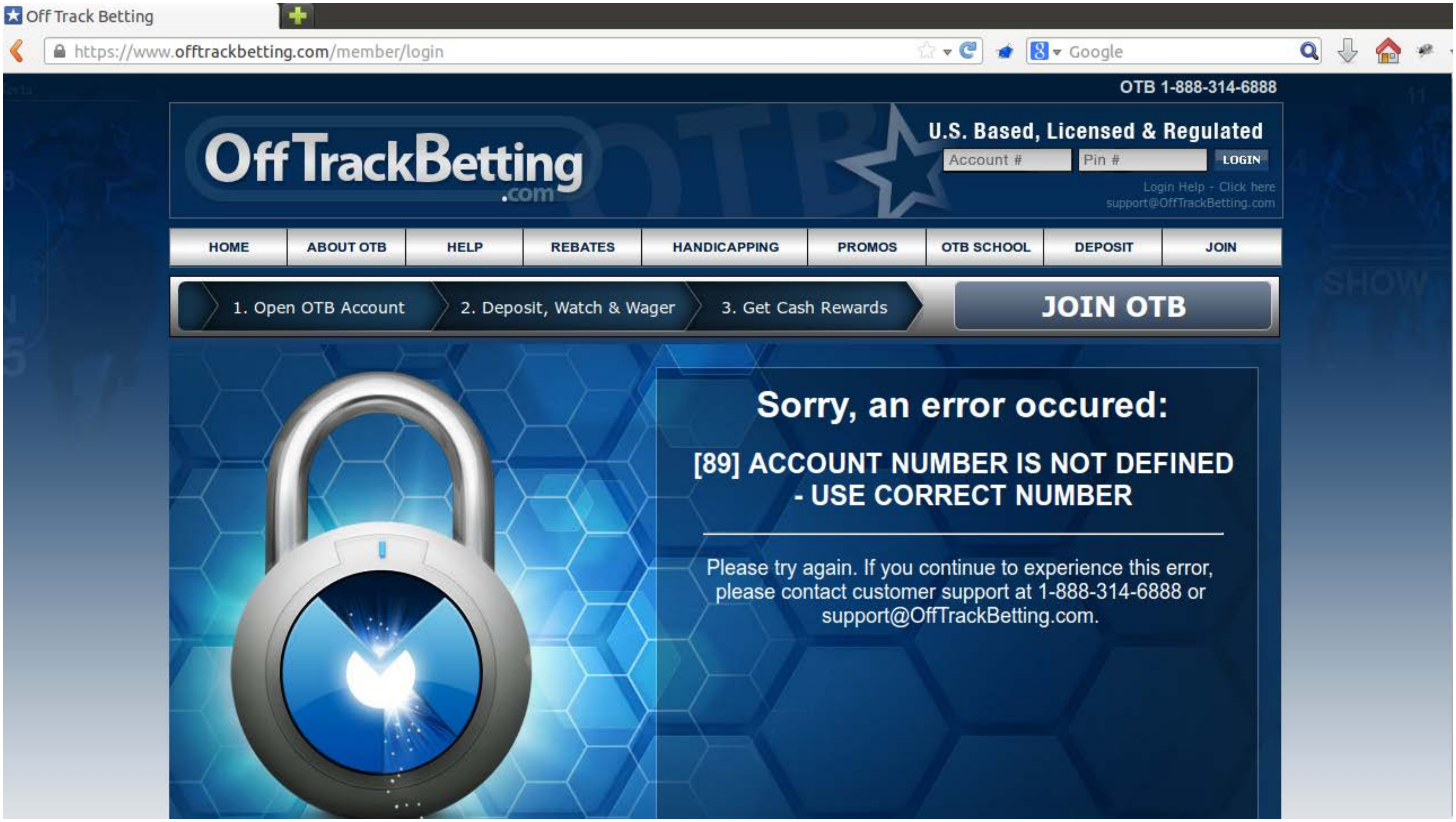
We offer three ways to wager quickly, securely and reliably.

There are five ways to deposit funds into your account.

Xpressbet wants you to enjoy watching and wagering on the

JSESSIONID=undefined

Account Number Enumeration

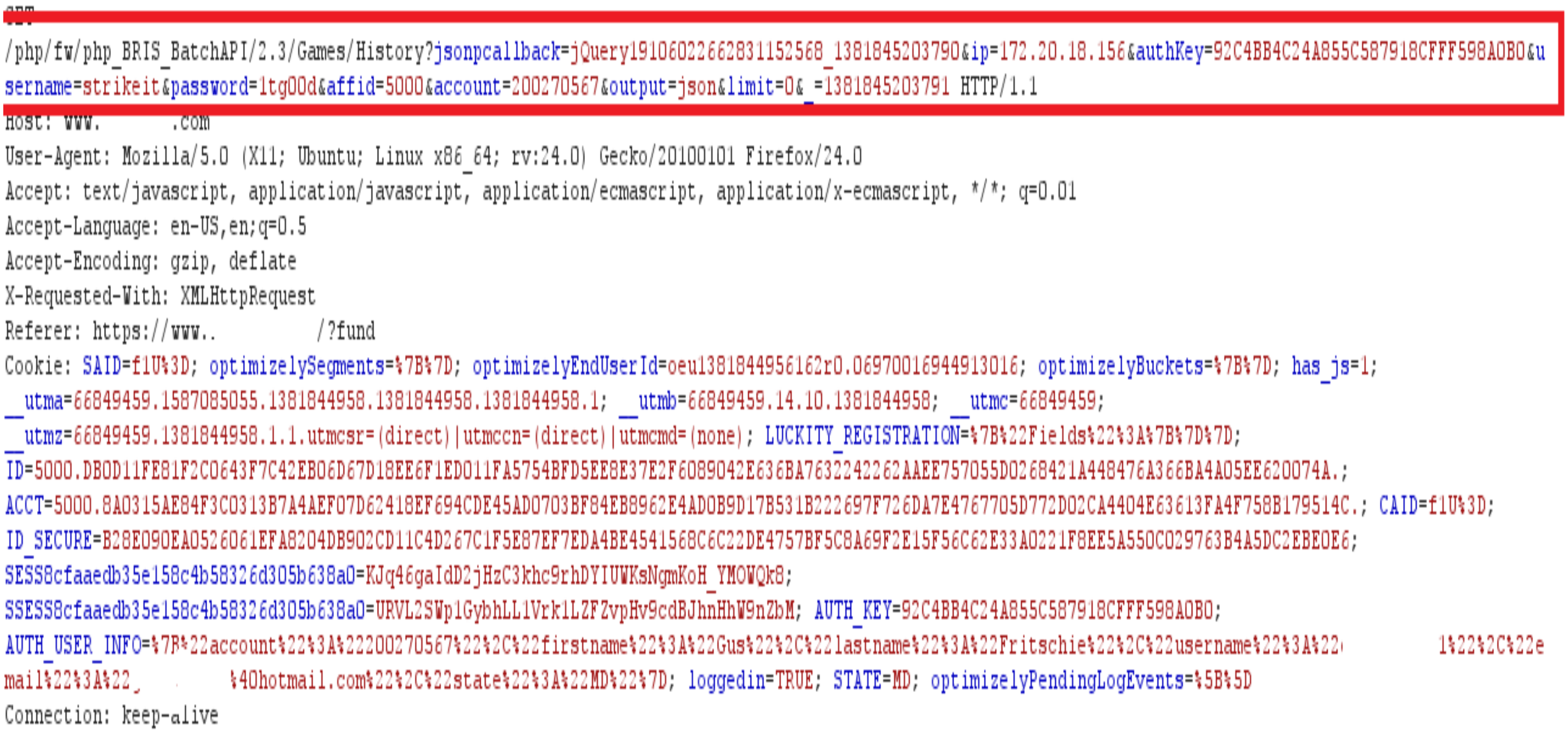


Sorry, an error occured:

[89] ACCOUNT NUMBER IS NOT DEFINED - USE CORRECT NUMBER

Please try again. If you continue to experience this error, please contact customer support at 1-888-314-6888 or support@OffTrackBetting.com.

Backend Password and Username Exposed in Request



```
GET
/php/fw/php_BRIS_BatchAPI/2.3/Games/History?jsonpcallback=jQuery19106022662831152568_1381845203790&ip=172.20.18.156&authKey=92C4BB4C24A855C587918CFFF598A0B0&u
sername=strikeit&password=1tg00d&affid=5000&account=200270567&output=json&limit=0&_=1381845203791 HTTP/1.1
Host: www.      .com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:24.0) Gecko/20100101 Firefox/24.0
Accept: text/javascript, application/javascript, application/ecmascript, application/x-ecmascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Referer: https://www..         /?fund
Cookie: SAID=f1U%3D; optimizelySegments=%7B%7D; optimizelyEndUserId=oeu1381844956162r0.06970016944913016; optimizelyBuckets=%7B%7D; has_js=1;
__utma=66849459.1587085055.1381844958.1381844958.1381844958.1; __utmb=66849459.14.10.1381844958; __utmc=66849459;
__utmz=66849459.1381844958.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none); LUCKITY_REGISTRATION=%7B%22Fields%22%3A%7B%7D%7D;
ID=5000.DB0D11FE81F2C0643F7C42EB06D67D18EE6F1ED011FA5754BFD5EE8E37E2F6089042E636BA7632242262AAEE757055D0268421A448476A366BA4A05EE620074A.;
ACCT=5000.8A0315AE84F3C0313B7A4AEF07D62418EF694CDE45AD0703BF84EB8962E4AD0B9D17B531B222697F726DA7E4767705D772D02CA4404E63613FA4F758B179514C.; CAID=f1U%3D;
ID_SECURE=B28E090EA0526061EFA8204DB902CD11C4D267C1F5E87EF7EDA4BE4541568C6C22DE4757BF5C8A69F2E15F56C62E33A0221F8EE5A550C029763B4A5DC2EBE0E6;
SESS8cfaaedb35e158c4b58326d305b638a0=KJq46gaIdD2jHzC3khc9rhDYIUWKsNgmKoH_YMOWQk8;
SSESS8cfaaedb35e158c4b58326d305b638a0=URVL2SWp1GybhLL1Vrk1LZFZvpHv9cdBJhnHhW9nZbM; AUTH_KEY=92C4BB4C24A855C587918CFFF598A0B0;
AUTH_USER_INFO=%7B%22account%22%3A%22200270567%22%2C%22firstname%22%3A%22Gus%22%2C%22lastname%22%3A%22Fritschie%22%2C%22username%22%3A%22         1%22%2C%22e
mail%22%3A%22_         %40hotmail.com%22%2C%22state%22%3A%22MD%22%7D; loggedin=TRUE; STATE=MD; optimizelyPendingLogEvents=%5B%5D
Connection: keep-alive
```

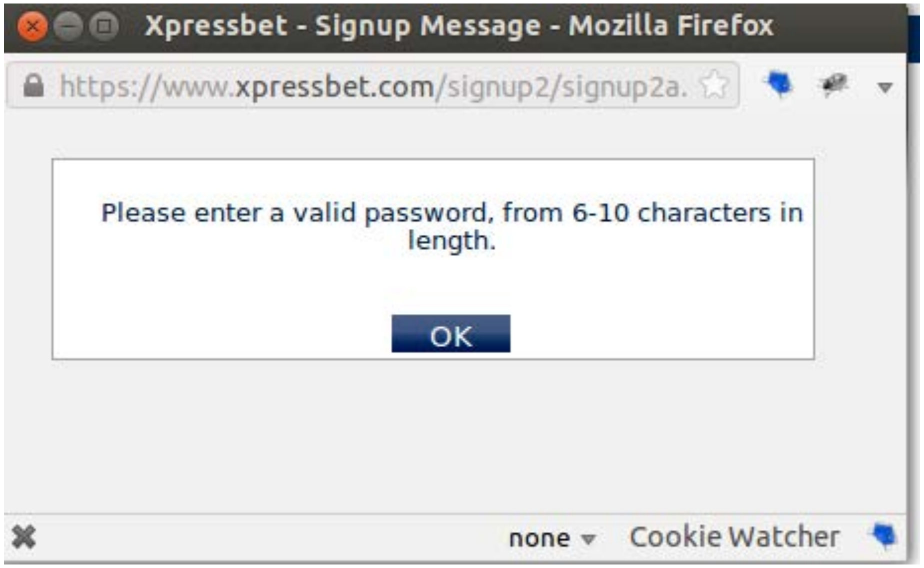
Backend Password and Username Exposed in Request (Cont.)

```
php/fw/php_BRIS_BatchAPI/2.3/Games/Payouts?ip=172.20.18.156&username=strikeit&password=1tg00d&affid=5000&output=json HTTP/1.1
```

What is this?

123456

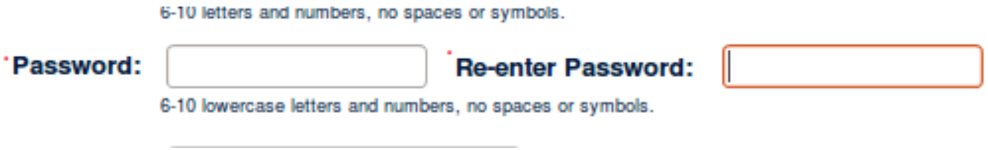
Weak Password Policy



Xpressbet - Signup Message - Mozilla Firefox

https://www.xpressbet.com/signup2/signup2a.

Please enter a valid password, from 6-10 characters in length.



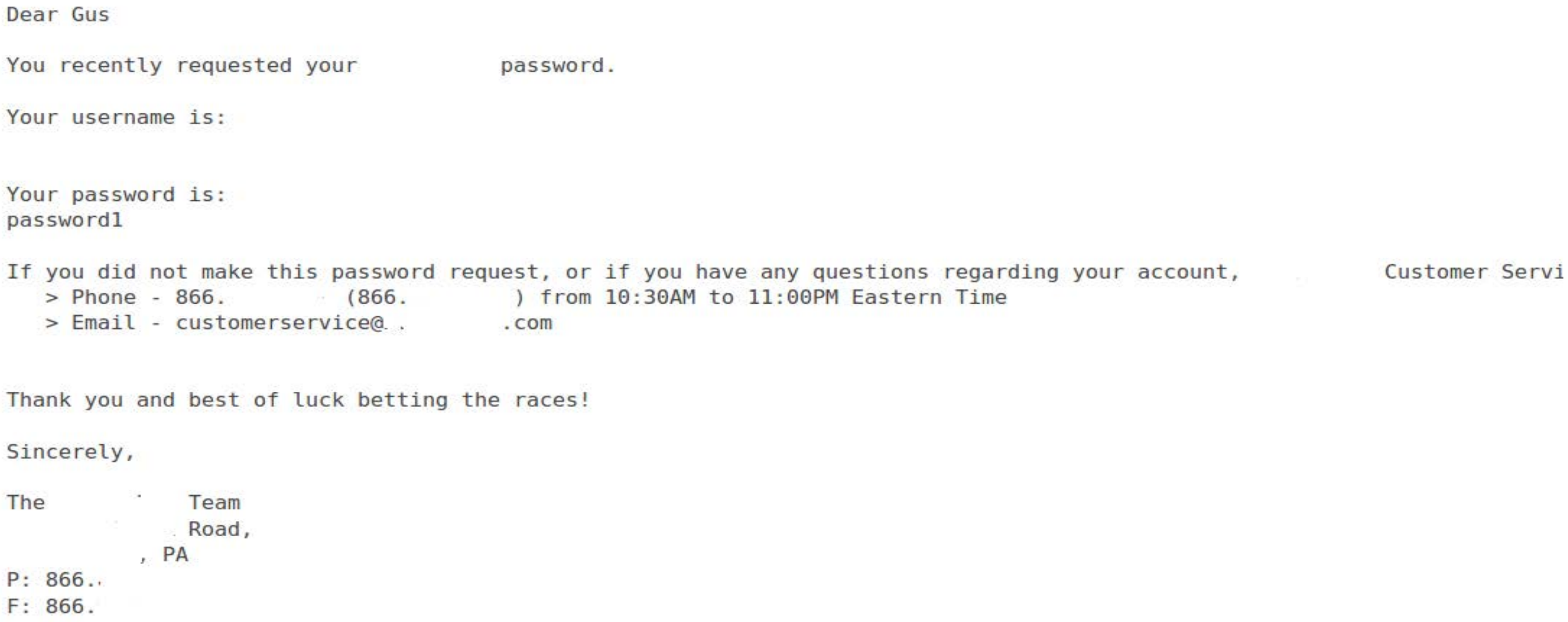
6-10 letters and numbers, no spaces or symbols.

*Password: *Re-enter Password:

6-10 lowercase letters and numbers, no spaces or symbols.

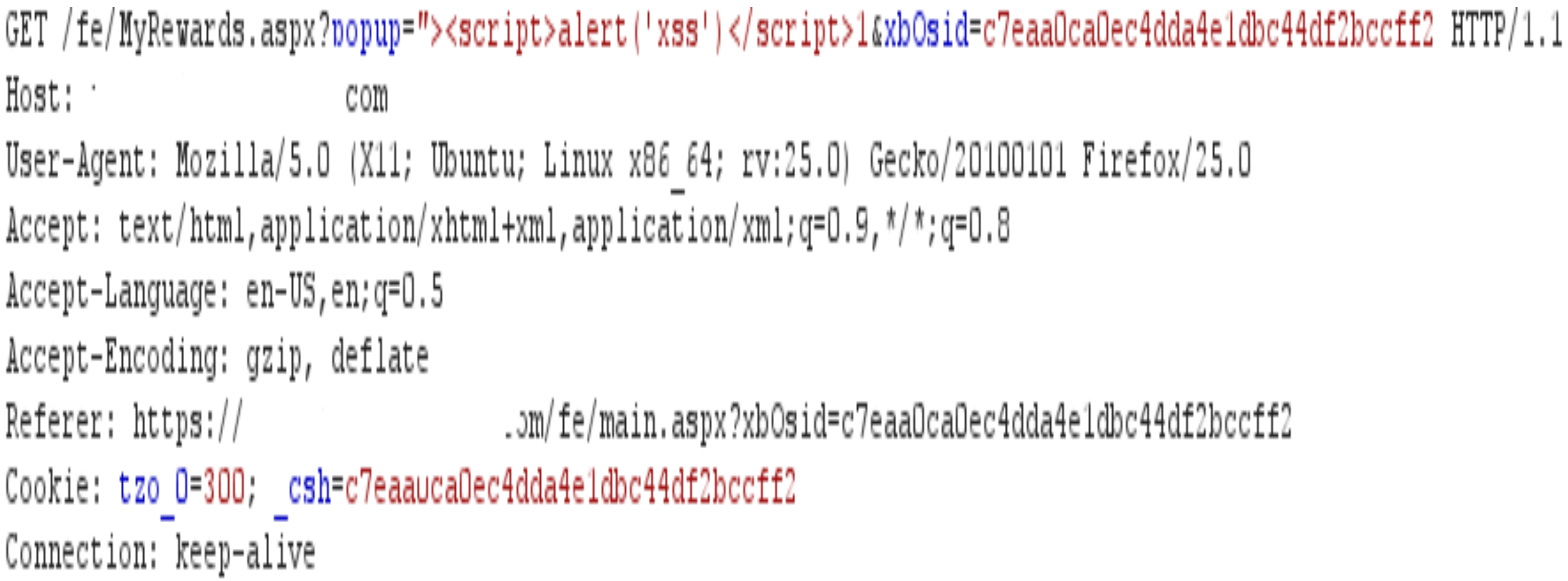
Password Stored in Clear-text in Database

Using the forgot password function the password is sent via email and is the same password as initially set. This indicates passwords are stored in clear-text.



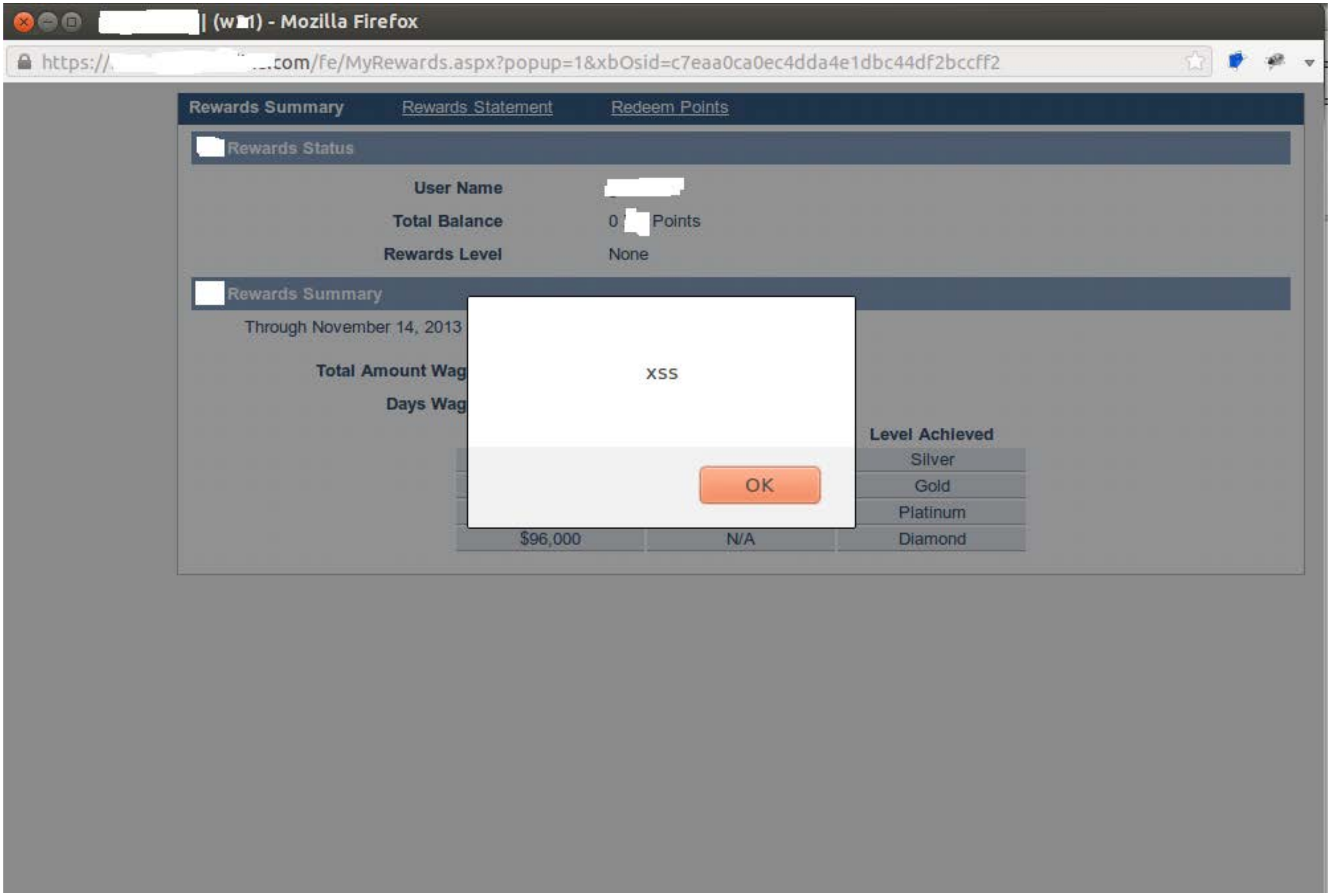
```
Dear Gus

You recently requested your            password.

Your username is:


Your password is:
password1

If you did not make this password request, or if you have any questions regarding your account,          Customer Servi
   > Phone - 866.         (866.         ) from 10:30AM to 11:00PM Eastern Time
   > Email - customerservice@ .       .com


Thank you and best of luck betting the races!

Sincerely,

The             Team
              Road,
            , PA
P: 866..
F: 866.
```

Cross-site Scripting (XSS)



```
GET /fe/MyRewards.aspx?popup="><script>alert('xss')</script>1&xb0sid=c7eaa0ca0ec4dda4e1dbc44df2bccff2 HTTP/1.1
Host: '                    com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:25.0) Gecko/20100101 Firefox/25.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://                  .om/fe/main.aspx?xb0sid=c7eaa0ca0ec4dda4e1dbc44df2bccff2
Cookie: tzo_0=300; _csh=c7eaauca0ec4dda4e1dbc44df2bccff2
Connection: keep-alive
```

Cross-site Scripting (XSS)



[redacted] | (w[redacted]) - Mozilla Firefox

https://[redacted].com/fe/MyRewards.aspx?popup=1&xbOsid=c7eaa0ca0ec4dda4e1dbc44df2bccff2

[redacted] Rewards Status

User Name	[redacted]
Total Balance	0 [redacted] Points
Rewards Level	None

[redacted] Rewards Summary

Through November 14, 2013

Total Amount Wag

Days Wag

xss

		Level Achieved
		Silver
		Gold
		Platinum
$96,000	N/A	Diamond

SeNet

Conclusion

- This introduction presentation just touched on some of the security issues that the Online Racing Industry need to take into account.

- All examples used were discovered via passive analysis, no active or scanning was performed on sites.

- Less than a few hours were used to locate these “low-hanging” vulnerabilities, certainly more exist.

- During the rest of this panel discussion we will dive deeper into some of these attack vectors and others that you need to be aware of.